Mansaf Alam
Kashish Ara Shakil
Samiya Khan *Editors*

Internet of Things (IoT)

Concepts and Applications

Springer

Internet of Things (IoT)

Mansaf Alam • Kashish Ara Shakil
Samiya Khan
Editors

Internet of Things (IoT)

Concepts and Applications

Springer

Editors
Mansaf Alam
Department of Computer Science
Jamia Millia Islamia
New Delhi, India

Samiya Khan
Department of Computer Science
Jamia Millia Islamia
New Delhi, India

Kashish Ara Shakil
College of Computer & Information Science
Princess Nourah bint Abdulrahman University
Riyadh, Saudi Arabia

ISBN 978-3-030-37467-9 ISBN 978-3-030-37468-6 (eBook)
https://doi.org/10.1007/978-3-030-37468-6

This Springer imprint is published by the registered company Springer Nature Switzerland AG.
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The emergence and rise of the Internet of Things (IoT) promises to revolutionize the way humans lead their lives by connecting all the devices that we possibly use to a common network, the Internet. Some of these devices include sensors, home appliances, health monitoring devices, and any device that produces quantifiable data. This concept has given birth to unlimited application areas that use the interactions between humans and devices to build inferences and make predictions for improving the quality of life and optimizing the use of existing resources.

A recent survey of McKinsey has shown that the number of deployed IoT devices is expected to reach one trillion by 2025. Moreover, the economic impact of this technology on the world economy can be assessed from the fact that it is expected to capture 11% of the same by the end of 2025. With that said, Internet of Things, as a technological paradigm, suffers from several challenges that must be addressed before its vision can be realized.

Some of the evident challenges include identification and development of architectures that can meet the scalability requirements of the IoT ecosystem. Data and resource management along with the need to maintain the security and privacy of the system also remain prevalent, in addition to several others. All the devices that fall under the umbrella of the Internet of Things are commonly referred to as smart devices. Therefore, the concept of IoT acquires and integrates data from these smart devices. Furthermore, this data is stored and processed to generate useful analytics.

The vision of IoT is to visualize the world as a collection of connected entities. The most obvious application of such a paradigm is smart city as the connected nature of the city is expected to make resource management simpler. Among other applications of IoT, healthcare and infrastructure management are frontrunners because of their need for real-time solutions in critical scenarios. In addition, there are a plethora of applications that can be developed and commercialized for human use.

The objective of this book is to explore the concepts and applications related to the Internet of Things with the vision to identify and address existing challenges. Besides this, it shall also provide future research directions in this domain. This book is meant for students, practitioners, industry professionals, researchers, and

faculty working in the field of Internet of Things and its integration with other technologies to develop integrated, comprehensive solutions to real-life problems.

Part I introduces the basic concept of the Internet of Things and provide an insight into other parts of the book and what they are expected to cover. In order to implement Internet of Things solutions, the architecture must support the specific requirements of such applications. These requirements include scalability, transition from closed platforms to open platforms, and designing of protocols for interaction at different levels. This part also covers the architectural issues and available solutions related to IoT.

Once the architectural issues are discussed and elaborated upon, the next part is expected to cover the solutions available in this domain for elemental IoT processes like data and device management. The heart of the IoT ecosystem is a smart device and the programming framework that uses the data made available by the smart device to create useful insights. Part II covers components that allow development of solutions and applications using the IoT paradigm.

The concept of the Internet of Things has just hit the shore. There are a number of challenges and limitations that need to be mitigated to make this technology workable and usable across diverse domains. Some of the identified challenges include security, robustness, reliability, privacy, identity management, and designing of management policies to ensure smooth functioning. Part III covers the different aspects of IoT challenges and devised solutions for the same.

The emergence and growing popularity of the Internet of Things has given rise to the identification of many areas where it can be put to use. Some of the obvious applications of this paradigm include social computing, mobile computing, crowd sensing, and crowd sourcing. Part IV includes chapters that have implemented IoT to create applications for these domains.

Smart cities is the most popular application of IoT and uses the same in conjunction with other technologies like cloud computing and big data. Smart cities is a large domain of applications that include domains like healthcare, logistics, manufacturing, and agriculture, in addition to many others. Part V includes chapters that explore the different facets of smart cities and solutions created for the same.

Next-generation smart applications make use of many state-of-the-art technologies like machine learning, computer vision, and artificial intelligence in conjunction with the Internet of Things (IoT). Moreover, deep learning has also found many integrative applications with IoT. These applications are popularly termed as cognitive IoT applications and promise to serve a wide range of areas and domains like healthcare, logistics, smart cities, and supply chain, in addition to many others. Part VI elaborates on the concepts and applications related to cognitive IoT analytics and its applications.

New Delhi, India — Mansaf Alam
Riyadh, Saudi Arabia — Kashish Ara Shakil
New Delhi, India — Samiya Khan

Acknowledgments

The making of this book is a long journey that required a lot of hard work, patience, and persistence. We wish to express our heartfelt gratitude to our families, friends, colleagues, and well-wishers for their endless support throughout this journey.

We would particularly like to express our gratitude to Mr. A. P. Siddiqui, Registrar, Jamia Millia Islamia, New Delhi, for his constant encouragement. We would also like to thank Prof. Haroon Sajjad, Dr. Arshad Khan, Dr. Israr Ahmad, Dr. Khalid Raza, and Mr. Abdul Aziz for their unconditional support. Besides, we owe a deep sense of appreciation to other members of our research lab for their cooperation.

Lastly, we wish to acknowledge and appreciate the Springer team for their continuous support throughout the entire process of publication. Our gratitude is extended to the readers, who gave us their trust, and we hope this work guides and inspires them.

Mansaf Alam
Kashish Ara Shakil
Samiya Khan

Contents

Part VI Next Generation Smart Applications

Contributors

Preeti Agarwal Department of Computer Science, Jamia Millia Islamia, New Delhi, India

Salman Basheer Ahmed Department of Computer Engineering, Faculty of Engineering and Technology, New Delhi, India

Mansaf Alam Department of Computer Science, Jamia Millia Islamia, New Delhi, India

Syed Arshad Ali Department of Computer Science, Jamia Millia Islamia, New Delhi, India

N. Ambika Department of Computer Applications, SSMRV College, Bangalore, India

Ankit Anand Department of Information Science & Engineering, Ramaiah Institute of Technology, Bangalore, Karnataka, India

Manzoor Ansari Department of Computer Science, Jamia Millia Islamia, New Delhi, India

Navneet Arora Department of ME, IIT- Roorkee, Roorkee, Uttarakhand, India

Lakshita Bhargava Computer Science & Engineering Department, Maharaja Agrasen Institute of Technology, Guru Gobind Singh Indraprastha University, New Delhi, Delhi, India

Senad Bušatlić International University of Sarajevo, Sarajevo, Bosnia and Herzegovina

Akshay Chamoli Department of Computer Science, Jamia Millia Islamia, New Delhi, India

D. K. Chaturvedi Department of Electrical Engineering, DEI-Agra, Agra, Uttar Pradesh, India

Suchismita Chinara National Institute of Technology, Rourkela, Odisha, India

Sakshi Dhall Department of Mathematics, Jamia Millia Islamia, New Delhi, India

Department of Computer Science & Engineering, Delhi Technological University, New Delhi, India

Subha P. Eswaran CRL, Bharat Electronics Limited, Bangalore, Karnataka, India

Elias Eze Department of Computer Science and Technology, University of Bedfordshire, Luton, UK

Joy Eze Department of Computer Science and Technology, University of Bedfordshire, Luton, UK

Zameer Fatima Computer Science & Engineering Department, Maharaja Agrasen Institute of Technology, Guru Gobind Singh Indraprastha University, New Delhi, Delhi, India

Xiaohua Feng Department of Computer Science and Technology, University of Bedfordshire, Luton, UK

Disha Garg Department of Computer Science, Jamia Millia Islamia, New Delhi, India

Lakshay Grover Department of Computer Science, Christ University, Bangalore, India

Hina Gupta Department of Electrical Engineering, Jamia Millia Islamia, New Delhi, India

Mayank Gupta IT Consultant, TCS, Noida, Uttar Pradesh, India

Sachin Kumar Gupta Department of Electronics & Communication, Shri Mata Vaishno Devi University, Katra, Jammu, India

Abid Haleem Department of Mechanical Engineering, Faculty of Engineering and Technology, Jamia Millia Islamia, New Delhi, India

Nabeela Hasan Department of Computer Science, Jamia Millia Islamia, New Delhi, India

B. M. Jabarullah Pusa Institute of Technology, New Delhi, India

R. Kavitha Department of Computer Science, CHRIST (Deemed to be University), Bangalore, India

Mohd Imran Khan Department of Mechanical Engineering, Faculty of Engineering and Technology, Jamia Millia Islamia, New Delhi, India

Shahbaz Khan Department of Mechanical Engineering, Faculty of Engineering and Technology, Jamia Millia Islamia, New Delhi, India

Ahmed Khattab Electronics and Electrical Communications Engineering Department, Cairo University, Giza, Egypt

Fekher Khelifi Laboratory of Electronics and Microelectronics, University of Monastir, Monastir, Tunisia

V. B. Kirubanand Department of Computer Science, Christ University, Bangalore, India

Alok Kumar Computer Science & Engineering Department, Maharaja Agrasen Institute of Technology, Guru Gobind Singh Indraprastha University, New Delhi, Delhi, India

Deepak Kumar Amity Institute of Information Technology, Amity University, Noida, India

Rajendra Kumar Jamia Millia Islamia, New Delhi, India

Ranjit Kumar National Institute of Technology, Rourkela, Odisha, India

Anjali Kumari College of Engineering Roorkee, Roorkee, Uttarakhand, India

Enjie Liu Department of Computer Science and Technology, University of Bedfordshire, Luton, UK

S. R. Mani Sekhar Department of Information Science & Engineering, Ramaiah Institute of Technology, Bangalore, Karnataka, India

Kamta Nath Mishra Department of Computer Science & Engineering, Birla Institute of Technology, Ranchi, Jharkhand, India

Tabish Mufti Department of Computer Applications, Faculty of Computer Science and System Studies, Mewar University, Chittorgarh, Rajasthan, India

Srinivas Narasegouda Department of Computer Science, Jyothi Nivas College (Autonomous), Bengaluru, Karnataka, India

Neha Department of Computer Science and Engineering, School of Engineering Sciences and Technology, Jamia Hamdard, New Delhi, India

P. K. Nizar Banu Department of Computer Science, CHRIST (Deemed to be University), Bangalore, India

Saibal K. Pal Scientific Analysis Group, DRDO, New Delhi, India

Shabir Ahmad Parah Department of Electronics and Instrumentation Technology, University of Kashmir, Srinagar, India

Bina Patro University of Berhampur, Berhampur, Odisha, India

Joy Paulose Department of Computer Science, Christ University, Bangalore, India

Šemsudin Plojović Department of Computer Sciences, University of Novi Pazar, Novi Pazar, Serbia

Rachana Subbaiah M Department of Computer Science, CHRIST (Deemed to be University), Bengaluru, Karnataka, India

Mamoon Rashid School of Computer Science & Engineering, Lovely Professional University, Jalandhar, India

Rohit Rastogi DEI Agra, Agra, India
ABESEC, Ghaziabad, Uttar Pradesh, India

Amrit Sahani Siskha 'O' Anusandhan University, Bhubaneswar, Odisha, India
Institute of Technical Education and Research, Bhubaneswar, Odisha, India

Nahid Sami Department of Computer Science and Engineering, School of Engineering Sciences and Technology, Jamia Hamdard, New Delhi, India

Paul Sant Department of Computer Science and Technology, University of Bedfordshire, Luton, UK

Muzafer Saračević Department of Computer Sciences, University of Novi Pazar, Novi Pazar, Serbia

Santosh Satya Department of Rural Development, IIT-Delhi, New Delhi, India

Kapil Sharma Department of Information Technology, Delhi Technological University, New Delhi, India

Vinita Sharma New Delhi Institute of Management, New Delhi, India

Mitul Shukla Department of Computer Science and Technology, University of Bedfordshire, Luton, UK

G. M. Siddesh Department of Information Science & Engineering, Ramaiah Institute of Technology, Bangalore, Karnataka, India

Jamshed Siddiqui Department of Computer Science, Aligarh Muslim University, Aligarh, India

Parul Singhal DEI Agra, Agra, India
ABESEC, Ghaziabad, Uttar Pradesh, India

Shahab Saquib Sohail Department of Computer Science and Engineering, School of Engineering Sciences and Technology, Jamia Hamdard, New Delhi, India

Anjaneya Tiwari Department of Information Science & Engineering, Ramaiah Institute of Technology, Bangalore, Karnataka, India

Himani Tyagi Jamia Millia Islamia, New Delhi, India

Ummesalma M Department of Computer Science, CHRIST (Deemed to be University), Bengaluru, Karnataka, India

Aabid Rashid Wani Department of Electronics & Communication, Shri Mata Vaishno Devi University, Katra, Jammu, India

Nouran Youssry Electronics and Electrical Communications Engineering Department, Cairo University, Giza, Egypt

Zaheeruddin Department of Electrical Engineering, Jamia Millia Islamia, New Delhi, India

Sijing Zhang Department of Computer Science and Technology, University of Bedfordshire, Luton, UK

Part I
Internet of Things (IoT) Architecture

Chapter 1
Foundation of IoT: An Overview

Zaheeruddin and Hina Gupta

Abstract The advancement in technology has depreciated the size of the gadget by leaps and bounds during the last few decades. The usage and dependence of human beings on electronic gadgets has grown exponentially with the passage of time. The substantial scaling of such kind of devices gave birth to a new technology called 'Internet of Things' (IoT) in the year 1999. The concept of IoT adheres to the need of round the clock and ubiquitous connectivity. It provides means for establishing interconnectivity and interactions between such devices. IoT has carved out the path for new innovations leading to novel type of communication among humans and things. The interactions would enable the realization of services utilizing these resources for improving the quality of life. This chapter is an attempt in this direction with the basic introduction of IoT, basic architectures, challenges and the plethora of services provided by IoT.

Keywords Internet of Things (IoT) · Smart objects · IoT architecture

1.1 Introduction

The modern living trends of the society have turned out to be addictive to 24 × 7 connectivity. In order to provide this round the clock connectivity, the notion of 'Internet of Things (IoT)' came into existence after a gap of almost four decades following the invention of Internet. Internet can be defined as a massive pool of applications and protocols built on top of network of computers (Cohen-Almagor 2011). In today's era, ubiquitous computing and seamless connectivity is no more a challenge. Earlier the concept of connectivity was restricted to the interactions between humans and machines. But gradually with the advancement in technology of connectivity, today one can relate connectivity between anything as in IoT. The most important feature of IoT is that it can transform an object into smart object by providing sensing, actuating, computing and communicating capability to the object

Zaheeruddin · H. Gupta (✉)
Department of Electrical Engineering, Jamia Millia Islamia, New Delhi, India
e-mail: zaheeruddin@jmi.ac.in

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_1

(Sadiku et al. 2018). The huge workspace for IoT is fueled by the smooth integration of the technologies like digital electronics, microelectromechanical system and nanotechnology etc. (Bello and Zeadally 2015). The functionality of the objects and technologies together provide an environment where the sharing of the information can be carried out across the varied platforms. IoT is carving out its path in all the domains and is on the verge of becoming Internet of Everything (Miorandi et al. 2012).

The term "Internet of Things" was first coined by Kevin Ashton with contextual reference to supply chain management in the year 1999 (Kevin 2010). The term was further redefined by various researchers to include applications like transport, mining, healthcare, and utilities etc. The tenure which marks the emergence of IoT is stated to be during 2008–2009. In this period, the human populace began to be eclipsed by network allied devices. With the passage of time the number of linked "things", which included human and gadgets showed exponential escalation. This carved out the necessity for "Internet of Things". IoT can be defined as the usage of internet that bridges the gap between varied services and things including humans (Singh et al. 2014). As per the conceptual framework of 2020, IoT can be expressed in terms of mathematical language as (Alhafidh and Allen 2016).

$$IoT = \text{Sensor} + \text{Network} + \text{Data} + \text{Services}$$

IoT can be treated as the extension of the contemporary internet services to enclose each existing object. These objects can be living or non living thing which can appeal for a service or offer a service. This global connectivity has been possible by embedding sensors, actuators, microcontrollers etc. in the things, which facilitates the Internet to become more persistent. The miniaturization and advancements in the field of electronics and computers has made the materialization of IoT visible in many fields during the last few years. Some major applications of IoT are depicted in Fig. 1.1.

1.2 Historical Development

Communication has been an integral part of our day to day life. It can be defined as the transmission of information from one entity or object (sender) to another entity or object (receiver) with the help of some medium. In the early age, smoke signals, drum beats, chirping of birds, waving of handkerchiefs or flags were used as means of communication. Some other modes of communication were pigeons, hydraulic semaphore system, chain of beacons at the hilltops etc. Later electric telegraph came into existence in 1816 followed by the communication of audio messages using telephone in 1870s. In order to improve the range of communication, the invention of radio waves was made in 1880s**.** With the novel inventions of different modes of communication, the use of radio and televisions for communication was termed as 'Telecommunication' (Cohen-Almagor 2011; Leiner et al. 2009). The word

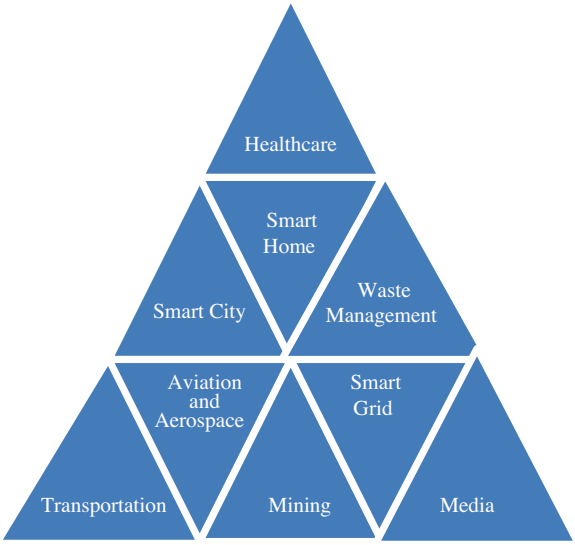


Fig. 1.1 Domains supported by IoT. (Alhafidh and Allen 2016)

Telecommunication consists of two words, *tele* means 'from far distances' and *communication* means 'to share information'. In other words it means communication at a distance. The next innovation in this field highlighted in the late 1890s in the form of Fax (facsimile). This mode of communication helped in the transmission of scanned printed material over the telephone connected to printers or some other input device. This was also called telecopying. It worked by scanning the original document with the fax machine. The machine processed the contents of both image and text in the form of a single fixed graphic image. This image was converted into a bitmap and transmitted in the form of audio-frequency tones through the telephone system. The receiving fax machine interpreted the tone and reconstructed the image by printing it on the paper. In 1940, the concept of a better mode of communication came into existence, where some calculations were done on one computer and the result was displayed on the other remote computer. This concept of a main computer and the other connected remote computers became popular in 1950s. Later in 1960s, researchers were on toes and investigated a new technology called packet switching. Packet switching breaks the data into small chunks and sends it to different computers. This differed from the previous means of communication as it would not pass the data through a centralized mainframe system. However, it was not until the personal motive of Department of Defense's Advanced Research Projects Agency (ARPAnet) that the concept of 'networking' came into existence (Leiner et al. 2009). In this project, a network of military computers was formed for communication in order to survive a disastrous nuclear attack. This small network of defense computers laid the first stone of the world of INTERNET.

In the next phase of development around 1970s, protocols were designed to connect devices to the network of computers. This protocol was termed as the Transmission Control Protocol and Internet Protocol (TCP/IP). This protocol

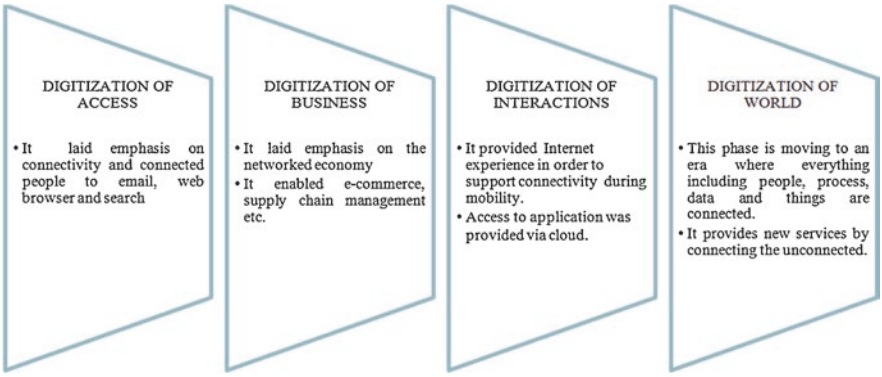


Fig. 1.2 Evolutionary phases of the internet. (Perera et al. 2014)

offered standards stating how the transmission could be carried out in a network of computers. The paradigm then shifted towards the concept of network of networks. Finally, the term 'Internet' was coined by Vinton Cerf, Yogen Dalal and Carl Sunshine in 1974 (Cohen-Almagor 2011). Internet can be interpreted as an union of two terms 'Inter' and 'net', meaning network between devices. Internet can be defined as the global connection of computer networks that transmits data using TCP/IP. The popularity of internet grew slowly and steadily as it digitized access, digitized business, digitized world and finally is digitizing everything including people, process and things as shown in Fig. 1.2.

1.3 Internet of Things (IoT)

Internet of Things endeavors to provide an epoch wherein digital and physical entities will be able to seamlessly communicate to provide a new domain of applications and services**.** Many applications and features we use these days prove as an ascending wave in the computing era. In the imminent time, the Internet will have its existence as flawless connection of objects and network. IoT can well be explained by a Venn diagram as shown in Fig. 1.3, where two different sets namely Information Technology (IT) and Operational Technology (OT) unite to form Internet of Things.

The IT domain consists of 'things 'like servers, databases and applications. These 'things' run on the network and are controlled by IT. IT assists secure connectivity of the data and gadgets for smooth flow within the vicinity of an organization. On the other hand, OT is generally concerned with the industrial work and contains 'things' like sensors and devices connected to the machines or some other equipment. It supervises devices and processes on physical systems (Perera et al. 2014). These systems incorporate industries, roadways systems, production services etc. Prior to the existence of IoT, the concept of IT and OT were considered to be

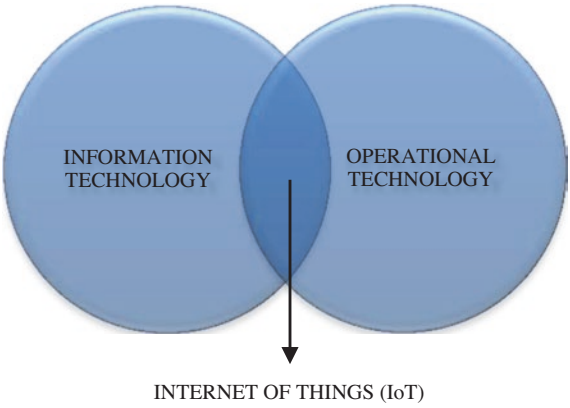


Fig. 1.3 Venn diagram

poles apart that worked independently and had little requirement to interact with each other. IoT has changed this paradigm to some extent and is still working in order to collaborate IT and OT into a single concept. The concept of IoT focuses on an interconnected world in which every "thing" is connected to any "thing".

The obligatory part of IoT is to provide smart association with the in-use network and context-aware computations using network assets (Singh et al. 2014). Some requisites for achieving the stated motives are: (a) a mutual discernment of the circumstances of the gadgets and their associated users, (b) the investigative tools that seek for autonomous and smart actions, and (c) software architectures and pervasive communication networks to process and convey the contextual information to where it is relevant.

Internet is the actual backbone that has carved out the path for ubiquitous computing. It enables inter device communication across the globe. The two basic pillars for the growth of ubiquitous computing are: Internet of Things and Cloud Computing. Cloud computing provides reliable service by providing virtual storage and computing zone for processing. On the other hand, Internet of Things provides a seamless connectivity between objects using RFID, which provides a unique code to each and every object (Chemudupati et al. 2012). All the work carried out in the background of IoT and cloud computing are completely hidden from the user. The smart environment consisting of the sensor-actuator-internet framework has given rise to a common operating picture (COP), where the generated data and information is efficiently shared across varied platforms and applications. Internet of Things is a shift towards ubiquitous computing evolved due to the presence of Wi-Fi and ad hoc wireless networking. However, for the successful and widespread use of Internet of Things, networking exemplar has to step out of its boundary of mobile computing.

There are ample of technologies that exist and some that are about to spring up to interconnect the devices. The foremost goal of Internet of things is to make the environment intelligent. The existence and functioning of IoT environment is possible due to the concept of digital electronics, microelectromechanical system and nanotechnology etc. All the said technologies converge to provide the ability of

capturing data, providing connectivity, computing and storing data for usage. The sensors, actuators, RFID, Bluetooth and Wireless Sensor Network etc. are embedded into physical items to turn them into 'SMART' objects thus leveraging the connectivity amongst the actual and implicit realms (Yassein et al. 2017). Context related computations and well tuned connectivity with existing networks are the prime requisites for the IoT. As humans use Internet to communicate, the "smart things" use the Internet of things to communicate. Eventually, the quantity and quality of data collected and analyzed to land up to a solution determine the smartness of the object.

1.4 Smart Object

In the late 1980s, tremendous efforts were made by the researchers to use technology as a bridge for human-to-human communication. As a result, the concept of ubiquitous computing came into existence. The major motive of ubiquitous computing was to embed technology in order to cater the everyday needs of public. In today's era of smart phones and other handheld or pocket devices, the environment has turned out to be more interactive and informative. The focus of the interaction has shifted to smart communication. A communication is smart if it is between anything that is capable of judging its context and state. Smart communication is only possible if the environment is also smart. According to Mark Weiser, smart environment is an environment containing heterogeneous combination of objects embedded with sensors, actuators, computational capability, display area which are seamlessly connected through a network (Mühlhäuser and Gurevych 2010; Bohn et al. 2003). The implications that came out from the early studies conducted by Weiser were that any physical object is smart if it acts as the source of digital information.

Marcelo Kallman and Daniel Thalmann introduced the concept of smart object (Kallmann and Thalmann 1999). They termed an object as smart object if it is capable of describing its own possible interactions. These objects have the ability of sensing, computing and communicating wirelessly both in short distance and long distance. The resemblance of smart objects and IoT can be understood by the fact that the basic building block of human body is cell. Each cell performs its operation and assists in the good functioning of the body. In a similar manner, smart objects act as the basic building block of IoT which combine to form a smart network. Each smart object assists in the formation of a network where a lot of data or information can be gathered, processed and analyzed. With strong affirmation it can be said that the real strength of IoT comes from the transformation of an isolated ordinary object into interactive smart object. The synonyms widely used for smart object are IoT device, smart device, intelligent device, intelligent node etc.

1.4.1 Characteristics of Smart Object

Any object or device can be categorized as smart object if it possesses certain characteristics. The Smart Object consists of Sensors/Actuators, Memory, Communication Device, Power Source, and Processing Unit as shown in Fig. 1.4. The detailed description of each component is given below:

1. **Sensors:** As the name implies, sensors are used for sensing. A human body has five sense organs. The sense organs are responsible for interacting with the environment. The sensing performed by sense organs may be visual sensing, physical sensing or audio sensing. As soon as something is sensed, a message is send to the brain which in turn takes some decisions. In a similar manner, sensors embedded in the device helps the smart object in sensing and measuring the changes in the environment. This physical quantity when measured is converted into digital representation. This digital representation is then passed onto some other computational unit where the transformation of data is done so that it can be used by other devices or humans as shown in Fig. 1.5 (El Jai and Pritchard 2007; Lannacci 2018; Pinelis 2017). A lot of sensors are available to measure various quantity and quality of the physical and virtual things in the environment.
2. **Actuators:** The sensors are used for sensing data. The data is collected from various sources and devices. This data is then processed, analyzed and needs to be used to produce some productive result. This sensed data now triggers the actuators. The actuators are complements to sensors as shown in Fig. 1.5. It receives control signal and produces some response to the physical

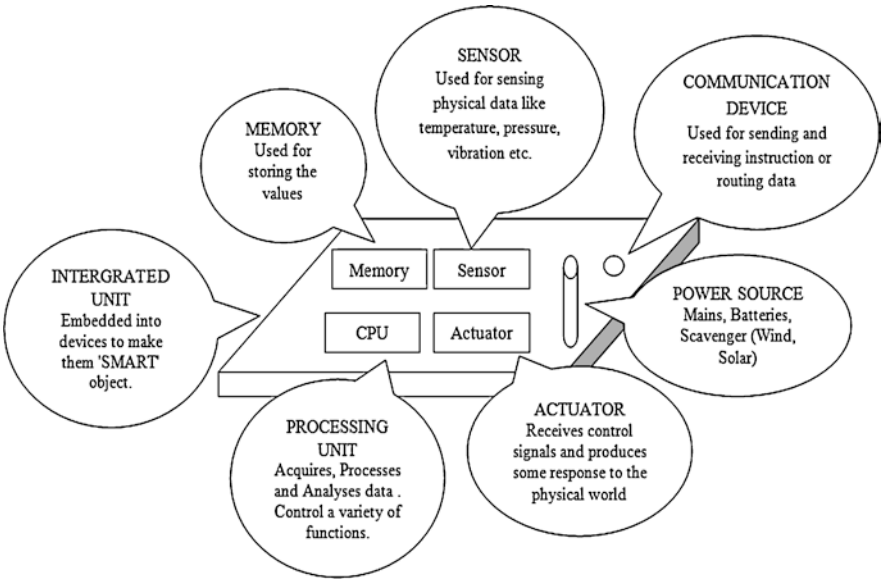


Fig. 1.4 Components of a Smart Object

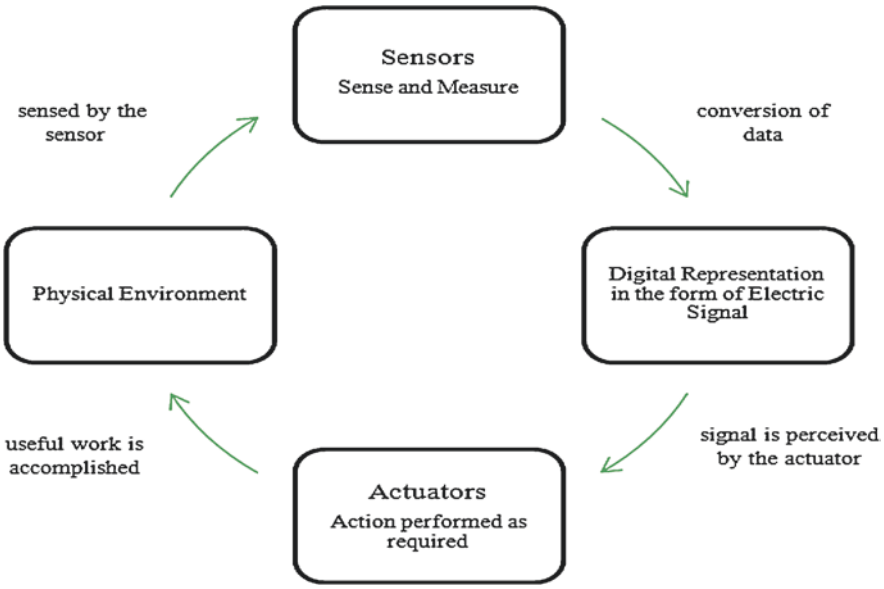


Fig. 1.5 Relationship between sensor and actuator

world (Anjanappa et al. 2002). In short we can say that sensors sense and send whereas actuators act and activate. A smart object may either have sensor or actuator or both and their number can vary from zero to multiple values depending on the requirement.

The relationship between sensors and actuators can be understood with a simple example. Suppose there is a water tank marked with a level. The water pump should be switched on as soon as the water reaches below the marked level. In order to design such a system both sensor and actuator will be employed. Sensor will sense the level of water in the tank. When the water level reaches the marked level, a notification message will be sent to the controller embedded into the system. At this point of time the controller will trigger the actuator to turn on the water pump. In short we can say that actuators are triggering device that converts energy into motions (Alhafidh and Allen 2016; El Jai and Pritchard 2007; Lannacci 2018). Actuators can generate rotary, linear or oscillatory motion. The actuators can be classified on the basis of various parameters.

In the context of IoT, switching on and off another device or equipment by the application of force is handled by actuator. IoT is an amalgamation of not only sensing and processing the data but also triggering varied devices into operation on the basis of the dynamics of data. Sensors and actuators that complement each other in terms of functionality work in collaboration to attain the maximum benefit from Internet of Things.

3. **Memory:** The interaction of smart object is not only limited to physical world objects but it also includes interaction with the virtual objects. A smart object

may have a physical existence and physical properties such as size, shape etc. or a virtual existence in the form of software objects. In both the cases, the smart objects should have a unique identifier. This identifier would be an address which would play a huge role in sending and receiving data. The existence of the smart objects also demands a possession of minimum communication and computation capability. This includes the ability to be discovered, accepting the incoming message and replying to them, discovering services and performing the tasks related to network management. All the above stated functions require a memory range from a few Kilobytes to Gigabytes as per the need. The memory helps in the storage of data. This data is then used for analysis, computations and decision making.

4. **Processing unit:** A smart object has a processing unit for gathering, processing and analyzing the data acquired from the sensors. The computations done call for control signals that prompt the actuator according to the need. Various functions of the smart object are controlled by the processing unit like communication and power system. The type of processing unit to be used can vary according to the needs and kind of processing to be used by the applications. Microcontroller is the most widely used processing unit due to its small size, simplicity of programming, less power consumption, flexibility and low cost.
5. **Communication unit:** All the smart objects need to communicate to each other for the sharing of information. This communication may take place between two or more smart objects or to the outside world through network. The communication is only possible if the smart object has a unit meant for communicating over a wire or wirelessly. The wireless connectivity is preferred more over the wired connectivity for various reasons like cost, ease of deployment and limitations associated with the infrastructure. The communicating unit follows a set of rules, generally termed as protocols to share the information across the network.
6. **Power source:** There are various components in a smart object. These components need power to operate. The different sources from which power can be attained are batteries, solar power, wind power, main supply etc. Communicating unit of a smart object accounts for the maximum power consumption. The requirements of power consumption vary greatly according to the scenarios like the area of deployment, switching between the active and sleep mode, accessibility, the power source being used (battery, solar or wind etc), area of application, criticality of the information etc. The different combination of scenarios or conditions calls for different selection of power source.

1.4.2 Trends in Smart Object

Smart objects show vast variability in their basic characteristics like technical requirements, functions, conditions of deployment etc. Today we can see and infer the macro trends in smart objects taking the world towards a planned smart future. Some major generalization and trends impacting IoT are:

1. **Decrease in size:** The size of the sensors are decreasing day by day, The process of miniaturization has excelled so much that in some cases the sensors are not visible from the naked eyes. A trend can be seen in the decrease in the size of the sensors. In general, the smart objects are embedded into everyday objects. The smaller size of the smart objects makes the process of embedding easier.
2. **Increase in the processing power:** With the passage of time the potential of processors has risen continuously and the size has reduced to a large extent. This advancement in the smart objects have made them more complex and connected.
3. **Declination in the power consumed:** A smart object comprises of different parts. These parts continuously consume power. The sensors may be active or passive. These days sensors are turning out to be completely passive having no requirement of the external power supply. On the contrary the battery powered sensors are also being designed in such a manner that they are able to last for many years without any need of replacement.
4. **Improvement in the communication capabilities:** A great improvement can be seen in the speed and range of communication provided by the wireless technologies. With the growth in the use of IoT network, more and more specialized communication protocols are being developed to support various applications and environments.

The stated trends in smart object provide ground for the development of sophisticated devices that are capable of performing complex task with increased efficiency. These trends have resulted due to improved inter-object and inter-system communication. The actual power of IoT is visible only when the smart objects are allied collectively in the network of sensors and actuators.

1.5 Features and Challenges of IoT

The term IoT relates to the increasing number of smart and linked entities that emphasizes on the innovative opportunities associated with them. Every entity is possessed with some attributes that makes it unique and different from others.The changing nature of the objects is the fundamental property that makes smart object different from other objects. The term ‘SMART’ in smart objects means that these objects are active, can work autonomously, can form a network, are reconfigurable and have a local control of the resources such as energy and data storage. Some major features and challenges associated with IoT are described below:

1. **Heterogeneity:** In IoT, various types of devices interact with each other to form a network. These devices are heterogeneous in terms of size, shape and functionality (Miorandi et al. 2012). They may include small sensors embedded in a pen to a huge gigantic machine installed in a factory. These devices have diverse capabilities from the view point of communication and computations. Mutual functioning and interaction of such devices in IoT is the most crucial barrier to be dealt with. It involves the interaction between IoT devices, gateway and cloud

(Alam 2012). The different data format generated also needs to be handled aptly (Malhotra et al. 2017). Therefore, the architectural models and protocols assisting the functioning of IoT should be managed efficiently to handle this heterogeneity.

2. **Scalability:** IoT is a huge network with an enormous amount of objects being connected to a global information infrastructure. The number of connected devices has increased many folds giving rise to the scalability issue in the IoT. For a proper communication to take place, a unique sender and receiver have to be recognized along with the identification of an appropriate path or channel. In order to identify the unique sender and receiver, a unique global identity should be provided to them. The IPv4 addressing (32-bit addressing) scheme used till date offers only 4,294,967,296 unique addresses. This count of addresses is not adequate for the future, where the count of IoT devices will outnumber the world's population (Gusmeroli et al. 2009) as given below in Table 1.1. The increase in the number of devices will also deteriorate the quality of communication due to an increased number of interconnections established amidst a large number of entities. The increase in the number of devices will also give rise to huge data which will demand for authentic sources to manage the data and information efficiently (Ali et al. 2019a).

3. **Ubiquitous exchange of data by means of proximity wireless technologies:** In the modern and imminent future, people are and will be addicted to instant access to data. Today's generation that have been termed as the always-online generation (AO Generation) will exhibit an eagerness for instantaneous gratification and quick fixes. In order to calm down this anxiety for access to anything, IoT will make the most use of wireless technologies. The wireless technology will enable the isolated, living and non-living objects to be networked together. This feature of wireless technology will provide immediate access to nearly the entirety of human knowledge, and incredible opportunities to connect, create and collaborate (Gubbi et al. 2013). The basic necessity for the wireless communication to take place is the availability of spectrum. For a wireless communication to take place, a wireless adapter is required. This adapter converts the data into radio signals. These radio signals are then transmitted with the help of an antenna and received by the wireless receiver. The transmission and receiving of data is only possible when the radio waves are able to travel form transmitter to receptor. The wireless spectrum, therefore works as a medium for the radio signals to travel. Thus, we can say that the wireless spectrum plays the role of oxygen in-

Table 1.1 Categorization of the installed base units (Millions of units) (Tung 2017)

Category	2016	2017	2018	2020
Consumer	3963.0	5244.3	7036.3	12,863.0
Business: cross-industry	1102.1	1501.0	2132.6	4381.4
Business: vertical specific	1316.6	1635.4	2027.7	3171.0
Grand Total	6381.7	8380.7	11,196.6	20,415.4

order to keep the network alive and provides it the capability to work at its full potential. The issue that arises with IoT is the availability of an appropriate spectrum. The requisite of the spectrum works as a as an obligation for the acceptance of dynamic/cognitive radio system.

4. **Solutions for optimizing the energy consumption:** The entities involved in the setting up the network for IoT vary from a small sensor in a handheld device to big sensors in factories. Some sensors work only when required and some may switch between active and sleep mode as required by the application. Many sensors may have the external power supply to work but many of them will be operated on the batteries. In the case of external power supply, communication and computation is a not a hindrance. But in the case, when sensors are battery operated, communication and computation prove to be an overhead. The constraints that are imposed by the operations of the battery are relieved to some extent by the technique of energy harvesting, but still since the energy will constantly be an inadequate source, it needs to be handled with care (Ali et al. 2019b). There arises need in IoT to devise solutions that tend to optimize energy usage (even at the expenses of performance) will become more and more attractive.
5. **Capability of being tracked and localized:** The term Radio Frequency Identification commonly known as RFID is extensively used in IoT. All the entities that are a part of IoT network need to be identified. This boon of being identified helps them to be tracked with the aid of applications and RFID tags embedded into the objects. RFID is a short range wireless communication technique that uses electromagnetic field for the detection and identification of the RFID tags attached to objects. These tags are then tracked and interrogated for detecting the location of IoT entities in the physical realm (Gubbi et al. 2013).
6. **Capability of being self-organized:** IoT is merely a network that is a mixed bag of static network and ad hoc network. The major difference that exists between both the networks is in terms of the stability of position of entities. In static network, the location of the physical existence of the object does not change frequently leading to stability in the network. On the other hand, the physical position of the entities involved in IoT often keeps changing, thus carving out the path for complexity. Here comes in the call for a self organizing network that is capable of being planned, organized and maintained on its own. The IoT network is an ad hoc network with intelligence distributed throughout the network. The objects involved in IoT are termed as smart object whose position and functions keep on changing. They are able to work autonomously by reacting to a varied range of different situation with minimum human intervention. As per the request of the user and the need of scenario, smart nodes in IoT arrange themselves autonomously into a short lived ad hoc network. Using this transient network smart nodes gain the capability to share data and perform tasks in coordination with each other. Abilities to execute service and device discovery, auto tuning to protocol behavior and adaptation to the current context without an external trigger are also included in the scenario discussed above.
7. **Semantic interoperability and data administration:** The increase in the number of objects being connected to IoT has given rise to huge bulk of data. This

massive quantity of data is exchanged and analyzed at infrequent short intervals. This collection of data is unstructured and lacks a standardized format, semantic description of the related content (Alam and Ara 2013; Shakil and Alam 2013). In order to make IoT a powerful network, this raw and unorganized data needs to be converted into useful information by eradicating all the above issues. This will enforce interoperability among different applications.

8. **Privacy conservation and enhanced security:** The rationale behind IoT is to provide connectivity between devices and the Internet. Since more devices are being connected potential risks of data breach, malware ingestion, digital burglary etc. gains momentum. The customers and enterprises are quiet apprehensive about security owing to occurrence of various attacks. The surveys and reports regarding the IoT security provide a clear status regarding the threat to the end user data. Due to the basic engrossment into the physical domain, the technology of IoT needs to conserve privacy and be secure by design (Alam et al. 2015). Therefore, the architecture designs, protocols and other methods for IoT solutions should consider security as a key facet to be taken into account. Breach of security in IoT is the sole reason which will setback the users from accepting and using the technology. Hence, security feature should be well placed in order to support wide adoption of IoT (Gandotra et al. 2017; Maple 2017).

The issues and remedies associated with the implementation of IoT has been represented in a simplified tabular form in Table 1.2.

Table 1.2 IoT key issues and requisites needed

S.No.	Challenge	Requisite
1	Heterogeneity	Special concern should be shown towards the architectural models and protocols in order to support various devices and data generated by them.
2	Scalability	A huge address space should be provided so that unique identification of each entity is possible
3	Ubiquitous exchange of data by means of proximity wireless technologies	An appropriate spectrum should made available for ubiquitous data.
4	Solutions for optimizing the energy consumption	Designing of IoT devices and solutions that minimize the energy usage.
5	Capability of being tracked and localized	Employment of RFID tags, DSRC or any other short range communication
6	Capability of being self-organized	The node should be able to execute service, device discovery, auto tuning to protocol behavior and adaptation to the current context without an external trigger.
7	Semantic interoperability and data administration	Quick conversion of raw and unorganized data from various sources into useful information.
8	Privacy conservation and enhanced security	The architecture designs, protocols and other methods for IoT solutions should consider security as the prime feature.

1.6 IoT as an Industrial Commodity

Although the concept of IoT is not new, its perception and handling varies from industry to industry. The efficiency of every company is analyzed by their new products in the market. In order to develop the product, projects are undertaken by the industries. In different phases of the project, knowledge, skills, tools and techniques are applied to accomplish the goals in well defined tenure. In case of an IoT project, the completion of such project comprises of effective handling of data and keeping a tab on the scope of high complex systems. The complexity of system is expressed in terms of number of things, velocity of the generation of data, volume of the data generated, geography, diversified manufacturers and analytics. It is observed from the literature survey that no two implementations of the IoT project are same. The reason for this discrepancy lies in different architectures of IoT that are used by the industries. The basic five steps required in any IoT project are shown in Fig. 1.6.

1. **Linkage of Objects:** The first essence of an IoT system is to connect to different objects such as devices, machines or sensors. On the establishment of connection, the generated data can be collected. The generation of data can vary from application to application. Data may be generated at every small change or event, or periodically. The tenure in which the data is collected will influence the volume of data gathered.
2. **Collection of data:** The second essence in the project is to capture the generated data. The data collected in the previous stage is required to be sent to the next stage comprising of centralized data centre or cloud. Immediate or predictive

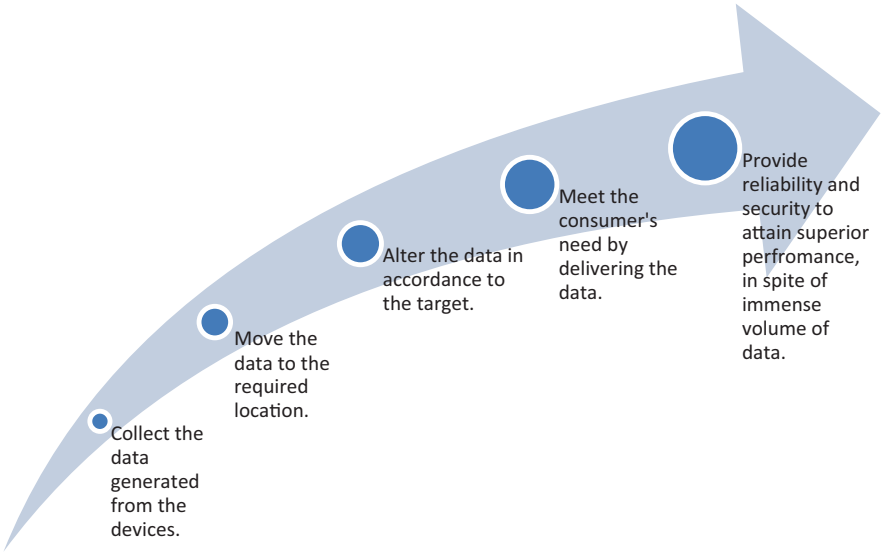


Fig. 1.6 Steps in an IoT project

analysis of data can be carried out at the cloud. If required, data may be ported to the main application for further analysis.

3. **Transformation of data:** As the data is in progression in the third stage, normalization and modification is performed on the data. This modification is done to customize the data as per the application. Various operations that take place in this stage are buffering of data, filtering of data, aggregation and compression of the data. The reduced and useful data is now sent to the next stage of delivery.
4. **Delivery of data:** The reduced and transformed data is ready for delivery at this stage. Delivery of data is made to the target end points, applications and analytics platform. The prime requisite for delivery is to eradicate any loss of data. Any three mechanisms namely request-reply, message based or publish-subscribe can be used for delivering the data. Transmission Control Protocol (TCP), Hyper Text Transfer Protocol (HTTP) or Web Sockets can be used as transport interfaces by the message routers. The transport interfaces can provide messaging infrastructure for communication.
5. **Management of data:** The data obtained from the above said stages can now be consumed by the companies. This transformed and reduced data can help the companies to increase their efficiency, reduce risk, predict services and support that they can provide. The data across the IoT system is needed to be controlled and synchronized reliably. This would incorporate managing the network, connectivity of the devices, application provisioning and automation (Khan et al. 2015). A huge volume of data will flow amongst the devices thus having the need for high security. Therefore every enterprise would need to adhere to the strict rules and regulations in this regard.

1.7 Applications

A lot of potential is hidden in the network of IoT which makes the development of numerous applications possible. Many applications can be developed and deployed on the basis of IoT. As the saying goes 'Rome was not built in a day', similarly advancements take time. It is step by step process in which development plans can be easily made but the deployment of it takes time (Agarwal and Alam 2018). In this section many applications of IoT have been highlighted. Some common and significant applications of the IoT are briefly discussed below:

1. **Aerospace and aviation industry:** Counterfeit products and elements can easily be identified with the help of IoT. This can improvise the safety and security of products as well as services. For instance, the industry of aviation is susceptible to the issue of the unapproved part of aircraft that is commonly known as Suspected Unapproved Parts (SUP) (Sletten 2000). There is no assurance of the fact that SUP copes up to the necessities of a standard aircraft part and may lack behind in confirming the stringent limitations of quality of the aviation industry. Thus, security standards with respect to the aircraft are seriously violated

by the SUPs. The authentication and security of the aircraft parts can be easily be infringed by forging the documents. Solution to this problem is to introduce electronic pedigrees. These electronic pedigrees will work for a limited group of aircraft parts. In order to improve the safety and operational reliability of aircrafts, the aircraft parts in their lifecycle, will make a record of their origin and critical security related events. These pedigrees will then be stored and secured within RFID tags and a decentralized database. The RFID tags will be attached to the parts. Whenever a new aircraft part has to be installed in the aircraft authentication can easily be done by verifying the digital signatures and comparing the RFID tags pedigree with the database. These steps can upgrade the safety and operational reliability of the aircrafts.

2. **Automotive industry:** A lot of up gradation can be seen in the automotive industry as generally all the means of transport are getting equipped with sensors, actuators etc. The installed sensors and actuators are known for their increased processing power (Szmelter 2017). Smart things are used for building and implementing the applications in the automobiles. The applications may monitor and report various parameters of the automobiles like proximity of the other vehicles, pressure in tyres etc. The RFID technology is being used to rationalize the production of vehicles, to improvise logistics, to enhance the quality control and improve customer services. The real time data in the manufacturing process and maintenance operations is provided by the RFID technology. This provides effective assistance in managing the product and the automobiles. In order to achieve high bit rate and reduction in the interference with the other equipment, Dedicated Short Range Communication (DSRC) is employed. The applications of the Intelligent Transportation System (ITS) which include traffic management and safety services of vehicle can fully be incorporated in the IoT infrastructure by using communications like Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication.
3. **Telecommunications industry:** The alliance between dissimilar technologies can be made possible with the help of IoT. This will work as the foundation for creating new services. An illustrative scenario for the above alliance is the mutual use of GSM, Bluetooth, Near Field Communication (NFC), Wireless Local Area Network (WLAN), Global Positioning System (GPS), multi-hop networks and sensor network with Subscriber Identity Module (SIM)-card technology (Deshpande et al. 2017). The different technologies stated above have significant features which help in the implementation of the services. In these services or applications the SIM-card is attached to the mobile phone. The mobile phone has the reader (i.e. tag) and different applications share the SIM-card. A secure and simple communication among objects can be enabled by the use of NFC. This is achieved by placing the objects in the vicinity of each other. In this scenario the mobile phone can read all the data by imitating as a NFC-reader. This data is then transmitted to a central server. The SIM-card in the mobile plays an important role by storing the authentication credentials like ID information, ticket numbers etc. and NFC data. For specialized purposes the robustness of the communication channel and networks can be

increased by facilitating peer-to-peer communication. In order to achieve it the 'things' can connect to form a network. An ad-hoc peer-to-peer network can also be formed to handle the situation of disaster or a condition of telecommunication infrastructure failures.

4. **Medical and healthcare industry:** There are many applications in the healthcare sector that can be framed by using the features of IoT. Monitoring the medical parameters and tracking the delivery of drugs can easily be done by using cell phones with RFID-sensor capabilities. Some of the advantages that can be achieved by using the said feature are: (a) monitoring of diseases can be made easy, (b) ad-hoc diagnosis can be done, and (c) instant medical aid can be provided in case of accidents. Health records can be saved and secured by using implantable and wireless devices. These health records can be used to save patient's life and special treatment can be given to people in emergency situation especially those suffering from heart disease, cancer, diabetes, stroke, cognitive impairments, Alzheimer's etc. Guided action on a body can be taken by introducing biodegradable chips into the human body (Machorro-Cano et al. 2017). Muscular stimuli can be delivered to paraplegic persons for restoring the movement functions. This can be attained by implanting a smart thing-controlled electrical simulation system.
5. **Pharmaceutical industry:** Safety and security of the pharmaceutical products are the prime requirements that need to be fulfilled for the effective use of the drug. Using the technique of IoT smart labels can be attached to the drugs. These smart labels enable the tracking and monitoring of the drug in the supply chain management. The status of the drug can be monitored providing many potential benefits. For instance, many products of pharmacy like vaccines and some drugs are required to be stored at a cool temperature. An appropriate maintenance of the cool chain can be monitored with the help of IoT. In case, if the required cool temperature is not maintained during storage or transportation, then the product can be discarded. The developing countries are affected by counterfeiting of the drugs. Drug tracking and e-pedigrees can be used in order to eradicate fraudsters and detect the counterfeit products (Fantana et al. 2013).
6. **Retail, logistics and supply chain management:** The operations of retailing and supply chain management (SCM) can benefit from IoT. Many applications can be optimized by the retailer by implanting RFID chips to the products and using smart ledges to follow up the availability of items in real time. For instance, automatic inspection of goods receipt, tracking the goods that are out of stocks, real time monitoring of the stocks and many such activities can be done by the retailer. It has been found that loss in sales is also detected when the customer does not find the required product in the shelves and returns back without the product. This loss of the retail store can be reduced with the help of IoT. Moreover, the logistics of the whole supply chain management can be optimized by providing the availability of data from the retail store. The availability of stock and sales data from the retailers will help the manufacturers to produce and dispatch the appropriate amounts of product. This will in turn

avoid the situation of over production or under production. The exchange of RFID data can prove beneficial to several sectors of industry by improvising the supply chain incorporating the logistic processes (Da Xu and He 2014).

7. **Environment monitoring:** Environmental monitoring and conservation can be considered as one of the booming segment in the market in the coming future. Identifiable wireless devices can be utilized for efficient monitoring of the environment. The monitoring may include scrutinizing of the weather condition, level of humidity, level of pollution etc.
8. **Transportation industry:** IoT has the capability of providing many solutions for improving the transportation industry. It can provide solutions for automatic toll and fare collection, thus reducing the traffic and waiting queues on road. With the help of IoT, the transportation system can be modified by the deployment of Intelligent Transportation System (ITS). ITS will help in the commuting of people and goods efficiently. It will monitor traffic jams and provide free pathways to emergency vehicles. It can also provide support and improve the security policies across the globe by providing means for the automatic screening of commuters and their baggage's boarding the cargo system (Skabardonis 2008).
9. **Agriculture and breeding:** A technology like IoT can be used to regulate the traceability of animals used for agriculture purpose. This can assist the detection of animals in real time especially during the eruption of infectious syndrome. In many countries farmers and shepherds are given subsidies as per the basis of the number of animals like cattle, goat, sheep etc. People can do fraud with the government by misleading them with the count of animals. The detection of such deceptions is a difficult task. Therefore, IoT can be employed to reduce the fraud as it can provide appropriate methods of identifications. Many other applications like conducting survey, controlling and prevention of diseases can easily be done by using varied features of IoT. IoT can be used to accurately identify the different specimens of blood and tissues and provide certification regarding the health status of animals in a region. The concept of IoT will also benefit the farmers as they can have a direct contact with the consumers. The farmers can then make direct deliveries of crop to not only smaller regions but also wide area markets. This will provide new way of supply chain and prove beneficial both for the producers and consumers (Maple 2017).
10. **Media, entertainment industry:** Online videos and news have become very common now days. An enhancement that IoT technology can show in this area is to deploy multimedia devices at different locations. Using these devices ad hoc news can be gathered on the basis of the location of the users. Financial offers can be provided to the people at these locations for collecting the footages. More information can be congregated by affixing the NFC tags to the posters. The tag readers are connected to a URI address possessing exhaustive details about the poster.
11. **Insurance industry:** The privacy of an individual is very important but IoT technology is considered as a serious hinder in maintaining it. But in order to avail the monetary benefits people are willing to compromise with their privacy.

Let's take an example of vehicle insurance which has been equipped with electronic recorders with the permission of their owners. The advantage of this recorder is that it can record dangerous driving pattern and communicate this information to the car owner or insurer. Similarly in case of house insurance, in-home sensors can monitor the water and fire damage and inform the insurer. The advantage of this kind of insurance is that the insurer can be informed of the imminent damages and can trigger the best possible economic action. Same kind of insurances can be provided on different assets like machinery, factories etc. The innovation provides cushion for maintenance at cheaper rates before the occurrence of the incident.

12. **Home Automation:** These days' people rely more on technology to address concerns regarding lifestyle led by them and security of their homes. The advancements in the technology of sensors, actuators and wireless sensor network are the main pillars behind the popularity of converting homes to smart homes. In smart homes, intelligent and automated services are provided to the user by the deployment of sensors at different locations. The smart sensors not only automate the day to day tasks of an individual but also help in energy conservation by switching off the electronic gadgets like fans, lights etc. when not in use. Energy conservation in smart homes is made possible by the use of sensors and the concept of context awareness. Different data like (temperature, light, humidity, fire event, gas etc.) are collected by the heterogeneous sensors and fed to the context aggregator. The aggregator passes on the collected data to the context aware service engine. On the contextual basis, different services are selected and the required task is achieved (Pal et al. 2018). For instance, an increase in the humidity level will switch on the AC automatically. A lot of modification in smart homes can be done as and when required.

1.8 Conclusion

The living standard in the modern society has moved to a different level by the emergence of Internet of Things. The Internet of Things has enabled communication amongst smart objects, contradicting the previous definition of interaction that was confined to the interactions amongst human and machines. In the present scenario, the term interaction encompasses communication between 'anything' irrespective of location, time and type of communication. This chapter introduces IoT as a combination of Information Technology and Operational Technology. IT supports protected connectivity of the data and gadgets within an organization whereas OT administers devices and processes on physical system. The new paradigm of IoT has shown an immense progress in digitization and has framed an aura where everything including people, process, data and things are connected. In order to assist the global connectivity of things new features have to be added to the existing objects and internet. The ordinary objects are upgraded to the smart object by integrating

communication and computation capability. The characteristics, trends and features of IoT objects have been covered in detail in the chapter.

Various types of project can be undertaken by IoT involving different inputs, attributes and solutions. Each project can follow a different architecture as per the requirement. In this chapter, two basic possible architectures namely oneM2M and IoT World Forum Architecture have been illustrated. The perception and handling of IoT can vary from industry to industry. Therefore, any IoT project should progress in a sequence employing and modifying the architecture as per the requirement. Each commodity provided by the industry will pave the path for new applications. Upcoming developments and growth in IoT will also optimize the flow of information thus revolutionizing private and business communications. The various applications of IoT are described in the last section of the chapter.

With firm determination it can be said that a lot good can be achieved in the field of IoT if the networking and communication research are carried out together in the laboratories of industries and academic institutions complementing each other.

References

Agarwal, P., & Alam, M. (2018). Investigating IoT Middleware Platforms for Smart Application Development. *arXiv preprint arXiv:1810.12292*, pp. 1–14.

Alam, M. (2012). Cloud algebra for handling unstrucured data in cloud database management system. *International Journal on Cloud Computing: Services and Architecture, 2*(6), 35–42.

Alam, M., & Ara, K. (2013). A decision matrix and monitoring based framework for infrastructure performance enhancement in a cloud based environment. In *International conference*, pp. 174–180.

Alam, B., Doja, M. N., Alam, M., & Mongia, S. (2013). 5-layered architecture of cloud database management system 5-layered architecture of cloud database management system. *AASRI Procedia*, *5*(January 2015), 194–199.

Alhafidh, B. M. H., & Allen, W. (2016). Design and simulation of a smart home managed by an intelligent self-design and simulation of a smart home managed by an intelligent self-adaptive system. *International Journal of Engineering Research and Applications, 6*(8), 64–90.

Ali, S. A., Khan, S., & Alam, M. (2019a). Resource-Aware Min-Min (RAMM) algorithm for resource allocation in cloud computing environment. *International Journal of Recent Technology and Engineering, 8*(3), 1863–1870.

Ali, S. A., Member, S., Affan, M., & Alam, M. (2019b). A study of efficient energy management techniques for cloud computing environment. In *International conference on cloud computing, data science & engineering*, pp. 13–18.

Anjanappa, M., Datta, K., & Song, T. (2002). Introduction to sensors and actuators. In R. Bishop (Ed.), *The mechatronics handbook* (pp. 1–15). Boca Raton: CRC.

Bello, O., & Zeadally, S. (2015). Intelligent device-to-device communication in the Internet of Things. *IEEE Systems Journal, 10*(3), 1–11.

Bohn, J., Coroam, V., Langheinrich, M., Mattern, F., & Rohs, M. (2003). Disappearing computers everywhere – Living in a world of smart everyday objects 1. In *New media, technology and everyday life in Europe* (pp. 1–20).

Chemudupati, A., Kaulen, S., Mertens, M., & Zimmermann, S. (2012, November). The convergence of IT and operational technology. *Atos Scientific Community* (pp. 3–16).

Cohen-Almagor, R. (2011). Internet history. *International Journal of Technoethics, 2*(2), 45–64.

Deshpande, P., Damkonde, A., & Chavan, V. (2017). The Internet of Things: Vision, architecture and applications. *International Journal of Computers and Applications, 178*(2), 1–14.

El Jai, A., & Pritchard, A. J. (2007). Sensors and actuators in distributed systems. *International Journal of Control, 46*(4), 1139–1153.

Fantana, N. L., et al. (2013). IoT applications – Value creation for industry. In *Internet of Things: Converging technologies for smart environments and integrated ecosystems* (pp. 153–206). River Publishers.

Gandotra, P., Kumar Jha, R., & Jain, S. (2017). A survey on device-to-device (D2D) communication: Architecture and security issues. *Journal of Network and Computer Applications, 78*(July 2016), 9–29.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660.

Gusmeroli, K., Haller, S., Harrison, M., Kalaboukas, K., Tomasella, M., Vermesan, O., & Wouters, K. (2009, April). Vision and challenges for realizing the internet of things. In *Cluster of European research projects on the Internet of Things* (Vol. 1, pp. 44–58).

Kallmann, M., & Thalmann, D. (1999). Direct 3D interaction with smart objects. In *ACM symposium on virtual reality software and technology* (pp. 124–130).

Kevin, A. (2010). That' Internet of Things' thing. *RFiD Journal, 22*, 97–114.

Khan, I., Naqvi, S. K., & Alam, M. (2015). Data model for big data in cloud environment. In *2nd IEEE international conference on computing for sustainable global development*, pp. 582–585.

Lannacci, J. (2018). Internet of things (IoT); internet of everything (IoE); tactile internet; 5G – A (not so evanescent) unifying vision empowered by EH-MEMS (energy harvesting MEMS) and RF-MEMS (radio frequency MEMS). *Sensors and Actuators A: Physical, 271*, 187–198.

Leiner, B. M., et al. (2009). A brief history of the internet. *Computer Communication Review, 39*(5), 22–31.

Machorro-Cano, I., Alor-Hernandez, G., Cruz-Ramos, N. A., Sanchez-Ramirez, C., & Segura-Ozuna, M. G. (2017). A brief review of IoT platforms and applications in industry. In *New perspectives on applied industrial tools and techniques* (pp. 293–324).

Malhotra, S., Doja, M. N., Alam, B., & Alam, M. (2017). E-GENMR: Enhanced generalized query processing using double hashing technique through MapReduce in cloud database management system. *Journal of Computer Science, 13*(7), 234–246.

Maple, C. (2017). Security and privacy in the internet of things. *Journal of Cyber Policy, 2*(2), 155–184.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of Things: Vision, applications and research challenges. *Ad Hoc Networks*, *10*(7), 1497–1516.

Mühlhäuser, M., & Gurevych, I. (2010). Introduction to ubiquitous computing. In J. Symonds (Ed.), *Ubiquitous and pervasive computing: Concepts, methodologies, tools, and applications* (pp. 1–19).

Pal, D., Funilkul, S., & Charoenkitkarn, N. (2018). Internet-of-Things and smart homes for elderly healthcare : An end user perspective. *IEEE Access, 6*, 10483–10496.

Perera, C., Liu, C. H., Jayawardena, S., & Chen, M. (2014). A survey on Internet of Things from industrial market perspective. *IEEE Access, 2*, 1660–1679.

Pinelis, M. (2017). *Sensors and electronics for the cockpit of the future*. Retrieved May 21, 2019, from https://www.smart-mobility-hub.com/sensors-and-electronics-for-the-cockpit-of-the-future

Sadiku, M. N. O., Tembely, M., & Musa, S. M. (2018). Internet of vehicles: An introduction. *International Journal of Advanced Research in Computer Science and Software Engineering, 8*(1), 11.

Shakil, K. A., & Alam, M. (2013). Data management in cloud based environment using k- median clustering technique. In *4th international IT summit confluence 2013 – The next generation information technology summit* (pp. 8–13).

Singh, D., Tripathi, G., & Jara, A. J. (2014, March). A survey of Internet-of-Things: Future vision, architecture, challenges and services. *2014 IEEE world forum internet things, WF-IoT 2014*, pp. 287–292.

Skabardonis, N. G. A. (2008). Real-time monitoring and control on signalized arterials. *Journal of Intelligent Transportation Systems, 12*(2), 64–74.

Sletten, S. J. (2000). Suspected unapproved parts in the aviation industry: Consideration of system safety and control. *The Journal of Aviation/Aerospace Education & Research, 9*(3), 11–16.

Szmelter, A. (2017). The concepts of connected car and internet of cars and their impact on future mobility. *Information Systems Management, 6*(3), 234–245.

Tung, L. (2017). *IoT devices will outnumber the world's population this year for the first time*. [Online]. Available: https://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/. Accessed 20 Mar 2019.

Xu, L. D., He, W., & Li, S. (2014). Internet of things in industries: A survey. *IEEE Transactions on Industrial Informatics, 10*(4), 2233–2243.

Yassein, M. B., Aljawarneh, S., & Masa'deh, E. (2017). A new elastic trickle timer algorithm for Internet of Things. *Journal of Network and Computer Applications, 89*, 38–47.

Chapter 2
Cloud Computing for IoT

Himani Tyagi and Rajendra Kumar

Abstract The Internet of Things (IoT) combined with cloud computing is an extensively stimulating technologies existing today. IoT is all about sensors, actuator, networks and widely distributed smart devices with limited storage and processing capability with prevalent security and privacy issues. Due to the communication between interconnected devices, the enormous amount of data generated in IoT often referred as Big Data that brings heaps of strain on the internet infrastructure. This has made organization to look for a solution or alternative to reduce this load and introduce cloud computing to solve this problem by providing on demand and virtual services like unlimited storage and processing power. These both technologies are inseparable and work in integration towards increasing the efficiency of every day task. Continuously cloud systems are evolving to provide great support to the Internet of Things (IoT). IoT produces continuous or streaming data and cloud computing on another hand gives meaning and provides path to this data. In addition to this, by providing remote storage and access to data, cloud allows developers to implement projects with no delays. Also, taking advantages of this, many cloud providers provide pay-as-you use strategy and charge users for the services used. This chapter discusses the cloud based support to IoT, applications offered by the paradigm, platforms available, challenges faced by integration.

Keywords Internet of Things · communication · Internet · Big Data · Cloud

2.1 Introduction

The current development towards cloud-based infrastructures for Internet of things (IoT) ecosystem is providing a relationship between interconnected devices, data generated from these devices (embedded with sensors, actuators, RFID tags) and the way cloud infrastructure is maintained. In the first phase, The IoT frameworks offer implementation ranging from processing, collecting and deploying up to

H. Tyagi · R. Kumar (✉)
Jamia Millia Islamia, New Delhi, India
e-mail: rkumar1@jmi.ac.in

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_2

service delivery. The next phase is to deploy horizontal IoT frameworks that support on demand access to the deployed framework. Lastly, the cloud infrastructures must support interactions in order to share data and manage operations (Alam 2012a). The Internet of Things brings the real and virtual world tighter than ever before (Atlam et al. 2017). This chapter discusses the cloud based support to IoT and existing cloud based IoT platforms.

A study by Cisco showed that the number of networked devices in 2012 was estimated to be 9 billion and is expected to reach 24 billion by 2020. Thus, proving IoT as trending and the main source of big data (Doukas and Maglogiannis 2011). This big data has real values to be analyzed using cloud computing platforms. It generates a huge amount of unstructured and structured data having three characteristics Volume (refers to data size), velocity (refers to data generation frequency), variety (refers to data types) (3V) (Yu Liu et al. 2015).

IoT applications are built on the principle of mobility and distributed networks. The deployment requires reliable communication network. Cloud systems play a crucial role in providing utility driven integrated solution for cloud based enterprise services.

Despite having many cloud computing models (explained in proceeding section) and infrastructure it is very difficult to manage and control IoT-Cloud based environment (Alam 2012a). Therefore, cloud based IoT applications should be build to make the most out of their combination. Cloud computing is a popular service that offers numerous benefits to IoT, by allowing users to perform normal computation tasks using services hosted on the Internet (Botta et al. 2016). An employee may need to finish a major project that must be submitted to a manager but they encounter with memory and space constraints that can be minimized if an application is hosted on the internet. The employee can use cloud computing services because data is managed remotely by a server. IoT and cloud computing are 'tightly coupled". The combination of these two will enable monitoring services and processing of sensory data generated by devices embedded through sensors.

IoT can be stated as "a world-wide network of interconnected object that are uniquely addressable (through IP addresses), with the point of convergence as internet. It is totally based on intelligent and self-configuring nodes that are capable of computing, interconnected in a global network infrastructure, responsible to collect, send and receive data. Moreover, Complexity of this network not only includes mobile devices but objects like food, clothing, paper, furniture, watches, cars etc. (Botta et al. 2016) the data generated by these devices put a lot of strain on internet infrastructure. So, this pushes companies to find a solution to minimize this pressure and solve the problem of transferring data. Accordingly, Cloud computing has become one of the major paradigm of IoT and their association is sometimes referred as cloud-IoT paradigm (Botta et al. 2016; Yu Liu et al. 2015). This combination has led to success of the IoT. IoT projects have additional complexity as compared to other cloud centric technology applications likely

1. Different gateway network requirement.
2. Diverse operating systems.
3. Diverse hardware requirements.

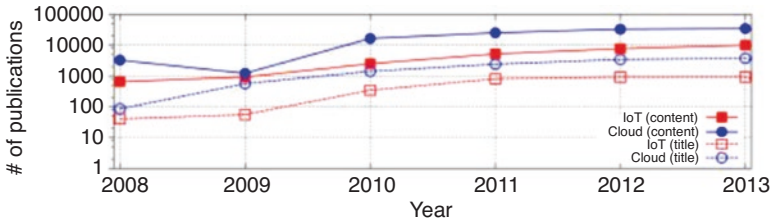


Fig. 2.1 Popularity metrics of IoT with respect to cloud (Botta et al. 2016)

4. Diversity of devices involved.
5. Difficult to manage data generating devices and power constrained small sensors (Stergiou et al. 2016).

With the advanced technology IoT, anything (person, bulb, food, any physical object) which is beyond imagination can become part of internet and generates useful data. Moreover, data generated needs to be processed in order to create more valuable services (Stergiou et al. 2016). For this purpose, integrating IoT with cloud generates new avenues in information and technology field.

Interest and current trend in cloud computing and IoT by content and title for IoT and cloud separately is shown in Fig. 2.1 (Botta et al. 2016) from the year 2008 to 2013.It depicts the increment in interest in both the technology within a time period of 5 years.

2.2 Basic Concepts

What if umbrella could sense the weather and provide advises to the user, or if some wearable device could monitor patients' health or if a car could have some predictive analysis about the upcoming service schedules to avoid certain prompt failures beforehand. IoT and internet-connected-cloud platform as a service (PaaS) can make the above said situation true in real life. The large magnitude of data generated from large number of devices especially from wireless sensor networks, health devices, machine components in industries can be collected, stored, accessed using cloud services. Cloud management is a complex task (Botta et al. 2016).

2.2.1 Cloud Computing

Microsoft Azure defined Cloud Computing as "the delivery of computing services-including servers, databases, networking, software, analytics, storage and intelligence over the internet ("the cloud") to offer faster, innovation, flexible resources (Kim et al. 2016). Cloud computing has changed the way businesses view of IT

resources (Atlam et al. 2017; Kim et al. 2016). It is required that cloud computing should reduce computation and processing cost and time. The organizations are adopting Cloud Computing. Here are some common reasons organizations are turning to cloud computing services:

1. Cost
   Cloud computing has eliminated the capital expenses of buying hardware, software datacentres, servers, electricity for power and cooling. Additionally, it has removed the cost of IT experts for managing the infrastructure.
2. Performance
   Cloud should support and provide high performance to large groups of diverse users (Alam 2012a). Interoperability and scalability between heterogeneous and distributed internet connected objects (actuators, sensors, etc) is always a challenging task.
3. Speed
   High speed services offered by cloud computing and vast amounts of computing resources can be provisioned with just a few mouse clicks for IoT based applications makes it adapted by organizations.
4. Security

The security and privacy of user information are the most challenging task identified in IoT framework (Atlam et al. 2017). Cloud provides policies and technologies that strengthen overall security (Kim et al. 2016).

2.2.2 Importance of Cloud Computing for IoT

Though IoT lacks scalability, interoperability, reliability, scalability, flexibility, availability and security.Cloud has provided these all. It has proved to provide the flow of data, processing and collection while maintaining low cost making data driven decisions and algorithms for predictions possible. The motivation behind combining these two technologies depends on three factors communication, storage and computation. Their challenges and solutions provided are discussed in Fig. 2.2 (Table 2.1).

There are some reasons listed below for considering cloud essential for the success of IoT (Fig. 2.3).

1. Provides remote processing power:- cloud empowers IoT to get beyond home appliances such as refrigerators, air conditioners, coffee makers etc. with the advancement in internet technologies like 4G to higher internet speed, the cloud will allow developers to offload fast computing process.
2. Provides security and privacy:-Security in terms of Cloud Computing refers to all the policies to controls and protects data, applications and associated infrastructure. IoT skills are incomplete without security features. Often, the devices bought by users are equipped with default passwords provided by the manufacturers that are easily approachable by eavesdropper. Sometimes, the users don't

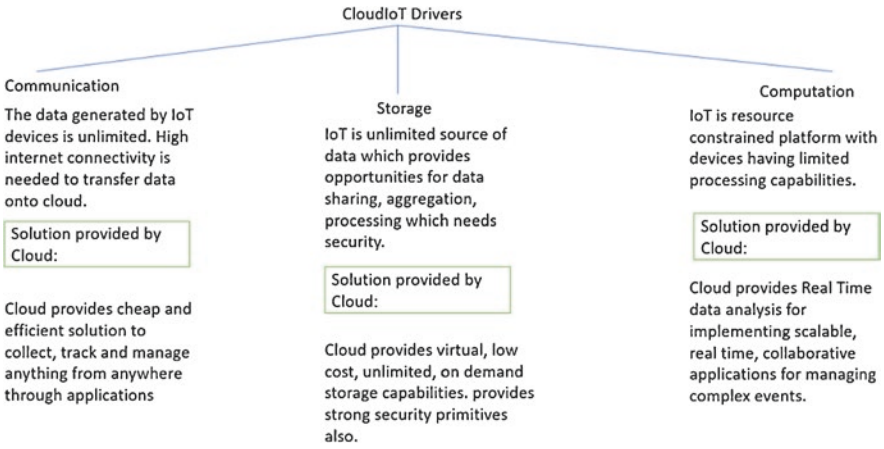


Fig. 2.2 Cloud IoT drivers

Table 2.1 Companionship between IoT and Cloud

IoT[1,3]	Cloud computing[1,3]
Source of data (data generated by sensors)	Manager of data(storage, collection, computation)
Act as a point of convergence	Acts as means of delivering services
Limited storage and computing capabilities.	Unlimited storage and computing capabilities.

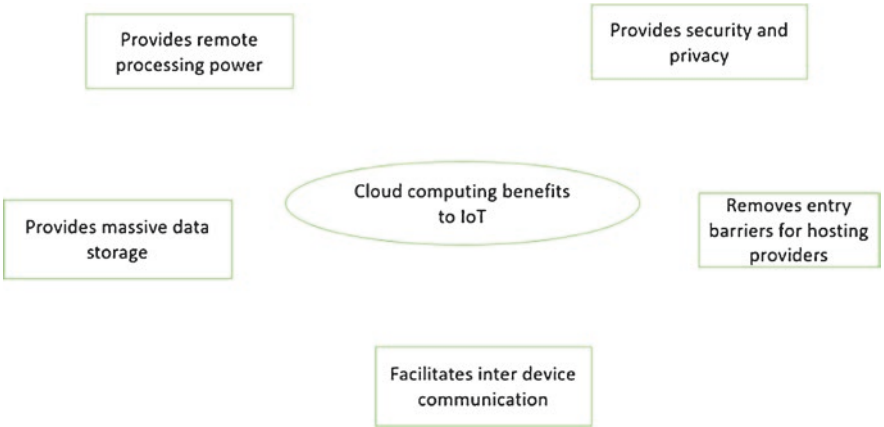


Fig. 2.3 Reasons for considering cloud beneficial to IoT

use strong enough password to protect their devise and leads to serious problems. Cloud has made IoT more secure by considering protective, detective and corrective controls.It has enabled users with authentication and encryption protocols and provide strong security measures. Many other methods like biometrics are also used to protect users' identity.

3. Provides massive data storage:-In IoT there are millions of devices involved that are continuously or periodically generating data. The data that is outside the capacity of normal systems to handle. This is an open challenge for IoT and cloud together to handle and store the data. Two different cloud models based on usage:
   - Service Models (SaaS, PaaS and IaaS)
   - Deployment Models (Private, Public and Hybrid)
4. Facilitates inter-device communication:- cloud behaves as a mediator when comes with IoT communication. The data generated by devices can be analysed and processed on cloud for making intense decisions.
5. Remove entry barriers to the host providers:- With cloud, most hosting providers can allow their clients a ready-to-roll model, removing entry barriers for them.

2.3 Cloud Based IoT Architecture

1. Perception layer

   It is responsible for collecting all information from its surroundings (sensors and actuators) and sends it through gateway for further processing. The attacks on sensors are the most common and constant in IoT framework. Here, the parameter values are evaluated by RFID tags, sensors, GPS, RSN other devices (Fig. 2.4).
2. Network layer

   Based on the distance for communication the protocols are used as Bluetooth (small distance communication), ZIGBEE/LAN (communication within a building), WiFi (communication from anywhere in the world).the security con-

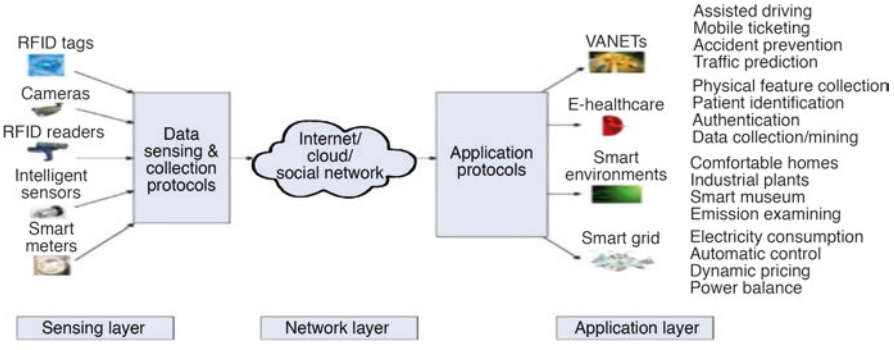


Fig. 2.4 Cloud-IoT Architecture[18]

sideration here are based on data as well as on network. The attacks on network includes WIFI sniffer, malware, eavesdrop, brute force, Man In Middle attack, Man at end attack (MATE) (Vermesan and Friess 2014). Attacks on data includes modification, non-repudiation and provides privacy, confidentiality, availability, integrity as major security considerations.

3. Application layer

The advanced layer which is responsible for all classes of business services and intelligent computation, resource allocation and data processing (Rochwerger et al. 2009), where the user can interact with smart devices and control according to their demand. Application layer protocols specially designed for IoT are HTTP (Hyper Text Transfer Protocol) and CoAP (constrained application protocol).

2.3.1 Models

The introduction of integrated CloudIoT enables new smart applications [33] based on the extended cloud scope to deal with real life states or scenarios providing way to the birth of things as a service. Some of the new models introduced by this paradigm are given below:

1. CSaaS (Cloud-based-sensing as a Service) (Carnaz and Nogueira 2016):-provides multi-tenancy, virtualization and dynamic provisioning. Making it possible to abstract the data between sensor provider and consumer even sharing the same infrastructure.
2. DBaaS (Database as a Service) (Chen et al. 2010):-allows ubiquitous database management.
3. DaaS (Data as a Service) (Chen et al. 2010):-allows ubiquitous access to any kind of data.
4. EaaS (Ethernet as a Service) (Chen et al. 2010):-allows ubiquitous layer-2 connectivity to remote devices.
5. SenaaS (Sensor as a Service) (Chen et al. 2010):-allows ubiquitous management of remote sensors.
6. MBaaS (Mobile backend as a Service):[30] provides web and mobile applications to connect to the backend cloud storage. It Provides features like user management, social networking services.
7. VSaaS (Video Surveillance as a Service)[31]: provides all video storage requirements like stored media is secured, scalable, on demand, fault-tolerant and video processing.
8. SaaS (Sensing as a Service) (Chen et al. 2010):-allows ubiquitous access to sensor data.

2.4 CloudIoT Applications

The integration of cloud with IoT brings many opportunities as well as challenges that are discussed in proceeding section. The CloudIoT paradigm is a great evolution in Information and Communication Technology (ICT). This paradigm has taken many industries including agriculture, healthcare, energy management, transportation, smart city, environment protection that are discussed in next chapters. Cloud has provided the ability to store and stream data over the internet, possible visualization in a web browser, controlling devices from anywhere and anytime in the world (Prati et al. 2013). The usage of cloud in IoT has acted as a catalyst for the development and deployment of scalable applications. The two technologies provide platform to each other for success (https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/). Cloud computing has brought a revolution how technologies can be managed, accessed and delivered (Atlam et al. 2017).

The integration has given birth to numerous applications as depicted by Fig. 2.5 and most of the applications affects everyday tasks. Cloud can provide benefits to *IoT by extending its scope to deal with real world things in a more dynamic and distributed way*. In most cases, Cloud can provide the middle layer between the things and applications, abstracting all the complexity and functionalities necessary to implement the applications (Botta et al. 2016). In this section, we describe the applications offered by CloudIoT paradigm (Fig. 2.6 and Table 2.2).

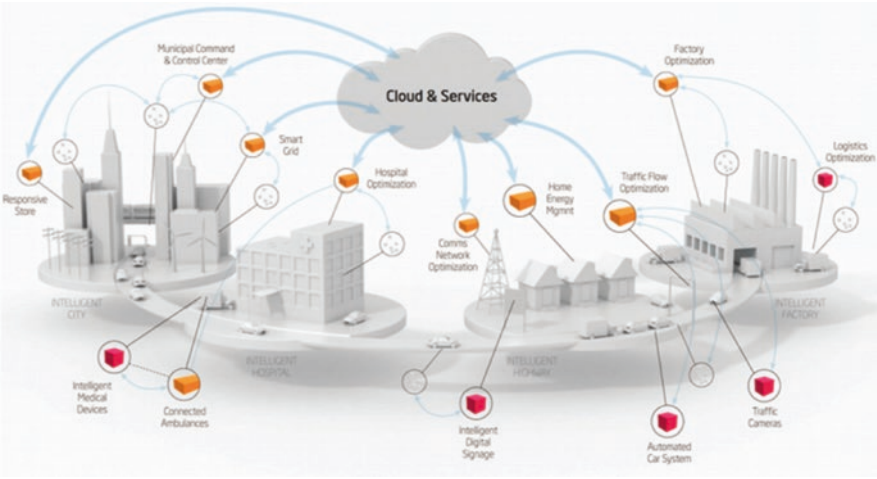


Fig. 2.5 Services offered by CloudIoT paradigm (Source: https://siliconangle.com/)

Fig. 2.6 Applications offered by CloudIoT paradigm[1]

Table 2.2 IoT applications description

IoT applications	Importance of integration of cloud and IoT
Health care system	Collecting patient's important data (ECG, BP, Heartbeat) via network of sensors connected to human body, delivering this data to medical centre's cloud for storage. further processing and sharing medical report data (Botta et al. 2016). It can improve health care services and health care processes by providing cost effective and high quality services. It also aims at providing Ambient Assisted Living (AAL) (Kaur and Alam 2013) means easing the daily lives of old person, person with physical and mental disabilities.
Smart city	The smart city solutions should cover the notions like, Smart Lighting, Smart traffic management, Smart building, Smart parking, Wi-Fi Internet access & City Surveillance, Solid Waste Management, Smart Metering, Water Quality, water clogging management in cities, etc. It also aims at easing the urban life, protecting environment, encourage sustainable development (Alam 2012b).
	For the efficient and flawless operation of smart cities, deployment of IoT and cloud computing is most important. It is impossible to offer above mentioned services and visualization, management, processing of enormous amount of vital data that is useful for public or private organization without cloud.

(continued)

Table 2.2 (continued)

IoT applications	Importance of integration of cloud and IoT
Smart home and smart metering	Cloud has automated all the common household activities. The association of computing with physical objects transforms the environment into informative and appliances into intelligent. Smart lighting is responsible for 19% global use of electrical energy and emission of greenhouse gases (Alam 2012b). To emphasis on sustainable development this emission and usage should be reduced. Smart lighting control systems has proved to reduce the light consumption by 45% (Botta et al. 2016).
	Cloud offers flexible framework for building smart applications making home automation a trivial task.
	Cloud offers remote control of appliances and services.
	Cloud offers direct communication of users and sensors.
	Cloud can satisfy that any digital appliance can be connected to any other.
Video surveillance	The intelligent video surveillance make it possible to monitor anything at anytime from anywhere. CloudIoT in this context can be used to store, manage and process video contents evolving from IP cameras (Botta et al. 2016; Atlam et al. 2017) and automatically extract knowledge. Because of cloud,
	Security can now be offered as a service that is managed remotely and freely that no longer require human.
	VSaaS[31] given cloud model satisfies all the video storage requirements i.e, the media is centrally secured, scalable, fault tolerant and also provides video processing facilities to identify patterns.
Automotive and Smart mobility	Intelligent transport system (ITS) is offering a great opportunity in the field of transportation system and automobile industry by providing traffic state prediction, notification (Atlam et al. 2017). The integration of Cloud with IoT technologies (WSN and RFID) brings many opportunities (Botta et al. 2016).
	Vehicular cloud data mining service provides road safety, reducing road congestion, smart parking system, recommending car maintenance system. Vehicle to vehicle communication, vehicle to infrastructure communication is possible [30,32].
Smart energy and Smart Grid	The integration cloud with IoT has an excellent application in the field of smart energy and smart grid by providing intelligent energy distribution and consumption (smart meters, smart appliances, renewable energy resources) (Botta et al. 2016; Atlam et al. 2017).
Smart Logistics	The CloudIoT paradigm in the field of logistics provides automated management of flow of goods from the point of source(origin) to the point of destination in a cost effective and timely manner (Botta et al. 2016). It has made the tracking in transit possible effortlessly (Botta et al. 2016; Atlam et al. 2017). The implementation of Cloud computing can overcome the bottleneck by allowing complex decision-making systems with automated algorithms to retrieve information for further planning and tracking.
Environmental Monitoring	The integration offers a great scope in the area of environment monitoring by deploying environmental sensors in any area. some applications include water level needed in field, lighting condition, gas concentration in air, natural hazards occurrence like landslides, detecting infrared radiation (Botta et al. 2016; Atlam et al. 2017).

2.5 Cloud Platforms Available for IoT

A number of IoT platform are available for sensor data management either free or open source (ThingSpeak, iCloud, Dropbox) or commercial (AWS, Azure, Kura, SmartThings, google cloud platform).

2.5.1 Commercial IoT Platform

1. Aws IoT platform
   AWS IoT (https://ap-south-1.console.aws.amazon.com/console/home?region=ap-south-1), A cloud platform provided by amazon for the internet of things (IoT). This framework provides smart devices to connect easily and securely interact with AWS (Amazon Web Services) cloud. The most exciting feature of AWS is it allows devices to communicate even when they are offline (https://azure.microsoft.com/en-in/solutions/). This framework offers services like for computing (Lambda, EC2), for storage (Amazon S3, storage gateway), database (DynamoDB), machine learning (Amazon DeepLens, Amazon forecast), for Analytics (kinesis), blockchain (Amazon Managed Blockchain) (Ammar et al. 2018) (Fig. 2.7 and Table 2.3).
2. Microsoft Azure
   Azure is a platform offered by Microsoft that allows end users to interact with IoT devices, receive data, performs aggregation, multi-dimensional analysis and transformation. AWS, as discussed and Azure are two famous names in public

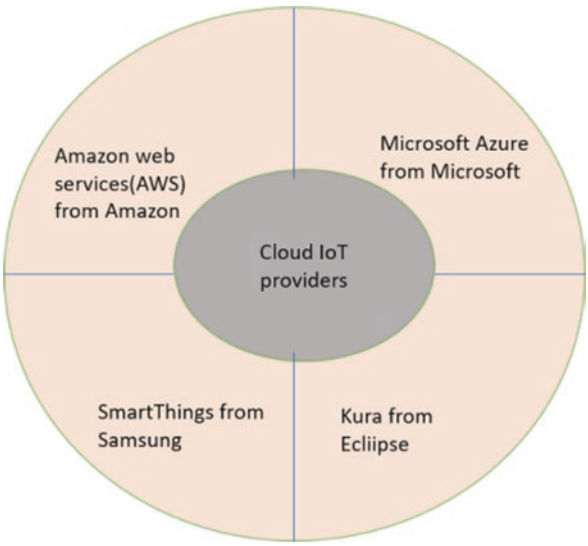


Fig. 2.7 Cloud providers to IoT

Table 2.3 AWS Description and Applications

Aws IoT components[16]	Description	Applications
Cloud services	Kinesis, DynamoDB, Blockchain, Lambda.	Machine learning, computation, blockchain, Database, storage
Smart devices	Anything ranging from human being to bulb.	
Device gateway	Supports application protocols like MQTT, Web Socket, HTTP 1.1	Provides security, manageability, and scalability
Message broker		Publishing and subscribing messages
Registry		Tracking and identification
		To devices
Rule engine	Rules like SQL syntax queries	Processing, analyzing, Gathering, action on data
Language support	Any language	Supports
Cryptography	128 bit AES	Security
Security	X.509 certificate (Eclipse Organization 2019), AWS cognito identities	Authentication
Communication (SmartThings 2019)	SSL/TLS	Confidentiality and encryption
SDK language support	C, node.js, Arduino	Allow accessing any device
Device Shadow	JSON document	Retrieve current state of certain device

cloud computing. It supports wide range of operating system, programming languages. IoT devices interact with azure cloud through a gateway (Eclipse Organization 2019). The data from devices is stored on cloud for further processing and analysis by applying machine learning service offered by azure. The real time monitoring of data is also possible (Table 2.4).

3. SmartThings

   SmartThings is a IoT cloud platform released by Samsung mainly has applications in smart homes by enabling users to have control over smart devices.it is a platform where developers can implement applications allowing their users to control smart appliances in homes through mobile applications (Alharbi and Aspinall 2018) (Table 2.5).

4. Kura platform

It is an extensible open source Java/OSGi (open services gateway initiative) IoT Edge framework. It is an advanced software framework that abstracts the developer from hardware complexity and complexity of networking sub-systems. It is a project that provides platform for building IoT gateway (Jing et al. 2014). It is a smart application container, which provides re0mote management of the gateways and APIs for building your own IoT application (Table 2.6).

Table 2.4 Azure platform Description and Applications

Azure components	Description	Applications
Cloud services		Machine learning, Azure stream analysis
Smart devices	Anything ranging from human being to bulb	
Field gateway		Aggregation, storing and forwarding data to IoT hub.
Azure IoT hub	Commands/notification	Provides bi-directional communication.
Identity Registry		Provides device Identification and Management
Security	X.509/TLS based handshake and encryption	Provides authentication
SDK language support	C, Node.js, python, java, .NET	Provides device management
Azure access Directory		Provides authorization and access control
communication	SSL/TLS	Encrypt communication and ensures confidentiality and integrity of data.

Table 2.5 SmartThings Description and Applications

SmartThings components	Description	Applications
SmartThings mobile client app	Supports Android and iOS	Smoothly access the smart appliances.
SmartThings cloud backend	Abstraction and intelligence	Hosting and running smart apps, running virtual software image of physical smart devices.
SmartThings Hub	128-bit AES encryption, Zigbee product	Security enabled Z-wave product
Smart devices	Should facilitate connection via WiFi/IP protocol	Connecting these devices to cloud for further processing
Home controller	Supports communication protocol Z-wave, WiFi, Zigbee, BLE	Gateway for communication between devices and cloud
communication	SSL/TLS	Encryption communication to ensure confidentiality and integrity
Security protocol	OAuth/OAuth2 protocols	Authentication

Table 2.6 Kura Platform Description and Applications

Kura components	Description[18]	Applications
OS support	Only Linux	Provides remote management
Programming language support	java	For developing smart applications
Supported protocols	MQTT, CoAP	Authenticate communication
Communication	SSL/TLS	Secured communication
Device abstraction layer	Using OSGi services	Abstracting hardware complexities
Cryptography	Multiple cryptography primitives	

2.5.2 *Open Source IoT Platform*

- ThingsBoard:- An open source platform for processing, collection, visualization and management of data produced by sensors communication involved in IoT ecosystem (Table 2.7).
- The devices are connected via IoT protocols MQTT, CoAP (constrained application protocol) and HTTP which also supports cloud deployments. ThingsBoard provides scalability, fault-tolerance and performance to the data. It supports both cloud and on premises deployments. You just have to create account and manage your smart devices smartly. There is special provision to raise alarms on incoming telemetry data. Figure 2.8 shows real time monitoring of smart meters IoT system on ThingsBoard platform.

Table 2.7 ThingsBoard IoT platform

ThingsBoad components	Description
IoT rule engine	Allows to create complex chains of rules for data processing from your devices
Real time IoT dashboard	Realtime visualization and remote ontrol of data
Security	Supports device authentication management, encryption for both HTTP and MQTT

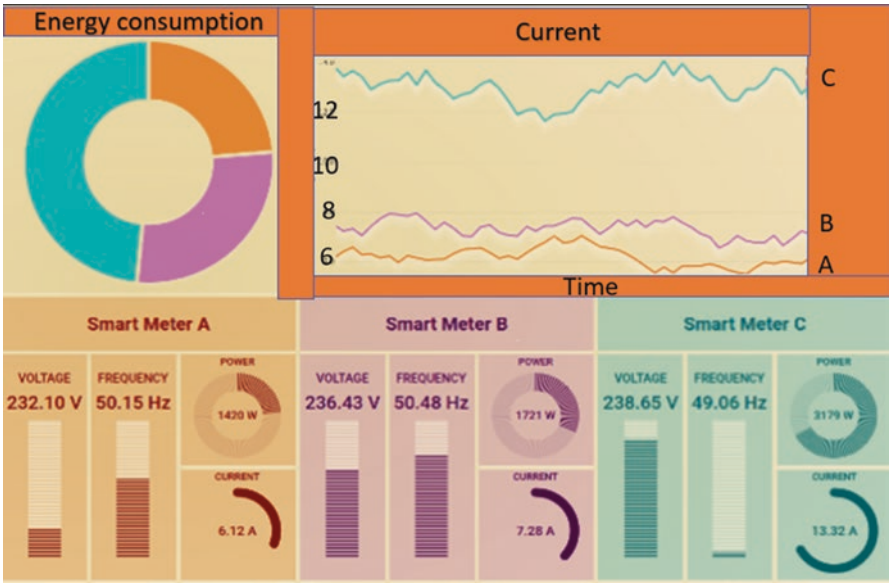


Fig. 2.8 Showing cloud platform for smart grid application

Table 2.8 Challenges in applications

Application	Challenges					
	Security	Legal and social aspects	Large scale	Privacy	Reliability	Heterogeneity
Healthcare system	√	√	√	√	√	√
Smart city	√	√		√	√	√
Smart home and metering					√	√
Video Surveillance	√				√	√
Automotive and smart mobility	√				√	√
Smart energy and smart grid	√	√		√	√	√
Smart logistics		√	√	√		
Environment monitoring	√		√		√	√

2.6 Challenges

In the previous sections the benefits of cloud and IoT integration has shown. This can be accurately and confidently said that the integration is a buzz in technological industry which brings tremendous amount of business and job opportunities. But the integration also brings certain serious challenges that needs to be discussed. Based on the applications discussed the challenges can be summed up as shown in the Table 2.8.

2.7 Conclusion

This can be accurately said that cloud can accelerate the growth of IoT. However, deploying cloud technology also comes with certain challenges and shortcomings. Cloud computing and the IoT are the next-generation technologies. Cloud offer an effective solution for IoT like service management, implementing applications and services. It can benefit IoT by enabling it to deal with real world things in a more efficient and scalable manner. It can work as a middle layer between things and applications. Both technologies fills gap for each other like cloud provides IoT with unlimited storage capabilities and IoT extend the scope and application of cloud. The integration of these two technologies provides path for various business opportunities and innovative research areas as discussed in the chapter. The applications presented by integrated technology and challenges derived are discussed in the chapter. The security challenges pertaining to CloudIoT paradigm are power and

efficiency, security and privacy. Future scope include finding out a way to deal with heterogeneous environment providing scalability and security, environmental sensors for providing better results, identification of definitive solution for addressing things uniquely, extended support to multi networking.

References

Alam, M. (2012a) Cloud algebra for cloud database management system. In *The second international conference on Computational Science, Engineering and Information Technology (CCSEIT-2012), Coimbatore, India*, Proceeding published by ACM, October 26–28, 2012.

Alam, M. (2012b, December) Cloud algebra for handling unstructured data in cloud database management system. *International Journal on Cloud Computing: Services and Architecture (IJCCSA), 2*(6), ISSN: 2231-5853 [Online]; 2231-6663 [Print], https://doi.org/10.5121/ijccsa.2012.2603, Taiwan.

Alharbi, R., & Aspinall, D. (2018). An IoT analysis framework: An investigation of IoT smart cameras' vulnerabilities. *IoT, 2018*.

Ammar, M., Russello, G., & Crispoa, B. (2018). Internet of things: A survey on the security of IoT frameworks. *Journal of information security and Applications*, 8–27.

Atlam, H. F., Alenezi, A., Alharthi, A, Walters, R. J., & Wills, G. B. (2017). *2017 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (Green Com) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (Smart Data), IEEE*. pp. 671–675. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.105

Botta, A., de Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: A survey. *Future Generation Computer System, 56)*, 684–700.

Carnaz, G., & Nogueira, V. B. (2016). An overview of IoT and healthcare. In S. Abreu & V. B. Nogueira (Eds.), *Actas das 6as Jornadas de Informática de Universidade de Évora*. Natal: Escola de Ciências e Tecnologia.

Chen, P., Freg, C., Hou, T., & Teng, W.-G. (2010, December). Implementing RAID-3 on cloud storage for EMR system. In *Proceedings of the 2010 International Computer Symposium (ICS), Taiwan, 16–18* (pp. 850–853).

Doukas, C. & Maglogiannis, I. (2011). Managing wearable sensor data through cloud computing. In *Third IEEE international conference on cloud computing technology and science, 2011*.

Eclipse Organization. (2019). *Kura framework*. http://www.eclipse.org/kura/. Online. Accessed July 2019.

Jing, Q., Vasilakos, A., Wan, J., Lu, J., & Qiu, D. (2014). Security of the internet of things: Perspectives and challenges. *Wireless Networks, 20*, 2481–2501. https://doi.org/10.1007/s11276-014-0761-7. https://thingsboard.io/, 2014.

Kaur, A., & Alam, M. (2013). Role of knowledge engineering in the development of a hybrid knowledge based medical information system for atrial fibrillation. *American Journal of Industrial and Business Management, 3*(1), 36–41. https://doi.org/10.4236/ajibm.2013.31005.

Kim, M., Asthana, M., Bhargava, S., Iyyer, K. K., Tangadpalliwar, R., & Gao, J. (2016). Developing an on-demand cloud-based sensing-as-a-service system, internet of things. *Journal of Computer Networks and Communications*. https://doi.org/10.1155/2016/3292783,2016. Article ID 3292783, 17 pages.

Prati, A., Vezzani, R., Fornaciari, M., & Cucchiara, R. (2013). Intelligent video surveillance as a service. In *Intelligent multimedia surveillance* (pp. 1–16). Berlin/Heidelberg: Springer.

Rochwerger, B., Breitgand, D., Levy, E., Galis, A., Nagin, K., Llorente, I. M., Montero, R., Wolfsthal, Y., Elmroth, E., Caceres, J., Ben-Yehuda, M., Emmerich, W., & Galan, F. (2009). The RESERVOIR model and architecture for open federated cloud computing. *IBM Journal of Research and Development, 53*(4).

SmartThings. (2019). *Smart things documentation*. http://docs.smartthings.com/en/latest/. Online. Accessed July 2019.

Stergiou, C., Psannis, K., Kim, B.-G., & Gupta, B. B. (2016). Secure integration of internet-of-things and cloud computing. *Future Generation Computer Systems, 2016*, 964–975.

Vermesan, O., & Friess, P. (2014). *Internet of things from research and innovation to market deployment*. Aalborg: River Publishers.

Yu Liu, Beibei Dong, Benzhen Guo, Jingjing Yang, & Wei Peng. (2015). Combination of cloud computing and internet of things (IOT) in medical monitoring systems. *International Journal of Hybrid Information Technology, 8*(12), 367–376.

Chapter 3
Open Service Platforms for IoT

Preeti Agarwal and Mansaf Alam

Abstract With the advent of Internet of Things (IoT), anything on earth with embedded processor, storage, and communication technology can communicate with each other. IoT can interconnect billions and trillions of devices on earth. This is considered as next revolution in the world of internet. It is expected that this revolution will drastically improve quality of daily life, will bring new forms of collaboration, interaction, and activities. IoT is not considered a single technology, but it is an aggregation of various underlying technologies, making the application development task bit challenging. In order to cope up with this challenge, number of vendors are coming up with IoT platforms for application development. IoT platforms provide support for connecting, storing, computing, and analysing data from heterogeneous devices. This chapter, presents a reference architecture for IoT service platforms, outline a set of service and architectural requirements for IoT platform, and review four major IoT platforms (AWS IoT platform, IBM Watson platform, Microsoft Azure IoT Platform, and Google Cloud Platform) from these requirements viewpoint. Further, gaps and issues in present IoT platforms are discussed with future research directions.

Keyword Internet of Things (IoT) · IoT platform reference architecture · IoT platform service requirements · IoT platform architectural requirements

3.1 Introduction

The term "Internet of Things" was first coined by Kevin Ashton in 1999 (Ashton 2009). According to IoT concept, every sensor, every device, and every software can be connected to each other. These devices can communicate remotely with each other via. IoT platform. The main idea behind IoT was to provide ubiquitous

P. Agarwal (✉) · M. Alam
Department of Computer Science, Jamia Millia Islamia, New Delhi, India
e-mail: malam2@jmi.ac.in

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_3

computing with minimum human intervention (Al-Fuqaha et al. 2015; Atzori et al. 2010). The concept gained popularity by embedding processors, storage and communication technology in devices, and these technologies converted devices into smart devices. Smart devices are now capable of sensing the environment, storing information, and can also communicate with each other, eliminating human in the loop. Enabling interaction, collaboration and communication among various devices has foster application development in many domains such as healthcare, smart homes, agriculture, traffic, and energy management (Asghari et al. 2019). In order, to provide centralized control over these smart devices, number of vendors came up with different platforms. At present, market is flooded with IoT platforms, and identifying a suitable one for a particular application is a big challenge (Agarwal and Alam 2019). Some of the popular platforms are AWS IoT, IBM Watson, Microsoft Azure, Google cloud IoT. The main objective of this chapter is:

- To provide general IoT reference architecture,
- Identify key service and architectural requirements for IoT platforms,
- Review four most popular IoT platforms from requirements view point,
- Present gaps and challenges to be addressed by future IoT platforms.

The structure of chapter is as follows: Sect. 3.2 gives general IoT reference architecture, Sect. 3.3 provides key service and architectural requirements of the platform. Section 3.4 discusses four case studies of the most popular IoT platforms AWS IoT, Microsoft Azure IoT, Google Cloud IoT, and IBM Watson IoT from requirements viewpoint. Finally, Sect. 3.5 presents challenges and open research directions to be addressed by future IoT platform.

3.2 IoT Reference Architecture

IoT is considered next revolution in World Wide Web. To provide Quality of Service (QoS), special consideration need to be taken to while defining its architecture (Fahmideh and Zowghi 2020). Many IoT architectures have been presented in literature, but the most accepted one is four layer architecture consisting of: sensor layer, gateway and network layer, service management layer, and application layer (Yaqoob et al. 2017), as shown in Fig. 3.1. Each layer is described in following subsections.

3.2.1 Sensor Layer

The first layer, called as sensor layer or perception layer. It consist of sensors and actuators, that sense the environment, collect information for processing to gain useful insights. Different kind of sensors can be deployed at this layer, like temperature, motion, humidity, sensing events etc. At this layer heterogeneous devices are deployed in plug and play manner. The perception layer digitalizes, creates secure

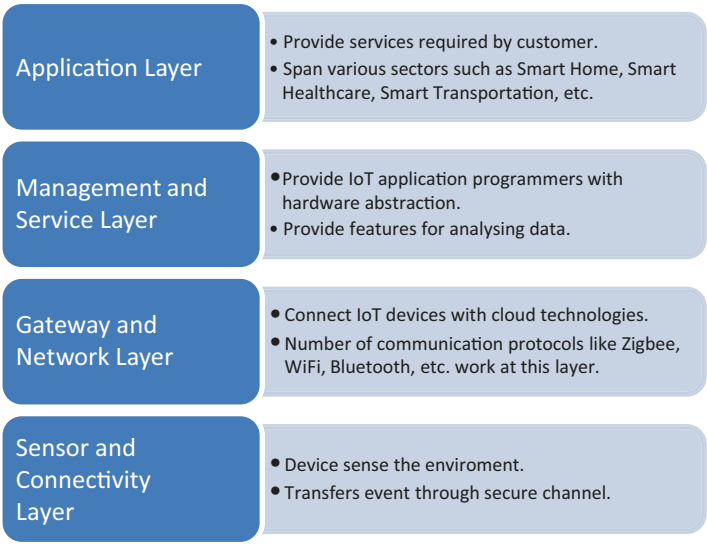


Fig. 3.1 IoT architectural layers

channel, and transfer data to the next layer. This layer is major source of big data to be processed by next layers.

3.2.2 Gateway and Network Layer

The gateway and network layer transfers data created through secure channels by the sensor layer to the above layer. Various wireless technologies such as Zigbee, RFID, Wi-Fi, etc. are used to transmit data. Furthermore, storage and processing of data needs to be addressed at this layer. One of the possible solution for storage is cloud. Multiple cloud based storage solutions for IoT generated big data exist (Khan et al. 2017; Alam and Shakil 2016). Different ways to process both structured and unstructured data exist (Alam 2012). Most of the data management as well as resource management is carried out at this layer. Many algorithms for efficient resource management can be deployed (Ali et al. 2019).

3.2.3 Service Management Layer

Management or Middleware layer binds a service with its requestor. This layer provides features that enables the IoT application programmers to work with the sensor objects in a seamless manner, without any concern to underlying hardware. Also, this layer processes received data, make smart decisions, and based on decisions

deliver the services over the network through protocols. Various analytical solutions can be applied at this layer to provide intelligent decisions.

3.2.4 Application Layer

The application layer provides the requested services to its users. For example, the application layer can provide acceleration and heart beat values to the medical care provider for its patient to continuously monitor them. This layer has ability to provide superior services to meet the user's need. The application layer provide services to many sectors such as smart home, smart healthcare, smart transportation, industrial automation and smart energy management.

3.3 IoT Platform Requirements

IoT platform is a responsible for integrating devices on network for different applications through software packages. IoT Platforms are deployed on service management layer of the IoT architecture. The platforms provide users a layer of abstraction, hiding the implementation details. IoT platforms provides an ecosystem upon which different smart applications can be built (Tiwana 2013).

Like other software's, IoT platforms also need to satisfy certain user requirements. These user requirements are divided into service requirements and architectural requirements (Razzaque et al. 2015; da Cruz et al. 2018). The service requirements can be functional and non-functional, as shown in Fig. 3.2.

3.3.1 Service Requirements

Service requirements can be classified as functional and non-functional. Functional requirements describe the required functionalities of the IoT platform, whereas non-functional requirements focus on providing QoS parameters (Razzaque et al. 2015).

The various functional requirements are described as follows:

- **Resource Discovery**: The IoT connects heterogeneous devices in dynamic environment. There must be some automated mechanism to publish, discover, and subscribe to resources in centralized manner. In order to carry out this task middleware platform maintains a registry component in which devices register themselves using necessary API's. After registration the device becomes discoverable to other devices in the network. The registered device can publish metadata about its services. Even other devices in the network can query the device by suitable query mechanism, can surf the required services and resources provided by the

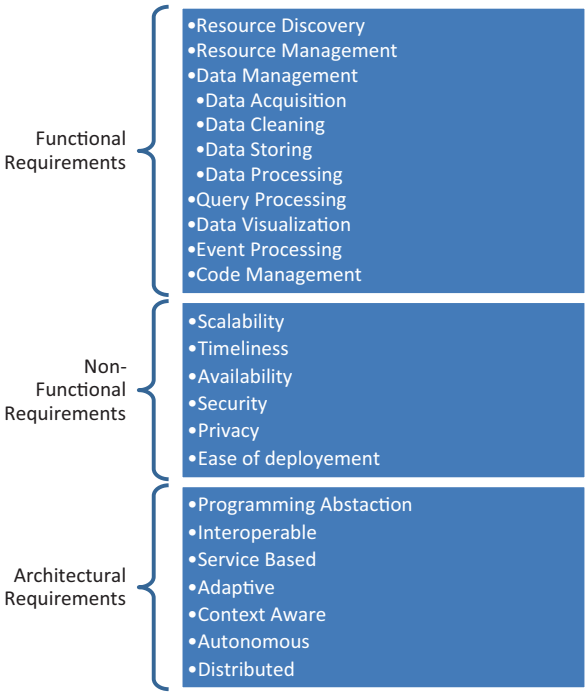


Fig. 3.2 IoT platform requirements

device. To explore services provided by a device semantic match making mechanism is used (Fabisch and Henninger 2019). The various challenges associated with discovery includes interoperability (Nitti et al. 2017), security (Zhang et al. 2017), and unique addressing (Cheng et al. 2015).

- **Resource Management:** To provide QoS, it is required to deploy certain module on IoT platform to manage resources. Resources need to be monitored, scheduled and allocated in a fair, conflict free manner (Razzaque et al. 2015) by the platform. To carry out this task platforms must maintain data about device battery time, memory usage, processing power, and other relevant information for efficient resource management (da Cruz et al. 2018).
- **Data Management**: Data management plays a vital role in any application development. In case of IoT, data refers to the data sensed by the IoT devices. IoT platform is required to provide data management services which include data acquisition, data processing, querying and visualisation.
- **Data Acquisition**: IoT platforms acquire data sensed by devices from various sources. The sensed data can be structured or semi-structured (Cheng et al. 2015). Following are the main sources of data captured by the platform (Santana et al. 2018; Khan et al. 2015):
  - Real time data about physical devices such as traffic, city maps, citizen's data.
  - Data available in form of software such as libraries, codes, documents.
  - Historically stored data in the form of logs, historic actions.

The challenges associated with designing data acquisition are addressing, scalability, configuration, security and interoperability of objects (Apolinarski et al. 2014).

- **Data Cleaning**: This data acquired through sensors may be incomplete, inconsistent, noisy or irrelevant. To increase the reliability of the system it is required to be cleaned and preprocessed for further execution. The algorithms for anomaly detection (Cheng et al. 2015), maintaining semantic consistency, data normalization (Silva et al. 2018), and data filtering (Petrolo et al. 2014; Filipponi et al. 2010) need to be designed. Some platforms even employ strategies that allow users to collect data of interest only by filtering irrelevant data through algorithms (Soldatos et al. 2015).
- **Data Storing**: It deals with storing the data acquired through the sensors. IoT platform is mainly responsible for managing huge volume and variety of IoT sensed data. Mainly relational databases and No SQL databases are used for storage (Fahmideh and Zowghi 2020). Relational databases are used for structural, transactional data. No SQL databases are used for dynamically changing schema. Some of the popular choices of No SQL databases are Hadoop, CouchDB, HBases, and MangoDB.
- **Data Processing**: This includes the power of IoT platform to analyses sensor data for meaningful inferences. Data is usually analyzed in two modes: Real time analytics or Streaming mode, and batch processing or historical analysis (Al-Fuqaha et al. 2015). In real time analytics the concern is over timely efficient processing of fast running IoT stream data. Some of the technologies that support fast streaming data are Apache Spark, Storm. Historic analysis deals with processing batch of historically stored sensor data and finding inferences in it. Data mining techniques such as classification, regression and clustering can be done on data to find classes, groups or abnormalities, trends in acquired sensor data.
- **Query Processing**: It is the process for querying the data stored in the IoT platform. Querying mechanism also uses publish/subscribe mechanism like data acquisition (Cheng et al. 2015). The query can be a simple query or complex query aggregating data from multiple databases.
- **Data Visualization**: in response to users query on stored data, visualization techniques provide graphical view of the analysis results. Results can be in form of dashboards, maps or reports.
- **Event Processing**: The function of the platform is to process event successfully. Event is nothing, but a change in environment, which is captured by sensor, and requires certain action to be taken over it. Usually event processing is required to be carried out in real time (Cretu 2012). The platform should provide flexibility to the users in terms of executing own code and define event conditions (Sarhan 2019). The main challenges associated with event processing in IoT platform is to combine data from multiple sensor stream in different forms and combine them for one common goal. Events are usually represented in form of ontologies enabled by metadata for their correct interpretations (Fahmideh and Zowghi 2020).

- **Code Management**: IoT platform plays an important role in deploying code for IoT applications. For this code allocation, and migration services are required (da Cruz et al. 2018). Code allocation deals with selecting appropriate sensor devices and executing code on that particular sensor device. Code migration deals with providing portable facilities for migrating code on different programming services.

Non –functional requirements: The various non-functional requirements are described as follows:

- **Scalability**: The IoT platform needs to accommodate large number of devices. The IoT platform must provide features that can add any number of devices, and can remove any number of devices (Al-Fuqaha et al. 2015). Adding large number of devices must maintain QoS (da Cruz et al. 2018)
- **Timeliness**: Event processing mainly rely on timely execution on data. Most of the events require real time processing. Real time means execution of data quickly, without any delay. The time required for processing is critical and is determined by different applications processing them.
- **Availability**: For critical applications 24X7 availability of the platform is must. The platform must be available for services, even it is facing internal failures (Razzaque et al. 2015). The recovering time from failure should be very small, not affecting the system performance. Reliability and availability both are important factors and deals with fault tolerance.
- **Security and privacy**: Another important requirement of IoT platform is to provide security to the user's data. Most of the applications require to store user's personal data and information such as GPS cation, password, etc. Proper security mechanisms need to be deployed to protect user's information during transmission and storage to protect it from malicious attacks. Proper security and privacy preserving mechanisms need to be deployed at both functional and non-functional level (Al-Fuqaha et al. 2015).
- **Ease of deployment**: IoT platforms are used for end user application deployment. Most of the time they are used by application developers to integrate their own device. So, it is required from platform to be user friendly, to be easily integral with device, and must not require lot of expertise. Must be easy to install and set up.

3.3.2 Architectural Requirements

Architectural requirements supports application development. It deals with the requirements which can ease the application development task, such as programming abstraction from hardware implementation, inbuilt API's, libraries. The major architectural requirements are as follows:

- **Programming Abstraction**: The application developing programming interface of an IoT platform must be able to hide the internal working of the system. At the time of designing the IoT platform, it is required to design the level of abstraction to be provided to the different level of users.
- **Interoperable**: An IoT platform must be able to interoperate heterogeneous devices, technologies and diverse applications. These heterogeneous devices must be able to communicate with each other, exchange information, and can work collaboratively to achieve final goal. Interoperability can be achieved at network, semantic, and syntactic level (Fahmideh and Zowghi 2020).
- **Service based**: IoT platforms must support service-based framework, where new service interfaces for diverse applications can be easily added, without affecting the underlying hardware interfaces. Service oriented framework provides flexible architecture for building diverse applications.
- **Adaptive**: IoT platform architecture should be capable of adapting itself to changing environment. IoT applications usually work in dynamic environment. So, it is required that platform should incorporate this dynamicity in its architecture.
- **Context Aware**: Context awareness adds value to the information sensed by the IoT devices. Context awareness means IoT device must be capable of capturing user's information and device information for providing more meaningful inferences.
- **Autonomous**: All devices in IoT environment must work in self-governing mode. They must be able to work autonomously in collaboration with other devices in the network without human intervention (Gubbi et al. 2013; Wang et al. 2010). Automaticity can be provided by embedded intelligence, analytics, and autonomous agents (Guo et al. 2011).
- **Distributed**: In order to support distributive applications like transportation, traffic. The IoT platform must be able to provide distributed, decentralised processing. Platform must support functions that can be performed in physically distributed infrastructure environment.

3.4 Case Study of IoT Service Platforms

The market is overwhelmed with number of IoT middleware platforms. Out of hundreds of IoT platforms, this chapter presents case study of four most popular platforms namely: Amazon Web Service (AWS) IoT, Microsoft Azure IoT, Google Cloud Platform, IBM Watson IoT. Each one of the following is discussed with requirements viewpoint.

3.4.1 Amazon Web Service (AWS IoT)

AWS IoT platform is developed by Amazon Web Services (AWS IoT 2019). It can connect millions of IoT devices through secure gateway. It is an integration of large number of middleware technologies working collaboratively. AWS has lot of inbuilt technologies supporting integration with heterogeneous devices, capturing data, securely transmission on cloud, support for device authorization and authentication, analytics tools. Besides these, AWS also supports number of third party applications. The technologies supported by AWS, to satisfy service and architectural requirements of the platform are given below.

Functional Requirements AWS follows publish subscribe mechanism for resource discovery. Each device connects to AWS via. gateway through secure channel protocols. Data is then passed through Rules Engine, which transforms data and pass it to the cloud services. At cloud end, Dynamo DB for NoSQL storage is deployed, lambda functions are used for event management. AWS supports dashboards for visualisation of data.

Non-functional Requirements AWS can scale millions of devices. It interconnects devices irrespective of their underlying architecture using API's and SDK's. It supports large number of programming language, and supports code migration. It can integrate with large number of Operating system through command line interface. Each device is authenticated and authorised using certificate, and is assigned unique ID. Data during transmission is secured through encryption and decryption. Overall AWS is easy to deploy, and uses pay as you use policy.

Architectural Requirements AWS provides programming abstraction, as user can program in any language. AWS has support for large number of interfaces. It has high fault tolerance and availability. Things Shadow maintains data related to device such as identification, location. It has centralized architecture, but supports distributed processing with Elastic MapReduce. The different features corresponding to requirements are summarized in Table 3.1.

3.4.2 Microsoft Azure IoT

Microsoft Azure IoT is developed by Microsoft (Azure IoT | Microsoft Azure 2019). It is considered to be only hybrid cloud service solution. Unlike, AWS IoT it can support pre-configured solutions. Azure has one of the powerful artificial intelligence support engine. It has number tools and technologies for securing capturing data, storing, and processing data. In response to various service and architectural requirements, various tools and technologies deployed are discussed below.

Table 3.1 AWS IoT features

Service requirements	
Functional requirements	
Resource discovery	Publish and subscribe mechanism via. Message broker on device gateway through MQTT or HTTP protocol
Resource management	Things registry is used to manage resources allocated with each device. Elastic load balancing to manage load in network
Data management	Amazon simple storage service (S3) provides scalable storage, dynamo DB provides NoSql databases, lambda for virtualization
Query processing	Rules engine using SQL language for message processing
Data visualization	Dashboards for visualization
Event processing	Amazon Kenesis for real time event processing. Simple notification service is used for event notifications. Lambda functions can trigger different events
Code management	Through in built SDK's can code in any language
Non-functional requirements	
Scalability	Can scale billions of heterogeneous devices
Timeliness	Amazon Kenesis with Kenesis analytics is used for real time processing
Availability	24 × 7
Security and privacy	Certificates for authentication, supports encryption decryption of data, user can define its own security rules and policies
Ease of deployment	Easy. With just registration
Architectural requirements	
Programming abstraction	Command line Interface is compatible with number of OS such as windows, Linux, and OSX. AWS SDK's allow user to program in any language
Interoperable	Rules engine makes it interoperable with other services
Service based	Support for large number of API's and SDK's make architecture service based
Adaptive	Not very adaptive friendly platform
Context-Awareneness	Things shadow maintain current state information of device
Autonomous	Each device can autonomously collaborate with other devices to exchange data using its unique identification number
Distributed	It has centralized architecture, but uses elastic MapReduce for processing

Functional Requirements Each device registers itself with azure directory service, which provides it a unique identification. Load balancing by azure platform is carried out both at local as well as global level. Supports both NoSQL storage for semi structured data, as well as support for SQL storage. It supports large azure analytics engine. Number of powerful tools for visualisation are also available. Supports real time event processing and code management.

Non-functional Requirements Azure can be scaled to large number of devices. Supports both real time as well as historic processing of data. In order to improve

availability, back up mechanism is deployed to make system fault tolerant. To provide device authentication, two way secure protocol is deployed.

Architectural Requirements Azure can be deployed either in windows, or linux platform. It has support for number of programming languages such as python, java, PHP, Node.js, etc. To interconnect large number of heterogeneous devices with different underlying architecture, number of inbuilt SDK's and APIs are available. Mean Time to Failure is quite low. Supports decentralized serverless architecture.

The service and architectural requirements of Microsoft azure are summarized in Table 3.2.

3.4.3 Google Cloud Platform

Google Cloud Platform (GCP) is developed by Google. It can connect heterogeneous IoT devices. It can support lightweight applications. It is considered to be server less architecture. GCP has support for large number of analytics libraries like tensor flow, etc. GCP is one of the powerful emerging IoT platform supporting large number of features, including support mobile applications. Various features supporting functional, non-functional and architectural requirements are given below:

Functional Requirements GCP uses publish subscribe mechanism for resource discovery. A registry of device is maintained. It supports BigTable storage solution, and firebase solution for real time processing of the event. Supports large number of programming languages interface.

Non-functional Requirements Can scale millions of devices. In order to make system fault tolerant, it deploys back up mechanism. Security and privacy is provided by authorisation and authentication of device. Firebase solution deals with the timeliness of the event execution. It supports large number of machine libraries like tensorflow to provide intelligent solutions.

Architectural Requirements GCP provides good programming abstraction by supporting large number of programming languages. Context aware applications are easy to deploy as each device in the network can be tracked by unique ID, and location. Suitable for lightweight mobile apps as well as client web applications. It uses centralized architectural approach.

The Service and architectural requirements of Google Cloud Platform are summarized in Table 3.3.

Table 3.2 Microsoft Azure features

Service requirements	
Functional requirements	
Resource discovery	Not much support for resource discovery
Resource management	Azure active directory. Supports both global level and local level load balancing
Data management	Support storage using Cosmos DB and processing, support for in-motion analytics. Data can also be stored in blob storage and Postgre storage
Query processing	Azure analytics through SQL syntax
Data visualization	Dashboards, power BI, web apps
Event processing	Support for predictive analytics, user can set a thresholds and alert limits through event hub
Code management	Supports code migration
Non-functional requirements	
Scalability	Scalability of ten million devices per instance
Timeliness	Support both historic and real time processing. Supports stream analytics
Availability	24 × 7. supports fault localization. Maintains backup to improve reliability
Security and privacy	Device authentication through two way secure protocol
Ease of deployment	Medium level difficulty
Architectural requirements	
Programming abstraction	Can scale with number of programming languages and command line interface through inbuilt tools and technologies
Interoperable	Agent libraries, SDK's allow interoperability within heterogeneous systems
Service based	Provides certain pre- configured solutions. Support number of architectures like event driven, microservices, n-tier, web-queue, and worker
Adaptive	MTTR is very low
Context-awareness	Azure active directory
Autonomous	Heterogeneous devices can work autonomously in collaboration to each other
Distributed	Decentralized serverless architecture

3.4.4 IBM Watson IoT

IBM Bluemix platform is recently named as IBM Watson IoT platform. It supports large number of cognitive analytics, and considered one of the popular platform for researchers (IBM Knowledge Center 2019). The various technologies provided by IBM Watson in view of functional, non-functional and architectural requirements are as follows:

Functional Requirements Each device in the network is connected via. Message broker through secure gateway. Each device is assigned a unique organisation ID. It supports both SQL databases and NoSql databases. Cognitive engine is deployed

Table 3.3 Google Cloud platform features

Service requirements	
Functional requirements	
Resource discovery	Uses pub/ sub scheme. Devices register through device id. Maintains registry of devices
Resource management	Devices managed through device drivers and protocol bridge. Deploy resource allocation
Data management	Cloud BigTable is used for data storage. Firebase database for real time processing. Supports both historic and real time data processing
Query processing	BigQuery is use for query processing
Data visualization	Dashboards
Event processing	Firebase database for real time event time processing
Code management	Support number of programming languages and libraries
Non-functional requirements	
Scalability	Can scale millions of devices
Timeliness	Real time processing though firebase
Availability	24 × 7. Fault tolerance through backup
Security and privacy	Authentication, authorization of device
Ease of deployment	Easy
Architectural requirements	
Programming abstraction	Number of programming languages
Interoperable	Number of libraries, lightweight libraries, APIs, SDK
Service based	Supports mobile apps, and end to end applications
Adaptive	Not very adaptive
Context-Awareness	With each device there is unique id, state information, telemetry
Autonomous	Each device with unique id can send stream of telemetry
Distributed	Centralized approach

for query processing. Dashboards and Jupyter notebook for visualization. Supports both historic and real time event processing.

Non-Functional Requirements can scale millions of devices. Kafka REST APIs are used to provide timeliness of event processing. Provide authentication, authorisation mechanism through protocols, with support for risk management. Platform is quite easy to deploy, making it popular choice among researchers.

Architectural Requirements Supports large number of programming language. Usually Node Red editor is used for programming. Suitable for deploying context aware apps. Supports large number of SDKs. Can be used to build lightweight as well as web apps. It has centralized architecture with support for distributed processing. The service and architectural requirements for IBM Watson are summarized in Table 3.4.

Table 3.4 IBM Watson features

Service requirements	
Functional requirements	
Resource discovery	Message broker for secure device registration via. Gateway
Resource management	Each device registers through unique organization id
Data management	Cloudant NoSql DB for real time processing. Data lake for SQL storage. DB2 for long term schema storage
Query processing	Has cognitive engine for providing data analytics capability. Supports machine learning. Supports both predictive and prescriptive analytics
Data visualization	Dashboards, support jupyter notebook
Event processing	Support historic and real time event processing
Code management	Supports code migration
Non-functional requirements	
Scalability	Can scale millions of devices
Timeliness	Real time processing through no SQL event streaming and Kafka REST APIs
Availability	High availability
Security and privacy	Unique authentication code for device identification. Supports risk management. Secure communication via. Protocols
Ease of deployment	Easier to deploy
Architectural requirements	
Programming abstraction	User can choose own programming language and architecture. Red node visual programming editor
Interoperable	Large number of SDK's
Service based	Framework supports client side application, mobile micro apps
Adaptive	Can adapt to changing environment
Context-awareness	Stores device id, last activity, geographic location
Autonomous	Each device has unique social id and can autonomously collaborate with each other
Distributed	Centralized architecture with support for distributed processing

3.5 Challenges and Open Research Problems

The IoT Platforms, still have lot of research challenges that need to be addressed in future research. The various challenges and open research problems related to IoT platforms are discussed below:

- Need for improved and more accurate models for resource discovery. IoT platform needs to address large number of request in timely and accurate manner. The present registry methods such as distributed, hybrid, or probabilistic does not fully cater this requirement (Teixeira et al. 2011). So, there is a need for designing better resource discovery models.

- Need for more efficient resource scheduling and management policies. Conflict of resources among IoT devices is a very common scenario. At present very few IoT platforms deploy strategies for resource conflict resolution. So, this is one of the area which need to be addressed in the future.
- More focus on support for data filtering. Data aggregation and filtering is one of the major steps in analysis. Most of the platforms provide data aggregation solution, but very few support on filtering of relevant and irrelevant data.
- Support for data compression. IoT generates huge amount of data, requiring large amount of storage. Proper data compression solutions can be deployed to reduce the amount of storage required.
- Support for changing business logic or IoT environment. Business logic and requirements keep on changing with time. Proper code allocation and migration strategies need to be deployed with support for firmware update.
- Support for Hard real time processing is required. Soft real time processing of events is done efficiently IoT. But, still addressing Hard time event is a challenge.
- Seamless replacement of modules to provide reliability in case of faults and failures is still a challenge.
- Service provising in case of failure to improve availability of a platform in seamless manner needs to be addressed in future research.
- Human intervention is required for deployment of devices on IoT platform. There is a need for pre-configured solutions to address this issue and reduce human efforts, making things automated and ease for deployment.
- Need to address syntactic and semantic interoperability. Most of the IoT platforms provide hardware interoperability with lesser focus on syntactic and semantic interoperability.
- Need for more dynamic rules and policies for making deployed system adaptable to run time environment.

3.6 Conclusion

In IoT scenario heterogeneous devices are connected and work collaboratively to achieve a particular goal. At the lowest layer, lies the resource constrained sensors, that senses the environment. To convert this information into meaningful insights, the data through sensors need to be stored and processed. All these packages need to be consolidated into one platform called as IoT platform. Number of vendors are available in the market with different requirements and specifications. Choosing the right one according to the need of application is the major key factor in successful deployment of application. The IoT platforms have come a long way, still they need to work on certain aspects to provide better functionality like security, resource provision, making more user friendly, easy device discovery, deployment and integration, better storage and resource management policies.

References

Agarwal, P., & Alam, M. (2019). Investigating IoT middleware platforms for smart application development. *arXiv preprint arXiv, 1810*, 12292.

Alam, M. (2012, December). Cloud Algebra for handling unstructured data in cloud database management system. *International Journal on Cloud Computing: Services and Architecture (IJCCSA)*, *2*(6) ISSN: 2231 – 5853 [Online], 2231 – 6663 [Print], https://doi.org/10.5121/ijccsa.2012.2603, Taiwan.

Alam, M., & Shakil, K. A. Presented "Big Data analytics in Cloud environment using Hadoop. In International conferences on Mathematics, Physics & Allied sciences-2016, March 03–05, 2016, Goa.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials, 17*(4), 2347–2376.

Ali, S. A., Affan, M., & Alam, M. (2019). A study of efficient energy management techniques for Cloud Computing environment. *2019 9th International conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 13–18), Noida, India. https://doi.org/10.1109/CONFLUENCE.2019.8776977.

Apolinarski, W., Iqbal, U., & Parreira, J. X. (2014, March). The GAMBAS middleware and SDK for smart city applications. In *2014 IEEE International conference on pervasive computing and communication workshops (PERCOM WORKSHOPS)* (pp. 117–122). IEEE.

Asghari, P., Rahmani, A. M., & Javadi, H. H. S. (2019). Internet of things applications: A systematic review. *Computer Networks, 148*, 241–261.

Ashton, K. (2009). That 'internet of things' thing. *RFID Journal, 22*(7), 97–114.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks, 54*(15), 2787–2805.

AWS IoT. (2019). Retrieved September 12, 2019, from https://docs.aws.amazon.com/iot/index.html

Azure IoT | Microsoft Azure. (2019). Retrieved September 12, 2019, from https://azure.microsoft.com/en-in/overview/iot/

Cheng, B., Longo, S., Cirillo, F., Bauer, M., & Kovacs, E. (2015, June). Building a big data platform for smart cities: Experience and lessons from santander. In *2015 IEEE International congress on Big Data* (pp. 592–599). IEEE.

Cretu, L. G. (2012). Smart cities design using event-driven paradigm and semantic web. *Informatica Economica, 16*(4), 57.

da Cruz, M. A., Rodrigues, J. J. P., Al-Muhtadi, J., Korotaev, V. V., & de Albuquerque, V. H. C. (2018). A reference model for internet of things middleware. *IEEE Internet of Things Journal, 5*(2), 871–883.

Fabisch, M., & Henninger, S. (2019). ESPRESSO–systemic standardisation approach to empower smart cities and communities. *Smart Cities in Smart Regions, 2018*, 115.

Fahmideh, M., & Zowghi, D. (2020). An exploration of IoT platform development. *Information Systems, 87*, 101409.

Filipponi, L., Vitaletti, A., Landi, G., Memeo, V., Laura, G., & Pucci, P. (2010, July). Smart city: An event driven architecture for monitoring public spaces with heterogeneous sensors. In *2010 Fourth International Conference on Sensor Technologies and Applications* (pp. 281–286). IEEE.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660.

Guo, B., Zhang, D., & Wang, Z. (2011, October). Living with internet of things: The emergence of embedded intelligence. In *2011 International conference on internet of things and 4th international conference on cyber, physical and social computing* (pp. 297–304). IEEE.

IBM Knowledge Center. (2019). Retrieved September 12, 2019, from https://www.ibm.com/suport/knowledgcenter/SSQP8H/iot/overview/architecture.html

Khan, Z., Anjum, A., Soomro, K., & Tahir, M. A. (2015). Towards cloud based big data analytics for smart future cities. *Journal of Cloud Computing, 4*(1), 2.

Khan, S., Shakil, K. A, & Alam, M. (2017). *Cloud based Big Data Analytics: A survey of current research and future directions, Big Data Analytics* (pp 629–640). Springer, Print ISBN: 978-981-10-6619-1, Electronic ISBN: 978–981-10- 6620-7.

Nitti, M., Pilloni, V., Giusto, D., & Popescu, V. (2017). Iot architecture for a sustainable tourism application in a smart city environment. *Mobile Information Systems, 2017*.

Overview of Internet of Things | Solutions | Google Cloud. (2019). Retrieved September 12, 2019, from https://cloud.google.com/solutions/iot-overview

Petrolo, R., Loscri, V., & Mitton, N. (2014, August). Towards a smart city based on cloud of things. In *Proceedings of the 2014 ACM international workshop on wireless and mobile technologies for smart cities* (pp. 61–66). ACM.

Razzaque, M. A., Milojevic-Jevric, M., Palade, A., & Clarke, S. (2015). Middleware for internet of things: A survey. *IEEE Internet of Things Journal, 3*(1), 70–95.

Santana, E. F. Z., Chaves, A. P., Gerosa, M. A., Kon, F., & Milojicic, D. S. (2018). Software platforms for smart cities: Concepts, requirements, challenges, and a unified reference architecture. *ACM Computing Surveys (CSUR), 50*(6), 78.

Sarhan, A. (2019). Cloud-based IoT platform: Challenges and applied solutions. In *Harnessing the Internet of Everything (IoE) for accelerated innovation opportunities* (pp. 116–147). Hershey: IGI Global.

Silva, B. N., Khan, M., & Han, K. (2018). Internet of things: A comprehensive review of enabling technologies, architecture, and challenges. *IETE Technical Review, 35*(2), 205–220.

Soldatos, J., Kefalakis, N., Hauswirth, M., Serrano, M., Calbimonte, J. P., Riahi, M., et al. (2015). Openiot: Open source internet-of-things in the cloud. In *Interoperability and open-source solutions for the internet of things* (pp. 13–25). Cham: Springer.

Teixeira, T., Hachem, S., Issarny, V., & Georgantas, N. (2011, October). Service oriented middleware for the internet of things: A perspective. In *European conference on a service-based internet* (pp. 220–229). Berlin/Heidelberg: Springer.

Tiwana, A. (2013). *Platform ecosystems: Aligning architecture, governance, and strategy*. Oxford: Newnes.

Wang, H., Zhou, X., Zhou, X., Liu, W., Li, W., & Bouguettaya, A. (2010, December). Adaptive service composition based on reinforcement learning. In *International conference on service-oriented computing* (pp. 92–107). Berlin/Heidelberg: Springer.

Yaqoob, I., Ahmed, E., Hashem, I. A. T., Ahmed, A. I. A., Gani, A., Imran, M., & Guizani, M. (2017). Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges. *IEEE Wireless Communications, 24*(3), 10–16.

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. S. (2017). Security and privacy in smart city applications: Challenges and solutions. *IEEE Communications Magazine, 55*(1), 122–129.

Part II
Solutions and Enablers for IoT

Chapter 4
Resource Management Techniques for Cloud-Based IoT Environment

Syed Arshad Ali, Manzoor Ansari, and Mansaf Alam

Abstract Internet of Things (IoT) is an Internet-based environment of connected devices and applications. IoT creates an environment where physical devices and sensors are flawlessly combined into information nodes to deliver innovative and smart services for human-being to make their life easier and more efficient. The main objective of the IoT devices-network is to generate data, which are converted into useful information by the data analysis process, it also provides useful resources to the end-users. IoT resource management is a key challenge to ensure the quality of the end user's experience. Many IoT smart devices and technologies like sensors, actuators, RFID, UMTS, 3G, and GSM etc. are used to develop IoT networks. Cloud Computing plays an important role in these networks deployment by providing physical resources as virtualized resources consist of memory, computation power, network bandwidth, virtualized system and device drivers in secure and pay as per use basis. One of the major concerns of Cloud-based IoT environment is resource management, which ensures efficient resource utilization, load balancing, reduces SLA violation, and improve the system performance by reducing operational cost and energy consumption. Many researchers have been proposed IoT based resource management techniques. The focus of this paper is to investigate these proposed resource allocation techniques and finds which parameters must be considered for improvement in resource allocation for IoT networks. Further, this paper also uncovered challenges and issues of Cloud-based resource allocation for IoT environment.

Keywords IoT · Cloud computing · Resource allocation · Parameters · Fog computing

S. A. Ali (✉) · M. Ansari · M. Alam
Department of Computer Science, Jamia Millia Islamia, New Delhi, India
e-mail: arshad158931@st.jmi.ac.in; manzoor188469@st.jmi.ac.in; malam2@jmi.ac.in

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_4

4.1 Introduction

The Internet of Things (IoT) is a set of connected smart device and sensors over the Internet. These devices are connected using the wired/wireless network technologies to communicate and transfer data from one node to another (Al-Fuqaha et al. 2015; Horrow and Sardana 2012; Pourghebleh and Navimipour 2017; Yang et al. 2013). The things in the IoT infrastructure network are sensors, smart devices, sensor data, software agents and human beings (Yan et al. 2014). These networked independent devices make local network and connected to the global network to share information with others in real-time to realize that the Things are connected into the real world and connect all devices (Alaba et al. 2017; Lee and Lee 2015; Mattern and Floerkemeier 2010). In the cyber-physical ecosystem, each edge-node is supposed to an IoT device which can dynamically cooperate with other devices in the network to execute one or more user's tasks allocated to the system network. Resources like processing power, storage, network bandwidth, RAM are usually limited in these IoT networks, though these infrastructures and computing resources are provided by the Cloud service providers. IoT devices produce a huge amount of real-time data from the sensors. Cloud storage is used for storing these real-time data on different local networked data centres, which upload these data to the global networked data centres to allow access for all globally situated smart devices (Bassi et al. 2013). In this paper, the author studied various resource allocation techniques for Cloud-based IoT system. Classification of these techniques has been done based on parameters like QoS, context, cost, energy consumption and SLA. Furthermore, the author also discussed various parameters of resource allocation techniques of the IoT system.

4.2 Basic Concepts of IoT, Cloud and Resource Management

4.2.1 What Are the Basic Elements of the IoT Environment?

Internet of things offers numerous advantages and services to the users. Therefore, to use them correctly, some elements are needed. The IoT elements will be discussed in this section. Figure 4.1 shows the elements required to provide IoT functionalities.

4.2.1.1 Identifiers

Within the network, it offers an explicit identity for each object. In identification, two processes exist naming and addressing. The naming relates to the object's title whereas the addressing explains the address of an object. These two processes are very different even though two or more objects could have the same name, but they

Fig. 4.1 Basic elements of the IoT environment

are always different and unique. There are several approaches accessible which expedite the naming of objects in the network, such as ubiquitous codes (uCode) and electronic product codes (EPCs) (Koshizuka and Sakamura 2010). Using IPv6, each object has a unique address. First, IPv4 was used to allocate the address, but due to a huge amount of IoT devices, it was unable to address the need. IPv6 is therefore used because it uses a 128-bit addressing system.

4.2.1.2 Sensing Devices

This involves acquiring information from the environment and transferring it to a local, remote or Cloud-based database as an instance of the IoT sensor. We can identify intelligent devices, portable sensors or actuators. The collected information is transmitted to the storage medium. Numerous detection devices to collect data on objects such as RFID tags, actuators, portable sensors, smart sensors, etc.

4.2.1.3 Communications Devices

To achieve smart services, IoT communication techniques communicate heterogeneous artifacts. One of the main goals of the Internet of things is Communication in which various devices connect and communicate with each other. In the communication layer, devices can transfer and deliver messages, documents and other information. There are many methods which facilitate communication, for example

Bluetooth (Mcdermott-Wells 2004), radio frequency identification (RFID) (Want 2006), long term evolution (LTE) (Crosby and Vafa 2013), Wi-Fi (Ferro and Potorti 2005) and near-field communication (NFC) (Want 2011).

4.2.1.4 Compute Devices

The computation of the data collected by the objects is achieved using sensors. It is used to develop processing in IoT applications. Raspberry Pi, Arduino, and Gadgeteer are utilized for hardware platforms, whereas the operating system plays a significant role in the processing of software platforms. There is various kind of operating systems are used, including Lite OS (Cao et al. 2008), Riot OS (Baccelli et al. 2013), Android, Tiny OS (Levis et al. 2005) etc.

4.2.1.5 Services IoT

Applications provide four types of services (Gigli and Koo 2011; Xing et al. 2010). The first service that is associated with an identity. It is used to acquire the identity of the objects which sent the request. The aggregate of information is another service aimed at collecting all the data about the objects. The aggregation service also performs the processing. The third service refers to co-operative service that makes decisions based on the information gathered and transfer suitable rejoinders to the devices. The last service is the pervasive service, which is used to replace devices immediately without rigidity in terms of time and place.

4.2.1.6 Semantics

They are the IoT's concern to facilitate the consumers who perform their tasks. To fulfil its responsibilities, it is the most important component of IoT. It performs as the IoT's brain. It accepts all the information and makes the appropriate decisions to send responses to the devices.

The key techniques used in each IoT component are presented in Table 4.1.

Table 4.1 Key technologies used by IoT components

IoT components	Main technologies
Identification	IPv4, IPv6 Electronic product code(eCodes), ubiquitous code (uCode),
Sensing	Actuators, Sensors, Wearable Sensing Devices, RFID Tags.
Communications	Wireless Sensor Network (WSN), Long Term Evolution (LTE), Bluetooth, Near Field Communication (NFC), Radio Frequency Identification (RFID),
Computation	Intel Galil Operating System, Arduino, Raspberry Pi.
Services	Collaborative-Aware, Ubiquitous Identity-Related, Information Aggregation
Semantics	EXI, OWL, RDF

4.2.2 What Are the Various IoT Architecture Frameworks?

An IoT architecture can be viewed from three viewpoints: Things-oriented, Internet-oriented and semantic-oriented (Atzori et al. 2010). In things-oriented viewpoint, the intelligent autonomous smart devices are connected to each other using NFC and RFID technologies for specific daily life applications. Internet-oriented viewpoint focuses on how these smart devices connect to the internet using unique identification (IP addresses) and standard communication protocols to facilitate the global connections among these applications based smart devices. In the semantic viewpoint of IoT architecture, the data generated by the IoT devices are used to generate useful information and handle the architectural modelling problems efficiently using these produced information (Marques et al. 2017).

In the opinion of most researchers on conventional IoT architecture, it is considered at three layers: -Perception Layer, Network Layer, Application Layer. In addition, some researchers have analyzed another layer also included in the latest IoT architecture, which is a support layer located between the network layer and the application layer. Multi-tier architecture of IoT is displayed in Fig. 4.2.

The support layer consists of fog computing and Cloud Computing. In this section, we define seven-tier architecture: collaboration and processes, applications, data abstraction, data accumulation, edge computing, connectivity, physical devices and controller. The basic layered architecture of IoT and its components in each layer have been depicted in Fig. 4.3.

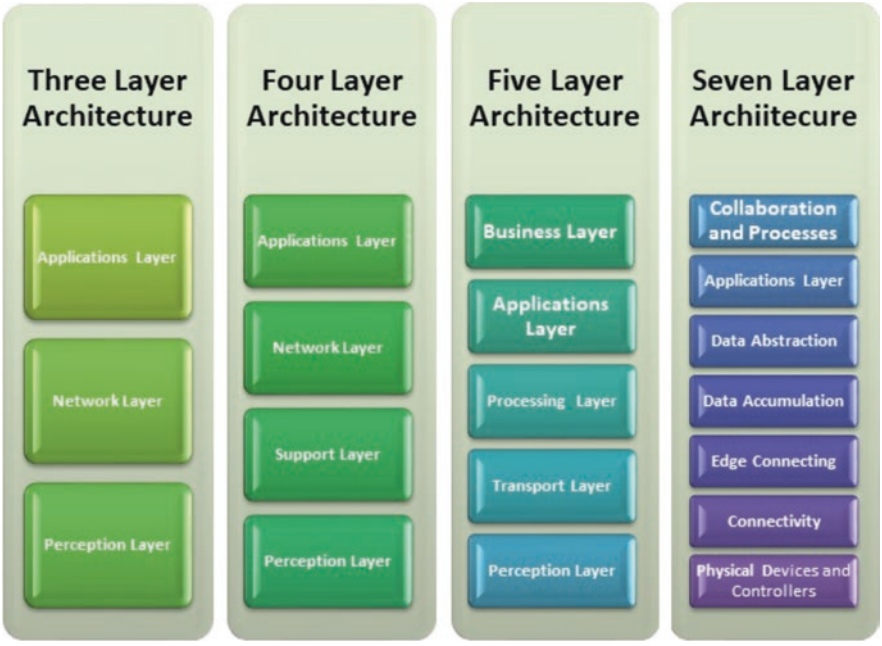


Fig. 4.2 Multi-tier IoT architecture

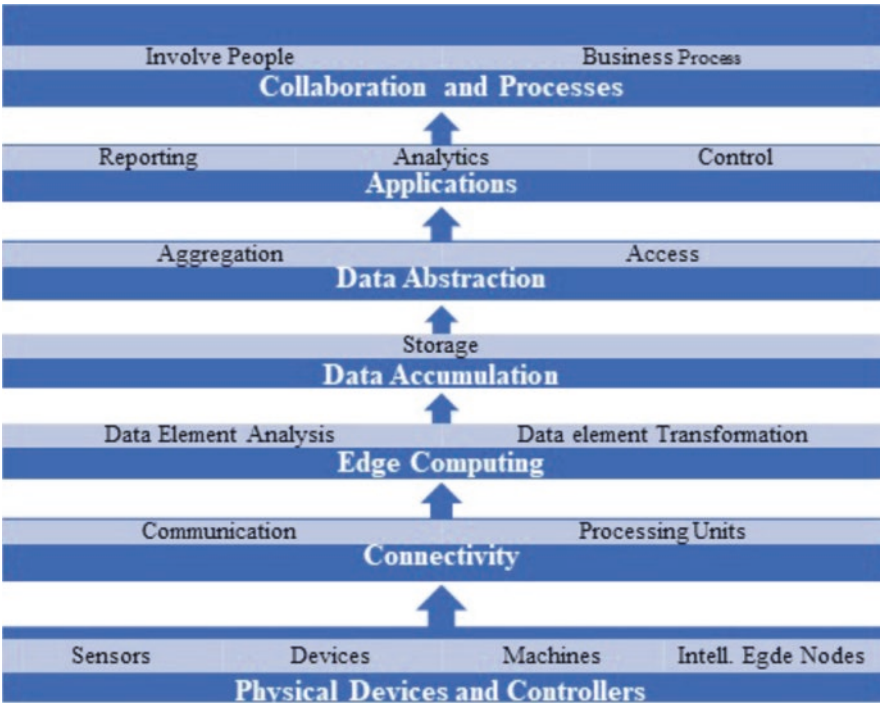


Fig. 4.3 Basic architecture of IoT

4.2.2.1 Layer 1: Physical Devices and Controllers

It is a layer of perception or hardware that collects and sends information from the physical world to the next layer. This layer includes objects and physical sensors. Basically, this layer is intended to detect various objects and collect environmental data such as humidity, temperature, water quality, pressure, air quality, motion detection etc. Controllers and Physical devices can control multiple devices. These are the "things" in the IoT containing a wide range of endpoint devices for sending and receiving information. The list of devices is already extensive today. It will be effectively unlimited as more devices will be added to the IoT over time.

4.2.2.2 Layer 2: Connectivity

This layer is used to interact with various IoT components via interconnecting systems such as switches, gateways as well as routers. In addition, it transfers data collected strongly from the sensors to the top layer for processing. It includes transferring data from physical devices to Cloud or other devices, which may be in the form of ZWave, SigFox Zigbee or Bluetooth. This layer extends to Cloud transport services from the "intermediate" of an Edge Node device.

4.2.2.3 Layer 3: Edge Connecting

The next phase is Edge Computing, or more appropriately "Cloud Edge" or "Cloud Gateway". Layer 3 requires data from the connectivity phase and makes it suitable for archiving and higher-level processing information. The processing elements in this layer work with a large volume of data that could transform some facts to moderate data size.

4.2.2.4 Layer 4: Data Accumulation

They must be stored after the data is accumulated. It is important where information is stored. While some data may be stored to the limit, most data will have to be delivered to the Cloud. Big Data machines will be able to exploit their computing power and analyze the data. The main objective of this layer is to store the data of Phase 3. Acquire and store a large amount of data and place them in the warehouses so that they are accessible from the upper layers. As a result, it simply modifies event-based data in query-based processing information for the higher layer. This layer can be deployed in SQL or requires a more sophisticated Hadoop and Hadoop file system, Mongo, Cassandra, Spark or other NoSQL solutions.

4.2.2.5 Layer 5: Data Abstraction

This layer combines data from different sources and converts the stored data to the appropriate application format in a manageable and efficient way (Atlam et al. 2017). A main component of the large-scale high-performance implementation architecture is a publishing/subscription software framework or a data distribution service (DDS) to simplify data movement between edge computing, data accumulation, application layers and processes. Whether it's a high-performance service or a simple message bus, this infrastructure simplifies deployment and improves performance for all applications, except for the simplest.

4.2.2.6 Layer 6: The Application Layer

It applies to information elucidation from different IoT applications. It comprises several IoT applications, like medical care, smart city, smart network, smart agriculture, smart building, connected car etc. (Stallings 2015). This phase is self-explanatory where the application logic of the control plan and the data plan are performed. Process optimization, logistics, statistical analysis, control logic, Monitoring, alarm management, consumption models are just certain cases of IoT applications.

4.2.2.7 Layer 7: Collaboration and Processes

At this phase, application processing and collaboration are presented to users, and the processed data in the lower layers are incorporated into commercial purposes. It encompasses collaboration, people, businesses, and decision-making processes based on IoT-derived information. This layer classifies people who can collaborate and communicate to use IoT data proficiently. It delivers additional features, such as the creation of commercial graphics and models and other data-based recoveries from the application layer. It also helps executives make accurate business decisions based on data analysis (Muntjir et al. 2017).

4.2.3 How Cloud Computing Supports IoT Infrastructure?

National Institute of Standards and Technology (NIST) defined Cloud Computing as a paradigm that enables global, appropriate and on-demand self-serviced shared pool of computing resources (network, storage, applications and services) to the end-user on pay per use basis with minimal effort or service provider communication (Mell and Grance 2011). Cloud Computing is used rapidly by IT industries and professional for the deployment of their projects due to minimal cost and rapid elastic characteristics of Cloud- services (Varghese and Buyya 2018). Cloud Computing is an Internet-based technology that facilitates both service-consumers and providers by its essential features of On-demand self-service, broad network access, resource pooling, rapid elasticity and measured services (Zhang et al. 2010). Cloud Computing has three service models and four deployment models. Cloud Service provider's software running on Cloud set-up is used by the Cloud consumers in Software as a service (SaaS) model. Cloud consumers can deploy their applications on to the provider's infrastructure using software design languages, libraries and tool provided by the Cloud infrastructure in Platform as a Service (PaaS) model. In Infrastructure as a Service (IaaS) model, a consumer can provide a pool of resources like storage, processing elements, network and another basic computing requirement for running any software and operating system provided by the Cloud provider as a virtual machine (VM) (Wang et al. 2010). Cloud Computing also provides four deployment model as per the user priorities and features named as public, private, community and hybrid Cloud deployment models (Subashini and Kavitha 2011). Due to massive features and ability, Cloud Computing is used by many growing technologies, IoT is one among them. Integration of IoT with Cloud Computing has been intensively used by many real-life applications like smart cities, healthcare, agriculture industries, transportation, smart vehicles and many more (Malik and Om 2018). The current trends of technologies are moving towards the use of globally connected smart devices, which produces a huge amount of data that cannot be stored in locally due to limited storage capacity. The running fuel of all industries is the data, data is useless without its analytics to get useful information for industries future-plans and policies. The huge amount of data gathered by the

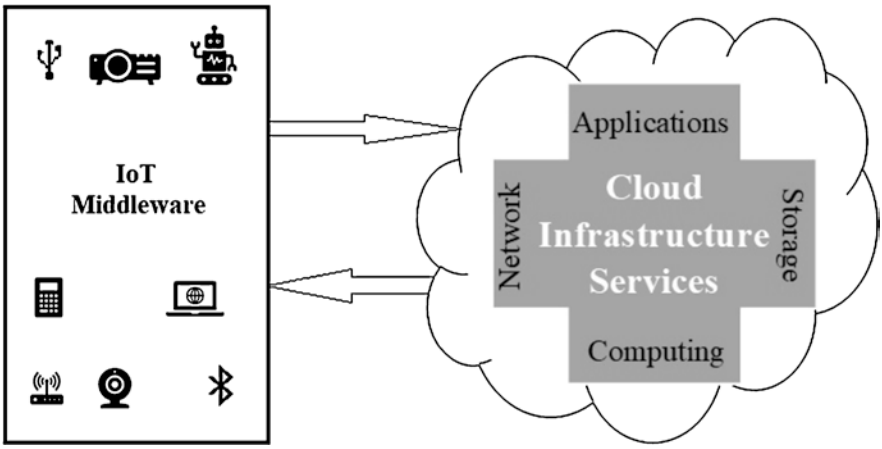


Fig. 4.4 How cloud support IoT applications

smart connected devices needs powered computing systems that should capable enough to compute this huge amount of data. The local systems are not capable enough to process these data for analytics. These limitations of huge storage space, computing power and network bandwidth can be overcome using pooled resources provide by Cloud Computing. Figure 4.4 illustrates how Cloud Computing supports IoT for smooth functionality. Cloud Computing infrastructure is used between the applications and IoT devices as a hidden layer, where all functionalities are hidden from the implementation of IoT based applications (Evans 2011).

4.2.4 Why Resource Allocation Is Important for IoT?

Highly efficient maintained and cost-benefit network ensures the Quality of Service (QoS) standards. IoT architecture has various resources connected with the network. The resource allocation is an important aspect for QoS standards because of the efficient and effective allocation of resources in the IoT network. Resource allocation is also responsible for a high standard of security because in IoT architecture the data is divided into many data streams gathered from different sensors and different types of services are provided by the networked devices. The IoT networked resources consist of computing elements, storage and energy. Efficient Cloud resource allocation helps IoT networked devices to utilize these resources in an efficient and cost-effective way to improve system performance and productivity. IoT devices and resources are heterogeneous and globally distributed in nature, therefore, resource allocation and management are very important aspect of the IoT environment. The entity in the IoT network system can be an object, a human being or a place that is used to communicate between the IoT system application and the system user. These allocated objects are known as resources which can be

categorized based on the information they communicate in the network. The three-layered IoT system mainly used are classified in IoT things, edge and Cloud infrastructure as described in Fig. 4.5. Allocation of resources by the system to accomplish the user tasks required various phases, first, the system selects the required resource from these three layers, then it selects the nodes which are capable to execute the user's tasks and after that, it schedules the user's task to the selected node for its execution. Finally, communication among these networked resources is done to accomplish the successful execution of the user's task. Resource allocation has many aspects of resource discovery, resource provisioning, resource scheduling and resource monitoring as well. An effective Resource allocation supports standard Quality of Service (QoS), cost minimization, energy consumption reduction, increase resource utilization and moreover, it guaranteed the Service level agreement between the Cloud-based IoT system application providers and costumers where user's requirements should be matched in an effective way.

Resource allocation for IoT devices has many challenges due to heterogeneity and distance between the devices. A lot of research work has been done by the industries and academic researchers, but many challenges and issues related to IoT resource allocation are up till now untouched. Many researchers are working to solve these challenges and proposed new methods and algorithms for this. In this paper, the author systematically reviewed many proposed methods for resource allocation in Cloud-based IoT environment and classifies these techniques based on characteristics and resource allocation parameters improved by the technique.

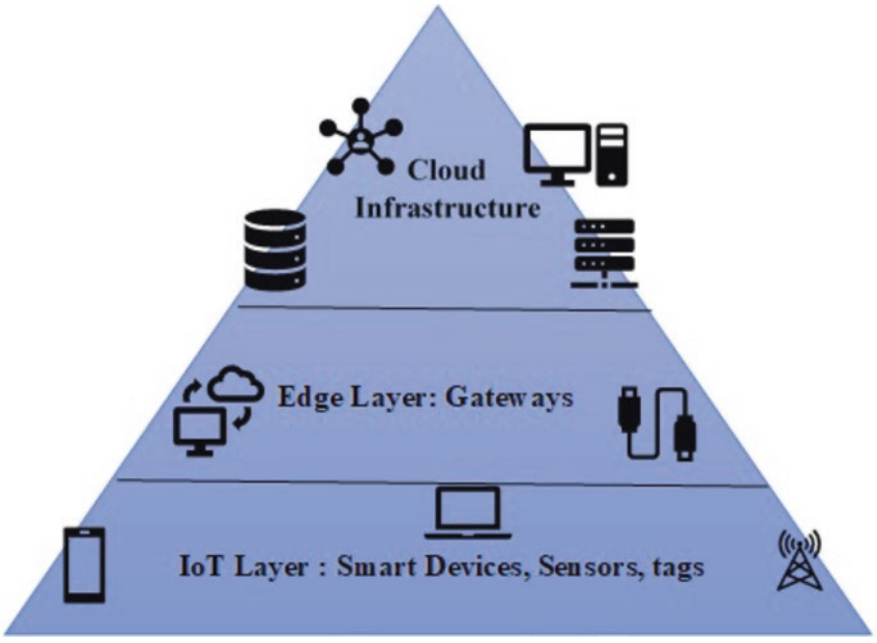


Fig. 4.5 Three-tier architecture (IoT, Edge and Cloud)

Furthermore, the author discussed various parameters of IoT resource allocation and what parameters are still needed more improvements.

4.3 Related Works

Many research papers have on been published related to survey and review of IoT technologies, wireless sensor network, integration of IoT and Cloud Computing and IoT architectures. But there is only one survey paper is present on the resource allocation in the IoT environment. Many researchers are working on various aspects of IoT architecture. The proposed methods and technologies that support the IoT networked system for smooth and cost-effective performance. No review paper exists for Cloud-based IoT resource allocation techniques. The author presented an important survey in (Lin et al. 2017), that discussed various challenges and issues of IoT resource allocation from the architectural viewpoint. In this review paper, the author discussed the architectures and infrastructures that are responsible for resource allocation of the IoT environment. Resource scheduling and optimization techniques form the Cloud perspectives are not discussed in this paper. Another review paper is (Delicato et al. 2017) based on various IoT technologies and their challenges. In this paper, the author finds the relation between fog computing and IoT also discussed various existing resource allocation techniques in fog based IoT environment. The author discussed two main challenges in fog based IoT infrastructure, first is that the fog computing neither cares about the nearest node which provides computing resource nor data processing, it only cares about the minimum delay. The second issue the author found is that the resource allocation between the fog and IoT smart devices, because of the limited resource capacity of fog computing. To solve this problem of scarcity of fog resources, the author suggests the use of Cloud Computing above fog computing. In this paper, the author studied various Cloud-based IoT resource allocation techniques and classified these techniques in different groups. Further limitation and improvement were done in these techniques are also discussed and presented in the tabular form. Various resource allocation parameters have been listed out and defined. The author also discussed How much improvements have been done in these parameters and how much improvement still needed in remaining parameters.

4.4 Classification of Cloud-Based IoT Resource Management Techniques

In this section, the author studied and classified Cloud-based IoT resource allocation techniques in various categories according to the feature provided by the technique under study. The detailed classification of IoT resource allocation techniques is described in Fig. 4.6. Various papers have been studied and categorized under these categories of IoT resource allocation.

Fig. 4.6 Classification of IoT resource allocation techniques

4.4.1 SLA-Aware IoT Resource Allocation

Service level agreement between the providers and consumer is very important in any service-oriented system. The SLA violation should be minimum to increase the profit of the service provider and satisfied the customer's requirements. Many kinds of research have been done in this area of interest to reduce the SLA violation to improve the system acceptability among the costumers. Some research works are also done related to the SLA oriented resource allocation for IoT enable the system. In (Choi and Lim 2016), the author considered the penalty cost of SLA violation.

A combinatorial auction method is proposed to reduce the penalty of SLA violation by calculating the provider's profit and announce a winner to the user who gives maximum profit to the providers so the penalty cost would be minimized to avoid SLA violation. Another SLA violation-based technique is proposed in the paper (Singh and Viniotis 2016). The author proposed a method to limit the user's task and schedule it efficiently to minimizes SLA violation. The proposed method divides the user task into multiple subtasks and increases the server's capacity to decrease the total measurement time of task execution to reduce SLA violation and maximize providers profits. Another SLA-aware resource allocation method for IoT devices is proposed in (Alsaffar et al. 2016), the author presented an architectural based service delegation and resource allocation method for Cloud and fog computing based IoT environment. An SLA and QoS oriented algorithm have been proposed that used linearized decision tree to manage user tasks. A new SLA oriented IoT resource allocation problem handled in (Singh and Viniotis 2017), by buffering scheduling and limit the rate of user's tasks to achieve SLA. The proposed method conforms

Table 4.2 SLA-aware IoT resource allocation techniques

Algorithm	Improvement	Limitations
SLA-Based Resource Allocation (Choi and Lim 2016)	Reduce SLA violation and increase system performance	The proposed method is not compared with other techniques
Cloud-based SLA-aware Resource Allocation (Singh and Viniotis 2016)	User's task is divided into subtasks to reduce SLA violation	The task arrival time is not calculated dynamically
IoT service delegation and resource allocation (Alsaffar et al. 2016)	Improve system performance and efficiency	There is no evidence of practical implementation.
Resource allocation for IoT applications (Singh and Viniotis 2017)	Improve system performance and reduce SLA violation by reducing the measurement time of task arrival.	The proposed method is not working in a multi-tenant environment like multiple data centres

the SLA violation without knowing the arrival pattern of the user's task in advance and works better in huge traffic of IoT devices in the IoT network. These algorithms and their improvement and limitations are described in Table 4.2.

4.4.2 Context-Aware IoT Resource Allocation

Game theory has been applied in many types of research for resource allocation in the device to device communication for IoT devices. Resource allocation is an important aspect for the high performance of data transportation in a wireless network for device to device communication. A location-aware method has been extended in (Huang et al. 2015), that applied the Nash Equilibrium game model for D2D communication in a cellular network. The author proposed a context-aware algorithm that determines the bandwidth of the network to maximize the total use of each station for communication according to the different situations. A cell association problem has been formulated in (Hamidouche et al. 2017) as a two-way matching process between the communicating devices. The proposed model used a correlation among the devices that are present in each area network to enhance the cell association technique and guaranteed to a prevalent outcome. Another one-many devices' association based optimal resource allocation method proposed in (Abedin et al. 2015) that increased the resource utilization among the network devices. Dynamic QoS requirements have been achieved by the proposed context-aware resource allocation method between peer to peer IoT network system. Table 4.3 shows the improvements and limitations of context-aware resource allocation techniques.

Table 4.3 Context-aware IoT resource allocation techniques

Algorithm	Improvements	Limitations
A game-theory based D2D communication in a Cloud-Centric IoT network (Huang et al. 2015)	D2D communication improved by applied Nash equilibrium game model, maximize bandwidth utilization	This approach is only Cloud-centric and compared with the existing algorithms
Correlation-based resource allocation method (Hamidouche et al. 2017)	Repeated information generated by the different devices has been reduced for better performance in cell association method	The practical evidence is not mentioned in the method
Optimal resource allocation method (Abedin et al. 2015)	Resource utilization and performance have been increased	The method has not practical evidence

4.4.3 QoS-Aware IoT Resource Allocation

Quality of Service (QoS) is an important aspect of any service-based application. The quality of service should be matched with the service level agreement (SLA). Several pieces of research have been done in this area for a different scenario. A QoS-based IoT resource allocation method has been proposed in (Chen et al. 2012), which reduced the intrusion between the device to device communications. With the help of PFR method and intrusion limited area control method, the use of resources can be restricted to D2D users. The D2D users get the resources according to the wireless network channel gain, which balances the system workload and enhances the system performance. An analytical model for heterogeneous traffic of M2M devices has been proposed in (Shorgin et al. 2015), which used fixed transmission nodes for M2M devices according to the user's requirements to achieve QoS constraints. An optimization protocol has been proposed in (Colistra et al. 2014a), which is based on the consensus algorithm for robust and efficient resource allocation in the heterogeneous IoT networks. The algorithm considered the task frequency and buffer occupancy of nodes that are involved in the communication. The method is adaptive in dynamic and heterogeneous feature of IoT device networks. Two communication-based resource allocation method for IoT has been proposed in (Colistra et al. 2014b), which used broadcast and gossip methods among the nodes for exchange and update the communication information. The proposed method has been evaluated in three different scenarios: the entire network, single task — single frequency and single task — total frequency. The output error of the system has been reduced to 5% with compared to the centralized solution for the reduction of message transfer and increase the system reliability. QoS-based resource allocation methods with features and limitations are described in Table 4.4.

Table 4.4 QoS-aware IoT resource allocation techniques

Algorithm	Improvements	Limitations
Downlink resource allocation method (Chen et al. 2012)	The intrusion among the communication channel has been reduced and enhanced the system performance	Practical implementation is missing
Radio Resource Allocation Scheme (Shorgin et al. 2015)	The traffic among the M2M devices has been reduced	The method is not implemented in real conditions
Task allocation in group of IoT devices (Colistra et al. 2014a)	The optimal resource allocation has been achieved with 5% error	The QoS parameter needs more attention
Consensus-based task allocation in IoT (Colistra et al. 2014b)	Gossip and broadcast methods are used in which broadcast gives better results	The QoS and real conditions have less considered.

4.4.4 Energy-Aware IoT Resource Allocation

Due to the huge amount of heterogeneous and more electric power consumed smart devices, it is important to handle the efficient use of electricity or power to reduce the carbon footprints and produce a green computing environment. In many fields like Cloud Computing, fog computing and edge computing, many researchers have been already done a lot of work to reduce power consumption. In IoT based environment there is also some evidence of work in the reduction of power consumption. In (Baccarelli et al. 2017) a novel resource allocation method for the fog of everything (FoE) has been proposed that presents the energy-delay performance of virtual fog of everything (V-FOE) and compared with the V-D2D technological platform. Three ways of communication between the devices in fog computing architecture network (FOCAN) (Naranjo et al. 2017) has been described to meet the QoS and reduce power usage in an effective way. This approach is used in Fog-supported smart cities architecture to share infrastructure resources among smart devices. A generalized Nash equilibrium (GNE) approach and its unique conditions are derived in (Abuzainab et al. 2017), to handle the heterogeneity of IoT resources, in terms of QoS and resource constraints. A cognitive hierarchy game theory has been used in this method to enable the devices to reach CH equilibrium (CHE) for rationally corresponds to the heterogeneous computing capability and access information of each MTDs and HTDs. The proposed model reduces energy consumption by MTDs by 78%. Another novel ECIoT architecture has been proposed in (Li et al. 2018), to additional, improve the system performance by control the process admission and control the power consumption of the resource of the IoT system. A Lyapunov stochastic optimization based cross-layer dynamic network optimization method is used in ECIoT to enhance the system utility. Table 4.5 shows the limitations and improvements done in these proposed algor**ithms.**

Table 4.5 Energy-aware IoT resource allocation techniques

Algorithm	Improvements	Limitations
Energy-efficient resource allocation for Fog of Everything (Baccarelli et al. 2017)	Reduce energy consumption and delay and enhance the performance of the FOE system	Real-time testing has not done
FOCAN: A Smart city architecture for resource allocation (Naranjo et al. 2017)	The method reduces energy consumption and improves latency.	Implementation is not done
Cognitive hierarchy theory for resource allocation (Abuzainab et al. 2017)	The method reduces power consumption by 78%	The only Simulation is done
Joint admission control resource allocation (Li et al. 2018)	Increased System Throughput and reduce the delay between devices communication	No evidence of practical implementation.

4.4.5 Cost-Aware IoT Resource Allocation

IoT network consists of many heterogeneous and many powerful resources needed smart devices which are managed by Cloud Computing, fog computing as well as edge computing infrastructures. These multiple network devices of IoT request the resources for their task completion to fulfil the QoS. The total utilization cost has been calculated according to the served resources and activation cost of each interface devices in the network to serve demand. This cost estimation problem is known Service-to-Interface Assignment cost problem. Two SLA methods are proposed mathematically in (Angelakis et al. 2016) to reduce the computational cost. In the first method, the demand for the resource has been fulfilled in one round but in the second method, demand has been fulfilled in multiple rounds. The proposed method splits the activation cost and distributes it in multiple interfaces to reduce the cost of activation. The effective and efficient allocation and release of Cloud resource are important to reduce the service cost of Cloud resource. A multi-agent-based Cloud resource allocation method for IoT devices has been proposed in (Manate et al. 2015), to audit the dynamic use of resources by the IoT devices. The audit of resource usage help to control the bad resource utilization and increase the utilization of the resources that in turn improve the performance and reduce the total cost of the system. Another method (Lan et al. 2013), based on Stackelberg game model has been proposed to reduce the network resource cost. The method analysis the lower and upper layer of the network and verifies the Nash equilibrium point of the no n-cooperative game between the upper layer of the network to reduce the cost. An iterative method is used to reach the Nash equilibrium by creating the Stackelberg game of the entire network. Multiple heterogeneous network interfaces have been used IoT devices that used a huge amount of services. A resource to heterogeneous service model has been proposed in (Angelakis et al. 2015), which is based on mixed-integer linear program (MILP) formulation. The cost of services can be reduced by splitting the services over the different interfaces dynamically.

Table 4.6 Cost-aware IoT resource allocation techniques

Algorithm	Improvements	Limitations
Heterogeneous resource allocation for flexible services (Angelakis et al. 2016)	The Cost has been reducing by splitting the services among the interfaces	The cost has been slightly increased in multi-round method
Optimizing cloud resource allocation architecture (Manate et al. 2015)	Increase system performance, reduce the total cost by minimizing the use of VMs	The cost of ideal resource usage must be reduced
Heterogeneous-oriented Resource Allocation Method (Lan et al. 2013)	Cost resources usage has been reduced	No evidence of practical implementation
Flexible Allocation of Heterogeneous Resources (Angelakis et al. 2015)	The cost has been reduced and increase the system performance	The more theoretical discussion presents not practically implemented

Improvement and limitations of cost-aware resource allocation techniques for IoT environment have been discussed in Table 4.6.

4.5 Parameters of IoT Resource Management Techniques

There are various IoT resource management technique parameters, which are described below. This section aims to answer the following questions related to parameters of resource allocation techniques for IoT.

4.5.1 What Are the Various Parameters of Resource Allocation?

Resource allocation is an important aspect of Cloud-based IoT environment. The devices are connected in the IoT environment by the internet and produced a huge amount of data which are stored in Cloud for further analysis to infer useful information for the organization and application of the system. Many resource allocation parameters have been discussed in (Ali et al. 2019a, b; Ali and Alam 2016). In this section, the author defines the various parameters of resource allocation for IoT environment which should be considered for improvement in the development of the IoT resource allocation techniques.

- **Performance** It is an amount of work done by the IoT layer to accomplish the on-demand services of the user's task. Performance of the system should be high.
- **Throughput** The total number of task or job completed by the IoT system is measured as the throughput of the IoT system. Throughput must be high in IoT systems to accomplish all the user's task.

- **QoS** Quality of Service (QoS) is the measurement of the quality services provided by the Cloud system to the end-user which are agreed on the SLA agreement.
- **Delay** Amount of time to respond to a waiting user's task when the system is busy in another task execution. The delay should be minimum in the channel to enhance the system performance.
- **Bit Rate** It an amount of rate at which IoT devices transfer data from one location to another location. Data transfer rate must be high in internet-based IoT environment.
- **Reliability** It is the ability to execute the given task in time without affecting by the system failure. Reliability of the system should be high to ensure the user's task completion in time.
- **SLA** Service level agreement between the service provider and the service consumers must be met to overcome the cost overhead and reduce the risk of users and providers relationships violation.
- **Time** It is an important factor in the IoT environment because smart devices produced a huge amount of data regularly. It is a plan to schedule a task in the IoT environment for their execution.
- **Cost** IoT environment uses many services from the Cloud infrastructure providers and in return give money to the service provider. The Cost of services is measured in the performance of the system and how much the system is productive. The cost of the system should be minimum.
- **Energy** IoT environment consists of many network nodes and smart devices which are connected to large data centres. These devices and data centres consumed a huge amount of energy for their proper functioning. The energy consumption should be minimized to reduce cost and make environment carbon footprint-free.
- **Availability** Resource availability is the measure of time and reliability of the resource in the given period. The availability of the resources should be high to reduce the delay in service.
- **Utilization** Resource utilization is the amount of portion, a resource must be occupied by the system. The resources should be efficiently utilized to enhance the system performance and the reliability of the system.

4.5.2 How Much Degree of Improvement Have Been Done in These Parameters?

In this paper, the author studied various Cloud-based IoT resource allocation techniques and classified them into the number of groups. In this section, the parameters of resource allocation which are improved by the given techniques in the classification have been discussed and in Table 4.7 these parameters are marked corresponding to the method or algorithm under study. From Fig. 4.7, we can observe that how much a parameter has been improved and which ones require more attention from the research community.

Table 4.7 IoT resource allocation parameters

Reference	Delay	Performance	Bit rate	Reliability	Throughput	QoS	Utilization	Context-Aware	SLA	Time	Availability	Cost	Power	Latency
Choi and Lim (2016)	–	√	–	–	–	–	–	–	√	–	–	–	–	–
Singh and Viniotis (2016)	–	√	–	√	–	–	–	–	√	√	√	–	–	–
Alsaffar et al. (2016)	–	√	–	–	–	–	–	–	√	–	–	–	–	–
Singh and Viniotis (2017)	–	–	–	–	–	–	–	–	√	√	–	–	–	–
Huang et al. (2015)	–	√	–	–	–	–	√	√	–	–	–	–	–	–
Hamidouche et al. (2017)	–	√	√	–	–	–	–	√	–	–	–	–	–	–
Abedin et al. (2015)	–	–	–	–	–	√	√	√	–	–	–	–	–	–
Chen et al. (2012)	√	√	–	–	–	√	–	–	–	–	–	–	–	–
Shorgin et al. (2015)	–	√	–	√	–	√	–	–	–	–	–	–	–	–
Colistra et al. (2014a)	–	√	√	–	√	–	–	–	–	–	–	–	–	–
Colistra et al. (2014b)	–	√	–	–	–	√	–	–	–	–	–	–	–	–
Baccarelli et al. (2017)	√	√	–	–	–	–	–	–	–	–	–	–	√	–
Naranjo et al. (2017)	–	√	–	–	–	–	–	–	–	–	–	–	√	√
Abuzainab et al. (2017)	–	√	√	–	–	–	–	–	–	–	–	–	√	–
Li et al. (2018)	–	√	–	–	–	–	–	–	–	–	–	–	√	–
Angelakis et al. (2016)	–	√	–	–	–	√	–	–	–	–	–	√	–	–
Manate et al. (2015)	–	√	–	–	–	–	–	–	–	–	–	√	–	–
Lan et al. (2013)	–	√	–	–	–	–	–	–	–	–	–	√	–	–
Angelakis et al. (2015)	–	√	–	–	–	√	–	–	–	–	–	√	–	–

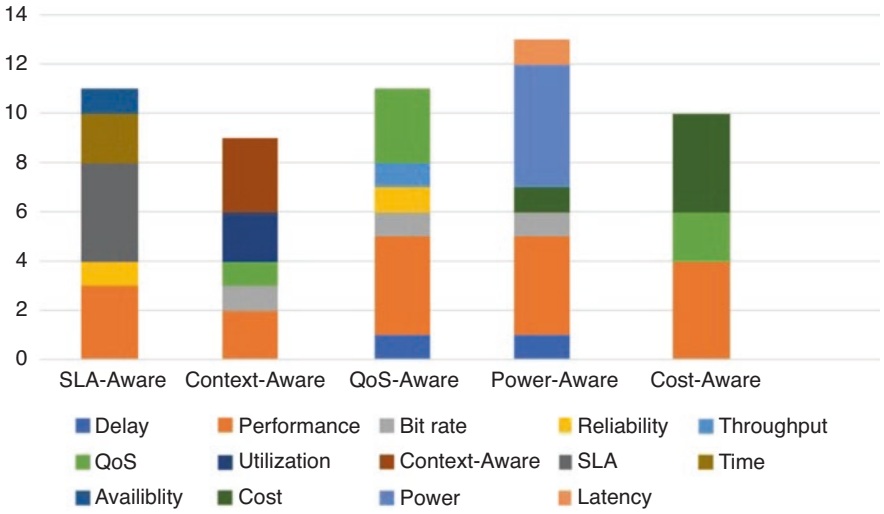


Fig. 4.7 Degree of improvement in resource allocation parameters

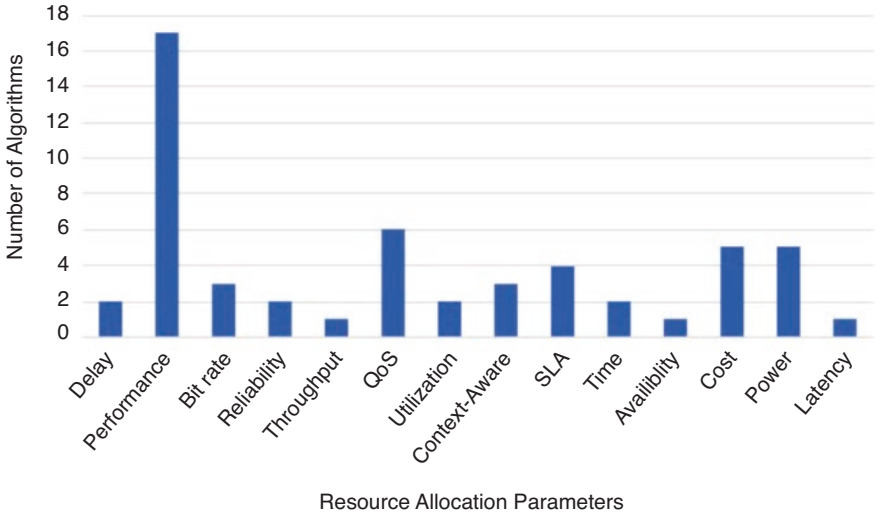


Fig. 4.8 Resource allocation parameters and the corresponding number of algorithms

4.5.3 How Much Improvement Is Required in the Remaining Parameters?

In the above section, we have already seen that the number of resource allocation parameters have been improved in the proposed algorithms or methods. But still, various resource allocation metrics need improvement and require much attention from the researchers. In Fig. 4.8, various parameters and their corresponding number of algorithms in which they are improved have been shown. From the figure, we can easily identify that the performance of the system has been much improved by many researchers. But the reliability, latency, availability of resources and delay in communication channel have not been improved so much. Therefore, there is a scope for the researchers to propose more resource allocation algorithms that can improve more and more these resource allocation parameters. Multi-objective and nature-inspired algorithms can be implemented by the researchers.

4.6 Challenges and Issues

The IoT environment provides potential services to improve the productivity of the Cloud-based IoT ecosystem. Regardless of its potential benefits, there are silently many challenges are present in the Cloud-based IoT resource allocation. In this paper, there are many research papers studied related to IoT resource allocation problem. Most of the papers are based on one or two aspects of the resource allocation, there should be more work needed in the collaboration of IoT with Cloud, Fog and Edge computing for better implementation of IoT ecosystem. Most of the research work done so far has based on simulation and no evidence of implementation of the proposed algorithm for real IoT ecosystem. Real IoT ecosystem has its own challenges and properties and when these algorithms are implemented in real IoT world then there may be some problems occur because of no proper implementation has been tested in real IoT environment. Another challenge in the resource allocation methods studied in this paper is that all aspect of resource allocation like resource discovery, resource modelling, resource provisioning, resource scheduling, resource estimation and resource monitoring has not considered. Optimization in resource allocation techniques is another issue, more of the research only work on the resource allocation technique but optimization in resource allocation is more important for effective and efficient IoT environment.

4.7 Future Directions

IoT environment makes the life of human being so easy. All daily routine work can be done efficiently with the help of IoT devices. Many industries are planning to launch more IoT devices that can make an easier daily task for the human. Many other technologies give life to the IoT infrastructure and provide services. Cloud-based IoT environment for industries application has a future for implementation. The reliability, productivity and cost-effective industry-based applications require more effective and efficient resource allocation. These applications are known as Industries Internet of Things (IIoT) application. Data captured by the smart IoT devices are stored in Cloud and further processed in Cloud infrastructure for inferring knowledge. The amount of data captured by IoT devices is very large that why many researchers proposed Big data as a service to the other industries and Cloud users (Khan et al. 2018, 2019). Machine learning-based resource allocation has a scope to automate the resource allocation in IoT infrastructure. ML-based resource allocation techniques can overcome the scarcity, over and underutilization of Cloud resources. Blockchain technology is also an emerging technology which is used for cryptocurrency (Dittmann and Jelitto 2019). Blockchain is a secure method for transferring data from one node to another. It provides privacy and secure communication in a P2P network. Many types of research have been done in IoT and blockchain integration with Cloud Computing (Abedin et al. 2015; Qiu et al. n.d.), but the blockchain is not used in Cloud-based IoT resource allocation.

4.8 Conclusion

Resource allocation is an important aspect of Cloud-based IoT environment for effective and efficient working of the novel paradigm. In this paper, Cloud-based resource allocation techniques for IoT environment have been studied and categorized into different groups: SLA-Aware, Context-Aware, QoS-Aware, Power-Aware and Cost-Aware resource allocation. The author systematically reviewed all these techniques and find out the limitations and improvements of these algorithms. Moreover, resource allocation parameters determined for improvements have also listed and defined. A graphical representation of the degree of improvement in these parameters has been shown in the paper. Lastly, challenges and future directions of the study have been discussed.

References

Abedin, S. F., Alam, M. G. R., Il, S., & Moon, C. S. H. (2015). An optimal resource allocation scheme for Fog based P2P IoT Network. In: 년 동계학술발표회 논문집 (pp 395–397).

Abuzainab, N., Saad, W., Hong, C. S., &Poor, H. V. (2017). *Cognitive hierarchy theory for distributed resource allocation in the Internet of Things,* arXiv preprint.

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications, 88*, 10–28.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials, 17*, 2347–2376.

Ali, S. A., & Alam, M. (2016). A relative study of task scheduling algorithms in cloud computing environment. In *2016 2nd International Conference on Contemporary Computing and In- formatics (IC3I)* (pp. 105–111). https://doi.org/10.1109/IC3I.2016.7917943.

Ali, S. A., Affan, M., & Alam, M. (2019a). A study of efficient energy management techniques for cloud computing environment. In *2019 9th international conference on cloud computing* (pp. 13–18). https://doi.org/10.1109/CONFLUENCE.2019.8776977.

Ali, S. A., Khan, S., & Alam, M. (2019b). Resource-aware min-min (RAMM) algorithm for resource allocation in cloud computing environment. *International Journal of Recent Technology and Engineering, 8*(3), 1863–1870. https://doi.org/10.35940/ijrte.C5197.098319.

Alsaffar, A. A., Pham, H. P., Hong, C. S., Huh, E. N., & Aazam, M. (2016). An architecture of IoT ser- vice delegation and resource allocation based on collaboration between fog and cloud computing. *Mobile Information Systems*. https://doi.org/10.1155/2016/6123234.

Angelakis, V., Avgouleas, I., Pappas, N., & Yuan, D. (2015). Flexible allocation of heterogeneous re- sources to services on an IoT device. In *2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 99–100).

Angelakis, V., Avgouleas, I., Pappas, N., Fitzgerald, E., & Yuan, D. (2016). Allocation of heteroge- neous resources of an IoT device to flexible services. *IEEE Internet of Things Journal, 3*, 691–700.

Atlam, H. F., Alenezi, A., Walters, R. J., Wills, G. B., & Daniel, J. (2017). Developing an adaptive risk- based access control model for the Internet of Things. In *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (Green- Com) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 655–661).

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks, 54*(15), 2787–2805.

Baccarelli, E., Naranjo, P. G. V., Scarpiniti, M., Shojafar, M., & Abawajy, J. H. (2017). Fog of every- thing: Energy-efficient networked computing architectures, research challenges, and a case study. *IEEE Access, 5*, 9882–9910.

Baccelli, E., Hahm, O., Günes, M., Wählisch, M., & Schmidt, T. C. (2013). RIOT OS: Towards an OS for the Internet of Things. In *Proceedings of the IEEE conference INFOCOM WKSHPS* (pp. 79–80).

Bassi, A., Bauer, M., Fiedler, M., & Kranenburg, R. V. (2013). *Enabling things to talk*. New York: Springer.

Cao, Q., Abdelzaher, T., Stankovic, J., & He, T. (2008). The liteos operating system: Towards unix-like abstractions for wireless sensor networks. In *Proceedings of the international conference on information processing in sensor networks* (pp. 233–244).

Chen, X., Chen, L., Zeng, M., Zhang, X., & Yang, D. (2012). Downlink resource allocation for device-to-device communication underlying cellular networks. In *2012 IEEE 23rd international symposium on Personal Indoor and Mobile Radio Communications (PIMRC)* (pp. 232–237).

Choi, Y., & Lim, Y. (2016). Optimization approach for resource allocation on cloud computing for IoT. *Journal of Distributed Sensor Networks*. https://doi.org/10.1155/2016/3479247.

Colistra, G., Pilloni, V., & Atzori, L. (2014a). Task allocation in group of nodes in the IoT: A consensus approach. In *2014 IEEE International Conference on Communications (ICC)* (pp. 3848–3853).

Colistra, G., Pilloni, V., & Atzori, L. (2014b). The problem of task allocation in the Internet of Things and the consensus-based approach. *Computer Networks, 73*, 98–111.

Crosby, G. V., & Vafa, F. (2013). Wireless sensor networks and LTE-A network convergence. In *Proceedings of the IEEE 38th Conference on Local Computer Networks (LCN)* (pp. 731–734).

Delicato, F. C., Pires, P. F., & Batista, T. (2017). The resource management challenge in IoT. In *Resource Management for Internet of Things* (pp. 7–18). Springer.

Dittmann, G., & Jelitto, J. (2019). A Blockchain proxy for lightweight IoT devices. In *2019 Crypto Valley Conference on Blockchain Technology (CVCBT)* (pp. 82–85). https://doi.org/10.1109/CVCBT.2019.00015.

Evans, D. (2011). *The Internet of Things how the next evolution of the internet is changing everything*.

Ferro, E., & Potorti, F. (2005). Bluetooth and Wi-fi wireless protocols: A survey and a comparison. *IEEE Wireless Communications, 12*, 12–26.

Gigli, M., & Koo, S. (2011). Internet of things: Services and applications categorization. *Advanced Internet of Things, 01*, 27–31.

Hamidouche, K., Saad, W., & Debbah, M. (2017). Popular matching games for correlation-aware re- source allocation in the internet of things. In *IEEE International Symposium on Information Theory (ISIT) submitted to IEEE*.

Horrow, S., & Sardana, A. (2012). Identity management framework for cloud based internet of things. In *Proceedings of the first international conference on Security of Internet of Things* (pp. 200–203).

Huang, J., Yin, Y., Duan, Q., & Yan, H. (2015). A game-theoretic analysis on context-aware resource allocation for device-to-device communications in cloud-centric internet of things. In *2015 3rd International Conference on Future Internet of Things and Cloud (FiCloud)* (pp. 80–86).

Khan, S., Shakil, K. A., Ali, S., & Alam, M. (2018). On designing a generic framework for big data as-a-service. In *2018 1st International Conference on Advanced Research in Engineering Sciences (ARES)* (pp. 1–5). https://doi.org/10.1109/ARESX.2018.8723269.

Khan, S., Ali, S. A., Hasan, N., Shakil, K. A., & Alam, M. (2019). Big data scientific workflows in the cloud: Challenges and future prospects. In H. Das, R. K. Barik, H. Dubey, & D. S. Roy (Eds.), *Cloud computing for geospatial big data analytics* (Vol. 49). Cham: Springer.

Koshizuka, N., & Sakamura, K. (2010). Ubiquitous ID: Standards for ubiquitous computing and the Internet of Things. IEEE Pervasive Comput. *Sensors, 9*, 37.

Lan, H. Y., Song, H. T., Liu, H. B., & Zhang, G. Y. (2013). Heterogeneous oriented resource allocation method in internet of things. *Applied Mechanics and Materials, 427*, 2791–2794.

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons, 58*, 431–440.

Levis, P., Madden, S., Polastre, J., Szewczyk, R., Whitehouse, K., Woo, A., Gay, D., Hill, J., Welsh, M., & Brewer, E. (2005). *An operating system for sensor networks*.

Li, S., Zhang, N., Lin, S., Kong, L., Katangur, A., & Khan, M. K. (2018). Joint admission control and resource allocation in edge computing for Internet of Things. *IEEE Network, 32*, 72–79.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal, 4*, 1125–1142.

Malik, A., & Om, H. (2018). Cloud computing and internet of things integration: Architecture, applications, issues, and challenges. In *Sustainable cloud and energy services* (pp. 1–24). Springer.

Manate, B., Fortis, T. F., & Negru, V. (2015). Optimizing cloud resources allocation for an Internet of Things architecture. *Scalable Comput, 15*, 345–355.

Marques, G., Garcia, N., & Pombo, N. (2017). A survey on IoT: Architectures, elements, applications, QoS, platforms and security concepts. In *Advances in Mobile cloud computing and big data in the 5G era* (pp. 115–130). Springer.

Mattern, F., & Floerkemeier, C. (2010). *From active data management to event-based systems and more*. New York: Springer. From the internet of computers to the Internet of Things.

Mcdermott-Wells, P. (2004). What is bluetooth? *IEEE Potentials, 23*, 33–35.

Mell, P., & Grance, T. (2011). The NIST definition of cloud. *Computing*.

Muntjir, M., Rahul, M., & Alhumyani, H. A. (2017). An analysis of internet of things (IoT): Novel architectures, modern applications, security aspects and future scope with latest case studies. *International Journal of Engineering Research and Technology, 6*(6), 422–447.

Naranjo, P. G. V., Pooranian, Z., Shojafar, M., Conti, M., & Buyya, R. (2017). FOCAN: A fog-supported smart city network architecture for management of applications in the internet of everything environments. *Journal of Parallel and Distributed Computing*, arXiv, preprint.

Pourghebleh, B., & Navimipour, N. J. (2017). Data aggregation mechanisms in the Internet of Things: A systematic review of the literature and recommendations for future research. *Journal of Network and Computer Applications, 97*, 23–34.

Qiu, C., Yao, H., Jiang, C., Guo, S., & Xu, F. (n.d.). Cloud computing assisted blockchain-enabled Internet of Things. *IEEE Transactions on Cloud Computing*. https://doi.org/10.1109/TCC.2019.2930259.

Shorgin, S., Samouylov, K. E., Gaidamaka, Y. V., Chukarin, A., Buturlin, I. A., & Begishev, V. (2015). Modeling radio resource allocation scheme with fixed transmission zones for multiservice M2 M communications in wireless IoT infrastructure. *ACIIDS, 2*, 473–483.

Singh, A., & Viniotis, Y. (2016). An SLA-based resource allocation for IoT applications in cloud environments. *Cloudification of the Internet of Things (CIoT)*, 1–6.

Singh, A., & Viniotis, Y. (2017). Resource allocation for IoT applications in cloud environment s. *International Conference on Computing, Networking and Communications (ICNC)*, 719–723. 2017.

Stallings, W. (2015). The Internet of Things: Network and security architecture. *Internet Protocol Journal, 18*(4), 381–385.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*(1), 1–11.

Varghese, B., & Buyya, R. (2018). Next generation cloud computing: New trends and research direc- tions. *Future Generation Computer Systems, 79*, 849–861.

Wang, L., Laszewski, G. V., Younge, A., He, X., Kunze, M., Tao, J., & Fu, C. (2010). Cloud computing: A perspective study. *New Generation Computing, 28*(2), 137–146.

Want, R. (2006). An introduction to RFID technology. *IEEE Pervasive Computing, 5*, 25–33.

Want, R. (2011). Near field communication. *IEEE Pervasive Computing, 10*, 4–7.

Xing, X. J., Wang, J. L., & Li, M. D. (2010). Services and key technologies of the Internet of Things. *ZTE Commun, 2*, 11–11.

Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. *Journal of Network and Computer Applications, 42*, 120–134.

Yang, L., Yang, S. H., & Plotnick, L. (2013). How the Internet of Things technology enhances emergency response operations. *Technological Forecasting and Social Change, 80*, 1854–1867.

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications, 1*(1), 7–18.

Chapter 5
Data Management for the Internet of Things

Amrit Sahani, Ranjit Kumar, Suchismita Chinara, Anjali Kumari, and Bina Patro

Abstract IoT is the administration systems which are worldview used and where all the interconnected, keen articles constantly create information and sends it over the Internet. A significant part of the IoT activities is equipped in the direction of assembling minimal effort and vitality proficient equipment for these articles, just as the correspondence innovations that give objects interconnectivity. Moreover, the answers and solutions for managing and using the monstrous volume of information created by these articles of IoT are yet to develop. Conventional database arrangements miss the mark in fulfilling the refined application demands for an IoT device that has a global scale. The recent answers for IoT information the board conveys halfway parts for IoT conditions along an extraordinary spotlight on sensor systems and interconnection. This chapter provides an overview of information and the arrangements which are opted for IoT and the subsystems of IoT. We feature the unmistakable and distinctive plan that we accept to be tended into IoT data management solutions and examine how they are drawn closer by the proposed arrangements. We, at last, suggest the information and the board structure for IoT that deliberates over the talked about plan components and goes about as a seed to an exhaustive IoT information arrangement procedure. The framework we work will adopt a federated, data- and the information-significant method to loop the diversified items along with the profusion of information for the devices that are coined for IoT.

Keywords IoT · Sensor · Data management · Framework

A. Sahani (✉)
Siksha 'O' Anusandhan University, Bhubaneswar, Odisha, India

Institute of Technical Education and Research, Bhubaneswar, Odisha, India

R. Kumar · S. Chinara
National Institute of Technology, Rourkela, Odisha, India

A. Kumari
College of Engineering Roorkee, Roorkee, Uttarakhand, India

B. Patro
University of Berhampur, Berhampur, Odisha, India

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_5

5.1 Introduction

The Internet of Things is where each and every physical element is allotted with the web through the channel of framework devices, switches or routers and trade data and exchange information. IoT empowers things to be controlled remotely across over existing framework establishment. The idea of IoT is as a rule incredible and technically knowledgeable framework which reduces human effort similarly as straightforward access to physical contraptions. This procedure has autonomous control including any contraption which gets controlled with no human correspondence (Vermesan et al. 2009).

The objective of IoT is to try is to attain and provide a stage for making pleasing organizations, co-employable administrations and applications that outfit the total force of advantages for the individual "Things" and other subsystems planned for handling the recently referenced "Things".

Any point of convergence of such advantages has the plenitude of information which is made available by following the mixing of data and is conveyed continuously similarly as data set away in never-ending storage facilities and archives. This information can make the affirmation of creative and unique applications and worth included organizations possible and will give a significant source to float assessment and essential possibilities. A careful organization arrangement of information which is made, set away from the following articles inside IoT is henceforth expected to attain the referenced target (Pujolle 2006).

The board of information is a wide and far reaching idea inferring to the designs, models, usability, and strategies in running the organization properly although the data lifecycle needs of a particular structure. Taking into the thought with regards to IoT the information the executives ought to go as a layer between the items and gadgets producing the information and the applications which are getting to the information for investigation, assessment and organizations. The contraptions are to be organized into different underlying systems with individuality in an organization inside which different levels are available for the boarding. The convenience and data given by these subsystems are to be made available to the course of action of IoT, dependent upon layers of security needed by the owners of the underlying-levels (Wu et al. 2011).

IoT information ought to have specific traits which can make standard and conventional social based database an obsolete game plan. An enormous volume of heterogeneous, spilling and topographically dissipated progressing data will be made by countless various devices once in a while transmitting signals over particular watched and checked marvels else specifying about the occasion of peculiar interesting events. Time to time supervision and observations taken periodically which are similar to correspondence overhead and limit on account of their spilling and unending quality, whereas, occurrences that are available timely and responsively from the beginning till the finished rebounding reaction times depending upon the intensity irritability of the reply needed to complete the assigned task (Cooper and James 2009).

It has been foreseen that there is a reestablished enthusiasm for database structures investigating the spotlights on substitute representation rather than standard conventional prototype. The move from ordinary database models has different viewpoints that are especially profitable to IoT, for instance, the utilization of remote amassing at the Things layer, non-assistant data support, loosening up of the Atomicity, Consistency, Isolation, and Durability (ACID) properties to trade off consistency and availability, and blend of indispensable profitability as a combination of vitality effectiveness just as information the executives plan crude.

5.2 Management of Data in IoT

Conventional information and data systems management framework, which handle the capacity, recovery, update the basic information and organize records. In respect to the IoT, information the administrative frameworks must abridge information online and through different perspective while giving stockpiling and inspecting offices, also facilities for auditing for disconnected and offline investigation through analysis (Ramakrishnan and Gehrke 2002; Cattell 2010).

This grows the information idea on the board from offline capacity, question (querying) handling, and exchange the operational activities into online-offline correspondence/storage dual tasks. We carry out the settings of IoT and examine the parts of the IoT and after that layout the vitality utilization for different parts and stages accomplished so as to have a superior comprehension of the information management for the Internet of Things.

5.2.1 Life-Cycle of Information

The circulated information, and resources inside an IoT framework—continues from information generation to accumulation, move, discretionary sifting, filtering and preprocessing, lastly to the storage, file-logging and archiving. Questioning (Querying) and the investigation is the end focuses that initiate demand and expend information creation, yet information generation may be opted to be "pushed" to the IoT devouring administrations and preparing for the client's requirement. This includes creation, accumulation, separation, and some essential basic querying and preparatory handling operational tasks, which can be viewed on the web. Concentrated preprocessing, long-term stockpiling information and archiving data are considered for disconnected/offline storage activities (Ozsu and Valduriez 2011).

Storage tasks target making information accessible in the extended term for steady access. On the other hand, authentication is worried just about only reading the information. As many of the frameworks of Internet Of Things(IoT) may produce, process, and store information in-organize for ongoing and restricted administrations, with no compelling reason to proliferate this information further up to

focus focuses on the framework, "edges" that consolidate both preparing and capacity components may exist as independent items in the propaganda. In the accompanying sections, every component in the IoT information phenomenon is clarified (Pungila et al. 2009).

Questioning
Intensive information frameworks depend on questioning (querying) for the centre procedure to get to and recover information. With regards to IoT, an inquiry can be issued either to demand continuous information to be gathered for transient checking purposes or to recover a specific perspective on the information put away inside the system framework. The primary case is regular when a (for the most part confined) constant request for information is required. The subsequent case speaks to more globalized perspectives on information and top to bottom examination of patterns and examples (Sen and Ramamritham 2005).

Creation (Production)
Data generation includes detecting and move of information by the "Things" inside the IoT system and announcing this information to invested individuals at irregular intervals (as in a buy-in/sell model), pushing it up the system to conglomeration focuses and along these lines for the servers of database, or transmitting it through a reaction activated from inquiries which seek the information through the devices which act as a sensor and keen determined articles. Information is normally time-stepped, conceivably geo-stepped and globalized where it can be as straightforward key-esteem sets, or it might contain superior quality sound/picture/visuals, along with differing ranks of multifaceted nature of varying natures of complexity (Güting and Mamoulis 2011).

Accumulation (Heap)
The sensing materials and keen items inside the IoT accumulate the information in a specific time interim and account it to administer parts. Information might be gathered at focus focuses or entryways inside the system where it is additionally sifted and prepared, and potentially intertwined into reduced structures for productive transmission. Remote correspondence advancements, for example, Wi-Fi cells being utilized by articles to send information for gathering focuses.

Total (Aggregation)
Remitting out all the crude information from the systems progressively is restrictively costly given the expanding information gushing rates and the constrained transfer speed. Collection and combination strategies send synopsis and consolidating activities progressively to pack the volume of information to be put away and transmitted (Spiess et al. 2009).

Conveyance
As information is separated, amassed, collected and perhaps prepared from the fixation focuses else through the independent indirect elements inside the IoT, consequences from the particular procedures might be forbade for further framework, in a way as definite reactions, or for capacity and top to the bottom investigation.

Wired or remote broadband correspondences might be utilized there to move information to last information at stable, secured and established repositories (Guinard et al. 2010).

Preliminary Processing
The information through the IoT might originate through various provenances in accordance to fluctuating arrangements and patterns. Information may be preprocessed to deal with missing information, expel redundancies and incorporate information from various sources into a brought together outline before being focused on storage capacity. The preliminary processing, a known system in information mining, is called information cleansing. Pattern combination do not infer forceful power fitting of the considerable number of information into a fixed social (tables) composition, yet rather an increasingly conceptual meaning of a steady method to get to the information without tweaking approach in the information format(s). Randomness at various steps in the mapping might be added at this stage to IoT information things so as to deal with a vulnerability that might be available in the information or to manage the absence of trust which might have existence in information repositories.

Capacity/Competency
The following stage controls the productive stockpiling association of information similar to the consistent reconditioning of information along with fresh data as it winds up accessible. Filing alludes to the disconnected long haul stockpiling of information that isn't quickly required for the framework's continuous activities. The centre brought together capacity is the sending of capacity structures that adjust to the different information types and the recurrence of information catch. Social database the board frameworks are a well-known decision that includes the association of information into a table outline with predefined interrelationships and metadata for proficient recovery at later NoSQL key-esteem stores are picking up prevalence as capacity advancements for their help of enormous information stockpiling with no dependence on social composition or solid consistency prerequisites run of the mill of social database frameworks. Capacity can likewise be decentralized for self-sufficient IoT frameworks, where information is kept at the articles that produce it and isn't sent up the framework. Be that as it may, because of the constrained abilities of such articles, stockpiling limit stays restricted in contrast with the unified stockpiling model.

Handling/Analysis
This stage includes the continuous recovery and examination activities performed and put away and chronicled-archived information so as to pick up bits of knowledge into recorded information and foresee future patterns, or to recognize variations from the norm out from the information which may trigger for the upcoming examination or activity. Undertaking explicit pretreatment might be expected to channel and clean information before important tasks happen. At the point when a subsystem of IoT is self-sufficient and need not require a perpetual capacity of its information, rather keeps the handling and capacity for the following system, at that

point in-organize preparing might be performed in light of ongoing or limited inquiries.

Glancing back, the progression of information may take one of three ways: a way for independent frameworks inside the IoT that returns from inquiry to generation to in-arrange handling and after that conveyance, a way that begins from creation and continues to accumulation and sifting/conglomeration/combination and finishes with information conveyance to starting (potentially worldwide or close ongoing) inquiries, lastly a way that stretches out the generation to total further and incorporates preprocessing, perpetual information stockpiling and authentic, and top to bottom preparing and investigation. In the following area, the requirement for information the executive's arrangements that outperform the present capacities of customary information the board is featured in light of the recently sketched out life cycle.

5.2.2 Management of Information for IoT and Data Management Systems for the Traditional Methods

Following the view of the IoT information lifecycle examined thoroughly, we can separate the working of IoT information executive's framework into a real-time web application that can continuously communicate straightforwardly with the any other interconnected IoT articles and sensors, and with the help of a offline backend system that can handles the mass stock-piling, gathering of the information and examination from top to bottom of IoT information. The information management frontend is correspondence escalated; including the spread of inquiry demands and result from the sensors and tech-savvy materials. The backend is capacity concentrated; including the data stockpiling of created information for the preparation of later and investigation for more top to bottom questions. In spite of the fact that the capacity components live toward the back, they communicate with the frontend on a successive premise by means of constant updates and are therefore implied on the web. The self-ruling autonomous limits in the existence process which is viewed as more correspondence concentrated than storage escalated, as they give constant information to specific inquiries (Sen and Ramamritham 2005).

This imagined information and the board engineering parts significantly oozing out from current management frameworks of database, which are primarily working for storage. The conventional frameworks, which have the main part of the information gathered from predefined and limited sources and put away in scalar structure as indicated by severe standardization controls in relations. Inquiries are utilized to recover explicit "rundown" perspectives on the framework or update explicit things in the database. New information is embedded in the database when required, likewise by means of addition inquiries. Inquiry activities are normally neighborhood, with execution costs bound to handling and middle of the road stockpiling. Exchange the board instruments ensure the ACID properties so as to authorize generally

speaking information uprightness. Regardless of whether the database is appropriated over various locales, inquiry preparing and conveyed exchange the board are implemented. The execution of appropriated questions depends on the straightforwardness guideline, which manages that the database is still seen intelligently as one unified unit, and the ACID properties are ensured through the two-stage submit convention (Cattell 2010).

The frameworks of IoT, imagination is drastically unique, along with a gigantic—and development of information sources; sensors, RFIDs, inserted frameworks, and portable devices. In spite of infrequent updates and inquiries submitted to customary Data Base Management Systems (DBMS) information is spilling always from the large number of "Things" to IoT for storing information, and questions increasingly visit and with progressively adaptable needs. Various leveled information detailing and collection might be required for versatility ensure just as to empower progressively brief handling usefulness.

The severe social database pattern and the social standardization practice might be loose for progressively unstructured and adaptable structures that adjust to the various information types and refined questions. Albeit dispersed Database Management Systems (DBMSs) advance inquiries dependent on correspondence contemplations, streamlining agents base their choices on fixed and well-characterized mappings. This may not be the situation in IoT, where new information sources and spilling, confined information make an exceptionally unique condition for inquiry streamlining agents. Endeavoring to ensure the straightforwardness prerequisites forced in appropriated DBMSs on IoT information the board frameworks is testing, if certainly feasible.

Moreover, straightforwardness may not be required in IoT, on the grounds that imaginative applications and administrations may require area and setting mindfulness. Keeping up the mind of ACID properties in limited subsystems when the changes are being executed and exchanges will be overseen, yet trying for more space in a globalized way. Nonetheless, the component of versatile information resources and singly created information may be joined into the formally settled information extent is a novel test which is to be tended from the devices of IoT information and management frameworks (Hauer et al. 2008).

The most accompanying area gives subtleties of certain information that the board answers for IoT that incorporates most of the things above in an operational mechanism. Those propositions which then dissected a lot of structure natives which is regarded essential for the information management for IoT are seen.

5.3 Systematic Survey of the Management for the Devices of IoT and Design Primitives

Numerous different kinds of elementary designs are possible that can be used to regulate the logical, insightful, tangible and physical structure for the management for the IoT solutions.

Identifying the basic elementary designs is important in constructing a comprehensive solution for the data administration.

These designs categorize into the three major segments:

Collection of Data
System design for Data management
Refining and Processing of the Data

Collection of data elements make the discovery of the objective and objects of IoT and sub-systems identifiable where data is given to data repositories.

This includes management of data and design for the architectural components of the data management system and the process in which data is being stored and managed in the design framework.

Finally, the processing of the data and information is done with the real-time access to actual data (Cooper and James 2009).

5.3.1 Data Collection and Information Management Systems

One of the worth included administrations that IoT is foreseen is to give is the capacity to take advantage of assorted information that might not really have a place with the equivalent proportional IoT subsystem. Along these lines, at the origin recovery implementation is required for applications using IoT with the goal of reporting their administration requirements and getting reactions from sources whose information might fulfill – those necessities. On the other hand, sources can intermittently declare their administrations; the information they can report and create.

A model structure that tends to the disclosure of information sources as a fundamental piece of information the board is proposed in. A model structure that keeps an eye on the exposure of data sources as a crucial snippet of data the will be proposed. The framework on which the system is established may find out the data sources either by methods for creeping, or by methods having pre-defined sources of data that can build new ones as found.

Essentialness gainful responses for managing data from compact sources of data that were outlined. Desire of position has been cut down to imperativeness usage of position following advances, and setting or checking was proposed to cut down the pointless counts and correspondence. Position expectation was utilized to bring down the vitality utilization of position following advances, and setting checking

was proposed to diminish superfluous computational calculations and correspondence (Ozsu and Valduriez 2011).

5.3.1.1 Collection Strategy for Data

The accumulation of information from the "Internet of Things" layer might be temporal or modular. Fleeting information gathering incorporates gathering information from all "Things" at determined interims, or stipulated time intervals while modular accumulation includes gathering information relating to explicit components. The variety assortment of information needs will be normal in IoT (Internet of Things) frameworks which might oversee in having more than the required database example for obliging the dual information aggregation approaches (Pungila et al. 2009).

5.3.2 Design Elements for Database Framework

United Architectural Planning
Theories from conveyed, unified data directory frameworks have to be adjusted for the requirements of IoT (Internet Of Things) information administration. Disseminated database frameworks deal with a solitary and single database conveyed over numerous locales. Federated database frameworks, then again, oversee autonomous and conceivably heterogeneous information stores at different locales. In a unified design, at the complete and the full self-sufficiency along the information is kept up when it takes part in a repository alliance, in light of that site's operational necessities.

On the off chance that the various subsystems shaping IoT are to be seen as free "information manufacturing plants" with self-governing database frameworks, at that point it is fascinating to investigate the adjustment of inquiry optimization focused at circulated heterogeneous database frameworks to the characteristically disseminated and heterogeneous IoT subsystems (Pujolle 2006).

Information and Sources-Driven IoT Middleware
The requirement in information-driven software acts as a gap between the correspondence-driven "things" and the storage-driven information repositories. This middleware layer will serve to give increasingly adaptable abilities to finding information sources and getting to and dissecting heterogeneous and topographically appropriated information, data distributed throughout. The intermediate layer will likewise focus on adaptable exchange in huge chunks of information volume sent from the system and is stored in the information repositories. The need for using maximum capacity of information is to be tackled in various information sources inside IoT by giving the way to find such useful reference which have

dependence with methodology, area or worldwide question needs that are skeptic for the fundamental system (Agarwal and Alam 2018).

An engineering which joins the middle software for information handling in enormous scale WSNs to cover arrange for diversity and encourage information conglomeration that are proposed for. The center and main component in the mechanism is a virtual sensing device which coordinates different information streams from genuine sensors in bottom layers and to a solitary information branches. Information branch inquiries has to be assessed, the outcomes from the devices are to be put away in brief relations, and the consequence of joining these branches is put away forever just whenever required, else needed by the application (Pujolle 2006; Wu et al. 2011).

Adaptable Prototype

The database using relational model frameworks, standards of individuality at, practical reliance, dependency on functional activities and standardization utilized for the characterization of the framework of the relations in the model of the database structure. The models of database which can leave from the social model for an increasingly adaptable database structure are now-a-days increasing extensively and found everywhere, despite the fact that it's been demonstrated that social and analogous DBMSs knocks out the unstructured ideal models and is way ahead of the traditional data base model.

Layered Capacity Stage

Contrary to conventional database frameworks, where "steady" information is gathered from the earlier and put away in incorporated, appropriated storage networks, Information from IoT gets constantly refreshed as the level of things gets an observation phenomenal substitute. Regardless of whether it was feasible for the majority of information produced by the Internet of things in any one end so as to be put away in changeless permanent capacity, it will rapidly end up old and new information will wind up accessible. Stream and ongoing databases are not new ideal models and their standards were utilized for natural sensor systems. Be that as it may, the structure of such frameworks tends to concentrated capacity areas and isn't appropriate in the scaling and conveyance in the maintenance of information capacity created by the devices using IoT, indeed requiring much proficient update and accessing mechanism process (Agarwal and Alam 2018).

Two methodologies are to be received for addressing the capacity issue areas of IoT information: every frameworks, which make out to utilize the IoT is its solely devoted repository framework, putting away information from the units in the memory and articles that produce the information and treat it as a database having decentralized. Through the principle perspective, crude or mostly collected information is moved to total focuses and mass storerooms inside an IoT subsystem. The most committed storerooms required to various frameworks shaping IoT (Internet of Things) represents various difficulties.

Database access issues, for example, question/exchange preparing and simultaneousness control should embrace the proposed mechanism to find IoT frameworks with storage since it isn't plausible to give a limited rundown of the considerable

number of frameworks connected to the IoT foundation. The presence of exclusive IoT frameworks will direct a requirement for qualifications the executives and consistent access authorizations. The substantial reliance on the transmission of spilling information from sources to storerooms will bring about high correspondence costs. This is made progressively entangled by the requirement for various correspondence advancements for various item classes and transmission situations (Chen et al. 2010; Ramakrishnan and Gehrke 2002).

5.3.3 Preparing Elements

5.3.3.1 Access Model

In request to get to information, questioning dialects have been utilized for social frameworks, and later adjusted to sensing systems. SQL (Structured Query Language) provides the true calibration for accessing information, along with leveled choice/join/prediction/projection/total operational mechanism which can be settled in complicated complex questions. Extra builds is being added to the language for compelling new and different categories of information, for example, TinySQL for sensing devices and StreamSQL for information stream handling.

In addition to SQL (Structured Query Language) turned out to be excessively mind boggling because of the persistent augmentations as new abilities are included, designers for the different applications imagined for IoT will think that its difficult to gain proficiency with the majority of SQL's vernaculars and stunts while they may require just a subset of them. Consequently, it has been recommended that a progressively adaptable structure be utilized, in which a SQL lingo or predefined arrangement is picked by the particular prerequisites of the current situation. Also, a move from particular programming to include situated writing computer programs is proposed to alter programming that is utilized to get to databases. This empowers the improvement of adaptable information the board contingent upon the basic framework's ideal highlights (Bowman et al. 2007; Sen and Ramamritham 2005).

5.3.3.2 Proficient Handling Procedure

The two primary motivations behind gathering information through the "Things" surface in IoT frameworks for announcing and examination. This duo includes handling information sooner or later in the framework so as to total/gather helpful data. Deciding the area at which information is to be prepared in IoT frameworks is an essential structure worry that should think about the decentralized idea of the framework and the volume of information delivered.

Two preparing methodologies can be conveyed for IoT frameworks: in-organize handling and incorporated preparing. In-arrange handling includes making out space for the "program" downwards to the information and projecting back the

outcomes to the user(s), accordingly diminishing the magnitude of information which should be moved to concentrated capacity at top building layers in the framework. Incorporated handling, then again, necessitates that information—either in its crude structure or in a totaled, progressively smaller structure—be shipped to persevering stockpiling to empower advanced investigation errands. A half breed of the two methods can be utilized for an increasingly adaptable handling mode, with shifting customizable degrees to oblige assorted needs of applications that run on IoT.

5.3.3.3 Versatile Query Handling, Streamlining and Optimization

Query preparing is customarily performed close information stores so as to give inquiry execution plans, which are essentially information getting plans. Conventional question enhancement includes appointing an expense to every one of the various designs for getting information so as to pick the arrangement that is least exorbitant. With regards to IoT, question handling also includes discovering plans to bring information from the sensing devices, routers as well as gadgets that are geologically circulated and returning total readings as results.

Along these lines, there is a need for huge chunks of information as messages and trades to convert into correspondence overhead. Bringing down this overhead includes relocating inquiry preparing nearer to things which are paired in lower layer, and receiving temporary improvement to represent restricted questions. Querying improvement for WSNs ought to be seen broadly exploring in writing for WSNs are the most eminent subsystem of Web of Things (IoT); an inside and out and thorough knowledge could be searched for.

Improvement in the queries and optimal management which includes picking out the desirable inquiry plans dependent for their individual opinion expenses which gets investigated for WSNs systems. Detecting and directing information and metadata gathering are fused into a query analyzer so as to locate the best inquiry plan with low energy efficient costs. Improvements that are accomplished to the unaccompanied question do not consider the dynamicity of the system. In, fundamental database tasks, for example, read/compose and join activities are allocated power profiles, and an inquiry plan is allocated out a power cost as an element of the activities used to execute that particular plan. Adjusting a comparable methodology for IoT inquiries will include information of the power profiles of middle of the hubs and lower level sensors so as to accomplish the maximum capacity of intensity advanced question (query) plans for questions that are not restricted to information living disconnected of servers.

Vitality proficient streamlining of various questions is investigated in ecoDB for appropriated huge scale database frameworks. Bunch enquiry handling uses the nearness of regular segments in different questions, inside a task at hand. This is accomplished by lining inquiries and not executing them right away. Regular subarticulations that might be available in the lined inquiries are then combined and executed. This multi-question improvement accomplishes investment funds in

vitality utilization to the detriment of an expanded normal reaction time coming about because of the express postponements.

Multi-inquiry improvement was likewise utilized for vitality proficient question preparing in Wireless Sensor Medium. The two levels are utilized to advance the course of action of questions: A sink node (main station) level revamps about lot of inquiries to deliver an engineered set of inquiries with redundancies evacuated and regular sub-questions consolidated.

Various in-organize improvements are then used to advance the transmission of the inquiry set outcomes. Each of the three strategies has been utilized to accomplish in-organize improvement: time sharing between worldly range questions, having common regular measurement among comparative inquiries through readings communicate, and accumulation of consequence out coming from the sensors reacting for the queries from the sink-node (base station) that has successfully send the manufactured inquiries.

Conglomeration Supportability

The ceaselessly adaptive nature of information created from tech-savvy items reduces attainability to put resources into mass information gathering and capacity at one store just like the case in traditional DBMS systems. When this is done, information of time-delicate nature will have lapsed. Subsequently, it is attractive to take into consideration for the information to stockpile and occurrence that is continuously progressed as information is created.

Be that as it may, this makes the test of broadcasting chunks and huge quantity of information to the facilities where storage is available. Conglomeration as well as combination of sensor information is basic for bringing down the correspondence overhead and anticipated from transmitting crude raw streaming information. Moreover, accumulation and combination might be prerequisites for specific applications where raw information stockpiling has no additional worth. One sound cause that might have thought is about the potential loss of precision coming about because of dropping hidden detailed information. In this way, quick collection ought to be a plan factor for IoT information management systems.

Management of Data Framework Systems for IoT

The greater part of the present information recommendations are focused on WSNs, that are just a part of the worldwide IoT system, and in this way don't expressly address the more complex structural attributes of IoT. WSNs are a full grown systems administration worldview whose information arrangements rotate for the most part around in-organize information preparing and enhancement. Sensing devices are generally of constant aligned objects which are asset compelled in nature, which does not encourage modern investigation and administrations.

The principle focus in WSN-centric information the executive arrangements are to gather ongoing information immediately for speedy basic leadership, with constrained perpetual capacity capacities with regards to long haul utilization. This speaks to just a subset of the more adaptable IoT framework, which targets saddling the information accessible from an assortment of sources; stationary and versatile, shrewd and installed, asset obliged and asset rich, ongoing and documented. The

fundamental focal point of IoT-based information the board thusly expands the arrangements made for WSNs to include arrangements of a consistent method to take advantage of the volumes of heterogeneous information so as to discover intriguing worldwide examples and key chances (Pujolle 2006; Wu et al. 2011).

A mix of information from heterogeneous systems is done in such a way that adjustment and consistent mix of other IoT subsystems is accomplished. Strong and complete information the executive arrangements that help interoperability between assorted subsystems and incorporate the general lifecycle of information the board with the nearness of versatile items and setting mindfulness prerequisites are yet to be created.

Here we put forward a system for the Internet of things information the executives which is progressively perfect in the IoT information cycle and approach the structure natives talked about before. The proposed structure includes a overlapping layered methodology which focuses only in the information and information-driven middleware, and gets ideas from the combination of data repository and then board the frameworks to ensure the self-governance of autonomous IoT sub-spaces just as adaptable join/leave engineering.

System Representation

The IoT information and the executives structure comprises of six(6) stacked layers, out of which two are incorporated layers under the main system and rest are the integrated layers. Here the structure layers maps near the periods of the IoT information lifecycle depicted in, with query/coordination viewed as an additional procedure that isn't carefully a piece of the information lifecycle.

The "Things" Layer incorporates IoT sensors and shrewd items (information generation objects), just as modules for in-arrange preparing and information accumulation/constant collection (handling, total). The Communication Layer offers help for transmission of solicitations, inquiries, information, and results (gathering and conveyance). The information dual layers separately take care of the revelation along with classification of information and the capacity and ordering of gathered (information stockpiling/documented).

The Data Layer additionally handles information and inquiry preparing for neighborhood, independent information store locales (separating, preprocessing, preparing). The Federation Layer gives the deliberation and reconciliation of information vaults that is fundamental for worldwide question/investigation demands, utilizing metadata put away in the Data Sources layer to help ongoing mix of sources just as area driven solicitations (preprocessing, coordination, combination).

The Querying Layer takes the responsibilities of subtleties for inquiry, preparing as well as streamlining the participation along with the Federation Layer forming a part of the integral Transactions Layer (preparing, conveyance).

References

Agarwal, P., & Alam, M. (2018). *Investigating IoT middleware platforms for smart application development*. arXiv preprint arXiv:1810.12292.

Bowman, I. T., Bumbulis, P., Farrar, D., Goel, A. K., Lucier, B., Nica, A., Paulley, G. N., Smirnios, J., & Young-Lai, M. (2007, April 17–20). SQL anywhere: A holistic approach to database self-management. In *Proceedings of IEEE 23rd International Conference on Data Engineering Workshop (ICDE 2007)*, Istanbul, Turkey, pp. 414–423.

Cattell, R. (2010). Scalable SQL and NoSQL data stores. *ACM SIGMOD Record, 39*, 12–27.

Chen, L., Tseng, M., & Lian, X. (2010). Development of foundation models for Internet of Things. *Frontiers of Computer Science in China, 4*, 376–385.

Cooper, J., & James, A. (2009). Challenges for database management in the Internet of Things. *IETE Technical Review, 26*, 320–329.

Guinard, D., Trifa, V., Karnouskos, S., Spiess, P., & Savio, D. (2010). Interacting with the SOA-based Internet of Things: Discovery, query, selection, and on-demand provisioning of web services. *IEEE Transactions on Services Computing, 3*, 223–235.

Güting, R. H., & Mamoulis, N. (2011). Special issue on data management for mobile services. *VLDB Journal, 20*, 641–642.

Hauer, J.-H., Handziski, V., Köpke, A., Willig, A., & Wolisz, A. (2008). A component framework for content-based publish/subscribe in sensor networks. In R. Verdone (Ed.), *Lecture notes in computer science: Wireless sensor networks* (pp. 369–385). Berlin/Heidelberg: Springer.

Ozsu, M. T., & Valduriez, P. (2011). *Principles of distributed database systems* (3rd ed.). New York: Springer.

Pujolle, G. (2006, October 3–6). An autonomic-oriented architecture for the Internet of Things. In *Proceedings of IEEE John Vincent Atanasoff international symposium on modern computing* (JVA 2006), Sofia, Bulgaria, pp. 163–168.

Pungila, C., Fortis, T.-F., & Aritoni, O. (2009). Benchmarking database systems for the requirements of sensor readings. *IETE Technical Review, 26*, 342–349.

Ramakrishnan, R., & Gehrke, J. (2002). *Database management systems* (3rd ed.). New York: McGraw-Hill.

Sen, R., & Ramamritham, K. (2005, April 5–8). Efficient data management on lightweight computing devices. In *Proceedings of the International Conference on Data Engineering* (ICDE 2005), Tokyo, Japan, pp. 419–420.

Spiess, P., Karnouskos, S., Guinard, D., Savio, D., Baecker, O., Souza, L., & Trifa, V. (2009, July 6–10). SOA-based integration of the Internet of Things in enterprise services. In *Proceedings of IEEE International Conference on Web Services* (ICWS 2009), Los Angeles, CA, USA, pp. 968–975.

Vermesan, O., Harrison, M., Vogt, H., Kalaboukas, K., Tomasella, M., Wouters, K., Gusmeroli, S., & Haller, S. (2009). *Internet of Things strategic research roadmap*. Brussels: IoT European Research Cluster.

Wu, G., Talwar, S., Johnsson, K., Himayat, N., & Johnson, K. D. (2011). M2M: From mobile to embedded internet. *IEEE Communications Magazine, 49*, 36–43.

Chapter 6
Machine Learning for IoT Systems

Ahmed Khattab and Nouran Youssry

Abstract The rapid increase in the number of smart devices hosting sophisticated applications is significantly affecting the landscape of the information communication technology industry. The Internet of Things (IoT) is gaining popularity and importance in man's everyday life. However, the IoT challenges also increase with its evolution. The urge for IoT improvement and continuous enhancement becomes more important. Machine learning techniques are recently being exploit-ed within IoT systems to leverage their potential. This chapter comprehensively surveys of the use of algorithms that exploit machine learning in IoT systems. We classify such machine learning-based IoT algorithms into those which provide ef-ficient solutions to the IoT basic operation challenges, such as localization, clus-tering, routing and data aggregation, and those which target performance-related challenges, such as congestion control, fault detection, resource management and security.

Keywords Internet of Things (IoT) · Wireless sensor network (WSN) · Machine learning · Unsupervised learning · Supervised learning · Fuzzy logic

6.1 Introduction

The Internet of Things (IoT) is a networking paradigm that offers pervasive and distributed services in the move towards ubiquitous computing. IoT is a network of objects or things that communicate with each other and with the surrounding environment and share information through the Internet. IoT enables millions of devices, including sensors and smart phones/devices, to be connected for performing different tasks. According to the International Data Cooperation (IDC), the number of

A. Khattab (✉) · N. Youssry
Electronics and Electrical Communications Engineering Department, Cairo University, Giza, Egypt
e-mail: akhattab@ieee.org

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_6

IoT devices worldwide will exceed 50 billion by 2020 producing more than 60 ZB of data (Van der 2017; Sam 2016).

Wireless Sensor Networks (WSNs) are playing a main role in IoT. WSNs have attracted significant attention in recent years. A WSN is composed of a set of application-specific sensor nodes equipped with communication modules. Such nodes gather data from their environment to monitor and record target conditions at diverse locations. While there are sensors that measure almost every environmental aspect, the widely monitored parameters are air temperature and humidity, wind speed and direction, illumination intensity, flow pressure, vibration intensity, sound intensity, power-line voltage, pollution levels, chemical concentrations, and vital body functions. WSNs are powerful in developing application-specific systems.

WSNs joins the IoT networking paradigm when the sensor nodes dynamically connect to the Internet to cooperate to achieve their tasks. Both IoT and WSNs face several challenges and issues that should be addressed. Examples include energy efficiency, node localization and clustering, event scheduling, route establishment, data aggregation, fault detection and data security. Exploiting machine learning provides solutions to such problems. Machine learning could significantly boost the performance and distributive characteristic of IoT.

Machine learning (ML) emerged as an artificial intelligence (AI) technique in the late 1950s (Ayodele 2010). Since then, its algorithms gradually evolved to become more robust, effective and accurate. Recently, ML classification and regressing techniques have been widely exploited to improve the performance of many of application domains such as bioinformatics, facial and speech recognition, agriculture monitoring, fraud detection and marketing.

Machine learning could be used to improve the performance of various IoT systems by exploiting the history of the collected data of given tasks to autonomously optimize the performance without the need to re-program the system. More specifically, the main reasons that make ML important in IoT applications are:

- The rapidly changing dynamic nature of the environments typically monitored by IoT systems. Therefore, developing IoT systems that efficiently operate by autonomously adapting to such changes is required.
- The unreachable and dangerous settings in which exploratory IoT applications, such as wastewater and volcano eruption monitoring, operate to collect new knowledge. Consequently, the ability of ML-based IoT systems to self-calibrate to the acquired new knowledge is needed to ensure robustness.
- Machine learning does not only improve the autonomous control in IoT applications but also ameliorate their intelligent decision-making capabilities.

Nevertheless, the use of ML in IoT still face several challenges that should be carefully considered. For instance, IoT devices are resource limited. Using ML to extract consensus relationships between the collected data samples and predicting the accurate hypotheses significantly drain the energy of the IoT devices. This necessitates trading-off the ML algorithm's computational complexity and the targeted accuracy of the learning process.

In this chapter, we present a brief introduction of IoT: its concept, history, architecture and its processing data layers. We also present a comprehensive survey of machine learning techniques classifying them into five categories which are supervised learning, unsupervised learning, reinforcement learning, evolutionary computational and fuzzy logic techniques. We present a detailed study of the applications of machine learning techniques in solving IoT challenges. Moreover, we classify those applications into operational applications which are concerned with the main functions of the IoT system and performance applications which are more concerned with enhancing the performance of IoT systems.

The remainder of the chapter is organized as follows. Section 6.2 briefly introduces IoT. Section 6.3 overviews of the different machine learning algorithms. The role of machine learning in solving operational and performance challenges in IoT and WSN systems are discussed in Sects. 6.4 and 6.5, respectively. Finally, our conclusions are drawn in Sect. 6.6.

6.2 IoT Overview

IoT is a network of objects "things" which sense, accumulate and transfer data over the Internet without any human intervention. Kevin Ashton, British technology pioneer and co-founder of MIT's Auto-ID Center, first used the term "Internet of Things" in 1999. Ashton used the term to illustrate the power of using Radio-Frequency Identification (RFID) tags to connect goods to the Internet, then count and track them without needing human intervention. Since then, the idea of globally connecting computers and servers through the Internet has been expanded to the Internet of Things in which anything can be connected and accessed through the Internet. This created a whole new connectivity dimension where anything can be connected at anytime and anyplace (Vashi et al. 2017). The industries that are adopting IoT are expected to achieve revenue growth of 22% (Kotha and Gupta 2018).

Several IoT architectures have been developed to handle the use of heterogeneous devices in such systems. The number and type of used devices, the application and the amount of collected and processed data control the choice of the most suitable architecture to be used.

One simple IoT architectural model is the three-layer model shown in Fig. 6.1 which consists of perception, network and application layers (Ghasempour 2019).

- Perception Layer: This is the physical layer of the IoT system. It is composed of the sensors which gather information about the environment and actuators which implement the actions that accordingly change the environment. A temperature controller in an air conditioner is an example of an actuator.
- Network layer: This is the transmission layer that is responsible for handling the routing decisions. It is also handling the transmission and processing of the data received from or transmitted to the perception layer.

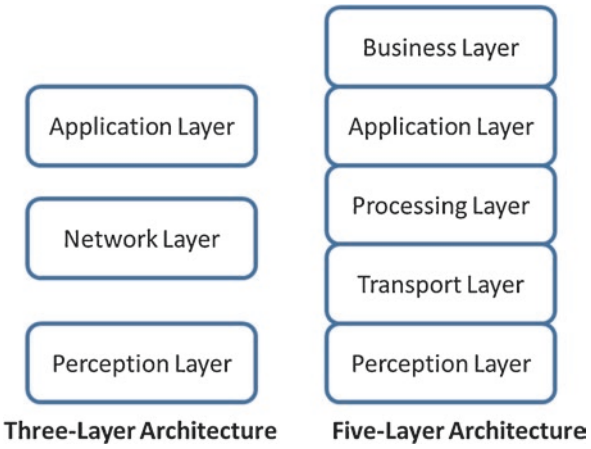


Fig. 6.1 IoT architecture models

- Application Layer: This layer delivers application-specific services to end users. It also provides the interface between humans and the IoT system.

Such three-layer architecture represents the simplest IoT architecture. As the data size of the system increase, this architecture becomes inefficient. That is why the five-layer model shown in Fig. 6.1 was proposed in (Sethi and Sarangi 2017), adding the following three layers to the perception and application layers:

- Transport Layer: This layer handovers data from the perception layer to the processing layer and actions in the reverse direction. Several network types are used for this purpose such as wireless LAN, NB-IoT, LoRA, RFID, and NFC.
- Processing Layer: This is the middleware layer that stores and processes the huge amounts of data received from the transport layer. It also prepares the data for the application layer. The processing layer manages and provides a wide range of services to the lower layers. Cloud computing, databases and big data analysis are examples of the technologies used in this layer.
- Business Layer: This layer encompasses the overall IoT application alongside its business and profit models. It is also responsible for the end users' privacy and security.

Another architecture presented in (Navani et al. 2017) proposed the same division of layers with only changing their names. The layers in this architecture are the object, object abstraction, service management, application and business layers.

Cloud computing was originally used to implement the processing layer because it provides significant flexibility and scalability. A cloud database management system based on a five-layer architecture was introduced in (Alam et al. 2013). Significant efforts were carried out to enhance cloud computing system's database with query processing mechanism in (Malhotra et al. 2018) and to enhance the task scheduler as in (Ali et al. 2019). As energy is known to be a scarce resource in IoT

systems, the authors of (Ali and Alam 2016) proposed energy management techniques for cloud computing environments. IoT devices generate valuable data readings that need to be transferred. Therefore, merging cloud computing technology with big data analysis (Alam and Shakil 2016) is a very important in many platforms as discussed in (Khan et al. 2016, 2018, 2019a, b, c, d; Shakil et al. 2017).

Lately, the increase of real-time applications requiring the least possible latency caused a migration towards another processing architectures that involve either fog or edge computing. In fog computing paradigms, the data and its processing take place in decentralized computing structures that physically reside between the data sources and the cloud. Hence, fog computing results in low-latency and is suitable for time-sensitive IoT applications as data is processed close to where it is originated. Its efficiency is also higher as less data is uploaded to the cloud. On the other hand, data processing takes place either on the IoT device generating the data or on a local gateway device that resides in the vicinity of the IoT device in the edge computing paradigm. Thus, both fog and edge computing reduce the dependence on the cloud infrastructure in data analysis, which in turn reduce the system latency, and hence, allow the data-driven decisions making process much faster. However, fog computing is the better option where data aggregation from different sources is needed whereas edge computing is better where the least latency is allowed. The differences between cloud computing, fog computing and edge computing are illustrated in Fig. 6.2.

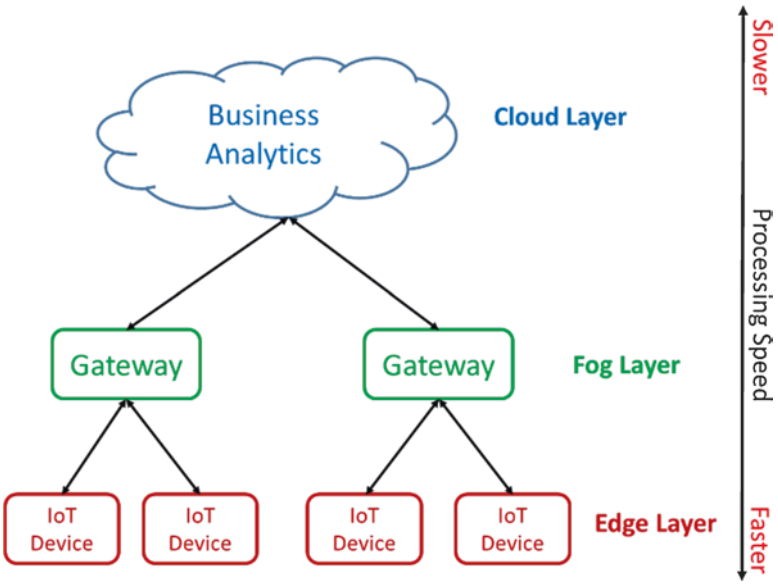


Fig. 6.2 Mapping IoT processing layers to system devices

6.3 Machine Learning Taxonomy

Machine learning techniques are designed to automatically benefit from prior experience in acting in the future without explicit reprogramming. Existing ML approaches are typically classified as either supervised, unsupervised or reinforcement learning. However, artificial intelligence techniques have recently played a great role in enhancing ML techniques. Therefore, this chapter categorizes ML techniques into supervised learning, unsupervised learning, reinforced learning, evolutionary computation and fuzzy logic. This section briefly overviews the different ML approaches in addition to their most updated algorithms in the context of IoT and WSNs.

6.3.1 Supervised Learning

In supervised learning, the input and targeted output data are both labeled for classification. This presents the learning base on which future data processing is centered. The key supervised learning algorithms are:

1. *k*-nearest Neighbor (*k*-NN): In this supervised learning approach, a data sample is classified according to the labels of nearby data samples. Simple methods (e.g., the Euclidean distance between the IoT devices) are typically used to compute the average measurements of neighboring devices within a specific range. It is a simple computational algorithm but may be inaccurate in large data sets. In IoT, *k*-NN is used in fault detection (Warriach and Tei 2017) and data aggregation approaches (Li and Parker 2014).
2. Support Vector Machine (SVM): Decision planes are used in SVM approaches to define decision boundaries. A decision plane separates groups of objects each with different class memberships as depicted by the example shown in Fig. 6.3.

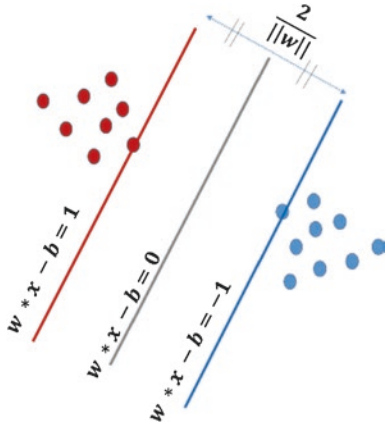


Fig. 6.3 Support vector machine example

SVM supervised learning is typically used for localization problems (Kang et al. 2018) to detect malicious behaviors and to address several security issues in IoT and WSNs (Zidi et al. 2018) due to its high accuracy.

3. Neural Network (NN): An artificial neural network (ANN) imitates biological neurons by interconnecting layers of artificial neurons. These artificial neurons map the different sets of input data onto a set of appropriate outputs. Figure 6.4 presents the model of a neural network. Even though ANNs provide solutions to non-linear and complex problems, they are computationally complex. Artificial NNs improve the efficiency of IoT localization (Banihashemian et al. 2018; El Assaf et al. 2016), detect faulty nodes (Chanak and Banerjee 2016), and establish routing (Mehmood et al. 2017).
4. Bayesian Interface: Unlike most machine learning algorithms, Bayesian inference uses a reasonably small number of samples for training. Bayesian methods efficiently learn uncertain perceptions by adapting probability distributions while avoiding overfitting. However, they need prior knowledge about the environment. Bayesian interface is suitable for fault detection (Warriach and Tei 2017), cluster head selection (Jafarizadeh et al. 2017) and localization (Sun et al. 2017; Wang et al. 2017; Guo et al. 2018) approaches.
5. Decision Tree (DT): A tree-like model of decision or classification is used in such a decision-support tool. DTs are created using a set of if-then conditions. For boosting DT accuracy, the random forest (RF) algorithm is introduced. RF is an ensemble decision tree method that operates by constructing multiple classifiers. Each classifier is a decision tree. RFs are used in intrusion detection as in (Varsha et al. 2017).

6.3.2 Unsupervised Learning

Unsupervised learning algorithms operate over datasets in which the input data does not have labeled responses. Inferences are drawn in such algorithms by classifying the unlabeled input data into groups that are called clusters.

1. Principal Component Analysis (PCA): PCA reduces the dimension of a large set of variables to a much smaller set that contains almost all the information in the

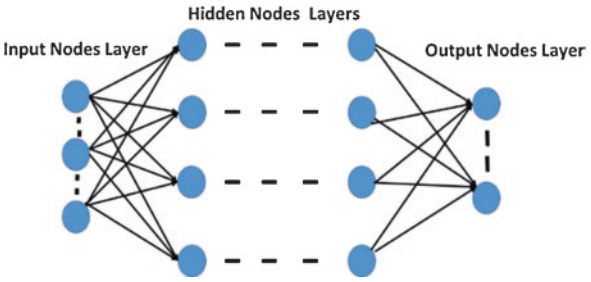


Fig. 6.4 Neural networks' structure

original large set. PCA application in IoT systems for data dimensionality reduction takes place either at the sensor or the cluster head levels. PCA results in a reduction in the communication overhead (Wang et al. 2019) which is very useful in data aggregation (Liu et al. 2017).

2. *k*-means Clustering: It is used to classify different data in classes or clusters (Jain et al. 2018). *k* random centroids are initially chosen. The other nodes then join the clusters of the nearest centroid. Averaging over the nodes in each cluster, new centroids are determined. The algorithm repeats the previous steps until convergence is reached.
3. Self-Organizing Maps (SOM): A self-organizing map is also considered as a method for dimensionality reduction as explained in (Miljković 2017). However, a SOM is a type of artificial neural network which result in a discretized low-dimension representation of the input data, called a map, using unsupervised learning for training. SOMs are very suitable to be used in building clusters in IoT.

6.3.3 Reinforcement Learning

Reinforcement learning (RL) does not have knowledge about the inputs nor their corresponding outputs. It is a very important ML technique whose idea, illustrated in Fig. 6.5, is that an agent will learn from the environment by interacting with it and receiving rewards for performing actions. Over the past few years, RL algorithms have been used for designing routing protocols in IoT systems and WSNs to reduce the energy consumption and improve the network performance (Habib et al. 2018).

An extensively used RL algorithm is Q-learning. First, a Q table is initialized, then an action a is performed. A reward is then measured to update the Q table. In order to assess how good to take a certain action a at a particular state s, the action-value function $Q(s, a)$ is learnt by the algorithm. Initially, the action a is randomly chosen until the Q table is constructed, then the best action is chosen from it.

Fig. 6.5 Reinforcement learning concept

6.3.4 *Evolutionary Computation*

Unlike other ML approaches, evolutionary computation techniques solve problems using computational models that mimic the biological behavior of either humans or animals in problem solving tasks.

1. Genetic Algorithms (GA): Such algorithms use biologically inspired heuristic search techniques to find the best solution for problems with large search spaces. GAs work in parallel on a population of solutions rather than processing a single solution. First, a chromosome structure is defined, typically in the form of an array of bits as shown in Fig. 6.6. Then, an initial chromosomes population is randomly generated for which fitness is evaluated. Chromosomes with higher fit-ness are selected in the selection process. A crossover process combines two parents to introduce a new child to the population. Finally, mutation randomly up-dates the parents to introduce new children. An example GA cycle is shown in Fig. 6.6. GAs are suitable for data aggregation approaches and searching for optimal clusters.
2. Ant Colony Optimization (ACO): ACO probabilistically searches for the optimal path in a graph in ways similar to how ants find the path between a food source and the colony. First, ants move randomly, leaving traces or pheromone on the taken path. More pheromone on a path indicates that the path probability to be the shortest/optimum one is high. This algorithm is efficient for routing in IoT.
3. Particle Swarm Optimization (PSO): PSO is inspired by swarm theory, fish schooling, and bird flocking. As an evolutionary computation approach, PSO searches for the best solution in a population. The algorithm starts with a random

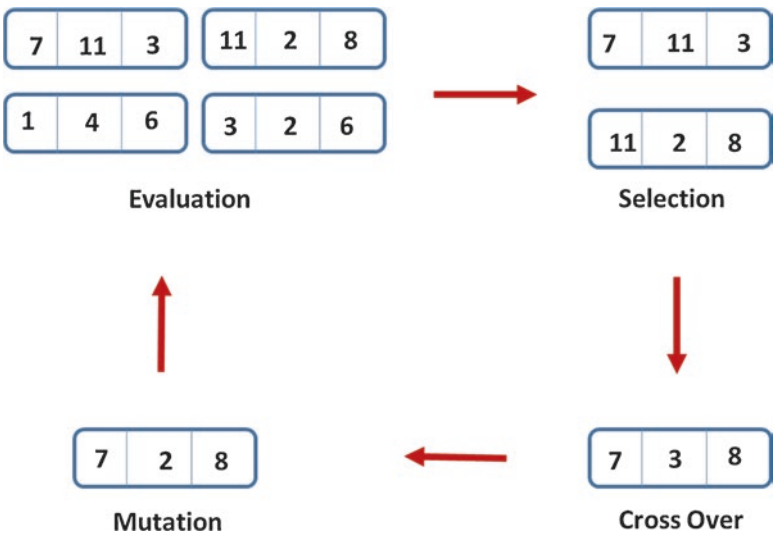


Fig. 6.6 Genetic algorithm example

population of solutions referred to as particles. A fitness function is used to compute the particle's fitness value which is optimized in each generation. IoT clustering algorithms recently exploit PSO to improve their performance.

6.3.5 Fuzzy Logic

Traditional ML techniques used to work with binary values: either 0 (False) and 1 (True). However, fuzzy logic (FL) imitates the way of decision making in a human which considers all the possibilities between 0 and 1 digital values (Umarikar 2003). FL introduces the concept of degree of truth. Its value does not have to be exactly 1. It can be any real value between 0 and 1 instead. Fuzzy logic is an attractive solution for localization typically used to combine the node's residual energy, centrality, and distance from the data sink node for electing the best cluster heads (Umarikar 2003).

6.4 Machine Learning for IoT Basic Operation

In this chapter, we categorize the challenges that face IoT systems into basic operation and performance-related challenges. In this section, we take a closer look on how ML is making an effective contribution in solving the basic system operation challenges such as node localization, clusters formation, routing, and data aggregation. Figure 6.7 summarizes how ML is used in addressing such challenges.

6.4.1 Node Localization

The procedure of determining the geographic coordinates of the nodes is known as localization. As much as it is crucial to be aware of IoT nodes' locations, it is impractical to use GPS hardware in every node as it dramatically consumes the nodes' energy. Alternatively, localization can exploit machine learning alongside some parameters such as the received signal strength (RSS) and the time and angle of arrival.

An approach was introduced in (Sun et al. 2018) to use neural networks in localizing WSN nodes. The proposed solution uses the variations of the RSS between the sensor nodes. RSS is measured from all the nodes once without the presence of any target, then with the target presence. The ANN uses the difference in RSS values and the corresponding matrix indices as inputs. The ANN outputs are the nodes' locations. The ANN is trained to approximate a nonlinear function to map the inputs and outputs.

The use of SVM in localization was proposed in (Kim et al. 2013). What makes this approach different is the use of ensemble SVM technique. The ensemble technique employs multiple ML techniques, then decides the result by voting. In

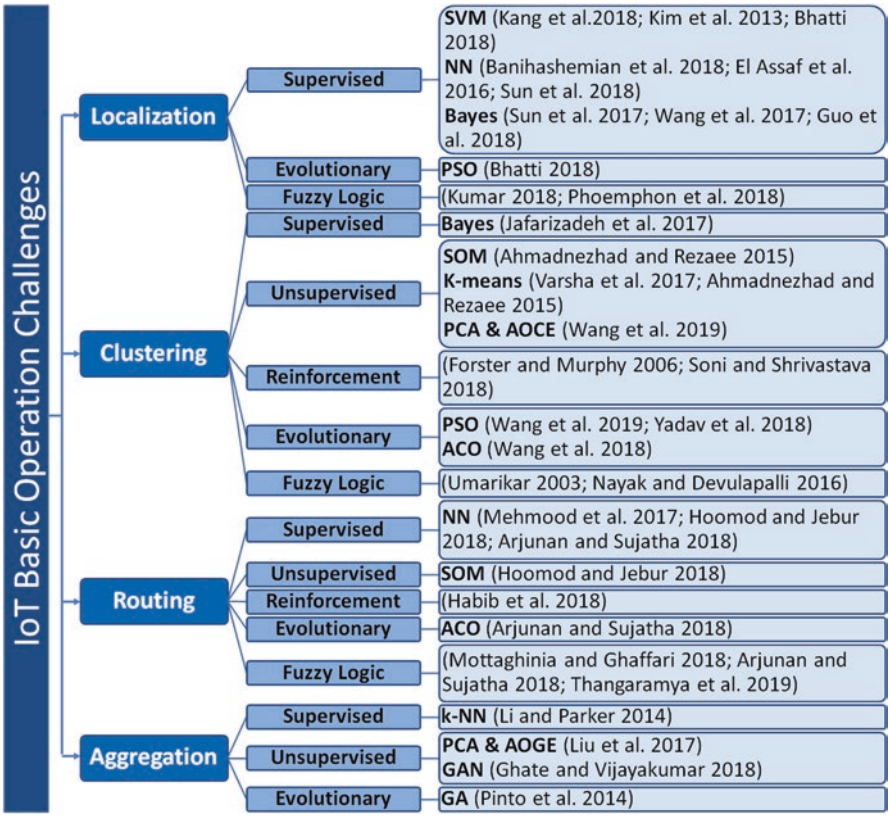


Fig. 6.7 Machine learning exploitation for IoT basic operation

(Kim et al. 2013), the authors used multiple SVMs by dividing the WSN to many subnetworks. Each subnetwork is trained using SVM. The resulting sub-predictions are then combined as ensemble combination. Each training problem has a smaller size compared to the size of the original problem. Consequently, better results are obtained. Another advantage of having fewer sensor nodes per subnetwork is the reduction in the transmission power and communication energy as the nodes become close to each other. The idea of treating localization problem as regression problem in-stead of a classification one was introduced in (Bhatti 2018). The algorithm is divided into two phases. The training dataset for localization in WSN contains of the feature vectors related to each anchor and its true location coordinates which are already known. The feature vector of an anchor node is composed of the RSS values of the signals received from other nodes as measured by that anchor node. In the second phase, the sensor nodes' coordinates are estimated. The input of the learned model is the target WSN nodes' feature vectors. The produced output is the nodes' coordinates. Comparing the extended feature vector (readings from anchor and sensor nodes) versus the reduced feature vectors (readings from anchor vectors only) showed that the extended features provide a better prediction accuracy.

Another localization technique was explained in (Kumar 2018) using fuzzy logic ML technique. The proposed technique was a hybrid Sugeno-Mamdani fuzzy system using RSS for localization which outperformed the traditional fuzzy logic. The authors then proposed the idea of cooperative localization. In such scheme, whenever an unknown node gets localized, it acts as anchor or landmark for the next iteration and transmits beacons to other unknown nodes. Since it has already been localized now and can broadcast beacons which contain its position, identity to be received by other unknown nodes. A low-complexity centroid-based scheme is proposed in (Kumar 2018). The resulting precision error is high. Hence, the authors used a FL algorithm to improve the nodes' location estimation based on FL weights. For more optimization, the consequences of unbalanced node placements in non-uniform networks are alleviated using PSO. This approach proved its efficiency in networks with few nodes and limited sensing coverage. As the number of nodes and/or the sensing coverage increase, integrating extreme machine learning techniques (as NN) with the centroid scheme showed better results in (Phoemphon et al. 2018).

6.4.2 Clustering

IoT systems are energy-constrained networks. Transmitting all the data packets to the sink node is inefficient and dramatically consumes the nodes' energy. A local aggregator, or a cluster head (CH), is used to improve the energy-efficiency by collecting the data from the cluster members within its vicinity and transmitting only the aggregation of the data to the sink node. Machine learning algorithms can help in deciding the number of clusters needed and electing the cluster heads.

An integrated approach in which clustering is performed using a SOM phase followed by a *k*-means phase was introduced in (Ahmadnezhad and Rezaee 2015). The SOM input parameters are the energy levels and the nodes' coordinates. The weight vectors of the SOM map units are selected nodes with maximum energy levels. Such maximum-energy nodes attract the nearest lower-energy nodes, thereby, creating energy-balanced clusters. Fuzzy logic techniques can also be used in electing cluster heads as proved in (Nayak and Devulapalli 2016). The authors of (Nayak and Devulapalli 2016) proposed a fuzzy logic clustering approach using the battery power, node mobility and node centrality as input parameters to a FL system that finds the probability of a node to serve as a cluster head. Simulation results showed that the fuzzy logic cluster head election system outperforms the well-known LEACH clustering protocol in terms of the network lifetime defined as the time until first node dies, last node dies or half the nodes die.

A cluster formulation method in which a node individually decides its ability to serve as a CH rather than executing an election process is presented in (Forster and Murphy 2006). This clustering method exploits Q-learning alongside a set of dynamic parameters such as the nodes' energy levels. A reinforcement learning technique was also used in (Soni and Shrivastava 2018) to implement an on-demand

mobile sink traversal. Recently, evolutionary computation algorithms are used showing enhancement in solving the clustering problem as in (Wang et al. 2018) where ACO-based approach is used. Likewise, Energy Centers Searching using Particle Swarm Optimization (EC-PSO) is proposed in (Wang et al. 2019). A geometric method is initially used to elect the CHs. Then, EC-PSO performs clustering when the nodes' energies start to be heterogeneous. EC-PSO elects the nodes close to the energy center to be CHs using an improved PSO technique that searches the energy centers. PSO algorithm increases the network lifetime as proved in (Yadav et al. 2018).

6.4.3 Routing

Designing a routing protocol for IoT systems is very challenging due to their nature of restricted processing, compact memory, and low bandwidth. Routing protocols address several issues including scalability, energy utilization, data coverage, and fault tolerance while optimizing their tradeoffs. Machine learning can effectively address this challenge as it continuously discovers the optimal routing paths that result in the best tradeoffs is the dynamically changing IoT networks. ML also reduces the complexity of a typical routing problem by breaking it down to subrouting problems that only consider the local neighbors of the nodes. Finally, ML effectively achieves the routing QoS requirements despite the use of computationally inexpensive algorithms and classifiers (Alsheikh et al. 2014).

A wireless routing protocol that uses SOM alongside a modified radial-based neural network was presented in (Hoomod and Jebur 2018). It starts with clustering the networks using SOM as previously explained. Then, an ANN will be responsible for finding the optimal path. However, the used ANN is modified by having the weights to the output layer computed and attuned using the parallel Moore-Penrose generalized pseudo-inverse which accelerates the learning process and accuracy. Taking time as a comparison metric, the proposed protocol outperformed the traditional Dijkstra in fixed and mobile topologies.

FL was also used in solving the routing challenge. In (Mottaghinia and Ghaffari 2018), two fuzzy logic-based systems were proposed to route data messages and specify their priority. When a source node encounters other nodes, it checks the data delivery probability of each node alongside the node's energy. A node is not considered as a potential router if either the residual energy and delivery probability is low, or both is low. Ultimately, the fuzzy system will select the best candidate for data transmission from the nodes' neighbors. The proposed approach shows its efficiency by increasing the data delivery rate and decreasing the associated delay.

Another approach combines FL (for clustering) and ACO (for routing) (Arjunan and Sujatha 2018). The node's residual energy, degree, centrality and distance to both the Base Station (BS) and neighboring nodes are used as inputs to the FL-based clustering algorithm which maximizes the network lifetime while balancing the nodes' energies. ACO is used to get the shortest paths. Also, periodic random choice

of paths occurs to exploit unused paths and to balance the nodes' energies. Again, FL is used in (Thangaramya et al. 2019) but this time for enhancing the NN to be used in discovering energy-efficient routes. The NN discovers new routes by investigating the consumed energy in the nodes and the routing patterns. The routes' weights are attuned by applying FL rules to reach the most efficient route.

6.4.4 Data Aggregation

Data aggregation is very crucial to reduce the IoT system power consumption. It combines and summarizes the data packets of several nodes properly at the cluster head. Data aggregation decreases the number of transmitted data packets, thereby, increases the bandwidth utilization and minimizes the energy consumption. In what follows, we demonstrate the power of machine learning techniques in this field.

First, (Pinto et al. 2014) proposed using genetic algorithms in information fusion to perform a trade-off between the Quality of Fusion (QoF) and efficiency by dynamically adjusting the sending probability. According to the effect of a node's input on the system performance, each node is given a reward that will decide whether to send data or fuse it with another node instead.

A priority-based data aggregation approach was introduced in (Ghate and Vijayakumar 2018). It works in supervised mode if the input data has class labels. For example, the health issue or the disease may be known previously in certain cases, hence, it can be used as a class label in the output vector. Alternatively, this approach may work in unsupervised mode with input data lacking class labels. A novel approach combining PCA and Angle Optimized Global Embedding (AOGE) was introduced to tackle the concept drift problem (Liu et al. 2017). In ML context, concept drift implies that the target variable, to be predicted by the model, has time-varying statistical properties that vary in unforeseen ways. Consequently, the prediction process results in less accurate predictions with time. AOGE takes advantage of several techniques. The projection variance of sampled data is first analyzed. Then, PCA is used to define the dispersion in the data. The principal components are then selected considering the maximized projection variance. Unlike PCA, AOGE analyzes the projection angle of sampled data to choose the principal components. Consequently, AOGE outperforms PCA when tested using real-life datasets with significantly noisy data. This implies that even though PCA and AOGE separately detect concept drift in a data stream, their combination is more effective and robust in detecting concept drift.

6.5 Machine Learning for IoT Performance Aspects

While the basic operational challenges are directly associated with functional behavior of IoT systems, performance aspects are mostly associated with performance enhancement. The performance enhancing requirements include fault detection, mitigation and controlling congestion provide quality of service and maintain security. This section sheds the light on the exploitation of machine learning in such performance-related aspects (summarized in Fig. 6.8).

6.5.1 Congestion Control

Congestion negatively impacts the performance of IoT applications as it causes packet losses, increases the encountered delays, wastes the nodes' energies and significantly degrades the IoT application fidelity. The purpose of IoT and WSN congestion control is to improve the network throughput and reduce the time of data

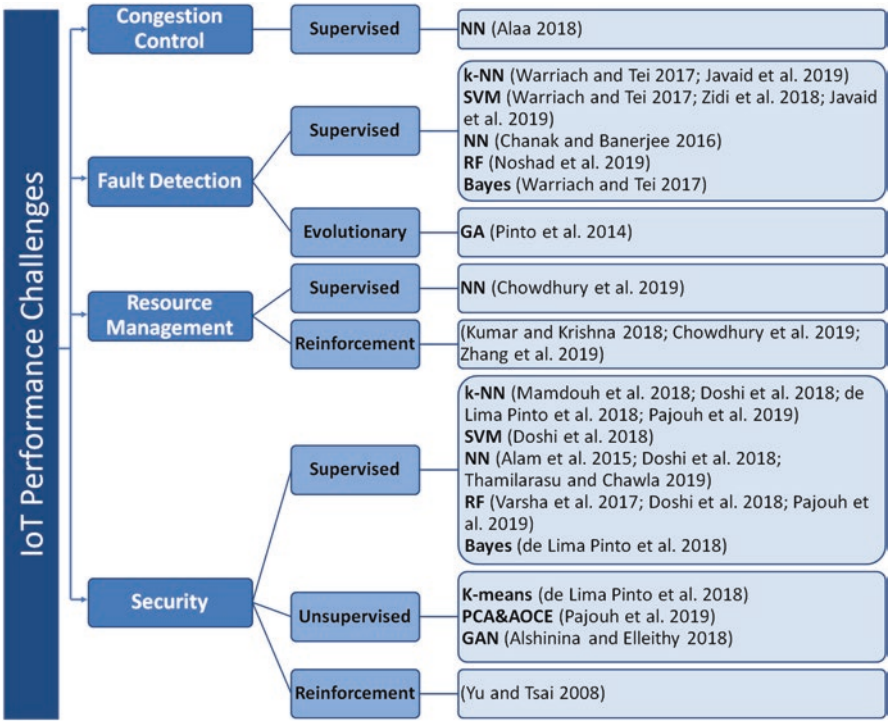


Fig. 6.8 Machine learning exploitation for enhancing IoT performance

transmission delay. Thus motivated, the authors of (Alaa 2018) proposed to have a congestion detection phase followed by a congestion monitoring phase. The system detects the congestion through measuring the data loss rate. The congestion monitoring system is simply an ANN for learning about the congestion scenarios to reduce and stop them before they even occur. This approach proved significant improvement when compared against the traditional case of not having congestion control.

6.5.2 Fault Detection

As explained in (Warriach and Tei 2017), faults occur when one or more of the IoT system characteristics or parameters deviate from their normal operation or value. Faults occur when node is faulty because of a physical damage, a low battery, communication interference, or environmental interference. An error is defined as an incorrect sensing of a state or event in the given space due to a fault. Faults can be classified into:

- Offset fault: This fault occurs when the data always differ from its expected value by a constant amount because of faulty calibration of the sensing module.
- Gain fault: This fault occurs when the rate of change of the sensed data in a period of time differs from its expected value.
- Stuck-at fault: This type of faults happens when the sensed data is constant and does not vary with time (zero-variance).
- Out-of-bounds fault: This fault happens when the values of the sensed data exceeds the normal operation bounds.

In (Warriach and Tei 2017), the fault detection problem is changed into a simple classification problem where the received data either belongs to a normal or a defected class. Three machine learning approaches were used for this purpose: *k*-NN, SVM and Naïve Bayes. *k*-NN has the least classification error in the least computing time followed by SVM. However, Naïve Bayes showed the worst performance. In (Zidi et al. 2018), the authors brought attention to a different kind of faults and how to solve it. This fault was the random fault that is defined as an instant error in which data is disturbed just for an instant of time. This error causes many positive or negative sharp peaks that influence the data of the sensors. These perturbations are very fast which makes them more difficult to detect. The authors proposed an SVM classifier for detecting instant errors which showed a high accuracy that reached 99%. Evolution of the traditional classifiers is proposed in (Javaid et al. 2019) by implementing Enhanced SVM (ESVM) which combines SVM and GA. Also, the authors implemented Enhanced KNN (EKNN) and Enhanced Recurrent Extreme Learning Machine (ERELM) which gives the most accurate results. Another classifier was introduced in (Noshad et al. 2019) which uses RF algorithm and shows better results compared to SVM and NN.

6.5.3 Resource Management

To satisfy the enormous resource demands of the various IoT applications, robust resource management techniques are needed to minimize the energy consumption and the response time. Since IoT systems are dynamic in nature, RL is one of the most suitable ML technique in IoT resource management as proposed in (Kumar and Krishna 2018). However, RL complexity increases with the increase in action pairs. Researchers combined NN and RL to introduce Drift Adaptive Deep Reinforcement Learning (DA-DRL) in (Chowdhury et al. 2019) to enhance traditional RL methods. Another scheduling technique was suggested in (Zhang et al. 2019) as Q-Learning Scheduling on Time Division Multiple Access (QS-TDMA) to improve the real-time reliability.

6.5.4 Security

As IoT systems are resource limited, securing such systems against security at-tacks presents an immense challenge. Several approaches for secure authentication in IoT systems through cloud computing exist (Kumari et al. 2018; Alam et al. 2015). However, the majority of contemporary IoT commercial devices suffer severe security flaws and vulnerabilities as shown in (Williams et al. 2017). That is why the demand for using ML techniques is rapidly growing to save such networks from different security attacks. Here, we discuss the major five IoT attacks (Mamdouh et al. 2018).

- Distributed Denial of Service (DDOS) Attack: In this cyber-attack, the attackers overload the system making it difficult to be used by its intended users by sending multiple requests to exceed its capacity, and therefore, crushing.
- Spoofing Attack: Is a cyber-attack where attackers aim to masquerade and deceive the system by pretending to be an authorized node to trick them in performing legitimate actions or giving up sensitive data.
- Malware Attack: Is a cyber-attack in which a malware or a malicious software performs activities on the victim's operating system, usually without the node's knowledge.
- User to Root (U2R): In this attack, the attacker attempts to escalate a user's privilege from being limited to become a super user or be able to access the root. This is achieved using stolen credentials or through a malware infection.
- Remote to Local (R2L): In this attack, the attacker imitates a legitimate user to gain remote access to a victim device.

In (Doshi et al. 2018), the authors detect DDOS attacks through capturing the data traffic and analyzing its features. It was proved that normal IoT traffic differs from DDOS traffic in terms of packet size, inter packet arrival, used protocol, the bandwidth and node/IP destination. Based on that observation, normal ML

classification techniques such as SVM, *k*-NN, ANN and Random Forest were used. It was shown that Random Forest and *k*-NN perform best. However, an updated technique was presented in (Thamilarasu and Chawla 2019) which combines ML and deep learning algorithms to form a deep neural network to detect DDOS attacks more precisely. NN is used with cooperation on cloud trace back technique to detect DDOS attacks as in (Alam et al. 2015).

Detecting spoofing attacks needs four main stages as illustrated in Fig. 6.9. ML techniques are commonly used in the feature detection and attack detection stages. In (de Lima Pinto et al. 2018), feature detection was achieved using a *k*-means algorithm and a *k*-NN classifier was proposed. Another technique was proposed in (Pajouh et al. 2019) that uses PCA in dimension reduction in addition to two classifiers: Naïve Bayes classifier followed by a *k*-NN classifier. This two-tier classification has high detection rates and accurate detection of the U2R and R2L hard-to-detect security attacks.

Malware detection was approached as a classification problem using random forest and *k*-NN in (Pajouh et al. 2019). An interesting approach for intrusion detection was shown in (Yu and Tsai 2008) in which each sensor node is equipped with an intrusion detection agent (IDA). As nodes cannot trust each other, IDAs do not cooperate. A Local Intrusion Detection Component (LIDC) is responsible for extracting the local features such as the packet delivery and collision rates, delays, number of neighbors, cost of routing and consumed energy. Meanwhile, Packet based Intrusion Detection Component (PIDC) infers if a suspected node is launching an attack on the host by analyzing the suspected node's packets and investigate the packets' RSS, the arrival rate of the sensed data and retransmission rate of the attacker's packets. Then, SLIPPER machine learning algorithm is used for detection.

Finally, securing WSN and IoT middleware using Generative Adversarial Networks (GANs) was proposed in (Alshinina and Elleithy 2018). The proposed approach is composed of two networks. A generator network that generates fake data that mimics the real sensed data and confuses the attacker by combining both the fake and real data. A discriminator network is then used to separate the fake data from the real data. This does not only protect data from adversaries but also improves the data accuracy compared to conventional techniques.

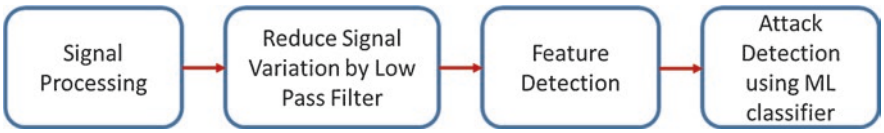


Fig. 6.9 The detection stages of spoofing attacks

6.6 Concluding Remarks

The unique nature of WSNs and IoT systems gives us no choice but to address their challenges and limitations through suitable tools and specified techniques. Here comes the need for machine learning techniques either supervised learning, unsupervised learning, reinforcement learning, evolutionary computation or fuzzy logic. All such techniques offer different solutions to most of the challenges. In this chapter, we have discussed these solutions for addressing the IoT basic operation challenges such as node localization, cluster formulation, routing and data aggregation. Moreover, we have discussed the role of machine learning in solving the performance-related challenges such as congestion control, fault detection, resource management and security. We conclude with the following remarks:

- Performance related aspects mainly exploit supervised learning techniques. Such challenges are handled as classification tasks where the algorithm needs to predict discrete value or identify the input data into a particular class. This requires prior knowledge and that is why supervised ML techniques are suitable here.
- Evolutionary techniques are used for solving basic operation rather than performance related aspects. Their objective is injecting new actions and measuring their effect e.g. by imitating ants in reaching their destination. This makes evolutionary technique not suitable for performance challenges which are typically modelled as classification tasks.
- Since fuzzy systems are capable of handling uncertainties and giving wide range of truth, they are recently being adopted for IoT routing and node localization.
- Resource management is solved using reinforcement learning (Q-learning technique). IoT systems are very dynamic. Managing their resources also needs a dynamic technique that always interacting with the surrounding environment to make the right immediate actions. Hence, RL comes as a perfect match here.

References

Ahmadnezhad, F., & Rezaee, A. (2015). Increasing the lifetime of wireless sensor networks by self-organizing map algorithm. *International Journal of Computer Networks and Communications Security, 3*(4), 156–163.

Alaa, M. (2018). Radial basis neural network controller to solve congestion in wireless sensor networks. *Iraqi Journal for Computers and Informatics, 44*(1), 53–62.

Alam, M., & Shakil, K. A. (2016). Big data analytics in cloud environment using Hadoop. In *International conferences on mathematics, physics & allied sciences*.

Alam, B., Doja, M., Alam, M., & Malhotra, S. (2013). 5-layered architecture of cloud database management system. *AASRI Procedia Journal, 5*, 194–199.

Alam, M., Shakil, K.A., Javed, M. S., & Ansari, M. (2015). Ambreen: Detect and filter traffic attack through cloud trace back and neural network. In *International conference of parallel and distributed computing*.

Ali, S. A., & Alam, M. (2016). A relative study of task scheduling algorithms in cloud computing environment. In *2nd international conference on contemporary computing and informatics (IC3I)*.

Ali, S. A., Affan, M., & Alam, M. (2019). A study of efficient energy management techniques for cloud computing environment. In *9th international conference on cloud computing, data science & engineering (Confluence)*.

Alsheikh, M., Lin, S., Niyato, D., & Tan, H. (2014). Machine learning in wireless sensor networks: Algorithms, strategies, and applications. *IEEE Communication Surveys and Tutorials, 16*(4), 1996–2018.

Alshinina, R., & Elleithy, K. (2018). A highly accurate deep learning based approach for developing wireless sensor network middleware. *IEEE Access, 6*, 29885–29898.

Arjunan, S., & Sujatha, P. (2018). Lifetime maximization of wireless sensor network using fuzzy based unequal clustering and ACO based routing hybrid protocol. *Applied Intelligence, 48*(8), 2229–2246.

Ayodele, T. (2010, February). Introduction to machine learning. In Y. Zhang (Ed.), *New advances in machine learning*. IntechOpen.

Banihashemian, S., Adibnia, F., & Sarram, M. (2018). A new range-free and storage-efficient localization algorithm using neural networks in wireless sensor networks. *Wireless Personal Communications, 98*(1), 1547–1568.

Bhatti, G. (2018). Machine learning based localization in large-scale wireless sensor networks. *Sensors, 18*(12), E4179.

Chanak, P., & Banerjee, I. (2016). Fuzzy rule-based faulty node classification and management scheme for large scale wireless sensor networks. *Expert Systems with Applications, 45*(C), 307–321.

Chowdhury, A., Raut, S., & Narman, H. (2019). DA-DRLS: Drift adaptive deep reinforcement learning based scheduling for IoT resource management. *Journal of Network and Computer Applications, 138*, 51–65.

de Lima Pinto, E., Lachowski, R., Pellenz, M., Penna, M., & Souza, R. (2018). A machine learning approach for detecting spoofing attacks in wireless sensor networks. In *IEEE international conference on Advanced Information Networking and Applications (AINA)*.

Doshi, R., Apthorpe, N., & Feamster, N. (2018). *Machine learning DDoS detection for consumer Internet of Things devices*. arXiv preprint arXiv: 1804.04159.

El Assaf, A., Zaidi, S., Affes, S., & Kandil, N. (2016). Robust ANNs-based WSN localization in the presence of anisotropic signal attenuation. *IEEE Wireless Communications Letters, 5*(5), 504–507.

Forster, A., & Murphy, A. (2006). CLIQUE: Role-free clustering with Q-learning for wireless sensor networks. In *IEEE international conference on distributed computing systems*.

Ghasempour, A. (2019). Internet of Things in smart grid: Architecture, applications, services, key technologies, and challenges. *Inventions, 4*(1), 22.

Ghate, V., & Vijayakumar, V. (2018). Machine learning for data aggregation in WSN: A survey. *International Journal of Pure and Applied Mathematics, 118*(24), 1–12.

Guo, Y., Sun, B., Li, N., & Fang, D. (2018). Variational bayesian inference-based counting and localization for off-grid targets with faulty prior information in wireless sensor networks. *IEEE Transactions on Communications, 66*(3), 1273–1283.

Habib, A., Arafat, M., & Moh, S. (2018). Routing protocols based on reinforcement learning for wireless sensor networks: A comparative study. *Journal of Advanced Research in Dynamical and Control Systems*, (14), 427–435. http://www.jardcs.org/backissues/abstract.php?archiveid=6166

Hoomod, H., & Jebur, T. (2018). Applying self-organizing map and modified radial based neural network for clustering and routing optimal path in wireless network. *Journal of Physics: Conference Series, 1003*, 012040.

Jafarizadeh, V., Keshavarzi, A., & Derikvand, T. (2017). Efficient cluster head selection using naïve bayes classifier for wireless sensor networks. *Wireless Networks, 23*(3), 779–785.

Jain, B., Brar, G., & Malhotra, J. (2018). EKMT-k-means clustering algorithmic solution for low energy consumption for wireless sensor networks based on minimum mean distance from base station. In *Networking communication and data knowledge engineering*. Springer.

Javaid, A., Javaid, A., Wadud, Z., Saba, T., Sheta, O., Saleem, M., & Alzahrani, M. (2019). Machine learning algorithms and fault detection for improved belief function based decision fusion in wireless sensor networks. *Sensors, 19*(6), 1334.

Kang, J., Park, Y., Lee, J., Wang, S., & Eom, D. (2018). Novel leakage detection by ensemble CNNSVM and graph-based localization in water distribution systems. *IEEE Transactions on Industrial Electronics, 65*(5), 4279–4289.

Khan, S., Shakil, K. A., & Alam, M. (2016). Educational intelligence: Applying cloud-based big data analytics to the Indian education sector. In *2nd international conference on contemporary computing and informatics (IC3I)*.

Khan, S., Shakil, K. A., Ali, S. A., & Alam, M. (2018). On designing a generic framework for big data-as-a-service. In: *IEEE international conference on advanced research in engineering sciences*.

Khan, S., Shakil, K. A., & Alam, M. (2019a). PABED – A tool for big education data analysis. In *20th IEEE international conference on industrial technology*.

Khan, S., Liu, X., Ara Shakil, K., & Alam, M. (2019b). Big data technology – Enabled analytical solution for quality assessment of higher education systems. *International Journal of Advanced Computer Science and Applications (IJACSA), 10*(6). ESCI/Scopus.

Khan, S., Arshad Ali, S., Hasan, N., Ara Shakil, K., & Alam, M. (2019c). Big data scientific workflows in the cloud: Challenges and future prospects. *Cloud Computing for Geospatial Big Data Analytics*, 1–28.

Khan, S., Shakil, K. A., Alam M. (2019d). Big data computing using cloud-based technologies: Challenges and future perspectives. *Networks of the Future: Architectures, Technologies and Implementations*.

Kim, W., Park, J., Yoo, J., Kim, H., & Park, C. (2013). Target localization using ensemble support vector regression in wireless sensor networks. *IEEE Transactions on Cybernetics, 43*(4), 1189–1198.

Kotha, H., & Gupta, V. (2018). IoT application – A survey. *International Journal of Engineering & Technology, 7*, 891–896.

Kumar, A. (2018). *A hybrid fuzzy system based cooperative scalable and secured localization scheme for wireless sensor networks*.. International Journal of Wireless & Mobile Networks (Vol. 10, pp. 51–68).

Kumar, T., & Krishna, P. (2018). Power modelling of sensors for IoT using reinforcement learning. *International Journal of Advanced Intelligence Paradigms, 10*(1–2), 3.

Kumari, A., Abbasi, M. Y., Kumar, V., & Alam, M. (2018). The cryptanalysis of a secure authentication scheme based on elliptic curve cryptography for IOT and cloud servers. In *IEEE International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*.

Li, Y., & Parker, L. (2014). Nearest neighbor imputation using spatial–temporal correlations in wireless sensor networks. *Information Fusion, 15*, 64–79.

Liu, S., Feng, L., Wu, J., Hou, G., & Han, G. (2017). Concept drift detection for data stream learning based on angle optimized global embedding and principal component analysis in sensor networks. *Computers and Electrical Engineering, 58*, 327–336.

Malhotra, S., Doja, M. N., Alam, B., & Alam, M. (2018). Generalized query processing mechanism in cloud database management system. In *Big data analytics* (pp. 641–648). Singapore: Springer.

Mamdouh, M., Elrukhsi, M., & Khattab, A. (2018). Securing the Internet of Things and wireless sensor networks via machine learning: A survey. In *IEEE International Conference on Computer and Applications (ICCA)*.

Mehmood, A., Lv, Z., Lloret, J., & Umar, M. (2017). ELDC: An artificial neural network based energy-efficient and robust routing scheme for pollution monitoring in WSNs. *IEEE*

Transactions on Emerging Topics in Computing, 1–1. https://ieeexplore.ieee.org/abstract/document/7859382/citations#citations

Miljković, D. (2017). Brief review of self-organizing maps. In *IEEE international convention on information and communication technology, electronics and microelectronics (MIPRO)*.

Mottaghinia, Z., & Ghaffari, A. (2018). Fuzzy logic based distance and energy-aware routing protocol in delay-tolerant mobile sensor networks. 100(3): 957–976.

Navani, D., Jain, S., & Nehra, M. (2017). The Internet of Things (IoT): A study of architectural elements. In *13th international conference on Signal-Image Technology & Internet-Based Systems (SITIS)*.

Nayak, P., & Devulapalli, A. (2016). A fuzzy logic-based clustering algorithm for WSN to extend the network lifetime. *IEEE Sensors Journal, 16*(1), 137–144.

Noshad, Z., Javaid, N., Saba, T., Wadud, Z., Saleem, M., Alzahrani, M., & Sheta, O. (2019). Fault detection in wireless sensor networks through the random forest classifier. *Sensors, 19*(7), 1568.

Pajouh, H., Javidan, R., Khayami, R., Dehghantanha, A., & Choo, R. (2019). A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks. *IEEE Transactions on Emerging Topics in Computing, 7*(2), 314–323.

Phoemphon, S., So-In, C., & Niyato, D. (2018). A hybrid model using fuzzy logic and an extreme learning machine with vector particle swarm optimization for wireless sensor network localization. *Applied Soft Computing, 65*, 101–120.

Pinto, A., Montez, C., Araújo, G., Vasques, F., & Portugal, P. (2014). An approach to implement data fusion techniques in wireless sensor networks using genetic machine learning algorithms. *Information Fusion, 17*, 90–101.

Sam, S. (2016). Internet of Things' connected devices to triple by 2021, reaching over 46 billion units. Juniper Research.

Sethi, P., & Sarangi, S. (2017). Internet of Things: Architectures, protocols, and applications. *Journal of Electrical and Computer Engineering, 1*, 1–25.

Shakil, K. A., Zareen, F. J., Alam, M., & Jabin, S. (2017). BAM health cloud: A biometric authentication and data management system for healthcare data in cloud. *Journal of King Saud University – Computer and Information Sciences* (in press). https://www.sciencedirect.com/science/article/pii/S1319157817301143

Soni, S., & Shrivastava, M. (2018). Novel learning algorithms for efficient mobile sink data collection using reinforcement learning in wireless sensor network. *Wireless Communications and Mobile Computing*, 2018:7560167, 13 pages.

Sun, B., Guo, Y., Li, N., & Fang, D. (2017). Multiple target counting and localization using variational Bayesian EM algorithm in wireless sensor networks. *IEEE Transactions on Communications, 65*(7), 2985–2998.

Sun, Y., Zhang, X., & Wang, X. (2018). Device-free wireless localization using artificial neural networks in wireless sensor networks. *Wireless Communications and Mobile Computing*, *2018*, 4201367, 8 pages.

Thamilarasu, G., & Chawla, S. (2019). Towards deep-learning-driven intrusion detection for the internet of things. *Sensors, 19*(9), 1977.

Thangaramya, K., Kulothungan, K., Logambigai, R., Selvi, M., Ganapathy, S., & Kannan, A. (2019). Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT. *Computer Networks, 151*, 211–223.

Umarikar, A. (2003). *Fuzzy logic and brief overview of its applications*. University Västerås Suecia.

Van der Meulen, R. (2017). Gartner says 8.4 billion connected things will be in use in 2017, up 31 percent from 2016. Garther Research.

Varsha, S., Shubha, P., & Avanish, T. (2017). Intrusion detection using data mining with correlation. In *2nd international conference for Convergence in Technology (I2CT)*.

Vashi, S., Ram, J., Modi, J., Verma, S., & Prakash C. (2017). Internet of Things (IoT): A vision, architectural elements, and security issues. In *IEEE international conference on IoT in Social, Mobile, Analytics and Cloud (I-SMAC)*.

Wang, Z., Liu, H., Xu, S., Bu, X., & An, J. (2017). Bayesian device-free localization and tracking in a binary RF sensor network. *Sensors, 17*(5), 1–21.

Wang, J., Cao, J., Sherratt, R., & Park, J. (2018). An improved ant colony optimization-based approach with mobile sink for wireless sensor networks. *The Journal of Supercomputing, 74*, 6633–6645.

Wang, J., Gao, Y., Liu, W., Sangaiah, A., & Kim, H. (2019). An improved routing schema with special clustering using PSO algorithm for heterogeneous wireless sensor network. *Sensors, 19*(3), 671.

Warriach, E., & Tei, K. (2017). A comparative analysis of machine learning algorithms for faults detection in wireless sensor networks. *International Journal of Sensor Networks, 24*(1), 1–13.

Williams, R., McMahon, E., Samtani, S., Patton, M., & Chen, H. (2017). Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach. In *IEEE international conference on Intelligence and Security Informatics (ISI)*.

Yadav, A., Kumar, S., & Vijendra, S. (2018). Network life time analysis of WSNs using particle swarm optimization. *Elsevier, 132*, 805–815.

Yu, Z., & Tsai, J. (2008). A framework of machine learning based intrusion detection for wireless sensor networks. In *IEEE international conference on sensor networks, ubiquitous, and trustworthy computing*.

Zhang, B., Wu, W., Bi1, X., & Wang, Y. (2019). A task scheduling algorithm based on Q-learning for WSNs. *The Abel Prize*, 521–530.

Zidi, S., Moulahi, T., & Alaya, B. (2018). Fault detection in wireless sensor networks through SVM classifier. *IEEE Sensors Journal, 18*(1), 340–347.

Chapter 7
Supervising Data Transmission Services Using Secure Cloud Based Validation and Admittance Control Mechanism

Kamta Nath Mishra

Abstract In the recent era cloud computing is being extensively used for numerous services. Since, adoption has security concerns. Therefore, this research work presents attestation innards to evaluate the metamorphosis utility of mobile and electronic health data transmission through cloud network and it better comprehends the idea of infiltration trialing and susceptibility assessment. The proposed approach of this research work contains information on common threats to cloud based mobile health services and their corresponding solutions. The idea of this research work is to utilize Internet Communication Technology (ICT), Internet of Things (IoT) and Embedded Computing Technology (ECT) to enhance the performance of secure cloud (SecC) based m-health data transmission services. In this research work the author has explored a new and secure cloud based service which can upgrade the concert of cloud based m-health transmission systems. Here, an advanced internet communication machinery (ICM) based on IP-WSN (Internet Protocol-Wireless Sensor Network), scattered scheme architectures, web-computing, wisdom and motivation is used for enhancing the performance of cloud based m-health data communication systems. The cloud server of proposed m-health system will also provide access and control mechanism for multiple types of vehicles on roads and hence the proposed system will be helpful in enhancing the safety of passengers while they are travelling from their houses to the e-health hospitals. The services and safety of cloud based m-health data transmission services can be optimized in real-time situations.

Keywords Cloud computing · e-health · Embedded computing technology · Internet communication technology · m-health data transmission services · Secure cloud

K. N. Mishra (✉)
Department of Computer Science & Engineering, Birla Institute of Technology, Ranchi, Jharkhand, India

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_7

7.1 Introduction

The web Computing is a web dependent latest computing system which is allocating facilities in a favor of clients e.g. platform computing infrastructure, sharing network resources, and software products. The Cloud benefit actualize in this dynamic market fragment are: Amazon, Microsoft, Google, IBM, Oracle, Eucalyptus, VMware, Eucalyptus, Citrix, Sales power and rack space just as there are a wide range of trader offering distinctive cloud administrations (Albeshri and Caelli 2010). With the enormous increase of cloud and web crime based services, the terms of suitable web system defense system has become essential in order to look after integrity, confidentiality, and accessibility of transportation facilities.

The necessities of real time transmission in the pulling strategy and bring into play of ongoing systems administration aptitude for all customers winds up imperative to keep up adaptability and Quality of Service (QoS) in web systems. If we need to provide user friendly accessibility, reliability and secrecy of essential data positioned on a web computing network, a variety of safekeeping measures will be needed. If the cloud wants to retain a stable and secure web network, the web server requires all the essential measures to be implemented, the faithful access privileges have to be implemented and outer boundaries are to be appropriately defined (Sedigh et al. 2014; Alger 2005).

Many researchers, industry experts and academicians have tried to define the term web computing and its characteristics. The researchers Buyya et al. (2008) and Khodadadi et al. (2015) have defined it as the cloud is a collection of interconnected virtualized dynamically provisioned computers which provide parallel and distributed computing environment and it presents one or more unified computing resources established through negotiation between the service provider and consumers. Van Bon et al. (2007) described that clouds are a large pool of easily usable/accessible virtualized resources which are dynamically reconfigured to adjust to a variable load (scale) and it optimizes resource utilization. The pool of resources in cloud computing environment is shared according to pay-per-use model. Here, guarantees are offered by the infrastructure provider as per the service level agreements. Miller (2008) claimed that clouds are hardware based services where computation, network and storage capacity are offered with highly elastic infrastructure capacity.

A report from the University of California says that the key characteristics of cloud computing are infinite computing resources, up-front commitment elimination and pay per use. Similarly, the researcher Alger D. (2005) said that cloud is more often used to refer as the information technology infrastructure deployed on an IaaS data center. Here, a resource means compute application, system assets, platform, software services, virtual servers and compute infrastructure. Web Computing is being widely used in many industries. The Cloud computing has a lot of usage in many areas like accounting applications, customer relationship management, communications and collaboration, electronic mails and shared calendars,

financial management, office productivity suits, online storage management, human resource and employment etc. The cloud computing has various advantage like 24/7 support, reimburse as much as you use, scalability, high level computing, virtualized and self-motivated atmosphere (Mell and Grance 2009; Khalid et al. 2013).

The services and safety of cloud based transmission system can be optimized in real-time situations. The SeC with ICT can take an interest a vital role to set up link among different servers of the clouds and end users to improve accident preclusion. When in doubt, the assurance is a joint trustworthiness of the web customer and web server as the records well being and secrecy issue trick genuine trepidation (Plummer et al. 2009; Singh et al. 2015a). To stay away from these critical issues, the creator's present a legitimate and idiot proof confirmation strategy to inspect the execution of pulling administrations (Singh et al. 2015b). The explanation in web compute merges amenity safety, amenity supervision, and observes of resources. In the current era no standard rules and regulations are existing for deploying applications in cloud based systems. Further, there is a serious be deficient in consistency power in the web environment. Various new processes have been planned and imposed in web. But, these presented techniques are not enough to ensure total security because of the dynamics of web environment. The intrinsic issues of data safety, management, supremacy and control of cloud data are discuss in (Mahmood 2011). Sun et al. (2011) described the key protection, isolation, and dependence issues in the accessible environment of cloud computing and provided help to the users to identify the substantial and insubstantial fear related to cloud computing. As per the author's opinion, there are three core possible terrorization namely safety, isolation and faith in cloud computing, here, safety plays a decisive role in the existing era of cloud and distributed computing. The cloud security can further be categorized into four subcategories namely safety mechanism, data confidentiality, web server monitoring, and preventing illegal operations & service hijacks.

A records safety structure for web computing networks was anticipated by Pandey et al. (2013). Here, the researchers mostly discuss the protection concerns linked to the storage of cloud data. Various patent concerning the security of statistics techniques for cloud and distributed systems were filed by (Klein 2013). Younis and Kifayat provided a analysis on web security supervision for critical infrastructures (Younis and Kifayat 2013). A security and isolation structure for radio frequency identification (RFID) in web computing environment was projected by Kardaş et al. (2013) which efficiently integrates RFID technology with internet of things (IoT) using web computing environment.

In a nutshell, it very well may be said that the main issues of web data insurance comprise of records security, records openness, data assurance, and safe data correspondence. The fundamental security challenges in distributed computing condition incorporate danger location, recuperation of information misfortune, benefit disturbance aversion, discovery and avoidance of pernicious assaults (Behl 2011). The scientists Chen and Zhao (2012) investigated information security and protection issues in the cloud and conveyed processing condition by concentrating on

protection insurance, cloud security and information isolation. Subsequently, it tends to be said that the information security issues are principally at SaaS, PaaS, and IaaS levels. Further, the most extreme test in distributed computing is information sharing. The association of information security and protection issues in distributed computing condition is exhibited in Fig. 7.1.

In this research work the author has explored a new and secure cloud based service which can upgrade the concert of cloud based transmission systems. Here, advanced internet communication machinery (ICM) based on IP-WSN (Internet Protocol-Wireless Sensor Network), dispersed framework structures, distributed computing, detecting and activating is utilized for upgrading the execution of cloud based information correspondence frameworks. The cloud server of proposed system will also provide access and control mechanism for multiple types of vehicles on roads and hence the proposed system will be helpful in enhancing the safety of passengers. The remaining parts of this research work are organized as follows. The Sect. 7.2 describes the objectives and challenges of cloud based research. The area 7.3 shows a short discourse about distributed computing condition and its security worries for transportation framework. This area likewise depicts a safe cloud based transportation administrations. The segment 7.4 presents secure cloud test-bed setup model and shows of proposed design are assessed in this segment. At long last, the creator has finished up the substance of this exploration work in area 7.5.

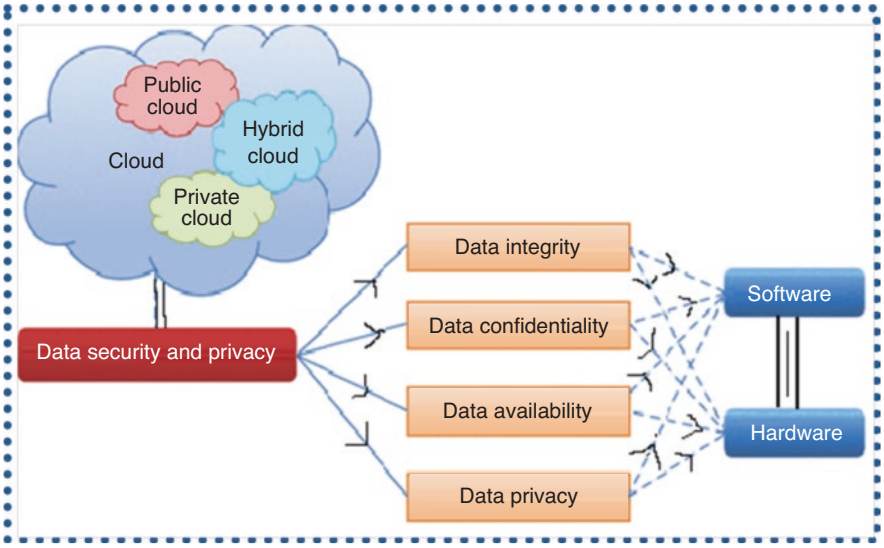


Fig. 7.1 Association of information security and protection issues in distributed computing condition

7.2 Objectives and Challenges of Cloud Based Data Transmission Research

However, virtualization and web computing provide a wide variety of active resources. The problem of protection is professed specifically as the big problem on the web, which causes users to oppose utilizing Distributed computing advancement. Security is the rule worry of the cloud; cloud master focuses and clients facing huge security issues.

7.2.1 Objectives

The fundamental target of this examination is to comprehend security dangers and recognize the suitable security systems used to moderate them in Cloud Computing administrations, to comprehend cloud security issues and strategies utilized in the present Cloud world. Distinguishing security in the difficulties of the cloud, it is normal that later on of distributed computing it will recommend measures to counter the future difficulties that distributed computing administrations confront. As we probably are aware, in an open cloud framework we have a foundation underlined with numerous virtual machines. A few associations utilize virtual machines to get to their secret information.

7.2.2 Challenges

The cloud computing environment addresses the challenges of next generation cloud computing architectures. It also addresses the challenges of permitting application platforms and development platforms to take advantage & reimbursement of web computing. The examined on web computing is tranquil in the beginning period. Many presented issue have yet not been address whereas the new challenge are emerging on daily basis. Several of these challenges are: Service Level Agreements (SLA's), Web Data Management & Security, Data Encoding, and Relocation of virtual Machines and Server Consolidation (Wijaya 2011; Handley and Rescorla 2006).

Further, this world needs to find the answer of following questions which are related to cloud based m-health data transmission and security (Hogan et al. 2011; Almulla and Chon 2010; Tan et al. 2011):

- What are the different security systems which are being utilized by the main cloud specialist co-ops when the information is being transmitted among the mists and neighborhood m-health systems?

- What is the variety of safety technique being used to stop unlawful entrance of m-health data within the web?
- What are the key safety issue and challenge which the world is expecting in future about m-health data transmission in cloud computing environment?
- How the world can tackle these safety troubles which are predictable to arise in potential web processor systems for m-health data transmission?

7.3 Access Control Mechanisms of Data Transmission Using Cloud Services

The access Control is a control access list is prepared in-order to specify and control who can access & what can be accessed. As Cloud computing is used by multiple users and multiple enterprises and heterogeneous infrastructure, so new cloud safety concerns arrive which are Multi-tenancy, Velocity of Attack, Information Assurance and Data Privacy and Ownership.

To make the cloud infrastructure secure, the users need to use various cloud safety mechanism. In a virtual environment, the computer, network and storage are virtualized so, to maintain safety. The Fig. 7.2 shows cloud safety method which is applicable for all cloud based m-health communication systems (http://searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting; Ahmed et al. 2013; Hogan et al. 2011).

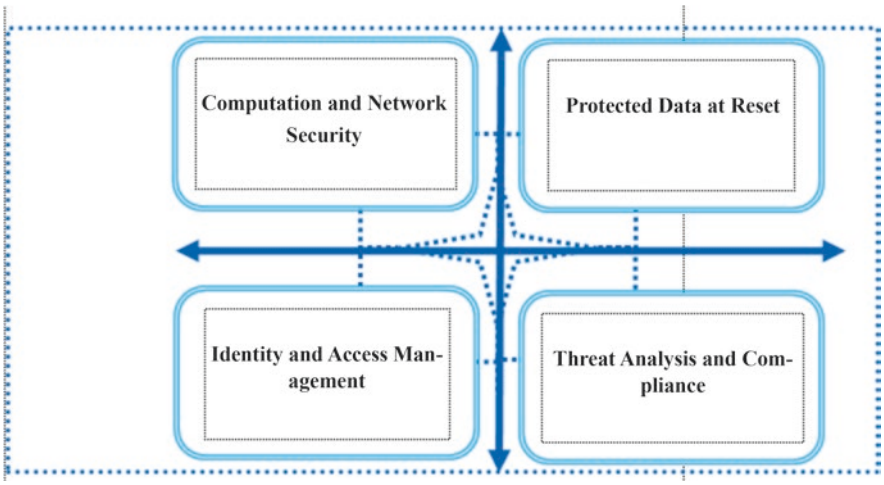


Fig. 7.2 The cloud safety method

7.3.1 Securing Virtual Machines

The virtual machines (VMs) can be secured by hardening the virtual machines. There can be one more component which can be the point of attack is Hypervisor Management System. This software will manage the hypervisor. Securing virtual machines (VMs) may further include virtual machine (VM) isolation and VM hardening. If one virtual machine has been attacked and compromised in the cloud infrastructure then that VM need to be isolated from the rest of the VM's to make sure that this attacker does not get control over the rest of the virtual machine or the infrastructure. Hardening is the method of shifting the evasion arrangement in organizes to accomplish superior safety. By limiting the resource that VM can consume to prevent denial of services attacks, disable unused functions and devices on virtual machine, use a directory service for authentication; perform vulnerability scanning and penetration testing of the guest operating system secures virtual machine (Albeshri and Caelli 2010; Ahuja 2011; Bellare et al. 2001, 2002).

The operating system needs to be updated very regularly and the safety software's are up to date. The applications also need to be updated regularly so that they are secure. The identity management is one more concern as public cloud infrastructure has multiple user belonging to multiple organizations and ensuring authorization that the user is who the user claims to be so by adding multiple layers of safety like multifactor authentication and biometric authentication, can make sure that only authorize users can login to our system (Alger 2005; http://cloudcomputing.sys-con.com/node/612375/print).

7.4 Governance and Operations in Cloud Computing Environment

The domination refers to the policy, process, law and institution that describe the configuration by which company are intended for and manage. Each organization will have its safety policies which will have a different set of policies at its information technology level so making sure that these policies are enforced correctly on a cloud infrastructure is also important. There are also external regulations like banking sector has its own set of laws making sure that the confidential data of the user is not compromised, healthcare industry has its own set of laws. All these government regulations have to be followed by the company else the company can be prosecuted. Internal and external regulations are also followed. In case of a traditional data centre, the IT department of that company will take care of it. In case of cloud, the cloud service provider along with the organization's IT department has to ensure that the organizations policies are also applied in cloud environment (Alger 2005).

Now, in these days web computing process can challenge several conformity examination necessities at present in place. Statistics location; web computing

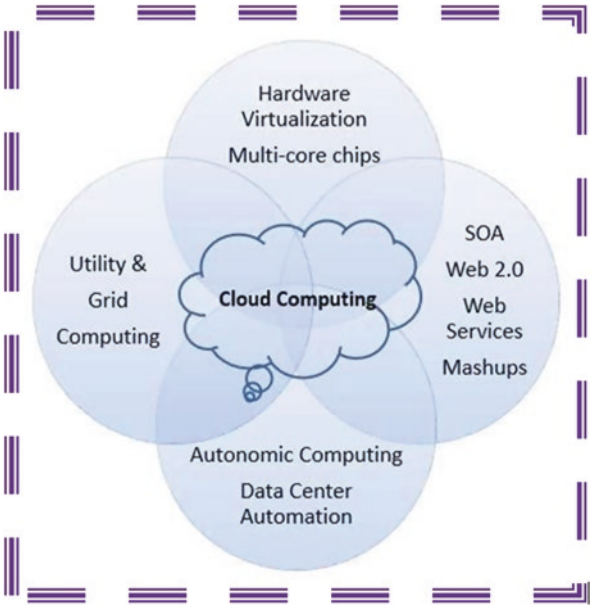


Fig. 7.3 The overview of governance and operations on m-heath in cloud networks

safety guidelines lucidity; and IAM, are all tough issues in agreement audit efforts. The example of the agreement requirements include confidentiality and law; Payment Card Industry (PCI) necessities; and monetary coverage laws. It is a fear of company about the resiliency of web computing, since statistics may be commingled and scattered roughly different servers and biological region (Alani 2010; Whiting et al. 2002).

It may be achievable that the statistics for a precise certain point cannot be recognized. Distinct recent swarm, the venture know accurately where the position is of their statistics, to be fast retrieve in the event of failure healing. In the web computing representations, the principal Cloud examination supplier might farm out capability to third parties, who might too farm out the healing process. This will become more difficult when the primary Cloud service provider does not ultimately hold the data. The Figs. 7.3 and 7.4 show the overview of cloud safety and cloud security (SeC) framework of cloud based network systems (Whiting et al. 2002; Chadwick and Fatema 2012; Saldhana et al. 2014).

7.5 Security Issues for Cloud Servers and Transmission Systems

Web processing is generally utilized in different ventures and is encountering noteworthy development in around humankind. The important peculiarity of web processing is to a great extent access to the framework; in requires self-benefit, quick

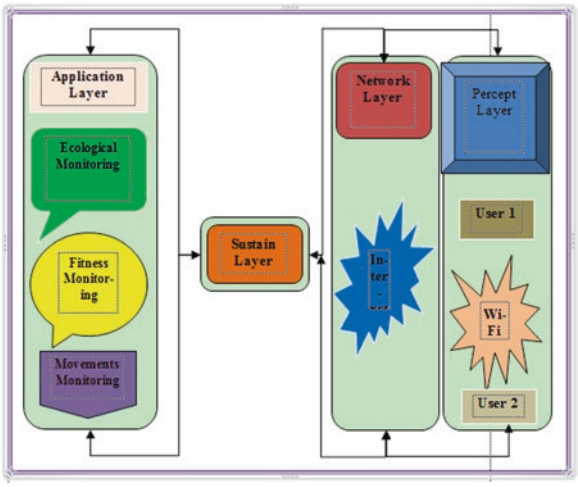


Fig. 7.4 The SecC framework for m-health data transmission in cloud networks

adaptability, reservation booking and exhaustive examination. Passage to the immense framework is the contact of a few properties facilitated in money organizes from a wide scope of areas and offers online access.

On-request self-benefit is the availability of administrations and assets from cloud specialist organizations when required. Speedy flexibility gives adaptable administrations dependent on the necessities of the provider. The gathering of assets serves clients and clients through versatile and impermanent administrations. The deliberate administration directs the administrations given by the providers to the purchaser, which incorporate the receipt and adequate utilization of assets.

The key three building squares which are usually utilized administration models in distributed computing condition are: Software as A Service (SaaS), Platform as A Service (PaaS), and Infrastructure as A Service (IaaS). Here, SaaS will give the product and applications according to the requests over the web. In this way, the expense of programming, upkeep and activities will be limited.

The PaaS will give the stage on interest all through the web for creating programming items utilizing instruments/libraries from the specialist organization. The PaaS will likewise bolster programming organization and arrangement settings. The IaaS will give the framework on interest all through web for data/information preparing, stockpiling and system assets. The association of arrangement model and basic qualities with crucial building squares of distributed computing condition is exhibited in Fig. 7.5 (Whiting et al. 2002; NIST Publication 2001).

As cloud is increasing greater fame, an ever increasing number of associations need to move towards cloud yet the key worry about moving towards cloud has been security. Today security is required in every one of the organization models. As per NIST, the cloud display is made out of four noteworthy organization models to be specific Public, Private, Community and Hybrid mists. The general population cloud foundation is free for open use by the overall population of web. The private cloud framework is saved for the advantaged utilization of an association comprising

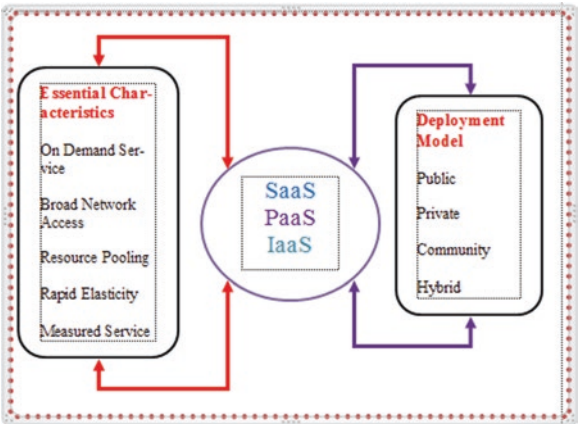


Fig. 7.5 Cloud computing building blocks internaction with other components for m-health data and videos/images transmission

of numerous customers. The people group foundation in the cloud is gotten for an advantaged use by a particular network of buyers who have shared interests, for instance. Mission, governmental issues, and so forth. The mixture cloud foundation is an association of at least two diverse cloud frameworks that have a novel presence, however are connected by an institutionalized innovation that gives the convenience of information and applications (Caballero et al. 2007; Black and Rogaway 2000; Rogaway and Black 2002).

7.5.1 Security Concerns in Data/Video Transmission Through Cloud Server

Most cloud users are unaware of the risks involved in storing and transmitting private information in a shared environment. Therefore, the main technological constraints such as transparency, multiple ownership, attack speed, information security, privacy and data ownership, compliance, cryptography and integrity must be addressed carefully. Therefore, customers are not completely safe or immune from Internet threats and this requires an appropriate secure cloud mechanism and periodic reviews to manage current technologies. To reach the highest level of secure cloud server, it is important that every client (controller) in the cloud network is secure and aware. IETF defines the denial of service attack (DoS) (Singh et al. 2015b) in which one or more machines attack a victim and try to prevent the victim from doing useful work. In general, DoS attacks can be detected by analyzing the characteristics of the victim's network. The most effective defenses against DoS and DDoS attacks must filter routers, disable IP transmissions, apply security patches and disable unused services that perform intrusion detection tasks (Robert et al. 2011; Johnson 1999; Masson and Loftus 2003).

Figure 7.6 presents four key key processes for each customer to identify and test individually in the cloud server, and these key processes are: Induction, Research,

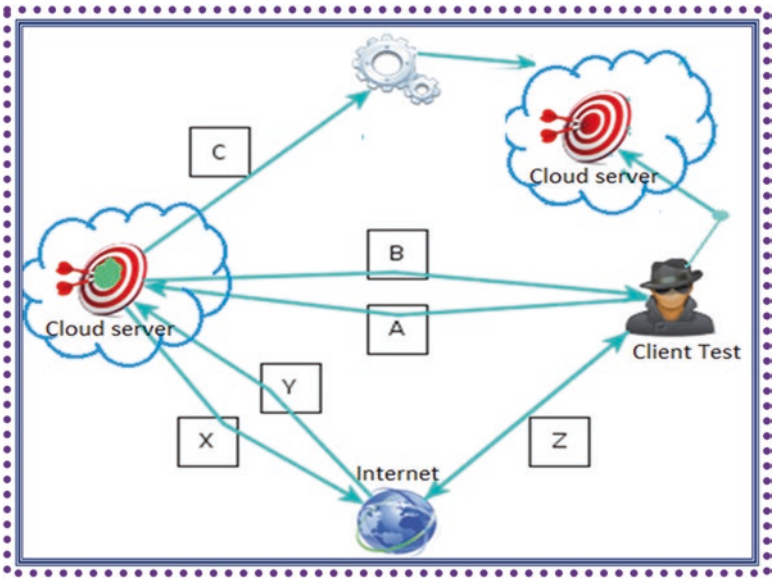


Fig. 7.6 Interaction mechanism of 4PP for transferring client's/patient's data in cloud computing environment

Interaction, and Intervention. Induction is the process of understanding the objective by analyzing the environment in which it is located. It is because the reliability of the objectives in their surrounding environment. The induction process is represented by the variable "Z" in Fig. 7.6. The search concept marked as an identifier ("C") can simply be explained as the search process of the objective foundation. In this process, the objective is analyzed to detect any emanation or any identifier of these emanations. Identified interaction identifier ('A' and 'B'), these interactions are simply answers to questions or agitations initiated by the analyst. From examples of such interactions, ICMP responds and tracks course operations. Finally, the intervention is the process of the analyst who imitates some resources and services that the objective requires for the operation. This process helps to identify the extreme levels in which the target could still operate and is shown by the variables "X", "Y" and "Z" in Fig. 7.6. Multiple ownership is an important security problem for cloud networks. Here, surface attacks have increased due to the co-location of several virtual machines for a single server.

7.5.2 Transportation System Requirements

Today the economy of each country is growing at a tremendous rate. People in all parts of the world have cars to travel. Some buy it as a status symbol, while others buy it as a necessity. We often observe the growing overflow of cars on every road

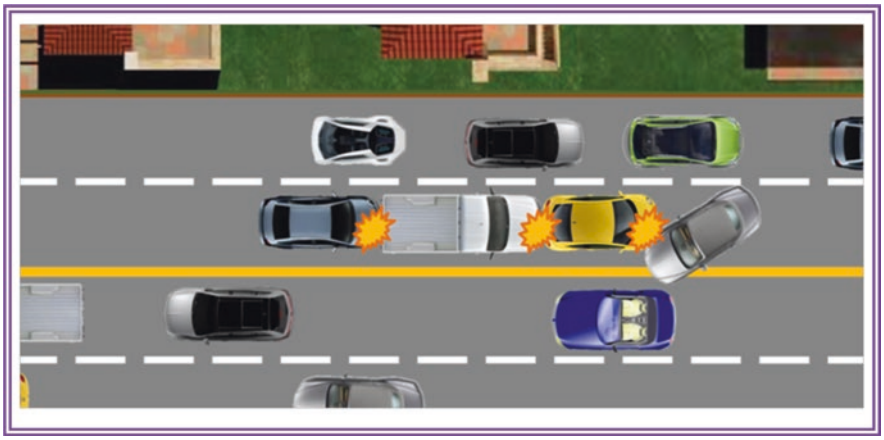


Fig. 7.7 Current transportation system

in developed countries. On the other hand, the car accidents are increasing every day and many people of this earth are forced to leave this earth permanently within fractions of seconds after the occurrence of accident. The Fig. 7.7 shows a road accident which has occurred in the current transportation system.

To limit auto collisions, a confirmation instrument for the vehicle framework is introduced in the cloud, displayed in Fig. 7.8. In the vehicle scope of the proposition it is said that the utilization of the Wi-Fi/Bluetooth module associated by means of their individual interfaces to the coordinated processor can transmit pictures and information to the equipped specialists inside the predetermined time and, in this manner, the lives of numerous individuals caught in episodes can be spared. The proposed consistent cloud topology (SeC) of Fig. 7.8 will be introduced inside every vehicle. In this way, the association among vehicles and other traffic control offices will be moved forward. This enhanced and enhanced correspondence and control framework dependent on distributed computing will be extremely valuable to avoid vehicle mishaps on streets and motorways.

7.5.3 Secure Cloud Test Setup Model

The setup model of the SeC test to test the cloud-based correspondence framework is displayed in Fig. 7.8. Here, the customer server consistent topology is executed in the test seat. The test setup display organize is intended to interface and coordinate with basic corporate norms. Utilize a various leveled approach that utilizes excess, versatility, and key usefulness dependent on connection total. In the test setup model of Fig. 7.8 there are two associations between the Core and every appropriation switch. All in all, virtual neighborhoods virtual local area networks (VLANs) are utilized in the WAN of the proposed server-based correspondence display in the

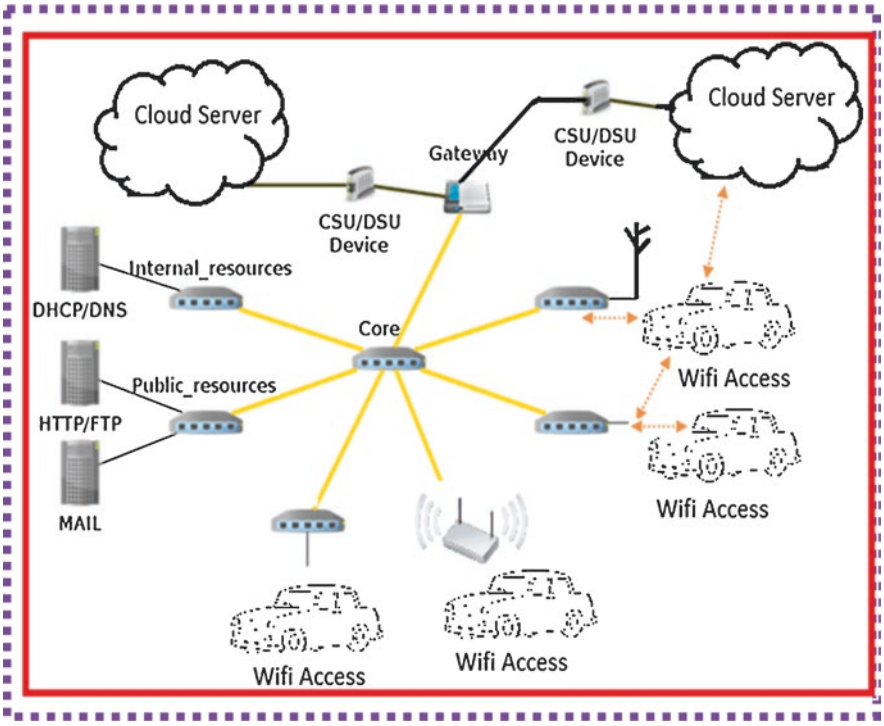


Fig. 7.8 The SecC based logical topology for taking patients to e-health hospitals

cloud. The execution of VLANs in the proposed correspondence show altogether expands time productivity and helps the system head in charge of arranging remote gadgets through Telnet sessions (Shakil et al. 2015; Khan et al. 2017a). To encourage the way toward arranging the VLAN and to bring together this movement, the virtual transport convention (VTP) was utilized halfway as a server and as a customer in whatever is left of the gadgets in the system.

In this way, the VLANs are designed in the focal switch and the VTP server running in the part sends intermittent updates over the system to guarantee that every gadget has bare essential information on the setup of the VLAN. These updates contain an amendment number, so when they land at the customer, these modification numbers can be analyzed and the customer will refresh the data of its VLAN database dependent on that procedure. The two associations between the system center and every conveyance switch are designed as connections to have VLAN traffic. Here, every association underpins the local VLAN to permit the vehicle of label less VLAN traffic over the system, between various sections (Miller 2008; Singh et al. 2015b; Caballero et al. 2007).

The creator has set up two passageways to test the organization on two free dispersion level switches. System address interpretation (NAT) has been arranged to secure residential areas to guarantee that it can't be gotten to through unprotected

transport conventions, for example, ICMP. NAT has been designed to enable certain delivers to be unmistakable to the outside world (e.g. Web and record server). All together for the switch to perform steering between VLANs, the EIGRP (Enhanced Internal Gateway Routing Protocol) is favored in this inquiry report. The connection and trade of data between various clients/vehicles of the proposed cloud-based correspondence framework is exhibited in Fig. 7.9.

The bearers are the principle correspondence joins for clients with the specialist co-op's cloud. These vectors have been appeared in Fig. 7.9. Essentially, every one of these vectors can be associated with a different test situation. This enables better outcomes to be accomplished because of its compartmentalized structure, with the goal that the presence of an excessive number of changes can be kept away from. The past advances were taken to finish the data gathering and the test arranging stage. Nonetheless, the checking procedure was not performed independently for every bearer. This examining and list process produces general data on noticeable advancements and transport administrations (Shakil et al. 2017; Khan et al. 2017b). The cloud vector correspondence arrangement of Figs. 7.8 and 7.9 utilize computerized signals for a wide range of correspondence. Regardless, on the off chance that one of the clients utilizes the simple flag, the relating simple signs are changed over

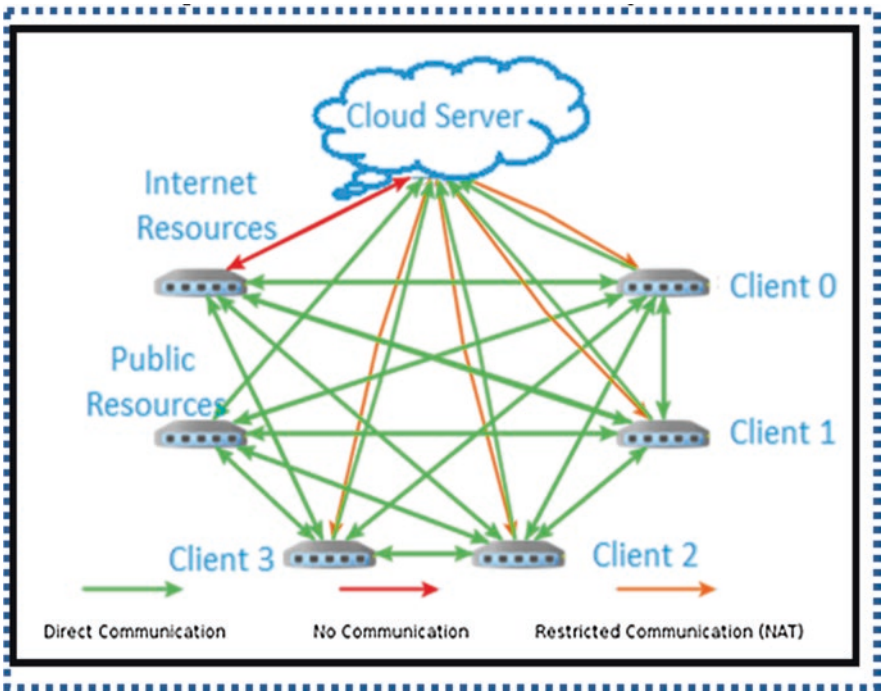


Fig. 7.9 Communication vectors necessity for cloud server based health service providers and patients interaction

into computerized signals utilizing a simple advanced converter before transmitting the signs (Ali and Alam 2016; Malhotra et al. 2017).

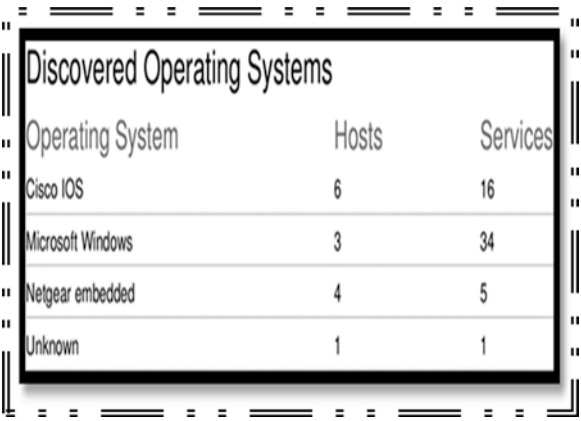
7.5.4 Performance Evaluation

The Metasploit is a valuable utilization and weakness testing tool which helps using dividing the saturation testing workflow into smaller and further manageable jobs. With the help of Metasploit the cloud computing researchers can control the power of the Metasploit framework. The Metasploit helps using automating the process of in depth utilization of cloud networks, and provides the required tools to perform manual testing of penetration test cases. The researchers can use Metasploit to scan the open ports and services of cloud computing networks; The Metasploit utilizes vulnerabilities, gathers evidences, and generates the detailed reports of test results.

The Metasploit Pro is a multi-user collaborative tool which helps us in the distribution of tasks and information with other group members of a diffusion testing group. In order to perform penetration testing using the team members can share the host's data, examine the composed evidences, and generate host notes to distribute awareness about any or particular target. The Metasploit was utilized as the fundamental data get-together and helplessness appraisal apparatus to all the more likely comprehend the hidden reasons for vulnerabilities in the executed proving ground. This segment shows the outcomes gathered from the Graphical User Interface (GUI) of Metasploit structure.

The outcomes assembled from Metasploit are as reports, yet these reports have excess data which won't all be utilized for assessment and investigation in this examination work. In any case, just the essential data, pertinent to this idea has been introduced in this examination work. The proposed system was tested in the self created test set-up where clients were allowed to use different types of operating systems for cloud communication. The outputs given by proposed system corresponding to clients, servers, and used operating systems are presented in Fig. 7.10 (Singh et al. 2015b; Caballero et al. 2007; Black and Rogaway 2000).

The CDP-Snarf is a cloud computing network sniffer tool which was exclusively written for digging out information from CDP packets. It is a Linux based bundle which is utilized for picking up data about the gadgets in the system and sniffing Cisco Discovery Packets (CDPs). The CDP-Snarf provides all types of information through a command "show cdp neighbors detail". This command can be executed on any Cisco router. The CDP-Snarf can be easily tested with internet protocol version 4 (IPV4) and IPV6. The information displayed for a cloud computing network using CDP-Snarf are: Time intervals between CDP advertisements, Source MAC address, CDP Version, Checksum, Device ID, Software version, Platform, Addresses, Port ID, Save packets in PCAP dump file format, Read packets from PCAP dump files, and Debugging information. The Fig. 7.11 is showing a screenshot where the proposed cloud based communication system is communicating with network gateway for providing interaction between different clients.



Discovered Operating Systems

Operating System	Hosts	Services
Cisco IOS	6	16
Microsoft Windows	3	34
Netgear embedded	4	5
Unknown	1	1

Fig. 7.10 OS fingerprints enumeration in the created test set-up

```
[#0] Sniffed CDP advertisement with a size of 359 bytes.
Source MAC address: D0:57:4C:51:84:01

CDP Version: 2
TTL: 180 ms
Checksum: 0x16A2

Device ID: gateway

Software version: Cisco IOS Software, 2800 Software (C280
rsion 12.4(15)T14, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Tue 17-Aug-10 09:00 by prod_rel_team

Platform: Cisco 2821

Addresses:
   Address #: 1
   Protocol type: [1] NLPID format
   Protocol: IP
   Address: 80.0.0.1


Port ID: GigabitEthernet0/1

Capabilities:
   [0x01]       Router
   [0x08]       Switch
   [0x20]       IGMP

VTP Management Domain:

Duplex: [0x01] Full
```

Fig. 7.11 The output obtained from CDPSnarf

The CGE.pl is a bundle of purl that works in a Linux situation. This bundle can possibly over-burden the ports on system gadgets and consequently thinks of them as unusable. Figure 7.12 demonstrates the achievement of the specialized adventures that have been performed in the cloud-based correspondence framework proposed utilizing the CGE.pl device (Singh et al. 2015b; Ahmed et al. 2013; Caballero et al. 2007). Zenmap is a ground-breaking examining apparatus utilized for checking and identifying systems. The Fern WiFi Cracker is a modified apparatus that

Fig. 7.12 Peak load testing of proposed cloud based e-health communication system using CGE.pl packet

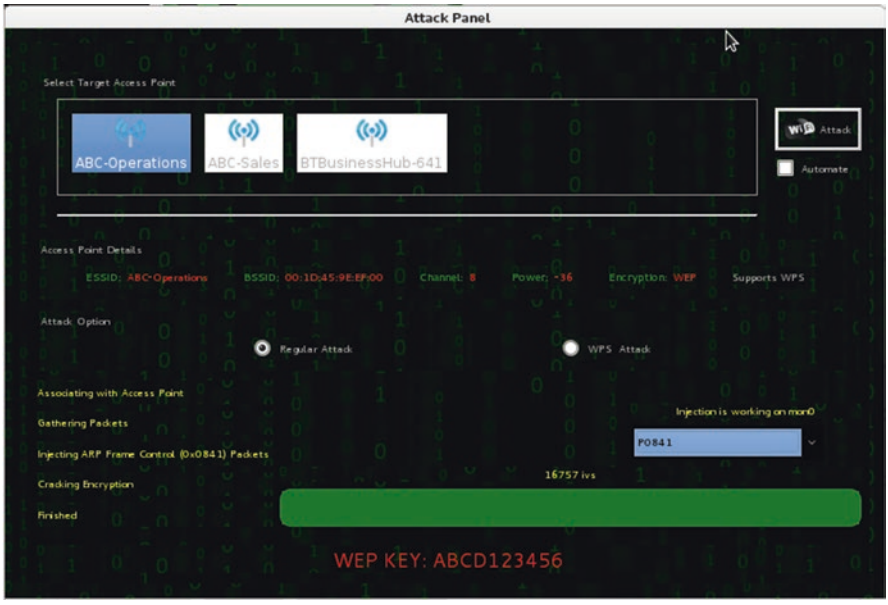


Fig. 7.13 Fern-WiFi-Cracker attack successfully handled in an e-health communication system

utilizes extra bundles to break passwords from remote passageways utilizing distinctive strategies, for example, lexicon documents. In Fig. 7.13 the creator demonstrated the catch of the trial leave screen in which the outside assaults on the

AP of a Wi-Fi based cloud correspondence framework were effectively overseen by the proposed framework.

According to the reports generated, the v2.0 population chains of the Simple Network Management Protocol (SNMP) are vulnerable to exploitation. Therefore, it can be easily broken if used in a cloud communication system. This issue isn't explicit to a piece of the system however to the whole system. In this manner, approaching the network channels utilized by the SNMP programming likewise implies approaching all and every one of the gadgets associated with the system, including the principle segment of the organization support. Subsequently, the capturing of the SNMP v2 session can have troublesome outcomes. Any accomplished robber can control arrange setups by getting to SNMP certifications and can cause DoS assaults. Thusly, data on the organization system can be acquired illicitly (Singh et al. 2015b; Black and Rogaway 2000; Rogaway and Black 2002; Robert et al. 2011).

Another imperative viewpoint to consider would be the development of CDPs into the system. Any abnormal state master/ruffian can undoubtedly decide the open ports and the different functionalities of the gadgets utilizing the data incorporated into these bundles. Programming forms of Cisco gadgets are likewise promoted on the CDP. In this manner, aggressors and thieves can search for adventures that are impressions of the system interconnect working framework (IOS). To counter this damage, the creator of this exploration recommends crippling CDP reports on all Cisco gadgets on the off chance that they don't take care of the issues. To keep up availability amid such assaults, the creator suggests utilizing directing conventions, for example, the fringe portal informing convention (BGMP) on the grounds that it can keep up numerous doors. Subsequently, availability will be kept up in the cloud-based correspondence framework regardless of whether one of the doors is blocked.

The Fern-Wifi-Cracker is an unsafe device, since it underpins multi-abuse systems and utilizations modernized word reference documents to split the passwords on remote APs. The Zenmap is an extremely solid data gathering instrument which can be utilized to assemble a gigantic amount of data about the objective system. The significant sweep utilizing Zenmap can distinguish open ports, working framework fingerprints and a partial topology chart. In any case, the Zenmap isn't a period talented apparatus for system testing. At last, the most grounded instrument for cutting a system is the Metasploit structure which produces reports for further assessment and investigation notwithstanding perform assaults. Accordingly, the similarity test can be allowed to enhance the comprehension of system status (Johnson 1999; Masson and Loftus 2003).

7.6 Conclusions

This exploration work plainly demonstrates that the development of innovation produces the requirement for cutting edge safety efforts that are affected by expanded vulnerabilities and complex assaults. On the positive side, the development of inno-

vation has a negative effect from an aggressor's perspective. As per the aggressor's perspective, the absence of top to bottom learning of the framework can be misused in the following procedure.

As a rule, the principal finish of this examination work is that arrange security should basically be finished with deceivability. Its significance is that if an individual can conceal their system assets from aggressor gatecrashers, the likelihood of system dangers will be incredibly decreased. This is because of the structure through which infiltration tests are performed. List is one of the underlying phases of every infiltration test. On the off chance that it must be isolated from the cycle, the accompanying advances will be out of date. There is dependably a harmony between security dangers and relating countermeasures, yet these measures by and large focus on recognizing and blocking dangers as opposed to concealing vital system assets from them. Accordingly, it very well may be said that cloud specialist organizations have less straightforwardness than others. Therefore, it can make clashes inside the corporate data the executives' framework.

References

Ahmed, I., James, A., & Singh, D. (2013). Critical analysis of counter mode with cipher block chain message authentication mode protocol—CCMP. *Security and Communication Networks, 7*(2), 293–308.

Ahuja, R. (2011). SLA based scheduler for cloud storage and computational services. *International Conference on Computational Science and Applications (ICCSA)*, pp. 258–262.

Alani, M. M. (2010). Testing randomness of block-ciphers using diehard test. *International Journal of Computer Science and Network Security, 10*(4), 53–57.

Albeshri, A., & Caelli, W. (2010). Mutual protection in a cloud computing environment. *12th IEEE international conference on High performance Computing and Communications (HPCC)*, pp. 641–646.

Alger, D. (2005, June). *Build the best data center facility for your business*. Indianapolis: Cisco Press Book.

Ali, S. A., & Alam, M., (2016). A relative study of task scheduling algorithms in cloud computing environment. In *Proceedings of the 2nd international conference on contemporary computing and informatics* (IC3I 2016), pp. 105–111.

Almulla, S., & Chon, Y.-Y. (2010). Cloud computing security management. *2nd international conference on engineering systems management and its applications*, pp. 1–7.

Behl, A. (2011). Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. In *Proceedings of the World Congress on Information and Communication Technologies* (WICT'11), pp. 1–5.

Bellare, M., Kilian, J., & Rogaway, P. (2001). The security of the cipher block chaining message authentication code. *Journal of Computer and System Sciences, 61*(3), 362–399.

Bellare, M., Kohno, T., & Namprempre, C. (2002). Authenticated encryption in SSH: Provably fixing the SSH binary packet protocol. In V. Altari, S. Jajodia, & R. Sandhu (Eds.), *Proceedings of 9th annual conference on Computer and Communications Security – CCS 2002*, held 18–22 November 2002 in Washington, USA (pp. 1–11). New York: ACM Publication.

Black, J., & Rogaway, P. (2000). A suggestion for handling arbitrary-length messages with the CBC-MAC. In M. Bellare (Ed.), *Proceedings of 20th annual international conference of advances in cryptology – CRYPTO 2000, Lecture notes in computer science 1880*, held 20–24 August 2000 in Santa Barbara, USA (pp. 197–215). Berlin: Springer.

Buyya, R., Yeo, C. S., & Venugopal, S. (2008). Market oriented Cloud Computing: Vision, hype, and reality for delivering IT services as computing utilities. In *Proceedings of the 10th IEEE international conference on High Performance Computing and Communications (HPCC 2008, IEEE CS Press, Los Alamitos, CA, USA)*, Dalian, China, September 25–27, pp. 1–9.

Caballero, J., Yin, H., Liang, Z., & Song, D. (2007). Polyglot: Automatic extraction of protocol message format using dynamic binary analysis. In P. Ning (Ed.), *Proceedings of the 14th ACM conference on Computer and Communications Security – CCS 2007,* held 28–31 October 2007 in Whistler, Canada (pp. 317–329). New York: ACM Publication.

Chadwick, D. W., & Fatema, K. (2012). A privacy preserving authorization system for the Cloud. *Journal of Computer and System Sciences, 78*(5), 1359–1373.

Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. In *Proceeding of the International Conference on Computer Science and Electronics Engineering* (ICCSEE'12), pp. 1–5.

Handley, M., & Rescorla, E. (2006). Internet denial-of-service considerations. In *Internet engineering task force* (Technical report, pp. 1–38).

Hogan, M., Liu, F., Sokol, A., & Tong, J. (2011). *NIST cloud computing standards roadmap – Version 1.0* (National Institute of Standard Technology Special Publication, 500-291, pp. 1–63).

http://cloudcomputing.sys-con.com/node/612375/print. Accessed on May 5 2016.

http://searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting. Last Accessed On: May 5, 2017.

Johnson, D. H. (1999). The Insignificance of Statistical Significance Testing. *The Journal of Wildlife Management, 63*(3), 763–772.

Kardaş, S., Çelik, S., Bingöl, M. A., & Levi, A. (2013). A new security and privacy framework for RFID in cloud computing. In *Proceedings of the 5th IEEE international conference on cloud computing technology and science* (CloudCom'13), pp. 1–5.

Khalid, U., Ghafoor, A., Irum, M., & Awais Shibli, M. (2013). Cloud based secure and privacy enhanced authentication and authorization protocol. *Procedia Computer Science, 22*, 680–688.

Khan, S., Shakil, K. A., & Alam, M. (2017a). Cloud based big data analytics: A survey of current research and future directions. In *Big data analytics, electronic* (pp. 629–640). Springer.

Khan, S., Liub, X., Shakil, K. A., & Alam, M. (2017b). A survey on scholarly data: From big data perspective. *Information Processing & Management, 53*(4), 923–944.

Khodadadi, F., Calheiros, R. N., & Buyya, R. (2015). A data-centric framework for development and deployment of internet of things applications in clouds. In *Proceedings of the 10th IEEE international conference on Intelligent Sensors, Sensor Networks and Information Processing* (ISSNIP 2015), Singapore, April 7–9, pp. 1–6.

Klein, D. A. (2013). Data security for digital data storage. U.S. Patent Application 14/022,095, 2013.

Mahmood, Z. (2011). Data location and security issues in cloud computing. In *Proceedings of the 2nd IEEE international conference on Emerging Intelligent Data and Web Technologies* (EIDWT'11), pp. 49–54.

Malhotra, S., Doja, M. N., Alam, B., & Alam, M. (2017). *Generalized query processing mechanism in cloud database management system, big data analytics.* Electronic, Springer, pp. 641–648.

Masson, M. E. J., & Loftus, G. R. (2003). Using confidence intervals for graphically based data interpretation. *Canadian Journal of Experimental Psychology, 57*(3), 203.

Mell, P., & Grance, T. (2009). *The NIST definition of cloud computing*, version 15, National Institute of standards and Technology (NIST), Information Technology Laboratory, pp. 1–3. Online Available On: www.csrc.nist.gov. Last Accessed on July 21, 2017.

Miller, M. (2008). *Cloud computing: Web based applications that change the way you work and collaborate online*. Indianapolis: Que Publication.

NIST Publication. (2001). *Statistical test suite for random and pseudorandom number generators for cryptographic applications*. http://csrc.nist.gov/publications/nistpubs/800-22/sp-800-22-051501.pdf. Online available May 6, 2017.

Pandey, A., Tugnayat, R. M., & Tiwari, A. K. (2013). Data security framework for cloud computing networks. *International Journal of Computer Engineering & Technology, 4*(1), 178–181.

Plummer, D. C., Smith, D., Bittman, T. J., Cearley, D. W., Cappuccio, D. J., Scott, D., Kumar, R., & Robertson, B. (2009). Gartner highlights five attributes of cloud computing. *Gartner Report, G00167182*, 1–5.

Robert, A. E., Manivasagam, G., Sasirekha, N., & Hemalatha, M. (2011). Reverse engineering for malicious code behaviour analysis using virtual security patching. *International Journal of Computer Applications, 26*(4), 41–45.

Rogaway, P., & Black, J. (2002). A block-cipher mode of operation for parallelizable message authentication. In L. R. Knudsen (Ed.), *Proceedings of the international conference on theory and applications of cryptographic techniques, advances in cryptology – EUROCRYPT 2002, Lecture notes in computer science 2332*, held 28 April–2 May 2002 in Amsterdam, Holland (pp 384–397). Berlin: Springer.

Saldhana, A., Marian, R., Barbir, A., & Jabbar, S. A. (2014). OASIS Cloud Authorization (CloudAuthZ). *International Journal of Multimedia and Ubiquitous Engineering, 9*(9), 81–90.

Sedigh, A., Radhakrishnan, K., Campbell, C. E.-A., & Singh, D. (2014). Trust evaluation of the current security measures against key network attacks. *MAGNT Research Report, 2*(4), 161–171.

Shakil, K. A., Sethi, S., & Alam, M. (2015). An effective framework for managing university data using a cloud based environment. *computing for sustainable global development (INDIACom), IEEE 2nd international conference*, pp. 1262–1266.

Shakil, K. A., Anis, S., Khan, S., & Alam, M. (2017). Dengue disease prediction using weka data mining tool. In *Proceedings of IIRAJ International Conference (ICCI-SEM-2K17)*.

Singh, I., Rai, R., & Murarker, S. (2015a). Password authentication in cloud. *International Journal of Engineering Research and Applications, 9*(2 (Part I)), 56–59.

Singh, I., Mishra, K. N., Alberti, A., Singh, D., & Jara, A. (2015b). A novel privacy and security network for the cloud network services. *17th IEEE international conference on advanced communication technology*, pp. 355–359.

Sun, D., Chang, G., Sun, L., & Wang, X. (2011). Surveying and analyzing security, privacy and trust issues in cloud computing environments. In *Proceedings of the international conference on advanced in Control Engineering and Information Science* (CEIS'11), pp. 1–5.

Tan, Y., Sengupta, S., & Subbalakshmi, K. P. (2011). Analysis of coordinated denial-of-service attacks in ieee 802.22 networks. *Selected Areas in Communications, IEEE Journal, 29*(4), 890–902.

Van Bon, J., & Van Der Veen, A. (2007). *Foundations of IT service management based on ITIL* (Vol. 3). Zaltbommel: Van Haren Publishing.

Whiting, D., Housley, R., & Ferguson, N. (2002). *AES encryption & authentication using CTR mode & CBC-MAC*. http://csrc.nist.gov/groups/ST/toolkit/BCM/current_modes.html#03. Online available May 6, 2017.

Wijaya, C. (2011). Performance analysis of dynamic routing protocol EIGRP and OSPF in IPv4 and IPv6 network. *First international conference on Informatics and Computational Intelligence* (ICI), pp. 355–360.

Younis, M. Y. A., & Kifayat, K. (2013). *Secure cloud computing for critical infrastructure: A survey*. UK Liverpool John Moores University.

Part III
IoT Challenges and Issues

Chapter 8
Tackling Jamming Attacks in IoT

N. Ambika

Abstract Internet-of-things has brought in solutions for many problems. These devices work on sensor technology. They aim in sensing and making suitable adjustments in environment to improve the environment. These unsupervised devices are liable to different kinds of attacks. The proposed paper provides solution for reactive jamming attack. The previous contribution aims at using artificial noise to distract the adversary and accomplishes the transmission task. The proposed work tries to bring in the jammer in confidence by using the cooperation of all the devices in the network. Comparing with the previous work the proposed work conserves 7.89% of energy, increases the confidence of jammer by5.66% and increases communication overhead by 7.46%.

Keywords Jamming attack · Internet of things · Cooperative strategy · Security

8.1 Introduction

Internet-of-things (Alaba et al. 2017; Atzori et al. 2010; Ahmad 2014; Stankovic 2014) provides solutions for a lot of unattended problems. The technology aids the devices to communicate with each other irrespective of their capability and capacity. Many applications (Hegde and Kumar 2017; Liu and Zhu 2014) use this technology to bring in a better outcome. Some of the Smart homes (Al-Ali 2017; Alam et al. 2012; Mano et al. 2016) applications include aiding elderly monitoring (Yang et al. 2013; Rathore et al. 2016; Muhammad et al. 2017; Arcelus et al. 2007), to provide security (Andrea et al. 2015; Jabarullah et al. 2012; Alam et al. 2014; Sivaraman et al. 2015), home automation (Kodali et al. 2016). Other areas where these devices are utilized include designing smart city (Mitton et al. 2012), smart parking system (Khanna and Anand 2016), smart transportation (Melis et al. 2016; Sutar et al. 2016; Masek et al. 2016; Jisha et al. 2017), smart hospital management (Yu et al. 2012), agriculture (Mat et al. 2016; Popović et al. 2017), smart industry (Shrouf et al. 2014).

N. Ambika (✉)
Department of Computer Applications, SSMRV College, Bangalore, India

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_8

These devices are programmed to do certain activities to minimize human efforts. Human intervention would be only at the time of setting up the application, performing some kind of activation and removing the setup. Hence most of the time these devices are left unsupervised. The adversary will be able to introduce any kind of attack in these environments. Jamming attack (Grover et al. 2014; Babar et al. 2013; Xu et al. 2005) is one such attack which exhibits behavior with some variations based on its type – reactive jamming attack (Wilhelm et al. 2011), constant jammers (Han et al. 2018), Deceptive jammers (Lee et al. 2014), Random jammers (Wei et al. 2014; Sanguanpong 2018), Statistical jammer (Ren and Wang 2013) and Protocol-aware jammer (Sufyan et al. 2013; Toledo and Wang 2008). In this proposal, the reactive jamming attack is considered and a novel method is suggested to tackle the same.

The proposed work aims –

- Gaining the cooperation of the nodes of the network.
- Creating real-time illusion to the adversary.
- Tackling the attack better than the previous work (Pang and Xue 2017).

- The work is divided into 6 sections. Literature survey is detailed in Sect. 8.2. The proposed work is explained in Sect. 8.3. The analysis of the work is given in Sect. 8.4. Simulation of the work is detailed in the next section. The work is concluded in final section.

8.2 Literature Survey

Internet-of-things is used to link two devices and enables communication among them. As these devices are not under continuous supervision they are liable to different kinds of attacks. The proposed work aids in minimizing jamming attack in the environment. The reactive jamming attack is considered in the work. Radio interference attacks are responsible to cause serious injury in the network. The following section provides a detailed study of the jamming attacks proposed by various authors.

In Xu et al. (2005) jamming attacks are analyzed in wireless networks. The work is evaluated in two stages. In the first stage, the problems that crop up when radio interference attack is encountered is scrutinized. In the second stage, critical issues of diagnosing the presence of the attack are dissected. Four kinds of jamming attacks are introduced into the network and the effect on the wireless network, their ability to receive and send messages is evaluated. The work is analyzed considering the signal strength and carrier sensing time. The proposed work used Mica2 as the platform to conduct the respective experiments. The MAC protocol (Hamza et al. 2016) waits for the idle slot for a random amount of time to transmit the packets. The four kinds of jammer – constant jammer, reactive jammer, random jammer, and deceptive jammer were evaluated. Berkeley motes are used in the system. They useChipCon CC1000 RF transceiver and TinyOS operating system were used to

implement and evaluate the working of the study under the four kinds of jamming (Noubir et al. 2011) attacks. The channels were disabled to sense the packets and the backoff operations to bypass MAC protocol to introduce the attacks in the network. The study will not be able to analyze the difference between the congested packet and jamming attack.

Reactive jamming is evaluated in Wilhelm et al. (2011). An IEEE 802.15.4 network is used to examine the proposed work. The loss occurred at the physical layer are identified and a solution is provided to tackle reactive jamming attack. To discover the attack detection of jamming, scheduling and initialization of jamming and jamming burst to destroy the packet is calculated against the minimal time required for jamming. The proposed work concluded that minimal jamming duration is 26 μs, jamming initialization time was set to 15 μs and the detector added a delay of less than 4 μs. The accounted data is used to check the same against USRP2-based reactive jamming prototype.

In Raya and Hubaux (2007) jamming attack was experimented on vehicular networks. Analyzing the threat analysis appropriate security architecture was devised. Digital signatures were used to protect the message legacy from the adversaries. The work adopts to use a set of public/private keys pairs to sign the messages digitally and validate (Shakil et al. 2017) themselves to the receivers. To tackle revocation of certificates a set of revocation protocols are used. Revocation Protocol of the Tamper-proof Device (RTPD), Revocation protocol using Compressed Certificate Revocation list (RCCRL) and Distributed Revocation Protocol (DRP) are utilized in the work. Using the protocol the malicious behavior can be detected.

A game-theoretic analysis is used to avoid the attack of an airborne jammer on a communication channel (Bhattacharya and Başar 2010). The kinematic model of the nodes is considered. To obtain optimal strategies, saddle point strategies are used. This is a zero-sum game which has a set of strategies for the players are used to arrive at the equations governing the saddle point strategies. In Brown et al. (2006) the authors have considered an attacker disrupting an encrypted victim wireless Adhoc network using jamming practice. Jamming at the Transport/network layer is considered in the work. The analysis revealed that TCP-SYN and TCP-SYN-ACK packets prevent TCP connection. ARP-REQUEST and ARQ-RESPONSE will prevent IP from associating IP and MAC address. Sensing is considered to be both online and offline. Online sensing packets are identified as they are received by the destination. Offline sensing is used to categorize the packets received in the history doings. The spread spectrum proposed in the work provides a jamming immunity proportional to the spreading factor. The authors used Linux laptops running AODV-UU protocol while conducting testbed.

The authors in Li et al. (2007) have provided a solution for single-channel wireless sensor networks. The sophisticated jammer in the work controls the probability of the jamming and transmission range aims to corrupt the communication links in the network. The monitoring node is responsible to monitor the doings of the other nodes in the network. The supervising node conveys the alert message to the respective. The monitoring node is responsible to estimate the percentage of incurred collisions and draw out the outcome of optimal detection test. The network computes

channel access probability to aid in minimizing jamming detection and reporting time. The study focuses to understand the problems regarding the structure, identifying the tradeoffs and capturing the impact of different parameters on its performance. The study is made to bring in a strategy which aims to handle the situation in case of a knowledge-based/without knowledge-based scenario. The network and monitor node without the knowledge uses the formulation and resolving optimization problems.

Path-based Dos attack is dealt in Deng et al. (2005). The wireless sensor network will undergo serious damage. The intruder either injects replays the packets into the network or spurious packets. The adversary aims to block the path by introducing jamming packets and initiating the base station to re-boot the OHC (a sequence of numbers) for all the nodes on the path. Two methodologies are adapted aiding to minimize jamming and forgo the above scenario. OHC proactive bootstrapping employs to bootstrap the nodes near the jamming path and refreshing the OHC sequence. Another approach is known as lazy OHC bootstrapping where the addition of a new node to the network does not commence bootstrapping but still maintains resilience to stop Dos attack.

In Hamieh and Ben-Othman (2009) the authors have designed a solution for jamming attacks in mobile Adhoc networks. The authors have used a scenario where the jammer gets itself into its doings when valid radioactivity is signaled. The adversary moves to sleep state when it is not jamming the signals. To find the solution to this kind of attack, dependence among the periods of error and correct reception times are analyzed. The correlation coefficient is used to compute the same. The coefficient is the statistical measure of the relation between two random variables. To evaluate the jammer, error probability and correlation coefficient is measured.

In Sampath et al. (2007) 802.11 networks are considered. A detailed study on Single-channel jamming and multi-channel jamming attacks is done in this work. In the case of single-channel jamming attack, the adversary transmits high power signals on the channel. The impact of jamming depends on the size of the packets, length of inter-jamming interval and size of jamming packets. The adversary is observed to transmit 50-byte size packets to disrupt the data link. According to the experiment conducted in the work 100%,—40% of packets suffer from degradation. Considering the second scenario, multiple radio devices are used to cause multi-channel jamming attacks. The impact can cause 5-100 ms switching delay.

The solution to Spoofing-jamming attack in wireless smart grid network is detailed in Gai et al. (2017). The work considers both jamming and spoofing to intrude in the communication. The frequencies used to transmit jamming packets vary with time. Spectrum adversarial occupations are used to maximize the attack effect. The study uses dynamic programming to solve power distribution optimal problem. The study is evaluated using the simulator MAS-SIM.

In Pang and Xue (2017) the authors have provided a solution to tackle intelligent jamming attacks. The method uses the adversary location as a precondition to restoring the transmission links. The synthetic noise generated by synergistic sensor nodes the channel of the adversary is degraded. New types of a jamming attack like clear-to-send frame attack, DATA frame attack and ACK frame attack is considered

to provide a solution. The anti-jamming method can tackle the adversary in carrier sense multiple access with collision avoidance protocol (CSMA/CA). An artificial noise is created and the same use jammer localization methods as a precondition. A cooperative strategy that aids in jamming the intelligent adversary is enabled at the physical layer. The high signal-to-noise ratio disables the jammer to decipher the receiving packets. This methodology aids the network not to interfere in a special frame timely. The ratio of the packet transmitted and received are calculated in the work. The proposed work uses a similar scenario with some modifications is utilized in IoT (Riedel et al. 2010; Lopez et al. 2017). The proposal aids to minimize energy (Chiu et al. 2017) in the devices.

8.3 Proposed Study

Reactive jamming attack (Fadele et al. 2018; Sciancalepore et al. 2018) the adversary emits radio signals on sensing the activity in the channel. These packets keep the channel busy. The packets dispatched by the legitimate devices may die before reaching the destination or they may get lost in the channel.

In Pang and Xue (2017) the authors have provided a solution to tackle intelligent jamming attacks. The method uses the jammer location as a prerequisite to restoring the communication links. Based on using the artificial noise generated by synergistic sensor nodes (Narayanan et al. 2016) the channel of the jammer is degraded. New types of a jamming attack like clear to send frame jammer, DATA frame jammer and ACK frame jammer is considered to provide a solution. The anti-jamming method can tackle the jammer in carrier sense multiple access with collision avoidance protocol (CSMA/CA). An artificial noise is created and the same use jammer localization methods as a precondition. A cooperative strategy that aids in jamming the intelligent jammer is enabled at the physical layer. The high signal-to-noise ratio disables the jammer to decode the receiving packets. This methodology aids the network not to interfere in a special frame timely. Packet-send-ratio (PSR) and packet delivery ratio (PDR) is calculated in the work. The proposed work uses a similar scenario with some modifications is utilized in IoT (Mala et al. 2017). The proposal aids to minimize energy in the devices.

In the proposed work the devices cooperate to create a different illusion to the adversary. The adversary will try engaging its packets in the different direction and hence the actual packets to be successfully delivered to the respective destination.

8.3.1 Notations Used in the Study

The notations and its decription is given in Table 8.1.

Table 8.1 Notations and its description

Notations	Description
N	Network in consideration
Hello	Hello message
L_i	Location of ith device
Ack	Acknowledgement message
id_i	Identification of ith device
<<null>, id_i>	Null packet with identification of ith device

8.3.2 Assumptions Made in the Study

- The network is free of all kinds of attacks till the initial identification of communicating device is made.
- The network is liable for reactive jamming attack.
- The system uses carrier sense multiple access with collision avoidance protocol (CSMA/CA).

8.3.3 Creating Awareness

The IoT devices first communicate among themselves to know each other. They send their location and their identity during communication. In notation (1) let A is broadcasting the hello message along with its location and identification to the network. Let r be the communication radius. The devices which are able to hear each other will respond with the Ack message. The acknowledgement message contains Ack, location and identification of the sender. In the notation (2) IoT device B is transmitting the message to the device A.

$$A \rightarrow \left(hello, L_i, id_i\right) : N \tag{8.1}$$

$$B \rightarrow \left(Ack, L_j, id_j\right) : A \tag{8.2}$$

8.3.4 Identifying the Jammer Location

The devices irrespective of the type have a certain capacity to transmit the packets. The number of packets for a device varies but it is accountable. The devices maintain the packet delivery ratio (PDR) and the packet sent ratio (PSR) entries. The regular report of the packets delivered and received is transmitted to the control unit. Analyzing the device capacity, the frequency, threshold with device id for each device is set. The same is communicated by the control unit to the devices. If the

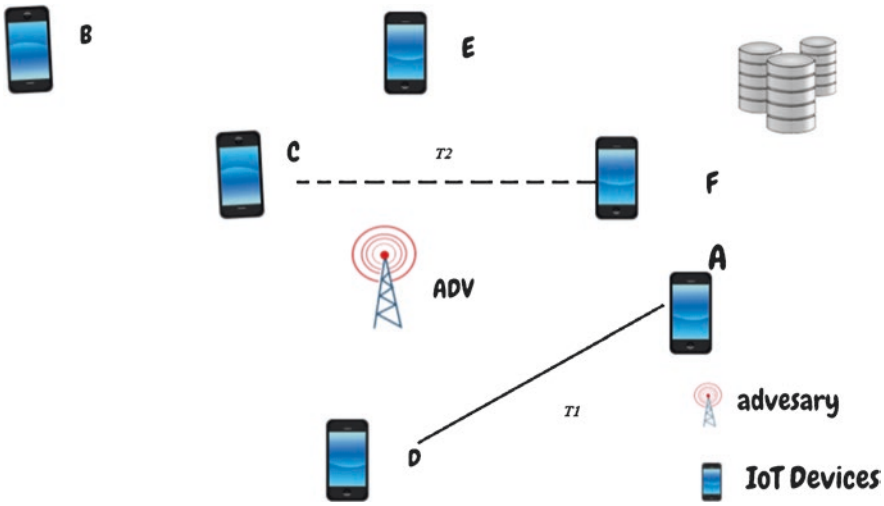


Fig. 8.1 Representation of the network of IoT devices with an adversary

devices receive data from inappropriate source, the same is reported to the control unit. Other parameters – packets received, frequency are reported of the inappropriate device to the control unit. The control unit analyses the same and if the device id is not registered in its storage, the jammer is identified and notified to the network.

8.3.5 Choosing Appropriate Path for Delivery

From the Fig. 8.1, Let us assume that the device C has to deliver the data to the device F. as the jammer gets notified, the distraction approach is adopted. The device C sends a null packet to D with the identification of device A. in the Eq. (8.3) the device C is delivering the null packet to the device D. Once the device D gets the message, the device D sends some packets to A to provide a distraction. The jammer tries to introduce the packets between D and A. In the meantime, device C delivers the packet to F.

$$C \rightarrow null, id_A : D \tag{8.3}$$

8.4 Analysis of the Work

Security (Farash et al. 2016) is necessary in the network to increase reliability (Li et al. 2012a, b), confidentiality and privacy. In Pang and Xue (2017) the authors have provided a solution to tackle intelligent jamming attacks. The method uses the

adversary location as a precondition to restoring the transmission links. The synthetic noise generated by synergistic sensor nodes the channel of the adversary is degraded. New types of a jamming attack like clear-to-send frame attack, DATA frame attack and ACK frame attack is considered to provide a solution. The anti-jamming method can tackle the adversary in carrier sense multiple access with collision avoidance protocol (CSMA/CA). An artificial noise is created and the same use jammer localization methods as a precondition. A cooperative strategy that aids in jamming the intelligent adversary is enabled at the physical layer. The high signal-to-noise ratio disables the jammer to decipher the receiving packets. This methodology aids the network not to interfere in a special frame timely. The ratio of the packet transmitted and received are calculated in the work. The proposed work uses a similar scenario with some modifications is utilized in IoT. The proposal aids to minimize energy in the devices.

8.4.1 Energy Consumption

Energy is one of the important resources. As these systems are installed in a hospital or home setup, tackling the attacks becomes essential.

In the proposed work the system uses carrier sense multiple access with collision avoidance protocol (CSMA/CA). The devices cooperate among themselves for effective communication. In Pang and Xue (2017) artificial noise is generated. When the noise is generated at the same location every time, the jammer will be able to identify the same and try performing using a different strategy. To avoid such a scenario, the proposed work has suggested some real-time methodology. The method aids in confusing the jammer with its tactics. The work (Pang and Xue 2017) has to use a lot of energy to create artificial noise. Comparing the proposed work with the work (Pang and Xue 2017), the proposed work uses 7.89% of less energy and gains the confidence of the jammer. The same is depicted in Fig. 8.2.

8.4.2 Taking Jammer into Confidence

The work (Pang and Xue 2017) uses artificial noise to distract the jammer. The proposed work is also accomplishing the task by the cooperation of the devices in the network. The jammer position is identified in the proposed work using data provided by the control unit. When the devices have to send some communication to the other device, to distract the jammer the device transmits a null packet to another device. The device that receives the packet sends some packets to the mentioned device. In the meantime, the actual packets reach the destination without any hindrance. Hence the proposed work proves to be 5.66% more reliable (Ahmad 2014) than the work (Pang and Xue 2017). The same is represented in Fig. 8.3.

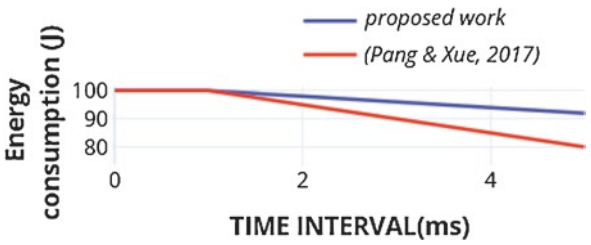


Fig. 8.2 Comparison of Energy consumption (Joules)

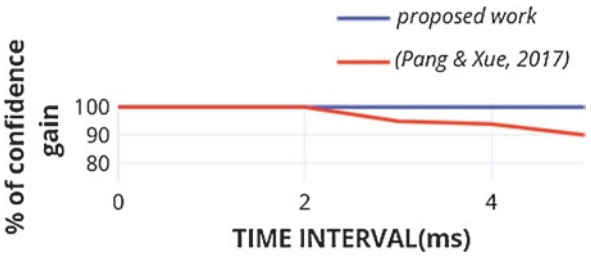


Fig. 8.3 Comparison of confidence gain of the jammer

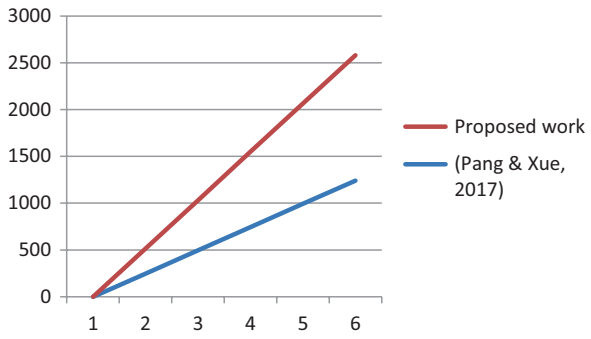


Fig. 8.4 Comparison of the work (Pang and Xue 2017) with the proposed work w.r.t communication overhead

8.4.3 Communication Overhead

The work (Pang and Xue 2017) does not impose any load on the devices rather the noise is generated by the artificial noise generated meant for the same purpose. The proposed work adds some amount of transmission load on the other devices to accomplish the task. Comparing the work (Pang and Xue 2017) with the proposed work, the proposed work has 7.46% overhead. The same is depicted in Fig. 8.4.

8.4.4 Simulation of the Work

The work is simulated using NS2. The following parameters as described in the Table 8.2 are used to simulate the work.

Table 8.2 Parameters used in the simulation work

Parameters	Description
Dimension	200 m ∗ 200 m
No of devices considered	5
Jammer considered	1
Number of packets delivered per unit time	248
Simulation time	60s
Null packet size	13 bits
Packet size identification of device	12 bits
Packet size of the location	24 bits
Packet size of hello/ acknowledgement packet	6 bits

8.5 Conclusion

Internet-of-things is a boon to mankind. The technology aids in bringing different kinds of devices with varying size and capacity into a common platform for communication. As these devices are unsupervised the network is liable for different kinds of attacks. Reactive jammer attack is one such attack where the adversary introduces the attack on sensing any packets in the channel. In this scenario, the source will not be successfully transmitting all its packets to the desired destination.

In the earlier work proposed by Pang and Xue, artificial noise was created to distract the adversary from the desired location. The proposed work suggested using the cooperation of the devices to bring in the real-time scenario and gain the confidence of the adversary. The proposed work increases its confidence with an adversary by 5.66% compared to work proposed by Pang & Xue and energy is conserved by 7.89%. The communication overhead is increased by 7.46% compared with the previous work.

References

Ahmad, M. (2014). Reliability models for the Internet of Things: A paradigm shift. In *IEEE international symposium on software reliability engineering workshops, Naples, Italy*.

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, 10–28.

Al-Ali, et al. (2017). A smart home energy management system using IoT and big data analytics approach. *IEEE Transactions on Consumer Electronics, 63*(4), 426–434.

Alam, M. R., Reaz, M. B. I., & Ali, M. M. (2012). SPEED: An inhabitant activity prediction algorithm for smart homes. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 42*, 985–990.

Alam, M., Shakil, K. A., Javed, M. S., Ansari, M., & Ambreen. (2014). Detect and filter traffic attack through cloud trace back and neural network. In *International Conference of Data Mining and Knowledge Engineering (ICDMKE)*. London, UK: Imperial College.

Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015). Internet of Things: Security vulnerabilities and challenges. In *IEEE Symposium on Computers and Communication (ISCC), IEEE* (pp. 180–187).

Arcelus, A., Jones, M. H., Goubran, R., & Knoefel, F. (2007). Integration of smart home technologies in a health monitoring system for the elderly. In *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), Niagara Falls, ON, Canada* (Vol. 2, pp. 820–825).

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*, 2787–2805.

Babar, S. D., Prasad, N. R., & Prasad, R. (2013). Jamming attack: Behavioral modelling and analysis. In *International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE)* (pp. 1–5).

Bhattacharya, S., & Başar, T. (2010). Game-theoretic analysis of an aerial jamming attack on a UAV communication network. In *American control conference, Baltimore, MD, USA* (pp. 818–823).

Brown, T. X., James, J. E., & Sethi, A. (2006). Jamming and sensing of encrypted wireless ad hoc networks. In *7th ACM international symposium on Mobile ad hoc networking and computing, Florence, Italy* (pp. 120–130).

Chiu, W.-Y., Sun, H., Thompson, J., Nakayama, K., & Zhang, S. (2017). IoT and information processing in smart energy applications. *IEEE Communications Magazine, 55*, 44.

Deng, J., Han, R., & Mishra, S. (2005). Defending against path-based DoS attacks in wireless sensor networks. In *3rd ACM workshop on Security of ad hoc and sensor networks , Alexandria, VA, USA* (pp. 89–96).

Fadele, A. A., Othman, M., Hashem, I. A. T., Yaqoob, I., Imran, M., & Shoaib, M. (2018). A novel countermeasure technique for reactive jamming attack in internet of things. *Multimedia Tools and Applications*, 1–22.

Farash, M. S., Kumari, S., & Bakhtiari, M. (2016). Cryptanalysis and improvement of a robust smart card secured authentication scheme on SIP using elliptic curve cryptography. *Multimedia Tools and Applications, 75*(8), 4485–4504.

Gai, K., Qiu, M., Ming, Z., Zhao, H., & Qiu, L. (2017). Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks. *IEEE Transactions on Smart Grid*, 2431–2439.

Grover, K., Lim, A., & Yang, Q. (2014). Jamming and anti-jamming techniques in wireless networks: A survey. *International Journal of Ad Hoc and Ubiquitous Computing*, 197–215.

Hamieh, A., & Ben-Othman, J. (2009). Detection of jamming attacks in wireless ad hoc networks using error distribution. In *IEEE international conference on communications, Dresden, Germany* (pp. 1–6).

Hamza, T., Kaddoum, G., Meddeb, A., & Matar, G. (2016). A survey on intelligent MAC layer jamming attacks and countermeasures in WSNs. In *84th vehicular technology conference* (pp. 1–5).

Han, G., Liu, L., Zhang, W., & Chan, S. (2018). A hierarchical jammed-area mapping service for ubiquitous communication in smart communities. *IEEE Communications Magazine*, 92–98.

Hegde, S., & Kumar, S. G. (2017). IoT approach to save life using GPS for the traveller during accident. In *IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, India* (pp. 2424–2428).

Jabarullah, B. M., Saxena, S., Kennedy Babu, C. N., & Alam, M. (2012). Hybrid approach of face recognition. *Cyber Times International Journal of Technology & Management, 6*(1), 6–12.

Jisha, R. C., Jyothindranath, A., & Kumary, L. S. (2017). Iot based school bus tracking and arrival time prediction. In *International Conference on Advances in Computing, Communications and Informatics (ICACCI), Udupi, India*.

Khanna, A., & Anand, R. (2016). IoT based smart parking system. In *International Conference on Internet of Things and Applications (IOTA), Pune, India* (pp. 266–270).

Kodali, R. K., Jain, V., Bose, S., & Boppana, L. (2016). IoT based smart security and home automation system. In *International conference on computing, communication and automation (ICCCA), Noida, India* (pp. 1286–1289).

Lee, T. H., Wen, C. H., Chang, L. H., Chiang, H. S., & Hsieh, M. C. (2014). A lightweight intrusion detection scheme based on energy consumption analysis in 6LowPAN. *Advanced Technologies, Embedded and Multimedia for Human-Centric Computing*, 1205–1213.

Li, M., Koutsopoulos, I., & Poovendran, R. (2007). Optimal jamming attacks and network defense policies in wireless sensor networks. In *26th IEEE international conference on computer communications, Barcelona, Spain* (pp. 1307–1315).

Li, L., Jin, Z., Li, G., Zheng, L., & Wei, Q. (2012a). Modeling and analyzing the reliability and cost of service composition in the IoT: A probabilistic approach. In *IEEE 19th International Conference on In Web Services* (pp. 584–591).

Li, W., Miao, Y., Tang, Y. W., Liu, D., & Hu, B. (2012b). IOT system reliability testing and evaluate technology. *Software*, 1.

Liu, S. J., & Zhu, G. Q. (2014). The application of GIS and IOT technology on building fire evacuation. *Procedia Engineering, 71*, 577–582.

Lopez, D. A. R., Lopez, J. R. R., Prieto, M. A. Z., & Quinde, L. D. S. (2017). Towards a method for the integration of IoT and GIS applications deployed on cloud platforms. In *International Conference on Information Systems and Computer Science (INCISCOS), Quito, Ecuador*.

Mala, N. S., Thushara, S. S., & Subbiah, S. (2017). Navigation gadget for visually impaired based on IoT. In *2nd International Conference on Computing and Communications Technologies (ICCCT), Chennai, India*.

Mano, L. Y., Faiçal, B. S., Nakamura, L. H., Gomes, P. H., Libralon, G. L., Meneguete, R. I., & Ueyama, J. (2016). Exploiting IoT technologies for enhancing Health Smart Homes through patient identification and emotion recognition. *Computer Communications, 89*, 178–190.

Masek, P., et al. (2016). A harmonized perspective on transportation management in Smart Cities: The novel IoT-driven environment for road traffic modeling. *Sensors, 16*(11), 1872.

Mat, I., Kassim, M. R. M., Harun, A. N., & Yusoff, I. M. (2016). IoT in precision agriculture applications using wireless moisture sensor network. In *IEEE Conference on Open Systems (ICOS), Langkawi, Malaysia* (pp. 24–29).

Melis, A., Prandini, M., Sartori, L., & Callegati, F. (2016). Public transportation, IoT, trust and urban habits. In *International conference on internet science* (pp. 318–325).

Mitton, N., Papavassiliou, S., Puliafito, A., & Trivedi, K. S. (2012). Combining cloud and sensors in a smart city environment. *EURASIP Journal on Wireless Communications and Networking*, 1–10.

Muhammad, G., Rahman, S. M. M., Alelaiwi, A., & Alamri, A. (2017). Smart health solution integrating IoT and cloud: A case study of voice pathology monitoring. *IEEE Communications Magazine, 55*(1), 69–73.

Narayanan, R. P., Sarath, T. V., & Vineeth, V. V. (2016). Survey on motes used in wireless sensor networks: Performance & Parametric Analysis. *Wireless Sensor Network, 08*, 51–60.

Noubir, G., Rajaraman, R., Sheng, B., & Thapa, B. (2011). On the robustness of IEEE 802.11 rate adaptation algorithms against smart jamming. In *Fourth ACM conference on Wireless network security* (pp. 97–108).

Pang, L., & Xue, Z. (2017). A novel anti-jamming method in wireless sensor networks: Using artificial noise to actively interfere the intelligent jammer. In *4th international conference on systems and informatics* (pp. 954–959).

Popović, T., Latinović, N., Pešić, A., Zečević, Ž., Krstajić, B., & Djukanović, S. (2017). Architecting an IoT-enabled platform for precision agriculture and ecological monitoring: A case study. *Computers and Electronics in Agriculture, 140*, 255–265.

Rathore, M. M., Ahmad, A., Paul, A., Wan, J., & Zhang, D. (2016). Real-time medical emergency response system: Exploiting IoT and big data for public health. *Journal of Medical Systems, 40*(12), 283.

Raya, M., & Hubaux, J. P. (2007). Securing vehicular ad hoc networks. *Journal of Computer Security, 15*, 39–68.

Ren, K., & Wang, Q. (2013). Opportunistic spectrum access: From stochastic channels to non-stochastic channels. *IEEE Wireless Communications*, 128–135.

Riedel, T., Fantana, N., Genaid, A., Yordanov, D., Schmidtke, H. R., & Beigl, M. (2010). Using web service gateways and code generation for sustainable IoT system development. *Internet of Things*, 1–8.

Sampath, A., Dai, H., Zheng, H., & Zhao, B. Y. (2007). Multi-channel jamming attacks using cognitive radios. In *16th international conference on computer communications and networks, Honolulu, HI, USA* (pp. 352–357).

Sanguanpong, S. (2018). Secrecy outage performance analysis for energy harvesting sensor networks with a jammer using relay selection strategy. In *Special section on security and trusted computing for industrial Internet of Things* (pp. 23406–23419).

Sciancalepore, S., Oligeri, G., & Di Pietro, R. (2018). Strength of Crowd (SOC)—Defeating a reactive jammer in IoT with decoy messages. *Sensors, 18*, 3492.

Shakil, K. A., Zareen, F. J., Alam, M., & Jabin, S. (2017). BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud. *Journal of King Saud University – Computer and Information Sciences*.

Shrouf, F., Ordieres, J., & Miragliotta, G. (2014). Smart factories in industry 4.0: A review of the concept and of energy management approached in production based on the Internet of Things paradigm. In *IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Bandar Sunway, Malaysia* (pp. 697–701).

Sivaraman, V., Gharakheili, H. H., Vishwanath, A., Boreli, R., & Mehani, O. (2015). Network-level security and privacy control for smart-home IoT devices. In *IEEE 11th International conference on wireless and mobile computing, networking and communications (WiMob), Abu Dhabi, United Arab Emirates* (pp. 163–167).

Stankovic, J. A. (2014). Research directions for the Internet of Things. *IEEE Internet of Things Journal, 1*(1), 3–9.

Sufyan, N., Saqib, N. A., & Zia, M. (2013). Detection of jamming attacks in 802.11 b wireless networks. *EURASIP Journal on Wireless Communications and Networking*, 208.

Sutar, S. H., Koul, R., & Suryavanshi, R. (2016). Integration of Smart Phone and IOT for development of smart public transportation system. In *International Conference on Internet of Things and Applications (IOTA), Pune, India* (pp. 73–78).

Toledo, A. L., & Wang, X. (2008). Robust detection of MAC layer denial-of-service attacks in CSMA/CA wireless networks. *IEEE Transactions on Information Forensics and Security*, 347–358.

Wei, X., Hu, Y., Fan, J., & Kan, B. (2014). A jammer deployment method for multi-hop wireless network based on degree distribution. In *Ninth International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA)* (pp. 261–266).

Wilhelm, M., Martinovic, I., Schmitt, J. B., & Lenders, V. (2011). Short paper: Reactive jamming in wireless networks: How realistic is the threat? In *Fourth ACM conference on Wireless network security, Hamburg, Germany* (pp. 47–52).

Xu, W., Trappe, W., Zhang, Y., & Wood, T. (2005). The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing* (pp. 46–57). ACM.

Yang, L., Yang, S. H., & Plotnick, L. (2013). How the Internet of Things technology enhances emergency response operations. *Technological Forecasting and Social Change, 80*(9), 1854–1867.

Yu, L., Lu, Y., & Zhu, X. (2012). Smart hospital based on Internet of Things. *Journal of Networks, 7*(10), 1654.

Chapter 9
Bioinspired Techniques for Data Security in IoT

S. R. Mani Sekhar, G. M. Siddesh, Anjaneya Tiwari, and Ankit Anand

Abstract Data Security is a protective privacy measure which is used for prevention of unauthorized access in various domains such as computers network, web application, database etc. Bio-inspired computing is a branch of Machine learning deals with the biological properties of living organism. These techniques are used in the fields of data security and feature extraction in combination with different IoT architecture for secure data transition and maintenance. This chapter discusses some of the biologically inspired computational algorithms like Ant Colony Optimization, Artificial Bee Colony, Genetic bee colony, and Firefly which are used in solving real world problem in the field of IoT for providing data security. Finally the chapter concludes by stating the effectiveness of these algorithms on the bases of the case studies and thus provides a wider perspective towards Bio-inspired techniques and their use for data security in IoT.

Keywords Security · Bioinspired · IoT · Internet of Things · Ant colony optimization · Artificial bee colony optimization · Genetic bee colony · Firefly

9.1 Introduction

Data Security are protective privacy measures which are used for prevention of unauthorized access in various domains such as computers, websites or databases. It is also used for the protection of data from getting corrupted. Since data security is necessary in the field of information technology, it is also known as information security or computer security. It is an important aspect of IT in the organisations of all sizes and types. Authentication is the most common method of applying data security with the help of password, usernames or some other kind of data such as

S. R. Mani Sekhar (✉) · G. M. Siddesh · A. Tiwari · A. Anand
Department of Information Science & Engineering, Ramaiah Institute of Technology, Bangalore, Karnataka, India

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_9

biometric in order to verify someone's identity before granting them access to system. Some examples of data security in day-to-day world are masking of data and data erasure.

Encryption is a data security technology where digital data, hard drives, software or hardware are encrypted. Some of the very important fields where data security is being applied include health care record security, protection of a brand, capital and customer's information and in IoT applications.

Data security includes a set of standards which helps in the protection of data from getting destructed accidentally or intentionally. Methods such as applying data security using administrative controls, organisational standards, logical controls, physical security or other safeguarding techniques helps in limiting access to malicious or unauthorized users or processes.

The main objective of using Biological techniques is to incorporate how living being solve their daily life problems by applying various characteristic functions and use these in solving complex computerised problems. The foundations on which the biologically inspired computational algorithms depends upon, includes subjects such as biology, computer science and mathematics. The analysis of these fields in relation with nature allows the creation of biologically inspired algorithms.

Bio inspired computing deals with studying various designs, patterns and variations among the living beings which are further used for computing different compound problems such as the NP hard problems etc. These techniques are used in the fields of data security and feature extraction in combination with its integration with IoT for providing data security (Banu et al. 2016; Sari 2017).

In the following section, this chapter discusses about key objectives of data security in IoT and how it can be achieved using Bio inspired algorithms. Firstly, it gives a detailed information about what the keyword actually means like data security in IoT, what is Bio inspired computing, the various types of algorithms available. After this, the chapter mainly describes three algorithms which are currently in use for securing data and proved to very efficient. The algorithms which are covered in this chapter include Ant colony optimization algorithm, artificial bee colony optimization algorithm, genetic bee colony algorithm, and firefly algorithm. In the detailed description of each algorithm the chapter presents two case studies in each algorithm to widen the knowledge base about these algorithms thus providing better understanding. After this we sum up by stating the effectiveness of these algorithms and by providing a detailed conclusion about the chapter.

9.2 Data Security in IoT

IoT refers to internet of things which is a combination of network of various devices and appliances containing software, electronics and connectivity which help in the connection and interaction of data along with exchange of data. IoT includes involvement of devices beyond that of standard devices such as mobiles, laptops or

pc's. IoT allows interaction of these devices which communicate and interact with each other via internet thus allows easy controlling and monitoring of these devices.

IoT is seen as next revolution in the coming future so it is very important that protection of data in IoT technology is assured in order to allow fluent communication between devices with very little or no human intervention. IoT will include integration of communication devices, chips and sensors along with appliances (physical objects) which will enable communication between them and other devices including laptops, smart phones, computers and cloud servers. IoT has certain implications which must be considered including:

- Generation of huge amount of data by these devices, so faster networks, large storage and wider bandwidth are needed to support its growth.
- Requirement of an ecosystem for hosting of these devices to make an interoperable system.
- Switching from IPv4 to IPv6 which is a more scalable protocol.

Measures such as well protected devices, inculcating best practices for protection against security exploits and an interoperable interface are very important before switching to IoT.

9.3 Bioinspired Computing

It is a research based method which is aimed at giving solutions to problems with the help of computer models, involving biological principles in the nature. This approach puts focus on dependability and is a bottom-up approach. The three key features of this approach are connectionism, emergence and social behavior. It puts the use of computers in modeling the living phenomena and studying of life simultaneously in order to improve its usage. The models of computers derive their abstractions from living organism of real world along with their behavior socially. This field is a branch of machine learning relating very closely to artificial intelligence.

Since it involves subjects such as computer science, mathematics and biology, it can go up to a wide level in studying the diverse patterns and variations found among the living organisms thereby helping in building a better computer system for solving complex problems in future.

A few of the most popular bio-inspired computations algorithms which are used for creating a secured framework in the field of data security are neural networks, particle swarm algorithm, genetic algorithm, bee colony algorithm, ant colony optimization, bat algorithm etc.

The author will discuss all the above mentioned algorithms in detail with the help of supportive statements, case studies, problems and solutions.

9.3.1 Relationship Between Traditional and Bio-Inspired Data Security

The computing techniques which were used previously are good but still they require some changes for handling complex problems, they are not efficient at handling hard computations, pattern recognition, robust sensitive etc. Thus by using biological concepts with older techniques we can solve different kinds of complex problems and can enhance the robustness and efficiency too. Here we discuss bio-inspired computing techniques in detail, its purpose and use, computational methods used applications and restrictions as well. Although existing traditional hardware and software can not completely fulfill all the needs and failed to solve many of the problems. The main disadvantage of traditional techniques is well stated but still some hard problems such as NP hard problems (TSP Problem), intelligent human machine interaction, natural language understanding, real world autonomous robots, management and understanding. Some of the other options available are Bio-Computing which involves simulation of biological mechanisms, Quantum computing and DNA based computing. The main foundation of bio inspired computing is natural sciences, different theory, conforming algorithms and artificial life.

9.3.2 Achieving Security in IoT Using Bioinspired Techniques

The IoT is in its prime time involving different cities, smart homes, modular kitchens, smart buildings, smart appliances, smart health, smart machines and factories, smart transportation, and security. The management and buildings are based on smart systems consisting of sensors and participation of people as sources of information (Alam et al. 2013; Bello and Zeadally 2014; Perumal et al. 2016; Xu et al. 2014). The success of IoT in coming future depends upon the various new approaches in the field of evolution of technology and system security. The success of IoT is analyzed with the help of development in the field of system engineering and its processes along with the tools helping in overcoming the challenges in IoT network. The document discusses some bio inspired techniques for upcoming technology in communication in IoT platform which is an example of engineering in software. We talk about various optimization techniques such as computational iterative, which resulted in algorithms derived from nature, which are further derived from living creatures or organisms. Then further we explain examples obtained from the intellect of various existing organisms in nature. Bio inspired algorithm classifies evolution, ecology, immune, network, swarm in order to overcome difficulties such as security, scalability, mobility, heterogeneity, and resource constraint. The major goal of this chapter is to overcome and mention the emerging technologies for cyber security. This is used to prove that bio inspired techniques can really be used and further implemented to protect networks.

Biologically inspired models used in security have been flourishing for defending and securing ad hoc networks.

9.3.3 Types of Bioinspired Computing Algorithms

Computing inspired from nature tells about the variety for different solutions which we can learn from our natural surrounding and thus implement it for solving problem related to computing. The world is full of different kinds of creatures and organisms thus by knowing about their behavior and characteristics one can learn and apply those concepts in computing for solving problems such as the NP hard problem, travelling salesman problem. The most popular algorithms inspired from nature are the ant colony algorithms, cuckoo algorithm, firefly algorithm, bee colony algorithm, bat algorithm, fish swarm algorithm and various others. These algorithms are developed by noting down the various characteristics of ants, bees, bats, and various other living creatures on which these algorithms are designed. Thus in this chapter we represent a few of these algorithms along with their case studies for better understanding and thus show how data security can be achieved in IoT using algorithms which are inspired by nature.

9.4 Different Approaches for Data Security in IoT Using Bioinspired Computing

Bio-Inspired Computing involves the idea of natural computing which provides a field for performing research focusing on biology as an inspiration to solve complex computational problems along with using the experiences of the nature and natural world to solve real world problems. The various approaches used in bio inspired computing are described below.

The major topics of bio inspired computing are as follows:

(i) Ant colony Optimization
(ii) Genetic Bee colony algorithm
(iii) Firefly algorithm

9.4.1 Ant Colony Optimization (Birattari et al. 2007; Dorigo and Birattari 2011)

ACO consists of algorithms; the first one is called Ant System, which was given by Colorni, Maniezzo and Dorigo. The objective work, which is derived by the functions of real ants, has a similar find greater than various conforming gear which are

based on some restricted problem data which can be used with a active memory formation and has the information about the value of precious results. This kind of approach coming from the conversation of the diverse search gear has proved vital and helps in solving combinatorial optimization problems. In the past few years, the interest of the scientific community in ACO has grown immensely.

The first of the ant algorithm, named "Ant System" (AS), was given by Dorigo et al. in 1996 and successfully tested on the popular problems. The ACO Meta or data definition was given by to generate, the method (Dorigo and Di Caro 1999) of conforming combinatorial problems by aggregate solutions and the solution to these problems is obtained from the amount of the bee interactions. A randomly spread first population result is spread in the dimensional problem space. A designated bee provides a change to the location in the reminiscence given to the local result and determine amount of nectar required for the new source. Then there are various phases involved in which the following part are involved Reproduction, in which based on the availability of the food the artificial bees waiting chooses a food source. After choosing the nectar amount the bees verify with the previous results if the new one is effective or needs to change to get optimized nectar value which is the required end product. In the other phases we check if the functioning of the above approach is what is required or not and check if other solutions are possible to solver the same problem. If the food source in the first phase is not been found, we move to other approaches in which the same concept is applied in a different way.

In the next section we discuss the different case studies and present a broader perspective of what is being talked about here.

Below section illustrates the different case studies such as Routing Protocols based on ACO, Ant Colony for travelling salesman problem, Bee Algorithm in data security, Dependable data assembly in IoT using bee colony, Performance analysis of firefly algorithm for data Clustering High Performance Security System for Image in IoT.

9.4.1.1 Routing Protocols Derived from Ant Colony Optimization for Data Security in IoT (Liu 2017)

Routing which is of course most important part of network based on wireless sensors and has been in the eyes of the research groups for quite a few years. Routing derived from ant colony is a kind of broadcast methodology which has various characteristics. There are various kinds of chapters that give and relate routing protocols from various views, but the assessment on ACO derived routing is still not there. This chapter makes an effort to provide a detailed review on these routing protocols which is based on ACO. First we give a detailed report on what these algorithms are and what are their functions and further classify them. Second we find the best suited ACO based protocols and describe them in detail for further analysis.

Types of ACO Inspired Routing in WSNs

These algorithms are of various types. In this part, we give a comprehensive distribution of protocols which are mainly based on ant colony. The classification is given from different perspectives and is as follows.

Behavior of Operation

The ACO derived protocols are mainly of two types which are direction-finding of Energy Level Manage and Transmission Distance Manages. The above two types can be used depending on the type of behavior the operation has.

Main Aim

Based on the key objective, the routing protocol can also be separated into types which are Routing of life span addition and QoS requirements. The main objective of the first one is to increase the network duration, whereas the other aims at providing special QoS services.

Topology of Network

In the first type that is flat routing every node does the same work of path finding. Whereas in the other type that is Hierarchical routing many nodes are grouped to form clusters and path finding is carried out within these clusters.

Probability Transition

Based on the protocols of transition probability of ants, this type was derived and thus we say that it can be classified into two types Pheromone based and Heuristic based with only one pheromone. The first type the path finding is done by jointly pheromone trail and heuristic information.

In this case study the author gave a detailed investigation based on any colony protocols. We have also made a distribution on the bases of these protocols. We have efficiently analyzed a good number of protocols based on ACO.

9.4.1.2 Ant Colony Approach to Solve Travelling Salesman Problem (Beckers et al. 1992; Bolondi and Bondanza 1993)

Here the chapter state ant colony capable of clearing famous travelling salesman problem. Ants of the artificial colony are made so that they make successively smaller tours which are feasible also by using the information which is gathered by the deposits on the sides of the TSP graph. The machine then give the ant colony is worthy of making good choices. These methods are an example much like the wireless networking protocols, network involving neural and competitive coding of the hopeful use of this symbol to design algorithms for the optimization.

Ant Specific Algorithm

In this type of algorithms artificial ant is like an agent which goes from one city to another on a TSP graph. It then decides on which city to move by using a probabilistic function which can used or given by both trail gathered on edges and of a heuristic value, which was selected to be like a function of the edges which determines the length. Artificial ants mostly prefer going to cities that are well attached by edges with a lot of pheromone trail and which are close by. Firstly, 'n' artificial ants are located on randomly picked cities. Each one at a given point in time step move to different cities and changes the pheromone trail on the edges which can use this to termed local trail from updating their locations. When all the ants have at least done one tour the ant that made the shortest tour has the right to change the edges belonging to its tour termed global trail changing by the addition of amount of pheromone trail that is inversely proportional to the length of the tour.

The result obtained when these problems were tested and chosen mainly because there is a huge amount of data available to us in order to compare these results with historical. In the above case study, we compare the historic results which were either gathered from the bio inspired methods of the past and compare it with our new methodology. We find that our method is much more suited for solving NP hard problems and the famous travelling salesman problem as it is much more efficient to obtain the pheromone trail count or for that fact heuristic count to get the desired results. The key difficulty is to know the effective illustration for the problem and have an appropriate solution to it. In the experiments represented in this chapter local optimization was only used to enhance on the best results which we got from the various algorithms.

9.4.2 Genetic Bee Colony (GBC) Algorithm (Alshamlan et al. 2015)

Bee Colony Algorithm is an intelligence method (swarm) in which we select a gene hybrid method, which is GBC algorithm. The algorithm makes use of Genetic Algorithm in combination with use algorithms such as the ant colony algorithm. The

main aim which is focused is to combine the pros and benefits of both algorithms. A microarray gene expression profile is tested by applying this algorithm in order to obtain the gene which is the most predictive and gives more information for classifying cancer. For testing the accuracy and the performance of this algorithm, various experiments were also conducted. Three different binary data sets for a micro array were used, which consists of: leukaemia, lung and colon. Further, three different microarray datasets belonging to different classes were used, namely: leukaemia, SRBCT and lymphoma and then the results of the algorithm is also compared with the recently used technique. GBC algorithm was compared with various other algorithms which are closely related and that have been published recently with all the necessary datasets.

Below section illustrate the different case studies related to Genetic bee colony algorithm.

9.4.2.1 Bee Colony Algorithm Used for Data Security Using Routing System Protocols (Okdem et al. 2011)

In case of a fire, a very quick decision is required as every second counts in a condition where a factor such as low visibility, high anxiety and low environmental familiarity exists. The models for fire evacuation routing that are existing further involves the use of various bio inspired algorithms like the ant colony algorithm or else the swarm algorithm, which can also analyze the latency and calculate the delay caused due to congestion during process of evacuation properly nor can it determine the best desired and best suitable layout consisting of signs indicating guidance to emergency exit; henceforth, bee algorithm is used and is thus expected to be able to solve this problem. It objective is to create and develop a model for fire evacuation for routing called the "Bee-Fire", using bee colony algorithm for testing the model of routing. Bee-Fire is used for finding the optimal routing techniques for fire evacuation hence reducing the time of clearance and the net time for evacuation.

Fire Evacuation Routing and Artificial Bee Colony Optimization (BCO)

Fire evacuation is the process of movement from a dangerous place to a secure and a safer place. It is characterized into the following three phases: 1: validation of cue phase, 2: phase of decision-making, and 3: phase for refuge. The first phase and second phase are also called the pre evacuation phase whereas the refuge phase is called termed movement phase. The pre evacuation phase involves more decisions on survival than their actual movement. Decision should be made in a timely manner but in many situations evacuees get confused to follow a path. The main pattern in studying evacuation involves methods based on optimization that help creators to prepare evacuation plans with the help of various tools like scheduling model for optimization, routing models for optimization and network models for optimization. Evacuees use routes that they are familiar with. Table 9.1 discuss the evaluation of research in the field of human behavior in situation of a fire evacuation process.

Table 9.1 Evaluation of research in the field of human behavior in situation of a fire (Butler et al. 2017)

Factors considered during analysis of evacuation of a building	Methods used
Spirit of the times	Occupancy density and travelling speed are the two major factors. The latest factors including individual personality, per-son to person capacities and architectural design of buildings were also considered
Velocity of movement	Methods/ways used for documentation of the time required for purpose of movement were discussed
The link to fire and human behavior	This factor told that size/area of fire is dependent on the behavior of a personnel prior to or after commencing.
	The human behavior factor also came under discussion resulted that people pass through smoke to save other family members during escape.
Evacuation of the functionally impaired	Tall buildings were a key area of research during the phase of fire evacuation.
	Two methods are there: (1) proper use of lifts and elevators, (2) the strategy of defend-in-place.
Studies regarding WTC/11	New and special factors were discussed here i.e. the flow rates in staircases, times for escape and pre-evacuation, pre-evacuation actions
Time prior to evacuation	It is found that time for pre evacuation is far away more significant as compared to movement to a safe and a secure place.
	It is found that a delay in escape and count of deaths are interrelated.
Model for evacuation	Evacuation simulation models were designed which later on emerged. A few of them were based on the behaviour of human during evacuation, focusing only on the ways and the time required to interpret data being documented
Finding ways during evacuation	Conduction of case studies is a very important way as an approach.
	Spatial connections, architectural designs, and layouts are marked, that they generate some unnecessary problems to the occupants.

As illustrate in Table 9.2, respondents who participated in the survey consisted of more females than males. A large portion of these respondents belong to age group between 19 and 30 years, followed by age group of 31–50 years. Both the groups that are below 18 and between 51 and 70 have around same number of respondents i.e. (10% or 9.7%). The educational levels were subdivided into 5 groups consisting of secondary/high school, pursue diploma, pursue a degree, pursue masters, and pursue doctorate. Most of these respondents 63.1% have completed their education(higher) with degree, followed by around 12% of them completing diploma, 10.7% doing masters, 8.7% doing secondary school or lower, and remaining 5.8% doing doctorate.

Table 9.2 Demographic profiles of respondents (Olander et al. 2017)

Demographic characteristic	Frequency	Percentage
Gender		
M	45	43.7
F	58	56.3
Age group		
Below 18	10	9.7
Between 19–30	66	64.1
Between 31–50	17	16.5
Between 51–70	10	9.7
Educational qualification		
Secondary/high school	9	8.7
Pursue diploma	12	11.7
Pursue degree	65	63.1

Bee Colony Algorithm and Applications

Bee colony in the form of swarm intelligence which are inspired by bee collective intelligence for honey bee collection was used to overcome the limitations in traditional techniques of optimization. BCO algorithm involves the functions of honey bees so that it can find nectar locations around their bee hives, where they communicate via waggle dance. BCO algorithm has an advantage over other algorithms that it involves multiple control parameters. Bees can be grouped as socially linked insects which stay together in their colonies in the form of a dynamical system. The two essential components in a bee system are food sources and for agers. The food source value depends mostly on factors like its concentration of energy, closeness to the hives, richness, and the ease of extraction, but its "profitability" is generally given by the amount. Foragers are also categorized into three different groups (a) employed, (b) unemployed foragers, and (c) experienced.

The unemployed ones are responsible to look out for sources of food for exploiting. Scouter and onlooker's bees are the two types of bees which are unemployed ones. In this algorithm, half of the bees belonging to the colony are used as either employed and the other half are onlooker bees.

Finding Fire Evacuation Route Using BCO Algorithm

BCO algorithm helps in solving complex problems involving optimization and each of the artificial bees are responsible for generating at least a solution for a given problem. The position of food source near the bee hives gives a solution, which is potential and the amount of nectar reveals something about the quality, exactness and fitness regarding the solution. This algorithm works by assuming that most of

the bees (around 50%) in the bee hives are of onlookers category and other 50% are of employed bees category.

Also, it is assumed that the total population of onlooker bees and employed bees gives the total number of solutions. Initially, BCO algorithm creates a random distributed population solution which gives the position of food source. Each solution zi is a Dth -dimensional vector where D is number of products of input and cluster size for each and every data set. After initialization process, the positions population undergoes repeated cycles represented as one of the search processes formed by the three types of bees. The scout and employed bees choose their food sources randomly with same probability of each and every food source or the route of fire evacuation. Onlooker bees choose the food sources which are based on the probability which is proportional to the nectar amount in the food source.

Optimal Routing Solution for Fire Evacuation

This algorithm finds probability for every such possible solution for routing, which tells about the loyal nature of a bee which is employed towards a particular source of food. The solution having the least probability value is taken as the most close or the near fire evacuation route and an optimal one. The evacuees can escape from any emergency exits and need not select a path for the emergency exit having the smallest distance.

The result was obtained through a model for fire evacuation routing "Bee-Fire" developed by applying some ABC algorithm for finding optimal fire evacuation routes for evacuees; hence reducing total time for evacuation. The model can further determine the best location for emergency exit guidance signs. One limitation is regarding that the software do not simulate the levels of emotions and evacuees reaction during fire hence requiring updating. Another disadvantage is regarding the volume exclusion effect which is not guaranteed according to the model. Also, the model is verified without the use of real human experiments and relying on enforcing people choice for routes which is very difficult to get in real life. It is advised to take into account factors such as the behavior and nervousness level of evacuees in case of a fire to make the simulation look more accurate.

9.4.2.2 Dependable Data Gathering in IoT Using Bee Colony (Najjar-Ghabel et al. 2018)

The Internet of Things (IoT) technology helps and allows local users (devices) to converse with one other for sharing, preparation and meeting, hazardious warnings and some crucial information with no any human interference.

In the case of emergency applications in IoT technology, an important aspect is to provide an suitable method for gathering data. The proposed solution in the approaches that are existing is based on construction of a spanning tree over the IoT devices and collecting data using the tree.

The disadvantages of these algorithms are that they do not take into account or consider the probability of device's mobility or failure. These trees are arranged and are based on the desired preferences and are then later used for gathering data in succession. Each and every tree is a employed one and used for gathering data by splitting the preceeding one.

The studies are divided into two different groups. The first group consists and involves algorithms regarding routing, among the devices, that have not used a tree structure. The approaches have considered energy efficiency and reliability as measurements. One more category is based on a scheme based on tree building approach, which acts as a backbone for data tree transmission to the base main station in systems of IOT.

The Proposed Model

The IoT principle is displayed as a graph of undirected nature denoted by G = (Vertex, Edge) where Vertex, represent the collection of nodes containing the devices used and the base main station, and Edge denotes links which are there between the nodes. Every node ni has two of the main properties:

pi: Devices are moving in a random motion. The probability of mobility of the IOT devices can be found out based on their past records. The probability of mobility of ni, given by pi is a random number belonging to the range of [0,1]. This probability of base main station is set to null or 0 which tells that the mobility of the node is assumed to be 0.

ei: The variable gives the idea of residual energy of ni. The energy value of the base main station is considered to be infinite.

This algorithm is based on the construction of a spanning tree over the network. The spanning tree tk, has a feature namely mpk given by:

mpk: the mobility probability of internal nodes. The algorithm uses the most resident devices that are selected as internal nodes for increasing the reliability of trees.

Reliable Spanning Tree-Based Data Gathering in IoT

It includes the approach consisting of tree construction which are reliable in IoT systems. The algorithm creates a set of spanning trees that are reliable to gather data. Firstly, data gathering is carried out on the most suitable tree and it is operational until the devices which are internal lacks energy. It leads to the process of tree splitting and further interruption of data gathering. Therefore, the next most suitable and reliable spanning tree will be used next. This continues till all trees have been utilized and employed.

Here the author discussed the problem regarding gathering data that is reliable in IOT systems. Our algorithm that has been proposed, namely RST-IOT uses a struc-

ture of a tree for carrying out collection of data. In order to achieve the desired solutions with throughput being high, we modified the ABC algorithm leading to construction of a tree problem. The advantage regarding this is related to the fact that a swarm optimization algorithm which generates and results in many near-optimal trees. The amount of nectar in each and every solution is found using a few number of metrics such as residual energies of the devices, the number of hop distances count between various devices and base station, and the probabilities of their mobilities. A number of spanning trees are generated using the ABC algorithm. The trees are sorted based on the respective preferences and each of them is used to gather data. The results of simulation indicate that RST-IoT algorithm is superior to other approaches used in many terms such as reliability and consumption of energy. Hence it is a suitable way in handling emergency applications in IoT technology.

9.4.3 Firefly Algorithm (Yang 2008)

The firefly algorithm (FA) is an algorithm inspired by nature which depends on the fireflies and their behavior of flashing. This algorithm is inspired by various features of fireflies. They produce a clipped and pulsating flash which attracts their mate partners thus serving as a mechanism or tool for protective warning. Firefly Algorithm utilizes and formulates this lightning behavior of lightning bug.

The swarm of fireflies helps to solve the problem in an iterative way. The fitness value helps in giving information regarding the attractiveness of each member participating in the swarm. It is represented in terms of light intensity. The fireflies involved are firstly dislocated and further each and every firefly needs to find their mate depending on attractiveness of the rest of fireflies. They further approach their partner for improving condition and fitness. The performance is improved with the help of the F-Clust algorithm. A firefly is allowed to proceed towards its mate only if there exists a scope of improvement in the intensity value.

9.4.3.1 Analysis of Performance Using Firefly Algorithm Used for the Purpose of Data Clustering (Banati and Bajaj 2013)

A very important technique which is being used these days for organizing information and data is called clustering. The problem of clustering refers to the process in which partitioning of data objects that are unlabeled, takes place into a number of clusters with aim to maximize homogeneity within the clusters as well as heterogeneity between clusters. The algorithms performance obtained is made to compare with PSO algorithm and DE algorithms in terms of statistical criteria which make use of various data sets.

It is difficult to discover and extract relevant information due to the larger growth of data and information due to the popularization of web. The information extracted is based on the desired results of methods which are used to represent, organize and

access information at a same time. One such method used is clustering in which organizing of data takes place which facilitates the process of extraction of information (relevant). The problem of clustering involves the partitioning of data objects that are unlabeled into limited clusters. As the aim of clustering is focused at achieving homogeneity among clusters and then achieving heterogeneity among clusters, secondly and this task of the algorithm is defined as the optimization problem.

FA is generally a nature based inspired (bio inspired) approach used for solving of optimization problem which are nonlinear and which has been introduced recently (Yang 2008). It is based upon the physical related behavior socially related insects (fireflies) where each of the fireflies have their own purpose, agenda and coordinate values with respect to the various similar or dissimilar fireflies in that group in achieving the same as shown in Fig. 9.1.

A new and modified clustering approach for formulating the flashing/lightning behavior displayed by fireflies which are having the clustering problem's objective function.

The study has helped in calculating the performance of FClust algorithm in terms of accuracy and efficiency by carrying out comparison between the results of PSO and DE. Python language is used for the execution of algorithms and the other activities are carried out on a personal computer (PC). The effectiveness and its impact are calculated using following criteria:

(i) The value of best mean fitness
(ii) Success Percentage
(iii) Hoose and Stutzl (2004) proposed run length distribution (RLD).

Analysis of Performance

These analyses are done for getting better performance of the used algorithms and can be generally be divided in to the following types.

Using Artificial Data Sets

The value of mean best fitness is found using artificial data sets and is carried out for 20 runs for analysis as compared with the artificial data sets are reported and recorded in tabular form and then compares the results with that of PSO and DE algorithms.

Using Real World Data Sets

The values of mean best fitness is carried out for 20 runs for the analysis as compared to the bench marked data sets are reported and recorded which are further calculated for each data sets such as that of irises.

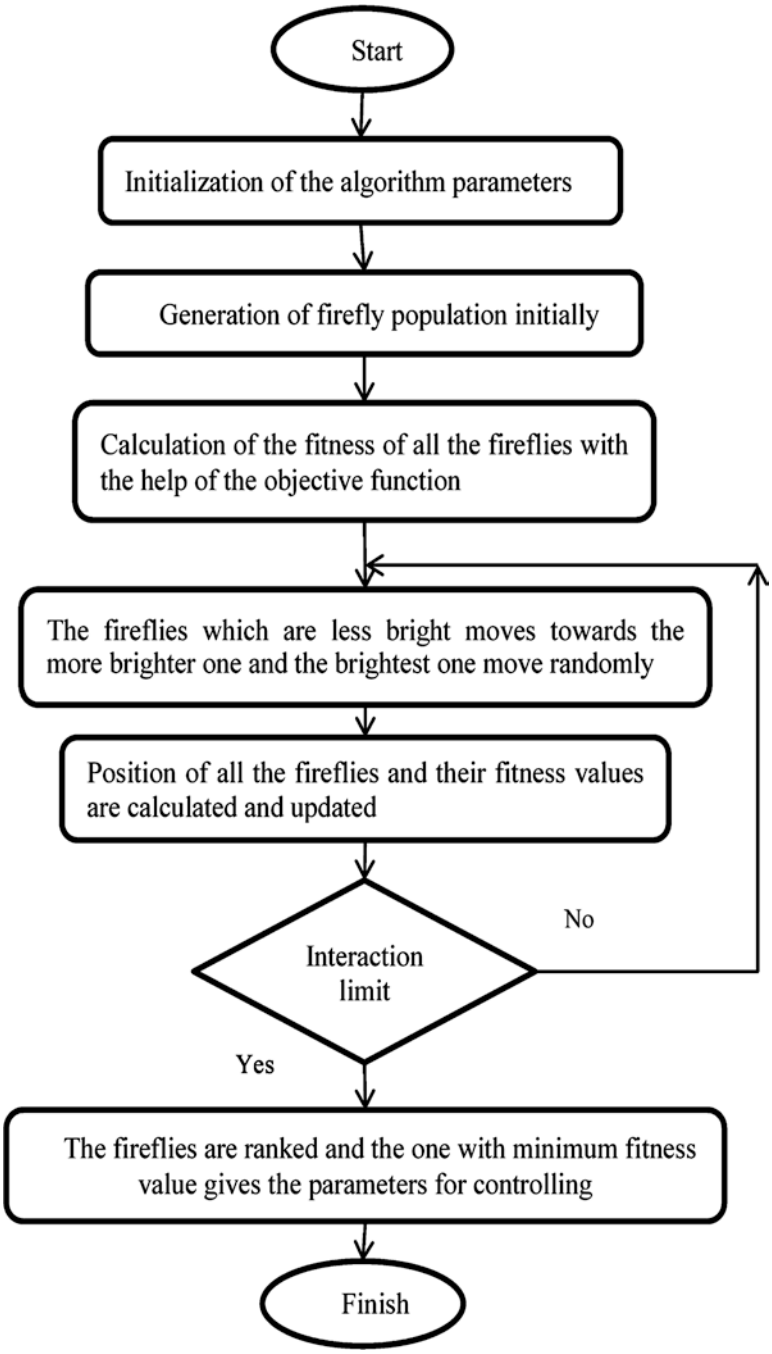


Fig. 9.1 Firefly algorithm flowchart (Yang 2008)

Percentage of Success

The rate of success in given as percentage of the number of runs, which gives the best value for the objective function carried out over 20 simulations.

The result shows that the algorithm used in clustering called, FClust is responsible for dealing with the firefly algorithm and its behavior in order to improve and modify the existing solution to the given problem occurring in clustering. The performance of FClust is calculated by using the result obtained by the comparison between PSO and DE with the help of various datasets. The experimental study has proved that FClust algorithm is having a probability higher than algorithms such as PSO and DE in achieving optimality.

9.4.3.2 Security System for Image in IoT with High Performance (Alam et al. 2013; Suwetha et al. 2017)

Exchanging image and video has become nowadays, one of the most important requirements to be used in the era of IOT. A Quad rotor is an application of IoT. In this type of rotor, images can be captured with Secure Digital Camera. After capturing of images, it is shared with the users who are intended, with a lot of security measures. It is achieved by using a technique of image hiding where an image which is secret is made hidden into another image (cover). After embedding and inserting the former image, the latter image will only appear. It is proposed for integrating and combining several algorithms with SDC for achieving security and long ranged transmission of images that are captured successfully. The algorithm used for integrating with SDC is called firefly which is used for hiding images. Thus an attempt is made to eliminate the concerns regarding privacy and security with the use of the integration of hybrid algorithms with SDC.

Methodology

Images that are captured in SDC have to be further transmitted with a lot of security for carrying out long ranged transmission; it is achieved by the integration of algorithms which are hybrid, with SDC like the firefly algorithm used for image hiding.

The algorithm that has been proposed offers protection as a two layer consisting of encryption and hiding images, which is responsible for covering issues that are related to domains such as security purpose, privacy of users and management of digital rights (DRM). The novel contributions are:

- Quality of the image is improved
- During the process of image hiding, less memory and space is acquired
- Peak signal, which is high and a noise ratio (PSNR) is being achieved here.
- Reduced Noise is attained for hidden image.
- Mean Square Error (MSE) is acquired.

- Lossless compression is implemented.

Henceforth, the SDC with the various hybrid algorithms is considered the most suitable and proved ways for facilitating the management of rights in the real time and is considered to be successful for applications in real time such as IoT.

Image Hiding Using Firefly Algorithm

The FA is basically an iterative technique in which the system which is proposed results or infers a new domain of frequency FA which depends on technique involving image hiding. The key idea involved in the technique is a two-fold idea: representation of image in multi resolution and odd-even quantization. The secret image is inserted into an another image called the cover image by the method of odd-even quantization for modifying the coefficients. Secret image is further encapsulated into the cover image with the help of a key image.

Process of Hiding Images

The two images, cover and secret images are categorized and divided into several 8×8 size non overlapping blocks. Each iteration involves finding an optimum location by the firefly algorithm and then the position of each firefly is updated. The most suitable location is found in the occurrence of certain conditions given below:

- When the performed number of iterations exceeds the maximum desired iterations being carried out.
- When there exists no any improvement obtained in the carried out iterations.
- A desired, acceptable and suitable result is found.

The secret image blocks are embedded in the most suitable possible pixel of every cover image block present and histogram shifting method is used for this purpose.

The histogram denoted by H(x) is generated. The maximum intensity pixel is also known as the peak point while the pixel with minimum intensity is also called zero point which can also be found using a histogram denoted as H(x). Peak/highest point of image block which is secret is inserted in the peak point of the second image block called the cover block. In a similar way zero point of a secret image block is inserted into zero or the null point of the cover image block.

After the completion of this process, SSIM (Structural Similarity Index Measure) is calculated for cover along with the embedded image. After this the BER value is analyzed and calculated. The SSIM describes the quality of embedded image. The Bit Error Rate (BER) gives information about how much robust an embedded image is. The BER value is between 0 and 1. If it is nearer to the value of 1 then the value of error for the extracted image is found to be higher. The sole purpose of the process is minimizing the BER and to maximize the SSIM ratio.

In this section, the author has developed hybrid algorithms which are implemented here with SDC accomplished in the work has successfully been done for carrying out image hiding, compression, long ranged communication and encryption efficiently. The algorithms have been classified and analyzed in reference to the parameters for evaluation of performance. The parameters used here, displays that the concerns in privacy as well as security in secured transmission of data could be obtained well as shown in Fig. 9.2.

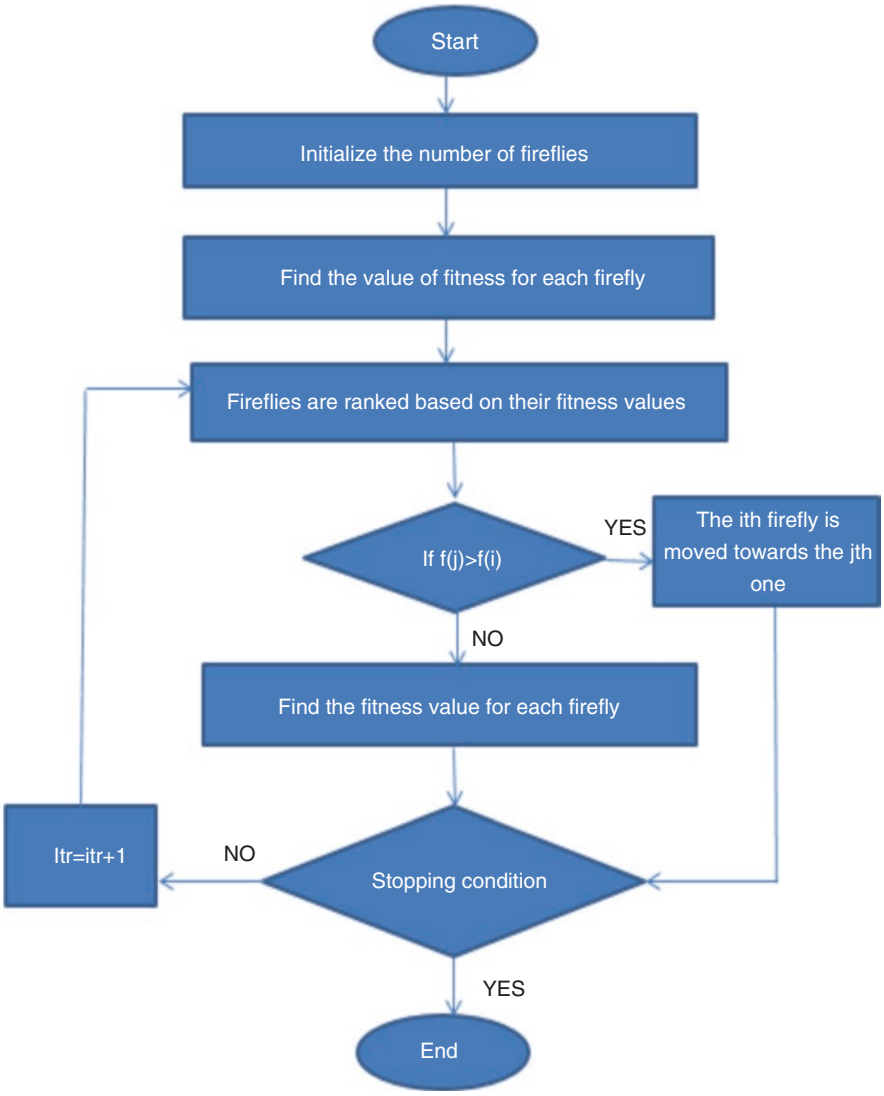


Fig. 9.2 Flowchart displaying the image hiding process (Okdem et al. 2011)

9.5 Conclusion

This chapter presented the work in the field of data security in IoT using bio inspires techniques, based on the behavior study of living organisms found in the nature. Subsequently it also illustrates algorithms used to solve real world problems in the case of data security in IoT. As mentioned in the chapter, the ant colony optimization algorithm is used to solve instances in data security in IoT such as routing protocols in wireless sensor devices which can be extended to various applications in this world through IoT. Also, ACO is used in TSP i.e. travelling salesman problem, which benefits the salesman in his sale.

Similarly, artificial BCO algorithm is used in solving issues related to evacuation system in case of fire. As very less time is present to make a decision in the case of a fire occurs. To overcome this issue ABC algorithm is used in helping the evacuees to find the best optimal path for the emergency exit. In later case studies ABC algorithm is used in gathering data for the internet of things.

Finally, firefly algorithm uses the flashing characteristics of the firefly in solving problems such as performance analysis for data clustering and a high performance security based system for an image.

The above algorithms mentioned and discussed along with the case studies involved gives a supporting hand for the cause of achieving data security in Internet of Things with the help of biologically inspired computing techniques. The mentioned case studies thereby prove that bio-inspired computing can be used as a option of better solution for security in IoT.

References

Alam, B., Doja, M. N., Alam, M., & Malhotra, S. (2013, September). Security issues analysis for cloud computing. *International Journal of Computer Science and Information Security, 11*(9), 117–125.

Alshamlan, H. M., Badr, G. H., & Alohali, Y. A. (2015). Genetic Bee Colony (GBC) algorithm: A new gene selection method for microarray cancer classification. *Computational Biology and Chemistry, 56*, 49–60.

Banati, H., & Bajaj, M. (2013). Performance analysis of firefly algorithm for data clustering. *International Journal of Swarm Intelligence, 1*(1), 19–35.

Banu, R., Ahammed, G. A., & Fathima, N. (2016). A review on biologically inspired approaches to security for Internet of Things (IoT). In *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*. IEEE.

Beckers, R., Deneubourg, J. L., & Goss, S. (1992). Trails and U-turns in the selection of the shortest path by the ant *Lasius niger*. *Journal of Theoretical Biology, 159*, 397–415.

Bello, O., & Zeadally, S. (2014). Intelligent device-to-device communication in the Internet of Things. *IEEE Systems Journal, 10*(3), 1172–1182.

Birattari, M., Pellegrini, P., & Dorigo, M. (2007). On the invariance of ant colony optimization. *IEEE Transactions on Evolutionary Computation, 11*(6), 732–742. https://doi.org/10.1109/TEVC.2007.892762.

Bolondi, M., & Bondanza, M. (1993). *Parallelizzazione di un algoritmo per la risoluzione del problema del commesso viaggiatore*. Masters thesis, Politecnico di Milano, Italy. Croes, G.A.

Butler, K., Kuligowski, E., Furman, S., & Peacock, R. (2017). Perspectives of occupants with mobility impairments on evacuation methods for use during fire emergencies. *Fire Safety Journal, 91*, 955–963.

Dorigo, M., & Birattari, M. (2011). Ant colony optimization. In C. Sammut & G. I. Webb (Eds.), *Encyclopedia of machine learning*. Boston: Springer.

Dorigo, M., & Di Caro, G. (1999). Ant colony optimization: A new meta-heuristic. *IEEE*. 2. 1477 Vol. 2. https://doi.org/10.1109/CEC.1999.782657.

Liu, X. (2017). Routing protocols based on ant colony optimization in wireless sensor networks: A survey. *IEEE Access, 5*, 26303–26317.

Najjar-Ghabel, S., Yousefi, S., & Farzinvash, L. (2018). Reliable data gathering in the Internet of Things using artificial bee colony. *Turkish Journal of Electrical Engineering and Computer Sciences, 26*(4), 1710–1723.

Okdem, S., Karaboga, D., & Ozturk, C. (2011, June). An application of wireless sensor network routing based on artificial bee colony algorithm. In *2011 IEEE Congress of Evolutionary Computation (CEC)* (pp. 326–330). IEEE.

Olander, J., Ronchi, E., Lovreglio, R., & Nilsson, D. (2017). Dissuasive exit signage for building fire evacuation. *Applied Ergonomics, 59*, 84–93.

Perumal, T., Sulaiman, M. N., Datta, S. K., & Leong, C. Y. (2016). Rule-based conflict resolution framework for internet of things device management in smart home environment. In *IEEE global conference on consumer electronics*.

Sari, I. R. F. (2017, October). Bioinspired algorithms for Internet of Things network. In *2017 4th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)*. IEEE.

Suwetha, K., Vinothini, K., & Shankar, R. (2017). High performance in security system for image in IoT. *International Journal of Engineering Development and Research*, 501–507.

Xu, L. D., He, W., & Li, S. (2014). *Internet of Things in industries: A survey*. *IEEE Transactions on Industrial Informatics*.

Yang, X. S. (2008). *Nature-inspired metaheuristic algorithms*. Beckington: Luniver Press.

Chapter 10
A Chaos-Based Multi-level Dynamic Framework for Image Encryption

Sakshi Dhall, Saibal K. Pal, and Kapil Sharma

Abstract Large scale internet and mobile usage has led the world witness ubiquitous increase in data transfer requirements as well as nature of data in transmissions on insecure networks. Internet of Things (IoT) has given an altogether new dimension to security challenges required to be addressed in the emerging world of smart cities specially with respect to data which is not necessarily text based and is magnanimous and requires to be processed in environments with adaptive needs. Images form one such type of data which forms significant proportions of modern day transmissions and is also equally significant when it comes to data being generated by devices including mobile phones, IoT devices like smart bells, surveillance devices, CCTVs etc. specifically when operating in environments requiring adaptability to dynamic changes in security requirements in balance with resource availabilities. Traditional schemes with proven security like AES use static operations involving significant computational expense and are suitable for securing textual data but no such standard exists till date for securing media like images. Since, images are bulkier and contains significant correlation in neighbourhood so there is a need to design new encryption approaches going beyond the conventional static encryption paradigm, hence, in this chapter we propose a paradigm shift opposed to the static approach for encryption.

This chapter proposes a chaos-based, multiple-round, adaptive and dynamic framework for image encryption with new levels of dynamism across different functional dimensions of the entire encryption process. The impact of the new levels of dynamism across the entire encryption process has been experimentally demonstrated. Observations and results show that such framework can be used to address

S. Dhall (✉)
Department of Mathematics, Jamia Millia Islamia, New Delhi, India

Department of Computer Science & Engineering, Delhi Technological University, New Delhi, India

S. K. Pal
Scientific Analysis Group, DRDO, New Delhi, India

K. Sharma
Department of Information Technology, Delhi Technological University, New Delhi, India
e-mail: kapil@ieee.org

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_10

dynamically changing encryption requirements and resist higher levels of cryptanalysis because the proposed dynamism of the framework makes it difficult for the attacker to identify and estimate the structure and operations of the encryption process to perform cryptanalysis.

Keywords Image encryption · Multimedia · Chaos · Dynamism · Adaptive · Dynamic framework

10.1 Introduction

Improvement in price-performance ratio of microelectronics technology has given a strong impetus to what we call as digital revolution. Digital information has found its inevitable presence in almost every sphere of life from military to medical science, banking to e-commerce, education to entertainment, tourism to social media to space exploration etc., and the list is endless. The digital technology has no doubt proved to be a marvel in its contribution to the kind of communications possible in today's world but it has also paved way for serious possible breaches when sensitive information is stored or shared through susceptible channels.

With the offshoot in mobile technology and internet becoming more and more permeant part of our everyday lives, the magnitude of available digital data and the need for voluminous information transfers have increased enormously. Applications like financial transactions, VoIP, medical and military imaging, social networking, real-time streaming, pay-TV, video conferencing etc. have resulted in bulk data exchanges to become indispensible for our professional and personal activities. These data exchanges may include copyrighted and confidential information exchanges including multimedia esp. images (Furht 2005; Gonzalez and Woods 2007) making it highly important to have impenetrable channels and safe end points so that digital data transfer and storage happens in a secured way.

As security of digital content impacts diverse sets of people ranging from large business houses to defense establishments to space research organizations to health care sector to entertainment industry to individuals and so on, it is imperative to equip all information generating and transmitting systems with appropriate data securing capabilities. This will ensure that the communicating parties feel safe and secure while exchanging confidential information over otherwise penetrable networks thereby providing them an ease and confidence in carrying out the required communication. Cryptographic techniques (Stallings 2004; Menezes 1996) like encryption play a vital role in securing confidentiality of sensitive information by converting them into non-perceivable forms thereby ensuring that any attempt of unauthorized access does not disclose any meaningful information to the adversary. Encryption refers to the process in which the meaningful plaintext is converted to the cipher text (non-perceivable form) using key and the reverse process of obtain-

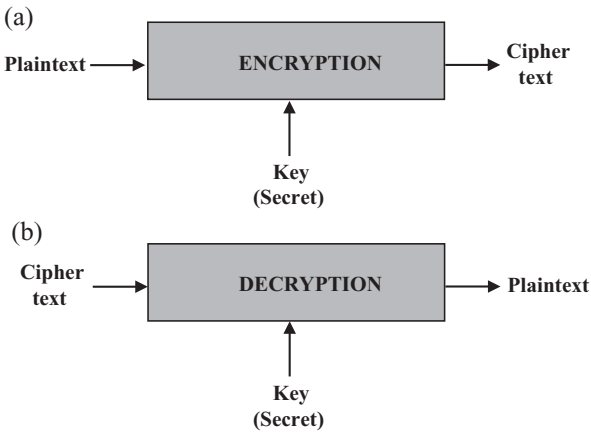


Fig. 10.1 (**a**) Basic encryption process. (**b**) Basic decryption process

ing back the plaintext from the cipher text is referred as decryption. Figure 10.1 shows the basic encryption and decryption processes in symmetric-key cryptography.

As evident, the digital data being mentioned is not restricted to textual content anymore. It contains significant amount of multimedia of which visual content forms a significant core. In fact, multimedia like images, video etc. has emerged out as major sources of digital content prevalent in storage and on networks today. With the increasing multimedia applications trends, the area of multimedia security esp. image security is also evolving and its scope has widened. Some of the applications requiring security measures for different forms of visual information are:

- Images – forensics, defence maps, biometrics etc.
- Video – surveillance, live-transmissions (esp. for defence, embassies, policing etc.), video-conferencing, DTH, social media etc.

Further, with the frequent advancement in the area of Internet of Things (IoT) and machine to machine communication, the requirement of securing all forms of data including visual content like images have increased manifolds (Rohokale and Prasad 2015; Meskanen et al. 2015; Abomhara and Køien 2015; Elmangoush and Magedanz 2017). With the concept of smart cities becoming reality, intelligent IoT devices are required to securely communicate visual content like images with each other for various applications like surveillance, medical imaging, expert systems etc.

At the first look, it appears that the conventional techniques, designed for securing text, should in principle be directly applicable on any form of data but, this does not hold true in practice. The reason is that multimedia data like images, videos etc. have special characteristics, i.e. they are bulky in size and possess strong correlation among neighbouring data bytes. These characteristics were missing in textual data, hence, these characteristics do not get directly addressed in traditional encryption schemes (Stallings 2004) like AES, DES, IDEA etc. when used in native ECB mode. Figure 10.2 show the original standard gray-scale 'Water Lilies' image and the corresponding cipher image obtained by encrypting it using AES in ECB mode.

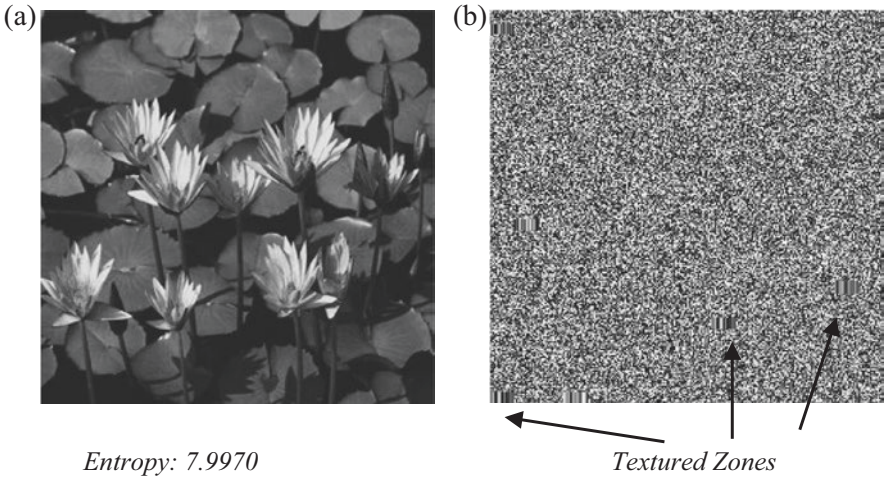


Fig. 10.2 (**a**) Original image (water lilies). (**b**) AES encrypted image (water lilies)

This clearly shows that the cipher image contains textured zones because the redundancy in the input plain image does not get completely removed after performing the said encryption. These textured zones acts as vulnerabilities and can be easily be exploited by the attackers.

Also, these traditional ciphers are static in their operations and secrecy is provided only by the private key. They largely rely on the mathematical complexity of the applied computations and secrecy of the key. They are computationally expensive and their static behaviour makes them susceptible to get broken, if not truly practically at least theoretically, when undergone significant analysis by the attacker (Phan 2004; Biryukov and Khovratovich 2009; Biryukov et al. 2009). Attacks are also proposed on AES family of cryptosystems even when used in, the otherwise considered secure, CTR mode (Biryukov et al. 2010). Also, in today's time, many applications require securing multimedia content like images in resource constrained environments like mobile phones (Paul and Irvine 2016; Herland et al. 2016; Ofori et al. 2016) and in such applications traditional schemes like AES will prove to be computationally more expensive.

Also, when it comes to communications of visual content including those by IoT devices, some applications have high security requirements while for others efficiency may be a more significant factor and hence, practically such devices are operating in environments with varying/dynamically changing security requirements as per the application needs and resource constraints at hand. Therefore, there is a need for encryption schemes which are adaptable based on the changes in the operating environment and changing security needs. Also, this idea of adaptability of encryption scheme is well aligned and will be well utilized with the dynamic AI capabilities supported in the upcoming 5G technology for modern day communications.

Though, there are several encryption schemes which have been proposed for securing multimedia including images yet there has been no encryption standard till date designed to cater to the special needs of multimedia content. In the light of traditional static standard schemes not being directly able to address security concerns for multimedia like images and absence of any image encryption standard, we feel strongly motivated to explore dynamic encryption as a paradigm shift for encrypting images. The approach can definitely be extended later to cater to other forms of multimedia as well. Introducing dynamism as part of the design of the encryption scheme does not take away the deterministic and reversible nature that every cryptosystem must possess. Despite offering dynamism in structure of the encryption process based on the key and also on the plaintext, the proposed work very well follows the Kerckhoff's principle according to which every cryptosystem should be secure even if everything else about it is publically known except the secret key. Also, introduction of chaos-based dynamism can ensure that without using intricate mathematical operations, the dynamic framework could provide high security itself. Statistical and cryptanalytic attacks will intuitively become difficult when the encryption algorithm is dynamically changing with change in key and/or plaintext. This argument can be made stronger by highlighting that cryptanalytic attacks are normally designed by identifying some weak operation or loophole within the design of the static encryption scheme and then it is tried to be cracked by exploiting the identified loophole to extract partial or complete information about the plaintext or key or both (Özkaynaka et al. 2012; Tu et al. 2013; Wang et al. 2013; Norouzi and Mirzakuchaki 2016). But identifying such loopholes in a dynamic cryptosystem will surely be much difficult as the adversary will not even be equipped with the complete knowledge of the structure of the cryptosystem itself, which, of course, will be dynamically changing. Thus, chosen/known plaintext attacks will not be possible on such encryption scheme involving dynamism.

In the following background section, a brief survey on existing subtle use of dynamism in encryption is also given. It shows that researchers have been suggesting use of dynamism in one form or the other as a means to enhance security of their proposed encryption schemes and to make it difficult for adversaries to attack. Extending the approach of dynamism, in this chapter, we propose a new chaos-based, multi-level dynamic framework for encryption using extendable 128-bit key and multiple rounds to encrypt images byte-by-byte.

New dimensions to dynamism have also been proposed in this work, which are not employed in the existing works. It is proposed that the number of operations performed per round of the encryption scheme be decided dynamically. Also, the sequence of encrypting pixels will also be dynamically decided. This is incorporated along with dynamic decision on the type of operations performed. This kind of multi-level dynamism has not been used in existing literature and it will ensure that structure of each round of operations dynamically changes in an unpredictable way. This is done with an objective to increase the level of difficulty manifolds for an attacker to perform cryptanalysis to break the cryptosystem. In absence of knowledge of the key, the attacker will be completely unaware about the number and

nature of operations performed in the different rounds thereby averting cryptanalytic attacks.

Also, as the type and number of per-round operations performed on the same pixel position will vary if the same key is applied with a slightly modified image hence proposed work will offer resistance against known/chosen plaintext attacks, differential and impossible differential attacks. Further, chaos has been made integral part of the framework to ensure high level of randomness in dynamism with less computational expense.

Chaos provides properties like high sensitivity to changes in initial conditions and control parameters, ergodicity, random-like behaviour etc. (elaborated in the next section) which are very well suited to meet the confusion and diffusion requirements (Shannon 1949) of any cryptosystem. Hence, chaos has been widely used in cryptographic applications for decades now. Though, some researchers also criticize use of chaos as it requires floating point number processing but this criticism does not stand much, as today's machines are well equipped to process real numbers with ease and efficiency. In fact, this very characteristic of chaos, i.e. playing with real numbers, actually possess great potential and makes it a strong contender to provide security solutions esp. for multimedia in post-quantum computers (Kartalopoulos 2010; Stojanovic et al. 2016; Geetha 2012; Akhshani 2015; Behnia et al. 2012; Akhshani et al. 2013; Ramos and Souza 2001; Ramos 2017). Further, it is to be highlighted that the proposed work is different from most of the other general chaos-based image encryption schemes due to its basic focus on use of chaos as a tool to generate dynamism in the encryption process, and not only as means to generate random sequences to be utilized in static permutation and substitution phases.

The organization of the rest of the chapter is as follows. The use of chaos and dynamism in encryption as a background study is presented in Sect. 10.2. Further, Sect. 10.3 details the proposed dynamic encryption framework for image security. In Sect. 10.4, security analysis and the obtained results are elaborated. Section 10.5 envisions the future scope and concludes the chapter.

10.2 Background

10.2.1 Chaos in Cryptography

Chaos (Devaney 1989) is a mathematical concept which offers special properties which can be well utilized in cryptosystems. Chaotic maps have non-linear dynamics, and they show random-like behaviour. They possess and show inherent avalanche properties as chaotic maps are highly sensitive to initial conditions and control parameters. Further, chaotic maps have high mixing property and ergodicity property which ensure that two initially very close points may get diverged after few iterations to points which are highly uncorrelated and the chaotic system uniformly

attains different possible states without quickly converging to fixed value(s). These properties of high sensitivity, ergodicity, randomness allow use of simpler and computationally efficient operations to design cryptosystems with chaos.

Chaotic maps may be continuous or discrete. The continuous maps can be generalized and discretized for application in encryption techniques. They can be used to generate random-like sequences which are normally utilized in key-stream generation, permutation and substitution steps of the encryption process. Due to ergodicity and the inherent avalanche property, the sequence generated by a chaotic function appears as a random noise with very small change in the initial conditions and/or control parameters. This adds to the unpredictability to the adversaries in absence of knowledge of the exact initial conditions and parameters. Further, as chaotic functions display deterministic behaviour therefore smooth recovery of the plaintext from cipher text during decryption is ensured.

Initially, 1-D chaotic maps were only used by researchers but vulnerabilities were identified. So, higher order chaotic maps like 2-D, 3-D maps have become popular choice of researchers, to ensure better security without compromising on simplicity of operations. Some of the well known chaotic maps include:

1D: logistic map, tent map, sine map.
2D: Baker's map, Arnold's cat map, Hénon map, Ikeda map.
3D: Lorenz System, Chen-Lee system.

Figure 10.3 displays sensitivity of a chaotic map namely logistic map with respect to the value of initial condition and parameter to the extent that highly uncorrelated orbits are generated by using the logistic map with same control parameter value i.e. set to 4 and minor change in the value of initial conditions i.e. x0 = 0.7 and x0 = 0.701. Both these plots represent the dynamics of the logistic map in terms of plots of 100 points obtained after skipping first 900 iterations to eliminate the transient effect (http://s3.amazonaws.com/complexityexplorer/NonlinearDynamics/Nonlinear.LogisticLabII.pdf).

In fact, researchers have also been proposing new, improved or hybrid chaotic maps (Zhou et al. 2014; Ramadan et al. 2016; Boriga et al. 2014; Zhang and Cao

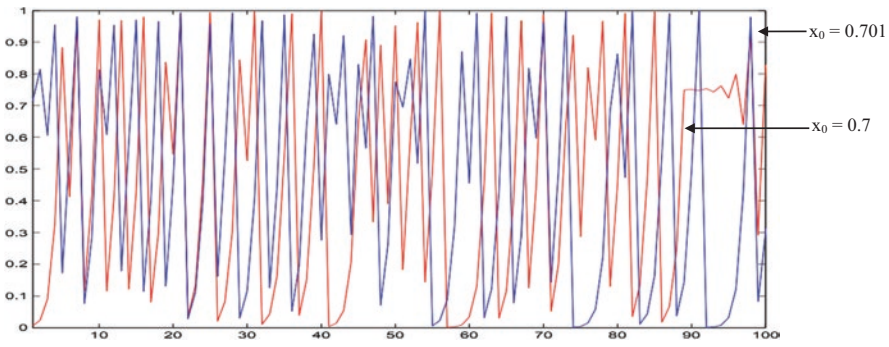


Fig. 10.3 Plots for Logistic Map with minor change in the value of initial conditions (control parameter value as 4)

2014; Elabady et al. 2014; Saraereh et al. 2013; Borujeni and Ehsani 2015; Maqableh 2015; Rui 2015) by making improvisations or by combining more than one chaotic map to enhance the chaotic behaviour of existing maps, like, making the new proposed maps which possess longer orbits, wider range of acceptable parameter values showing chaotic behaviour, higher randomness etc.

10.2.2 Survey on Dynamism in Encryption

Encryption process in any block cipher normally involves key-stream based permutation and substitution operations which are repeated over a number of rounds. There are various levels at which dynamism can be introduced in this encryption process like dynamism in encoding/decoding, dynamism in the number and type of operations used, dynamism in number of rounds employed, dynamically changing keys, dynamism during key-stream generation from the original key etc. Figure 10.4 pictorially represents these different components of the encryption process in a block cipher where dynamism can be introduced.

The roots of dynamism can be observed from polyalphabetic ciphers proposed as early as sixteenth century like Vigenere cipher where the idea to use of different transforms based on the secret key first surfaced. In 1984, S. Goldwasser and S. Micali (1984) proposed a new approach for encryption called Probabilistic Encryption. The authors highlighted that the traditional ciphers are deterministic trapdoor functions using secret information as trapdoor for security. And there exists a finite possibility that full or partial information about the plaintext may get revealed when attacked by adversary. To address this, the authors propose a proba-

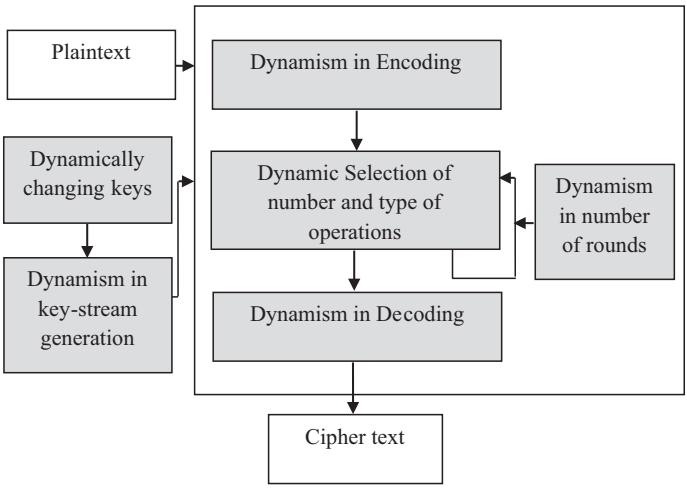


Fig. 10.4 Components of encryption process in any block cipher where dynamism can be introduced

bilistic framework replacing the static one. As per probabilistic encryption the same plaintext bit 0 or 1 could be encrypted in several encodings in the cipher text where a possible encoding is chosen through a random mechanism. It is evident that probabilistic encryption framework encourages dynamism in selecting possible encoding for the same message bits in the cipher text to make it tough for the adversary to attack.

In (Faraoun 2010) a stream-cipher structure is proposed and use of dynamism is proposed for generating chaos-based pseudo-random key stream being used to perform encryption. Pareek et al. (2005) proposed dynamism in deciding length of blocks, choosing one chaotic map (for encryption of the block) among four chaotic maps along with their initial conditions and the number of iterations made to the chosen chaotic map. Later, Wei et al. (2007) cryptanalyzed this work but did not criticize the dynamic approach, instead, they suggested improvements to strengthen the dynamism by making it plaintext-dependent besides being key-dependent. Such dynamism in choosing among multiple chaotic maps has been proposed in (Abuhaiba et al. 2012; Wang and Qing 2009; Sakthidasan and Santhosh Krishna 2011; Zhou et al. 2013; Vahidi and Gorji 2014) as well.

The papers (Ngo et al. 2010; Harmouch and Kouch 2015) proposed use of dynamically changing keys for encrypting different data packets of a communication so as to provide strength against cryptanalytic attacks by adversaries and to ensure that a compromised key do not reveal much information about the communication thereby not causing much harm. Several researchers (Cao 2013; Wang et al. 2015; Murillo-Escobar et al. 2015; Armand Eyebe Fouda et al. 2014a, b; Wang et al. 2016; Chai et al. 2017; Khan et al. 2017a, b; Ahmad et al. 2017) have taken the idea of dynamism in keys to another level by making keys used in the image encryption algorithm dependent on plaintext or using information extracted from the plaintext (like average intensity value, hash value etc.) and utilizing it in the image encryption operations thereby using this plaintext related information indirectly as the key which definitely needs to be communicated to the receiver along with the key for smooth decryption at the receiver's end. Communication of such plaintext related information in a secure manner to the receiver is required for smooth decryption. It can be done either by hiding such plaintext related information inside the cipher text itself (Cao 2013) or otherwise securely communicating it with the key, which is not always practically feasible especially in resource constrained environments.

Pareek et al. (2006) proposed a block cipher suitable for real time image encryption. The block cipher involves dynamism by making chaos-based selection of operations to be performed for encryption of each pixel of the image. In another work, Dhall and Pal (2010) proposed a 128-bit block cipher based on key-based conditional encryption. The algorithm comprises of two steps i.e. re-adjustment phase and substitution & shifting phase whose operations vary based on the key. This key-based conditional approach is then extended and adapted to make it suitable for multimedia in (Dhall et al. 2014). To suit multimedia, the block size is made customizable and three variants are suggested to ensure complete removal of redundancy in the cipher image. Later, Korstanje and Keliher (2015) cryptanalyzed the

scheme (Dhall and Pal 2010) by proposing distinguishing attacks and plaintext-recovery attacks for keys with certain specific characteristics but did not criticize the conditional nature of choice of operation as such.

Several encryption schemes like Blowfish (Schneier 1994), Twofish (Schneier et al. 1999) use key-dependent S-Boxes in the substitution step of the scheme. Key-based dynamic selection of S-Box for substitution is proposed in (Hussain et al. 2012; Anees et al. 2014). Further, papers (Khan et al. 2017b, c; Ahmad and Hwang 2015) proposed improvisations on the scheme proposed in (Anees et al. 2014). Also, several researchers in their works (Krishnamurthy and Ramaswamy 2008; Abd-ElGhafar et al. 2009; Subramanyan et al. 2011; El-Sheikh and El-Mohsen 2012; Juremi et al. 2012; Mahmoud et al. 2013; Pradhan and Bisoi 2013; Arrag et al. 2013; Dara and Manochehr 2013) have proposed use of key-dependent S-Boxes in the standard algorithms like AES and have demonstrated and proved the strength of introducing key-based dynamism in this form.

The idea of Dynamic Encryption has been discussed most explicitly by Knudsen in (Knudsen 2015) where it has been proposed that the while the performing encryption and decryption respectively at the sender's and receiver's ends, the receiver is kept unaware about the cryptosystem being used for encryption and only key is known to the receiver. The choice of cryptosystem being used for encryption is being kept to the sender who can change it as often as per message. To ensure smooth decryption at the receiver's end, the sender communicates the executable code for decryption or encrypted decryption algorithm to the receiver along with the cipher text. On receiving the decryption algorithm along with the cipher text, the receiver can decrypt the message using the known shared key. Knudsen proposes practical advantages of such dynamic encryption for email systems, cloud storage and mobile conversations. This idea has been extended in our present work but with a difference. Unlike dynamic encryption proposed by Knudsen (2015), in our work the dynamic framework itself takes care of offering key and plaintext dependent dynamically changing encryption operations for pixels while the receiver is fully aware of the decryption algorithm i.e. there is no need to communicate or send the decryption algorithm separately to the receiver. Following section 3 describes our proposal. The use of dynamism in choosing rule/method of encryption has also been shown in some more recent works including (Husni 2017; Gmira et al. 2019).

10.3 Proposed Approach

10.3.1 Description of the Proposed Framework

In this work, chaos has been primarily used to introduce random-like dynamism in the overall structure of the proposed framework. Each pixel is visualized to be composed of three parameters i.e. (x, y, color byte) and, as part of the encryption process, a new color byte value is to be generated for each pixel. To ensure complete

removal of redundancy existing in the plain image, besides these three parameters, each pixel is assigned a key-based 'chaotic value', where 0 < chaotic_value < 256. Hence, for encryption, each pixel has an additional parameter which is used in calculating pixel's counterpart in the cipher text. The encryption process uses operation look-up tables from which operations are selected dynamically to encrypt the pixels. The framework has three key features as stated below:

(i) The framework offers chaos-based dynamism at multiple levels during the encryption process.
(ii) Non-sequential data byte encryption is proposed to achieve faster diffusion results and to strengthen the encryption against known/chosen plaintext attacks, differential and impossible differential attacks.
(iii) The framework is also flexible and adaptive. The key sizes, the number and nature of operations in look-up tables, the minimum/maximum number of operations per round and number of rounds can be adjusted as per need so as to strike a balance between resource constraints and the security requirements.

As per the proposed framework, the different levels at which dynamism may be introduced using chaos include:

(i) Dynamism in choosing the number of operations performed per round.
(ii) Dynamism in choosing look-up table of operations.
(iii) Dynamism in selecting the operation from the chosen look-up table.
(iv) Dynamism in deciding sequence in which pixels are encrypted.

Clearly, new levels of dynamism have been introduced in this proposal, i.e., dynamic decision of number of operations performed per-pixel in different rounds and dynamic decision of the sequence in which pixels are encrypted. Very importantly, these decisions are made using chaos as it provides an easy means to achieve random-like dynamism with less computation. To elaborate, the additional chaotic value adds dynamism to the encryption operations applied as it can act as one of the deciding factors, along with pixel coordinates, for determining the look-up table. Further, from within this look-up table, an operation, to be operated on the pixel, is selected dynamically using chaos. Also, it is proposed to encrypt pixels in dynamically chosen non-sequential fashion, where the coordinates of the pixel to be encrypted is determined using chaos and previously encrypted pixel. Chaos is used to determine its x-coordinate while the y coordinate is calculated based on the value of the previous encrypted pixel value. For the first pixel, y-coordinate value is initialized to 0. In case the pixel at the generated pixel coordinates (x,y) is already encrypted in the current round of encryption process then the sequentially next pixel is chosen to be encrypted in its place. This way all the pixels get operated on in each round of encryption.

Clearly, the encryption of pixel bytes is not sequential and also the number and kind of operations operated on pixel values during multiple-round encryption process is also not fixed. Further, all this is decided with random-like dynamism using chaos, hence, there exists a large number of possible operation paths through which

a plain image pixel may pass before it gets transformed into corresponding cipher image pixel. As a result, even for the same key with a slightly modified plain image, the same pixel position gets operated upon by drastically different number and kind of operations. Thus, the proposed dynamic framework will offer high resistance against known/chosen plaintext attacks, differential and impossible differential attacks.

10.3.2 Description of Per-round Operations

Unlike conventional algorithms where the operations made per round are fixed and are same in each round, the proposed work provides a fixed basic framework for each round with flexibility to accommodate different number of different kinds of operations per round i.e. the number, type and sequence of operations performed per round varies across different rounds even for the same pixel. Besides the dynamically decided operations used to achieve confusion, a diffusion step is performed at the end of each round which diffuses the two halves of the intermediate cipher text with one another. This along with non-sequential byte encryption ensures that minutest change anywhere in the plain image gets diffused throughout the cipher image in subsequent rounds of the algorithm.

Following algorithm represents the per-round encryption rules as per the proposed framework:

ALGORITHM: Per-round encryption

```
INPUT: I (image), M (height of the image), N (width of the image)
1:  op_count = generate_chaos_based_per_round_op_count( );
2:  for i =1 to M*N
3:     (x, chaotic_value) = generate_chaos_based_dynamic_values( );
4:      y = (x * previous_encrypted_pixel) % N;
5:      if (is_pixel_encrypted(x,y))
6:         (x,y) = find_next_unencrypted_pixel_position(x,y);
7:      end if
8:      (op_table, op) = choose_op_table_and_op (x,y,chaotic_value);
9:       j = 1;
10:     C(x,y) = I(x,y);
11:       while (j d op_count)
12:         C(x,y) = C(x,y) op chaotic_value;
13:     end while
14:   previous_encrypted_pixel  = C(x,y);
15: end for
16: diffusion_stage( );
```

where,

$*$, % refers to the multiplication and modulus operation respectively,
op_table is the dynamically selected look-up table of operations chosen based on the pixel coordinates (x,y) and chaotic_value,
op_count is the number of operations performed (min<=op_count <=max), where min and max offers flexible limits to the number of operations performed per round
op is a dynamically selected operation from the look-up table op_table.

Figure 10.5 shows the per-round block diagram of the proposed dynamic framework.

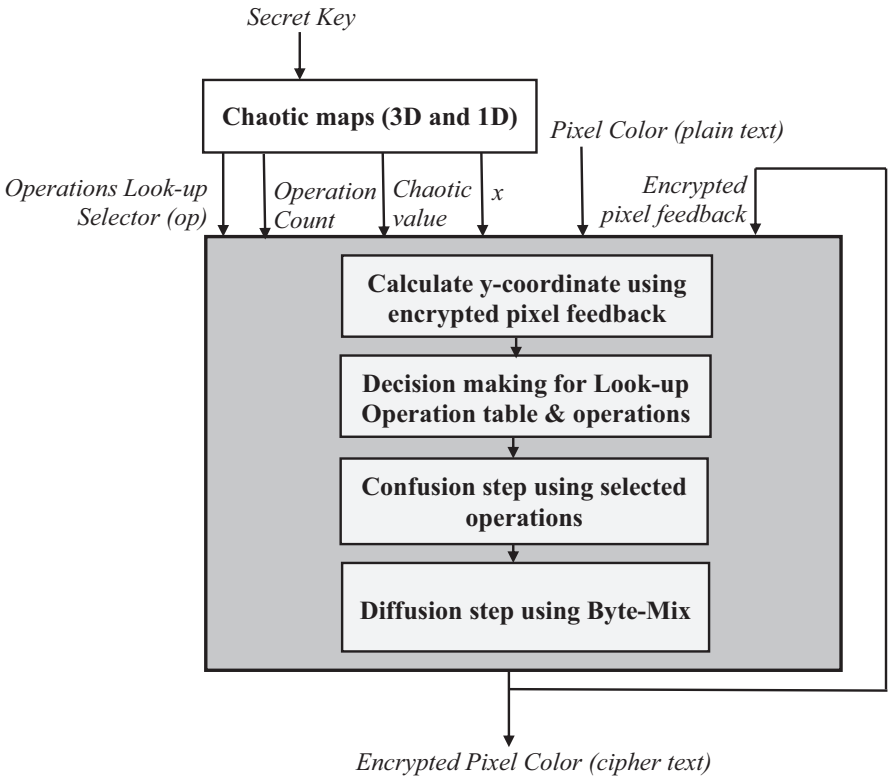


Fig. 10.5 Per-round block diagram for the Proposed Dynamic Framework

10.3.3 Definition of Diffusion Stage

In the diffusion stage the image is treated in two equal-halves (divided horizontally) and the corresponding pixel bytes of the two halves say a and b are then mixed to generate two new pixel bytes a' and b' for substitution in place of a and b respectively. The following represents generation of a' and b':

a = a1a2a3a4 a5a6a7a8
b = b1b2b3b4b5b6b7b8
a' = a5a6a7a8b1b2b3b4
b' = b5b6b7b8 a1a2a3a4

For observation purpose, in the current implementation of the proposed framework, we choose to incorporate dynamism at three levels i.e.

(i) dynamism in the number of operations performed per round,
(ii) dynamism in selection of the operations, and
(iii) dynamism in deciding order in which pixels are encrypted.

We have restricted use of a single look-up table containing the operations {<<, $\oplus$, negation, XNOR, >>}, where $\oplus$,<<,>> represent bitwise XOR, left-circular shift, right-circular shift operation respectively.

The choice of chaotic_value, op_count and x-coordinate value are made key-dependent by using a 3-D chaotic map (Kanso and Ghebleh 2012). Operations op are selected through random numbers generated using 1-D chaotic map i.e. Logistic-Tent map (Zhou et al. 2014) making the operation selection key-dependent. Hence, the number and kind of operations involved per-round in cipher generation are decided dynamically. To maintain a balance between efficiency and security, the maximum value of op_count has been restricted in the range 1–4. For higher security applications the minimum and maximum limit of operations can be adjusted. Also, note that the choices for operations op are reversible operations so that any combination of these operations can be used during encryption and decryption is always possible.

Following Eqs. (10.1, 10.2 and 10.3) give the details of the chaotic maps used for the current implementation of the proposed dynamic framework:

(i) Logistic-Tent Map

$$x_{i+1} = rx_n\left(1 - x_i\right) + \left(4 - r\right)\frac{x_i}{2} \bmod 1 \text{ if } x_i < 0.5 \tag{10.1}$$

$$x_{i+1} = rx_n\left(1 - x_i\right) + \left(4 - r\right)\frac{\left(1 - x_i\right)}{2} \bmod 1 \text{ if } x_i \geq 0.5 \tag{10.2}$$

where r ϵ (0,4]

(ii) 3D-Chaotic Map

$$X_{i+1} = \begin{pmatrix} x_{i+1} \\ y_{i+1} \\ z_{i+1} \end{pmatrix} = A \begin{pmatrix} x_i \\ y_i \\ z_i \end{pmatrix} (\mathrm{mod}\, 1) \tag{10.3}$$

where A is

$$\begin{pmatrix} a_x a_z b_y + 1 & a_z & a_x a_y a_z b_y + a_x a_z + a_y \\ a_x a_z b_y b_z + a_x b_y + b_z & 1 + a_z b_z & a_x a_y b_y + a_x a_y a_z b_y b_z + a_x a_z b_z + a_y b_z + a_x \\ b_y + a_x b_x b_y & b_x & 1 + a_x a_y b_x b_y + a_y b_y + a_x b_x \end{pmatrix}$$

such that all a's and b's are positive integers.

10.3.4 Key Description

Two chaotic maps (i.e. a 3-D chaotic map and a 1-D chaotic map) are used in the proposed work to have increased key space. Currently, only one out of three initial conditions (or seed values) of 3-D chaotic map and parameter value for 1-D logistic_tent map is made key-dependent, while other two seed values of 3-D chaotic map, seed value for 1-D chaotic map and all six parameters for 3-D chaotic map are kept fixed, such that ax = ay = az = 1 and bx = by = bz = 2. So, there is a scope to make other parameters and seed values also key-dependent by increasing the key-size.

In the current implementation, a 128-bit key is used. Parameter value for Logistic-Tent map is calculated by XORing the odd positioned bytes of the key together and the even positioned bytes of the key together to get two bytes and finally these two bytes are treated as a 16-bit integer value, which is further converted into a decimal no. (of 4 decimal precision) falling in the range 3.57–4. Further, one seed value for 3-D chaotic map is generated by treating the 128 bit key as 16 bytes, say key(0) to key(15), and calculating the seed value in the following way:

(i) tmp(i) = key(i) + key(i + 8), $0 \leq i < 8$
(ii) treat the obtained 8 tmp bytes as 64 bit unsigned integer, which is then transformed into decimal number (of 4 decimal precision) between 0 and 1 to be treated as a seed value for 3-D chaotic map.

As per the current implementation, all employed operations are very primitive and are directly implementable in hardware. From this perspective, per-round number of operations involved for encrypting M × N image using the implemented framework is on an average 9 MN. This is because, 3 operations per pixel are required for calculating y-coordinate of pixel in the non-sequential encryption pattern and verifying that this pixel has not been encrypted so far. Further, on an average for each pixel

there will be (1 + 2 + 3 + 4)/4 = 2.5 operations performed per round and before performing each operation firstly an operation is selected from the look-up table, so, doubling the average number of required operations per round. Therefore, on an average 3 MN + 5MN = 8 MN operations are employed in the confusion step and further MN operations in the diffusion step, making it 9 MN operations in total. In addition to these operations, some additional computations are required for generating chaotic sequences and for recalculating the position coordinates in case a pixel at position (x,y) is already encrypted.

Clearly, the per-round computational cost of current implementation of the proposed dynamic framework is much lesser than that of the per-round operations required in standard schemes like AES which involves computationally heavier operations including matrix multiplication of 4 × 4 state matrix (in Mix Columns step of AES per-round operations (Stallings 2004)). Mix Columns alone require much bulkier operations i.e. 4 multiplication modulo irreducible polynomial x8 + x4 + x3 + x + 1 {\displaystyle x^{8} + x^{4} + x^{3} + x + 1} and 3 addition (XOR) operations per byte besides other round operations.

10.4 Results

This section shows the results of the experiments made to prove the strength of the proposed work. The current implementation of the proposed dynamic framework is tested on a machine with Windows 7 32-bit operating system having 4GB RAM and Intel® core™ 2Duo processor @2.00GHz, using MATLAB R2011a. Observations have been taken on gray-scale images (size: 256 × 256), as in principle, the gray-scale logic can always be applied to the RGB planes corresponding to Red, Green and Blue components respectively of the colored images. Few of the observations are as discussed below.

10.4.1 NPCR, UACI and Co-relation Coefficient

Firstly, to demonstrate that with minutest change in original input image the scheme in generating entirely different output cipher image NPCR and UACI (Wu et al. 2011) observations are taken. NPCR refers to "Number of Pixel Change Rate" which measures the number of pixels changed in cipher image with change of single pixel in original input image. And, UACI refers to "Unified Average Change Intensity" which gives the average intensity change in pixels of the output cipher image with change of single pixel in the original input image. These observations are significant to prove strength of the proposed framework to resist differential attacks. The observations of Correlation Coefficient between the output cipher

Table 10.1 Image quality & security analysis measures with round variation for water lilies image

Round count	Entropy (cipher image)	NPCR (%)	UACI (%)	Correlation coefficient
2	7.9966	61.16	19.27	1.09×10^{-04}
4	7.9965	87.71	29.09	-6.34×10^{-05}
6	7.9974	92.91	30.94	-5.67×10^{-04}
8	7.9974	99.45	33.32	1.70×10^{-04}
10	7.9974	99.55	33.45	-2.52×10^{-04}
12	7.9973	99.58	33.48	-8.26×10^{-04}
14	7.9971	99.59	33.51	6.01×10^{-04}
16	7.9975	99.59	33.46	-12.00×10^{-04}

Table 10.2 Image quality & security analysis measures for different plain images

Grayscale image	Cipher image entropy	NPCR (%)	UACI (%)	Correlation coefficient
Baboon	7.9971	99.49	33.37	-5.39×10^{-05}
Water lilies	7.9974	99.45	33.32	1.70×10^{-04}
Lena	7.9973	99.40	33.32	-6.82×10^{-04}
Plain white	7.9974	99.54	33.45	-7.15×10^{-04}

image and corresponding original input image are also taken to display that the proposed scheme possesses strong resistance against statistical attacks.

Table 10.1 displays results for entropy, NPCR, UACI along with Correlation Coefficient taken for several rounds of the implemented framework on the grayscale Water Lilies image. The observations of NPCR, UACI & Correlation Coefficient are made by complementing a single pixel at a time for several randomly chosen pixel positions and averaging the results. The results show NPCR and UACI values approach their respective expected values i.e. more than 99% and 33% respectively (Wu et al. 2011) for round count 8 and beyond. This suggests that application of 8 or more rounds of the implemented framework leads to generation of the cipher image which is highly sensitive to any minor change in the original image. Correlation Coefficient having value very close to 0 indicate that the plaintext image and the cipher image are highly uncorrelated. The results demonstrate that the implemented framework with 8 or more rounds offers high resistance against statistical and differential attacks by adversary. Further, Table 10.2 shows these observations taken for several images including plain white image with 8 rounds of encryption, which again are favorable and demonstrate strength of the proposed work.

As the NPCR, UACI and Correlation Coefficient observations show that 8 rounds of the proposed implemented framework provides high strength against statistical and differential attacks, therefore, all further observations are taken with 8 rounds of the proposed work.

10.4.2 Histogram and Entropy

Figures 10.6 and 10.7 display the original 256 × 256 gray-scale images and corresponding encrypted Water Lilies and Baboon images respectively along with their corresponding histograms and entropy values. As can be seen clearly, the images encrypted with proposed scheme possess no redundancies which were present in the original plain image.

Block-wise variation of entropy in cipher Water Lilies image is observed to highlight the uniformity in entropy across the encrypted image when divided in equal sized blocks. Figure 10.8 shows the plot for block-wise variation of entropy in 256 × 256 encrypted Water Lilies image divided into 256 blocks each of size 16 × 16. It is evident from the plot that the entropy variation across blocks is very small which indicates uniformity in intensity distribution even at lower granularity levels.

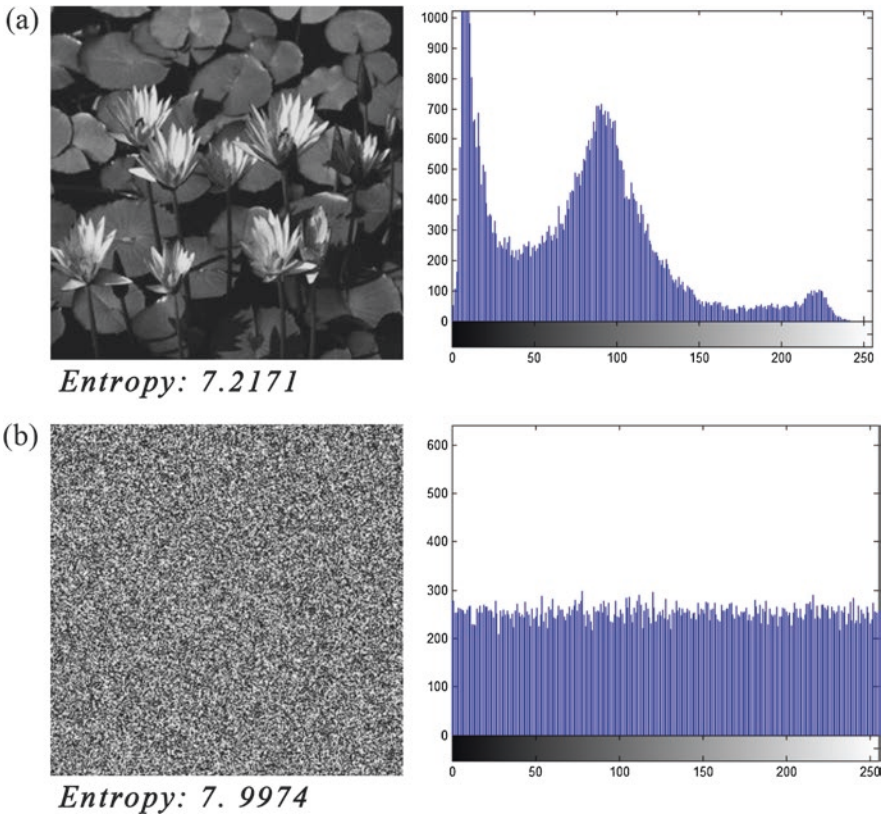


Fig. 10.6 (**a**) Original gray-scale image & histogram for water lilies. (**b**) Gray-scale encrypted image & histogram for water lilies

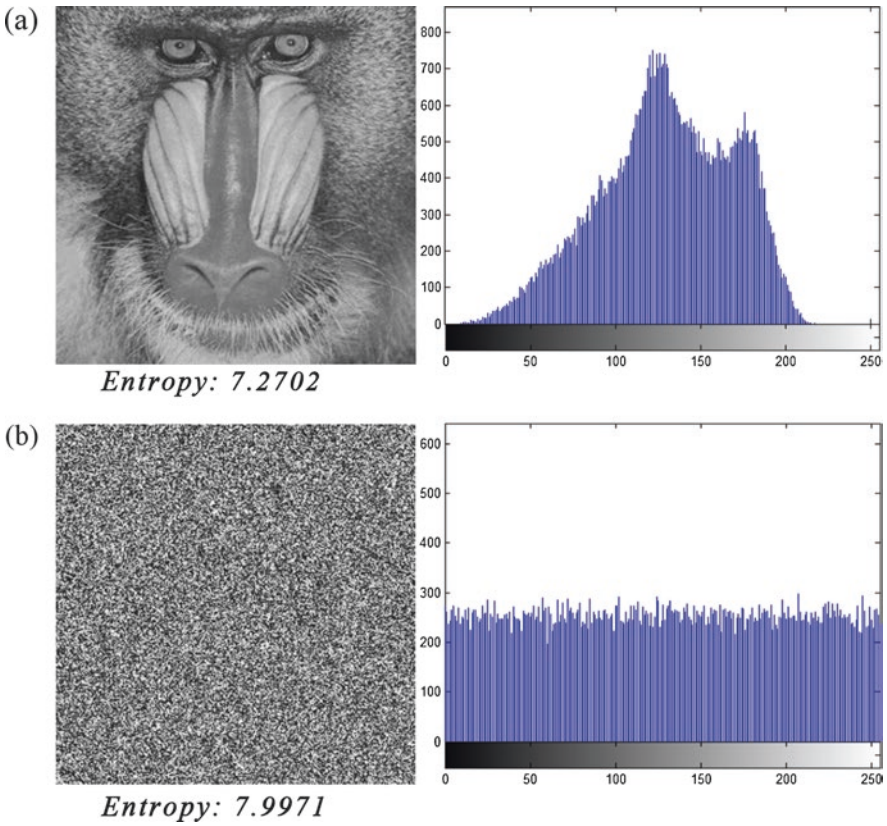


Fig. 10.7 (**a**) Original gray-scale image & histogram for baboon. (**b**) Gray-scale encrypted image & histogram for baboon

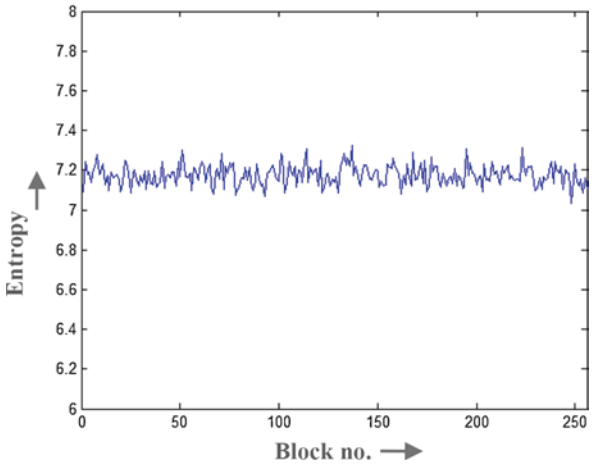


Fig. 10.8 Plot of block-wise entropy of gray-scale encrypted water lilies image

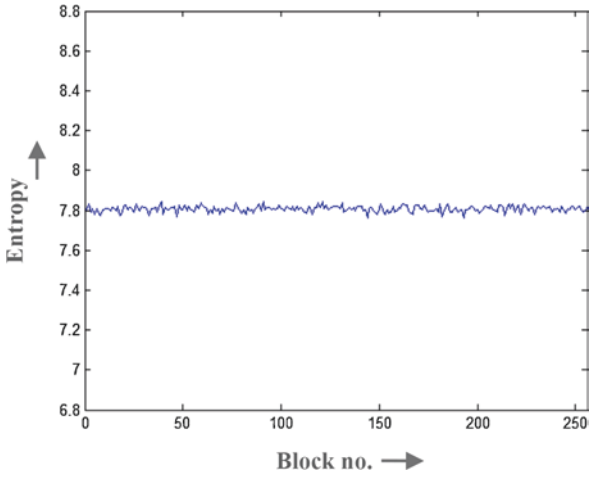


Fig. 10.9 Plot of block-wise entropy encrypted image (Lena – 512 × 512)

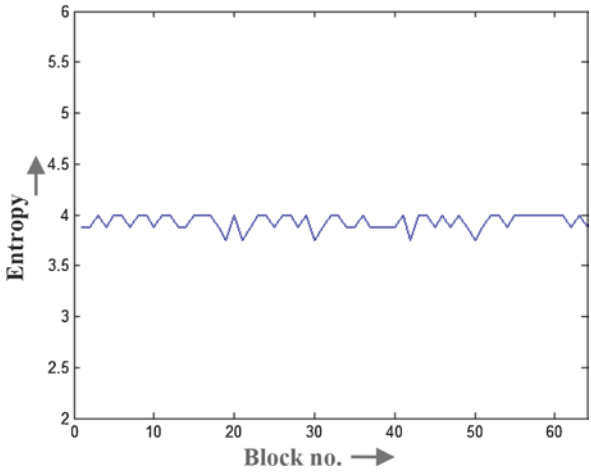


Fig. 10.10 Plot of block-wise entropy encrypted image (Lena – 32 × 32)

To observe the impact of variation of plaintext size, block-wise variation of entropy in the cipher image with the proposed scheme is also observed for images with sizes 512 × 512, 256 × 256, 128 × 128, 64 × 64 and 32 × 32 and the block-wise entropy is found nearly uniform irrespective of the plaintext size. Figures 10.9 and 10.10 shows the plot of block-wise entropy variation for Lena image with sizes 512 × 512 and 32 × 32 respectively. These observations show that though the present work considers image as a single block, however, sub-blocks of the image can be encrypted using specific or changing block-cipher operation modes like CBC, CTR etc.

The histogram obtained for plain white image encrypted using the implementation of the proposed dynamic framework is almost uniform as shown in Fig. 10.11. This observation verifies that redundancy gets completely removed in the cipher

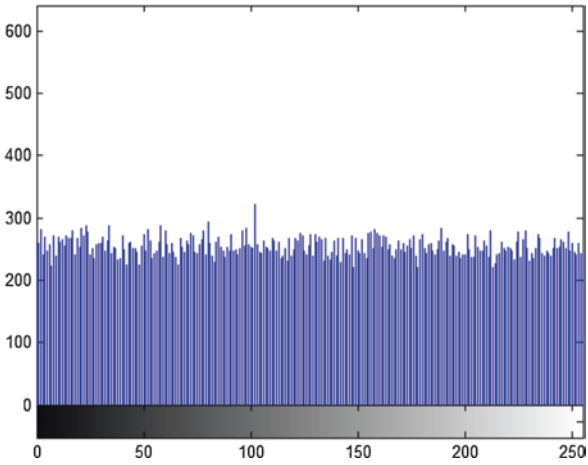


Fig. 10.11 Encrypted white image histogram

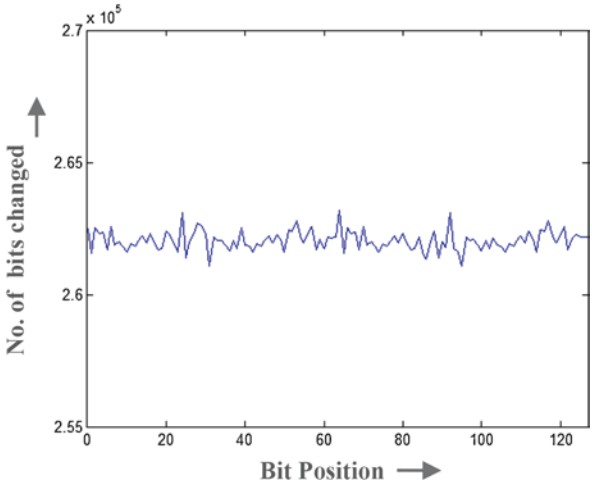


Fig. 10.12 Plot showing changed bit count in cipher image with change in single bit at each of the 128 positions of the key (Avalanche Property)

image and uniform distribution of intensities is obtained in the cipher image for the original image having complete redundancy and a single peaked histogram.

10.4.3 Avalanche Properties

To demonstrate strength against differential cryptanalysis, avalanche properties are also investigated. The plots Figs. 10.12 and 10.13 respectively show that with change of single bit in the key or change of single bit per pixel in the original image (256 × 256 Water Lilies), nearly 50% i.e. half of the bits change in the cipher image. Figure 10.14 shows that the decrypted image also changes by around 50% when

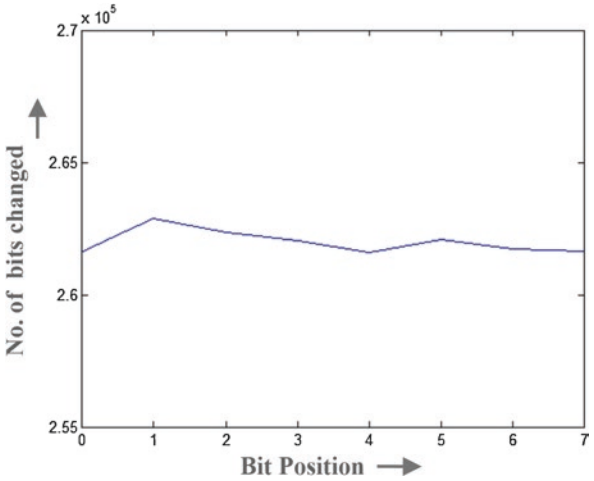


Fig. 10.13 Plot showing changed bit count in cipher image with change of single bit per pixel at each of the 8 positions (Avalanche Property)

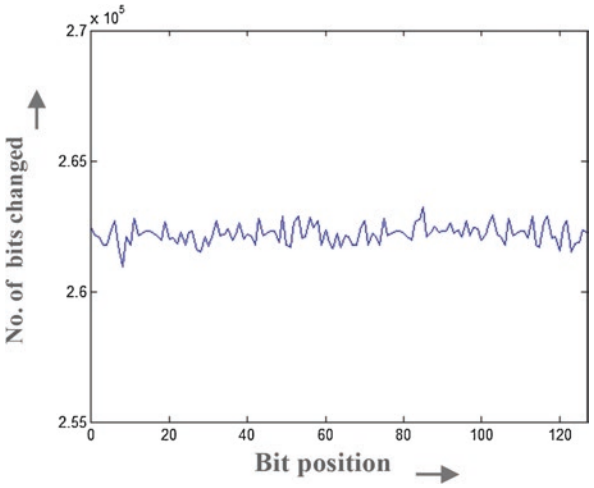


Fig. 10.14 Plot of no. of bits changed in the decrypted cipher image with change in single bit at each of the 128 positions of the key used during decryption (Avalanche Property)

decrypted by single-bit changed key. These plots show that the cipher demonstrates strong avalanche properties and the observations are nearly uniform irrespective of the position of the bit changed. These observations show significant and uniform contribution of each bit of the key to the pixels of the cipher image thereby establishing that implementation of the proposed framework possess strong confusion property.

Table 10.3 Results of NIST test-suite for randomness

Test name	Adjustment parameter	P-value	Test status
Frequency test	–	0.861854	Success
Block frequency test	Block length = 128	0.124819	Success
Run test	–	0.966985	Success
Longest run test	–	0.615741	Success
Binary matrix rank test	–	0.798075	Success
FFT test	–	0.476308	Success
Non-overlapping template matching test	Block length = 10	–	Success
Overlapping template matching test	Block length = 10	0.361665	Success
Universal statistical test	–	0.776738	Success
Linear complexity test	Block length = 500	0.406574	Success
Serial test (p-value1)	Block length = 16	0.971437	Success
Serial test (p-value2)	Block length = 16	0.868488	Success
Approximate entropy test	Block length = 10	0.853303	Success
Cumulative sums test	–	0.650924	Success
Random excursions test	–	–	Success
Random excursions variant test	–	–	Success

10.4.4 NIST Statistical Test Suite for Randomness

NIST statistical test suite (Rukhin et al. 2010) observations are also taken to verify randomness of the cipher image obtained using the proposed work. P-value is ≥ 0.01, indicate that the sequence under test is random (at 1% significance level). Table 10.3 displays the observations of all the NIST tests on 256×256 gray-scale Baboon image. Test status of all the tests emerged out to be success, which demonstate that the obtained cipher is completely random.

10.4.5 Resistance Against Known/Chosen Plaintext Attacks & Differential Cryptanalysis

The proposed dynamic framework with multi-level dynamism will avert any possible breach into the cryptosystem with high strength because it will be much harder for the attacker to design an attack targeting the structure or design of per-round operations as the type of operations, the number of operations performed on each pixel in different rounds varies and is unknown to the attacker. Also, the type and number of per-round operations performed on the same pixel position will vary if the same key is applied with a slightly modified image since the sequence of encrypting pixels is also dynamically decided based the plaintext besides the key. This will offer high strength to resist known/chosen plaintext attacks, differential and impossible differential attacks.

10.5 Conclusion & Future Scope

The work in this chapter focuses on dynamism as a paradigm shift from the conventional approach of static algorithm for encryption. Firstly, we propose new dimensions to dynamism:

Dynamism in the number of operations performed per round which may vary in different rounds of the encryption process.

Dynamism in deciding the sequence in which data bytes are encrypted which changes dynamically with minutest change in the plaintext without requirement of any extra information about the plaintext to be included as part of the key for encryption.

Combining this with dynamism in choice of operations and a diffusion stage per-round, a new and flexible dynamic encryption framework for image encryption is proposed which can be easily made adaptable to dynamically varying security requirements and resources at hand. This adaptable nature of the proposed work makes it a very strong approach for security applications in IoT devices and upcoming 5G technology. This strategy helps in providing high resistance against known/chosen plaintext attacks and differential attacks in a computationally efficient way. Use of multi-level dynamism offers high strength against any attempt to design statistical/cryptanalytic attacks because the adversary will be unaware about the overall structure i.e. the actual number and type of operations performed per-round of the encryption process.

Experimental results on the implementation of the proposed framework (with 8 or above rounds) demonstrates complete diffusion of redundancies, strong avalanche properties, high randomness, smooth block-wise entropy variation at a low average computational cost. It also offers high strength for varied block-sizes which demonstrates its flexibility to accommodate images of different sizes and its capability to be applicable on entire image as a whole or as a block cipher to be applied on an image divided into blocks or sub-images.

To increase security, the algorithm's design offers flexibility to accommodate a larger number of operations' look-up tables and each table having larger number of different operations to choose from, without incurring much of additional computational cost. Also, as mentioned earlier, the maximum and minimum number of operations performed per-round could also be changed, to adapt according to security requirements and resource constraints.

To add to the above, the size of the key can also be increased to generate one or more of the remaining seed and parameter values to enhance security at a fixed minor increase in computational cost. Further, besides the key, the used chaotic sequences can also be made dependent on the plaintext to increase cipher's dynamical dependency on both key and plaintext.

Though, gray-scale images have been used for taking the observations, yet it is very apparent that the work is easily applicable to colored images and other visual forms of media like videos also. For colored images, the algorithm can be run on the three RGB color planes separately and the encrypted planes can be combined

together. And, videos can be viewed as a collection of moving frames where each frame can be treated as an image.

In future, the strategy of having dynamically changing operations defined for each round can also be extended to generate different cipher text, for the same plaintext at different times without change in the key, by adding time-variant parameter while generating chaotic sequence. Also, more encryption schemes involving dynamism will be designed and their applicability and efficacy will also be verified on other forms of media/multimedia as well.

References

Abd-ElGhafar, I., Rohiem, A., Diaa, A., & Mohammed, F. (2009, May). Generation of AES key dependent S-boxes using RC4 algorithm. *13th international conference on Aerospace Sciences & Aviation Technology* (ASAT–13), pp. 26–28.

Abomhara, M., & Køien, G. M. (2015). Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security, 4*, 65–88. https://doi.org/10.13052/jcsm2245-1439.414.

Abuhaiba, I. S. I., AlSallut, A. Y., Hejazi, H. H., & AbuGhali, H. A. (2012). Cryptography using multiple two-dimensional chaotic maps. *International Journal of Computer Network and Information Security, 8*, 1–7. https://doi.org/10.5815/ijcnis.2012.08.01.

Ahmad, J., & Hwang, S. O. (2015). Chaos-based diffusion for highly autocorrelated data in encryption algorithms. *Nonlinear Synamics, 82*, 1839–1850. Springer.

Ahmad, J., Khan, M. A., Hwang, S. O., & Khan, J. S. (2017). A compression, sensing and noise-tolerant image encryption scheme based on chaotic maps and othogonal matrices. *Neural Computing and Applications, 28*(S-1), 953–967. Springer.

Akhshani, A. (2015). *Quantum chaotic cryptography: A new approach*. Universiti Sains Malaysia.

Akhshani, A., Behnia, S., Akhavan, A., Lim, S-C., & Hassan, Z. (2013). An image encryption approach using quantum chaotic map. In *Proceedings of 2013 2nd international conference on Advances in Computer and Information Technology* – ACIT. https://doi.org/10.3850/978-981-07-6261-2_36.

Anees, A., Siddiqui, A. M., & Ahmed, F. (2014). Chaotic substitution for highly autocorrelated data in encryption algorithm. *Communications in Nonlinear Science and Numerical Simulation, 19*, 3106–3118. Elsevier.

Armand Eyebe Fouda, J. S., Effa, J. Y., Sabat, S. L., & Ali, M. (2014a). A fast chaotic block cipher for image encryption. *Communications in Nonlinear Science and Numerical Simulation, 19*, 578–588. Elsevier.

Armand Eyebe Fouda, J. S., Effa, J. Y., & Ali, M. (2014b). Highly secured chaotic block cipher for fast image encryption. *Applied Soft Computing, 25*, 435–444. Elsevier.

Arrag, S., Hamdoun, A., Tragha, A., & Khamlich, S. E. (2013). Implementation of stronger AES by using dynamic S-box dependent of master key. *Journal of Theoretical and Applied Information Technology, 53*(2), 196–204.

Behnia, S., Ayubi, P., & Soltanpoor, W. (2012) Image encryption based on quantum chaotic map and FSM transforms. In *Proceedings of 2012 15th International Telecommunications Network Strategy and Planning Symposium (NETWORKS)*, pp. 1–6. https://doi.org/10.1109/NETWKS.2012.6381669.

Biryukov, A., & Khovratovich D. (2009). Related-key cryptanalysis of the full AES-192 and AES-256, ASIACRYPT 2009. *Advances in cryptology – ASIACRYPT 2009*, Lecture notes in computer science, Vol. 5912, Springer, pp. 1–18. https://doi.org/10.1007/978-3-642-10366-7_1.

Biryukov, A., Khovratovich, D., & Nikolić, I. (2009). Distinguisher and related-key attack on the full AES-256. *CRYPTO'09, Advances in cryptology – CRYPTO 2009*, Lecture notes in computer science, Vol. 5677, Springer, pp. 231–249. https://doi.org/10.1007/978-3-642-03356-8_14.

Biryukov, A., Dunkelman, O., Keller, N., Khovratovich, D., & Shamir, A. (2010). Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds. *EUROCRYPT 2010, Advances in cryptology – EUROCRYPT 2010*, Lecture notes in computer science, Vol. 6110, Springer, pp. 299–319. https://doi.org/10.1007/978-3-642-13190-5_15.

Boriga, R., Dăscălescu, A. C., & Diaconu, A. V. (2014). A new one-dimensional chaotic map and its use in a novel real-time image encryption scheme. *Advances in Multimedia*, Hindawi 2014, Article ID 409586, 1–15.

Borujeni, S. E., & Ehsani, M. S. (2015). Modified logistic maps for cryptographic application. *Applied Mathematics, Scientific Research, 6*, 773–782.

Cao, Y. (2013). A new hybrid chaotic map and its application on image encryption and hiding. *Mathematical Problems in Engineering, 2013*, 1–13. Hindawi.

Chai, X., Yang, K., & Gan, Z. (2017). A new chaos-based image encryption algorithm with dynamic key selection mechanisms. *Multimedia Tools and Applications, 76*(1), 9907–9927. Springer.

Dara, M., & Manochehr, K. (2013). A novel method for designing S-boxes based on chaotic logistic maps using cipher key. *World Applied Sciences Journal, 28*(12), 2003–2009.

Devaney, R. L. (1989). *An introduction to chaotic dynamical systems*. Redwood: Addison-Wesley Publishing.

Dhall, S., & Pal, S. K. (2010). Design of a new block cipher based on conditional encryption. In *Proceedings of 7th international conference on Information Technology: New Generations* (ITNG 2010), IEEE Press, pp. 714–718, https://doi.org/10.1109/ITNG.2010.90.

Dhall, S., Pal, S. K., & Sharma, K. (2014). *New lightweight conditional Encryption schemes for multimedia*. In *Proceedings of 3rd International Conference on Soft Computing for Problem Solving* (SocPros 2013), Advances in Intelligent Systems and Computing *258*, 365–377, Springer. https://doi.org/10.1007/978-81-322-1771-8_32.

Elabady, N. F., Abdalkader, H. M., Moussa, M. I., & Sabbeh, S. F. (2014). Image encryption based on new one-dimensional chaotic map. In *Proceedings of the international conference on Engineering and Technology* (ICET 2014), IEEE Press, pp. 1–6. https://doi.org/10.1109/ICEngTechnol.2014.7016811.

Elmangoush, A., & Magedanz, T. (2017). Adaptable protocol selection for reliable smart city services. *Journal of Cyber Security, 6*(1), 57–76. https://doi.org/10.13052/jcsm2245-1439.613.

El-Sheikh, H. M., & El-Mohsen, O. A. (2012, April). A new approach for designing key-dependent S-box defined over GF (2^4) in AES*, International Journal of Computer Theory and Engineering* 4(2).

Faraoun, K. (July 2010). Chaos-based key stream generator based on multiple maps combinations and its application to images encryption. *The International Arab Journal of Information Technology, 7*(3), 231–240.

Furht, B. (Ed.). (2005). *Encyclopedia of multimedia*. Boston: Springer.

Geetha, G. (2012). *New directions in quantum chaotic crypto schemes*. In Proceedings of 2012 international conference on computing sciences, pp. 316-321. https://doi.org/10.1109/ICCS.2012.47.

Gmira, F., Sabbar, W., Hraoui, S., & Jarrar Ouilidi, A. (2019). A new theoretical pattern based on a methods database for dynamic images encryption. In *Proceedings of first international conference on Real Time Intelligent Systems* (RTIS 2017), Lecture notes in real-time intelligent systems, advances in intelligent systems and computing, Vol. 756, pp. 477–484, Springer.

Goldwasser, S., & Micali, S. (1984). Probabilistic encryption. *Journal of Computer and System Sciences*, Academic Press, *28*(2), 270–299.

Gonzalez, R. C., & Woods, R. E. (2007). *Digital image processing* (3rd ed.). New York: Prentice Hall.

Harmouch, Y., & Kouch, R. E. (2015, January). A new algorithm for dynamic encryption. *International Journal of Innovation and Applied Studies*, *10*(1), 305–312.

Herland, K., Hämmäinen, H., & Kekolahti, P. (2016). Information security risk assessment of smartphones using Bayesian networks. *Journal of Cyber Security, 4*, 65–86. https://doi.org/10.13052/jcsm2245-1439.424.

Husni, E. (2017). Dynamic rule encryption for mobile payment. *Security and Communication Networks 2017*, Article ID 4975302, 1-11,. Hindawi. https://doi.org/10.1155/2017/4975302.

Hussain, I., Shah, T., & Gondal, M. A. (2012). Image encryption algorithm based on PGL(2, GF(2^8)), S-boxes, and TD-ERCS chaotic sequence. *Nonlinear Dynamics, 70*(1), 181–187. Springer.

Juremi, J., Mahmod, R., Sulaiman, S., & Ramli, J. (2012). Enhancing advanced encryption standard S-box generation based on round key. *International Journal of Cyber-Security and Digital Forensics*, 183–188.

Kanso, A., & Ghebleh, M. (2012). A novel image encryption algorithm based on a 3D chaotic map. *Communications in Nonlinear Science and Numerical Simulation, 17*(7), 2943–2959. Elsevier.

Kartalopoulos, S. (2010). Chaotic quantum cryptography: The ultimate for network security. In *Proceedings of the 2010 International Conference on Optical Communication Systems (OPTICS).*

Khan, F. A., Ahmed, J., Khan, J. S., Ahmad, J., & Khan, M. A. (2017a). A novel image encryption based on Lorenz equation, Ginegerbreadman chaotic map and S8 permutation. *Journal of Intelligent Fuzzy Systems, 33*(6), 3753–3765. IOS Press.

Khan, J. S., Ahmad, J., & Khan, M. A. (2017b). TD-ERCS map-based confusion and diffusion of autocorrelated data. *Nonlinear Dynamics, 87*, 93–107. Springer.

Khan, J. S., Khan, M. A., Ahmad, J., Hwang, S. O., & Ahmed, W. (2017c). An improved image encryption scheme based on a non-linear chaotic algorithm and substitution boxes. *Informatica*,. IOS Press*, 28*(4), 629–649.

Knudsen, L. R. (2015). Dynamic encryption. *Journal of Cyber Security, 3*, 357–370.

Korstanje, K., & Keliher, L. (2015). Weak keys and plaintext recovery for the Dhall-Pal Block Cipher. In *Proceedings of 2015 IEEE Symposium on Computers and Communication (ISCC)*, pp. 816–821, https://doi.org/10.1109/ISCC.2015.740561.

Krishnamurthy, G. N., & Ramaswamy, V. (2008). Making AES stronger: AES with key dependent S-box. *International Journal of Computer Science and Network Security, 8*(9), 388–398.

Mahmoud, E. M., El Hafez, A. A., Elgraf, T. A., & Zekry, A. (2013, January–February). Dynamic AES-128 with key-dependent S-box*, International Journal of Engineering Research and Applications (IJERA)*, *3*, 1662–1670.

Maqableh, M. (2015). A novel Triangular Chaotic Map (TCM) with full intensive chaotic population based on logistic map. *Journal of Software Engineering and Applications, Scientific Research, 8*, 635–659.

Menezes, A. (Ed.). (1996). *Handbook of applied cryptography*. Boca Raton: CRC-Press.

Meskanen, T., Niemi, V., & Nieminen, N. (2015). How to use garbling for privacy preserving electronic surveillance services. *Journal of Cyber Security, 4*, 41–64. https://doi.org/10.13052/jcsm2245-1439.413.

Murillo-Escobar, M. A., Cruz-Hernández, C., Abundiz-Pérez, F., López-Gutiérrez, R. M., & Acosta Del Campo, O. R. (2015). A RGB image encryption algorithm based on total plain image characteristics and chaos. *Signal Processing, 109*, 119–131. Elsevier.

Ngo, H. H., Wu, X., Dung Le, P., Wilson, C., & Srinivasan, B. (2010, May). Dynamic key cryptography and applications*. International Journal of Network Security*, *10*(3), 161–174.

Norouzi, B., & Mirzakuchaki, S. (2016). Breaking an image encryption algorithm based on the new substitution stage with chaotic functions. *Optik, 127*, 5695–5701. Elsevier.

Ofori, K. S., Larbi-Siaw, O., Fianu, E., Gladjah, R. E., & Boateng, E. O. Y. (2016). Factors influencing the continuance use of mobile social media: The effect of privacy concerns. *Journal of Cyber Security, 4*, 105–124. https://doi.org/10.13052/jcsm2245-1439.426.

Özkaynaka, F., Özer, A. B., & Yavuz, S. (2012). Cryptanalysis of a novel image encryption scheme based on improved hyperchaotic sequences. *Optics Communications, 285*, 4946–4948. Elsevier.

Pareek, N. K., Patidar, V., Sud, K. K. (2005). Cryptography using multiple one-dimensional chaotic maps. *Nonlinear Science and Numerical Simulation, 10*, 715–723, Elsevier.

Pareek, N. K., Patidar, V., & Sud, K. K. (2006). Image encryption using chaotic logistic map. *Image and Vision Computing, 24*, 926–934. Elsevier.

Paul, G., & Irvine, J. (2016). Practical attacks on security and privacy through a low-cost android device. *Journal of Cyber Security, 4*, 33–52. https://doi.org/10.13052/jcsm2245-1439.422.

Phan, R. C.-W. (2004). Impossible differential cryptanalysis of 7-round Advanced Encryption Standard (AES). *Information Processing Letters*, *91*(1), 33–38, Elsevier.

Pradhan, C., Bisoi, A. K. (2013, June). Chaotic variations on AES algorithm, International Journal of Chaos, Modelling and Simulation 2(2).

Ramadan, N., Ahmed, H. H., Elkhamy, S. E., & Abd El-Samie, F. E. (2016). Chaos-based image encryption using an improved quadratic chaotic map. *American Journal of Signal Processing, Scientific & Academic Publishing, 6*(1), 1–13.

Ramos, R. V. (2017). *Quantum-chaotic cryptography*. Available online: https://arxiv.org/ftp/arxiv/papers/1703/1703.06512.pdf

Ramos, R. V., & Souza, R. F. (2001). Using chaotic dynamics in quantum cryptographis systems: Chaotic cryptography and repeaters. *Journal of Optical Communication, 22*(3), 90–94. https://doi.org/10.1515/JOC.2001.22.3.90.

Rohokale, V., & Prasad, R. (2015). Cyber security for intelligent world with Internet of Things and machine to machine communication. *Journal of Cyber Security, 4*, 23–40. https://doi.org/10.13052/jcsm2245-1439.412.

Rui, L. (2015). New algorithm for color image encryption using improved 1D logistic chaotic map. *The Open Cybernetics & Systemics Journal, 9*, 210–216.

Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., Vo, S., & Bassham, L. E., III. (2010). *A statistical test suite for the validation of random number generators and pseudo random number generators for cryptographic applications*. Gaithersburg: NIST Special Publication. Available at: http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf.

Sakthidasan, K., Santhosh Krishna, B.V. (2011, June). A new chaotic algorithm for image encryption and decryption of digital color images. *International Journal of Information and Education Technology*, *1*(2), 137–141.

Saraereh, O. A., Alsafasfeh, Q., & Arfoa, A. (2013). Improving a new logistic map as a new chaotic algorithm for image encryption. *Modern Applied Science, Canadian Center of Science and Education, 7*(12), 24–33.

Schneier B. (1994). Description of a new variable-length key, 64-bit block cipher (blowfish), *Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993)*, Lecture notes in computer science, Vol. 809, pp. 191–204, Springer. https://doi.org/10.1007/3-540-58108-1_24.

Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C., & Ferguson, N. (1999). *The twofish encryption algorithm: A 128-bit block cipher*. New York: Wiley.

Shannon, C. E. (1949). Communication theory of secrecy system. *Bell System Technical Journal, 28*, 656–715.

Stallings, W. (2004). *Cryptography & network security principles and practices*. Hoboken: Pearson Education.

Stojanovic, A. D., Ramos, R. V., & Matavulj, P. S. (2016). Authenticated B92 QKD protocol employing synchronized optical chaotic systems. *Optical and Quantum Electronics, 48*, 285.

Subramanyan, B., Chhabria, V. M., & Sankarbabu, T. G. (2011). Image Encryption Based On AES Key Expansion*, 2011 Second International Conference on Emerging Applications of Information Technology, IEEE*. https://doi.org/10.1109/EAIT.2011.60.

Tu, G., Liao, X., & Xiang, T. (2013). Cryptanalysis of a color image encryption algorithm based on chaos. *Optik, 124*, 5411–5415. Elsevier.

Vahidi, J., & Gorji, M. (2014). The confusion-diffusion image encryption algorithm with dynamical compound chaos. *The Journal of Mathematics and Computer Science, 9*, 451–457.

Wang, X., & Qing, Y. (2009). A block encryption algorithm based on dynamic sequences of multiple chaotic sequences of multiple chaotic systems. *Science and Numerical Simulation, 14*, 574–581. Elsevier.

Wang, B., Wei, X., & Zhang, Q. (2013). Cryptanalysis of an image cryptosystem based on logistic map. *Optik, 124*, 1773–1776. Elsevier.

Wang, X. Y., Gu, S. X., & Zhang, Y. Q. (2015). Novel image encryption algorithm based on cycle shift and chaotic system. *Optics and Lasers in Engineering, 68*, 126–134. Elsevier.

Wang, L., Song, H., & Liu, P. (2016). A novel hybrid color image encryption algorithm using two complex chaotic systems. *Optics and Lasers in Engineering, Elsevier, 77*, 118–125.

Wei, J., Liao, X., Wong, K., & Zhou, T. (2007). Cryptanalysis of a cryptosystem using multiple one-dimensional chaotic maps. *Nonlinear Science and Numerical Simulation, 12*, 814–822. Elsevier.

Wu, Y., Noonan, J. P., & Agaian, S. (2011). NPCR and UACI randomness tests for image encryption. *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT)*, April Edition.

Zhang, X., & Cao, Y. (2014). A novel chaotic map and an improved chaos-based image encryption scheme. *The Scientific World Journal*, Hindawi 2014, Article ID 713541, 1–8.

Zhou, Y., Bao, L., & Philip Chen, C. L. (2013). Image encryption using a new parametric switching chaotic system. *Signal Processing, 93*, 3039–3052. Elsevier.

Zhou, Y., Bao, L., & Philip Chen, C. L. (2014, April). A new 1D chaotic system for image encryption. *Signal Processing*, Elsevier, *97*, 172–182.

Chapter 11
Privacy Challenges and Their Solutions in IoT

Nabeela Hasan, Akshay Chamoli, and Mansaf Alam

Abstract IoT (Internet of Things) is connecting inter-related computing devices and the main idea for this concept is to connect each device via internet so that it will be easy for the devices to communicate and share info among them. These days IoT has grown up to a massive extent and new and emerging topic in research. IoT is the new and vast technology for the upcoming future as almost all devices will be connected to each other and share data among them via internet. This chapter identifies various privacy challenges in IoT, and their respective solutions presented by several researches over the time. It presents various issues related to privacy and security in IoT like standardization, networking and addressing ones. The chapter also deals within solutions provided for academic, technical and industrial aspects for IoT enabled environment. The importance of data security and protection to overcome the vulnerabilities which can come for an IoT based environment and can reduce the risk for IoT infrastructure.

Keywords IoT privacy challenges and solutions · Security · Communication security

11.1 Introduction

By providing feature such that the devices or things can configure by its own is a newly feature based on the IEEE standards and interoperability feature so that the communication among protocols is appropriate and utilize the interfaces globally (Van Kranenburg 2008; Abomhara and Køien 2014). IoT is a new channel of communication for the existing channel between the human beings and the devices communicating which will become a new future era (Sundmaeker et al. 2010). With the

N. Hasan (✉) · A. Chamoli · M. Alam
Department of Computer Science, Jamia Millia Islamia, New Delhi, India
e-mail: nabeela151534@st.jmi.ac.in; malam2@jmi.ac.in

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_11

improvement in mobile communication, WSNs and RFIDs, IoT empowered devices to connect with one another (Bandyopadhyay and Sen 2011). IoT nowadays is applied in various common fields such as smart items, health, homes, cities, transport, living, and many others (Ul Rehman and Manickam 2016; Miorandi et al. 2012).

For business purposes, IoT involves a lot of vast areas to deal with or can increase this new technology for many organizations and companies, including applications related to IoT with service providers, platform providers and integrating this with telecom operation or software dealers (Abomhara and Køien 2014; Sundmaeker et al. 2010). In future, IoT surely will have a high demand in understanding features of IoT which is best for the higher education system (Aldowah et al. 2017). A massive increase in IoT applications has given up several privacy measures which need to be look upon.

As devices or things in future will surely become a part of a big Internet infrastructure, all devices may able to connect among each other and therefore issues will arise with continuous Internet global network expanding nature, it can open gateway to some or the other new security vulnerabilities. Such vulnerable thing can get accessed by hackers, and later can be used in an uncontrollable manner affecting privacy in billions of IoT devices. This will lead to increase the chances of attacks on network surfaces for hackers and other cyber criminals. So as the IoT technology is getting increased the security for this IoT global network must also get increased to a high level (Abomhara and Køien 2014).

A research by Hewlett Packard association (Gen and Controllers 2015) recommended that around 70% of the most normally utilized devices related with IoT are defenseless for hackers to assault and can make a misfortune to society. The IoT technology is on the starting phase so it will take time to develop all the security measures for this technology. IoT devices are not secure and are not fully secure, as due to their architectural mapping and the layers present in this IoT design. So, to improve IoT infrastructure some features like insecure communication medium among devices as well as insufficient authentication and authorization for devices should be looked because IoT will not get global success if these issues will not be taken care of for securing the infrastructure.

As when IoT network becomes prevalent everywhere, organization will get concerned about cross linking of objects like different devices have different features, but every device has IoT as their common feature will surely have new challenges to influence and to exchange. This can cause risks for security related to real data or information as well as protection of data is also necessary for the users and these things should be kept in mind while deploying IoT infrastructure and if it is not maintained this will surely create imbalance in adoption of the IoT technology by companies or any users or individuals working with this technology.

Privacy issues and challenges must be looked upon very seriously as by securing the IoT infrastructure to an extent such that no security breech can take place. This can happen when a proper guidance is provided to the designers and developers for integrating each security measure for IoT devices and after that it will automatically make the users to utilize IoT infrastructure embedded into these devices.

11.2 Privacy Requirements for IoT

IoT began to increase new energy in recent times as the result of the fast development of web associated sensors. Be that as it may, security is the serious issue involved in IoT and the main interest brought by various partners up in IoT which can possibly hinder its appropriation (Sicari et al. 2015; Jha and Sunil 2014). Thus, it is viewed as one of the serious issues which should be routed to advance the IoT utilization (Roman et al. 2013). Security is one of the central natures of an IoT framework which is identified by particular security highlights which are in many cases an essential for empowering reliability and secrecy characteristics in an IoT framework (Sicari et al. 2015).

IoT Security is the zone to concentrate on verifying the associated gadgets, ensuring information, and systems in the IoT (Yue et al. 2015). The figuring devices and implanted sensing instruments utilized in M2M (Machine-to-machine) correspondence, savvy domestic frameworks and in wearable widgets are the fundamental main thrusts of IoT (Minoli 2013). Feeble and deprived security practices and the flexibility structured in must be considered from the beginning, in both individual devices and entire frameworks. A huge number of extra web associated sensors in new areas and applications imply that the IoT world has expanded the intricacy of frameworks (Jan et al. 2016). With the continual increment in IoT devices, security issues are drastically increasing (Jing et al. 2014). In addition, customary security components can't be straightforwardly actualized to IoT innovations because of their structured system, for example restricted power just as this huge number of associated devices raise heterogeneity and adaptability issues (Sicari et al. 2015). The privacy and security of these frameworks can be jeopardized by a wide scope of dangers, both unsurprising and capricious, and consequently framework versatility ought to be a solid thought.

One of the most basic issue is heterogeneity, due to which security instruments that need to be coordinated into the IoT and has an impressive effect over the network security services that must be executed in the IoT (Roman et al. 2013). Devices will cooperate with different various devices either legitimately or via gateways (Vasilomanolakis et al. 2015; Botta et al. 2016). Security is needed in heterogeneity to conquer the difficulty of actualizing viable procedures and conventions on every device in IoT application (Sicari et al. 2015). In such situation, it is fundamental to actualize successful cryptographic systems that can give an extreme output and adjust trivial security practices that deal with end-to-end secure correspondence network. These procedures require credentials, so in this manner ideal key administration system must be executed to disperse these credentials and assist in setting up the essential session keys between companions (Roman et al. 2013).

Tending to adaptability for an extensive IoT organization is another major challenge. A critical problem is to give trustworthy resolutions, which are adaptable for huge number of devices that corresponds to various nearby or worldwide grids (Sicari et al. 2015; Issarny et al. 2011). Furthermore, many of them are portable devices and looking the area of and checking the uniqueness of specific item will be

a noteworthy issue for the IoT foundation (Sicari et al. 2015; Gubbi et al. 2013). In this way, key issues are the improvement of relevant methods that help heterogeneity and versatility, to anonymize client's information (Jara et al. 2013). Moreover, 398 H. Aldowah et al. IoT started to gain popularity in these recent years as due to the fact that increasing growth of network having devices connected via internet but still the concern will always remain security as one of the thing that must be taken care of in any network and in the scenario for IoT enabled architecture IoT will surely create a major impact in the world (Sicari et al. 2015).

So, this security concerned issue will always be an evergreen issue and this type of issue always needs to be addressed in on or the other way so that the practical implementation of IoT must be possible in real world (Jha and Sunil 2014) and this IoT enabled infrastructure can easily work (Roman et al. 2013). Security is a first and basic feature of an IoT infrastructure system and with some security features which are necessary for this infrastructure to work often deals with Trust management within network and features related to privacy in a system (Sicari et al. 2015). IoT Security is an open wide zone and security of connected devices must be emphasized by every part of the network, protecting data as well as authentication for the data in a network for the IoT (Yue et al. 2015).

The sensors which are used in various smart applications is the backbone of IoT infrastructure as they are used in the initial layer of IoT infrastructure called as perception or sensing layer (Minoli 2013). The logic of sensors is to sense the device and then to establish communication. The mechanism related to security or privacy need to be considered properly from the outside and inside in both single devices as well as in the whole network (Jan et al. 2016). It is said as if we assume a lot of connected devices are connected in a new location so surely the IoT infrastructure will increase the complexity of systems. The study says as the web associated devices gradually increasing with a massive rate so therefore the security issues will also be surely increased at an exponentially rate (Jing et al. 2014).

The complex thing in relation with IoT infrastructure is maintaining security which is difficult to apply straight away to IoT technologies due to their unique and complex infrastructure system and having limited power, so large network means wide range of web associated devices and because of that heterogeneity, scalability feature must be present. The safety of these devices in an IoT enabled network can be at risk for both predictable and unpredictable situations, and so the network security is of great concern for researchers. Heterogeneity is the common concern and complex issue with the issue related to security and should be embedded into the IoT infrastructure (Sicari et al. 2015) so that a major concern over an IoT network as well as security measures over network both feature to be implemented for real in IoT enabled infrastructure (Roman et al. 2013).

The Constrained devices present within a network can communicate with each other either directly or via gateways (Vasilomanolakis et al. 2015; Botta et al. 2016). The term Heterogeneity means different featured devices having IoT enabled feature are able to interact among them and this is a feature which needs to be implemented within security for implementing a unique, effective algorithms whose

feature is to give optimal results so that the protocols which work for the networking devices having IoT enabled feature must run smoothly (Sicari et al. 2015).

11.3 IoT Privacy Research Analysis

In scenario like an IoT environment, it is necessary to implement cryptographic algorithm and that must also behave in an efficient manner so that the throughput will be optimal as well as to support this security protocols that are easy in nature and can provide a communication channel having end to end connectivity over a proper communication channel and to do so the protocols must be secure with credentials so that systems having optimal key management distribute the credentials so that it is easy among the nodes for establishing session keys to make the communication secure and proper (Roman et al. 2013).

One more feature is the scalability among the network for a broad scale IoT network and its deployment is also another issue for the wide area IoT network (Sicari et al. 2015). The most challenging task for any open or wide network is always to provide reliable or effective solutions for an IoT based network and the environment must also be scalable and this scalability should be present in a global network (Sicari et al. 2015; Issarny et al. 2011). In an IoT network it is assumed that more of the objects are mobile objects and the concept in an IoT based network is to first sense the devices means finding the location and then to authenticate the devices for establishing an optimal communication channel and this authentication process is a complex task to get implemented in IoT network (Sicari et al. 2015; Gubbi et al. 2013).

The task to ensure scalability and to implement with respect to devices in an IoT based network is a complex task and as it is an open issue for the IoT based network (Jara et al. 2013). The threats related to Security are creating a major problem for IoT based devices. The concept to use network devices will always create problems for the IoT devices as the logic is to use devices having minimum capacity with easy going physical accessibility to sensors, so that the communication is smooth and easy among the network for communication among devices.

The most commonly known attacks used by hackers to disturb any large network is like for example DoS(Denial of Service)/DDoS(Distributed Denial of Service) attacks, man-in-the middle attacks and some problems which can disturb a healthy communication network is varied grid issue, application risk of IPv6, WLAN(Wireless Local Area Network) application and these issues (Haitao and Ying 2012; Tan and Han 2011; Henze et al. 2016) can also disrupt a fully functional IoT based infrastructure and moreover issues related to application layer security which must also be take care in mind while establishing an IoT infrastructure as access to information or data must be in a secure mode so that no one or any hacker can access the data unethically as well as authentication issue it means before making a secure connection the devices must clear that the other device they are making connection with must also be authentic else conflicts can also disturb the placement

of IoT security as well as the IoT infrastructure (Jing et al. 2014; Suo et al. 2013; Wan et al. 2013, 2014). According to the surveys and research related to IoT environment, there are mostly data security issues that can be commonly classified as: confidentiality, integrity, authenticity and data availability (Jing et al. 2014).

The issue which comes while deploying security over IoT infrastructure can get resolved if proper security measures can take place as the four issues mentioned above is confidentiality, integrity, authenticity, and data availability (Kim 2015, 2016). The confidentiality of data means the data travelling over any communication channel is in a secure medium so that any hacker if tries to find a path for accessing secured data they must fail, and this is possible only when security measures are more secure than any expectation. The term integrity of data deals with maintaining the accuracy or correctness of data. The term authenticity (Ning and Liu 2012) states that any invalid users are restricted to use network resource and available data which means there is no restriction for the authorized users to access data.

The IoT network is vulnerable to many threats. Securing an IoT network requires a lot of modern technology. As the increment of technology is taking place the vulnerability also comes with it. To make an infrastructure secure, properties such as identification, confidentiality, integrality and availability should be kept in mind to implement it with IoT enabled infrastructure (Kim 2015) so that the purpose of security in the network is established. The term authentication here deals with establishing a connection among the devices in a network and to secure concept of public and private keys via node to avoid data loss in a network.

The term confidentiality deals within the infrastructure of an IoT enabled device to check whether in communication no unauthorized user can communicate with authorized users in a network while data integrity means any data transmitting or present within a device must not get modified automatically or no wrong or corrupted data must receive at the receiver side while creating a high insecure environment over a network (Abomhara and Køien 2014).

11.4 Security and Privacy Concerns/Challenges

IoT architecture provides a secure communication for devices to interact and share info within a predefined network. Nowadays IoT creating a major impact in healthcare industry by making smart watches, smart homes, smart cities and much more has taken care of with this technology. The problems arise for this technology and the need to overcome these issues in an IoT based network so it can be faster, easily, reliable and consistent in communication.

- **No proper management for authentication/authorization**—as predicted for this network to take place many users as well as devices used to rely on easy and simple password which are easy to predict and hack. The password protection must be strong enough and changing from time to time.

- **Lack of transport encryption**—the encryption technique used by devices are light weighted. Most devices fail to encrypt data because of the light encryption technique used. So, in order to make a secure infrastructure an encryption technique that is easy and secure must be used.
- **Insecure web/mobile interface**—it is the application layer issue as mostly all IoT-based solutions have a web/mobile interface for device management or for management of data. The logic is that security breech can occur at any stage of the IoT layered design. For application layer, security must also be kept in mind before implementing this IoT technology.
- **Default credentials**—Generally default credentials (username or password) are used in most of the devices and sensors but it is not appropriate because once the hacker get to the details by any means then the network is in great danger to get exploited. Generally, default passwords are easy and simple. They make default passwords easy so that it would be convenient for user to remember but not modifying the credentials for a long time is indirectly giving threats to the network.
- **Privacy concerns**— the devices are being used in various domains, for example, in healthcare like smart watches have the feature to collect at least one piece of personal information and storing and analyzing it. Most devices featured to collect details about device credentials. The logical fact that devices used to transmit information across different networks and without the feature of encryption involves more privacy risks. Privacy risk mainly increases when the IoT objects gather information but are not secure.

A US-based software company tried to develop an IoT based secure travel product technology. The product that this company developed has the feature to provide real-time data about the location of the vehicles, people traveling on the vehicles and speed of vehicles which seems to be a complex task, but they managed to develop. The components involved with this technology include:

- Vehicle sensors
- Services
- Gateways
- Mobile interface
- Web interface

Some more things like modeling of any threat in a network using the help of STRIDE (spoofing, Tampering, Repudiation, Information disclosure, DoS, Elevation of privilege) software approach was done for the identification, attack scenarios and then formulate plans as shown in Table 11.1.

Table 11.1 Identifying/mitigating attacks using STRIDE

Components	Attack Scenarios	Mitigation
Gateway	Interception of and tempering with communication	Implement Secure Sockets Layer (SSL) transport layer security.
Services	DoS, sending large amounts of data based on spoofed identifier	Implement SSL transport layer security.
		Implement server monitoring for high traffic from a user.
Web Interface	Structured Query Language (SQL) injection attack on MySQL databases leading to data theft and database downtime	Use parameterized SQL statement.
		Sanitize user inputs for SQL injection.
Web app to third-party apps communication	Interception of and tempering with communication	Implement SSL transport layer security.
Data Stores	Weak database credentials that can pose privacy challenges	Gather only essential data.
		Implement strong database access controls per information security standards.

11.5 Theoretical Solutions Provided for IoT Technology

A new security solution proposed as DPBSV (Dynamic Prime Number Based Security Verification) (Puthal et al. 2017). This resolution exists because large data streams are being used with the logic of common key sharing and works as for getting updated periodically by getting synchronized with a pair of prime number for verification of security in real time on high data streams. Many studies and research have been done to get the optimality of this approach and to make sure that the protocol DPBSV always require less time to process and one more useful benefit of this approach is that it has the feature to prevent any malicious attack on big data stream.

Generally, most of the research about security challenges uses centralized approach (Hernández-Ramos et al. 2016) and a recent research study carried proposed fully distributed approach for IoT. For the architecture as well as for the implementation of this security mechanism for IoT the researchers have used an optimized approach said as ECC (Elliptic Curve Cryptography) approach (Ye et al. 2014). As designed for lightweight and flexible structure it is an ideal answer for resource constrained devices as it gives the advantage of dispersed security for methodology in an IoT framework to end-to-end security.

As indicated by researchers this arrangement has been tested utilizing AVISPA (Automated Validation of Internet Security Protocols and Applications) device and has additionally been executed in real over the Jennic/NXP JN5148 chipset dependent on a 32-bit RISC CPU and the outcomes are fruitful (Hernández-Ramos et al. 2016). The ECC a light weight algorithm provides authentication and access control to it. In this the access control work is to maintain authentication among sensory

nodes and devices. So, the risk at application layer can be minimized. Some proposed a thorough structural plan named as ARMY which depends on ARM (Architectural Reference Mode) (Hernández-Ramos et al. 2016). This architecture proposed is designed with different European IoT enterprises. For security based IoT model (Usman et al. 2017) a secure IOT SIT (Secure IoT) based on 64-bitblock cipher designed to deal with security and data encryption. Its architecture is a combination of Feistel cipher and a substitution-permutation. The researcher gave an explanation on this algorithm stating it is an encryption technique with light weight (Szczechowiak et al. 2008) and is better for IoT applications.

Some more software technique like SDN (Software Defined Network) and block chain technique are also present and can provide a massive security for IoT environment (Bull et al. 2016; Biswas and Muthukkumarasamy 2016). SDN on the other hand proposed its architecture and that can be used with Internet of Things and the logic behind this architecture is to perform anomaly detection. With block chain also multi layered security architecture is present to store heterogeneous IoT data. This helps in providing scalability and reliability.

11.6 Privacy or Security Solutions from Technical and Industry Areas

11.6.1 Impact of Security in Heterogeneous Environment

The solutions which are available for the IoT technology must be in working condition when used with applications and platform. The simple basic of IoT infrastructure depends on how private and secure this structure so that in near future no attacker must attack the privacy of that network. So before implementing the design the infrastructure phase for an IoT security must be studied and checked for better solution to heterogeneous environments and proper information and guidance for user's environment. To keep track of sensitive data, risk assessment, infrastructure etc. features which can develop an IoT infrastructure into a better technology and for that organizations must have ongoing researchers, labs that need to implement study. A person named Harbor research has developed an approach to IoT security and has given a three-step approach to monitor organizations or individuals involved in the maintenance for IoT security (Harbor White Paper 2016).

To guarantee a safe IoT arrangement over the whole authoritative grid, the planned solutions for IoT security must have five key functionalities as: data encryption, security, identification, client access and the board, and investigation. Thus, a protected end-to-end correspondence between the IoT devices, data centers and cloud models can be guaranteed. Application of primary security functions is to guarantee a safe IoT deployment over the whole hierarchical network to have a secure IoT design so that in near future the deployment of that infrastructure across multiple organization and with their related networks. A secure end-to-end

communication needed so that authentication is not a problem in between the devices to IoT inbuilt feature with data centers and architecture for cloud-based technology.

11.6.2 Industrial Solutions

Security is a key challenge in IoT environment, and the steps involved are first by checking the design accordingly and then the security must be maintained by the feature related to design (Jha and Sunil 2014). Secondly data minimization concept and lastly the transparency among the consumers must be maintained so no unexpected issues or error occurs.

11.6.2.1 Security Embedded with Respect to IOT Design

The concept to implement Security for IoT devices depends on various entities, like sensitive data present and to maintain that data properly. Ramirez (2015) presented some of these ideas for these related issues such as

At the design phase the security check assessment should be done.
The protection for sensitive data among devices having a proper storage management.
The analysis and monitoring of IoT devices in a network and regular updates of software so it will be up to date always and always to have a proper security measures, the organizations or anyone using the IoT enabled infrastructure environment should have various guiding conferences to employ administrative and technical privileges and full training module for technical employees.

The security measures should be considered starting from startup of the device to establishment of secure computing environment (Shipley 2015; Schaub et al. 2015). The researchers claimed that security for an IoT device must be in working state for its entire lifespan and regular update must be present to improve the device at regular intervals and the steps or the phases included in this approach are

- Secure booting
- Access control
- Device authentication
- Firewalling and IPS, and
- Updates and patches.

11.6.2.2 Data Minimization

This technique came into existence so the organizations using this IoT enabled infrastructure must maintain data repository while defining its time and duration also so that the creation and existence must exists in the form of records for data so that there is no alteration on data or on its information. The data used must have a specific lifetime so that data can get discarded also if not required and as data gets increased in future, large data repositories will be used and that can make the network vulnerable, so again concept of security came for existence.

11.6.2.3 Transparency Among Consumers

Since increasing industrial transparency is one of the necessary requirements, it will surely set ground work for successful solution to privacy in IoT. This goal can be accomplished either by governmental regulation or industry self-regulation involves receiving of meaning consent from consumer before data collection

11.7 Conclusion

The aim for this chapter has provided with an idea to raise an issue for security and privacy concern on IoT enabled infrastructure. As for any network infrastructure the basic requirement is security measures so that the infrastructure becomes strong enough to handle any attack and has the feature to secure itself. As the current research says as IoT enabled devices still used to face a lot of challenges to overcome any issue related to IoT. Heterogeneity is featured so that different origin devices can interact among IoT enabled devices.

The four basic needs of security like identification, confidentiality, integrality and availability must be considered while establishing a secure infrastructure for IoT. There will always be some vulnerabilities or potential gaps for a network infrastructure because nothing can be perfect, but it is good to provide as much security as possible because it helps in avoiding hackers to attack and to destroy the network environment. There are some key aspects that any organizations must keep into consideration to implement and enhance the security aspect of IoT by implementing features like minimization of data or secure authentication.

The logic to implement IoT enabled feature comprises a proper set of social, technological, and policy considerations across various areas. It is required to enable the use of IoT feature for real in live environment in technological developments. Effective measures have been taken for production, engineering, academic world and industry to provide measures for the efficient and safe use of these developments which are clearly needed for further research work in the future or to more secure the IoT framework in future.

References

Abomhara, M., & Køien, G. M. (2014). Security and privacy in the Internet of Things: Current status and open issues. *International Conference on Privacy and Security in Mobile Systems (PRISMS). IEEE*.

Aldowah, H., et al. (2017). Internet of Things in higher education: A study on future learning. In: Journal of Physics: Conference Series. IOP Publishing.

Bandyopadhyay, D., & Sen, J. (2011). Internet of Things: Applications and challenges in technology and standardization. *Wireless Personal Communications, 58*(1), 49–69.

Biswas, K., Muthukkumarasamy, V. (2016). Securing smart cities using blockchain technology. In: IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/Smart City/DSS). IEEE.

Botta, A., et al. (2016). Integration of cloud computing and Internet of Things: A survey. *Future Generation Computing Systems, 56*, 684–700.

Bull, P., et al. (2016). Flow based security for IoT devices using an SDN gateway. In: IEEE 4thInternational Conference on Future Internet of Things and Cloud (FiCloud). IEEE.

Gen, H.P.-C.S.A. Controllers, R. (2015). Hewlett-Packard Enterprise Development LP. Citeseer.

Gubbi, J., et al. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computing Systems, 29*(7), 1645–1660.

Haitao, L. B. C. H. W., & Ying, F. (2012). Security analysis and security model research on IOT. *Computer & Digital Engineering, 11*, 006.

Harbor White Paper. (2016). Security for the Internet of Things. *The Harbor Restaurant, 16*, 1–16.

Henze, M., et al. (2016). A comprehensive approach to privacy in the cloud-based Internet of Things. *Future Generation Computing Systems, 56*, 701–718.

Hernández-Ramos, J. L., et al. (2016). DCapBAC: embedding authorization logic into smart things through ECC optimizations. *International Journal of Computer Mathematics, 93*(2), 345–366.

Issarny, V., et al. (2011). Service-oriented middleware for the future internet: State of the art and research directions. *Journal of Internet Services and Applications, 2*(1), 23–45.

Jan, S., et al. (2016). Applications and challenges faced by Internet of Things – A survey. *International Journal of Engineering Trends and Applications*,. ISSN: 2393–9516.

Jara, A. J., Kafle, V. P., & Skarmeta, A. F. (2013). Secure and scalable mobility management scheme for the Internet of Things integration in the future internet architecture. *International Journal of Ad Hoc and Ubiquitous Computing, 13*(3–4), 228–242.

Jha, A., & Sunil, M. (2014). *Security considerations for Internet of Things*. Vadodara: L&T Technology Services.

Jing, Q., et al. (2014). Security of the Internet of Things: perspectives and challenges. *Wireless Networks, 20*(8), 2481–2501.

Kim, J. T. (2015). Requirement of security for IoT application based on gateway system. *Communications, 9*(10), 201–208.

Kim, J. T. (2016). Analyses of requirement for secure IoT gateway and assessment. International information institute (Tokyo). *Information, 19*(3), 833.

Minoli, D. (2013). *Building the Internet of Things with IPv6 and MIPv6: The evolving World ofM2M communications*. Hoboken: Wiley.

Miorandi, D., et al. (2012). Internet of Things: vision, applications and research challenges. *Ad Hoc Networks, 10*(7), 1497–1516.

Ning, H., & Liu, H. (2012). Cyber-physical-social based security architecture for future Internet of Things. *Advances in Internet of Things, 2*(01), 1.

Puthal, D., et al. (2017). A dynamic prime number based efficient security mechanism for big sensing data streams. *Journal of Computer and System Sciences, 83*(1), 22–42.

Ramirez, E. (2015). *Privacy and the IoT: Navigating policy issues*. Washington: US FTC.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. *Computer Networks, 57*(10), 2266–2279.

Schaub, F., et al. (2015). A design space for effective privacy notices. In: Eleventh Symposium on Usable Privacy and Security (SOUPS 2015) Security in Internet of Things: Issues, Challenges and Solutions 405

Shipley, A. (2015). *Security in the Internet of Things*. Wind River, September 2014.

Sicari, S., et al. (2015). Security, privacy and trust in Internet of Things: the road ahead. *Computer Networks, 76*, 146–164.

Sundmaeker, H., et al. (2010). *Vision and challenges for realising the Internet of Things. Cluster of European research projects on the Internet of Things*. Brussels: European Commission.

Suo, H., et al. (2013). Security and privacy in mobile cloud computing. In: 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC). IEEE.

Szczechowiak, P., et al. (2008). NanoECC: Testing the limits of elliptic curve cryptography in sensor networks. In *Wireless sensor networks* (pp. 305–320). Berlin: Springer.

Tan, Y., & Han, J. (2011). Service-oriented middleware model for Internet of Things. *Computer Science, 38*(3), 23–45.

Ul Rehman, A., & Manickam, S. (2016). A study of smart home environment and its security threats. *International Journal of Reliability, Quality and Safety Engineering, 23*(03), 1640005.

Usman, M., et al. (2017). Sit: a lightweight encryption algorithm for secure Internet of Things. arXiv preprint arXiv:1704.08688.

Van Kranenburg, R. (2008). *A critique of ambient technology and the all-seeing network of RFID*. Amsterdam: The Netherlands Institute of Network Culture.

Vasilomanolakis, E., et al. (2015). On the security and privacy of Internet of Things architectures and systems. In: 2015 International Workshop on Secure Internet of Things (SIoT). IEEE.

Wan, J., et al. (2013). From machine-to-machine communications towards cyber-physical systems. *Computer Science and Information Systems, 10*(3), 1105–1128.

Wan, J., et al. (2014). VCMIA: a novel architecture for integrating vehicular cyber-physical systems and mobile cloud computing. *Mobile Networks and Applications, 19*(2), 153–160.

Ye, N., et al. (2014). An efficient authentication and access control scheme for perception layer of Internet of Things. *Applied Mathematics & Information Sciences, 8*(4), 1617.

Yue, X., et al. (2015). Cloud-assisted industrial cyber-physical systems: An insight. *Microprocessors and Microsystems, 39*(8), 1262–1270.

Part IV
The IoT World of Applications

Chapter 12
Mobile Computing and IoT: Radio Spectrum Requirement for Timely and Reliable Message Delivery Over Internet of Vehicles (IoVs)

Elias Eze, Paul Sant, Sijing Zhang, Xiaohua Feng, Mitul Shukla, Joy Eze, and Enjie Liu

Abstract This Chapter studied the required amount of radio spectral resource enough to support timely and reliable vehicular communication via vehicular ad-hoc networks (VANETs). The study focussed on both DSRC/WAVE and the European standard ITS-G5 that are based on recently approved IEEE 802.11p specification, which uses a simplified version of CSMA/CA as MAC protocol, and an STDMA MAC recently proposed by European Telecommunications Standards Institute (ETSI). The Chapter further carried out a feasibility analysis of radio spectrum requirement for timely and reliable vehicle-to-vehicle (V2V) communication. In the feasibility analysis, synchronized STDMA MAC is compared with the CSMA/CA MAC protocol, which 802.11p is based on. Message Reception Failure (MRF) probability is used as a performance metric to investigate and ascertain the minimum spectrum requirement for efficient, timely, and reliable V2V communication. Simulation results show that even at the same allocation of 10 MHz channel bandwidth, STDMA MAC outperforms the CSMA/CA based MACs due to the fact that STDMA based MACs provide a structured shared medium access and prevent negative impact of unhealthy contention for shared channel access. The results further show that up to 40 MHz channel bandwidth over 5.9GHz band would be required to guarantee optimal reliability of safety packets exchange in vehicular networks as opposed to 10 MHz allocated in US.

Keywords Mobile computing · IoTs · IoVs · Intelligent Transportation System (ITS) · VANETs

E. Eze (✉) · P. Sant · S. Zhang · X. Feng · M. Shukla · J. Eze · E. Liu
Department of Computer Science and Technology, University of Bedfordshire, Luton, UK
e-mail: elias.eze1@beds.ac.uk; paul.sant@beds.ac.uk; sijing.zhang@beds.ac.uk; xiaohua.feng@beds.ac.uk; mitul.shukla@beds.ac.uk; joy.eze1@study.beds.ac.uk; enjie.liu@beds.ac.uk

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_12

12.1 Introduction

Although several studies have dwelled on different approaches of guaranteeing data packets transmission in vehicular networks with minimum tolerable latency, this study focused on the actual amount of radio spectrum required for reliable and timely road traffic safety communication since the key part of the emerging ITS applications hugely depend on real-time, delay-sensitive V2V and vehicle-to-Infrastructure (V2I) communications. Communication experts expect that at the end of 2020, smart vehicles will be manufactured and fully equipped with wireless electronic communication devices and multi-sensors that will enable them to prevent any vehicle collision that may occur with the help of timely and reliable vehicular information communication (i.e., exchange) (Eze et al. 2015; FTC Staff Report 2015). This exchange of road traffic safety messages is meant to provide vehicle drivers with safety alerts to warn them of impending traffic situations that may lead to road accidents. Thus, in VANETs, road traffic safety is accomplished with the help of two categories of messages, namely; (1) Cooperative Awareness Message (CAM) (ETSI TS 102 637-2 V1.2.1 2011), and (2) Decentralized Environment Notification Message (DENM) (ETSI TS 102 637-3 V1.1.1 2010). The CAM is a periodically generated and broadcasted short messages, which notifies the neighboring vehicles within one-hop transmission range about the sender's status information such as direction of movement, velocity, location, etc. The DENM, on the other hand, is used to alert nearby vehicles about an emergency like a situation that may lead to vehicle collision or an actual occurrence of accident along the road. Therefore, the efficiency of any road traffic safety application wholly relies on reliable and timely dissemination of these messages with minimum latency to ensure that the neighboring vehicles receive the broadcasted packets and on time, to enable them to take appropriate actions that can prevent the imminent road accident.

With reference to the considerable existing and on-going research and standardization efforts by academia, industries, and government agencies as discussed in detail in our previous survey article (Eze et al. 2016a), the development of DSRC/WAVE standard and the European standard ITS-G5 have been seen as the most current significant efforts to actualize the long anticipated vehicular network. However, both DSRC/WAVE and the European standard ITS-G5 are based on recently approved IEEE 802.11p specification, which uses a simplified version of CSMA/CA as MAC protocol that is usually characterized by unbounded media access delay and best-effort quality. In order to provide an alternative delay-sensitive MAC protocol for future vehicular network ITS-G5 system, ETSI recently proposed an STDMA MAC (Ma and Mathew 2015).

Recent studies conducted to investigate the performance of IEEE 802.11p-based vehicular safety communication system have identified its reliability and scalability challenges especially in high density vehicular networks such as urban or multi-lane highway vehicular network scenarios (Eichler 2007; Kosch et al. 2006; Kloiber et al. 2011). In the same vein, the authors in (Sethi et al. 2015; Alam and Sadaf 2015a, b; Shakil et al. 2015; Alam et al. 2015) have investigated Cloud computing,

which is an area of interest in terms of IoVs scalability. One of the possible explanations responsible for these reliability and scalability issues is inadequate and insufficient allocation of radio spectrum to V2V communication systems. In the US, the FCC has allocated 75 MHz bandwidth to WAVE-based ITS services within the 5.850GHz–5.925GHz band where only 10 MHz radio spectrum is dedicated to critical road safety application. In Europe, the situation is similar where radio spectrum of 10 MHz CCH is allocated to life-saving safety messages out of the 30 MHz bandwidth available in the allotted 5.875GHz – 5.905GHz band for vehicular communication systems (Soriga 2012). Generally, there are no well-established literatures yet on this issue to ascertain whether this allocated 10 MHz bandwidth would be sufficient for critical safety messages in CCH except an initial study conducted by CEPT (Department for Transport 2012). Hence, in this Chapter, an in-depth study of the required amount of radio spectrum sufficient to guarantee reliable and minimum latency requirement of critical road safety messages is carried out. Furthermore, a feasibility analysis of radio spectrum requirement for scalable and reliable vehicular safety communication is carried out. In the feasibility analysis, synchronized STDMA MAC protocol is compared with the DSRC/WAVE and European standard ITS-G5, which are based on IEEE 802.11p specification generally known for its unbounded media access delay and best-effort quality, as well as scalability and reliability issues. Additionally, the Message Reception Failure (MRF) is used as a performance metric to investigate and ascertain the minimum spectrum requirement for efficient, scalable, and reliable road traffic safety communication system.

12.2 System Model

In this research, it is assumed that the mobile vehicles are fully equipped with multi-sensors and radio transceivers specifically dedicated for road traffic safety communication systems. Figure 12.1 illustrates how DENMs are automatically generated at the event of an emergency like a road accident and broadcasted to neighboring vehicles within several hundred meters (i.e., one-hop) range with minimum latency. Additionally, all the mobile vehicles constantly check and monitor the advertisements and other activities on the CCH when those vehicles are not broadcasting either periodic CAMs or even-driven DENMs. If the intended neighboring receivers fail to receive or correctly receive the broadcasted message with acceptable minimum delay due to obvious reasons, the transmission will be considered lost and results in decreased probability of MRF (P_{MFR}), accordingly. The performance metric P_{MFR} as a measure for both CAMs and DENMs broadcast reliability, is given as the relationship of the number of transmitted messages that meet the acceptable minimum delay $N_{Min,\ Del}$ to the total number of transmitted messages N_{Total} over the vehicular communication network. Mathematically, the probability of MRF can be expressed as

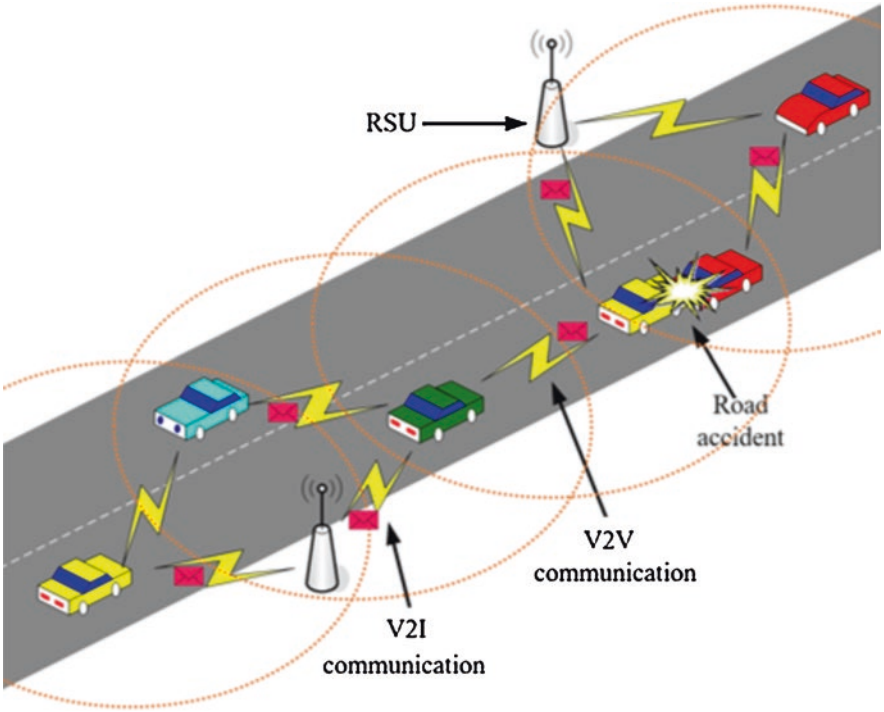


Fig. 12.1 System model of safety communication for mobile IoVs' traffic

$$P_{MFR} = \frac{N_{\min,Del}}{N_{Total}} \tag{12.1}$$

12.2.1 MAC Layer Models

Two different types of access protocols, namely STDMA and CSMA/CA based MAC schemes were implemented to effectively provide balanced assessment of minimum spectrum requirement necessary for reliable road safety vehicular communication with a guaranteed acceptable minimum latency. It is noteworthy to mention that both STDMA and CSMA/CA based MAC protocols are usually applied to control the shared medium access contention over the single medium specifically dedicated for road traffic safety application.

12.2.1.1 CSMA/CA Based MAC Algorithm

The recently approved 802.11p specification MAC algorithm employs the same exponential back-off procedures that is implemented by legacy IEEE 802.11 family. Hence, in accordance with the carrier sensing mechanism, each transmitter must first sense the channel to ensure that it is at least idle for a stipulated AIFS period of time prior to actually accessing the shared channel for packets transmission. Figure 12.2 shows a typical CSMA/CA based MAC algorithm. In the case where the shared medium becomes busy or occupied within the stipulated AIFS period of time, the transmitting vehicle must defer its shared medium access for another randomized time period specified by the contention window (CW). Unfortunately, under saturated vehicular network environment with increasing contention for channel access due to high channel load, a typical vehicular network, which uses

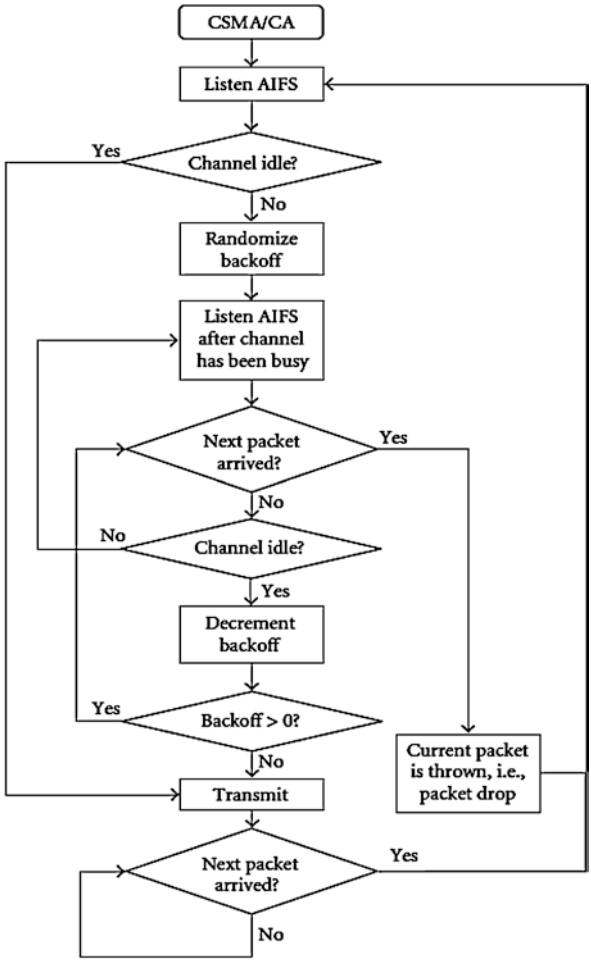


Fig. 12.2 CSMA/CA based MAC procedure in accordance with IEEE 802.11p/DSRC using a vehicular traffic model with broadcasted time-driven packets at pre-determined rates (i.e., at every 100 ms)

CSMA/CA based MAC scheme for shared channel access will certainly experience an unpredictable and exponentially increasing media access delay.

Although the issue of high shared media access delay in vehicular network has been treated in (Eze et al. 2016b) by ensuring the provision of acceptable minimum delay to safety-related messages for inter-vehicle communications in the proposed CARER protocol. In CARER protocol, the widely used priority-based IEEE 802.11e EDCA scheme is adopted and enhanced for service differentiation. However, in a highly saturated network scenario in a busy traffic which is generally the case in urban or city areas, especially during the rush hours in the morning and evening times, it is obvious that the media access delay may become unpredictable given the increased amount of communication load and overhead due to saturation in the channel. Consequently, there is a dire need to propose and implement a MAC scheme capable of guaranteeing reliable transmission of road traffic safety-related packets with minimum acceptable delay in vehicular networks.

12.2.1.2 STDMA Based MAC Algorithm

Unlike CSMA/CA based MAC schemes, whose shared media access delay becomes unpredictable and exponentially increases with increase in network/channel load, the STDMA based MAC schemes use a synchronized time-slot structure to guarantee reliable data packet transmission with a bounded media access latency even in highly saturated and congested network scenarios. Figure 12.3 shows a typical STDMA based MAC algorithm. Originally, this type of MAC scheme was first proposed and implemented for efficient coordination of maritime traffic (ITU-R M.1371-4 2010).

With STDMA, each vehicle in a vehicular communication network begins by first listening to the activities in the channel for a period of one-time frame in order to discover which timeslots are currently busy with the broadcasting of data packets from other vehicles. As a result, some nominal transmission slots (NTSs) will eventually be selected for the transmission of each data packet during one frame. Each of the few selected NTSs is usually picked from the available group of empty timeslots, which is called selection interval (SI). Then, where there are no available unoccupied timeslots within the SI, the timeslot occupied by the furthest away mobile node will be re-used, otherwise one slot will be randomly selected from the available group of empty slots. Hence, until another NTS is chosen by the use of the same procedure as described above, the originally selected NTS will continually be made use of, at least for a few successive frames. Consequently, the above illustrated mechanism helps to guarantee that the shared media access delay associated with STDMA based MAC schemes are reduced to the acceptable minimum level by ensuring that the shared media access delay is upper-bound by the length of the interval (i.e., the SI).

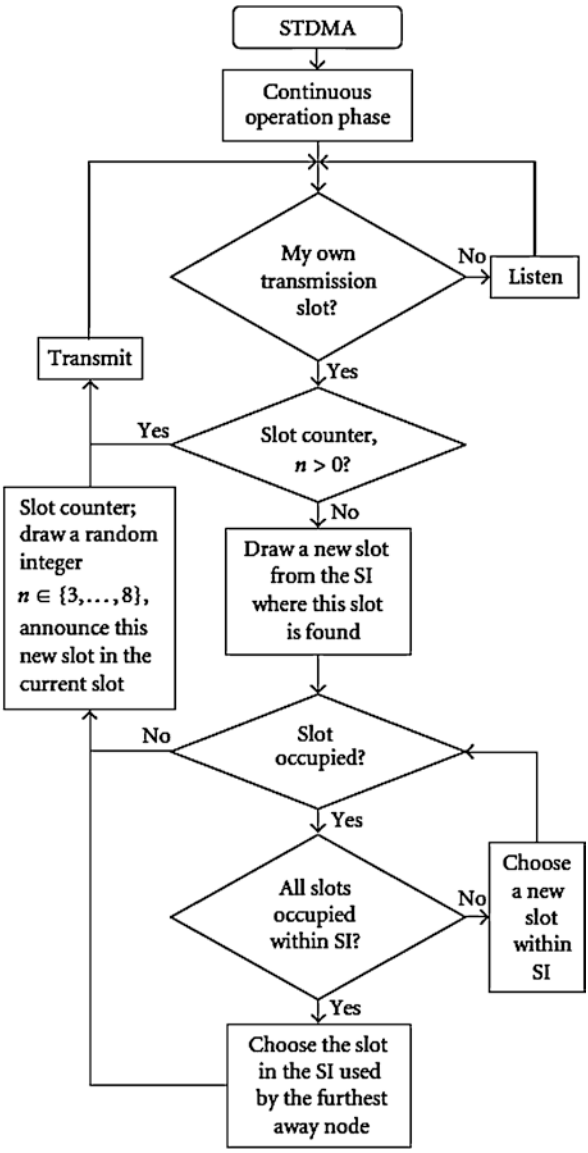


Fig. 12.3 STDMA based MAC procedure using a vehicular traffic model with broadcasted time-driven packets at pre-determined rates (i.e., at every 100 ms)

12.2.2 PHY Layer Model

In accordance with IEEE 802.11a specification, this study adopted a PHY layer model based on OFDM technique. Furthermore, in order to ensure the tractability of the simulation experiments while highlighting the correlation that exist between channel bandwidth and data packets transmission reliability, a simplification was made by assuming that a dynamic modulation scheme with a minimum SINR

threshold θ and a constant data rate is adopted to guarantee that the received packets will be successfully decoded. The minimum SINR θ can be expressed as

$$SINR = \frac{P_s}{\left(\sum_{n=0}^{N} P_{i,n} + N_0\right)} \geq \theta \tag{12.2}$$

where P_s denotes the strength of the received signal, $P_{i,n}$ represents the interference effect received from the current active transmitter, and N_0 is the single side thermal noise power spectral density. Additionally, the study is also based on the assumption that link data rate in a typical wireless network increases proportionally with respect to the amount of available channel bandwidth. As an example, a QPSK modulation scheme can achieve a link data rate of 6Mbps in a 10 MHz channel and the increment in data rate can double up to 12Mbps in a 20 MHz channel, accordingly.

Nevertheless, the assumption is rather optimistic given that the effect of Doppler fading as well as root mean square (RMS) delay spread in vehicular communication network media can impact the spectrum efficiency negatively with an increasing channel bandwidth (Strom 2011). Thus, representing the power delay profile (PDP) of the vehicular network channel also called the multi-path intensity profile by $A_c(\tau)$, which signifies the average power inherent in a given multi-path delay, it would be easily computed empirically. Hence, both the average delay of the channel and RMS delay spread can be easily expressed in terms of the PDP $A_c(\tau)$ as

$$T_{Av} = \frac{\int_0^{\omega} \tau A_c(\tau)\, d\tau}{\int_0^{\infty} A_c(\tau)\, d\tau} \tag{12.3}$$

and

$$T_{RMS} = \sqrt{\frac{\int_0^{\omega} (\tau - T_{Av})^2 A_c(\tau)\, d\tau}{\int_0^{\infty} A_c(\tau)\, d\tau}} \tag{12.4}$$

It is noteworthy to mention that if the probability density function (PDF) pT_r of the random delay spread T_r is expressed in terms of$A_c(\tau)$as

$$pT_r(\tau) = \frac{A_c(\tau)}{\int_0^{\infty} A_c(\tau)\, d\tau} \tag{12.5}$$

Thus, relative to the PDF, T_{Av} and T_{RMS} denote the average and RMS values of the random delay spread T_r, respectively. Consequently, defining the average and RMS delay spread using Eq. (12.3) and Eq. (12.4), respectively, or equivalently, evaluating the PDF of T_r using Eq. (12.5) measures the overall latency associated with a particular multi-path component by its relative power, in order to ensure that weak

multi-path components do not greatly increase the associated delay spread as opposed to strong multi-path components. In other words, the multi-path components that are below the stipulated noise threshold (i.e., noise floor) like the weak multi-path components will certainly not be able to significantly affect these characterizations of the delay spread.

Similarly, the delay spread associated with vehicular communication channel can be roughly characterized using the random time delay T_r with $A_c(\tau)$ asymptotically equal to zero for $\tau \geq T_r$. Typically, the approximated value is mostly assumed to be the achievable RMS delay spread, that is, $T_r = T_{RMS}$. Note that a linearly modulated transmission signal with symbol duration D_s using the above assumed approximation can suffer a significant Inter Symbol Interference (ISI), especially if D_s is much less than T_r. On the contrary, a linearly modulated transmission signal with symbol duration D_s under similar condition can suffer a negligible ISI when D_s is much greater than T_r. Obviously, it can be assumed that $D_s \ll T_r$ implies that $D_s < T_r/10$, and in the same manner, $D_s \gg T_r$ automatically implies that $D_s > 10T_r$. Accordingly, depending on the details of the channel, when D_s does not exceed a relatively acceptable minimum order of magnitude of T_r, it means that the system will likely experience a degree of ISI that may or may not lead to significant performance degradation. Therefore, the significance of delay spread depends on how it impacts on the ISI. In other words, if the symbol period D_s is long enough in contrast to the delay spread, then an equivalent ISI-free vehicular communication channel can be expected. On average, a symbol period that is 10 times as big in contrast to the achievable delay spread would be good enough to obtain an equivalent ISI-free vehicular communication channel. Similarly, the correlation between the delay spread and the frequency domain is the concept of Coherence Bandwidth (CB), which is the available bandwidth over which the communication channel can be presumed to be flat. In other words, the CB is directly related to the inverse of the obtainable delay spread. Thus, the larger the CB, the shorter the delay spread.

12.3 Performance Analysis

In this Section, the efficiency of both CSMA/CA and STDMA based MAC algorithms are investigated through performance analysis carried out as a measure of the probability of message reception failure, and RMS delay spread.

12.3.1 Safety Message Transmission (MAC-to-MAC) Delay

Providing channel access while ensuring the guarantee of QoS provision in terms of reliability and delay is a challenging but crucial task of the MAC layer. In a typical safety vehicular communication, not only is guaranteed transmission reliability highly required, but a predictable and acceptable minimum MAC-to-MAC delay

(Sjöberg et al. 2011), which contributes to timely transmission and reception of safety packets, is equally highly required. Road traffic safety related packets must be transmitted and received within a minimum attainable delay T_{dl}, which means that such high priority, delay-sensitive, time-critical packets must be delivered on time to the vehicles within the zone of interest (ZoI), i.e. the zone (or area) where a traffic emergency has occurred or is about to occur. Thus, in this contribution, MAC-to-MAC delays a performance metric is adopted for measuring the performance and efficiency of the MAC solutions (i.e. CSMA/CA and STDMA based MAC algorithms) investigated in the study. Hence, in both MAC algorithms, safety related packet transmission and reception deadline τ_{dl} can only be satisfied if and only if the deadline is bigger than MAC-to-MAC delay, T_{m2m}. That is, $T_{dl} > T_{m2m}$. In other words, T_{m2m} can be given as the total aggregate of the shared media access delay T_{ca}, packet propagation delay T_{pp}, and packet decoding delay T_{pd}. In Fig. 12.4, a shared medium access request at the source vehicle (Tx) occurs at t_0, and the length of period from t_0 to t_d represents the total MAC-to-MAC delay, since the message is successfully decoded at t_d. Thus, the following delays make up the total safety message transmission delay:

- **Channel (or Media) access delay**, T_{ca} represents the length of duration taken by a transmitter starting from media access request up to the time of actual packet transmission. For road traffic safety vehicular communication, a safety packet will be dropped if the deadline is lesser that the channel access delay, that is, $T_{dl} < T_{ca}$. This is as a result of the fact that when the media access delay of a particular safety message tends to infinity, i.e. $T_{ca} \rightarrow \infty$, its deadline expires, and it gets dropped at the source vehicle given that another new packet with updated kinematic details is generated periodically at least every 100 ms. Thus, once a new packet is generated, the old one is no longer relevant since the vehicle most have changed location due to mobility.

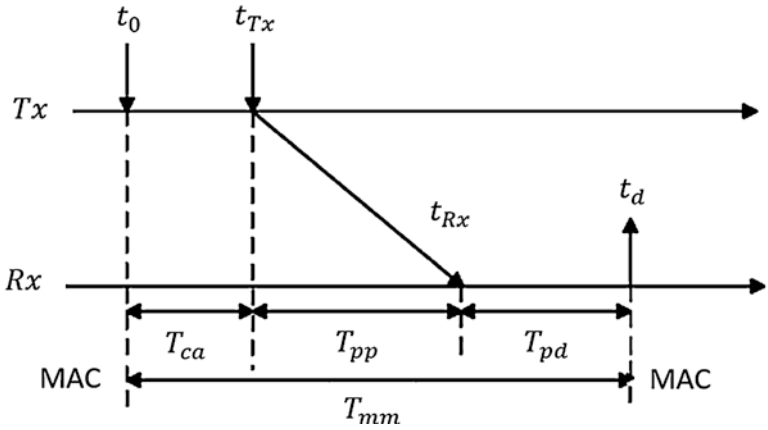


Fig. 12.4 Safety message transmission (MAC-to-MAC) delay

- **Packet propagation delay**, T_{pp} denotes the actual length of duration it takes the transmitted signal (i.e., packet) to travel from the source vehicle (i.e., the transmitter) to the receiver. Therefore, depending on the routing approach applied, if the routing is not successful due to intermediate node break-down, then$T_{pp} \rightarrow \infty$.
- **Packet decoding delay**, T_{pd} denotes the actual length of duration taken to convey a successfully decoded message to the upper layers of the recipient vehicle. It follows that $T_{pd} \rightarrow \infty$ if the decoding is not successful as a result of fading effect, interference or noise.

  Finally, total MAC-to-MAC delay T_{tdl} is given as

$$T_{tdl} = T_{ca} + T_{pp} + T_{pd} \tag{12.6}$$

It is noteworthy to mention that the critical safety/emergency alert is generally very short. Thus, its transmission time is omitted here. Hence, reliable and timely safety vehicular communication is said to be achieved if transmitted safety-related packet meets a hard deadline since missing the hard deadline could result in fatal costs or penalties such as vehicle collisions on the road, which mostly leads to loss of lives and properties. Specifically, in this study, it is said that a particular MAC (either CSMA/CA or STDMA based MAC) performed well if and only if at least 90% of all the received packets maintain media access delay that is less or equal to the deadline (i.e., 100 ms), otherwise such MAC performance is adjudged poor, and does not meet the hard deadline.

12.3.2 Simulation Setup

In this section, a comparison of the implemented CSMA/CA and STDMA based MAC approaches for vehicular communication is shown using simulation experiments, focusing on urban-highway scenarios with 150 vehicles, 300 vehicles, and 500 vehicles.

12.3.3 Simulation Settings and Assumptions

In this section, CSMA/CA and STDMA based MAC for vehicular communication were implemented in order to investigate the spectrum requirement of the two MACs and evaluate their performance in terms of transmission reliability using MatLab (Mathworks [Online]. Available at: http://uk.mathworks.com/products/matlab/). Similarly, close to real-life urban-highway vehicular network scenarios were simulated using sets of realistic parameter settings, which are commonly applied in the literature. For the purpose of minimum spectrum requirement for reliable vehicular communication and other obvious reasons, a typical urban-highway

is used, which has been considered (Eze et al. 2014, 2016b) as the worst-case scenario in term of high spectrum requirement and need for minimum acceptable delay for efficient road traffic safety communication as a result of high vehicle density, mobility and rapid topology changes (Kloiber et al. 2011). The urban-highway vehicular road considered in this simulation experiments is a 5×5 Manhattan grid road network as depicted in Fig. 12.5 with 2000 m edge length and BonnMotion tool (Nils et al. 2010) to generate suitable node mobility model. The arrival of vehicles is modelled as a Poisson process on each of the lanes with arrival interval of 3 seconds. The roads consist of eight (8) lanes of 5 m width with four (4) lanes on opposite direction.

In this simulation experiments, each of the lanes were assigned a different average speed in order to ensure that the dynamics associated with road safety vehicular communication is reflected in the simulated scenarios. Similarly, the velocity of the mobile nodes on each of the lanes obeys a normal distribution with the assigned velocity and a standard deviation of 1 m/s. The velocity of the outer most lane is set at 90 km/h, the three inner-most lanes are assigned the average speed of 130 km/h, and that of the one middle lane is 108 km/h. Thus, for this evaluation, the chosen set is the most critical especially for road traffic safety communication, that is, high dense vehicular traffic with fast moving vehicles. The vehicular traffic density, on average, is approximately eleven (11) mobile vehicles per kilometres on each of the lanes.

The safety-related data packet traffic that each vehicle generates are periodic CAM for vehicle status information awareness creation, and event-triggered DENM to inform other neighboring vehicles of an accident or impending vehicle accident. With either of these safety-related data packet traffic, each mobile node's initial broadcasting duration is random and independent. For the size of a safety packet,

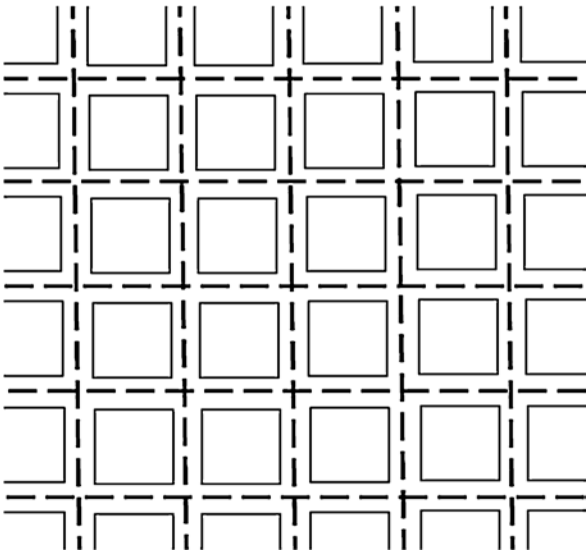


Fig. 12.5 A typical 5×5 Manhattan grid road network

the FCC standard recommended a 300byte message size as specified in IEEE 802.11p/DSRC specification with repetition rate of 10 Hz, while the ETSI suggested that safety related packets be broadcasted in 800bytes packet size using repetition rate of mere 2 Hz. The US standard IEEE 802.11p/DSRC specification is adopted in this simulation experiments since virtually all the use-cases that are based on either DENM or CAM demand a maximum delay of 100 ms with minimum periodic update frequency of 10 Hz (FTC Staff Report 2015; ETSI TR 102 638 V1.1.1 2009).

Similarly, a combination of Nakagami-m (Nakagami 1960) and dual-slope piecewise-linear model for fading effects (Cheng et al. 2007) and distance dependent path-loss (Torrent-Moreno et al. 2009), respectively, are used as the channel propagation model in the simulator. The parameters for the Nakagami radio propagation model were fine-tuned according to the reported actual measurements contained in (Taliwal et al. 2004). Furthermore, the piecewise-linear model uses a path-loss exponent γ_1 as well as standard deviation φ_1 within a critical safe distance d_c. Then, beyond this critical safe distance, the signal strength weakens with another path-loss exponent γ_2 and standard deviation φ_2. In a typical urban-highway vehicular environment, this dual-slope piecewise-linear model for a distance dependent path-loss is presented through a widely adopted log-normal model and expressed as

$$P(d) = \begin{cases} P(d_0) - 10\gamma_1 \log_{10} \frac{d}{d_0} + Y_{\varphi 1}, & d_0 \le d \le d_c \\ P(d_0) - 10\gamma_1 \log_{10} \frac{d_c}{d_0} - 10\gamma_2 \log_{10} \frac{d_c}{d_0} + Y_{\varphi 2}, & d > d_c \end{cases} \tag{12.7}$$

where $P(d)$ denotes the received signal strength at distance d, $P(d_0)$ represents its counterpart at reference distance d_0, $(Y_{\varphi 1}, Y_{\varphi 2}) \in Y_{\varphi}$ denotes a zero-mean, which is usually a randomly distributed variable characterized by a standard deviation φ. The path-loss exponent γ_1 and γ_2 are 2.1 and 3.8, respectively, while the critical safe distance d_c is 100 m. Moreover, it is noteworthy to mention that the fading effect of Nakagami-m is only averaged over a close proximity of the mobile node, while slow-fading, usually represented by a widely adopted log-normal model, can be summed and integrated for any distance over the piecewise-linear slope path-loss model that is beyond a certain wavelength (Chrysikos and Kotsopoulos 2012). Thus, the results discussed in Sect. 12.4 exclude the effect of fading so as to emphasize only on the adverse effect of heavy network congestion as a result of insufficient allocation of channel bandwidth.

In the simulation, it is assumed that all the mobile nodes have the same output power, i.e., 33 dBm per 10 MHz, which is the acceptable maximum output power allowed over the control channel according to ITS-G5A specification. Similarly, the noise and clear channel assessment (CCA) threshold are -99 dBm and -93 dBm per 10 MHz, respectively, which approximately corresponds to a 1 km sensing range. Lastly, in order to ensure successful packet reception with minimum latency, SINR threshold of 6 dB is needed. On the other hand, the MAC parameter settings for CSMA/CA such as CW and AIFS are set at 3 and 58 μs, respectively, in conformity with the highest priority accorded to safety messages in vehicular network. The total

number of timeslots in the case of STDMA based MAC per frame grows in line with the improvement of the data rate, while length of the frame is presumed to be 1 second (i.e., a constant). In other words, one timeslot duration tallies with the duration taken to transmit a packet of 300bytes size. Unless otherwise stated, in all the scenarios used in this simulation experiments, the time parameters applied are chosen from the IEEE 802.11p PHY specification.

Furthermore, in order to investigate the effect of available spectral resource on the reliability of safety packet transmission, the channel bandwidth of the CCH is varied from 10 MHz up to 40 MHz. The simulated urban-highway scenarios are filled up with the generated vehicular traffic. Finally, the broadcasted message reception was recorded over 60,000 ms (i.e., 1 min) period. From the definition of Eq. (12.1), the probability of message reception failure is calculated. The rest of the parameters with their settings as used in the simulation are shown in Table 12.1.

12.3.4 Results and Discussion

12.3.4.1 Probability of Message Reception Failure

As shown below, probability of message reception failure (P_{MRF}) as performance metrics is used to evaluate the efficiency and degree of performance gain between CSMA/CA and STDMA based MACs in road traffic safety vehicular communication. Firstly, safety packet transmission reliability over CSMA/CA and STDMA based MACs were measured in comparison between different spectral resource allocation, i.e., from 10 MHz up to 40 MHz. In order to demonstrate the effect of allocated spectral resource on vehicular message broadcast reliability as well as on the overall vehicular network performance, the resultant message transmission reliability of STDMA and CSMA/CA based MACs were measured as a function of the

Table 12.1 Values of parameters used in the simulation

Parameter	Value
Data rate	3Mbps
Packet size	300bytes
Sensing range	1000 m
CWmin (CSMA/CA)	3
CWmax	(CSMA/CA)
Latency requirement	100 ms
SINR threshold	6 dB
Frame length (STDMA)	1 s
AIFS (CSMA/CA)	58 μs
Slot time	9 μs
SIFS	16 μs
Back-off time	58 μs

allocated spectral resource and the amount of traffic (i.e., vehicular traffic density) across the entire vehicular network. Additionally, the channel bandwidth is varied from the US FCC officially allocated 10 MHz to 40 MHz and effectively increase the amount of packet generated (or network traffic load) from low to high. The simulated vehicular network urban-highway road segments are filled up with generated vehicular traffic during the initialization phase.

Figure 12.6a–c overleaf demonstrate that the higher the available spectral resource, the more the QoS and overall performance of the entire vehicular network will improve. From the results contained in Fig. 12.6a–c, it is evident that the performance of both STDMA and CSMA/CA based MACs in terms of transmission reliability show remarkable improvement with less probability of data packets transmission and reception failure at the receivers as the available spectral resource increases from 10 MHz to 40 MHz. Additionally, the result goes a long way to prove

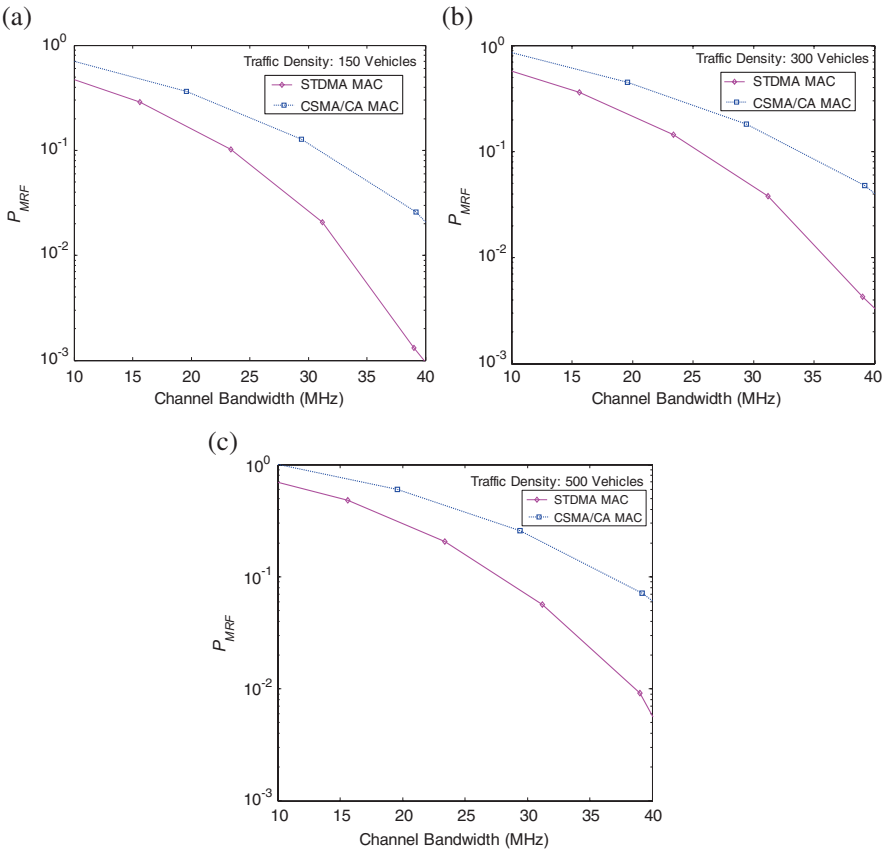


Fig. 12.6 (**a–c**): Performance comparison between the STDMA and CSMA/CA based MAC algorithms using as a function of the available channel bandwidth (measured in MHz) with increasing vehicular traffic density from 150 vehicles up to 500 vehicles

that higher spectrum (at least more than 10 MHz) is required for a high density urban or sub-urban vehicular environment with a maximum reliability demand. The performance demonstrated in the results makes it clear that over 40 MHz bandwidth is required in order to guarantee maximum (i.e., 99%) transmission reliability in certain cases. However, the overall improvement in transmission reliability is a lot higher with STDMA based MAC compared to CSMA/CA based MAC as can be witnessed in Fig. 12.6a–c. It is observed that STDMA based MAC offers a performance advantage of multiple orders of magnitude (i.e., over 10% performance gap) against CSMA/CA based MAC in terms of minimum obtainable probability of data message reception failure at the receivers as the available spectral resource increases from 10 MHz to 40 MHz. Obviously, from Fig. 12.6a–c, it is clear that the probability of data message reception failure is well beyond 20% with the allocation of 10 MHz channel bandwidth but steeply reduces as the available channel bandwidth (i.e., spectrum allocation) increases from 10 MHz up to 40 MHz.

Notwithstanding the impressive performance of both CSMA/CA and STDMA based MACs in terms of P_{MRF} by improving safety data packets transmission reliability, a more important striking different is seen between the two considered MACs. It is shown in Fig. 12.6a–c that even at the same allocation of 10 MHz channel bandwidth, STDMA out performs the CSMA/CA based MACs due to the fact that CSMA/CA MAC algorithm is strictly based on rigorous contention for shared channel access which leads to increased network overhead, whereas STDMA based MACs provides a structured shared medium access and prevents the negative impact of unhealthy contention for shared channel access even when the communication channel is fully loaded and saturated. In other words, the vehicles are synchronized by time slots. This means that each time that new vehicles enter the shared medium, they first give a listening to the activity of the shared channel for a one frame duration, and have the frame divided into several groups according to the number of messages they need to send per frame. Finally, as discussed in Sect. 12.2.1.2, each vehicle selects one NTS from each group for transmission of its own data packets and then starts to transmit continuously. Similarly, a reuse factor is assigned to each NTS to allow for adapting to the changes occurring in the shared channel, which represents a given number of the following frames where the transmission timeslot is utilized by the mobile node. Then, successively, another NTS will be carefully selected when the current counter (i.e., the pre-assigned reuse factor) is expired, out of the available NTSs within its SI. In other words, unlike CSMA/CA, STDMA based MACs always provide media access even when all the time-slots of the SI are occupied by selecting as another NTS the one utilized by the furthest vehicle as discussed in Sect. 12.2.1.2 above. Thus, this approach prevents the unhealthy shared channel congestion and increased overhead caused by heavy contention for channel utilization in the case of CSMA/CA based MAC algorithms, which in turn, leads to poor data packet transmission reliability, as is the case in Fig. 12.6a–c.

More interestingly, it can be seen from Fig. 12.6b, c that the volume of vehicular traffic density also has direct impact on the transmission reliability of safety related data packets. The reason for this may be due to the fact that increased channel load and congestion due to excessive network saturation sometimes result to deterioration

of the overall network QoS and may even lead to transmission collision. Thus, the end result becomes an overall increased probability of safety packets transmission and reception failure, which is noticeable in both Fig. 12.6b, c with increased traffic density from 300 vehicles (see Fig. 12.6b) to 500 vehicles (see Fig. 12.6c). However, in either case, STDMA based MAC algorithm always outperforms the CSMA/CA, again, due to the same reasons discussed above. Most importantly, this negative impact of increased vehicular traffic density is very conspicuous in Fig. 12.6c especially on CSMA/CA based MAC algorithm performance, where at exactly 10 MHz bandwidth allocation, the probability of safety data message reception failure is 100% (i.e., 1), meaning that no transmission is correctly received and decoded at the receivers due to poor network QoS. Similarly, it can be clearly seen that as the available channel bandwidth increased from 10 MHz up to 40 MHz, that the probability of safety data message reception failure reduced drastically and significantly in Fig. 12.6a towards 0%, which means that virtually all the transmitted safety data packets were correctly received and decoded at the intended receivers. However, the increase in vehicular traffic density from 150 vehicles (see Fig. 12.6a) to 500 vehicles (see Fig. 12.6c) categorically shows that more than 10 MHz bandwidth (i.e., at least 50 MHz channel bandwidth) is required for efficient and reliable transmission of safety related packets as opposed to the existing official 10 MHz bandwidth allocation for road traffic safety communication in VANETs. In other words, the performance depicted in Fig. 12.6a through Fig. 12.6c opposes in every sense the existing official regulatory resolution of allocating a meagre 10 MHz channel bandwidth over 5.9GHz band for exchange of safety packets by FCC in 1999. The result further suggests that a significant modification would be required in either the overall design of IVC system or the amount of spectrum allocation required to achieve efficient vehicular communication system, especially for safety traffic exchange in VANETs.

12.3.4.2 Safety Message Transmission Delay

As shown overleaf, message transmission delay performance of both STDMA and CSMA/CA based MAC algorithms were measured in comparison between different spectral resource allocations (i.e., from 10 MHz up to 40 MHz). In order to demonstrate the impact of available spectrum on the latency of vehicular communication as well as on the overall vehicular network performance, the resultant message transmission delay of both CSMA/CA and STDMA based MAC algorithms were measured as a function of the allocated spectral resource and the amount of vehicular traffic density across the simulated vehicular network scenarios. Additionally, the channel bandwidth is varied from the US FCC officially allocated 10 MHz up to 40 MHz in order to clearly obverse the impact on the two shared media access algorithms. In Fig. 12.7a–c, it can be observed that the safety related message transmission delay significantly reduces both in a low and in a high vehicular traffic density as the available spectrum (i.e., channel bandwidth) increases from 10 MHz up to 40 MHz. The results depicted in Fig. 12.7a–c also demonstrate that the wider the

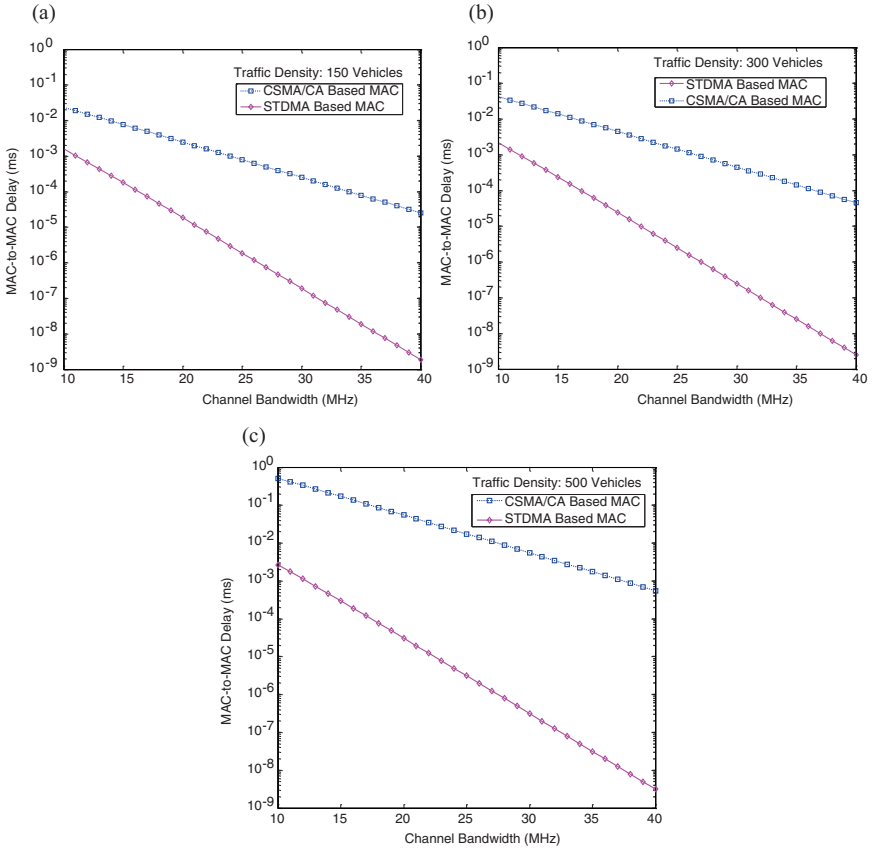


Fig. 12.7 (**a–c**): Performance comparison between STDMA and CSMA/CA based MAC algorithms using total safety message transmission delay (T_{idl}) as a function of the available channel bandwidth (measured in MHz) with increasing vehicular traffic density from 150 vehicles up to 500 vehicles

available spectral resource, the lower the overall delay (i.e., the total Safety Message Transmission Delay) performance of both the CSMA/CA and STDMA based MAC algorithms. The results also indicate that more than 40 MHz bandwidth is required to guarantee the minimum acceptable latency as well as 99% reliability in certain cases. Once more, as discussed in the case of providing reliability for safety related message transmission, the performance depicted in Fig. 12.7a–c glaringly contrasts the existing official regulatory resolution of allocating a meagre 10 MHz bandwidth for safety related message exchange in vehicular networks both in US by US FCC in 1999.

Figure 12.7b, c, it is evidently clear that the STDMA based MAC algorithm out performs the CSMA/CA based MAC algorithm in terms of safety message transmission delay when measured as a function of the available spectrum resource as well as the amount of vehicular traffic density. The results show that the STDMA

based MAC algorithm has a performance gap of multiple orders of magnitude as opposed to the CSMA/CA based MAC algorithm in terms of the minimum acceptable latency that can be tolerated in order to guarantee fast and timely transmission and reception of safety related packets in vehicular networks so as to avoid road accident occurrence. Obviously, from Fig. 12.7a–c, it is clear that the transmission delay experienced by the CSMA/CA based MAC algorithm is well above 15% compared to the STDMA based MAC algorithm even with the same allocation of 10 MHz channel bandwidth. Furthermore, the overall transmission delay resulting from using the CSMA/CA based MAC algorithm drastically increases even as the available channel bandwidth (i.e., spectrum allocation) increases from 10 MHz up to 40 MHz in contrast to the STDMA based MAC algorithm, whose delay reduces sharply to less than 1% as the available channel bandwidth increases from 10 MHz up to 40 MHz.

The poor performance of the CSMA/CA based MAC approach as against the STDMA based MAC approach in terms of transmission delay of safety packets is as a result of the fact that safety data traffic in VANETs applies high priority queues in contrast to non-safety related data traffic as provided by the EDCA mechanism, which is adopted by IEEE 802.11p. The high priority access accorded to safety related data traffic implies short sensing durations but also few back-off values from which to select from after sensing the channel to be occupied by another vehicle. Note that IEEE 802.11p MAC algorithm uses an exponential back-off scheduler. Hence, for a very low shared channel load (as is the case in Fig. 12.7a with only 150 vehicles), low shared media access delay is provided after the channel sensing duration. However, when the channel load increases (as is the case in Fig. 12.7b, c with 300 vehicles and 500 vehicles, respectively), the shared channel access delay increases exponentially. In other words, the channel access delay becomes unpredictable with the CSMA/CA based MAC approach as the traffic density increases, leading to increase in channel loads.

On the other hand, the STDMA based MAC approach uses a structured channel access mechanism to guarantee a predictable safety message transmission delay even in worst case vehicular network scenarios with high traffic density and high channel loads, which is the case in Fig. 12.7c with an increased number of participating vehicles. Thus, since the shared channel access delay of the STDMA based MAC approach is predictable even in a high traffic density as opposed to IEEE 802.11p MAC algorithm that is based on the CSMA/CA approach, the total safety message transmission delay of the STDMA based MAC approach is upper-bounded by the length of the selection interval (SI) as discussed in Sect. 12.2.1.2.

12.4 Conclusion

This Chapter investigated the required amount of radio spectral resource necessary to support timely and reliable message delivery over IoVs via VANETs. The study focused on both DSRC/WAVE and the European standard ITS-G5 that are based on

recently approved IEEE 802.11p specification, which uses a simplified version of CSMA/CA as MAC protocol, and an STDMA MAC recently proposed by ETSI. The Chapter further carried out a feasibility analysis of radio spectrum requirement for timely and reliable V2V communication. In the feasibility analysis, synchronized STDMA MAC is compared with the CSMA/CA MAC protocol, which 802.11p is based on. Probability of MRF is used as a performance metric to investigate and ascertain the minimum spectrum requirement for efficient, timely, and reliable V2V communication. Extensive simulation experiments were conducted using both CSMA/CA and STDMA based MAC algorithms over IoVs' communication in sub-urban scenarios. From the simulation results, it is evident that the performance of both STDMA and CSMA/CA based MACs in terms of transmission reliability show remarkable improvement with less probability of data packets reception failure at the receivers as the available spectral resource increases from 10 MHz to 40 MHz. Additionally, the result goes a long way to prove that higher spectrum (at least more than 10 MHz) is required for a high IoVs density in urban or sub-urban vehicular environment with a maximum reliability demand.

Furthermore, the simulation results show that even at the same allocation of 10 MHz channel bandwidth, STDMA MAC outperforms the CSMA/CA based MACs due to the fact that STDMA based MACs provide a structured shared medium access and prevent negative impact of unhealthy contention for shared channel access by the intelligent vehicles. The simulation performance demonstrated in the results makes it clear that over 40 MHz bandwidth is required in order to guarantee maximum (i.e., 99%) transmission reliability in certain cases. In other words, the results opined that up to 40 MHz channel bandwidth over 5.9GHz spectrum band would be required to guarantee optimal reliability of safety packets exchange in IoVs networks as opposed to 10 MHz allocated in US.

The use of real data collected from physical experiments other than simulation data to proof the validity of these algorithms will form an interesting future work. Further work could also focus on the possibility of reducing the spectrum requirements with respect to aggregation of information, especially in the case of emergency events where many intelligent vehicles will be triggered to broadcast redundant information (i.e., event-driven DENMs).

Acknowledgement We sincerely thank the anonymous reviewers for their helpful comments/suggestions on earlier draft of the manuscript.

References

Alam, M., & Sadaf, K. (2015a). *Relevance feedback versus web search document clustering*. IEEE 2nd International Conference on Computing for Sustainable Global Development (INDIACom), pp. 1665–1669.

Alam, M., & Sadaf, K. (2015b). Labeling of web search result clusters using heuristic search and frequent Itemset, Elsevier. *Procedia Computer Science, 46*, 216–222.

Alam, M., Sethi, S., & Shakil, K. A. (2015). Distributed machine learning based biocloud prototype. *International Journal of Applied Engineering Research, 10*, 37578–37583.

Cheng, L., Henty, B., Stancil, D., Bai, F., & Mudalige, P. (2007). Mobile vehicle-to-vehicle narrow-band channel measurement and characterization of the 5.9 GHz dedicated short-range communication (DSRC) frequency band. *IEEE Journal on Selected Areas in Communications, 25*, 1501–1516.

Chrysikos, T., & Kotsopoulos, S. (2012). *Characterization of large-scale fading for the 2.4 GHz channel in obstacle-dense indoor propagation topologies*. IEEE Vehicular Technology Conference (VTC Fall), Quebec City, QC, pp. 1–5.

Department for Transport (DfT). (2012). *Reported Road Casualties in Great Britain*: 2011 Annual Report, RAS10013. Available online: http://www.racfoundation.org/assets/rac_foundation/content/downloadables/factsheet-road_safety_data-jan13.pdf

Eichler, S. (2007). Performance evaluation of the IEEE 802.11p WAVE communication standard, in the proceedings of IEEE 66th vehicular technology conference, VTC-2007 Fall, pp. 2199–2203.

ETSI TR 102 638 V1.1.1. (2009). Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions.

ETSI TS 102 637-2 V1.2.1 (2011) Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service.

ETSI TS 102 637-3 V1.1.1 (2010) Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service.

Eze, E., Zhang, S., & Liu, E. (2014). *Vehicular ad hoc networks (VANETs): Current state, challenges, potentials and way forward*. Automation and Computing (ICAC), 2014 20th International Conference on, Cranfield, pp. 176–181.

Eze EC, Zhang S and Liu E (2015) *Improving reliability of message broadcast over Internet of Vehicles (IoVs)*, IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), Liverpool, pp. 2321–2328.

Eze, E. C., Zhang, S., Liu, E., & Eze, J. C. (2016a). Advances in vehicular ad-hoc networks (VANETs): Challenges and road-map for future development. *International Journal of Automation and Computing, Springer, 13*, 1–18.

Eze, E., Zhang, S., Liu, E., Nweso, E. N., & Eze, J. C. (2016b). Timely and reliable packets delivery over internet of vehicles for road accidents prevention: A cross-layer approach. *IET Networks, 5*, 127–135.

FTC Staff Report (2015) *The Internet of Things: Privacy and security in a connected world*. Available online at: https://www.ftc.gov/system/files/documents/reports/federaltrade-commission-staff-report-november-2013-workshopentitled-internet-things-privacy/150127iotrpt.pdf

ITU-R M.1371-4. (2010). Technical characteristics for an automatic identification system using time-division multiple access in the VHF maritime mobile band.

Kloiber, B., Strang, T., Rockl, M., & de Ponte-Muller, F. (2011). Performance of CAM based safety applications using ITS-G5A MAC in high dense scenarios. *IEEE Intelligent Vehicles Symposium (IV)*, 654–660.

Kosch, T., Adler, C. J., Eichler, S., Schroth, C., & Strassberger, M. (2006). The scalability problem of vehicular ad hoc networks and how to solve it. *IEEE Transaction on Wireless Communications, 13*, 22–28.

Ma, X., & Mathew, M. (2015). *Enhancement and analysis of VANET one-hop event-driven emergency services*, 2015 IEEE 82nd Vehicular Technology Conference (VTC fall), Boston, MA, pp. 1–6.

Mathworks [Online]. Available at: http://uk.mathworks.com/products/matlab/

Nakagami, M. (1960). *The M-Distribution, A Heneral Gormula of intensity distribution of the rapid fading*. Oxford: Pergamon.

Nils, A., Raphael, E., Elmar, G., & Matthias, S. (2010). *Bonn-motion: A mobility scenario generation and analysis tool*. In: Proceedings of the 3rd international ICST conference on simulation tools and techniques, pp. 51–60.

Sethi, S., Shakil, K. A., & Alam, M. (2015). *Seeking black lining in cloud*. IEEE 2nd International Conference on Computing for Sustainable Global Development (INDIACom), pp. 1251–1256.

Shakil, K. A., Alam, M., & Sethi, S. (2015). Exploring non-homogeneity and dynamicity of high scale cloud through hive and pig. *Indian Journal of Science and Technology, 8*, 1–8.

Sjöberg, K., Uhlemann, E., & Ström, E. G. (2011). *Delay and interference comparison of CSMA and self-organizing TDMA when used in VANETs*. In: Proceedings of 7th International Wireless Communications and Mobile Computing Conference, (Istanbul, Turkey), pp. 1488–1493.

Soriga, S. (2012). ITS-G5 and Mobile WIMAX performance in vehicle-to-infrastructure. *Communications, 74*, 143–156.

Strom, E. (2011). *Physical layer for VANETS: State of the art and future challenges*. IEEE VTS Workshop on Wireless Vehicular Communications, [Online] http://www.hh.se/download/18.43aaafb313382d5f99d80001389/1321113158509/

Taliwal, V., Jiang, D., Mangold, H., Chen, C., & Sengupta, R. (2004). Empirical determination of channel characteristics for DSRC vehicle-to-vehicle communication, in proceedings of the 1st ACM international workshop on vehicular. *Ad Hoc Networks*, 88–88.

Torrent-Moreno, M., Mittag, J., Santi, P., & Hartenstein, H. (2009). Vehicle-to-vehicle communication: Fair transmit power control for safety-critical information. *IEEE Transactions on Vehicular Technology, 58*, 3684–3703.

Chapter 13
Single Activity Recognition System: A Review

P. K. Nizar Banu and R. Kavitha

Abstract Human Activity Recognition (HAR) plays an important role in smart home assisted living system which is one among the growing research area in smart computing. In this modern era, Smart home assisted living is highly recommended for elderly people to monitor and assist in taking care of themselves. HAR is applied in various ambiences to recognize single activity and group activity as well. This chapter focuses on single activity recognition system with respect to variety of sensors used in smart homes, activity recognition methods and wide range of communication systems that helps to ease the living style of elderly people in healthy environment which can be linked to the advancement of IoT technology in smart building. This chapter reviews many applications with variety of sensors, real time smart home projects, and smart home assisted living systems including activity recognition methods and communication systems.

Keywords Smart home · Sensors · Activity recognition · Communication systems

13.1 Introduction

As the technology grows very fast every day, there is no doubt that it has carved its innovation in making the living home intelligent. Thus a smart home is a home which equips smart devices and sensors to sense the environment. Elders or specially-abled persons require no additional support like care takers or health care applications if they live in a smart home, as they will be assisted by the modern technology. Considering the importance of emotional and physical health of elders living independently, this chapter focuses on activity recognition of elders living alone in a smart home. Once the wave or any form of motion is sensed, it is forwarded to the server via network for monitoring the appropriate tasks that are relevant to the application. Smart home system for regular monitoring of elders living alone is developed by Dimitrios et al., in 2010 (Lymberopoulos et al. 2011) is shown in Fig. 13.1.

P. K. Nizar Banu (✉) · R. Kavitha
Department of Computer Science, CHRIST (Deemed to be University), Bangalore, India
e-mail: kavitha.r@christuniversity.in

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_13

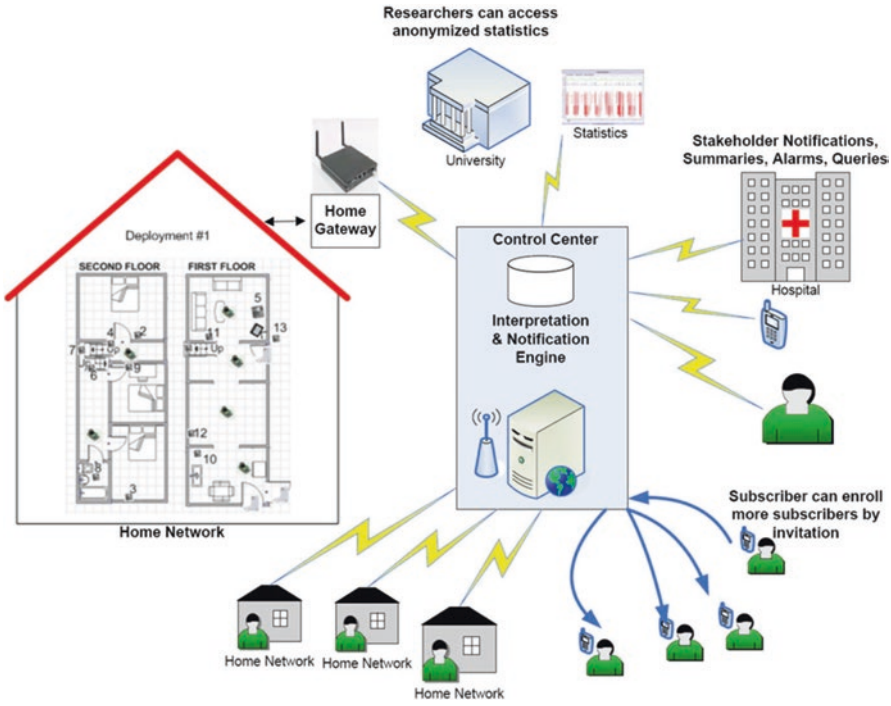


Fig. 13.1 Smart home system for regular monitoring

According to the sensing technology, sensors are classified as vision sensors, wearable sensors and ambient sensors. Video based sensing technology is the first sensing technology which was in use. This technology demands the users to fix video cameras in all the rooms where the motion to be detected. Either a number of cameras can be deployed with limited distance or a single camera can be used to cover a wide area. This extracts high computation power and occupies huge storage space to handle video type data. Technology used to sense and guide the wearable device is called wearable sensing technology. This draws less attention from the elders, patients and specially-abled as they have to carry or attach some form of device with them always. Ambient sensing technology is another form of technology that collects the data from the ambient sensors which are fixed in the resident. This sensor observes the motion of the user when some action is performed within the specific range.

A variety of sensors are in use for making a home smart with the arrival of smart home technology. The residents' regular activity is monitored by the ambient sensors such as motion sensor, temperature sensor, light sensor and magnetic sensor which are deployed in the home area. The purpose of the sensor, type of the data captured, speed of the data, and the parameter depends on the type of sensor we use. A list of vision sensors, ambient sensors and Wearable sensors are studied and their scopes with other details are given in Table 13.1.

Table 13.1 Sensors for smart home

S. No	Sensor Category	Name of the Sensor	Sensing Scope	Type of data	Data rate	Drawbacks
1	Vision sensors	Thermal video	Activity	Thermal images	Very low	Sensitive for lights, thermal factor
		Visible video		Images, video	High	Very expensive
						Needs high processing power
						Privacy issues
2	Ambient sensor	RFID	Object information	Categorical	High	Requires multiple sensors
		Magnetic switches	Door OPEN / CLOSE	Numeric	Medium	Sensor malfunction may give improper results
		Home electric appliances	Usage of appliances		Low	
		Smoke/heat sensor	Detect smoke or fire			
		Water flow sensor	Flow in tap/ shower	Numeric	High	
		Power/current sensor	Electricity usage			
		Temperature	Ambient temperature			
3	Wearable Sensors	EOG (Electrooculography)	Eye movement	Numeric	Very high	Not easily accepted
		Accelerometer	Acceleration Axis		High	Requires multiple sensors
		Gyroscope	Acceleration angle	Numeric	Very low	Not easy to wear
		Glucometer	Blood glucose			
		ECG (electrocardiography)	Heart activity			
		EEG (electroencephalography)	Brain activity			
		Thermal	Body temperature		Very low	

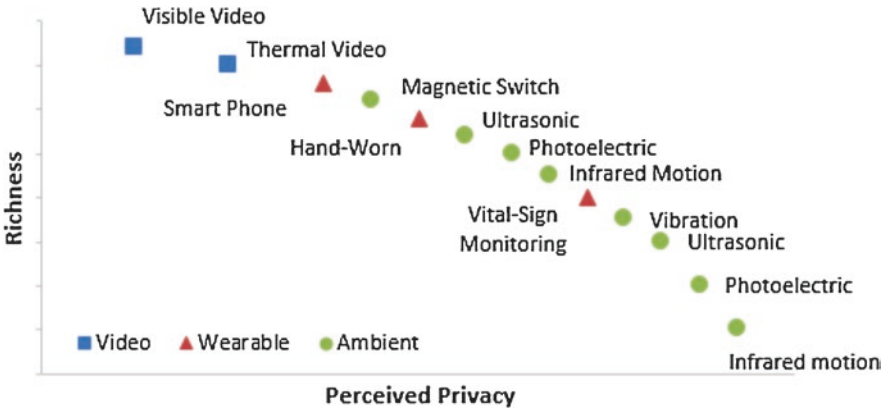


Fig. 13.2 Richness of sensor vs user's perception

The Fig. 13.2 shows the richness of the different smart home sensors and perceived privacy of a person using smart home sensors Privacy (Debes et al. 2016).

Deploying infrared motion sensor may not have any privacy issue as it does not give rich information about a resident.

Smart home projects were setup and monitored by various educational institutions. These projects were set in a laboratory, home and office. These environments are made smart by deploying sensors and the residents were asked to stay for some duration. Table 13.2 lists the details of smart projects set by institutions, the environment preferred, sensors deployed and the data genera**ted.**

All these projects were implemented in a real time environment and the sensing technologies like visual, wearable and ambient were adopted. Centre for Advanced Studies in Adaptive Systems (CASAS) is a smart home project at Washington State University in the United States of America which treats environment as an intelligent agent (Kavitha and Binu 2018). CASAS projects focuses on helping elders to live in comfort, safety and supportive health using different sensors. The CASAS has also designed a smart home kit called "Smart Home in a Box-SHiB" which is portable, easy to install, clear infrastructure plan and ready to use (Cook et al. 2013), which can be deployed in any sort of environment that needs to monitor the inhabitants.

A Situ-centric learning automation recommendation system to guide an inhabitants of a smart home is presented (Oyeleke et al. 2018). A non parametric AR system to monitor the activity of daily living for users in smart home environments is proposed (Wu 2019). The activities recognized can also be utilized for analysing users' behaviour patterns (Wu 2019). Group activity recognition in a smart building is reviewed (Fauzi et al. 2018). Integration of big data with IoT is suggested to support real life systems such as intelligent building system, security and monitoring (Fauzi et al. 2018). Recurrent Neural Network architecture (Machot et al. 2018) is proposed to predict future activities of a resident in a smart home, which addresses the problems faced by old people who suffer from Dementia or Alzheimer.

Table 13.2 Smart home projects

S. No	University/Institution	Settings	Sensor Type	Reference
1	University Politehnica of Bucharest	Laboratory	Vision sensor	AmI-Lab (Mocanu et al. 2017)
2	Centre for Usability Research & Engineering	Laboratory		HERMS (http://www.fp7-hermes.eu/)
3	CSTB	Home/ Laboratory		GER'HOME (http://www-sop.inria.fr/members/Francois.Bremond/topicsText/gerhomeProject.html)
4	Chiang Mai University, Thailand	Home	Wearable sensor	Fauzi et al. (2018)
5	Dalian University of Technology	Laboratory		Guo and Wang (2018)
6	Washington State University	Home/ Laboratory	Ambient sensors	CASAS (Cook et al. 2013; Mocanu et al. 2017)
7	University of Virginia	Home/ Laboratory		CAR (Virone et al. 2008)
8	University of Amsterdam	Home		Van Kasteren et al. (2008)
9	University of Missouri	Home		Tapia et al. (2004a)
10	University of Zagreb	Laboratory		Skocir et al. (2016)
11	Univ. Grenoble Alpes	Home		Jung (2017)
12	Institute of Information Science and Technologies, Italy	Office		Barsocchi et al. (2018)
13	University of Amsterdam	Home		Krose et al. (2008)
14	Grenoble TIMC-IMAG	Laboratory	Hybrid sensors	Fleury et al. (2010)

Multi-sensor data is collected with various activities such as watching TV, preparing lunch, grooming etc., with help of sensor activations (Park et al. 2018). A residual recurrent neural network with attention module which has high accuracy is proposed and proved that Residual-RNN outperforms other state-of-the-art competitors (Park et al. 2018).

Almost all the activity recognition methods uses one among the classification models such as supervised, unsupervised or semi-supervised. One of the important drawback of supervised classification is it learns from the previous activities or training set. But the classification model which has learnt one environment cannot be used in other environment as the activities of resident differs. This problem is addressed (Wang and Miao 2008) and a method for smart home activity recognition with binary sensors is proposed. It uses the characteristics of binary sensors, its activities and time information. It is claimed that this information is sufficient for a

classification model to be implemented in a new smart environment too. Comparison of a set of variables used in literature with time-domain variables with biomechanical meaning is explored (Rosati et al. 2018).

13.2 Smart Home Assisted Living System

Smart home assisted living system monitors the residents' movement continuously. It analyses the residents' behaviour and assists them in smart home living environment. The advancement of smart home assisted living system has led to the development of multiple applications that supports elders to live independently. Smart home assisted living system developed by (Kolovou and Lymberopoulos 2011) has the following features.

Provides health-care services
Improved security
Extends the lifespan of elders in their ideal environment
Enhanced life style for elders
Useful for caretakers and family members too
Avoids social isolation

Several applications are available to support elders and specially-abled persons. This chapter explores five different categories of assisted living system such as systems for energy saving, health care, safety and security anomalous situation detection and daily activity monitoring.

13.3 Assisted Living System for Energy Saving

A smart home (Hsu et al. 2017) was developed with multi sensor data fusion technology for energy management. A motion sensing device is mounted on residents shoe to enable the residents' location. A navigation system and positioning algorithm were used to understand the movement of the resident which also controls light at home to save energy. A smart home energy management system was developed to work in a real environment based on the IEEE802.15.4 standard and Zigbee sensor network. This system's sensor network integrates heterogeneous sensing devices and actuator which controls the smart device. Hu and Li in 2013 (Hu and Li 2013) designed architecture for energy management in smart home. This is combined with sensing technology, network and machine learning algorithms.

Smart office (Barsocchi et al. 2018) is a combination of motion, acoustic and power meter which was set at National Research Council of Italy, in Piza using ZigBee network. The data generated marks the occupancy as "Presence" and "No

Presence". This also analyses the topological data to control power meter for energy saving.

13.4 Assisted Living System for Health Care

Smart home assisted living system satisfies elders need. Instead of visiting clinics or hospitals frequently, this system authorizes the elders to stay in their convenient homes, providing the regular updates to the health professionals and care takers. This section briefs the research carried out for health care in terms of smart homes.

A client-server remote health monitoring system (Lee and Gatton 2010) was proposed to transfer health related data collected from smart home. Smart home remote technologies for health care services are reviewed along with advances in smart home health care and research directions (Majumder et al. 2017). This research also covered study on E-health services, E-prescription, M-Health services, emergency call, reminders and health assessment report.

A context aware system, which is based on ontology using IOT infrastructures, was developed (Alirezaie et al. 2017). Residents medical data like pulse rate and temperature are measured using shimmer sensors. Most of the health care applications provide health care solutions from the data collected using Body Area Network (BAN). Periodic patterns were identified from BAN data (Ismail and Hassan 2017). A Productive Periodic-Frequent Pattern (PPFP) growth algorithm is implemented for better decision making. Knee joint movement were keenly monitored and analysed using inertial sensors (Bertomeu-Motos et al. 2017). The analysis was helpful in creating an upper limb exoskeleton.

With the support of elders residing in old age home, regular habits and physiological status of elderly people were collected using a multi agent data analysis system m-health (Mendes et al. 2017). Data was collected using Fitbit wristbands (Diaz et al. 2015) and analysed using clustering algorithms.

13.5 Assisted Living System for Safety and Security

As there is high increase in number of elders staying alone, safety and security is also vital in building smart home systems.

An activity recognition system proposed by Tapia et al. (2004a, b), consists of environmental state change sensors (ESM), ESM which marks activity and pattern recognition algorithms to recognize patterns and classification algorithms to classify the patterns. This setup was implemented in a multi resident environment and it was found useful to detect the basic activities leading to understand the behaviour of the resident.

A smart home based on sensor network was well designed and verified to provide safety and security (Ransing and Rajput 2015) to elders. Temperature sensor, contact sensor and LPG sensors are used to detect leakage of gas and detect the status of the doors as open or closed. A smart home pilot system (Krose et al. 2008) was designed to recognize daily activity in a smart home using simple switch sensor with a combination of low power and low cost. This system was deployed in an apartment occupied by an old person and the activities are annotated. It was found that the activities should be considered for better annotation. An Intelligent model "Smart Monitor" (Frejlichowski et al. 2014) is introduced to identify the fall detection in smart home environment.

A Hybrid Inspection Facility (Jung 2017), is projected to monitor the safety and security of elders who lives in smart home. Wearable-motion sensor and environmental sensors are used to watch the movement and provide security. The health of the elders is recorded as positive or negative based on the duration of stay at each room.

13.6 Assisted Living System for Anomalous Situation Detection

An intelligent system to detect the abnormal usage of home appliances using usage logs was proposed (Nguyen and Minh-Thai 2015). This system identifies the correlation pattern to detect anomalies. A framework to understand the daily behaviour of the resident in a smart home is observed using sensor network data (Aran et al. 2016). Probabilistic spatio-temporal model is used to identify the anomalies. This method handles abnormal data from the sensor, difference in daily habitual work or unexpected and persistent change that happens with the behaviour of the elders.

13.7 Assisted Living System for Monitoring Daily Activities

As every human's behaviour is unique, recognizing activity of any human in a smart home is a challenging task. Regular activity recognition system solves many real time problems including health monitoring and assisted living. Survey on human activity recognition using wearable sensors is proposed by Lara et al., (Lara and Labrador 2013).

Clustering and classification techniques are applied for the activities recognized using passive Infrared sensors (Nef et al. 2015). A comparative study of daily living in smart home is presented (Chahuara et al. 2016). iCarer, a virtual carer project (Lotfi et al. 2017) was developed to assist informal carer. A variety of heterogeneous sensors are used to monitor the human activity and the data is recorded via cloud for

analysis. An integrated system (Demir et al. 2017) for dementia people was developed and deployed to collect and communicate the sensed data.

By 2050, the number of elderly people living independently will be more than 50% of current situation. During such situation smart home assisted living system will provide elders and specially-abled persons a friendly ambience to enjoy their life without dependency.

13.8 Activity Recognition in Smart Home Assisted Living

Automatic recognition of a physical activity happening in a smart home is called Activity Recognition (Kavitha and Binu 2018). Recognizing activity is very interesting and highly challenging task in the areas like human computer interaction, smart home assisted living system and ubiquitous computing. Activities of a single person or a group of people are identified with the help of sensor data and the information about the residents is presented. Activity recognition in a smart home assisted living system collects data from various sensors deployed in an environment and decides the reason behind every activity. This system has a few important steps such as Sensing, Pre-processing, segmentation, feature extraction, feature selection, activity learning (Zolfaghari and Keyvanpour 2016).

Context awareness, activity recognition and movement recognition are the different terms used for activity recognition (Elhoushi et al. 2017). Context awareness is one of the important research area in ubiquitous computing. It identifies the environment around a device or an object. This helps to identify whether the person is at home or at office etc.

Everyday activities like eating, cooking, sleeping, hygiene, swinging, phone call etc., are identified and called as activity recognition which helps in developing smart homes to monitor elders and patients. Identifying the movements such as walking, running, sitting, climbing up and down jumping helps in recognizing navigation.

Activity recognition approach is classified as knowledge driven approach and data driven approach (Liu et al. 2017). Data driven approach is classified as supervised, semi-supervised and unsupervised methods. Knowledge driven approach focuses on how knowledge is captured, illustrated and used (Chen et al. 2012).

Supervised method needs labels to classify. These labels are done using annotation which is more expensive and takes more time. But it gives good accuracy. To overcome this issue, unsupervised methods were introduced. This need no annotation but resulted in poor accuracy. To avoid the issues in both supervised and unsupervised, a hybrid method called semi-supervised was designed. Machine learning algorithms use the labelled data from supervised method and train the unlabelled data in the unsupervised frame to recognize the activity. Features extracted and used based on the domains such as time, frequency and Environment in smart home is listed in Table 13.3.

Table 13.3 Features in Smarthome

S. No	Domain	Features	Reference
	Time	Mean, Mode, Median, SD, Variance, IQR, Corelation, Kurtosis Zero-Crossings, Root mean square	Machot and Mayr (2016), Tapia et al. (2004a), Zdravevska et al. (2017)
	Frequency	Discrete Fourier Transform, Discrete cosine Transform	Chernbumroong et al. (2013), Zdravevska et al. (2017)
	Environment	Location_ID, Time_of_Day, Day of Week, Activity_ID, Main_Sensor ID, Activity Length, Num Sensor, Num M Sensor, Num T Sensor, Num D, Sensor, Num Event, Previous Activity, Next Activity	Fleury et al. (2010), Krose et al. (2008)
	Others	PCA, LDA	

Classification techniques (Theodoridis and Koutroumbas 2009) and machine learning techniques (Witten and Frank 2005) were used to classify the activity extracted from the data stream. Table 13.4 summarizes the work carried out so far for recognizing activity.

13.9 Communication System in Smart Home Assisted Living

The advancement of network technologies has led a way for making communication fast and easy for making the environment smart, be it an office or home. These made the researchers use handy, less powered and low cost sensors for smart applications. Every sensor is connected to the network for uninterrupted communication. Despite of strong connections, it requires lot of energy to capture the sensor data and communicate the same over the network. Due to the dynamic environment, poor battery, insufficient addressing format, transmission range, Routing has become a challenging task in sensor network. This issue is addressed in (Kavitha and Binu 2018) and the life time of network is increased. Wireless technologies used for smart home in shown in Table 13.5.

13.10 Conclusion

This chapter presented a review of variety of sensors for implementing a smart home. Human activity recognition methods will have more benefits when combined with IoT technology, as the sensors that are integrated with the Internet will enable HAR systems to become more flexible. Single activity or multi activity recognition

Table 13.4 Summary of activity recognition

S. No	Sensor	Segmentation Method	Machine Learning Algorithm	Evaluation Metric	Accuracy	Reference
1.	Motion	Activity Segmentation	SVM, RF, HMM, FKL	Accuracy	>70%	Debes et al. (2016)
2.	Motion	Dynamic Window	NB	Accuracy, F-score	5–100	Shahi et al. (2017)
3.	Motion	Dynamic, overlap, sliding	Computational Topology	Accuracy	>88	Barsocchi et al. (2018)
4.	Temperature or humidity	FNSW	HMM, CRF	Accuracy	>61	Van Kasteren et al. (2008)
5.	Bi-axial accelerometer	FOSW	SVM	Accuracy	>96	Achumba et al. (2012)
6.	State Sensor, RFID	Dynamic Window	PART, C4.5	Precision, Recall	>80	Laguna et al. (2011)
7.	State change	Static Widow	NB	Accuracy	25–85	Tapia et al. (2004a)
8.	Wearable	Dynamic Sliding Window	Knn,NB, SVM,LR,RF	Accuracy	>85	Zdravevska et al. (2017)
9.	Wrist worn	Static Widow	ANN, SVM	Accuracy, Precision, Recall	>90	Chernbumroong et al. (2013)
10.	Switch	Static Widow	HMM	Precision, recall	>71	Krose et al. (2008)
11.	Heterogeneous	Static Widow	SVM	Accuracy	>75	Fleury et al. (2010)
12.	PIR, Temp, Light	Clustering	NB, SVM, RF	Precision, Recall, Accuracy	>96	Nef et al. (2015)
13.	PIR	Activity Segmentation	SVM,RF	Accuracy	>80	Zdravevski et al. (2017)
14.	PIR	Sliding Window	ANN	Precision, Recall	>76	Skocir et al. (2016)

methods, wireless network technologies for smart home, wide range of communication systems with necessary details, classifiers used for recognizing activity, segmentation methods are also summarized. Still, Human activity recognition system or single activity recognition systems requires huge number of sensors. This is becoming a challenge to support real-life systems such as security and intelligent building systems. Focussing on these extents, yet there is a scope to improve in all these aspects for making a smart home more convenient for old aged and specially-abled people.

Table 13.5 Wireless technologies for smart home

S. No	Wireless Technology	Frequency	Range	Data Rate	Power (mW)	Maximum Nodes	Network topology	Security
1.	RFID	13.56 MHz 860–960 MHz	0–3 m	640 kbps	200	1 at a time	Peer-to-peer (P2P) passive	N/A
2.	Bluetooth	2.4–2.5 GHz	1–100 m	1–3 Mbps	2.5–100	1 M + 7 S	P2P, star	56–128 bit key
3.	ZigBee	2.4–2.5 GHz	10–100 m	250 kbps	50	65,533	P2P, star, tree and mesh	128-bit AES
4.	WiFi	2.4–2.5 GHz	150–200 m	54 Mbps	1000	255	P2P, star	WEP,WPA, WPA2
5.	Insteon	RF: 869.85, 915, 921 MHz powerline: 131.65 KHz	40–50 m	38 kbps (RF) 2–13 kbps (powerline)	–	64,000 nodes per network	P2P, star, tree and mesh	256-bit AES
6.	Wireless HART	2.4 GHz	50-100 m	250 kbps	2.23		P2P, star, tree and mesh	128-bit AES
7.	ANT	2.4–2.5GHz	30 m	20–60 kbps	0.01–1	65,533 in one channel	P2P, star, tree and mesh	64-bit key
8.	Z-Wave	860-960MHZ	100 m	9.6-100 kbps	100	232	Mesh	128-bit AES

References

Achumba, I. E., Bersch, S., Khusainov, R., Azzi, D., & Kamalu, U. (2012). On time series sensor data segmentation for fall and activity classification. In: *Proceedings of the 14th IEEE International Conference on e-Health Networking, Applications and Services (Healthcom)*, Beijing, China, 2012.

Alirezaie, M., Renoux, J., Köckemann, U., Kristoffersson, A., Karlsson, L., Blomqvist, E., Tsiftes, N., Voigt, T., & Loutfi, A. (2017). An ontology-based context-aware system for smart homes: E-care@home. *Sensors*.

Aran, O., Sanchez-Cortes, D., Do, M.-T., & Gatica-Perez, D. (2016). Anomaly detection in elderly daily behavior in ambient sensing environments. In *Proceedings of the 7th International workshop on human behavior understanding, ACM Multimedia*.

Barsocchi, P., Cassará, P., Giorgi, D., Moroni, D., & Pascali, M. A. (2018). *Computational topology to monitor human occupancy*. International Workshop on Computational Intelligence for Multimedia Understanding (IWCIM), Kos Island, Greece.

Bertomeu-Motos, A., Delegido, I., Ezquerro, S., Lledó, L. D., Catalan, J. M., & Garcia-Aracil, N. (2017). *Upper-limb motion analysis in daily activities using wireless inertial sensors*. Converging clinical and engineering research on neurorehabilitation II, Biosystems & Biorobotics 15.

Chahuara, P., Fleury, A., Portet, F., & Vacher, M. (2016). On-line human activity recognition from audio and home automation sensors: Comparison of sequential and non-sequential models in realistic smart homes. *Journal of Ambient Intelligence and Smart Environments*.

Chen, L., Hoey, J., Nugent, C. D., & Cook, D. J. Y. Z. (2012). Sensor-based activity recognition. *IEEE Transactions on Systems, Man, and Cybernetics, Part C, 42*(6), 790–808.

Chernbumroong, S., Cang, S., Atkins, A., & Yu, H. (2013). Elderly activities recognition and classification for applications in assisted living. Science direct-expert systems with applications., *40*, 1662–1674.

Cook, D. J., Crandall, A. S., Thomas, B. S., & Krishnan, N. C. (2013). CASAS: A smart home in a box. *Computer, 46*, 62–69.

Debes, C., Merentitis, A., Sukhanov, S., Niessen, M., Frangiadakis, N., & Bauer, A. (2016). Monitoring activities of daily living in smart homes: Understanding human behavior. *IEEE Signal Processing Magazine, 33*(2), 81–94.

Demir, E., Köseoğlu, E., Sokullu, R., Şeker, B. (2017). *Smart home assistant for ambient assisted living of elderly people with Dementia*. International workshop on IoT, M2M and Healthcare.

Diaz, K. M., Krupka, D. J., & Chang, M. J. (2015). Fitbit: An accurate and reliable device for wireless physical activity tracking. *International Journal of Cardiology, 185*, 138.

Elhoushi, M., Georgy, J., Noureldin, A., & Korenberg, M. J. (2017). A survey on approaches of motion mode recognition using sensors. *IEEE Transactions on Intelligent Transportation Systems, 18*(7), 1662–1686.

Fauzi, C., Sulistyo, S., & Widyawan. (2018). A survey of group activity recognition in smart building. In *2018 International Conference on Signals and Systems (ICSigSys), Bali*.

Fleury, A., Vacher, M., & Noury, N. (2010). SVM-based multimodal classification of activities of daily living in health smart homes: Sensors, algorithms, and first experimental results. *IEEE Transactions on Information Technology in Biomedicine, 14*, 274.

Frejlichowski, D., Katarzyna, G.'s., Forczmanski, P., & Hofman, R. (2014). SmartMonitor- an intelligent security system for the protection of individuals and small properties with the possibility of home automation. *Sensors, 14*, 9922.

Guo, M., & Wang, Z. (2018). Segmentation and recognition of human motion sequences using wearable inertial sensors. *Multimedia Tools and Applications, 77*, 21201–21220.

Hsu, Y.-L., Chou, P.-H., Chang, H.-C., Lin, S.-L., Yang, S.-C., Su, H.-Y., Chang, C.-C., Cheng, Y.-S., & Kuo, Y.-C. (2017). Design and implementation of a smart home system using multisensor data fusion technology. *Senors, 17*, 1631.

Get Your Own Smart Home, CASAS http://smarthome.ailab.eecs.wsu.edu

CURE, Center for Usability Research & Engineering, Austria, Available Online: http://www.fp7-hermes.eu/

GERHOME http://www.virtualworldlets.net/Resources/Hosted/Resource.php?Name=Gerhome

GER'HOME project. Francois Bremond, http://www-sop.inria.fr/members/Francois.Bremond/topicsText/gerhomeProject.html

Hu, Q., & Li, F. (2013). Hardware design of smart home energy management system with dynamic price response. *IEEE Transactions on Smart Grid, 4*, 1878–1887.

Ismail, W. N., & Hassan, M. M. (2017). Mining productive-associated periodic-frequent patterns in body sensor data for smart home care. *Sensors*.

Jung, Y. (2017). Hybrid-aware model for senior wellness service in smart home. *Sensors (Basel), 17*(5), 1182.

Kavitha, R., & Binu, S. (2018). *Activity recognition using machine learning techniques for smart home assisted living*. Dissertation, Christ University.

Kolovou, L. T, & Lymberopoulos, D. (2011). *The concept of interoperability for AAL systems*. Wireless Technologies for Ambient Assisted Living and Healthcare-Systems and Applications, Medical Information Science Reference.

Krose B, Van Kasteren T, Gibson C, & Van den Dool. (2008). CARE: Context awareness in residences for elderly. In: *Proceeding of the 6th International Conference of the International Society for Geron Technology, Paisa*.

Laguna, J. O., Olaya, A. G., & Borrajo, D. (2011). *A dynamic sliding window approach for activity recognition. User modeling adaption and personalization* (Vol. 6787, p. 219). Berlin/Heidelberg: Springer.

Lara, O. D., & Labrador, M. A. (2013). A survey on human activity recognition using wearable sensors. *IEEE Communications Surveys & Tutorials*, (15), 1192.

Lee, M., & Gatton, T. M. (2010). Wireless health data exchange for home healthcare monitoring system. *Sensors, 10*, 3243.

Liu, Y., Ouyang, D., Liu, Y., & Chen, R. (2017). A novel approach based on time cluster for activity recognition of daily living in smart homes symmetry. *A MDPI Journal*.

Lotfi, A., Langensiepen, C., Moreno, P. A., G'omez, E. J., & Chernbumroong, S. (2017). *An ambient assisted living technology platform for informal carers of the elderly* (LNICST 181). Springer.

Lymberopoulos, D., Bamis, A., & Savvides, A. (2011). Extracting spatiotemporal human activity patterns in assisted living using a home sensor network. *Universal Access in the Information Society, 10*, 125.

Machot, F. A., & Mayr, H. C. (2016). Improving human activity recognition by smart windowing and spatio-temporal feature analysis. In: *PETRA'16 proceedings of the 9th ACM international conference on PErvasive technologies related to assistive environment*.

Machot, F. A., Ranasinghe, S., Plattner, J., & Jnoub, N. (2018). Human activity recognition based on real life scenarios. In *2018 IEEE international conference on pervasive computing and communications workshops (PerCom Workshops), Athens* (pp. 3–8).

Majumder, S., Aghayi, E., Noferesti, M., Memarzadeh-Tehran, H., Mondal, T., Pang, Z., & Deen, M. J. (2017). Smart homes for elderly healthcare—Recent advances and research challenges. *Sensors*.

Mendes, S., Queiroz, J., & Leitão, P. (2017). Data driven multi-agent m-health system to characterize the daily activities of elderly people. In *2017 12th Iberian Conference on Information Systems and Technologies (CISTI), Lisbon*.

Mocanu, I., Cramariuc, B., Balan, O., & Moldoveanu, A. (2017). *A framework for activity recognition through deep learning*. In: ICIAP 2017, Part II, LNCS 10485.

Nef, T., Urwyler, P., Büchler, M., Tarnanas, I., Stucki, R., Cazzoli, D., Müri, R., & Mosimann, U. (2015). Evaluation of three state-of-the-art classifiers for recognition of activities of daily living from smart home ambient data. *Sensors*.

Nguyen, T., & Minh-Thai, N. T.-N. (2015). *An approach for developing intelligent systems in smart home environment*. Cham: Springer.

Oyeleke, R. O., Yu, C.-Y., & Chang, C. (2018). *Situ-centric reinforcement learning for recommendation of tasks in activities of daily living in smart homes* (pp. 317–322). https://doi.org/10.1109/COMPSAC.2018.10250.

Park, J., Jang, K., & Yang, S. (2018). Deep neural networks for activity recognition with multi-sensor data in a smart home. In: *2018 IEEE 4th world forum on Internet of Things (WF-IoT), Singapore* (pp. 155–160).

Ransing, R. S., & Rajput, M. (2015). *International conference on Nascent technologies in the engineering field*. IEEE.

Rosati, S., Balestra, G., & Knaflitz, M. (2018). Comparison of different sets of features for human activity recognition by wearable sensors. *Sensors, 18*, 4189.

Shahi, A., Woodford, B. J., & Lin, H. (2017). Dynamic real-time segmentation and recognition of activities using a multi-feature windowing approach. In: *Proceeding of the PAKDD 2017 trends and applications in knowledge discovery and data mining*.

Skocir, P., Krivic, P., Tomeljak, M., Kusek, M., & Jezic, G. (2016). Activity detection in smart home environment. In *20th international conference on knowledge based and intelligent information and engineering systems*. Procedia Computer Science.

Tapia, E. M., Intille, S. S., & Larson, K. (2004a). Activity recognition in the home using simple and ubiquitous sensors. In *Proceedings of the international conference on pervasive computing*. Springer-LNCS.

Tapia, E. M., Intille, S. S., Larson, K. (2004b). *Activity recognition in the home using simple and ubiquitous sensors*. International Conference on Pervasive Computing, Springer-LNCS.

Theodoridis, S., & Koutroumbas, K. (2009). Chapter 3. In *Pattern recognition* (4th ed., pp. 77–82). London: Elsevier.

Van Kasteren, T., Noulas, A., Englebienne, G., & Kröse, B. (2008). Accurate activity recognition in a home setting. In *Proceedings of the 10th international conference on ubiquitous computing, Seoul, South Korea*.

Virone, G., Alwan, M., Dalal, S., Kell, S. W., Turner, B., & Stankovic, J. A. (2008). Behavioral patterns of older adults in assisted living. *IEEE Transactions on Information Technology in Biomedicine, 12*, 387.

Wang, W., & Miao, C. (2008). Activity recognition in new smart home environments. In *PETRA 2008 Athens, Greece*.

Witten, I. H., & Frank, E. (2005). Chapters 2–6. In *Data mining: Practical machine learning tools and techniques* (2nd ed.). San Francisco.

Wu, C. (2019). Nonparametric activity recognition system in smart homes based on heterogeneous sensor data. *IEEE Transactions on Automation Science and Engineering, 16*(2), 678–690.

Zdravevska, A., Dimitrievski, A., Lameski, P., Zdravevski, E., & Trajkovik, V. (2017). Cloud-based recognition of complex activities for ambient assisted living in smart homes with non-invasive sensors. In *IEEE EUROCON 2017 -17th International Conference on Smart Technologies, Ohrid*.

Zdravevski, E., Lameski, P., Trajkovik, V., Kulakov, A., Chorbev, I., Goleva, R., Pombo, N., & And Garcia, N. (2017). Improving activity recognition accuracy in ambient-assisted living systems by automated feature engineering. *IEEE Access, 5*, 5262–5280.

Zolfaghari, S., & Keyvanpour, M. R. (2016). SARF: Smart activity recognition framework in ambient assisted living. In *2016 Federated Conference on Computer Science and Information Systems (FedCSIS), Gdansk* (pp. 1435–1443).

Chapter 14
Deep Learning and IoT for Agricultural Applications

Disha Garg and Mansaf Alam

Abstract Presently it is really difficult to deal with agriculture and its requirements. The majority of the country's population depends entirely on agriculture. Food production should also be improved as the world population is constantly growing. Recent technological advances have had a major impact on agriculture. Advancement of latest technologies like Internet of Things (IoT), Machine Learning (ML) and Deep Learning (DL) has attracted researcher's attention to apply these methods to agriculture. Smart agriculture/farming is one of IoT's emerging areas. Sensing temperature of soil, nutrients and humidity, controlling and analyzing water consumption for growth of plant are some of the recognized IoT based analytics applications. IoT devices collect and generate enormous quantities of data for various fields and applications. This chapter shows different farming issues that can be solved by applying deep learning and IoT technologies in agriculture domain.

Keywords Artificial neural networks · IoT · Machine learning · Deep learning

14.1 Introduction

According production will rise by 70% globally by 2050 (Food and Agriculture Organization of the United Nations n.d.). Indian farmers are facing many problems like lack of knowledge about their soil, sudden rains in their areas without any correct weather forecast, crop disease problem, and water management problem which directly affect the agricultural outcomes. We can see that there is a developing interest for food that makes the progress in agricultural practices. According to the United Nations Food and Agriculture Organization (FAO), there will be 8 billion individuals approximately globally by 2025 and 9.1 billion by 2050 (FAO 2009). Thus, it is easy to predict that food.

D. Garg (✉) · M. Alam
Department of Computer Science, Jamia Millia Islamia, New Delhi, India
e-mail: malam2@jmi.ac.in

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_14

In 1999, Internet of things (IoT) came into existence (Tzounis et al. 2017). Internet of Things (IoT) is being utilized in Agriculture which improves the quality of farming outcomes. IoT acts very well in other applications areas like health, smart city, transportation, traffic control system and security (Baranwal et al. 2016; Garg et al. 2020), supply chain and others. The size of data that is generated by sensor devices continuously generates structured and unstructured or semi-structured data in huge quantities. Analytics must be applied over such data so that we can predict the future and find recent information. Analyzing large quantities of information, however, is not an easy job. Data is helpful if it generates an action and a smart learning mechanism is needed to make it workable. The main concern is how to analyze large quantities of information from complex IoT data Recently Deep Learning (DL) Technology is attaining momentum. In various IoT applications since it has the capacity to achieve quick results. Using IoT devices we are familiar with the idea of connected devices but IoT with deep learning generates an idea of 'connected-intelligence'. Deep learning would be very effective in solving complex real-life issues (Li et al. 2018).

A large quantity of data collected by using remote sensing involves images, which is fully depiction of the agricultural environments and addresses various challenges. In the agricultural domain, imaging analysis is the most significant research region and for identification/classification or anomaly detection in these images, intelligent data analytics is used for various agricultural applications. The main motive behind this chapter is to investigate the applicability of these techniques in agriculture with the advent of the Internet of Things (IoT) to increase popularity of sensor-based applications. Machine Learning (ML) and Artificial Intelligence (AI) are likewise groundbreaking innovations which influenced many different domains like precision farming, automated agricultural growth and analytics of environmental forecasting and others.

The remainder of the section was structured as follows: Section 14.2 is IoT in Agriculture. Section 14.3 gives overview of Deep Learning. While in Sect. 14.4 we have explained Deep Learning for smart agriculture. Basically in this Section we have discussed various Deep Learning architectures, tools and applications that can be used in smart agriculture. Finally, Sect. 14.5 concludes with a understanding on the feasibility of the integrating IoT technologies and Deep Learning and research possibilities of this research zone.

14.2 IoT in Agriculture

In various real life applications, IoT is getting involved. IoT greatly affects streamlining the production in agricultural sector. In smart agriculture, we build up a framework by utilizing sensors like soil moisture sensor, water level sensor, temperature sensor for monitoring the agricultural activity like crop and plant monitoring, irrigation monitoring in addition to others. Likewise, agricultural field can be monitored by farmers from anyplace continuously. IoT-based smart farming is very productive when contrasted with the ordinary farming techniques like Planting,

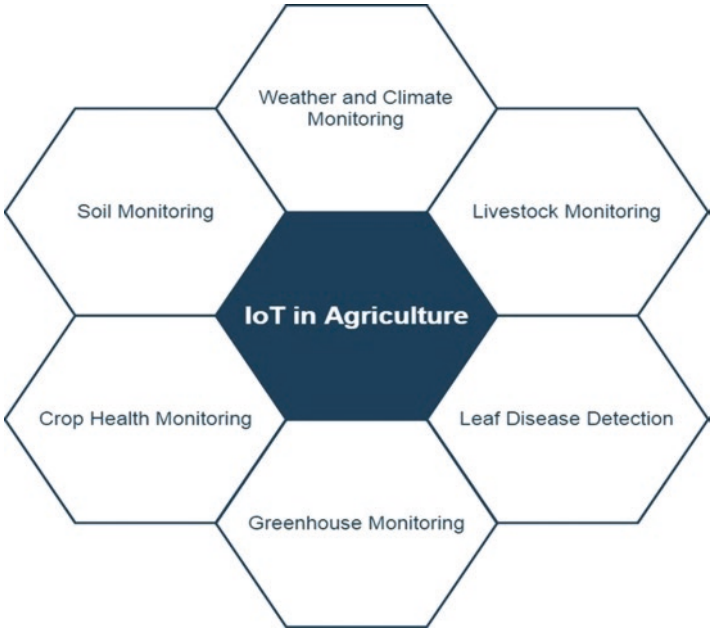


Fig. 14.1 IoT in agriculture

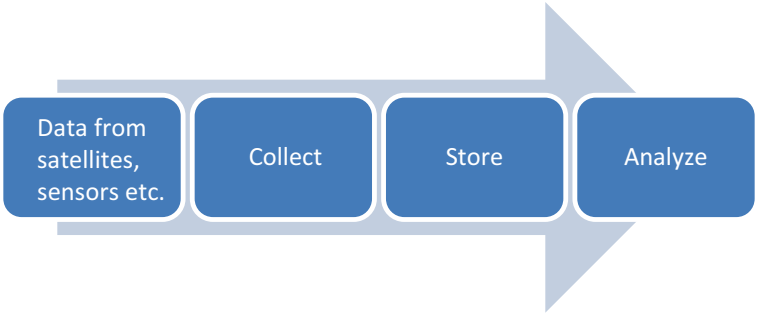


Fig. 14.2 Data analysis process

manual tilling, and reaping (Verma and Usman 2016).various applications of IoT based agriculture are shown in Fig 14.1.

Smart agriculture is one of IoT's emerging areas. The volume of data that is generated by sensor continuously generates enormous quantities of structured, unstructured or semi-structured data. This enormous data brings out notion of big-data, which is a huge quantity of data collected from various sources like business, sensor and social networking related large data. The foremost challenges encounters in IoT are to record, store, analyze, and search the data**.** The data analysis process in IoT is shown in Fig 14.2.

Table 14.1 Major farming problems

Problem	Description
Water Irrigation problems	Appropriate management of water is necessary as farming consumes 70% of global fresh water (Projectguru n.d.)
	Intelligent water management system should be used (Muangprathub et al. 2019)
Lack of soil knowledge	Due to varying weather conditions, the soil structure changes every day and farmers always face issues in identifying the soil for their crop (Mohanraj et al. 2016)
Disease Detection problems in Plant	Timely Detection of disease in leaves of plant (Thorat et al. 2017) is necessary but there may be delay in the detection of plant disease on the right time so automatic detection is required (International Atomic Energy Agency 1998)
Logistics Management Problem	The efficiency of the supply chain can be improved with the assistance of location-based sensors, showing improvements in transparency and client understanding (Razzak et al. 2018)
Nutrients deficiency detection	Evaluation of nutrient demands in soil and plant with the assistance of IoT devices should be carried out efficiently (Sundmaeker et al. 2016)
Detection of Nitrate Level	Nitrates are the pollutants present in water, fruits and vegetables to monitor the quantity of nitrate in water, fruits and vegetables (Alahi et al. 2018)

Like other application areas, smart farming produces enormous and complex data. In addition, the information originates from distinct kinds of sensor systems, resulting in heterogeneity in the information resource obtained. The primary issue is therefore how this complicated real-world IoT data (Mahdavinejad et al. 2018) can be analyzed to obtain helpful information. There are numerous analytical solutions for IoT big data to find out valuable insights of the large data generated by IoT devices.

IoT-based Smart farming can be helpful in delivering advantages such as water and fertilizer optimum use. In Table 14.1, we will address the significant agricultural issues that IoT-based intelligent farming can solve in order to revolutionize the agricultural domain:

14.3 Deep Learning Overview

Deep Learning is based on artificial neural networks (ANNs) or computational frameworks which mimic functioning related to brain of human. Natural language processing, Automatic Game Playing, voice control in tablets, phones, and hands-free speakers, Driverless cars in additions to others are the major applications of Deep Learning (DL).

In this, a computer model learns directly from speech, text, or pictures how to apply classification. Deep Learning models (DLM) are trained with help of large set

of data that is labeled data with neural networks architectures that consist various hidden layers.

Many deep learning approaches are using neural network architectures. This is the reason that Deep Learning (DL) models are called as Deep Neural Networks (DNN). The Deep Learning (DL) training method is called 'Deep' because ANNs are covering an enormous amount of levels as time goes by. Consequently, the procedure productivity is directly proportional to the network depth. NNs obtain learning algorithms and increasing big quantities of information to make the training processes more effective. If the dataset is bigger, there will be an effective processing.

Deep Learning utilizes distinct information processing algorithms (Liakos et al. 2018) and pursues the process of thinking. Some of the inventions connected with this sector such as self-driving cars and recognition of voice and picture. Machine learning models cannot manage high-dimensional and complex data with significantly high input and output sizes. Use cases such as image processing, image translation and natural language processing, which generate high dimensional information that is hard to process. Deep learning went into being to mitigate such difficulties Deep Learning contributes to the model more profundity or concealed layers and reflects information in a progressive manner that would then be able be used to detect and predict computerized farming tasks (Mohammadi et al. 2018).

Deep Learning's most exciting benefit is the extraction of features or characteristics from the raw data and focuses on the correct features or characteristics alone. This method is basically called feature extraction when input data is transformed into a collection of features which then depict the input data very clearly. Extraction of features or characteristics utilizes few algorithms to create significant characteristics of data automatically for practice, teaching and understanding. There is no requirement in Deep Learning to manually extract image characteristics. During training, the network learns to extract features. Simply insert the pixel or image into the network and represent the framework of the NNs and verified dataset. The process of Deep Learning (DL) is illustrated in Fig. 14.3.

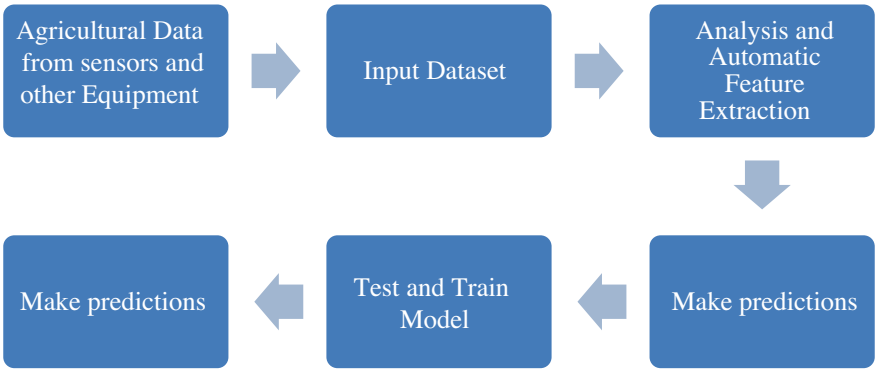


Fig. 14.3 Deep Learning process

DL and ML was used to boost analytics and learning with in IoT applications. IoT devices produce Big Data and Deep Learning is used to find the right analytics from this massive information. Numerous IoT applications use classification of images to recognize plant illness, Recognize traffic Signs (Marjani et al. 2017) and detect human poses.

In many IoT applications input information is in the form of pictures and videos for Machine Learning (ML) and Deep Learning (DL) Algorithms. Intelligent Videos Cameras are also used in most applications smart homes, smart agriculture, smart city and many more.

14.4 Deep Learning for Smart Agriculture: Concepts, Algorithms, Frameworks and Applications

Deep Learning is a resolution of automation of predictive analytics. DL utilized in agriculture for different Applications, for example fruit counting, and crop classification or plant classification, detection of fruit type (Sa et al. 2016), hydroponic agriculture. Healthy crops must be produced for supportable agriculture. Deep Learning has demonstrated effective in tackling complex issues like picture recognition, object detection, natural language processing, image classification, image segmentation (Mohammadi et al. 2018; Alahi et al. 2018). Classification accuracy of deep learning gives outstanding results on the large quantity of data so there is a need of big quantity of training dataset (Schmidhuber 2015). Deep learning is also used for multiple functions such as automatic farming forecast and detection. Previous work done on Smart agriculture including deep Learning and Machine Learning is discussed:

Shekhar et al. (2017) created a smart, fully automatic IoT-based irrigation system. In this system soil temperature and moisture data were captured using sensors and k-nearest neighbor classification Algorithm was used to assess sensor data to predict soil water irrigation. In this system various devices interconnect with each other and intelligent irrigation was used. To develop this system, they used Raspberry Pi3, Arduino Uno. The prepared data set and anticipated data were put aside on the cloud server to allow farmers to access information through their mobile phones.

Mehra et al. (2018) created a smart hydroponic framework based on IoT using deep neural networks (DNN). This smart framework offers appropriate control action for the hydroponic environment rely on various input parameters, for instance temperature, pH, lighting and moisture level without human interference. To train these parameters, Deep Neural Network is used. Over a number of weeks, they gathered all parameters in runtime and trained these parameters 10,000 numbers of times to obtain 88% accuracy. This framework is additionally created utilizing Arduino and Raspberry Pi3. The forecasted information was stored on the cloud in real time.

Sladojevic et al. (2016) created a model to classify images of the leaf and identify plant disease by utilizing deep convolutional networks. In this paper, they studied the technique of deep learning to classify and automatically identify plant disease by taking pictures of the leaf in consideration. This identification model is capable of identifying 13 plant diseases. Approx. 3000 initial pictures from Internet sources were used to create the database. For CNN training, they used Caffe which is a Deep Learning (DL) Framework. The model precision was accomplished at 96.3%.

Using WSN (Wireless Sensor Network), Varman et al. (2017) also worked on Deep Learning and IoT for intelligent farming. For the next crop rotation, the proposed plan predicts the suitable yield and improvises the field irrigation framework. This was accomplished when the field was regularly monitored. Soil parameters such as temperature, moisture and others were gathered for field surveillance purposes. They established WSN to retrieve sensor information, and the analysis was carried out by uploading cloud information.

14.4.1 Common Deep Learning Algorithms

In this section, we discuss a brief overview of various Deep Learning algorithms that are most commonly used:

14.4.1.1 Convolutional Neural-Network (CNN)

CNN is a collection of deep, feed-forward (not recurrent) artificial neural networks (ANN) that are used to analyze visual imagery. These networks are made up of neurons that have learnable weights and biases. Some inputs are given to each neuron and then a dot product is performed by them. A CNN accepts a Two-Dimensional input like an image or voice signal and produce characteristics through a sequence of hidden layers. Structure is comprised of the convolutional and the pooling layers for extraction feature and both connected layers work as a classifier. Also, CNN can be used in agricultural areas like crop and plant leaf disease detection, land Cover classification, plant recognition, weed identification and fruit counting.

14.4.1.2 Recurrent Neural Networks (RNN)

RNNs are a network of neuron- like nodes that composed in to successive “layers”. Every single node relates to a directed connection i.e. one-side connection to each node in the next consecutive layer and utilized in many agricultural territories, for example, soil cover classification, estimation of crop yield, weather prediction, soil moisture content estimation, animal research in addition to others. RNN is very much suitable to process time series data.

14.4.1.3 Generative Adversarial Networks (GAN)

Basically, GANs are made up of a framework of two contesting neural network models. These models can be used to inspect, interpret and mimic from the training dataset. Also, GAN has often been used to enhance datasets. Among these two neural networks, one is generative and the second one is discriminative networks, these networks work together so that they can produce high quality data. GAN is another classification of neural network however particularly in image processing; it has been considered a very useful method.

14.4.1.4 Long- Short Term Memory (LSTM)

This is the most prevalent algorithm among many deep learning algorithms. It can process single information points, (for example, image), as well as whole successions of data, (for example, voice or video). These are suitable for classification and making forecast depend on time series data. For agricultural applications, LSTM is used for crop type classification, crop yield prediction and weather prediction. LSTM is also applicable for handwriting recognition, speech recognition in addition to others.

14.4.2 Deep Learning Frameworks

Deep Learning framework is an interface or a tool which allows us to build deep learning models more easily and quickly without going into the details of underlying algorithm. We described some frameworks below:

14.4.2.1 TensorFlow

TensorFlow is an open source software library for Deep Learning and Machine learning and it uses various Deep Neural Networks. It is used to build neural network models by graph representations. Nodes depict mathematical operations according to the graph and edges depict the multi-dimensional data arrays (tensors) that stream between them. TensorFlow offers TensorBoard, a suite of imaging tools, to visualize the outcomes of TensorFlow.

14.4.2.2 Caffe (Convolution Architecture for Feature Extraction)

CAFFE is an open source framework which supports various types of Deep Learning (DL) architectures. This framework is based on C++ and it supports CUDA (Compute Unified Device Architecture) for GPU (Graphics Processing Units) com-

putations and provides interfaces for MATLAB & Python. It also supports various types of deep learning architectures for image segmentation and image classification. It supports CNN, LSTM and fully connected neural network designs.

14.4.2.3 PyTorch

PyTorch is an open source code framework for machine learning (ML). This is used for easy making of DNN models. It contains a broad range of DL algorithms**.** It builds on Torch, a scientific computing framework that is used to develop and train deep neural networks. The PyTorch framework makes the process of training and developing deep learning models easy to execute and learn because of its clean architectural style.

14.4.2.4 Theano

Theano is an open source Python language-based Deep and machine learning framework. Theano offers fast computation and it can be run on both CPU and GPU. Although it works faster on Graphics Processing Unit (GPU) rather than on CPU. To train deep neural network algorithms, Theano is used.

14.5 Applications of Deep Learning in Agriculture

Deep learning has numerous applications in farming. Some of the relevant previous work done in agriculture using deep learning is discussed in Table 14.2.

14.6 Conclusion

The population of the world is growing day by day and demand for food production is also steadily increasing (Wolfert et al. 2017). Government encourages farmers to use sophisticated methods to boost food production. Farmers use important insights from IoT data to improve investment returns. Detection of soil temperature, nutrients and moisture, examining and controlling utilization of water for plant development are the known uses of analytics built on IoT.

Deep learning and IoT are standing out for researcher on the grounds that these two methods have beneficially affected human life, urban networks, and the world. The association among IoT with Deep Learning is considered as a maker customer association, so IoT devices generate information and this raw data is broke down utilizing Deep Learning (DL) strategies the subsequent bits of knowledge are provided to IoT frameworks for administration improvement (Kamilaris and Prenafeta-Boldú 2018).

Table 14.2 Major Application Areas in Agriculture and sources of data

No.	Application Area in Agriculture	Problem Description	Framework Used	Dataset used	Reference
1	Plant recognition	Perceive seven perspectives related to different plants: whole-plant, flower, branch, fruit, Leaf, stem and scans	Caffe	data set of Plants (Life CLEF 2015) having 91759 Images	Reyes et al. (2015)
2	Crop type classification	Characterization of crops type such as sugar beet, maize, wheat, soybean and sunflower	Developed by the authors	19 multi-temporal scenes contained by Landsat-8 and Sentinel-1A RS satellites from Ukraine	Kussul et al. (2017)
3	Detection of Leaf diseases	13 distinct kinds of plant diseases in addition to healthy leaves	Caffe	Authors self-developed database having 4483 images	Sladojevic et al. (2016)
4	Fruit counting	Forecast of number of tomatoes from images	TensorFlow	24000 synthetic images generated by the authors	Rahnemoonfar and Sheppard (2017)
5	Forecast of soil moisture content	Forecast of the soil moisture content over a watered corn field	Developed by authors	Data related to Soil gathered from a watered corn field in North-west China	Song et al. (2016)
6	Detection of Plant diseases	Identify 14 crop species and 26 diseases	Caffe	Plant Village public data set of 54306 images of diseased and healthy plant Leave	Mohanty et al. (2016)

By utilizing un-supervised learning techniques of Deep Learning, a framework ends up more intelligent all alone. Deep Learning has the ability to identify the most important characteristics that help to deliver accurate and reliable outcomes. Since we understand that deep learning can produce characteristics without human interference, data scientists can save most of the time if they work with IoT Big data. When we contrast with conventional machine learning algorithms, deep-learning (DL) uses complicated sets of characteristics. IoT sensor systems need to be easy to use to enable farmers to take benefit of it. In the coming years, with the Deep Learning algorithm, we ought to create and redesign application for the real-time analysis of recorded information using IoT sensors.

References

Alahi, M. E. E., Nag, A., Mukhopadhyay, S. C., & Burkitt, L. (2018). A temperature-compensated graphene sensor for nitrate monitoring in real-time application. *Sensors and Actuators A: Physical, 269*, 79–90.

Baranwal, T., Nitika, & Pateriya, P.K. (2016). *Development of IoT based smart security and monitoring devices for agriculture*. 2016 6th International Conference - Cloud System and Big Data Engineering (Confluence), 597–602.

Food and Agriculture Organization of the United Nations. (n.d.). *How to feed the World in 2050*. http://www.fao.org/fileadmin/templates/wsfs/docs/expert_paper/How_to_Feed_the_World_in_2050.pdf

Garg, D., Khan, S., & Alam, M. (2020). Integrative use of IoT and deep learning for agricultural applications. In *Proceedings of ICETIT 2019* (pp. 521–531). Cham: Springer.

International Atomic Energy Agency. (1998–2019). *Agricultural water management*, https://www.iaea.org/topics/agricultural-water-management

Kamilaris, A., & Prenafeta-Boldú, F. X. (2018). Deep learning in agriculture: A survey. *Computers and Electronics in Agriculture, 147*, 70–90.

Kussul, N., Lavreniuk, M., Skakun, S., & Shelestov, A. (2017). Deep learning classification of land cover and crop types using remote sensing data. *IEEE Geoscience and Remote Sensing Letters, 14*(5), 778–782.

Li, H., Ota, K., & Dong, M. (2018). Learning IoT in edge: Deep learning for the internet of things with edge computing. *IEEE Network, 32*(1), 96–101.

Liakos, K., Busato, P., Moshou, D., Pearson, S., & Bochtis, D. (2018). Machine learning in agriculture: A review. *Sensors, 18*(8), 2674.

Mahdavinejad, M. S., Rezvan, M., Barekatain, M., Adibi, P., Barnaghi, P., & Sheth, A. P. (2018). Machine learning for Internet of Things data analysis: A survey. *Digital Communications and Networks, 4*(3), 161–175.

Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Hashem, I. A. T., Siddiqa, A., & Yaqoob, I. (2017). Big IoT data analytics: architecture, opportunities, and open research challenges. *IEEE Access, 5*, 5247–5261.

Mehra, M., Saxena, S., Sankaranarayanan, S., Tom, R. J., & Veeramanikandan, M. (2018). IoT based hydroponics system using deep neural networks. *Computers and Electronics in Agriculture, 155*, 473–486.

Mohammadi, M., Al-Fuqaha, A., Sorour, S., & Guizani, M. (2018). Deep learning for IoT big data and streaming analytics: A survey. *IEEE Communications Surveys & Tutorials*.

Mohanraj, I., Ashokumar, K., & Naren, J. (2016). Field monitoring and automation using IOT in agriculture domain. *Procedia Computer Science, 93*, 931–939.

Mohanty, S. P., Hughes, D. P., & Salathé, M. (2016). Using deep learning for image-based plant disease detection. *Frontiers in Plant Science, 7*, 1419.

Muangprathub, J., Boonnam, N., Kajornkasirat, S., Lekbangpong, N., Wanichsombat, A., & Nillaor, P. (2019). IoT and agriculture data analysis for smart farm. *Computers and Electronics in Agriculture, 156*, 467–474.

Projectguru. (n.d.). *Modern agriculture technology versus India's agricultural practices*. https://www.projectguru.in/publications/technology-indias-agricultural-practices/

Rahnemoonfar, M., & Sheppard, C. (2017). Deep count: Fruit counting based on deep simulated learning. *Sensors, 17*(4), 905.

Razzak, M. I., Naz, S., & Zaib, A. (2018). Deep learning for medical image processing: Overview, challenges and the future. In *Classification in BioApps* (pp. 323–350). Cham: Springer.

Reyes, A. K., Caicedo, J. C., & Camargo, J. E. (2015). Fine-tuning deep convolutional networks for plant recognition. *CLEF (Working Notes), 1391*.

Sa, I., Ge, Z., Dayoub, F., Upcroft, B., Perez, T., & McCool, C. (2016). Deepfruits: A fruit detection system using deep neural networks. *Sensors, 16*(8), 1222.

Schmidhuber, J. (2015). Deep learning in neural networks: An overview. *Neural Networks, 61*, 85–117.

Shekhar, Y., Dagur, E., Mishra, S., & Sankaranarayanan, S. (2017). Intelligent IoT Based Automated Irrigation System. *International Journal of Applied Engineering Research, 12*(18), 7306–7320.

Sladojevic, S., Arsenovic, M., Anderla, A., Culibrk, D., & Stefanovic, D. (2016). Deep neural networks based recognition of plant diseases by leaf image classification. *Computational Intelligence and Neuroscience*.

Song, X., Zhang, G., Liu, F., Li, D., Zhao, Y., & Yang, J. (2016). Modeling spatio-temporal distribution of soil moisture by deep learning-based cellular automata model. *Journal of Arid Land, 8*(5), 734–748.

Sundmaeker, H., Verdouw, C., Wolfert, S., & Pérez Freire, L. (2016). *Internet of food and farm 2020. Digitising the Industry-Internet of Things connecting physical, digital and virtual worlds*. Vermesan, O., & Friess, P. (Eds.), 129–151.

The state of food and agriculture. (2009). http://www.fao.org/3/a-i0680e.pdf

Thorat, A., Kumari, S., & Valakunde, N. D. (2017). *An IoT based smart solution for leaf disease detection*. In Big Data, IoT and data science, 2017 International conference on (pp. 193–198). IEEE.

Tzounis, A., Katsoulas, N., Bartzanas, T., & Kittas, C. (2017). Internet of things in agriculture, recent advances and future challenges. *Biosystems Engineering, 164*, 31–48.

Varman, S. A. M., et al. (2017). *Deep learning and IoT for smart agriculture using WSN*. 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), IEEE.

Verma, N. K., & Usman, A. (2016). *Internet of Things (IoT): A relief for Indian farmers*. In Global Humanitarian Technology Conference (GHTC), 2016 (pp. 831–835). IEEE.

Wolfert, S., Ge, L., Verdouw, C., & Bogaardt, M. J. (2017). Big data in smart farming – A review. *Agricultural Systems, 153*, 69–80.

Chapter 15
IoT for Crowd Sensing and Crowd Sourcing

Vinita Sharma

Abstract This chapter starts with the origin of the concept of crowdsourcing followed by the understanding of the concept of crowd sensing with the help of various examples of well-known International brands. The concept of IOT is explained in brief along with sensors and actuators etc. Due to existence of IOT, transformation of crowdsourcing into crowd sensing has evolved. Applications of crowd sensing in India and western countries are used as examples for explaining the concepts thoroughly. At the end the chapter includes the initiatives that the industry has taken up for adopting emerging technology for a better future and the challenges that the world is facing in deployment of the emerging technologies in the industry.

Keywords Internet of Things · Crowd sourcing · Crowd sensing · IOT

15.1 Introduction

Starting from Germany and other western countries, the technological advancements of 4th industrial revolution are now spreading their wings in India as well, and revolutionizing industrial production. Internet of Things is one of the emerging technologies used for this industrial revolution, that are blurring the boundaries between digital, physical and biological worlds.

In presence of Internet, if two or more physical devices can communicate with each other without any human intervention, the concept is known as Internet of Things. This concept of Internet of Things (IoT) was first introduced by Ashton in 1999. In IoT the Internet is an origin of World Wide Web and the core basis of the technology Internet of Things. The concept of Internet of Things starts with Radio-Frequency Identification Device (RFID). During a disaster, if people had an access to RFID equipment, they can accomplish things they could never do before. For

V. Sharma (✉)
New Delhi Institute of Management, New Delhi, India

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_15

example, people in the disaster-affected area can use RFID to connect and help other people within a certain radius. Such form of assistance is crucial for disaster management. IOT can extend the phenomenon of RFID to disaster management. It is, hence, indispensable in disaster relief, where even the smallest mistakes can be catastrophic.

The business environment today has shown remarkable changes in operation methods and processes. It has been observed that over a period of time and due to certain necessities, the customers have become much more demanding and want a change in the existing products. If an organization cannot fulfil those demands as per customers' interest and satisfaction, customers start showing their disinterest in the products or services resulting in lower profits. This scenario encourages the firms to look for more innovative ideas for creation of new products of customers' liking from outside the organization. Also, as per the concept of product development life cycle, products need to be changed with respect to time for sustainability in the market.

Social media technology has given strength to crowdsourcing. Social media is used extensively nowadays across the globe. There is large amount of User Generated Content (UGC) available on social media (e.g., Twitter, Facebook). This valuable information is widely analyzed and used and even helps Governments to take actions accordingly. Such crowdsourcing is defined as active crowdsourcing.

Another type is passive crowdsourcing which occurs when government agencies rely on social media to collect citizens' information about their respective knowledge, ideas and opinions about some specific topic(s) without giving any reaction.

On a similar note, the power of social media in disaster relief also cannot be ignored in the disaster-affected areas. The posted 'User Generated Contents' may provide valuable information for disaster response which might otherwise remain unexploited.

To make a customer an integral part of an organization for finding an innovative product development idea, crowdsourcing becomes an important methodology. When crowdsourcing is done via internet and social media, number of involved customers increase which in turn increases the chances of getting more innovative ideas. Increased online platforms and easy global connectivity are helping organizations to collect 'out of the box' ideas, not only from their customers, but also from public and that too of other countries as well.

SMEs in India need to adopt digital technologies at a large scale to remain competitive both in Indian and the global market. The industry is transforming from automatic work culture to autonomous work culture. While working, if any of the machines break down then other machine starts repairing it without any human intervention. This has become possible only because these machines are connected through a powerful network.

15.2 Internet of Things

Since it is a high tech strategic initiative plan in which internet based technologies improve all industrial processes, Industry 4.0 is going to affect almost all aspects of life and will bring a considerable transformation in the global economy too. This technological revolution will need specific skilled work force for which the Indian government, academia and industry need to come forward together and formulate plans to generate such workforce.

Starting from the manufacturing operations to sales and marketing campaigns, countries like Germany, China and USA took such initiatives to turn Internet environments into "smart environments". The current industrial revolution and crowdsourcing has enabled less powerful objects such as sensors or RFID tags to cooperate with more powerful machines to perform smarter applications for communication and cooperation among devices and standalone systems, so that a higher level of intelligence can be provided to all industrial processes.

But wireless signals are more prone to cyber-attack. To overcome this problem, specific security and privacy preservation technology is being developed. Provision of ubiquitous internet access has been evolved to fulfill industrial demands so that everything and everyone is connected all the time to exchange data and information.

Today even a non-technical person is quite familiar with the concepts of smart homes, smart cars, smart education and smart cities etc.

15.3 Crowdsourcing

The concept of crowdsourcing was devised by Jeff Howe in 2006. It can be explained as, 'to outsource few new business ideas from unknown or known people or community'. The task given by the company is either performed by individuals or a group. If the new idea clicks with the management of the organization, it is implemented and the product is launched in the market. This product is hence called a 'co-created product'. For the organizations in the western world, use of co-creation is very common. Organizations like P&G, Nike and Ikea got benefitted when they crowdsourced. Crowdsourcing helps the industries to create innovative products at much lower costs.

Crowdsourcing has been used for big projects also. Computer Scientists at Carnegie Mellon University created reCAPTCHA which uses humans to identify distorted words on any website. In fact, established brands in the international market have realized the importance and power of the crowd's opinion and learned how to couple it to their advantage. Internationally renowned organizations such as General Motors, PepsiCo, Heinz, Nestle and Starbucks had huge benefits through crowdsourcing and developing new products of the choice of the masses.

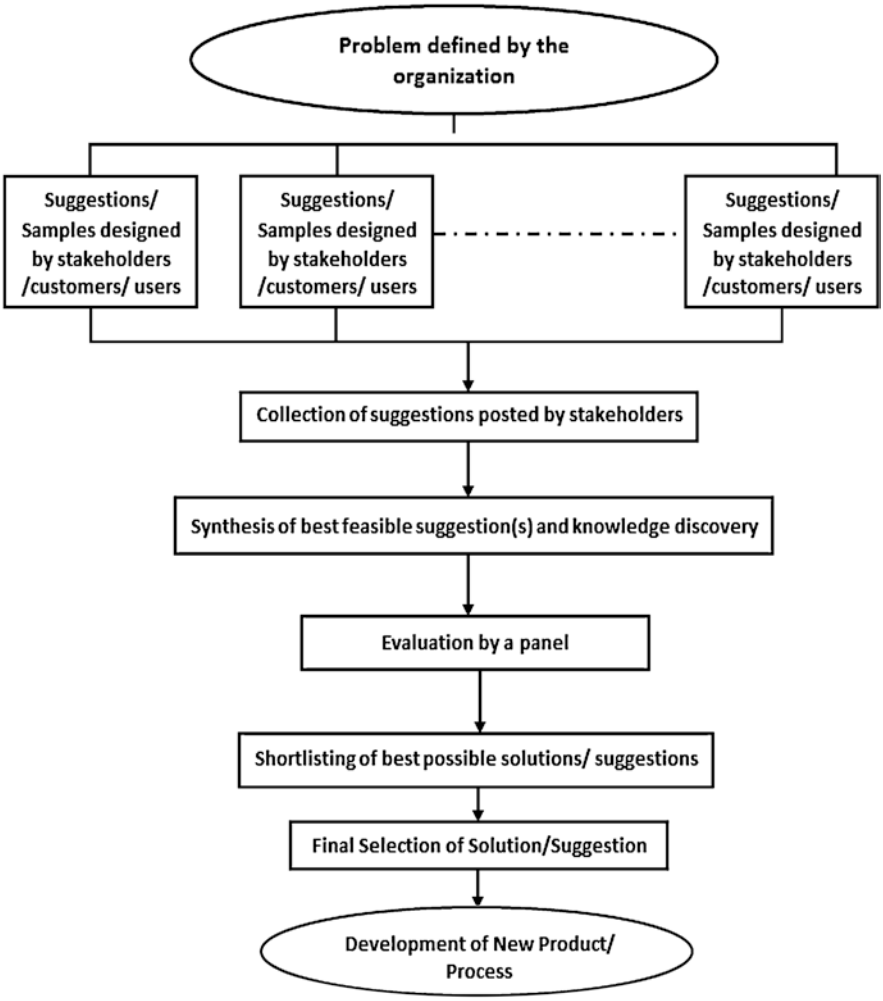


Fig. 15.1 New product development process through crowdsourcing

In fact, the organizations and their stakeholders, both, benefit from crowdsourcing. The stakeholder gets satisfied with the needs like social recognition, self-esteem and the development of individual skills and the organization gets reduced costs, better innovation, flexibility, scalability, and diversity. Crowdsourcing is usually designed as an open call or as a contest. A self-devised model for acquisition of suggestions or knowledge through crowdsourcing is shown in Fig. 15.1.

15.4 Classification of Crowdsourcing

15.4.1 Collective Intelligence for Problem Solving

Organizations use collective intelligence from different external sources to solve internal problems with the help of crowdsourcing. It is an appropriate method to explore activities in the areas of research and development, market research, knowledge management, and customer service.

Collective Intelligence represents sharing of knowledge through brainstorming by using some platform provided by the organization, where one can drop the idea or a related solution. Companies such as Dell and Starbucks are famous for using collective intelligence as a tool for solving different problems or producing new products.

15.4.2 Learning paradigms

Crowdsourcing is source for the generation of new ideas which contribute to organizational learning. Generally emerging and innovative organizations use crowdsourcing. Collection of ideas from stakeholders gives a learning opportunity to the organizations having saturated innovation. For example –

Smart India Hackathon
Smart India Hackathon (SIH) was launched by Government of India in 2017 with a philosophy that not everyone has a great talent, but a great talent can come from anywhere. That is exactly what was experienced in SIH.

In SIH, talented engineering students, academicians and industry practitioners from PAN India, worked in a team for continuously 36 h, searching for innovative solutions and competed for amazing prizes.

It was a great opportunity for the competitors to learn about challenges related to drones, robotics, IOT and 3D printing etc., which big companies like CISCO, Deloitte and various ministries of the Indian government were facing.

It can be considered as a good example of crowdsourcing. Live queries based on robotics, IOT, 3D printing, etc., solved by teams of students served the purpose of the various ministries of government of India and private sector organizations as well.

Hackathon is, hence, now emerging as the backbone of India's start-up ecosystem. Various ministries and organizations look for ideas as well as even try to hire talent at such events.

15.4.3 Open Innovation

Open innovation represents the needs of organizations to access new knowledge. Crowdsourcing is used to share, reuse, recombine, and accumulate knowledge to achieve external and internal innovation. In this sense, the crowd is considered as an innovation partner. For example, Coke and Maggi from Nestle.

The choice and behavior of the customers is changing very fast and becoming more and more diverse and demanding. Due to a huge customer base, even global brands are getting attracted towards India. For being a success in India, these brands must include the connection with the common people and hence crowdsourcing is extremely crucial for them. There are multiple examples which show that marketers are becoming more open to the crowd in India for increasing sales and productivity. The local Lays started 'Give Us Your Delicious Flavor' an initiative of PepsiCo India in 2009. The popular variants such as Cheesy Mexicana, Tangy Twist, Mastana Mango and Hip Hop Honey & Chilly (Campaign India, 2010) are results of that campaign.

Launching 'Baby Lips' of Maybelline
Maybelline invited millions of its Facebook fans to contribute to India's first ever crowd-sourced 'Kiss' song for launching the 'Baby Lips' lip balm. It made innovative use of a Facebook application to source the kisses of the crowd. More than 6000 females sent their kisses. Besides the crowdsourcing initiative on social media, 'Baby Lips' created a great visual impact of the video for the new product.

The Baby Lips Kiss song received approximately 3.7 million views on YouTube since it was launched in May, 2013. The sales of the lip balm during summer matched the sales of the product during December, which typically is the month that sees the highest usage of the product due to winters. Crowdsourcing helped to enrich communication, as well as represented the brand as it is seen by consumers. It thus built authenticity and a direct connection with the consumers.

15.4.4 New Product Development or Crowd Creation

It is the most common form of crowdsourcing. User innovations can be used to create new products, designs, and services which satisfy the needs of customers. The crowd can provide feedback to the organizations for their existing products in the process of creating new products. For example –

'My Expression' and 'My Expression 2' of Tanishq
'My-expression' of 'Tanishq' under the Tata Group of India is an innovation to highlight the beginning of the co-creation concept for generating a new product through crowdsourcing. The organization adopted crowdsourcing to co-create by attracting and involving customers and other stakeholders through a web application. Tata used crowdsourcing to collect innovative ideas online from the customers'

knowledge and information, and integrated these ideas into the profit-making processes of the organization.

Tanishq launched "Mia" in November, 2011 for a specific segment of working women. Along with market research for the product, it started a crowdsourcing campaign through a web application and later through social media platform too, known as 'My Expression' in the year 2012. In fact, working women were also looking for some unique and simple designs of jewelry which they could use at their work place without any hesitation, on daily basis.

To fulfil their needs, it was essential to understand the accurate desire of the working women. Hence, designs from the current and potential customers were collected. The participants were given the facility of an interface, a Do-It-Yourself (DIY) tool through which they could upload their designs, text, picture or YouTube link. The uploaded ideas were the shortlisted by the jury members based on their creativity, originality and feasibility to manufacture. Tanishq chose 10 finalists, and their designs were used in the Mia collection. More than 3200 entries were received from almost 40,000 individuals' online voting (crowd voting). Finally, Mia got 25 new innovative designs added in its collection through crowdsourcing.

After the grand success of 'My Expression', 'My Expression 2' was launched in 2013 to give shape to more inspirations and ideas in the form of Mia collection. With the aim to encourage women to source inspiration from the smallest thing and turn it into beautiful pieces of jewelry, 'My Expression 2' identified and rewarded the best creative minds across the country.

15.4.5 Collaborative Initiative Through Crowd Funding

Collaborative initiatives are an emerging trend in crowdsourcing. Many start-ups use crowdsourcing as a coordination and collaboration mechanism. Firms also seek partnerships or investment through crowdfunding, where entrepreneurs raise funds or donations from the crowd. New business models are being dedicated to crowdsourcing itself, with online platforms that enable third parties to launch and manage collaborative crowdsourcing initiatives.

Platforms like kickstarter.com enable people to raise money for their projects. There are platforms even for raising money for non-profit organizations. And now there is the emerging version which can allow for micro-angel investing.

15.4.6 Crowd Voting

It is one of the most popular form of crowdsourcing which generates the highest level of participation. It is based on crowd's judgment. Google's search engine is built upon the principle of Crowd Voting. Reality TV shows offer another example of Crowd Voting.

15.4.7 Crowd Curation

It is a process of gathering information relevant to a topic or area of interest. It is good for building and sharing knowledge but unable to solve defined problems. For example – Wikipedia, TripAdvisor, etc.

15.4.8 User-Generated Content (UGC)

UGC is any type of content such as videos, images, text or audios, posted on an online platform. This model helps to build large content repositories with a limitation that it cannot ensure the best possible quality of the content. E.g.- YouTube, iStockphoto.

15.4.9 Crowd Labour

An online platform to enable organizations or individuals to access an indefinite and unknown group of other organizations or individuals to solve specific problems or to provide specific services or products in exchange for payment. E.g.- OLA, Uber taxi services. Although considered as a powerful resource for companies and a strategic tool, co-creation through crowdsourcing is nonetheless very complex in practical sense and raises too many questions. It is deliberated that crowdsourcing can be a strategic tool. Generally, social media is used as a platform to perform crowdsourcing and is usually designed as an open call or as a contest. Crowdsourcing is a concept which can be used by the organizations in multiple ways. Few of the ways of deploying crowdsourcing are explained through examples below-.

The Wall Street Journal revealed the fact that in Australia, a mobile App 'Pizza Mogul' was launched by Domino's in 2014. This App helped the customers to design pizza of their own choice and upload it on social media for collecting views of other customers too. This App got so popular in Australia and within 6 months Domino's net profit increased by 67% to a record 29.1 million Australian dollars (US$22.6 million) on the back of a 29% surge in revenue (Fig. 15.2).

In fact, crowdsourcing creates a win-win situation for both, the organization and the stakeholder. The stakeholder's needs of getting recognized socially, self-esteem and the development of individual skills gets satisfied and the organization gets reduced costs, better innovation, flexibility, scalability, and diversity.

Fig. 15.2 Mobile App Pizza Mogul. (Source – CIOL Bureau, 2017)

15.5 Applications of Crowdsourcing in India

Although crowdsourcing creates an eco-system of engaging with stakeholders that are relevant and co-creating the future of business with them. (Exchange4media, 2013), but unfortunately it is little implemented by the organizations in a country like India. Few applications based on crowdsourcing in India can be discussed as below –

- **The Indian Rupee Symbol**

- The origin of the new Rupee symbol was not the output of any great creative designer, but the creation of a common man through crowdsourcing.
- **Ford EcoSport**
- Ford crowdsourced its 'Urban Discoveries' campaign to launch the car 'EcoSport' in India. Ford received more than 250 different videos from the stakeholders.
- **Crowdsourcing in Academic Institutions**

Recently Munger University of Bihar gave an open invitation to all Indian nationals to participate in various online competitions of designing of logo, monogram, flag and seal of the university, which is given in Fig. 15.3.

The best designs collected from PAN India were to be shortlisted by the panel assigned by the university and the best-chosen design of each category would be selected by the university. Winners would be rewarded for their hard work. This competition was ongoing when this paper was being written.

- **The website MyGov.in**

- Government of India has also taken various initiatives for collection of views of people of India through crowdsourcing and social media technology. MyGov is one of the world's largest crowdsourcing platform from India which uses hashtags, polls, interactive discussion forums and social media account integration (MyGov.in). It uses analytical tools for data mining which makes it easier to navigate and shows real time data about registered users, task submissions and number of comments across different discussion themes on the landing page.


Adv. No.03/19 Last date: 29.06.19 (5 P.M.)

MUNGER UNIVERSITY, MUNGER-811201

www.mungeruniversity.ac.in

State Univ. u/s 22 of UGC Act

Admin Block, Shastri Nagar, Munger- 811201

Competition for selection of design of Logo, Seal, Monogram and Flag for the University

Prize worth Rs. 2,00,000 to be won

Munger University is looking for designs of its logo, seal, flag and monogram. A nation-wide open competition is being launched for selection of the best drawing/design in each of the four categories. A cash prize of Rs. 50,000 will be given in each of the four competitions amounting to a total of Rs. 2,00,000. Additional prizes in form of gift- hampers are also proposed to be given to the adjudged winners. Ten participants in each of the four categories will be recognized by giving consolation certificates. Entries (soft copies/drawing) are to be sent through e-mail to logo@mungeruniversity.ac.in by 29.06.2019 (5 P.M.). Details can be seen on www.mungeruniversity.ac.in

Sd/- Registrar

Munger University, Munger

Fig. 15.3 Advertisement of Munger University, Bihar. (Source – Official website of Munger University)

- In fact, a day after the Finance Minister, Nirmala Sitharaman, tweeted her appreciation for public feedback ahead of the full Union Budget, the government put a link to its open forum, inviting more ideas and suggestions (NDTV, 2019).

- After joining hands with Internet of Things, the concept of crowdsourcing has emerged as an important innovation. This mind-blowing innovation has proved to be very useful for mankind. Combination of IOT and crowdsourcing has emerged as entirely new concept, known as crowd sensing.

15.6 Crowd Sensing

The technological revolution is transforming the concept of crowdsourcing into crowd sensing. Crowd sensing is a mix of crowdsourcing and emerging information technology in which the crowd is not asked to contribute data to solve a given problem. In fact, smart devices of the people (crowd) sense the data from its surroundings and share it with the central repository, which is used to take smart decisions. The technology of Internet of things (IoT), prediction applications, mobile phone apps and Internet based social media applications can be considered as the roots which enable crowd sensing.

The term crowd sensing emerged from the existence of sensors. Crowd sensing is also known as 'mobile crowd sensing'. It is used in three major areas:

- Monitoring the environment, monitoring air pollution level, air temperature etc.
- Monitoring the infrastructure, locating potholes
- Monitoring social activities, tracking health data within a community

Smartphones have become an integral part of our lives. The sensors embedded in smartphones observe several occurrences from our surroundings. People can be

considered as social sensors. The observations gathered from people can be used in various ways. For example, social media can be used to publish disaster related observations. Such data has already been used for early detection of disasters that can be used for decision making, as well as, for the situation awareness during disaster events. For example -

(i) **Recruitment 4.0 - TimesJobs.com Survey**

While factories are implementing Industry 4.0, consumers are hoping for 5G spectrum by the end of 2019, recruitment industry also moves to Recruitment 4.0. It is predicted that Recruitment 4.0 will be the beginning of an end for recruitment agencies. Technology will take over the typical recruitment business.

Recruitment 1.0 and 2.0 essentially focused on the active job seeker and traditional ways of hiring, recruitment 3.0 progressed to social media. Recruitment 4.0 will go a step further and focus on making the most out of the emerging trends of information technology and networking opportunities available online and offline.

Crowdsourcing adds benefit to Recruitment 4.0 to make it more efficient. Traditionally, for the process of recruitment, an organization would simply advertise a position opening and wait for candidates to come forward and apply for the vacancy. Now, with the current technology, recruiters will be able to find the best profiles themselves among the jobseekers and those who are already employed. These individuals try to gain visibility and present themselves to the organization they would wish to work for. It was possible due to the existence of the technology of crowd sensing. Mobile crowd sensing is an emerging technology with the help of which a recruiter can recruit a group of a mobile users via a platform and coordinate with them to perform some sensing tasks by using their smart phones or tabs.

A TimesJobs.com survey revealed that nearly 57% of the surveyed employers in Kolkata used crowd sensing for recruitment purposes. More than 60% of the organizations which have already used crowd sensing for HR functions, were highly satisfied, revealed the TimesJobs.com study. Also, more than 60% of the surveyed employers count, increased efficiency and cost-effectiveness as the key benefits of crowdsourcing.

(ii) **UIDAI Ecosystem - Aadhaar Card**

Unique Identification Authority of India (UIDAI), created by government of India, built an identity platform for people residing in India, known as Aadhaar which is biometric based identity database and authentication system. Smart phones and other smart devices can collect biometric information of individuals that can be used to connect to Aadhaar to authenticate the individuals' identities for crowd sensing applications in smart cities. It is an excellent example which shows the application for an integrated working of information technologies and processes of government of India through crowd sensing.

15.7 Industry Initiatives

There are few initiatives that are being taken up by the industry for adopting the latest technology for a better future. To transform their businesses many Indian industries are deploying emerging technologies like IOT, Cloud computing, AI etc. Few of such initiatives are discussed as follows -

- Vodafone Business Services provides smart IoT solutions in healthcare industry, in the form of Diabetacare's smart glucometers.
- India is prepared to face global competition by undertaking the 'Make in India' programme.
- As per, the Indian Brand Equity Foundation, the Government of India is planning to increase the contribution of manufacturing sector to 25% of GDP by 2025, which is currently at16%.
- India's first Smart factory is being set up at Indian Institute of Science's (IISc) Centre for Product Design and Manufacturing, Bengaluru which will be powered by data exchange in manufacturing and the Internet of Things (IoT).
- Andhra Pradesh government aims to turn the state into an Internet of Things (IoT) hub by 2020. The state government plans to set up 10 IoT hubs with the participation of the private sector which will create 50,000 direct employment opportunities in various IoT verticals.

15.7.1 Challenges Faced by the Industry

Although India is welcoming industry 4.0 with both the hands, industries are facing few challenges in deploying the emerging technologies and business ideas. The challenges are as below –

1. **Crowdsourcing issues**

   If any organization plans to launch a crowdsourcing campaign, suggestions shared by the stakeholders must be given proper care and all the decisions should be transparent for them as well. The organizations need to be ready for receiving funny and weird suggestions too. There are few examples of such organizations which faced negative impacts of crowdsourcing.

   (a) 'Henkel', a washing powder manufacturer faced an unsuccessful crowdsourcing campaign in 2011 as it tried to create a new design for the dishwasher liquid 'Pril'.
   (b) The crowd suggested weird names for a drink launched by 'Mountain Dew' and the company had to choose the name of the drink on its own due to which there was aggression among the people who had suggested the options.
   (c) There is no guarantee that the ideas given by the crowd are free from plagiarism. In such cases, organizations may face copyright issues later.

2. **Privacy issues**

   Since smart devices are capable of collecting, storing and transmitting personal data even without the person's conscious knowledge, privacy issues have become highly complicated and extremely crucial.

3. **Issues with digital system and infrastructure**

While implementing IOT, the industry may face the following issues -

(a) A much more powerful bandwidth is required in the industry for fast and heavy communication for transferring high volume of data.

(b) It is a challenge to incorporate diverse data repositories with different semantics for advanced data analytics. Data analytics is the need of hour because IOT will generate a lot of data.

(c) With the increased connectivity and use of standard communication protocols there is a big threat to cyber security systems. Around 60% of the organizations in India face operational disruptions due to cyber security breaches.

(d) Mobile crowd sensing comes with a challenge in privacy issues. Crowd sensing users are typically concerned that their personal information can be leaked from the collected data. There is a lack of skills and competencies in the technical workforce.

IOT and crowdsourcing make it possible to preserve India's edge in manufacturing and create a sustainable ecosystem with technically qualified employees which supports energy transition and can adapt to innovation and mass customization. Crowd sensing will add a pinch of salt in it and create an environment of convenient data collection through smart devices.

15.8 Conclusion

The chapter mainly focused on the concept of crowd sourcing, Internet of Things and crowd sensing which allow smart, efficient, effective, individualized and customized business processes and new product development at reasonable cost. After the conceptual introduction, classification of crowdsourcing is thoroughly explained with the help of such examples of products and services which are easily available in Indian market and can be observed by the readers easily. Specific examples of crowd sourcing in India have been chosen for easy understanding of impact of IOT technology over crowdsourcing.

The emergence of crowd sensing due to emerging technologies and existence of smart devices is explained in the next part of the chapter. Various benefits of crowd sensing are explained through examples like, Recruitments 4.0 and UIDAI Ecosystem.

The chapter also explained few facts and initiatives taken by industries to transform their businesses by deploying emerging technologies like IOT, Cloud

computing, AI etc. The presence of emerging technologies has also created challenges for the industries due to entire transformation of business processes. Issues with privacy, limitations of digital infrastructure, and emerging technology are discussed at the end of the chapter.

References

Alam, M., Shakil, K. A, Javed, M. S., Ansari, M., & Ambreen. (2014, July 2–4). Detect and filter traffic attack through cloud trace back and neural network. Imperial College, London, UK. *The 2014 International Conference of Data Mining and Knowledge Engineering (ICDMKE)*.

Alsheikh, M. A., Jiao, Y., Niyato, D., Wang, P., Leong, D., & Han, Z. (2017). The accuracy-privacy trade-off, of mobile crowd sensing. *IEEE Communications Magazine, 55*(6), 132–139.

APOSTROF. (2018). *Focus on recruitment 4.0*. https://www.apostrof.international/2018/01/focus-recruitment-4-0/

Brabham, D. C. (2008). Crowdsourcing as a model for problem solving. *Convergence: The International Journal of Research into New Media Technologies, 14*, 75–90.

Business Standard. (2017). https://www.business-standard.com/article/companies/govt-goes-silicon-valley-way-to-crowdsource-solutions-117040100973_1.html

Business Today. (2018). https://www.businesstoday.in/current/economy-politics/why-implementing-industry-4-is-becoming-an-imperative/story/286721.html

Campaign India. (2010). https://www.campaignindia.in/article/crowdsourcing-result-lays-launches-four-consumer-co-created-flavours/411983

Chandra, A., Sharma, V., Kumaraguru, P., & Kesharwani, S. (2009). Psychoanalysis of privacy policies of E-Commerce & BPO websites in Indian circumstances. *Global Journal of Enterprise Information System, 1*(1), 1–9.

Changing Government Through Crowdsourcing. (2018). https://crowdsourcingweek.com/blog/changing-government-through-crowdsourcing/

Charalabidis, Y., Loukis, E. N., Androutsopoulou, A., Karkaletsis, V., & Triantafillou, A. (2014). Passive crowdsourcing in government using social media. *Transforming Government: People, Process and Policy, 8*(2), 283–308.

CIOL Bureau. (2017). *7 digital innovations that changed the fortunes of Domino's Pizza*. https://www.ciol.com/7-digital-innovations-that-changed-the-fortunes-of-dominos-pizza/

Estellés-Arolas, E., & González-Ladrón-de-Guevara, F. (2012). Towards an integrated crowdsourcing definition. *Journal of Information Science, 38*(2), 189–200.

ET Bureau. (2013). *How 'crowdsourcing' can aid in stimulating a new point of view for brands*. //economictimes.indiatimes.com/articleshow/21935254.cms?from=mdr&utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

Exchange4media. (2013). *Is India ready for crowdsourcing?* https://www.exchange4media.com/advertising-news/is-india-ready-for-crowdsourcing-51057.html

Ganti, R. K., Ye, F., & Lei, H. (2011). Mobile crowdsensing: Current state and future challenges. *IEEE Communications Magazine, 49*(11), 32–39.

Geissbauer, R., Vedso, J., & Schrauf, S. (2016). *Industry 4.0: Building the digital enterprise*. Retrieved from PwC Website: https://www.pwc.com/gx/en/industries/industries-4.0/landing-page/industry-4.0-building-your-digital-enterprise-april-2016. pdf

Han, S., Huang, H., Luo, Z., & Foropon, C. (2018). Harnessing the power of crowdsourcing and internet of things in disaster response. *Annals of Operations Research*, 1–16.

Hopkins, M. M., Tidd, J., Nightingale, P., & Miller, R. (2011). Generative and degenerative interactions: Positive and negative dynamics of open, user-centric innovation in technology and engineering consultancies. *R&D Management, 41*(1), 44–60.

Howe, J. (2006). The rise of crowdsourcing. *Wired Magazine, 14*(6), 1–4.

Ikediego, H. O. et.al. *Crowd-sourcing* (Who, why and what). www.emeraldinsight.com/2398-7294.htm

Innovation Insights. https://stephenshapiro.com/types-of-crowdsourcing/Want, R. (2006). An introduction to RFID technology. *IEEE Pervasive Computing*, *5*, 25–33.

Khan, I., Naqvi, S. K., & Alam, M. (2015) Data model for big data in cloud environment. *Computing for Sustainable Global Development (INDIACom), 2015 2nd International conference* on, 11–13 March 2015, pp. 582–585. ISBN: 978-9-3805-4415-1, New Delhi, India, IEEE.

Khan, S., Liub, X., Shakil, K. A., & Alam, M. (2017a). A survey on scholarly data: From big data perspective, Information Processing & Management, *53*(4), 923–944, ISSN: 0306-4573, Elsevier.

Khan, S., Shakil, K. A., & Alam, M. (2017b). Big data computing using cloud-based technologies: Challenges and future perspectives. In M. Elkhodr, Q. F. Hassan, & S. Shahrestani (Eds.), *Networks of the future: Architectures, technologies and implementations* (Book series: Computer and information science series). Boca Raton: Chapman and Hall/CRC Press. Book ISBN – 9781498783972. [Scopus].

Khanna, L., Singh, S. N., & Alam, M. (2016) Educational data mining and its role in determining factors affecting students academic performance: A systematic review, India. *International conference on information processing, IICIP 2016 – Proceedings*, 7975354.

Lee, J. Y., Lin, W. C., & Huang, Y. H. (2014, May). A lightweight authentication protocol for internet of things. In *2014 International Symposium on Next-Generation Electronics (ISNE)* (pp. 1–2). IEEE.

MyGov, Mann Ki Baat. https://www.mygov.in/

Navya, A. et al. (2018). Electronic voting machine based on Blockchain technology and Aadhaar verification. *International Journal of Advance Research, Ideas and Innovations in Technology*. https://www.ijariit.com/manuscripts/v4i2/V4I2-1500.pdf

NDTV. (2019). https://www.ndtv.com/india-news/crowdsourcing-budget-2019-centre-seeks-ideas-suggestions-via-open-forum-2049804

Oliveira, E., Orrù, D., Morreale, L., Nascimento, T., & Bonarini, A. (2018). Learning and mining player motion profiles in physically interactive Robogames. *Future Internet, 10*(3), 22.

Palacios, M., Martinez-Corral, A., Nisar, A., & Grijalvo, M. (2016). Crowdsourcing and organizational forms: Emerging trends and research implications. *Journal of Business Research, 69*(5), 1834–1839. https://doi.org/10.1016/j.jbusres.2015.10.065.

Paniagua, J. et al. (2017). *Social media crowdsourcing*. https://www.researchgate.net/publication/316996005

Pénin, J., Hussler, C., & Burger-Helmchen, T. (2011). New shapes and new stakes: A portrait of open innovation as a promising phenomenon. *Journal of Innovation Economics Management, 1*, 11–29.

Piller, F., Reichwald, R., & Ihl, C. (2007). Interaktive Wertschöpfung – Produktion nach Open-Source-Prinzipien. In: Bernd Lutter-beck/Matthias Bärwolff/Robert A. Ge-hring (Eds.), *Open Source Handbuch 2007*. Zwischen Freier Software und Gesellschaftsmodell (S. 87–102). Berlin: Lehmanns Media. http://www.opensourcejahrbuch.de

Power, R., Robinson, B., & Ratcliffe, D. Finding fires with twitter. In Australasian language technology Association Workshop, Vol. 80, pp. 80–89.

Roitman, H., Mamou, J., Mehta, S., Satt, A., & Subramaniam, L. V. (2012). *Harnessing the crowds for smart city sensing*. New York: ACM.

Rüßmann, M., Lorenz, M., Gerbert, P., & Waldner, M. (2015, April 9). *Industry 4.0: The future of productivity and growth in manufacturing industries*, pp. 1–14.

Santos, B. P., Charrua-Santos, F., & Lima, T. M. (2018). *Industry 4.0: An overview*. In *Proceedings of the World Congress on engineering*, Vol. 2.

Sarmah, B., & Rahman, Z. (2017). Transforming jewellery designing: Empowering customers through crowdsourcing in India. *Global Business Review, 18*(5), 1325–1344.

Shepherd, H. (2012). Crowdsourcing. *Contexts, 11*(2), 10–11.

The Logical Indian. (2018). https://thelogicalindian.com/opinion/blockchain-elections/

The Wall Street Journal. (2015). *Crowdsourcing helps Domino's Pizza serve up rise in profit*. https://www.wsj.com/articles/crowdsourcing-helps-dominos-pizza-serve-up-rise-in-profit-1423634443

Thoben, K. D., Wiesner, S., & Wuest, T. (2017). Industrie 4.0 and smart manufacturing – A review of research issues and application examples. *International Journal of Automation and Technology, 11*(1), 4–16.

UNIDO. (2018). https://www.unido.org/sites/default/files/files/2018-11/UNIDO_GC17_Industry40.pdf

Vaidya, S., Ambad, P., & Bhosle, S. (2018). Industry 4.0 – A glimpse. *Procedia Manufacturing, 20*, 233–238.

Valdeza, A. C., Braunera, P., & Schaara, A. K. (2015, August 9–14). Reducing complexity with simplicity – Usability methods for industry 4.0. In *Proceedings 19th triennial congress of the IEA*, Melbourne.

Vinay, N., et al. (2011). Towards an integrated model for academia-industry Interface in India. *International Journal of Humanities and Social Sciences, 1*, 280–289.

Wang, S., Wan, J., Li, D., & Zhang, C. (2016) Implementing smart factory of industrie 4.0: An outlook. *International Journal of Distributed Sensor Networks, 2016*, 1–10, Article ID 3159805.

Yin, J., Lampert, A., Cameron, M., Robinson, B., & Power, R. (2012). Using social media to enhance emergency situation awareness. *IEEE Intelligent Systems, 6*, 52–59.

Chapter 16
Smart Infrastructures

Zameer Fatima, Lakshita Bhargava, and Alok Kumar

Abstract Internet of things (IOT) is an emerging branch in computer science, which is finding widespread application in a large number of places. In this chapter we will discuss how Internet of things can be used to make infrastructures like home and cities smart. In building infrastructures like smart home and smart cities IOT can be used extensively to achieve automation. Smart home is an Infrastructure in which various electronic devices can communicate with each other and achieve a certain level of automation. Internet of things can be used to achieve this automation in homes using a centralized internet network, sensors and identifiers (like RFID tags etc). An even better implementation of IOT can be done by adding a system to collect and analyse the data generated by sensors on a regular interval and hence improve the performance of overall system. Unlike home which is just a single unit, a city is a collection of many small infrastructures like smart lighting which can automatically adjust its illumination based on the lighting conditions, connected streets which helps in reducing traffic and improve mobility within the city, smart parking management to provide hassle free parking etc. All these infrastructures can be implemented using Internet of things.

Keywords IOT · Automation · RFID · Smart city · Smart home · Smart lighting · Smart parking

16.1 Introduction

Our world in the last decade have seen a rapid advancement in industrialization, technology and medication. All these factors combined together have made our life much easier and sustainable. Because of high sustainability and low death rates achieved through technology and development in the last decade, there has been an

Z. Fatima (✉) · L. Bhargava · A. Kumar
Computer Science & Engineering Department, Maharaja Agrasen Institute of Technology, Guru Gobind Singh Indraprastha University, New Delhi, Delhi, India

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_16

immense growth in population worldwide. The need of infrastructure which can sustain this huge population and provide a judicious use of our limited resources have never been felt more strongly than now. The answer for designing and maintaining such kind of infrastructures can come in the form of smart cities and smart homes. In this chapter of the book we will focus our study on these two smart infrastructures. Although smart home is a subset of smart city still it needs to be studied separately because of its independence from smart city. Hearing the term smart infrastructures makes most of us think as an infrastructure which is intelligent and highly automated. In reality a smart infrastructure is not just about automation. Automation and artificial intelligence can be used to make an infrastructure smart but it is not what exactly a smart infrastructure is. In simple terms a smart infrastructure is an infrastructure which can provide sustainable growth and development that could fuel a high quality of life and better resource management. In technical terms smart infrastructure is an infrastructure which is a collection of various sub infrastructure connected together so that they can share information among themselves and use the data generated in the process to take intelligent decisions by themselves without any or much human intervention. In case of smart homes these sub infrastructure can be smart rooms which itself can have micro infrastructures like smart lighting, smart tv, smart meters etc. In case of smart cities smart homes itself is a micro infrastructure along with other micro infrastructures like smart parking, smart traffic management etc. Smart cities and smart home have become a big trend in the past few years. Many big cities in the world like London, New York, Paris, etc. have adopted the concept of smart cities and many others are in the process of adoption. Internet of things(IOT) can be used to achieve this communication between sub infrastructures. Internet of things work by connecting all sub infrastructures together and to the internet by using connection protocols. This enables exchange of information and communication between subsystems which helps in achieving intelligent recognition, monitoring and management.

This chapter is divided into two sections. In the first section of the chapter we will focus our discussion on smart city, whereas the second section is focused on smart home followed by a conclusion section containing the essence of the whole chapter.

16.2 Smart City

A smart city is an infrastructure which uses different types of sensors to collect data and process that data to manage assets and utilize resources in such a way that there is minimum amount of wastage. A smart city usually serve two purposes:

1. To provide a way for optimal utilization of resources.
2. To provide a high standard of life to individuals who are the resident of that city

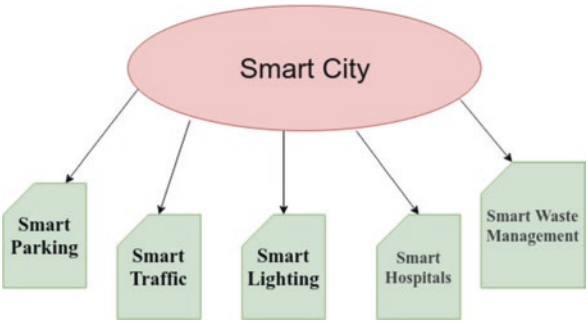


Fig. 16.1 Components of smart city

16.2.1 Components of smart city

As discussed in the introduction section of the chapter smart city is not a standalone infrastructure but rather a collection of many sub infrastructure. In this section we will discuss some of the sub infrastructure which together forms the backbone of any smart city. The components of smart city is given in Fig. 16.1.

16.2.1.1 Smart Parking

The outburst in the number of vehicles in the past couple of years has given rise to two major problems in urban areas, traffic congestion and unavailability of parking space. In highly developed cities with large number of population driver's often find it very difficult to find a parking spot especially during peak hours. A possible solution to this problem can be achieved through smart parking. A smart parking is an infrastructure that uses various technologies to manage the parking system in the efficient and hassle free manner. Smart parking system can be classified into various subsystems like parking guidance and information system (PGIS), transit based information system, smart payment system, E-parking and automated parking system. Each of these systems uses different kind of implementation to detect the presence of the car in the parking lot. In some implementations there is a system for continuous recording of videos which is processed to determine if the status of car slots in parking stations. The author in (Mago 2017; Saxena et al. 2018a) has discussed a computer vision based implementation of a smart parking system. In some implementations data sent from sensors is collected and processed to find if a particular slot is empty or not. This kind of implementation uses IOT for processing and analysing of data. Author in (Patil and Bhonge 2013) present a similar kind of implementation in which data from the wireless sensor network is used which allows vehicle drivers to find free parking space in the parking lot. This model is based on WSNs, Embedded Web-Server, Central. Web-Server and Mobile phone application.

In this model sensor node of each parking slot sends data to the embedded web server in the parking station. This real time data is analyzed to find the cur-

rent location of the parking slot, then this information is sent to the central web server from where application in the driver's mobile device pulls the information. Sensors used in such implementations are broadly of two types, intrusive and non-intrusive sensors. Intrusive sensors are sensors which are installed by tunneling under the road surface. Installation and replacement of such kind of sensors are difficult and costly. Some examples of intrusive sensors are Active Infrared sensors, Inductive loops etc. Unlike Intrusive sensors non-intrusive sensors can be easily installed and maintained as they don't require any modification in surface of infrastructure of the place in which they are installed. Some examples of non-intrusive sensors are RFID, Infrared sensors etc. Figure 16.2 shows the smart parking architecture.

16.2.1.2 Smart Traffic

One of the another bi product of outburst in the number of vehicles over the last couple of years is heavy increase in traffic density which has led to congestion on roads in urban areas. Traffic congestion is a problem that is not limited to a particular

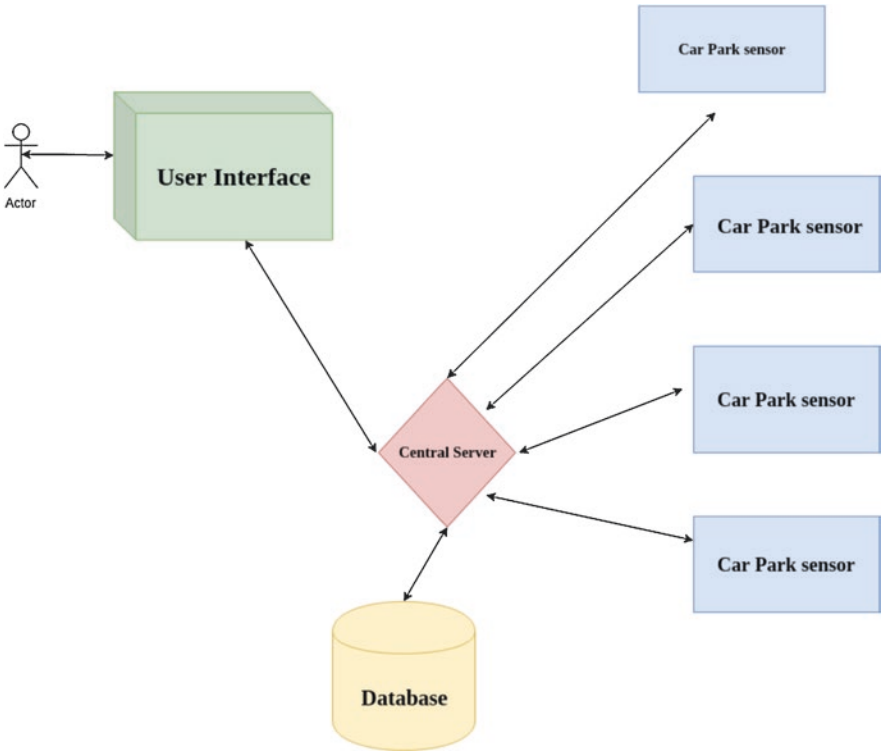


Fig. 16.2 Smart parking architecture

city or country but it has become a global issue. All the developed and developing countries are failing miserably in handling the large volume of ever growing traffic throughout the world. Many cities have tried to solve this problem by expanding their infrastructure which includes building wide roads, over bridges etc. But building new infrastructure for traffic management comes with quite a few challenges of its own. Demolition of old infrastructure and construction of new one requires a lot of capital. Also as most of the cities were built a long time ago so they don't have much scope of expansion. Even for cities that took the approach of constructing new infrastructures it became clear after some period of time that rate of construction of new infrastructures can't keep up with the rate at which traffic density is increasing overtime. So now it has more or less become evident worldwide that constructing new infrastructures can't be the only solution for traffic management. For managing the ever increasing volume of traffic we need a combination of new physical infrastructure and smart technologies which can help us in utilizing the full capacity of these infrastructures. Smart traffic system generally uses some kind of advanced technology like computer vision, image processing, artificial intelligence, internet of things and much more (Saxena et al. 2018b).

The Need for Smart Traffic Systems

All though it is quite clear that to handle this huge volume of traffic we need some kind of traffic management system. But don't we already have traffic management system? Yes we do and most of us are quite familiar with it in the form of traffic lights. Traffic lights are highly robust and time tested system which are in use of traffic management for the last 100 years. So, the question is why do we need a new and smart traffic system now? To answer this question we will need to look at the weakness of our current traffic management system. Most common and widespread system for traffic management is static traffic lighting system. The flaw of this system lies in its name only. As it is static, which means that the traffic light's time and its switching pattern is predetermined irrespective of the lane or time of the day. In simple terms it means that the conventional traffic light based management system doesn't take into account for the real time data. Because of this the system becomes inefficient in handling large volume of traffic. The solution to this problem is to implement a smart traffic system which takes into account for the real time traffic data.

IOT Based Smart Traffic System

Author in (Janahan et al. 2018) discuss a IOT based smart traffic management system. This system uses the count in number of vehicles in a lane using infrared sensor. The vehicle count data is sent to a server. The server implements some artificial intelligence algorithm like KNN on the dataset to find an optimized time slot for that particular. This time slot is sent to the microcontroller which is present in the

traffic light. This microcontroller uses the time slot data received from the server to control the duration of switching time of traffic light. Vehicles logs are saved in a database so that they can be analyzed to predict on factors like pollution level. This analysis helps in taking adequate measures to control the pollution level. This implementation of smart traffic management system is much cheaper than computer vision implementation as it doesn't require installation of high definition expensive video cameras (Jabarullah et al. 2012). Also as there is no image processing involved so this IOT based method is very fast and needs less computational power compared to computer vision based approach. The basic architecture of this model is shown in Fig. 16.3.

Smart Lighting

Street lights are one of the most important infrastructure of a city. In urban areas, many of the residents have late night jobs which means that the city needs to be awake and functioning even at night. So, in urban areas street light is a must thing. The normal street light that is most commonly in use at present doesn't manage the intensity automatically which means that they need to be switched on and off manually using some kind of switches. Because of this manual control of intensity there is a huge wastage of power. To stop this wastage of electricity some kind of smart implementation of street lights need to be done in which the lights can turn itself on or off by sensing the presence of sunlight and any nearby object. Such kind of smart

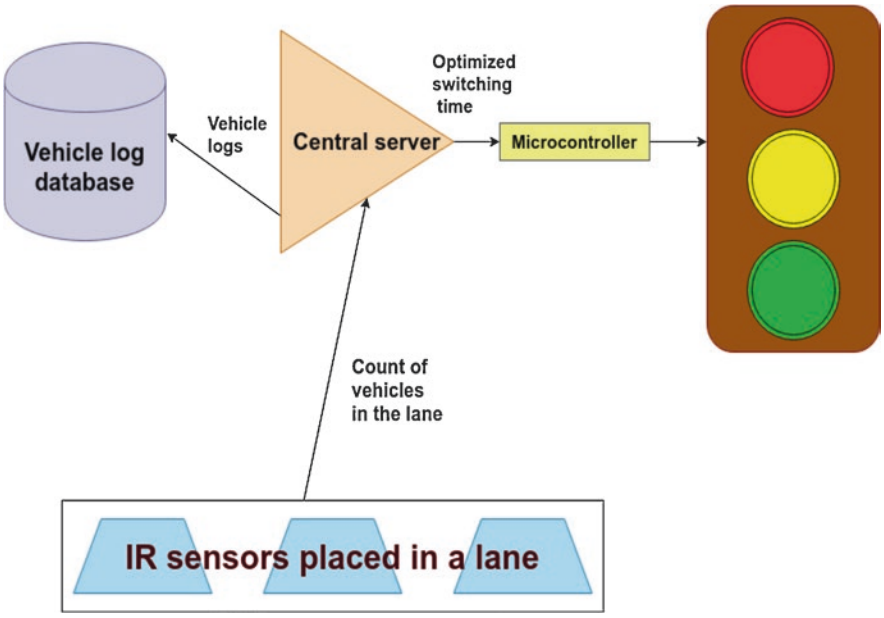


Fig. 16.3 Smart traffic control system architecture

implementation is possible using IOT. Author in (Tambare et al. 2016) proposes an implementation in which street light will turn itself on at night and off at day time. Also it can control and change its intensity by sensing the presence of any nearby object.

The intelligent street light system consists of IR sensors, LDR, microcontroller, relays, Wifi Module. The LDR (Light dependent resistors) is a component which have variable resistance when light falls on it the resistance of LDR becomes very low which in turn causes the relay to turn off and hence street light remains off during the day time. At night time when the resistance of LDR becomes high because of absence of sunlight relays inside the street light turns on and hence the street light turns own at night time. For controlling the intensity of light based on the presence or absence of any object nearby IR sensors are used. These sensors have the ability to detect the presence of an object using infrared light this information is sent to the microcontroller which uses this data to control the intensity of the light. A wifi module is also present in the street light which sends necessary data to the cloud so that proper monitoring of the street light can be done (Alam and Shakil 2013a). Smart street lighting system architecture is shown in Fig. 16.4.

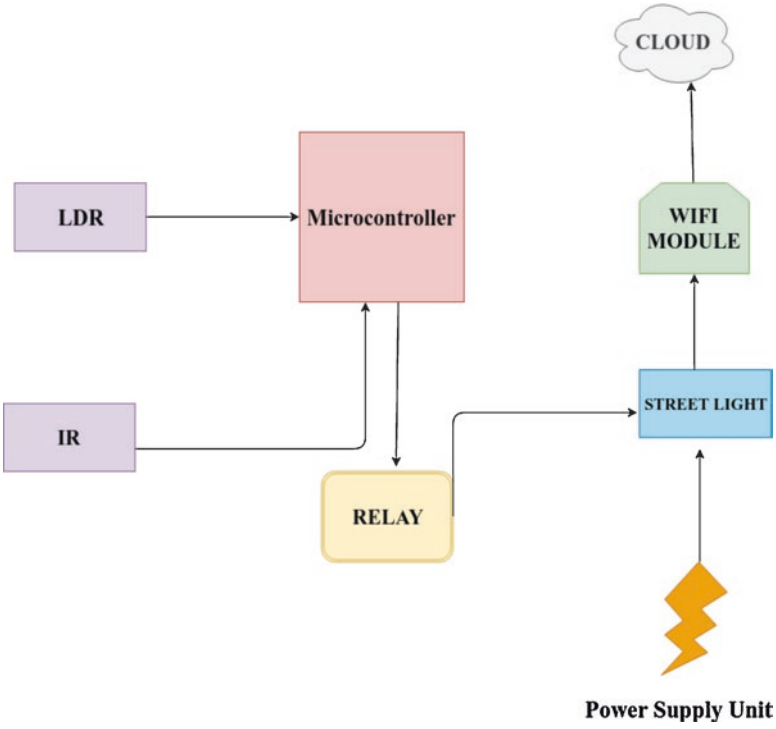


Fig. 16.4 Smart street lighting system architecture

Advantages of smart street light over conventional system:

- Automatic switching reduces manpower wastage
- Reduces wastage of power
- Cost efficient in the long run
- Much more convenient to use and operate
- Much more reliable than conventional system

Limitation of smart street lighting system:

- High initial setup cost
- Complicated architecture hence difficult to implement
- If something breaks then it is costly and difficult to repair the system

Smart Hospitals

Hospitals are one of the most important infrastructure of any city. Good hospitals are a must for maintaining a healthy and hygienic lifestyle for the residents of the city. Hospitals have a large number of patients who are undergoing different kinds of treatment at any particular time. To monitor the health and hygiene of this large patient pool is a very difficult task. Any error or negligence if occur in process of monitoring can cause very adverse effect on the life of patients. This also has an adverse effect on their time of recovery. Also staff working in hospital like nurses and doctors sometimes themselves gets affected because of frequent visit that they have to make in patient wards. The regular manual monitoring of patient's health also increases work load on hospital staff affecting their quality of work. Apart from this hospitals also uses a lot of heavy electrical appliances which often remain switched on even when not in use. This causes wastage of power and reduces the effective life of appliances. A possible solution for this can come in the form of building a real time automated monitoring and alarming system for patient health. Author in (Sonawdekar et al. 2018) have proposed an IOT based model. This model consists of a microcontroller with some sensors such as temperature sensor, sweat sensor, heart beat sensor, IR sensor, LDR sensor. Temperature sensor, sweat sensor and heart beat sensor are placed on the patient's body and are used for real time monitoring of patient healthcare. IR sensor is used for security purpose. Using infrared signals it can detect someone's presence in the patient's room. LDR sensor is used for automatically turning on and off the room light based on the time of the day. The data from all these sensors are sent to IOT server. Health supervisor assigned to the patient can monitor this data and use the analysis to take necessary measures. Data of the patients collected by the hospitals in their IOT server can also be stored in some kind of database. This data can be used in medical research. Also if a patient comes for treatment again, hospitals can use their previous records to provide a better and more personalized health care to the patients. Smart hospital architecture is shown in Fig. 16.5.

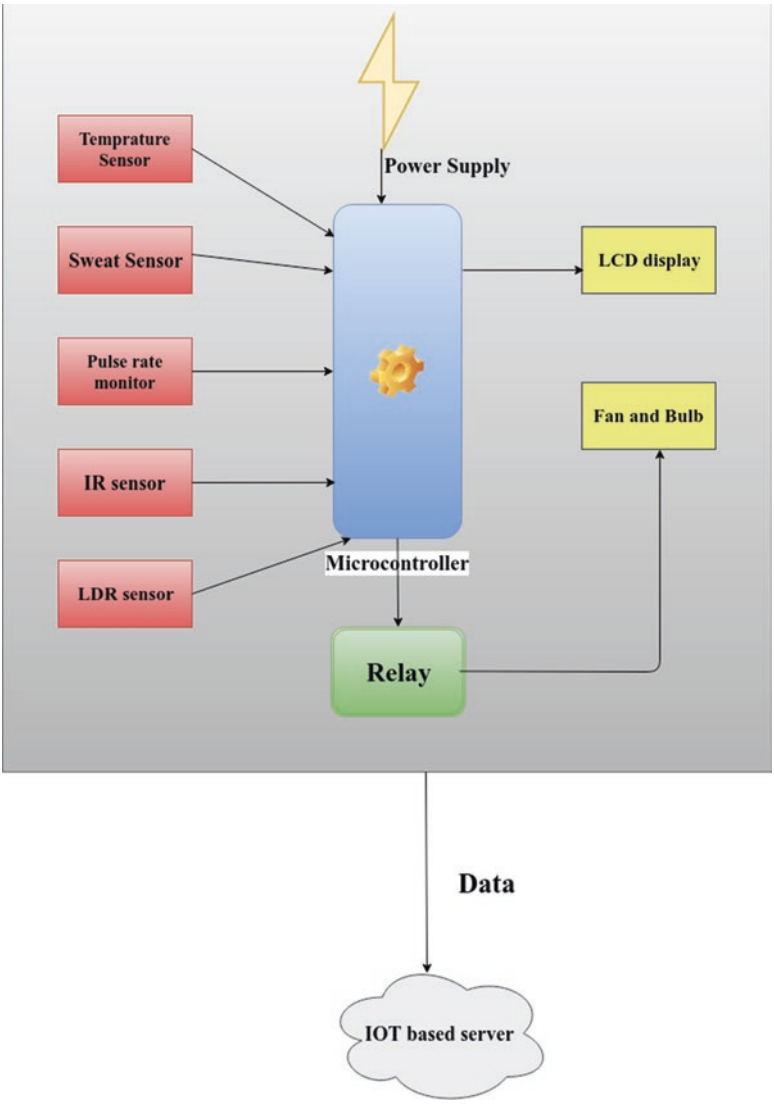


Fig. 16.5 Smart hospital architecture

Smart Waste Disposal

Today, all major developed and developing cities are facing the problem of implementing the system of waste disposal without making the city unclean. For the government waste disposal has become a behemoth task. A proper waste management system requires a huge infrastructure. Such kind of infrastructure requires large amounts of manpower and funds. Most of the developing and underdeveloped

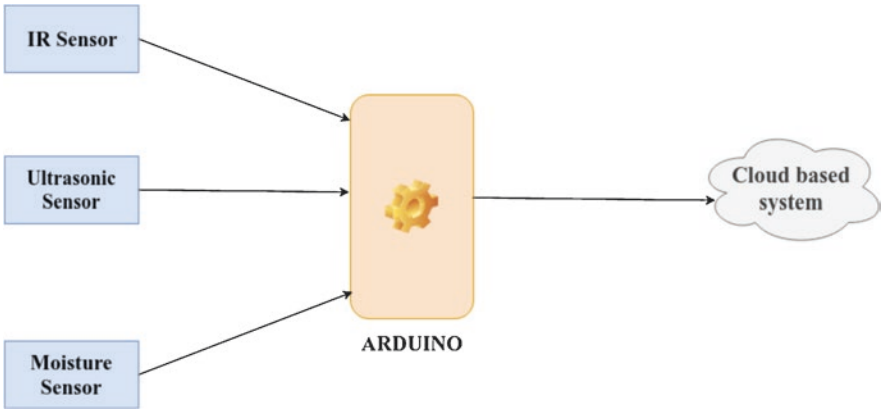


Fig. 16.6 Smart waste management system architecture

cities lack such kind of infrastructure and which causes of improper disposal of wastes. Improper waste management causes piling of garbage within the city which makes city unclean and unhygienic. Developed cities which do implement proper infrastructure for waste disposal have to pay a staggering amount of money to do so. Recent reports have shown that highly developed cities like New York spends billions of dollars to manage their waste. Hence there is an utmost need for having a waste management system which is reliable, easy to implement and cost efficient.

IOT Based Smart Waste Disposal System

IOT can be used to provide a solution for smart waste management system. This system consists of IR sensors, moisture detection system, ultrasonic sensor and an ARDUINO. Ultrasonic sensor is used to check the level of garbage in the garbage container inside the dumpster. This information is sent to ARDUINO which passes the information to the cloud system (Alam and Alam 2013). After analyzing this data cloud based system takes the action that whether the container needs to be emptied or not (Alam et al. 2013a). Moisture sensor is used for separating the dry and wet wastes. IR sensor sends information about the surroundings and atmosphere of the dumpster which is sent to the cloud for proper analysis (Malhotra et al. 2018; Shakil et al. 2015). Smart waste management system architecture is shown in Fig. 16.6.

16.3 Smart Home

Home automation is making human life more comfortable by providing facility to control home appliances from anywhere whether the person is near or far away from the home. Internet of Things (IOT) helps in making a home smart by connecting

various appliances called things to a network through communication technologies such as WiFi, Zigbee, Bluetooth, GSM etc. together to control over all aspects of home. Home Automation includes maintaining room temperature, humidity, luminosity, switching on or off electrical appliances, keeping track of the amount of LPG in the cylinder, home security such as access control and alarm systems, measuring energy consumption, remote monitoring and accessing automated appliances. Automating home is just a touch of your fingertips on a mobile app to control the appliances remotely.

As shown in Fig. 16.7 the architecture of home automation consist of following components.

1. Sensors
2. Microcontroller
3. Communication technology
4. IoT Server
5. User Interface

1. Sensors: Sensors are required to check the parameters such as luminosity, room temperature, humidity, air quality (dust level, amount of CO2 emission), switching on/off electrical appliances, camera surveillance, measuring the amount of energy used during peak and non-peak hours, keeping track of the amount of LPG in the cylinder, home security such as access control and alarm systems. Large amount of data generated through these sensors is transmitted to IOT server through some communication technology such as WiFi, ZigBee, Bluetooth, and GSM.
2. Microcontroller: It is used for processing and managing the data which is collected from sensors. There are a number of different microcontroller such as Raspberry Pi, NodeMCU, Arduno etc.. Each microcontroller has its own pros

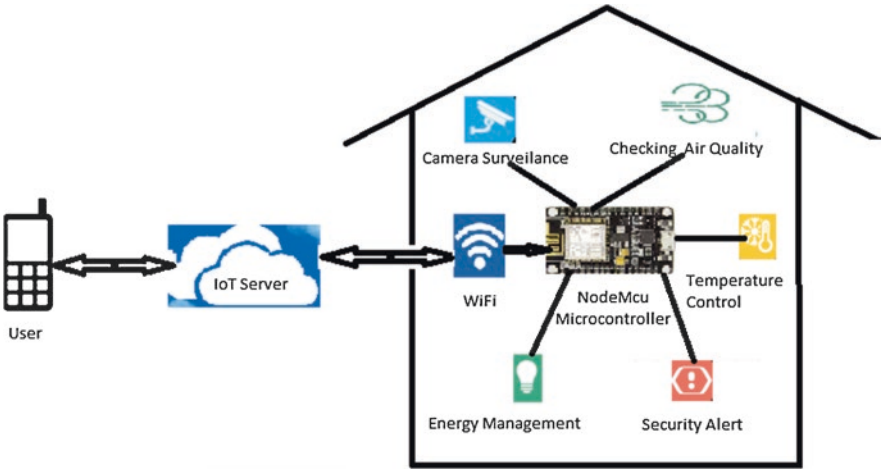


Fig. 16.7 Home automation architecture using IOT

and consequences. Raspberry Pi is a small single board computer. It is of credit card size having RAM, CPU, Ethernet port, USB Port which can be easily plugged in with screen and keyboard. Based on the different model of Raspberry Pi, Size of RAM can vary from 500 MB to 4 GB, cost range from $5 to $55. Main programming languages of Raspberry Pi are Python and Scratch. It also support other programming languages.

Arduino is a single-board microcontroller which is less powerful than Raspberry Pi and easier to handle, cheaper than Raspberry Pi (Gunge and Yalagi 2016). Arduino has a flash memory ranges from 8 KB to 256 KB, CPU speed ranges from 8 MHz to 400 MHz based on the different models. Arduino contains the web server application that communicates through the HTTP protocol with Web-based Android application. The system is highly flexible and scalable and expandable (Al-Kuwari and Ramadan 2018).

NodeMCU is a arduino based microcontroller with additional feature of ESP8266 WiFi chip with full TCP\IP Stack. Main Advantage of NodeMCU is that, it can directly connect to the internet without using any additional peripheral. One of the disadvantages of NodeMCU is that it can communicate or monitor with only one device because it has only one analog input. Although this disadvantage is overcome by using ASD115, which can convert 4 analog signals to digital signal (Singh et al. 2018).

3. Communication Technology: Data is Transmitted between sensors and microcontroller through various communication technology such as Bluetooth, ZigBee, WiFi, GSM, Dual Tone Multi Frequency (DTMF).
4. IoT Server: Entire data that is collected on microcontroller from sensors is uploaded on IoT server through Wifi.. Data size increases as the number of devices increases for making human life more comfortable through home automation. This large amount of data is handled by a server on cloud called IoT server (Shakil and Alam 2014).
5. User Interface: End User can control his/her home appliances remotely through the android based mobile App. For example if a person forgot to switch off his Air conditioner or any other appliances then he has to just open and click on his mobile app to switch off the air conditioner. This Mobile app will connect to the IoT server which in turn check the data on the microcontroller taken from sensors associated with each device to turn off the device.

16.3.1 Purpose of Home Automation

Home Automation is becoming a necessity with the fast moving life in urban areas. With the ever- evolving technology for making human life more comfortable and enhancing the standard of living, Home Automation is important. Following are the factors that makes Home Automation important.

Security: Now a days security of child at home is a major concern as both husband and wife are working and nobody is there to watch their child activity at home. With the use of webcam at home parents can keep track of their child's activity. Webcam will take note of all the activities of the children at home and parents can keep track of it remotely through their mobile phone (Alam and Sethi 2013; Alam et al. 2013b).

Saving Energy: Using home automation we can reduce the amount of energy wasted by managing each device in an energy efficient manner. Energy usage will be monitored by keeping track of which devices or appliances are consuming more energy during peak hours. Home automation system will automate each device in an optimal manner for example appliances such as washing machine and dishwasher during non-peak hours when the electricity is cheaper which is both time saving and money saving. A thermostat such as Nest can examine user behaviour pattern. It will turn off the air conditioner when user is outside the home and turn it on when the user is back home. Energy consumption can be reduced by auto scheduling of home appliances (Alam and Shakil 2013b).

Saving Water: user can get rebate in their water bill by adding sprinkler control home automation system which tells you how long the water runs through the mobile app.

16.4 Conclusion

In this chapter we have discussed on what smart infrastructures are and why we need them. We discussed on two most important infrastructures smart home and smart city. We have focused on their architecture why we need them and what purpose do they serve.

References

Alam, M., & Alam, B. (2013). Cloud query language for cloud database. In *Proceeding of the international conference on Recent Trends in Computing and Communication Engineering – RTCCE 2013*, Hamirpur, HP, pp 108–112, ISBN: 978-981-07-6184-4. https://doi.org/10.3850/978-981-07-6184-4_24.

Alam, M., & Sethi, S. (2013, January). Security risks & migration strategy for cloudsourcing: A government perspective. *International Journal of Engineering and Innovative Technology, 2*(7), 205–209. ISSN: 2277–3754, USA.

Alam, M., & Shakil, K. A. (2013a). Cloud Database Management System Architecture. *UACEE International Journal of Computer Science and its Applications, 3*(1), 27–31.

Alam, M., & Shakil, K. A. (2013b). A decision matrix and monitoring based framework for infrastructure. Performance enhancement in a cloud based environment. International Conference, Nov 08–09, 2013; Hyderabad: Elsevier.

Alam, B., Doja, M. N., Alam, M., & Malhotra, S. (2013a). 5-Layered Architecture of Cloud Database Management System. *AASRI Procedia Journal, 5*, 194–199. ISSN: 2212–6716, Elsevier.

Alam, B., Doja, M. N., Alam, M., & Malhotra, S. (2013b, September). *Security issues analysis for cloud computing, International Journal of Computer Science and Information Security, 11*(9), 117–125.

Al-Kuwari, M., & Ramadan, A. (2018). Smart-home automation using IoT-based sensing and monitoring platform. In *Proceeding of 12th international conference on compatibility, power electronics and power engineering (CPE-POWERENG 2018)*.

Gunge, V. S., & Yalagi, P. S. (2016). Smart home automation: A literature review. *International Journal of Computer Applications (0975–8887) National Seminar on Recent Trends in Data Mining (RTDM 2016)*.

Jabarullah, B. M., Saxena, S., Kennedy Babu, C. N., & Alam, M. (2012). Hybrid approach of face recognition, cyber times. *International Journal of Technology & Management, 6*(1), 6. October 2012 – March 2013, ISSN: 2278-7518.

Janahan, S. K., Murugappan, V., Arun, S., Kumar, N., Anandan, R., & Shaik, J. (2018). IoT based smart traffic signal monitoring system using vehicles counts. *International Journal of Engineering & Technology, 7*, 309. https://doi.org/10.14419/ijet.v7i2.21.12388.

Mago, N. (2017). Intelligent parking management system (PMS) based on video analytics. *International Journal of Advanced Research in Computer Science and Software Engineering., 7*, 142–147. https://doi.org/10.23956/ijarcsse/SV7I5/0254.

Malhotra, S., Doja, M. N., Alam, B., & Alam, M. (2018). Generalized query processing mechanism in cloud database management system. *Big Data Analytics*, Print ISBN: 978-981-10-6619-1, Electronic ISBN: 978-981-10-6620-7 (pp 641–648). Singapore: Springer.

Patil, M. S., & Bhonge, V. N. (2013). Wireless sensor network and RFID for smart parking system. *International Journal of Emerging Technology and Advanced Engineering, 3*, 188–192.

Saxena, S., Alam, M., & Jabarullah, B. M. (2018a, September). DS-HM model with DCT-HW features for face recognition. *International Journal of Scientific Research in Computer Science Applications and Management Studies, 7*(5). ISSN 2319–1953.

Saxena, S., Alam, M., & Jabarullah, B. M. (2018b, September). DS-HM model with DCT-HW features for face recognition. *International Journal of Scientific Research in Computer Science Applications and Management Studies, 7*(5). ISSN 2319 –1953.

Shakil, K. A., & Alam, M. (2014). Data management in cloud based environment using k-median clustering technique. *International Journal of Computer Applications (0975–8887), 3*, 8–13.

Shakil, K. A., Sethi, S., & Alam, M. (2015). An effective framework for managing university data using a cloud based environment. In *Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference* (pp. 1262–1266), IEEE.

Singh, H., Pallagani, V., Khandelwal, V. & Venkanna, U.. (2018). IoT based smart home automation system using sensors node. In *4th International Conference on Recent Advances in Information Technology* |RAIT-2018|

Sonawdekar, S., Katkar, G., Gaikwad, M., & Farhan, M. (2018, March). Smart Hospitals using IOT. *International Journal of Scientific & Engineering Research, 9*(3), 120.

Tambare, P., Venkatachalam, P., & Rajendra, D. (2016). Internet of things based intelligent street lighting system for smart city. *International Research Journal of Engineering and Technology, 5*(8). https://doi.org/10.15680/IJIRSET.2016.0505181.

Part V
IoT for Smart Cities

Chapter 17
IoT Application for Smart Cities Data Storage and Processing Based on Triangulation Method

Muzafer Saračević, Šemsudin Plojović, and Senad Bušatlić

Abstract This chapter presents the possibilities of applying the triangulation method in the IoT application for smart cities data storage and processing. The chapter includes a method in field of computational geometry (specifically polygon triangulation as a fundamental algorithm in computational geometry). The implementation of the application was done with two modules. Proposed first module has a storage function and collecting data in a smart city space, while the second module has a function of data processing and finding the minimum triangulation in the smart city space. The method is derived using triangulation and properties of Catalan numbers. The process of storing the coordinates of points using the Ballot method (walk on the integer lattice) is given. Due to its exceptional efficiency in terms of launching programs on various computer architectures and operating systems, Java programming language (Net Beans environment) enables an efficient implementation of our method. In experimental research, we tested a proposed solution based on the application of the triangulation method using the Ballot notation (for data storage) and minimal triangulation (for data processing).

Keywords Smart cities · IoT · Optimal triangulation · Data storage and processing · Java programming · GIS

M. Saračević (✉) · Š. Plojović
Department of Computer Sciences, University of Novi Pazar, Novi Pazar, Serbia
e-mail: muzafers@uninp.edu.rs; s.plojovic@uninp.edu.rs

S. Bušatlić
International University of Sarajevo, Sarajevo, Bosnia and Herzegovina
e-mail: sbusatlic@ius.edu.ba

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_17

17.1 Introduction

Navigating within smart cities is directly linked to sustainable, safe and efficient transport systems and infrastructure, such as their rejection at both local and national and international levels. So for a city to become smart, it is imperative that it innovates in transportation that will sustain it. These steps are used not only for the economy but also for the environment and provide a better quality of life for all citizens. Previous research and implementation of e-City services in the field of map usage and mapping uses GIS (*Geo-information Systems*) commercial solutions. Also, you can use Open Source GIS solutions as well as free Web Mapping Services, which in the last year have achieved the usable value of GIS commercial solutions, are overwhelming in a large segment. The possibility of combining GIS resources and free Web map services was explored, as well as presenting numerous information with external services within the projected maps, which enables a very rich presentation of the requested information. Research combining e-City services with the concept of creating "smart cities" (*Smart City*) is very current today. Superior analyzes and comparisons between GIS systems and free public ticketing services, towards finding the best solution for creating a centralized electronic service at the city level.

A modern technique for collecting data in the field is a system of terrestrial orbiting satellites that transmit precise weather signals to special electronic devices to record the position of an object on the ground. This system is referred to as "*The Global Positioning System (GPS)*". The receivers provide direct measurements of the position on the Earth's surface, with the location indicated by a standard system, using coordination using a triangle system. Triangulation is a process that is very important in computer geometry and graphics. Triangulation allows the representation of three-dimensional objects from a set of points. This process is very important for the speed, quality and resolution of the objects displayed. Polygon triangulation finds its application in geo-information systems as well as in the process of digital terrain modeling.

IoT-enabled smart city use cases span multiple areas: from contributing to a healthier environment and improving traffic to enhancing public safety and optimizing street lighting. Smart cities are servicing new digital technologies and are related to traffic management through smart traffic lights, parking space design, gathering information on their waste storage, rational use of refreshments, to build energy-efficient communications in the future with sufficient local government. All of these services involve reducing pollution, moving to cleanup transportation clean up and heating. The use of IoT (*Internet of Things*) traffic regulation is used to reduce costs and increase passenger satisfaction while reducing the number of traffic accidents. Future solutions will be based on main memory and environmentally sound vehicles and their connection to infrastructure facilities such as gas stations, parking lots, garages and the like. Wider use of advanced information technology, except vehicle communications with vehicle infrastructure, capability and communication.

IoT applications fot smart cities is just another solution that the modern age has to deal with the problems that are in line with achievements and to provide citizens with a healthy and safe lifestyle as it may have once been, or might even get better. Some examples of implementation of intelligent transport systems is: integrated traffic systems (traffic flow management, traffic lights, variable traffic messages, highway access control, speed checking, parking management, etc.), transportation management (traffic routing, incident management, identification of breaches, maintenance of transport infrastructure) and passenger information (providing information). Other appropriate sustainable transport practices that characterize smart cities may be linked to the introduction of an initiative such as car sharing, that is, the sharing of private passenger vehicles with the same final destination (using GIS and triangle methods).

The main motivation of this chapter is presents presents the possibilities of applying the triangulation method in the IoT application for smart cities. The chapter includes a method in field of computational geometry (specifically optimal polygon triangulation as a fundamental algorithm in computational geometry). The main contribution of this chapter is concrete solutions for storing and processing smart city data based on the optimal triangulation method.

This chapter consists of seven sections. In Sect. 17.2, similar research is presented in the field of the GIS technology in the realization of the concept of smart cities. In addition, similar research has been reported in the field of the main examples of triangles in the application of geo-information systems. In Sect. 17.3 of this chapter, some of the features of the Java NetBeans environment for working with data processing and storage are outlined. Section 17.4 describes the proposed method (first module) for storing and collecting data in a smart city space. In Sect. 17.5 has been presented the second module of the proposed method relating to data processing and finding minimum triangles in smart city space. Give specific examples of how to apply the proposed methods in a *Java NetBeans environment*. Sections 17.6 and 17.7 provides a discussion and concluding consideration.

17.2 Overview of Related Research

GIS offers user-friendly and advanced capabilities for smart city applications. The successful implementation of a smart city application requires the development of a system that can manage and visualize the geospatial data in a user-friendly environment. In paper (Yamamura et al. 2017) authors present a new method based on GIS for smart city planning. The research proposes a GIS based urban energy planning system and 3D visualization with a user-friendly interface. Authors in paper (Lella et al. 2017) discuss possible collection methods for waste management and presents methods for transportation of waste using GIS techniques through analysis of network.

Authors in paper (Cosido et al. 2013) construct a model for Smart City by using GIS techniques. Experimental results show that approach performs very well and that the presented methodology is promising for further application in other concrete scenarios. Paper (Tan and Wong 2006) presents applications for smart cities with concrete Google maps and GIS tools. The release of mapping API like Google maps has changed the way location systems work. Also, authors apply visualization tools as a study into the usefulness of functions of Google maps and GIS.

A multi-criteria GIS-based methodology for smart cities site selection presents in paper (Fashal et al. 2019). This research contributes to a site selection method that satisfies the decision maker's criteria. Layers corresponding to these criteria were built in GIS. In paper (Shahrour 2018) authors give concrete concept based on the use of geospatial data concerning the urban built environment and urban services. Authors show how a GIS could help in concrete implementation of smart city and describes its use in the construction of a model of the smart city. Also, authors in paper (Chen and He 2017) state that GIS plays a very important and fundamental role in supporting the smart city construction. This paper expounds the concrete model of the smart city construction with GIS technique.

The paper (Pradhan et al. 2017) proposes a new computational code for GIS using triangulated irregular network and Delaunay triangulation methods. The quality of surface (GIS) representation after using proposed model is compared with the original map, and results show that this model can be used for significant reduction of data set.

Authors in paper (Ledoux et al. 2014) present a novel approach to automatically repair GIS polygons, based on the use of a constrained triangulation. Their approach is simple to implement as it is mostly based on triangles and authors have implemented algorithms and show that this model is faster and more efficient than alternative methods. The paper (Roy and Mandal 2012) proposed a time-efficient graph-based spatial clustering for large scale GIS data. As the volume of GIS data is large, data is preprocessed using Delaunay Triangulation to reduce both: space and time complexities.

Implementing security in an IoT solution involves multi-layered access and observation of application security from multiple aspects: network, server, code, database, user, etc. For some concrete and specific examples of attacks on smart cities applications see paper (Saračević et al. 2019). The device must be safe at all times, from design to use in an operating environment. This includes the following measures: Safe Startup, Access Control, Device Authentication, Intrusion Prevention Systems, etc.

The security of an IoT solution should not be seen as additional functionality, but rather as a necessary component for the reliable functioning of the device. IoT techniques are connecting more devices in the Cloud Computing environment. In papers (Alam et al. 2013c; Alam and Shakil 2013a, b, 2016; Ali et al. 2019; Ali and Alam 2016) the authors discuss about management techniques for the Cloud Computing environment. In papers (Alam et al. 2013a, b; Alam 2012a, b; Alam and Alam 2013; Alam et al. 2014; Alam and Sethi 2013; Malhotra et al. 2015, 2018), the authors

emphasize importance of cloud database management system and data integration of cloud-based and relational databases. Also, authors in papers (Shakil and Alam 2014; Shakil et al. 2018; Shakil and Mansaf 2017) describe some techniques for exploiting data reduction principles in cloud-based data management and data management in cloud based environment. Additionally, papers (Imran et al. 2015; Khan et al. 2016, 2017, 2019; Kumar et al. 2017; Kumari et al. 2015; Samiya et al. 2017) describe cloud based big data analytics, data model and computing.

17.3 Data Processing and Storing in Java NetBeans Environments

In this part of the chapter, we have outlined the key packages and classes in Java that we used in the implementation process of the triangulation method for processing and storing data in a smart city space. The two essential packages we used to implement Java 3D solution are:

com.sun.j3d.utils.geometry (*GeometryInfo, Triangulator*),
org.j3d.geom (*TriangulationUtilis*).

The *Java Open Geometry Library (JOGL)* is actually a library for working with geometric shapes and contains packages and classes that are essential for programming in computer geometry. *JOpenGL* is a java link for the *OpenGL 3D Graphics API*. It provides full access to the OpenGL 2.0 specification and supports integration with Swing components. *JOpenGL* maintains its focus on 3D rendering with assistive libraries that make it easier to create geometric primitives.

JOpenGL to some extent offers an object layer that invokes the functions of this library. The implementation of the Java 3D version consists of three packages, with *OpenGL, DirectX* and *JOpenGL* backend (Davis 2004; Sowizral and Deering 1999). Access to the OpenGL interface was achieved through direct calls through the *Java Native Interface (JNI).* Some important classes for the problem of polygon triangulation from the Java 3D API are described below (Chen and Chen 2008).

The *GeometryInfo* class contains ready-made methods for working with string arrays for geometric objects:

TRIANGLE_ARRAY (takes a set of three vertices forming a triangle), using the GL_TRIANGLES method to create triangles,
POLYGON_ARRAY (a set of vertices for non-convex and convex polygons) creates a polygon using the GL_POLYGON method,
QUAD_ARRAY (takes a set of four vertices forming a quadrilateral) using the GL_QUADS method to create quadrilaterals,
TRIANGLE_FAN_ARRAY (set of scopes that forms a triangulation in the shape of a fan), using the GL_TRIANGLE_FAN method, creates a triangulation of a series of triangles around a common central spine,

TRIANGLE_STRIP_ARRAY (a set of vertices forming a ribbon-shaped triangulation), using the GL_TRIANGLE_STRIP method, creates a triangulation of a series of bound triangles.

To store the data, we used the JAVA API for working with databases (*JDBC – Java Data Base Connection*). This API is based on SQL language, that is, JDBC calls SQL interface for Java: *java.sql.Connection* and *javax.sql.DataSource*.

The JDBC API contains a number of abstract Java interfaces that allow you to connect to a specific database, execute a SQL command, and process the results.

Setting up a database of *JavaDB-Sun's Apache Derby* distribution was used to implement the method. In this way, it is possible to use any other database that provides the JDBC driver. The NetBeans environment provides an easy interface for creating databases and establishing connections (Heffelfinger 2011).

The corresponding Java DB (JDBC) driver is available under NetBeans. Figure 17.1 shows how to create a new connection (Fig.17.1, left) and start a Java DB server (Fig. 17.1, right).

After connecting to the server, the database is created for the records of triangulations in the smart city space (Fig. 17.2, left) and the creation of connections to the created database (Fig. 17.2, right).

The created database has tables of the form T_n where n is the number of selected points in the smart city space (polygon). Before generating triangulations, it is necessary to check that a JDBC form connection is established:

JDBC: <subprotocol>: <subname>, where *<subprotocol>* is a type of database access mechanism supported by one or more drivers (Fig. 17.3).

Figure 17.4 (left part) shows the *BlockTriangulation* database tables. Each table contains columns which is equivalent to the number of points of given polygon in a smart city space (Fig. 17.4, right).

The implementation of the Java Test application was done in a NetBeans environment. Below, we describe two modules of the proposed application. The fourth part of the chapter describes the proposed first module for storing and collecting data in a smart city space.

In the fifth part of the chapter, the second module is given, which deals with the process of data processing and finding the minimum triangulation in the smart city space.

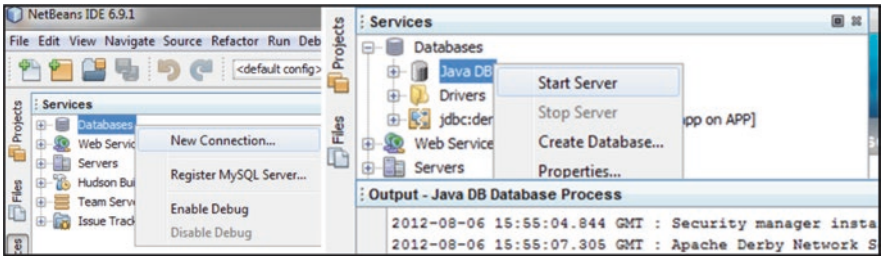


Fig. 17.1 Creating a new connection and starting the server

Fig. 17.2 Creating a database for triangulation blocks and connection to the created database

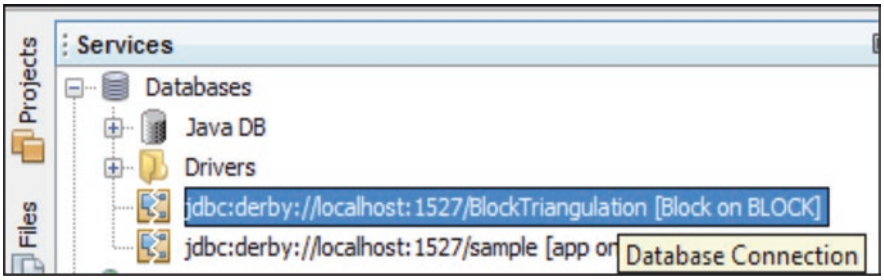


Fig. 17.3 Database access mechanism supported by the appropriate Java driver

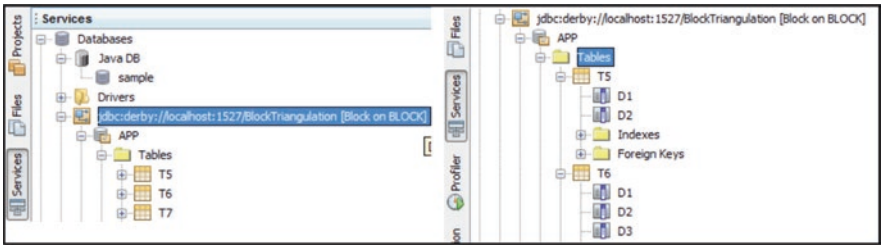


Fig. 17.4 The generated database tables BlockTriangulation and details

17.4 Triangulation Method for Data Storage in Smart City Space

This section describes the technique for storing a particular record in the Smart city space. We will apply the Ballot technique of recording movement through triangulation, which we have described in detail in previous work (Saračević et al. 2014; Saračević and Selimi 2019).

Notation of the Ballot problem can be represented graphically in an integer network consisting of a certain number of points in the Cartesian coordinate system. The problem relates to the number of calculations of paths through an integer network. The paths consist of n steps with some starting point and ending point m. As shown in Fig. 17.5 (left), we can encode each path in an integer network in a specific

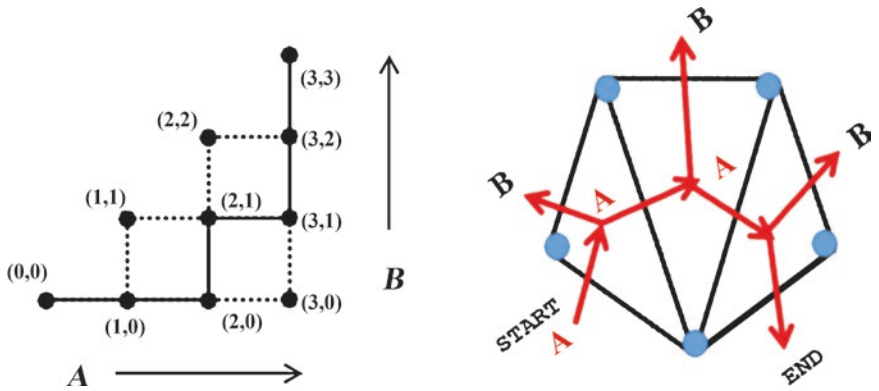


Fig. 17.5 Movement in the integer network (left) and Ballot notation of ABABAB triangulation (right)

order of the right-shift vector (1, 0) and the up-shift vector (0, 1). Combined with the Ballot problem, the choice of upward displacement positions (*mark B*) uniquely determines the path in the integer network because the remaining positions represent rightward shifts (*mark A*).

The number of possible movements through triangulation, analogous to the problem of the number of roads in an integer network, is equal to the Catalan number (see previous papers (Saračević et al. 2014; Saračević and Selimi 2019; Stanimirović et al. 2014)). The presented process of moving over the entire network in combination with the Ballot record served as a good idea for forming a system of recording (notation) of movement through triangulation in the smart city space (Fig. 17.5, right).

In Java, the Graphics2D class with the *Point.Cartesian* class makes it possible to work with the Cartesian coordinate system, where on the basis of roads in the entire network it is possible to realize movement through the triangulation of polygons based on Ballot records.

The storage of triangulations, following the model from previous paper (Stanimirović et al. 2012), can be performed by setting the diagonals of triangulation to be marked with *A* and the outer sides with *B*. The movement is clockwise. This direction of motion, as well as the start and end points of motion (*START / END*), must be the same for all triangulations because of the uniqueness of the record. The condition to complete the movement is to visit all pages (see Fig. 17.5, right).

The implementation of this movement through triangulation was done with following Java classes: *Triangulations, BallotPath, Graphics2D, Nodes, LNodes, ListBallot*.

The main class *BallotPath* contains a method *notation()* that realizes movement records through triangulation. This movement record is backed by *Node* and *LeafNode* classes, which are standard and used to work with polygon page tags and page markers.

Class *Triangulations* is responsible for generating triangulations in the smart city space based on the record produced by the *BallotPath* class. Navigating through Ballot-based triangulation in the BallotPath class was realized based on the described concept of Cartesian coordinates and the problems of paths in an integer network. Java 2D allows points on a flat surface to be accessed using the horizontal and vertical axes.

Class *Graphics2D* provides more sophisticated control over geometry, coordinate transformation, color management, and text layout. Generic points are immutable and can always report their Cartesian coordinates: *Point.OnSegment* and *Point. Cartesian*. The coordinates that deviate from the axis are called Cartesian coordinates, which are also used in Java 2D objects (Fig. 17.6). Java 2D defines coordinates in units and rendering occurs in a hypothetical plane called user space.

Figure 17.7 shows the contents of an output file containing Ballot records for various triangulations in smart city space.

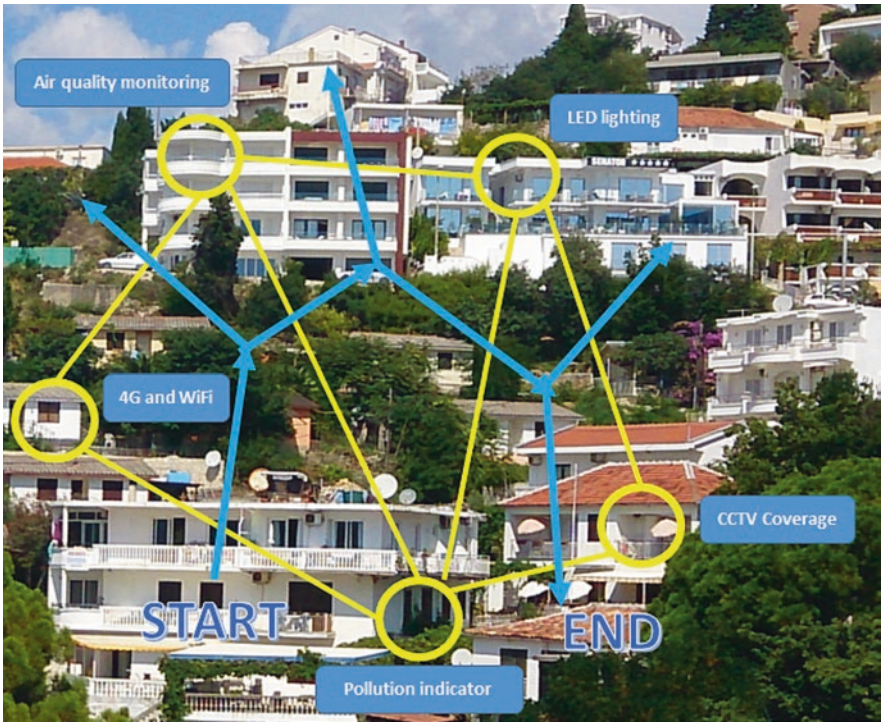


Fig. 17.6 Formation of triangulation in Smart city space

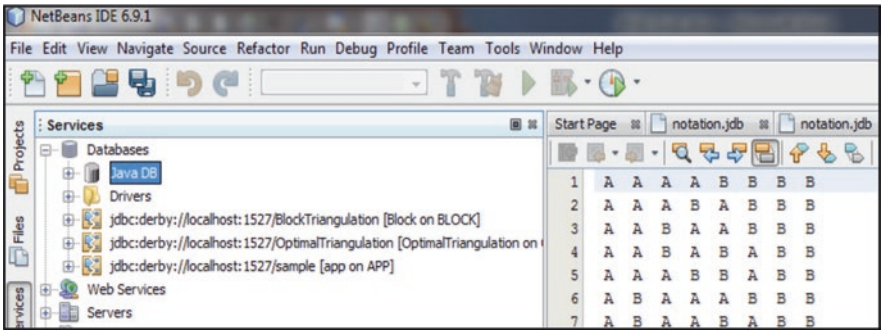


Fig. 17.7 The contents of the output file as a result of testing a Java application

17.5 Triangulation Method for Data Processing in Smart City Space

In this part of the chapter, a second module is presented that deals with data processing and finding the optimal (minimum) triangulation in a smart city space. Papers (Aybeyan et al. 2019; Saračević et al. 2018) deals with the problem of finding the minimum weight triangulation. The default role in storing weights for triangulations is the *Java* package *DefaultTableCellRenderer*, which allows multiple values to be stored in one field of a table (offering efficient division of fields into multiple columns and rows).

Let je V_0, V_1, …, V_{n-1} be the selected polygon in the smart city space. The given polygon is divided into (*n-2*) triangles with (*n-3*) diagonals that do not intersect. Generally, we can associate triangles with weight (i.e. measure: the length of the longest center of gravity line). For the chosen measure, triangulation can be determined such that the sum of these measures of triangles, into which the polygon is divided, is minimal. Each side of a polygon *(i, j)* in a given triangulation of a convex polygon, with k vertices, can form triangles, and for them the weights are calculated:

$$m[i,j] = m[i,k] + m[k,j] + w\left(\Delta v_i v_j v_k\right) \tag{17.1}$$

The method of storage weight triangulations is based on the formation of a square matrix of dimensions *(i = j),* where is also the number of rows, j is the number of columns. The matrix M is used to organize the vertices *(k)* of triangles *(i, j, k)* but also to represent their weights *(w)*. The matrix-based storage method *M* is used in the calculation. Matrix *M* can be permanently switched to table form using the *JDBC API*. The matrix is divided diagonally into two parts (the symmetry divides the matrix into the left and right parts), where the positions *(i, j)*, for which $i = j$ apply, are filled by zeros. On the one side of that symmetry (left part of the matrix), the *k*-vertices of the triangles are recorded and on the other side of the symmetry (right part), the corresponding weights are recorded: k [i, j] = w [j, i]. First, the left part of the matrix that defines triangles of (i, j, k) is filled. For (i, j) corresponding to

the row and column of the matrix, the corresponding allowed topics k are added. All allowances are those between (i, j).

The method for data processing in smart city space consists of 4 phases:

- In the first step, a square matrix is formed and fields are filled diagonally with values *0* (where $i = j$). Then the first diagonal line of the field of symmetry is filled. These are adjacent vertices and for them there are no k values with which a (i, j, k) triangle can be formed. After that, all values of k on (i, j) are added.
- The second step is to calculate all the weights (w) for the rows and columns of the matrix for which, by *Eq. (17.1)*. The additional values of k at position (i, j) add the corresponding weights to (j, i).
- In the third step, the corresponding triangulation of the polygons is joined to the obtained values in the matrix. From the obtained values, $(n\text{-}2)$ triangles are determined which determine the triangulation.
- The fourth step is to show the optimal triangulation in the smart city space (see Fig. 17.8).

Example 1

In the specific case, it is shown how the scenario described works. The four steps explain how optimal triangulation occurs in a smart city space.

Step 1: If the number of selected points in the smart city space is equal to 5, then a matrix of dimensions 5x5 is formed. Fill in the fields diagonally in the zero matrix, as well as the values for adjacent vertices.

Step 2: After that, fill in for all *(i, j, k)* triangles. In this case, there are a total of 10. There are as many calculated weights *(w)* and each triangle at the (i, j) position corresponds to the calculated weight at *(j, i)* position. The resulting matrix after 1 and 2 steps looks like this:

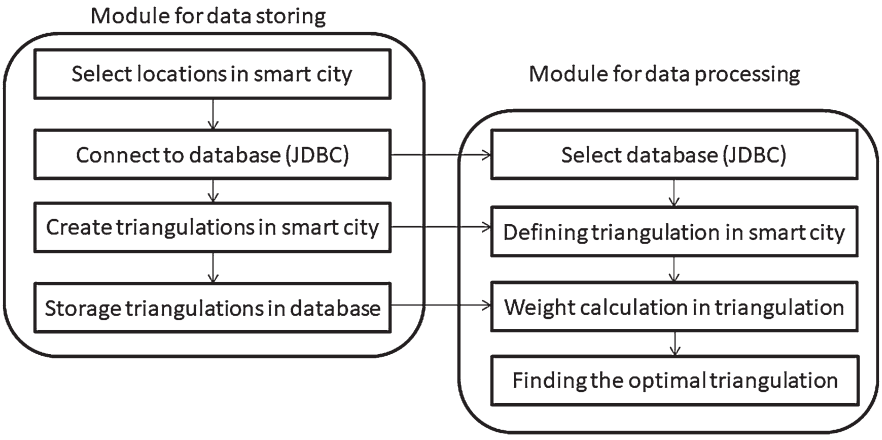


Fig. 17.8 Flowchart of proposed approach (for two modules)

$$opt5 = \begin{bmatrix} 0 & \{0\} & \{35\} & \{42,40\} & \{31,43,\langle 25\rangle\} \\ \{0\} & 0 & \{0\} & \{35\} & \{38,41\} \\ \{2\} & \{0\} & 0 & \{0\} & \{36\} \\ \{2,3\} & \{3\} & \{0\} & 0 & \{0\} \\ \{2,3,\langle 4\rangle\} & \{3,4\} & \{4\} & \{0\} & 0 \end{bmatrix}$$

Step 3: Summarize the weights *(w)*. A new column *W* is added to the table containing the sum of all triangulation weights in the current row. The triangulation storage table is expanded with a new column W (see Table 17.1):

Step 4: Find the lowest weight or minimum (optimal) triangulation:

$$OptT_w = \min\{sumAllW[T_1],\ldots,sumAllW[T_i]\}$$

In Table 17.1, the third row is the minimum weight triangulation *OptTw = 100.* It is determined by the diagonals *δ (2,4)* and *δ (1,4),* see Fig. 17.9.

In the Java NetBeans environment, the *OptimalSmartTriangulation* application has been implemented that implements the above steps. The main class has the *compute ()* method, which is in charge of calculating all the weights in *table T*. To work with the cells of the table, the *DefaultTableCellRenderer* class was used. In addition to the class specified, *JTable, TableCellRenderer, BasicTableUI* were used. An *OptimalTriangulation* database has been formed in a *Java* database service that contains tables with persistent triangulation weights.

The application works according to the scenario described:

1. The JDBC connection is first checked, followed by the weight calculation, by clicking on the "Weight Calculation" button (Fig.17.10)

After the corresponding table T_n is created, a new weight column *(w)* will be filled in order for each triangulation (i.e. for each row in the table).

Filling in the new column refers to recognizing *(i, j, k)* values from the matrix based on the diagonal *δ (i, j)* in table T_n (Fig.17.11).

After calculating the weights for all triangulations, the user will be shown the standard output *„status ok*"and the lowest weight triangulation will be plotted on *JPanel*. Figure 17.12 shows an application for finding the optimum (minimum) triangulation.

Table 17.1 Weight table

Calculation (i)	D1 (first)	D2 (second)	Weight
1	δ (1,3)	δ (1,4)	124
2	δ (1,3)	δ (3,5)	136
3	δ (2,4)	δ (1,4)	100
4	δ (2,4)	δ (2,5)	109
5	δ (2,5)	δ (3,5)	112

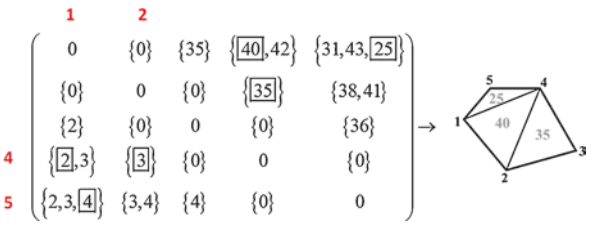


Fig. 17.9 Appropriate values in the matrix and graphical representation of optimal triangulation

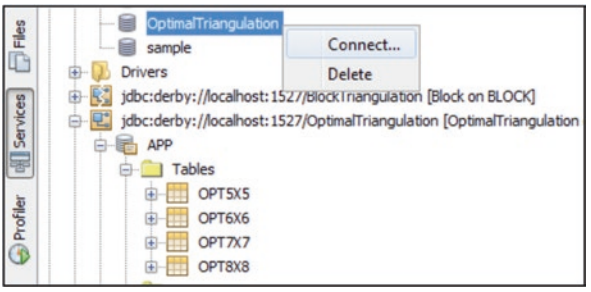


Fig. 17.10 Java service for connecting to the OptimalTriangulation

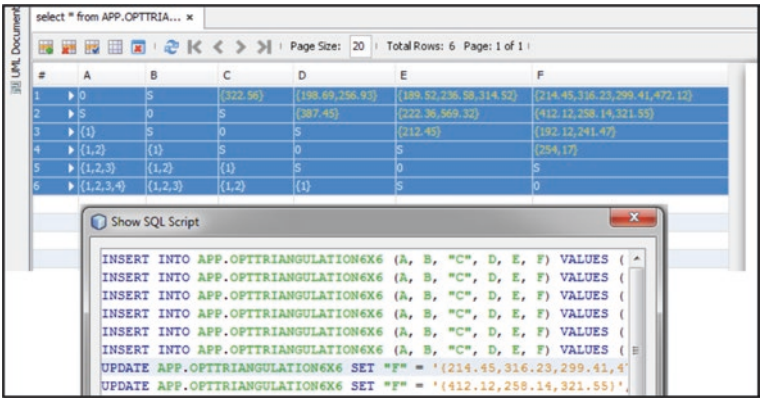


Fig. 17.11 Joining weights in triangulations in JTable

Figure 17.13 shows a standard output with generated parameters at each step of the proposed method.

17.6 Discussion

Utilizing technology and modern scientific advances, civilization is moving to a higher level and thus generating "smart" ideas to keep up with the ongoing challenges, risks and problems it faces. Smart cities are a concept of the future that will

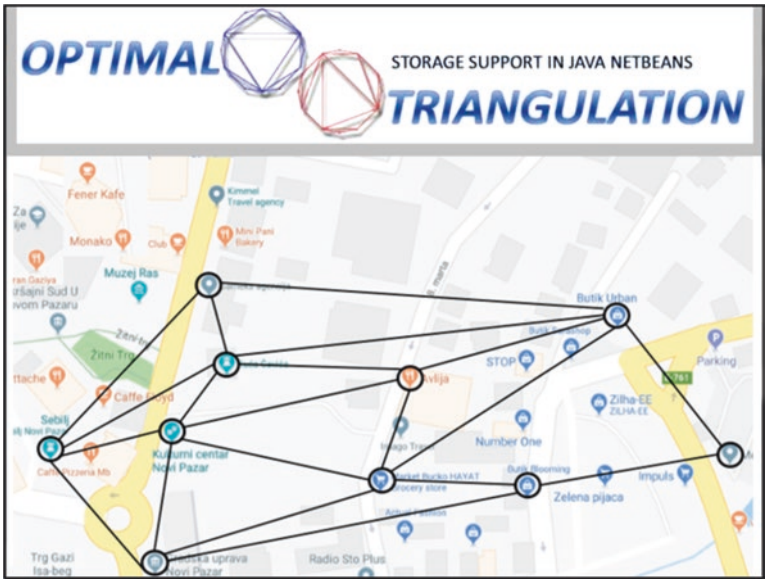


Fig. 17.12. Java application for finding optimal triangulations

need more and more attention and that becomes inevitable in the coming times. The aim of this concept is to ensure environmental, energy and social sustainability through the use of technology-information and other smart systems, with the city covered with various sensors, software and devices to monitor developments and changes in it. The city would not change its appearance, only its organization and way of functioning.

A smart city is just another solution that the modern age has to deal with the problems that are in line with achievements and to provide citizens with a healthy and safe lifestyle as it may have once been, or might even get better.

However, there are challenges and obstacles in creating the concept of smart cities in most cities, one of which is the complexity of existing infrastructure and the need for a large amount of human and material resources, and a particular challenge is the issue of security. When integrating different intelligent devices, it is common for protocols to be incompatible, which generally differ in the amount of data they exchange and the speed of their processing.

New applications and online services in IoT place high demands on scalability, reliability and flexibility. Traditional computer networks with a hierarchical architecture model are finding it increasingly difficult to fill them. The solution is software-defined networks that bring a high degree of programmability. As further directions for research in this field, we can say that it is useful to examine the possibility of applying triangulation methods in the field of software defined networks and openflow protocols.

```
STEP 2:
INSERT INTO APP.OptTriang[1,1] VALUES (0) COST(1,1)= w(0)
INSERT INTO APP.OptTriang[2,2] VALUES (0) COST(2,2)= w(0)
INSERT INTO APP.OptTriang[3,3] VALUES (0) COST(3,3)= w(0)
INSERT INTO APP.OptTriang[4,4] VALUES (0) COST(4,4)= w(0)
INSERT INTO APP.OptTriang[5,5] VALUES (0) COST(5,5)= w(0)
INSERT INTO APP.OptTriang[6,6] VALUES (0) COST(6,6)= w(0)


---
STEP 3:
INSERT INTO APP.OptTriang[6x6] VALUES ([1,2] k(3), COST(2,1)= w(446.01)
INSERT INTO APP.OptTriang[6x6] VALUES ([1,3] k(3), COST(3,1)= w(240)
INSERT INTO APP.OptTriang[6x6] VALUES ([2,3] k(3), COST(3,2)= w(446.01)
INSERT INTO APP.OptTriang[6x6] VALUES ([3,2] k(3), COST(2,3)= w(498.94)
INSERT INTO APP.OptTriang[6x6] VALUES ([4,2] k(3), COST(2,4)= w(333.54)
INSERT INTO APP.OptTriang[6x6] VALUES ([4,3] k(3), COST(3,4)= w(498.94)
INSERT INTO APP.OptTriang[6x6] VALUES ([1,2] k(4), COST(2,1)= w(353.46)
INSERT INTO APP.OptTriang[6x6] VALUES ([1,3] k(4), COST(3,1)= w(564.79)
INSERT INTO APP.OptTriang[6x6] VALUES ([1,4] k(4), COST(4,1)= w(500.33)
INSERT INTO APP.OptTriang[6x6] VALUES ([2,3] k(4), COST(3,2)= w(944.95)
INSERT INTO APP.OptTriang[6x6] VALUES ([2,4] k(4), COST(4,2)= w(353.46)
INSERT INTO APP.OptTriang[6x6] VALUES ([3,2] k(4), COST(2,3)= w(500.56)
INSERT INTO APP.OptTriang[6x6] VALUES ([3,4] k(4), COST(4,3)= w(412.8)
INSERT INTO APP.OptTriang[6x6] VALUES ([1,2] k(5), COST(2,1)= w(358.99)
INSERT INTO APP.OptTriang[6x6] VALUES ([1,3] k(5), COST(3,1)= w(652.8)
INSERT INTO APP.OptTriang[6x6] VALUES ([1,4] k(5), COST(4,1)= w(999.27)
INSERT INTO APP.OptTriang[6x6] VALUES ([1,5] k(5), COST(5,1)= w(334.05)
INSERT INTO APP.OptTriang[6x6] VALUES ([2,3] k(5), COST(3,2)= w(946.57)
INSERT INTO APP.OptTriang[6x6] VALUES ([2,4] k(5), COST(4,2)= w(687)
INSERT INTO APP.OptTriang[6x6] VALUES ([2,5] k(5), COST(5,2)= w(358.99)
INSERT INTO APP.OptTriang[6x6] VALUES ([1,2] k(6), COST(2,1)= w(126.46)
INSERT INTO APP.OptTriang[6x6] VALUES ([1,3] k(6), COST(3,1)= w(481.01)
INSERT INTO APP.OptTriang[6x6] VALUES ([1,4] k(6), COST(4,1)= w(1000.89)
INSERT INTO APP.OptTriang[6x6] VALUES ([1,5] k(6), COST(5,1)= w(667.6)
INSERT INTO APP.OptTriang[6x6] VALUES ([1,6] k(6), COST(6,1)= w(262.89)
---
STEP 4:
 VALUES ([1,2] k(6), COST(2,1)= w(126.46)
```

Fig. 17.13. The parameters obtained in the phases of the proposed method

17.7 Conclusion

In this chapter, we introduced one solution for smart cities data storage and processing based on the triangulation method. The proposed method has two modules: the first for storing and collecting data in a smart city space, while the second module relates to the data processing process and finding the minimum triangulation in a smart city space. We have provided specific examples of implementing and testing the proposed method in a Java NetBeans environment.

In particular, the proposed solution can find its application in the concept of realizing smart traffic or transportation. For traffic congestion, solutions are mainly found through projects based on the use of computer systems and simulations of different traffic cases, ie in the integration of IT and traffic infrastructures. The use of modern information technologies encourages the establishment of new infrastructure consisting of networks of roads, railways, airports, stations and ports connected by internet-based systems.

Efficiency and quality are significantly influenced by intelligent systems that improve the mobility and safety of road users, as they provide proactive maintenance and faster and better diagnostics. These advanced solutions, by the way, increase the productivity of business operations, shorten travel time and reduce environmental pollution.

References

Alam, M. (2012a). *Cloud algebra for cloud database management system*, The second international conference on Computational Science, Engineering and Information Technology (CCSEIT-2012), October 26–28, Coimbatore, India, Proceeding published by ACM.

Alam, M. (2012b). Cloud Algebra for handling unstructured data in cloud database management System. *International Journal on Cloud Computing: Services and Architecture (IJCCSA)*, *2*(6), Taiwan.

Alam, M, & Alam, B. (2013). Cloud query language for cloud database. In *Proceedings of the international conference on recent trends in computing and communication engineering – RTCCE 2013* (pp. 108–112), Hamirpur..

Alam, M., & Sethi, S. (2013). Security risks & migration strategy for Cloudsourcing: A government perspective. *International Journal of Engineering and Innovative Technology, 2*(7), 205–209.

Alam, M., & Shakil, K. A. (2013a). A decision matrix and monitoring based framework for infrastructure performance enhancement in a cloud based environment, international conference – Hyderabad, Nov 08–09, India, Elsevier.

Alam, M., & Shakil, K. A. (2013b). Cloud database management system architecture. *International Journal of Advances in Computer Science and Its Applications, 3*(1), 27–31, Australia.

Alam, M., & Shakil, K. A. (2016). *Big data analytics in cloud environment using Hadoop*. In International conferences on Mathematics, Physics & Allied Sciences-2016, March 03–05.

Alam, B., Doja, M. N., Alam, M., & Malhotra, S. (2013a). 5-layered architecture of cloud database management system. *AASRI Procedia Journal, 5*, 194–199, Elsevier.

Alam, B., Doja, M. N., Alam, M., & Malhotra, S. (2013b). Security issues analysis for Cloud Computing. *International Journal of Computer Science and Information Security, 11*(9), 117–125.

Alam, M., Sethi, S., & Sethi, S. (2013c). Covert channel detection techniques in cloud, confluence 2013: The next generation information technology Summit (4th International Conference), (pp. 127–132), IEEE.

Alam, M., Ara, K., Javed, M. S., & Ansari, M. (2014). *Detect and filter traffic attack through cloud Trace back and neural network, Imperial College*. The 2014 International Conference of Data Mining and Knowledge Engineering (ICDMKE) London, U.K., 2–4 July.

Ali, S. A, & Alam, M. (2016). *A relative study of task scheduling algorithms in Cloud Computing environment.* In Proceedings of the 2016 2nd international conference on contemporary computing and informatics, 7917943, (pp. 105–111).

Ali, S. A, Affan, M., & Alam, M. (2019). *A study of efficient energy management techniques for Cloud Computing Environment*. 9th International conference on Cloud Computing, data science & engineering (Confluence), (pp. 13–18), Noida, India.

Aybeyan, S., Krrabaj, S., Saracevic, M., & Pepic, S. (2019). Memoization method for storing of minimum-weight triangulation of a convex polygon. *Computer Science – AGH, 20*(2), 195–211.

Chen, J., & Chen, C. (2008). *Foundations of 3D graphics programming: Using JOGL and Java3D*. London: Springer.

Chen, X., & He, K. (2017). The function of GIS in the Smart City construction, smart computing and communication. *Book Series: Lecture Notes in Computer Science, 10135*, 374–380.

Cosido, O., Loucera, C., & Iglesias, A. (2013). *Automatic calculation of bicycle routes by combining meta-heuristics and GIS techniques within the framework of smart cities*. 2013 International conference on new concepts in smart cities: Fostering public and private alliances (SMARTMILE).

Davis, G. (2004). *Learning Java bindings for OpenGL*. Bloomington: Author-house publisher.

Fashal, N., El Khayat, G., Salem, B., & El Kaffas, S. (2019). A multi-criteria GIS based methodology for smart cities site selection, electronic governance and open society: Challenges in Eurasia. *Book Series: Communications in Computer and Information Science, 947*, 38–51.

Heffelfinger, D. (2011). *Java EE 6 development with NetBeans 7*. Birmingham: Pack publishing.

Imran, K., Naqvi, S. K., & Alam, M. (2015). *Data model for Big Data in cloud environment, computing for sustainable global development (INDIACom)*. 2015 2nd International Conference on, 11–13 March 2015, (pp. 582–585), New Delhi, India, IEEE.

Khan, S., Shakil, K. A, & Alam, M. (2016). *Educational intelligence: Applying cloud-based big data analytics to the Indian education sector*. In Proceedings of the 2016 2nd International conference on contemporary computing and informatics, IC3I 2016, 7917930, (pp. 29–34).

Khan, S., Shakil, K. A., & Alam, M. (2017). Big Data computing using cloud-based technologies: Challenges and future perspectives. In M. Elkhodr, Q. F. Hassan, & S. Shahrestani (Eds.), *Networks of the Future: Architectures, Technologies and Implementations* (Book series: Computer and information science series). Boca Raton: Chapman and Hall/CRC Press.

Khan, S., Arshad Ali, S., Hasan, N., Ara Shakil, K., & Alam, M. (2019). *Cloud Computing for geospatial Big data analytics* (pp. 1–28). Cham: Springer Book.

Kumar, V., Kumar, R., Kumar Pandey, S., & Alam, M. (2017). *Fully homomorphic encryption scheme with probabilistic encryption based on Euler's theorem and application in Cloud Computing, big data analytics* (pp. 605–611). Springer.

Kumari, M. Y., Kumar, A. V., & Alam, M. (2015). Design flaws and cryptanalysis of a standard mutual authentication protocol for Cloud Computing based healthcare system, Springer lecture notes in Electrical Engineering.

Ledoux, H., Ohori, K., & Meijers, M. (2014). A triangulation-based approach to automatically repair GIS polygons. *Computers & Geosciences, 66*, 121–131.9.

Lella, J., Mandlab, V., & Zhuc, X. (2017). Solid waste collection/transport optimization and vegetation land cover estimation using Geographic Information System (GIS): A case study of a proposed smart-city. *Sustainable Cities and Society, 35*, 336–349.2.

Malhotra, S., Doja, M. N., Alam, B., & Alam, M. (2015). Data integration of cloud-based and relational databases. *International Conference on Soft Computing Techniques and Implementations, ICSCTI, 7489542*, 83–86.

Malhotra, S., Najmud Doja, M., Alam, B., & Alam, M. (2018). Generalized query processing mechanism in cloud database management system. In V. Aggarwal, V. Bhatnagar, & D. Mishra (Eds.), *Big data analytics. Advances in intelligent systems and computing* (Vol. 654, pp. 641–648). Springer.

Pradhan, B., Sandeep, K., Mansor, S., Ramli, A., & Sharif, A. (2017). Second generation wavelets based GIS terrain data compression using Delaunay triangulation. *Engineering Computations, 24*(2), 200–213.

Roy, P., & Mandal, J. (2012). *A delaunay triangulation preprocessing based Fuzzy-Encroachment graph clustering for large scale GIS data*. In: 2012 international symposium on Electronic System Design (ISED 2012), (pp. 300–305).

Samiya, K., Shakil, K. A., & Alam, M. (2017). *Cloud based Big data analytics: A survey of current research and future directions, Big data analytics* (pp. 629–640). Cham: Springer.

Saračević, M., & Selimi, A. (2019). Convex polygon triangulation based on ballot problem and planted trivalent binary tree. *Turkish Journal of Electrical Engineering and Computer Sciences, 27*(1), 346–361.

Saračević, M., Stanimirović, P., Krtolica, P., & Mašović, S. (2014). Construction and notation of convex polygon triangulation based on ballot problem. *ROMJIST – Journal of Information Science and Technology, 17*(3), 237–251.

Saračević, M., Masovic, S., Stanimirovic, P., & Krtolica, P. (2018). Method for finding and storing optimal triangulations based on square matrix. *Applied Sciences – Geometry Balkan Press, 20*, 167–180.

Saračević, M., Selimi, A., & Plojovic, S. (2019). *Some specific examples of attacks on information systems and smart cities applications*. Advanced sciences and technologies for security applications (in Book: Cybersecurity and Secure Information Systems). Springer.

Shahrour, I. (2018). Use of GIS in smart city projects. *GIM international-the worldwide magazine for geomatics, 32*(5), 21–23.

Shakil, K. A., & Alam, M. (2014). Data Management in Cloud Based Environment using k-median clustering technique. *International Journal of Computer Applications, 3*, 8–13.

Shakil, K. A., & Mansaf, A. (2017). *Cloud Computing in bioinformatics and Big data analytics: Current status and future research, Big data analytics* (pp. 629–640). Berlin: Springer.

Shakil, K. A, Alam, M., Shakeel, S., Ora, A., & Khan, S. (2018). *Exploiting data reduction principles in cloud-based data management for cryo-image data.* In Proceedings of the 2018 international conference on computers in management and business (pp. 61–66), ACM.

Sowizral, H., & Deering, M. (1999). The Java 3D API and virtual reality. *IEEE Computer Graphics and Applications, 19*(3), 12–15.

Stanimirović, P., Krtolica, P., Saračević, M., & Mašović, S. (2012). Block method for triangulation convex polygon. *ROMJIST – Journal of Information Science and Technology, 15*(4), 344–354.

Stanimirović, P., Krtolica, P., Saračević, M., & Mašović, S. (2014). Decomposition of Catalan numbers and convex polygon triangulations. *International Journal of Computer Mathematics, 91*(6), 1315–1328, Taylor and Francis.

Tan, S., & Wong, O. (2006). Location aware applications for smart cities with Google maps and GIS tools. In *Advances in intelligent IT: Active media technology* (Book series: Frontiers in Artificial Intelligence and applications) (Vol. 138, pp. 223–228).

Yamamura, S., Fan, L., & Suzuki, Y. (2017) *Assessment of urban energy performance through integration of BIM and GIS for smart city planning*. International High-Performance Built Environment Conference, in Book Series: Procedia Engineering 180 (pp. 1462–1472).

Chapter 18
Intelligent Environment Protection

Subha P. Eswaran

Abstract Environment protection is the current need of the hour. The upcoming issues like global warming, air pollution and water pollution are due to the degradation of environment. Measures should be taken to save the nature from further degradation and retrieve back the lost wealth of the nature. This chapter provides insight on methods and approaches to protect the environment. IoT based architecture has been proposed to habituate the environment protection.

Keywords IoT eco-system · Intelligent environment · Monitoring · Self-diagnostic · Pollution · Environmental policies

18.1 Introduction

Environment protection is the process of protecting the ecosystem and preventing the environment from degradation. Protection of the environment is a collective approach exercised by individuals, organizations and governments. The objectives of the environment protection are preserving and conserving of natural resources. Preserving includes the measures to protect the ecosystem or natural environment from degradation or damages. Prevention is to be prepared to avoid any degradation in future.

The tremendous growth of population, exhaustive usage of natural resources, and technology improvements are the main causes of degradation of the nature environment. In a broader way, the causes of the environment degradation can be classified into two categories:

- Natural distortion
- Man-Made distortion

S. P. Eswaran (✉)
CRL, Bharat Electronics Limited, Bangalore, Karnataka, India
e-mail: subhape@bel.co.in

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_18

18.1.1 Environment Protection

Intelligent environmental protection is feasible if we have suitable environmental diagnostic system with real-time monitoring capability to acquire all the relevant data about the environmental conditions. The current state-of-art of environment protection is based on sensor networks that enable collection of data about the environment status. The information obtained from sensor network is processed at back end and preventive measures are carried out to avoid further degradation.

However, the emerging requirement for environment protection should have the potential of self- diagnostic and self-protective. The protection system of the environment should be self-aware and have the intelligence for self-healing with or without human intervention. In order to achieve such self-protection approach, the monitoring system should be provided with high-precision and timely information. The sensory information must be obtained from spatially distributed intelligent sensor devices and the system should have the potential to derive the decision with prior knowledge and prediction methodologies.

Natural disasters such as heavy rainfall, cyclones, earthquake, and tsunami can only be predicted earlier and it cannot be controlled. In such cases, protection can be accomplished by advanced sensor network, which can provide early warning to the public with high accuracy. It also estimates the support required for rescue operations. Disaster due to man-made such as industrial accidents, noise pollution, light pollution, water pollution and air pollution can be prevented. Preventive measures can be taken with the help of Artificial Intelligent (AI) driven IoT solutions. The response for such disasters can also be automated to large degree. The early warning, preventive and predictive systems became handy for such disasters.

18.1.2 Preventing the Environment Degradation

Preventing the environment from the hazardous changes can be accomplished by assessing mechanism. Environment assessment by regulations and policies is useful for finding the usage level of natural resources. Over consumption or illegal usage of natural resources will be controlled by the policy. Another type of assessment will be based on automated information processing about the conservation of natural resources. This can be accomplished with the help of ICT (Information and Communication Technology) and IoT. In this approach, an attribute set will be developed which is relevant to the chosen use case to derive the action for prevention. The choice of variables of the attribute set will be decided based on the context. For example, for understanding the pollution level, the measures such as CO_2 emission from the factories in the area, O_2 demand in the area and solid waste could be the attribute set. The resultant of the attribute approach will help to find the root causes of the problem and future road-map to improve the situation.

Environment protection is not a new concept for the human community. However, due to the ever increasing threat to anthropogenic of nature, there need a systematic and intelligent environmental protection method. With the advent of technology advancements and environment-awareness among human, the intelligent environment protection will bring back the wealth of Mother Nature.

18.2 Environmental Issues

In this section, causes of environmental degradation are discussed in detail. The environmental degradations can occur due to ***natural & manmade scenarios***. Natural means of environmental degradation are due to cyclone, flood, landslide, earthquake, etc. Manmade means of environmental degradations are noise pollution, sound pollution, water pollution, light pollution etc.

Sometime man also an indirect cause for creating natural distortions. Cutting of trees will lead to landslides. Since the water resources such as lakes are not maintained properly, their storage capacity is not enhanced and hence during heavy rain fall it may lead to floods (McColl 2015).

Human society is also the cause for developing famines, which is because of inappropriate land policies. Global warming is increasing, due to the emissions of hazardous gasses. Currently, the concentration of CO_2 is exceeded 400 ppm. Reports say that main cause of carbon emission is due to air conditioning systems, smoke of vehicles and industry production gas. Global sea-levels are increasing because of climate changes. The tall buildings and multi-stack apartments lead to soil erosions.

The ***man-made distortions*** are caused by the following reasons:

1. Unauthorized waste dumping
2. Constitutional nuisance
3. Unregulated usage of natural resources

18.2.1 Unauthorized Waste Dumping

There are two types of waste generating sources. One of source is the industry and other source is domestic or urban. Industrial wastes are the unwanted material disposed by factories during the manufacturing process. Industrial waste includes dirt, scrap metal, concrete, chemicals or gases. These industry wastes may be harmful to living or non-harmful. Factories situated near water sources, dispose the industry waste into the water source itself and polluting the water. Untreated industry waste or partially treated waste which is disposed in to water sources will kill the water living creatures. Hazardous waste mixed in the water sources will lead to affect the water eco system. It will also affect the health of the people who consume water of such water bodies. The industrial waste dumping has been regulated by RCRA

(Resource Conservation and Recovery Act) at USA. The USA has also been practicing the EPA (Environmental Protection Act) to manage the treatment and disposal of waste into water bodies.

Domestic/municipal waste includes the waste outcomes from homes, and urban areas. In the past few decades, the waste generated by average citizen is increased to half a ton. It leads to CO_2 emission of 4.2–10 kg per ton of waste. The unauthorized method of waste dumping leads to water pollution, soil pollution and air pollution. The type of municipal waste depends upon the consumer's income, community and commercialism. In general, municipal waste can be classified into organic waste or non-organic waste. Organic waste includes plant waste, food, wood rubber, leather, cloth etc. Non-organic waste includes glass, plastics and metals.

In olden days the mixed waste (Organic and non-Organic) is collected from homes and transported to waste dumping areas. This method is having lots of impacts for the living being and environment. Other than this traditional method, the few other methods of municipal waste disposal are landfilling, composite, recycling and incinerations. These days biological and chemical methods of treating the household waste are also tried out to effectively dispose the waste. Suitable disposal methods should be used to dispose the different waste particles. There are no more separate lands available for garbage dumbing. The existing landfills are exhausted. Currently, common bio-medical waste treatment facilities (CBWTF) are extended to major big cities to avoid landfills with garbage. The municipal waste must be segregated for organic and non-organic. The method of recycling and biomedical or chemical method of disposal of waste is the solution for this problem. The city will be called as smart city only when it has managed the air pollution and waste management to achieve clean water bodies and clean city.

18.2.2 Constitutional Nuisance

Pollution is the act of introducing undesirable elements into natural environment that will affect the natural form of existence of the natural resources such as air, water and soil earth. There are different forms of pollution that include water pollution, sound pollution, light pollution, soil pollution, thermal pollution, radioactive pollution etc. Any form of pollution that creates disturbance to the living being/nature constitution is illegal and called as constitutional nuisance.

Water pollution refers to the process of contaminating the water sources. The untreated industrial waste disposed into water bodies will lead to water pollution. The industry waste consists of harmful chemicals. It will affect the living being of water. The polluted water is the cause of bacterial infections, skin diseases, and productivity disorder in plants, human or any living being. Water pollution is classified into three categories which are surface water pollution, marine water pollution and water nutrient pollution. Surface water pollution refers to the contamination

happens to the surface water sources such as river, lakes, or ponds. Marine water pollution refers to the introduction of hazardous elements mixing in the ocean water that create unhealthy scenario for living being of ocean. The work in (Pan et al. 2018) lists the ways in which coastal line across Vietnam causes maritime pollution. Apart from oil spills and ship wreckages, domestic solid/liquid wastages are also turned into sea without treatment in many countries. Such pollutions cannot be controlled by a single country and it requires a collective effort from various agencies. Nutrient pollution is due to excessive nutrients in the water bodies.

Air pollution is caused by pollutants in the air that destroy the human health and the planet. Fossil fuel burning of the industry is the main cause of air pollution. Nitrogen oxide is the common pollutant of air pollution. Excessive Ammonia in air leads to repository problems. Heavy air impurities lead to irritation of eye, headaches, skin infection etc. Air pollution in the form of CO_2 is the major cause of climatic changes and Methane increase in air environment contribute to increase of global warming. Climate changes also create more cyclones, flood, and extreme weather conditions. Clean Air Act (CAA) of USA is reguprocess of protecting the ecosystem and preventing the environment from degradation.lating the amount of pollution emissions. The smoke emission from vehicle is also one of major cause of air pollution. Even the emission per vehicle is regulated, if there are thousands of vehicles are operated in a highly populated city, the collective amount of emission may go above tolerance level for the geographical area. An Ethiopian city named Addis Ababa can be taken as a live example for this case (Worku and Giweta 2018). Despite their effort to become sustainable city, the uncontrolled industrialization, rapid urbanization, and informal settlements are polluting the rivers around the city. The other major cause of environment pollution is the impact of radioactivity. The data published by UNSCEAR says that most of the radioactivity implications are caused by individual usage of radio devices such as mobile phones. The upcoming smart city applications of IoT are going to be threat to extensive spectrum usage in the environment. The intensive radiation will have impact on living being in the earth. The usage and optimal power level of radiation must be regulated. The optimal spectrum usage rules have been discussed in (Eswaran et al. 2014) for smart city applications. Similarly, the usage of IoT for vehicle-to-vehicle communication is also going to increase in future. It will also use the considerable amount of radio devices in vehicles to establish Intelligent Transport system (ITS). The extensive use of radioactivity for such application also will have effect on the environment. The effective spectrum regulation polices for vehicle communication is also essential for the same. One such approach is discussed in (Eswaran et al. 2015), which provides optimized spectrum usage solutions. The radiation regulation policies are of US government is discussed in (Andersson et al. 2009) that gives the bench marking threshold of spectrum radiation.

Noise pollution is mainly caused by industry, transport and transmission systems. Noise levels higher than 50 dB is creating higher impact on the hearing system of human being. Fire crackers and loud speakers are the major sound pollutants in residential areas.

18.2.3 Unregulated Usage of Natural Resources

Natural resources are limited. If the natural resources are used exhaustively, the human society will face the consequences such as soil erosion, oil depletion, ozone depletion, forced migration, metals & mineral depletion. The huge increases in population, advancement in sophisticated technology and commercialism have led to the exploitation of natural resources. The exhaustive mineral extraction will lead to soil degradation, water scarcity, destruction to environment ecosystem and global warming aggravation. The technology growth has also resulted in waste which cannot be managed or non-regulated. Such waste materials include nuclear wastages, electronic wastages and marine environment. The methods of handling marine pollution has been discussed in (Tran and Nguyen 2019), with the coastal line across maritime pollution at Vietnam. Collective efforts of multiple countries will be required to control marine pollution.

Usage of ground water needs regulation. Consumption of raw materials is increased manifold in this decade. The raw material consumption of developed countries has increased 32 times more in the developing countries. The phenomenon of over consumption is the outcome of different industries which include textile, footwear, building construction, beverages, cosmetics and medicines. These industries use different raw materials and exhaustive production leads to overconsumption of natural resources. The concept of renewable energy and recycling technologies must be encouraged, to compensate the exhaustive and unregulated usage of natural resources.

18.3 Monitoring of Environmental Hazards

In literature many ways are proposed to monitor the presence of major polluting agents on the environment. This section provides a brief of such efforts.

The work presented in (Al-Masri et al. 2018) comprises of an edge device connected with sensor attached to waste bins for monitoring the segregation of solid waste before dumping into the garbage bins. This helps in identifying the violations in real-time. There are methods to monitor the amount of garbage in the bin that helps to guide the garbage collectors for efficient collection of garbage. Air quality sensors can be used to monitor the decaying of the food and medical wastes in garbage bins to enable timely clearance of the garbage bins.

Satellite imagery is used to monitor the unauthorized dumping of waste in (Vambol et al. 2019). Image processing algorithms over satellite images are used to detect large scale dumping of wastes in any geo location. The location details are compared with local authorities to identify whether it is authorized dumping or unauthorized. There are open source hardware (such as Arduino boards) based environment to monitor temperature, pressure, humidity and seismic activities in a given geo-location.

Crowd sourcing based city air quality monitoring methods are available in literature, which measure the carbon footprint in the city, based on CO_2 sensors. While the usage of low cost sensors is widely accepted, they are prone to outliers due to erroneous output under extreme cases. The solution of this issue is discussed in (Cieplak et al. 2019) using a machine learning approach for removing outliers from the sensor data. In this work, industrial pollutants such as NO_2, NO_x, O_3, PM_{10}, $PM_{2.5}$, and SO_2 level in air are monitored to assess the air quality at Lublin, Poland.

Apart from progressive degrading, a gas leakage from industry or stoves used for domestic purpose can cause catastrophic accidents. There are various types of sensors to alert leaks of dangerous gases.

Industrial pollution at Russia is discussed in (Mazanik 2018), provides various industrial activities carried out since 1880 to 1917 at Moscow city of Russia. It also details their effect on river and water pollution.

FarolApp described in (Mihindukulasooriya et al. 2016) is used to monitor the artificial light pollution using a web application. This is an open data that can be accessed using mobile platforms. Night sky brightness monitoring work presented in (Zamorano et al. 2019) maintains the log of light pollution at Spain.

A geo reference based noise pollution monitoring system is presented in (Gómez et al. 2017). Public mobile phones are used for this purpose. The captured data is geo-tagged using GPS. At some urban areas, construction works are limited to certain time of the day. Similarly there are some zero noise zones. The urban noise classifier presented in (Alsouda et al. 2018) comes handy in identifying the type of noise produced at a location. This can be used by intelligent environment system for monitor the noise and categorize them.

In recent years, significant interest has been focused on communication networking companies that equip heavy energy consuming data centers. These kinds of data centers also emit huge heat into the environment. There need a regulation policies to formulate energy-efficient and eco-friendly data centers or cloud centers. One such approach is presented in (Ali et al. 2019). This method provides an optimal energy saving for cloud architectures. Now-a-days, the regulatory norms for data center emission and consumption are legalized with **EMAS (Eco-Management and Audit Scheme)** registration and **ISO 14001** certification.

18.4 Intelligent Environment

This section details the architecture for achieving intelligent environment. The anatomy of ‘intelligent environment’ refers to the environment which is intelligent to dynamically adapt with the changes that occurs to it and maintains its actual form. The technology of ‘intelligent car’ refers to the concept that the car that can manage with the road and traffic condition on its own, with a goal to reach the given destination safely. Similarly, anything refers to ‘intelligent object’ should be self-driven to adapt with the changes. In this regard, the ‘intelligent environment protection’ refers to the technology of self-sustainable and self-diagnostic protective system for the

environment with the help of advanced IoT driven sensor network. The IoT based environment sensor network will have the artificial intelligence for detecting the hazards and alert the needful to protect the environment.

In general wireless sensor network (WSN) comprises of diverse sensors with autonomous devices for cooperatively monitoring physical or environmental conditions at different locations. With the advent of IoT technology, the concept of WSN has become very much useful for the long-term environmental monitoring applications. IoT combined with WSN and RFID, has provisioned for quicker deployment for environmental monitoring applications with reliable and long-duration unattended services. The consistent design for environment monitoring is the key for intelligent environment protection system. The four layers of the architecture of '***intelligent environmental eco*-system'** are:

1. Physical Layer
2. Middleware Layer
3. Security Layer
4. Diagnosis Layer

18.4.1 Physical Layer of the IoT Eco-System

The sustainable design of '***intelligent environmental eco*-system'** should cater for economical-hardware, large scale deployment, energy efficiency, uninterrupted and unmanned service feasibility. The physical layer of the '***intelligent environmental eco*-system'** consists of three levels of implementation; sensor level, fog level and cloud level.

At **sensor level**, following guidelines will be essential:

- low-cost, small sensor nodes with self-testing, and error recovery capabilities and on-board processing
- fast and reliable end node deployment procedure
- Energy harvesting sources for end nodes
- Safety measuring devices such as watchdog timers or brown out detector
- In-built self-check for calibration, transducing, RTC
- Choice of communication protocol to suit for periodic messaging of health status and alerts
- Choosing transceiver or transmit only sensors depending on application needs
- Low-duty cycle communication protocol
- Frequency synchronization & calibration to avoid out-of-synchronize communication

Fog/Gateway Nodes

The fog node acts as an inter-mediator between sensor/end nodes and cloud/back end nodes. They communicate using Near Field Communication (NFC) technology

with sensor nodes and use wired/long range wireless communication channel to communicate with cloud nodes.

At fog level, following guidelines will be essential:

- Form factor/size of the fog nodes to suit for variety of applications NFC communication protocol is to optimize the communication with sensor nodes
- MAC protocol to improve the communication reliability
- In case of star topology, consider adequate repeater if required
- Remote configurability for fog nodes to adapt with configuration changes
- Capability with frequent self-checks and fault recovery mechanisms
- Error recovery with data back-up options
- Periodic firm ware update

Cloud Nodes

The cloud nodes process data received from fog nodes. The big data collected from all sensor nodes is stored at cloud nodes. The cloud nodes involve huge data collection, processing and apply analytics for predicting the required events. The cloud nodes are responsible for generating the triggers and alerts as per the requirements of the applications.

At cloud level, following guidelines will be essential:

- Extensible server architecture for easy adaptation to different use cases
- Rules for authentication of fog nodes
- Rules for authentication of sensor data
- Measures for pre-setting the threshold for sensory nodes
- Standard communication protocol between fog and cloud nodes
- API for extreme export/access of current of archived sensory data
- Data visualization capacity for real-time trend monitoring of sensor data
- Cloud based file data management system to manage digital media images/videos

18.4.2 Middleware Layer of the IoT Eco-System

The middleware layer is the sub-architecture for the management of communication protocols, firm-wares and software/tools. RODB (Real-time operational database) is recommended for managing the big-data generated by sensors and fog nodes, and it is also used for managing and archiving of tools, models and knowledge. The goals of the middleware layer is designed according to the end-user application requirements such as delivery of computing resources of end user services, flexibility, scalability, etc.

The middleware layer should provide basic amenities such as transparent connectivity among sensor, cluster and cloud nodes, device management, data collection procedure and provisioning for updates. It also should support for data interoperability among various stake holders. Commercial IoT middleware layer may have additional features such as data analytics tools, data storage, data

visualization and content metering. The self-diagnostic feature of intelligent environment should have a fundamentally strong and reliable IoT middleware platform as its backbone.

18.4.3 Security Layer of the IoT Eco-System

The level of criticality and complexity of the environment monitoring network is high that mandates the need of adapting safety principles in the implementation. Protection methods are classified according to the implementation of chosen application. In any application of IoT, there are basically four aspects of security implementation.

(a) Physical aspects of IoT
(b) Communication aspects of IoT
(c) Networking aspects of IoT
(d) Service aspects of IoT

(a) ***Security for Physical aspects of IoT***

Devices of the IoT eco-system have the limited data processing capacity and data storage resources. The technologies of the IoT devices are RFID/NFC, Bluetooth, ZigBee, LoRa, NB-IoT and 6LoWPAN. RFID technologies are considered as most trusted information exchange for the IoT environment. But due to insufficient authentication mechanisms, contents of the many makes of RFID are not secure. This also leads to attacks on data integrity. Tag cloning, identity attack, eavesdropping, de-synchronization attack, information theft are the popular attacks on RFID devices. In order to protect the RFID based IoT devices, security methods such as RFID-Tate (Sadikin and Kyas 2014), OTP authentication, VLFSR light-weight authentication (Garcia-Alfaro et al. 2015) are recommended. Similarly, Bluetooth based communication has the threats such as sniffing, malware attack, unauthorized direct access (UDDA), and MitM. The 6LoWPAN technology undergoes the security threats such as Sybil attack, Blackhole attack, wormhole attack, clone ID, Synchole attack, spoofing and selective forwarding attacks. The distributed hash table method, Version number and Rank Authentication (VeRA) method, parent-fail-over method and heart-beat protocols are some of the prevention solution for the threats on 6LoWPAN technology.

(b) ***Security for Communication aspects of IoT***

The communication modules are generally vulnerable to MitM attack, tag cloning, and sniffing attacks. In case of mesh networking, wormhole, Blackhole, and DoS/DDoS attacks are prominent ones. In environment monitoring, most of the environmental data are going to be publicly available. Hence, a simple eavesdropping will not be the intent of the adversary. It is advisable to either block the direct

communication between a sensor/end node and cloud backbone to avoid reporting of present situation to cause serious environmental damage (such as forest fire or industrial accident) or deny the communication between cloud backbone and actuator to stop corrective actions (such as emergency evacuation or notification to emergency response teams).

It is really challenging to perform communication layer security algorithm on low cost devices such as end nodes. Lightweight protocol suits are providing various defense mechanisms against these attacks with acceptable level of security grade. A minimal use of TLS/SSL protocols, combined with IDS (Intrusion Detection System) and other authentication protocols can be used to ensure the device identity, which will provide solid defense against most of the common attacks.

(c) ***Security for Networking aspects of IoT***

Networking aspects of IoT eco-system is responsible for data accumulation and data transferring. The traditional security threats of any network layer are applicable to network of IoT. Problems such as data integrity, availability, confidentiality, are common. The most common security challenges are DoS attack, eavesdropping, confidentiality breaches, integrity violation and MitM attacks (Chattha 2014).

(d) ***Security for Service aspects of IoT***

IoT eco-system offers variety of services and hence it is necessary to implement a vertical classification according security breaches with respect to commercial values of IoT applications. The common attacks are Cross site scripting, SQL injection, HTTP flooding, parameter tampering, slowloris attacks and heartbleed, etc., Most of these attacks are already addressed and solutions are available. Unlike the other aspects of IoT eco-system, services of IoT needs proper utilization of existing protocols than any necessity for inventing new ones.

18.4.4 Diagnosis Layer of the IoT Eco-System

IoT eco-system comprises of heterogeneous devices and components with different protocols and technologies. IoT is expected to build millions of applications. With the architecture of IoT eco system as mentioned in Sect. 18.4, any IoT use case can be deployed. However, IoT deployments are not just ‘deploy and go’, but need a continuous monitoring and diagnosis of the system functionalities. There need a periodic firmware updates and software updates. Some devices may fail to respond which need to be repaired or replaced. Some sensors will not give the required readings which may require calibration often.

Monitoring and diagnostics are essential for IoT eco-system to ensure the minimum down-time of any device in the system. Device management is a crucial task. There must be a device management tool hosted at centralized cloud level which can provide useful reports about the health of the multiple devices connected in the

eco-system. Fault diagnosis is the integrated part of monitoring and maintenance. Fault diagnostics will be carried at the each layer of the four layer architecture discussed in Sect. 18.4.

Diagnosis at the Physical layer is related to fault prediction and maintenance of sensors, actuators, smart devices, tags and other end nodes of IoT eco-system. The major concerns at the physical layer diagnosis are scale of sensors, diversity of parameters to be monitored and dynamic workloads according to use case requirements. The data from IoT sensors are associated with common faults such as spike, short comings, nulls, calibration and noise (Sharma et al. 2010). Short-coming kind of faults refers to the deviation in the sensor data from the reference threshold. Spikes are much greater outputs than expected. Null errors are the zero outputs. These kinds of faulty sensor readings require domain experts to correct them. The causes for such errors may be due to battery fluctuation, ADC error, sensor drifts, triggers or sensor malfunctions. A fall-curve based analysis has been proposed in (Chakraborty et al. 2018), that detects the sensor malfunctions. Similarly, the fault diagnostic process has to be different for analog and digital sensors.

Diagnosis at the middleware layer is practiced with the coordination among different agents at the edge computing network of IoT eco-system. The collective responsibility among various cluster heads at edge network is very much essential. There can be a local agent who can derive the fault prediction alarms based on the information collected from physical things and the reliability information from the connected things. The decision making on fault diagnosis at middleware layer will be based on reasoning process.

Assume there is a medical waste reported by local garbage bin. Any standalone garbage bin collection app will not be able to localize and find out which hospital is responsible for this unauthorized dumping of medical waste. When all the database is integrated over IoT enabled intelligent environment platform, the AI engine can be developed at the middleware layer which diagnose the consumption of hospitals with their officially reported medical waste treatment with local government. By collectively searching the discrepancy or inconsistency in the report and hospital consumption, the middleware fault diagnosis agent can locate which hospital is likely to violate the regulations and dumped the garbage over domestic garbage collection bins.

18.5 Protection Policies

The literature on policies for environmental attitudes has focused on socio-economic determinants (Kauder et al. 2017). Three main factors that influence the policies for environmental protection attitudes are:

- Social factors
- Psychological factors
- Political factors

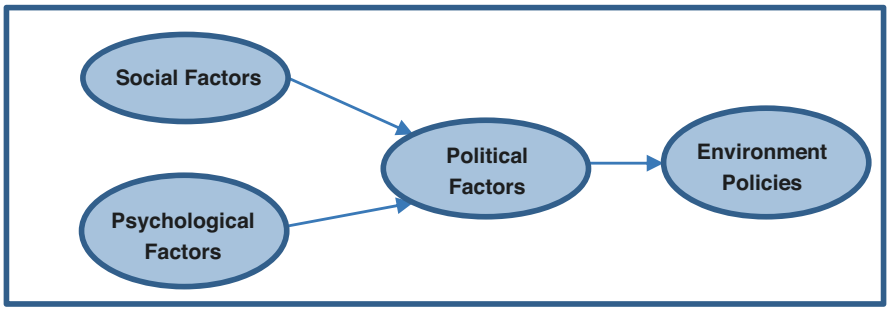


Fig. 18.1 Determinants of environmental policies

In Fig. 18.1, social factor is referring the citizens who believe that environmental problems being solved without government prescriptions and prohibitions. The psychological factor is referring the citizens who believe that environmental problems can be solved by organizing individual agents who interact locally in a self-regulating system administered by suitable rules (Kauder et al. 2017).

However, the combination of both the speculation has to be regularized with political system that will bring the solutions for the environmental pollutions.

There are a many ways to classify policies protect the environment. The basic classification is mandatory & voluntary, while others put into command & control-based and economic-based. The method of environmental protection can be classified into four types: regulatory, voluntary, economic and education & information.

18.5.1 Regulatory Method of Environmental Policy

Regulatory policies enforce legal restrictions on economic agents to realize environmental protection objectives (Hamilton et al. 2018). They are also referred to as "command-and-control" measures, because they prohibit or mandate certain actions. Different forms of environmental regulatory policies are:

- Prohibitions on specified activities such as discharging dyes/waste into water resources.
- Obtaining governmental permit before carrying out a specified activity such as pollution permits, operating licenses.
- Carryout specified actions in the interest of environmentally beneficial (e.g., weed control in agro-lands).

These policies are successful only if the government agencies constantly monitor the compliance and undertake costly litigation when breaches are discovered, The producers of these policy implementations also acquire legal and other costs while abiding with environmental regulations. In addition, regulatory policies do not provide incentives to encourage the reallocation of resources for environmental

benefits or provide any economic value to the individual or the agents who abide by the policies. However, regulatory methods are the best choice to the situations which allow distinct boundaries on the use of environmental resources. It also provides standard procedures for various environmental pollution cases to monitor and mandate norms.

18.5.2 Economical Method of Environmental Policy

Economic method will force agents to pay all or part of the social costs due to harmful activities to the environment. Formularizing the rules for different case of environment hazard is challenging. Problem arises in estimating the threshold of harmfulness and deciding the cost of it.

18.5.3 Voluntary Method of Environmental Policy

Voluntary method is a program in which involvement in this program is voluntary for the sake of environment protection. This program can be organized with or without government support. Voluntary team can work on deriving agreements between the polluters and regulators to protect the environment.

18.5.4 Education & Information Method of Environmental Policy

Information and education method promote environmental protection by creating public awareness. They also support regulator by reporting by pollution events. They conduct campaigns and advertise about protection policies.

18.6 Conclusions

This chapter has discussed the issues of the Mother Nature and different causes that degrade the environment. The limitations of the existing method of environment monitoring are discussed in this chapter. The four-tier architecture to evolve an intelligent environment has been proposed in this chapter. The requirements of robust hardware, middleware and firmware recommended for the architecture of IoT eco-system have been presented. The security procedures to be adhered in network layer and application layer of the architecture are presented in this chapter,

which will promise the secured intelligent environmental protection. This proposed architecture should be protected with the government policies and regulations. The successful deployment of IoT ecosystem is depending upon on the reliable and periodic fault diagnostic system, which is an integrated part of the intelligent environment architecture.

References

Ali, S. A., & Affan, M. et al. (2019). *A study on efficient energy management techniques for cloud computing environment*. 2019 9th International conference on Cloud computing, Data Science & Engineering (Conferences) (pp 13–18)

Al-Masri, E., et al. (2018). Recycle. io: An IoT-enabled framework for urban waste management. In *2018 IEEE International Conference on Big Data (Big Data)*. IEEE.

Alsouda, Y., Pllana, S., & Kurti, A. (2018). A machine learning driven IoT solution for noise classification in smart cities. In *Machine learning driven technologies and architectures for intelligent Internet of Things (ML-IoT)*. Euromicro.

Andersson, P., Whitehouse, P., et al. (2009). Protection of the environment from ionizing radiation in a regulatory context (protect): Proposed numerical benchmark values. *Journal of Environmental Radioactivity, 100*(12), 1100–1108.

Chakraborty, T., et al. (2018). Fall-curve: A novel primitive for IoT fault detection and isolation. In *Proceedings of the 16th ACM conference on embedded networked sensor systems* (pp. 95–107).

Chattha, N. A. (2014). *NFC – Vulnerabilities and defense, Conference on Information Assurance and Cyber Security (CIACS)* (Vol. 1, pp. 35–38).

Cieplak, T., Rymarczyk, T., & Tomaszewski, R. (2019). A concept of the air quality monitoring system in the city of Lublin with machine learning methods to detect data outliers. In *MATEC web of conferences* (Vol. 252). EDP Sciences.

Eswaran, S. P., et al. (2014). Event driven opportunistic communication enabler for smart city. In *2014 Eighth International conference on Next Generation Mobile Apps, Services and Technologies, Oxford* (pp. 313–319).

Eswaran, S. P., et al. (2015). Service driven dynamic hashing based radio resource management for intelligent transport systems. In *Communication technologies for vehicle, Nets4Cars 2015* (Lecture notes in Computer Science) (Vol. 9066). Cham: Springer.

Garcia-Alfaro, J., Herrera-Joancomartí, J., & Melià-Seguí, J. (2015). Security and privacy concerns about the RFID layer of EPC Gen2 networks. In G. Navarro-Arribas & V. Torra (Eds.), *Advanced research in data privacy* (pp. 303–324). Springer.

Gómez, J. A., et al. (2017). A case study on monitoring and geolocation of noise in urban environments using the internet of things. In *Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing*. ACM.

Hamilton, C., et al. (2018). Environmental protection and ecology. In *Encyclopedia of ecology* (2nd ed.). Elsevier Inc.

Kauder, et al. (2017). Behavioural determinants of proclaimed support for environment protection policies. *European Journal of Political Economy*.

Mazanik, A. (2018). Industrial waste, river pollution and water politics in Central Russia, 1880–1917. *Water History, 10*(2–3), 207–222.

McColl, S. T. (2015). Landslide causes and triggers. In *Landslide hazards, risks and disasters* (pp. 17–42). Academic.

Mihindukulasooriya, N., et al. (2016). FarolApp: Live linked data on light pollution. *International Semantic Web Conference (Posters & Demos)*.

Pan, P., et al. (2018). An intelligent garbage bin based on NB-IOT research mode. In *2018 IEEE International Conference of Safety Produce Informatization (IICSPI)*. IEEE.

Sadikin, M. F., & Kyas, M. (2014). RFID-Tate: Efficient security and privacy protection. In *5th international conference on information, intelligence, systems and applications* (pp. 335–340). IISA.

Sharma, A. B., Golubchik, L., & Ramesh, G. (2010). Sensor faults: Detection methods and prevalence in real-world datasets. *ACM Transactions on Sensor Networks (TOSN), 6*(3), 23.

Tran, C. T., & Nguyen, P. Q. P. (2019). Some main causes of marine pollution in Vietnam. *European Journal of Engineering Research and Science, 4*(3), 170–175.

Vambol, S., et al. (2019). The nature and detection of unauthorized waste dump sites using remote sensing. *Ecological Questions, 30*(3), 1–17.

Worku, Y., & Giweta, M. (2018). Can we imagine pollution free rivers around Addis Ababa city, Ethiopia. *What Were the Wrong-Doings*, 2.

Zamorano, J., et al. (2019). Night sky brightness monitoring in Spain. Highlights on Spanish Astrophysics X, *Proceedings of the XIII Scientific Meeting of the Spanish Astronomical Society* held on July 16–20, 2018, in Salamanca, Spain (pp. 599–604).

Chapter 19
A Decade Survey on Internet of Things in Agriculture

Ummesalma M, Rachana Subbaiah M, and Srinivas Narasegouda

Abstract The Internet of Things (IoT) is a united system comprising of physical devices, mechanical and digital machines, and different hardware components like sensors, actuators, cameras etc., monitored and operated by the software. The combination of devices and systems connected over the internet opens the pathway for development of various applications beneficial in terms of economic growth of a nation. IoT has evolved as a potentially emerging computer technology solving various real-life problems and issues. IoT covers vast group of applications, from warfare to surveillance, from habitat monitoring to energy harnessing, predictive analytics and personalized health care, and so on. Among various fields, agriculture is one important field having maximum scope of implementation and investment. The main aim of this book chapter is to furnish all the details related to applications of IoT in the field of agriculture. This includes the details related to data collection, types of sensors used, deployment details, data access through cloud. It also covers details related to various communication technologies used in IoT such as Bluetooth, LoRaWAN, LTE, 6LowPAN, NFC, RFID etc. And above all, the chapter focuses on the significance of IoT on agronomics, agricultural engineering, crop production and livestock production. This chapter is a decade survey conducted to study the contribution of IoT in the field of agriculture. Around 40 research papers for the duration 2008–2018 are collected from peer reviewed journals and conferences. The collected articles are analyzed to provide relevant information required for the various end users.

Keywords IoT · Agriculture · Cloud computing · Precision agriculture · Smart irrigation · Agronomics · Livestock management

Ummesalma M (✉) · Rachana Subbaiah M
Department of Computer Science, CHRIST (Deemed to be University), Bengaluru, Karnataka, India
e-mail: ummesalma.m@christuniversity.in; rachana.subbaiah@mca.christuniversity.in

S. Narasegouda
Department of Computer Science, Jyothi Nivas College (Autonomous), Bengaluru, Karnataka, India

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_19

19.1 Introduction

Food, clothing and shelter are the fundamental requirements of human beings. Man works and earns in order to fulfill his basic needs and to lead a healthy and peaceful life. But even today, not everyone is able to fulfill their basic requirements. According to the latest report of UNO more than 11% of the world's population live below poverty line (United Nations n.d.). UNICEF has treated 2.5 million children for malnutrition in 2017 and in 2018 each. They are estimated to treat 4.2 million children for severe acute malnutrition (SAM) (UNICEF n.d.).

WHO states more than 3.1 million children die because of malnutrition. The traditional and old methods of agriculture fail to fulfill the growing requirement of food across the world. The demand for food is expected to increase by 59% to 98% in less than five decades as considered from 2005 to 2050 (Stat Source: 2018 World fact report; Valin et al. 2014). Thus, it is the need of the hour to make use of emerging science and technologies to fulfill the food and other requirements of human beings. One disruptive technology that can provide solution to various agriculture based problems is Internet of Things (IoT).

IoT is a hybrid technology which connects various devices, softwares and people over internet. IoT has made a remarkable impact on various engineering and industrial sectors. However, many of the economic countries make use of IoT for agricultural applications too. Agricultural IoT (AgIoT) has played a greater role for the promotion of agriculture in many ways.

Some of the major contributions of AgIoT are- collection of agricultural data, construction of agriculture information network, development of agricultural information technology, weather forecasting and efficient usage of natural resources for the improvement of farming. The applications of artificial intelligence, micro and nano technologies, robotics and pervasive computing, ubiquitous network integration, in addition to others have significantly contributed in the development of smart agriculture and precision agriculture. All these technologies and many more falls in the main stream called as Internet of Things (IoT).

The main aim of the AgIoT is to increase the quantity and quality of the crops and other foods to meet the growing demands of the humans. Nevertheless, IoT has myriad applications in the field of agriculture, and some of the major applications include - The crop monitoring system, which has its practical significance as a large-scale application in converting agriculture into a fast-moving industry. Climate monitoring, where the local and global climate changes are monitored and reported to the agriculture departments so that the necessary measures are taken to avoid climatic damages on crops and/or to improve the yield.

The research is carried out world-wide to monitor the growth pattern and environmental parameters of crop growth, impact of climate on the crops and to check the effect of seasonal variations due to global warming so that it provides scientific guidance and counter measures for agricultural production. An environmental parameter model of different regions of crop and growth pattern of different environments can be established to improve the overall efficiency in agriculture.

Precision farming, a novel method carried out using IoT for crop growth, accomplishes a platform for the crop monitoring system with a full-fledged automated or semi-automated digital system that works to monitor the environmental parameter, and collects meteorological and soil information such as temperature, humidity, wind, air, rainfall, soil pH so that each and every minute detail is taken in to consideration and all possible measures are taken to get the maximum yield.

The image capture platform obtains crop growth images. The growth of crops and growing conditions are observed directly. A large number of nodes connected together monitor the crop to identify any abnormalities. This image monitoring systems are useful in assessing the health of the plants, weed identification at its earliest stage and also helps in intruder identification. Since the data is stored in the cloud and is connected via internet this can be monitored with the help of a simple mobile phone.

These are only a few applications of IoT in agriculture. However there are many such applications of IoT revolutionizing the field of agriculture. The main aim of this article is to conduct a decade-long survey and explore such new technological advancements in AgIoT. More than fifty articles collected from peer reviewed journals and conferences are identified, studied and explored in order to draft the survey paper. The articles in the survey are organized into four categories based upon the four main branches of agriculture namely crop production, livestock production, agronomics and agricultural engineering.

Articles related to each of the category are covered and analyzed to provide proper insight to the readers. The structure of survey paper includes introduction as discussed in Sect. 19.1. Preliminaries of IoT and Agriculture are explained in Sect. 19.2. Four-fold literature survey covering the articles from 2009 to 2019 is discussed in Sect. 19.3. Summary on overall view of AgIoT is discussed in Sect. 19.4 which concludes with the future directions in the field of is AgIoT.

19.2 Preliminary Research

19.2.1 Agriculture

Agriculture is the age-old occupation practiced by the man right from the beginning of civilization. It is an applied science involving the study of growing both plants and animals. The practice of growing plants and animals is also called as farming and the person who grows them is called as farmer or cultivator. Farming being the major occupation is practiced all over the world. According to 2005 World Bank report on an average two thirds of the world population spread across the rural areas depends upon agriculture as their major occupation. Based upon the climatic conditions over the geographical area various types of crops are grown.

On the basis of type of food to be grown the farming is further classified as horticulture, pisciculture, horticulture, sericulture, floriculture etc. Irrespective of the

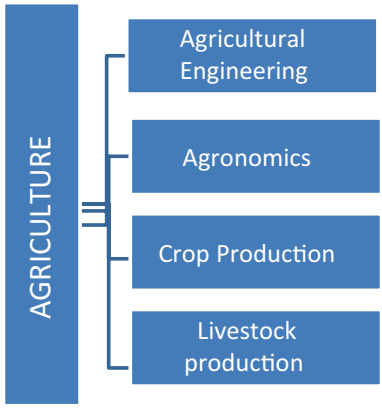


Fig. 19.1 Branches of agriculture

type of agriculture the main aim remains the same, i.e. to fulfill the food requirement of man. Even today agriculture is the major occupation of many countries significantly contributing towards the GDP of the country's economy and farmer is still considered as backbone of a nation. India is one among many such agriculture-based countries. The Sects. 19.2.1.1, 19.2.1.2, 19.2.1.3 and 19.2.1.4 deals with definition of agriculture, branches of agriculture, top 10 agriculture-based economies and technologies contributing to the growth of agriculture respectively.

19.2.1.1 Definition

"Agriculture is the systematic study and practice of growing plants and animals for food and commercial purpose."

19.2.1.2 Branches of Agriculture

There are four main branches of agriculture as given in Fig. 19.1, each having its own significance.

A. Agricultural Engineering: Agriculture engineering is the branch of agriculture which deals with the engineering aspects of agriculture. This includes design, usage and maintenance of agricultural machines, tools and micro and mega structures which reduces the labor and time and increases the productivity of work.
B. Agronomics: Agronomics is the other name of agricultural economics which deals with study of economic significance of agriculture.
C. Crop production: Crop production also known as cultivation deals with growing of plants in a systematic way to produce high yield. The crop grown may be field crops, seasonal crops or perennial crops. Pomology, viticulture, horticulture, olericulture etc., are all part of crop production.

Table 19.1 Agricultural contribution of various countries towards national economy (Shi et al. 2015)

SL. no	Country	Agricultural contribution (in billion USD) towards national economy
1.	China	1117
2.	India	414
3.	USA	185
4.	Brazil	162
5.	Indonesia	141
6.	Nigeria	123
7.	Russia	108
8.	Pakistan	76
9.	Argentina	70
10.	Turkey	64

D. Livestock Production: Livestock production famously recognized as animal husbandry deals with rearing of animals mainly for food purpose. Livestock production includes aqua farming, honey comb rearing, dairy farming, poultry etc.

19.2.1.3 Top 10 Agriculture Based Economies

An agriculture based country is a country whose main source of income comes from agriculture. That is the agricultural sector is the major sector that accounts for its major share in Gross Domestic Product (GDP) of the nation. Among various agriculture based countries, the lists of top ten countries is given in Table 19.1.

19.2.1.4 Technologies Associated with Agriculture

A. Science and technology has made a remarkable impact on the agriculture sector some of the main technologies that contribute in the growth of agriculture are:
B. Biotechnology: Biotechnology is an advanced technology which involves the engineering of organisms, in-vitro fertilization, enzymology tissue culture etc.
C. Tissue culture and genetically modified organisms played a significant role in agriculture where various hybrid crops producing high yield are developed with the help of this technology. E.g.: B.T cotton, B.T rice, B.T. brinjal. Bio-pesticides and bio-fertilizers also provide the protection and nutrition to the crops without causing any harm.
D. Chemical and Pharma technology: Chemical and Pharma technology played a significant role in increasing the resistance of plants and livestock towards microbial disease and increasing their life expectancy. On the other hand chemical fertilizers helped in fulfilling the micro and macro nutritional requirements

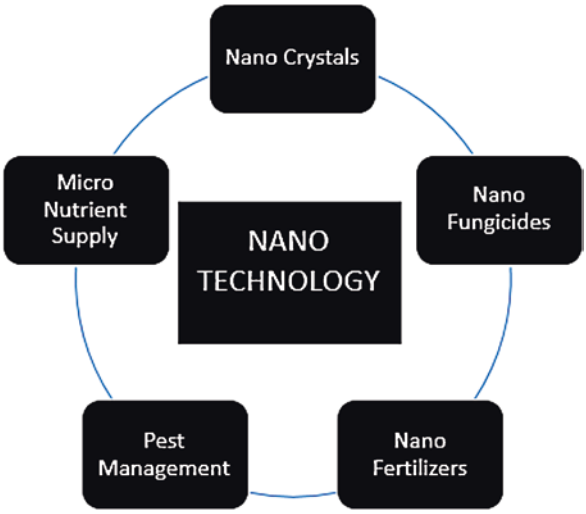


Fig. 19.2 Applications of nanotechnology in agriculture

of the plant. It is because of the contribution of pharma technology livestock are immune from Foot and mouth disease.

E. Information technology: Information technology is the revolutionary technology of twentieth century. E-commerce, E-agriculture, M-agriculture, agricultural databases etc. facilitated the farmers by providing the answers to their queries in few seconds and bringing information on their fingertips. Various farming softwares and apps provided information to learn new things pertained to agriculture. Information technology also contributed in community involvement and helped small and big farmers in better planning and decision making,
F. Nanotechnology: Nanotechnology is the technology which deals with the materials at molecular, i.e. at nano, level. The agricultural contribution of nanotechnology includes nano-fertilizers, nano-pesticides, nano-crystals, and nano-sensors, which are more efficient than many of the chemical fertilizers. The main advantage of nano materials is strength and efficiency because of their size. Some of the applications of nanotechnology in the field of agriculture are given in Fig. 19.2.

Among the various types of technologies facilitating the growth of agriculture, Internet of Things is an emerging disruptive technology which has the potential to revolutionize the agricultural sector. The entire article revolves around agriculture and IoT. Thus the Sect. 19.2.2 deals with general framework of IoT, its challenges and its applications.

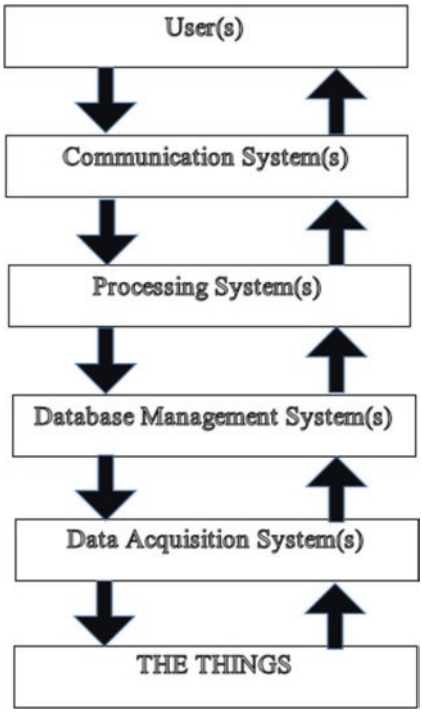


Fig. 19.3 General framework of IoT

19.2.2 IOT

Internet of Things popularly called as IoT is an emerging technology which has a wide range of applications from education to research from warfare to social welfare, and from oceans to sky. Every walk of human life is touched by this disruptive technology. IoT is not a single technology, but is an amalgamation of various technologies, devices and people connected over the internet. It is a giant network connecting people and devices and bringing transformation in all applied fields. Study of IoT involves machine learning, data analytics, data communication, artificial intelligence, robotics etc. The name "IoT" was suggested by Kevin Ashton of Procter & Gamble, in 1999. The main aim of IoT was to solve the complex real-world problems that require well defined sophisticated solutions. The general framework of IoT is shown in Fig. 19.3.

19.2.2.1 Definition

Rouse Margaret first introduced the concept of The **Internet of Things**, or **IoT**, and is defined as **"**a full-fledged system of interrelated computing devices which include sensors, electrical and mechanical devices, analog and digital machines;, real world objects, like animals, plants and people with unique identifiers (UIDs); and the

capacity to transmit the data through a well-defined network without or very minimal human-to-human and/or human-to-computer interaction."

19.2.2.2 Framework

The general framework of IoT is given in Fig. 19.2. However, same framework is to be followed for agricultural applications.

The IoT framework comprises all the people, plants, animals, devices, buildings etc. properly termed as THE THINGS, and specific systems for data sensing, communication and management bonded by APIs connected with internet. The end user receives the result either in the form of text, image, sound or any other desired format on their devices.

The working of the IoT framework involves the following four major systems:

- Data Acquisition system
  The process of acquiring the data is called as data acquisition system (DAS). In IoT data acquisition is done through the sensors/actuators or other devices like camera, mics, satellites etc. In order to sense the data, the sensors should be deployed as per the requirement(s). The sensors can be just mounted on the hardware or immersed inside water or soil, again, as per the requirements. A continuous stream of data is collected on a regular basis which is stored in the databases for further analysis.
- Data management system
  The process of management of the data is called as data management system (DMS). Data management deals with data aggregation, data storage, and data retrieval. In DMS data aggregation takes place by interacting with DAS. The data from various homogeneous and/or heterogeneous environment are aggregated at database server (personal or cloud based) and sent further for processing (Alam et al. 2013; Alam 2012a, b; Alam and Shakil 2013; Shakil and Alam 2016). For data management and data processing various application interfaces (APIs) are required for connecting various data sources and softwares. Whereas for sending and receiving the data a gateway is required. The communication system is responsible for handling the gateways.
- Data Processing system
  Data processing involves data computation where many machine learning and artificial intelligence algorithm are involved. However before the actual processing various pre-processing tasks are to be performed which depends upon the application. The computation takes place usually at server side. But, as the data becomes huge the feasible option is to use cloud based services. The main aim of processing system is to provide data prediction, analysis and visualization beneficial to the end user.

- Data communication system
  Data communication system involves protocols, topologies, algorithms and devices used to build a well-defined communication network. Data security is an integral part of the communication system where it involves implementation of encryption algorithm to secure the data communicated over the network. The medium for data communication can be wired or wireless. The choice of the medium of communication depends upon the application and investment cost. Some of the major communication technologies used in IoT are Bluetooth, Infrared, Ethernet, Wi-Fi, Li-Fi, RFID, Satellites, LoRWAN, 6LoWPAN etc. Out of many options available for communication, LoRWAN for wide area coverage and 6LowPAN for personal area coverage. Because of their efficiency and wide coverage they have emerged as the widely used communication technologies in recent times. The data rate of LoRWAN range between 2.5 and 5.5 kbps, whereas, 6LoWPAN has a data rate of 250 kbps.

  The processed data is communicated to the devices of the end user either in the form of text, images, signals or in any other desired formats based upon the requirement. Users also have the privilege to control and monitor the IoT system through their devices. The communicating device which is widely used by the users to access the information, to monitor as well as control the features, is smart phone.

19.2.2.3 Issues and Challenges

This section deals with general issues and challenges of IoT which is applicable to all fields including agriculture. The major concerns related to IoT are as follows:

(a) Handling big data sensed by various sensors: Sensors generate huge stream of continuous data. Storing processing and retrieving big data is always a computationally expensive task and is one of the major challenge. The solution to address this challenge is the usage of cloud technology.
(b) Dealing with different hardware (sensors and devices): Since IoT is a collection of variety of devices investment, maintenance and communication with different devices distributed over different networks is always a tedious task.
(c) Dealing with different communication protocols: Different networks follow different protocols, handling mixture of protocols is the biggest challenge in any IoT based system.
(d) Data security: Data transmitted over internet has always threat of getting breached. When there is a mixture of networks following different protocols, the chance of malicious access of data becomes high. Thus, data security issue is one of the major concerns, especially when the data transmitted is financial or medical.

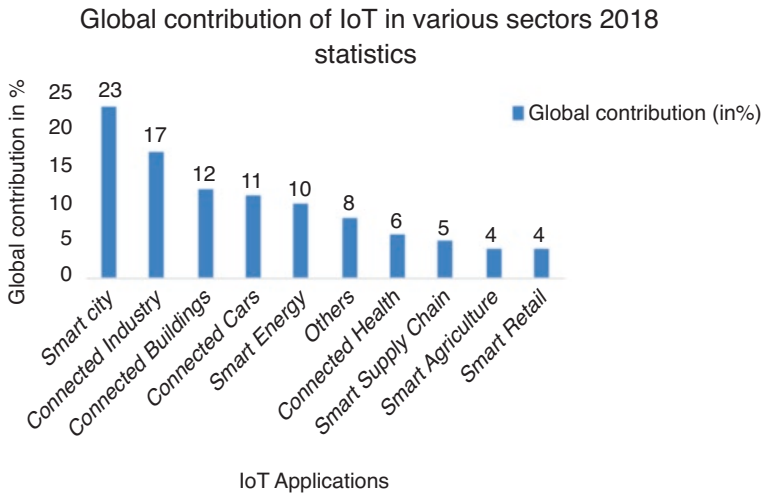


Fig. 19.4 Top 10 applications of IoT. (Image Source: IoT analytics 2018 global overview of 1600 enterprises IoT use cases)

(e) Uninterrupted power supply: In order to communicate with devices continuously an uninterrupted power supply is must. It is difficult to manage the power resources due to lack of power source especially in the rural area.
(f) Cost: A lot of cost is involved in terms of setting up an IoT system. The cost is associated with purchasing devices, communication medium, topology setting, implementation of communication protocols, ensuring data security, investment in databases, cloud services and softwares. Thus, cost is the major concern in setting up of IoT system for any application.

19.2.2.4 Applications

IoT is a disruptive technology having wide range of applications with some of the major applications across the world being given in Fig. 19.4. Figure 19.4 clearly indicates that among all applications, agriculture is at 9th position with only 5% of usage across the globe. According to 2018 statistics it is claimed that majority of the IoT based applications are implemented by the USA. Even though the global recognition of IoT in the field of agriculture ranks at 9th position, recent studies claim that there are numerous applications of IoT in agriculture which are worth implementing to improve the agronomics of the nation. The main aim of this article is to review the same, thus a decade survey on application of AgIoT is discussed under Sect. 19.3.

19.3 Literature Survey

IoT has myriad applications in the field of agriculture, for the purpose of organization the survey from 2009 to 2019 is categorized into four categories based upon the branches of agriculture as discussed above in the Sect. 19.2.

19.3.1 Crop Cultivation

The traditional soil examining and lab investigation is a tedious and costly task. It doesn't provide details related to soil diseases, depletion of nutrients like phosphorus and concentration of micro nutrients. It also fails to give the accurate quantities of dissolved salts. On the other hand the advancement of proximal soil sensors works efficiently for enhancing the comprehension of soil changeability. Regarding this issue, a review has been done by (Lobsey et al. 2010) to study the electrochemical sensors in developing proximal soil nutrients.

In the course of the most recent decade, compact, dynamic, active optical sensors (AOS) have progressed toward becoming devices for horticulture both for mapping products and soils and furthermore to apply agrochemicals. Unfortunately, only few people know how these sensors work. Hence, the authors of (Holland et al. 2012) have invested their time and resource to study, document, and create a mathematical model for the active optical sensors and their impact.

In an area of 5000 m^2, 27 temperature and 135 soil sensors were deployed in an apple orchard to study the impact of soil moisture on soil in terms of both time and space dimensionality. The wireless sensor network (WSN) deployment to collect the soil moisture information helped in exploring the hydrological processes (Majone et al. 2013).

The authors of (Kassim et al. 2014), proposed a WSN as the most ideal approach to take care of the horticultural issues. Utilizing the essential standards of Internet and WSN innovations for building a full-fledged horticulture framework is described in detail. Main topics covered in this article includes details related to equipment engineering, organization, design and programming, process control, and maintenance of the accuracy of water system framework.

The development of an internet based agriculture application which uses the knowledge and monitoring details to provide the useful information to the farmer was proposed by (Mohanraj et al. 2016). In this approach, authors suggested that the application collect the real time information such as production quantity, market price, and provide the same to the farmers who then take the appropriate decision.

India is an agriculture-based country where 70% of the people come from rural area depend upon the income from agriculture sector. The agriculture sector in India is contributing nearly one third of the nation's income. In order to improve the quality of life among the citizens, the increase in agriculture income is a must. Traditional farming is not providing enough income because of change in weather seasons.

Hence, one cannot depend upon only the traditional techniques in farming. Usage of technology can help in increasing in agriculture production. And this can be achieved by practicing the smart agriculture. The smart agriculture depends upon many factors such as using global positioning system in robots to do the task related to agriculture. Robots can be used to do many task such as providing security of crops from animals, birds and intruders;, monitoring of moisture, spraying, weeding, and so on. Once the crop is ready, protection of crops is also very important and it can be achieved by developing smart storage houses. All these operations can be operated remotely by using the smart devices with the help of IoT (Gondchawar and Kawitkar 2016).

Cloud computing technology provide users many computing resources as per their requirements on a pay-per-use basis. IoT on the other hand is used to collect the information, process, analyse and help in decision making. Now in many applications, cloud and IoT are combined to provide more sustainable applications in which IoT is used to collect the information and cloud is used for computation purposes. However, there are many challenges, and issues which, need to be addressed (Sasikumar and Priya 2017).

Smart farming is one of the best ways to increase the productivity of agricultural goods and get more profits. But there are millions of farmers who are unaware of this technology and they are still relaying on the traditional techniques. To help farmers, an IoT based model (Kothiya et al. 2018) was developed which was collecting information about soil moisture, temperature, humidity, intruders in the field and so on, and which gives the same information to the farmers. Farmers were then take the decision based on the information. The model also had the feature of making operating electric motors in the farm land automated.

19.3.2 Livestock Production

Smart feeding can be implemented using IoT. In smart feeding, IoT devices are used to monitor the grains' quality and quantity (Agrawal et al. 2016).

Poultry farm is being maintained by many people because of its low maintenance and high profit margins. In poultry, huge number of animals are maintained to minimize the cost effectiveness. However, this could be very problematic and catastrophic if any bird gets infected and that infection start spreading. In such cases monitoring of birds can play an important role in early detection of diseases, which in turn, could lead to proper medical treatment to minimize the loss (Balachandar and Chinnaiyan 2018).

Sheep farming is quite a profitable profession. In the vineyards, sheep farming has to be done very carefully because if neglected, then the sheep may eat fruits. Hence monitoring and controlling of sheep is required and it can be achieved using SheepIT project which uses WSN. In this project, apart from monitoring and controlling, the sheep activities are also noted to use the data to improve the project (Nóbrega et al. 2019). The deployment of WSN require the devices to communicate

with each other which means machine to machine communication/interaction. Hence, the SheepIT project was further studied and implemented to increase the efficiency in the communication module of the project (N'obrega et al. 2019).

19.3.3 Agronomics

Information has become very crucial in today's world. Anyone with the information can use it to make his/her life easier, and may even use it for developing new equipment. Further, the concept of open source is proving to be a life line. Using the open source anyone without any formal education can build IoT, cloud, or mobile application. Many people are developing application related to agriculture to help farmers (Dlodlo and Kalezhi 2015).

An architecture to automate the agricultural processes using IoT and servers was proposed in (Deksnys et al. 2015). The task of data acquisition and processing is done at IoT level. Since the processing at IoT is limited, the throughput of the sensors-OPC UA server is investigated. Most of the apps provide farming based information. However, there are some of the apps that provide agronomics-based information. Agronomics involves precision agriculture (also called as precision farming) at the cultivation level, and predictive analytics at the computation level.

Precision farming is all about first collecting the available data such as moisture in the soil, chemicals in the soil, pH level, nitrogen level, temperature, humidity, wind speed, CO2 concentration, climate change, and rainfall, and then analyzing the data to optimize the available resources to maximize the agricultural productivity. Precision farming can be more effective if we use historical data to analyze and provide strategy for decision making. Many researchers have proposed several techniques for precision agriculture and detailed information of such techniques is provided in (Kushwaha and Raghuveer 2017). The precision making is crucial not only for farmers but also for agronomist who are meant for the study of agricultural economics. The agronomists with the help of predictive analytics build a decision support system. This system propose the strategic plan for improving the economy of the country by investing in various industrial and economic sectors associated with agriculture. The agronomists also formulate sales and marketing strategies to increase the profit from agriculture.

Agricultural information technology (AIT) is playing a very important role in farmers' life to make their lives better. The information provided by AIT is very crucial in decision making of agronomy. In this regard, strategic details about designing and building of management information system related to agriculture is discussed in Yan-e (2011).

After carefully studying the traditional methods used in the agriculture, the limitations and drawbacks in existing agriculture system were identified. Lack of market knowledge, lack of awareness related to new technologies to improve agriculture, lack of information on the current condition of soil health, unknown future climatic changes etc., are some of the main setbacks of the existing agriculture system. To

overcome the problems, inefficiencies, and setbacks related to AgIoT an IoT based Supply Chain Operation Reference (SCOR) mode of agriculture method was proposed (Mo 2011). In this model predictive analytics was used to enhance the supply chain model on agricultural products.

19.3.4 Agriculture Engineering

Agriculture vehicles have important roles to play both on field and off the agriculture field. The main goal of providing a navigation is to ensure that when the vehicle is moving on the farm land it doesn't run over the crop. This can be achieved by using the vision sensors, gyroscope, and GPS. GPS helps to identify the location, vision sensors provides the visual details and gyroscope helps to maintain the angle and direction of trajectory (Zhang et al. 1999).

The world population is increasing and so is the demand for food. But the quantity of land available for cultivation is not increasing. In fact it is decreasing day by day. This has motivated the researchers to look for the solution through agronomy which can use the available land and produce higher quantity of food by using the latest available technology. As a result, more and more fertilizer, pesticides were used. This has resulted in creating another problem of contamination of food, soil, ground water, and rivers. Through consumption of such contaminated food, the chemicals have entered human body. This has to be controlled and removed from our eco system. In this regard the first step is to identify such microbes and remove them. The Nano technology can play an important role to achieve this objective. The nanotechnology can provide sensors which can sense such nano materials. Using nano sensors, microbes can be identified and removed from the food, soil, and water (Baruah and Dutta 2009).

Different types of vehicles are used in agriculture as these are required in doing many tasks. The automation of vehicles can save time and energy of farmers but automation of vehicles is a very difficult task. In order to make any vehicle automated many factors are needed to be considered such as navigation, routing, dead end detection and so on. Apart from this, vehicle should be able to collect the information, process the data and act accordingly. For these tasks there are many sensor devices and technologies which are available such as global positioning system for routing, sensors for directions, machine vision. Once the data is collected, computation is done to extract the features and finally algorithms are used to control the vehicles movement and to do the necessary tasks. A prototype has been developed by (Li et al. 2009) but it is yet to be commercialized.

In the twenty-first century, imagining the life without using the cloud computing and internet of things is almost impossible. Our life is connected to these two technologies in one or the other way. These two technologies have made human life easier and luxurious. There are many application domains where these two technologies are used, and agriculture is no different. Both the technologies have their own advantages. By combining the two technologies creating CloudIoT paradigm

may serve the agriculture sector more efficiently than using cloud or IoT alone. Hence, many researchers have developed techniques using CloudIoT to help farmers to increase the productivity of the crops (Bo and Wang 2011).

The monitoring system of precision agriculture is very important in getting a precise and accurate result. A WSN application of monitoring was developed by (Liqiang et al. 2011) consisting of both hardware and software. Apart from the tiny OS, the software also has an energy saving module to save the sensor energy and increase the life time of the WSN. The proposed monitoring model adopted the collection tree protocol for collection and sending the data to the base station for further analysis.

The government, industry, and the academicians all are promoting the use of IoT in agriculture to increase the agricultural productivity. The promotion of idea of using IoT in agriculture is done through detailed analysis of IoT technology which includes electronic product code, radio frequency and so on. After detailed analysis of key technologies involved in IoT, an agriculture application using IoT has been proposed in (Chen and Jin 2012).

Water management is a very difficult task for the farmers due to shortage of water. However, using the information regarding the soil can be used to manage the water requirement. In this regard WSN application with a central node ZigBee connected to a Central Monitoring Station can be used. Sensors in the WSN sense and collect the information such as the soil moisture, temperature, humidity and send it to the monitoring station. For communication purpose, GPRS or GSM technologies is used. Farmers can use the information available in the monitoring station to evaluate the soil condition and take the decision accordingly (Satyanarayana and Mazaruddin 2013).

Along with many countries including India, China's agriculture sector is traditional and needs to be made modernized. The use IoT, Machine to Machine telemetry (M2M), Service Orient Architecture (SOA), Radio Frequency Identification and Detection (RFID), and cloud computing can be used together to solve many agriculture related problems and make China's agriculture sector modernized (TongKe 2013). China is the top most country to use M2M technology to its maximum.

Disease and insects are the major concern for the farmers. Monitoring of the entire farm is very difficult and if early detection of disease and insects were not identified then it can turn into a disaster. Use of IoT can be very helpful in monitoring and early detection of disease and insects. Monitoring of the farm using IoT is very feasible and easy option for the farmers. A detailed information of how IoT can be used and what are its role is given in (Shi et al. 2015).

Precision agriculture has been used in many developed and developing countries to increase the productivity in the agriculture sector. But India is still far behind in using key technologies such as IoT, cloud computing, data science to help farmers to utilize it. All these key technologies could be used to develop a mobile based AgroCloud module which can monitor all the details such as soil analysis, market requirements, current stock production, agro governance, and can be used to provide best strategy to the farmers. In order to utilize AgroCloud module, all the stake

holders such as farmers, marketing and sales, and governance related people must become part of it (Channe et al. 2015).

Nano technology is proving to be an outstanding performer in many industrial applications. But despite being the next generation technology, its use in agriculture is still very limited. Many people believe that the investment in nano technology in agriculture may not be feasible and believe that return is very low because of which industrial people are taking steps in this direction cautiously. On the other hand many people believe that nano applications in agriculture will return a good profit in the long term (Parisi et al. 2015).

Farmers are the end users of IoT in agriculture sector and their demand is that the technology should be easy to use and maintain, cost effective, and more importantly it should be non-destructive. If these criteria are met then the farmers will be willing to use IoT for continuous monitoring of soil quality, to monitor changes in chemical and physical characteristics of crops, to keep track of climatic changes etc. so that if there is any problem then it would be identified in the early stage and appropriate action might be taken to minimize the loss and to increase the productivity of the crops. In this regard a detailed survey of recent technologies used in the agriculture sector has been done (Cozzolino et al. 2015).

An IoT, cloud, mobile based monitoring system was proposed in (Vani and Rao 2016). Low cost sensors for sensing soil moisture are used to collect the information. The collected information is then uploaded to the cloud where the analysis is done. And finally, the results are provided through a mobile application to the end user.

Latest technologies such as remote sensing and, satellite images, are used to analyze and come up with a strategy to increase the productivity in the agriculture sector. Many researcher have proposed how satellite images and remote sensing can be used and a detailed survey can be found in (Wójtowicz et al. 2016).

Precision agriculture is one way of increasing the quality of crops and productivity by optimizing the available resources using the IoT. IoT is used to collect all the details and cloud can be used for computation purpose for analysis of the data. Once the analysis is done, the results can be used for decision making to increase the efficiency of the precision agriculture (Khattab et al. 2016).

Water is becoming a scarce resource and it is affecting the agriculture sector very seriously. One of the best way to deal with it is to use smart irrigation techniques in which soil humidity is calculated so that only required amount of water can be used for irrigation. Apart from this, humidity, soil quality, and pH level reading can also be collected to analyze and decide which crop is best suited for irrigation to get more profit and how much fertilizer is required (Parameswaran and Sivaprasath 2016).

The excess use of chemicals has damaged the soil, crop, and environment. One way of dealing with it is to use the nano-encapsulated pesticides, fertilizers, and other chemical on the plants to provide necessary nutrition without effecting the environment. A detailed discussion of how nano technology can benefits in the precision agriculture is discussed in (Duhan et al. 2017).

The authors of (Karim and Karim 2017), proposed a WSN as the most ideal approach to take care of the horticultural issues identified with cultivating assets.

Utilizing the essential standards of Internet and WSN innovation, exactness horticulture frameworks in light of the web of things (IOT) innovation is clarified in detail particularly on the equipment engineering, organize design and programming process control of the accuracy water system framework.

The most important technology that the twenty-first century has produced is wireless sensor network and internet of things. Both these technologies are playing an important role in many applications across many fields. One such application is monitoring the greenhouse system. Traditionally, greenhouses are monitored by laying cables to monitor the climate in greenhouses in different parts of the greenhouse. But usage of cables is very expensive, it requires high maintenance, and in case of relocating it is very difficult. However, this could be avoided if we use MicaZ nodes for monitoring the greenhouse. The deployment of sensor networks doesn't require the cabling hence avoids all the problems which come with cabling. The deployed sensor network could be used to monitor and control the greenhouse environment such as temperature, humidity, light, and pressure. And, IoT makes sure that farmers can actually control the entire system through the mobile app from anywhere (Akkaş and Sokullu 2017).

19.4 Conclusion

The article entitled- A decade survey on IoT in agriculture is intended to provide the details related to contribution of IoT in the field of agriculture. Information from around 40 articles from various peer reviewed journals and conferences are analyzed to provide an insight on four main branches of agriculture namely agronomics, agricultural engineering, crop production and livestock production.

The agronomics deals with agricultural economics using IoT. Here precision farming and predictive analytics play a major role. Precision farming works at the ground level where the main aim is to increase the yield of the crops by carefully monitoring the minute details such as pH, temperature, amount of water and fertilizers required for the specific yield. On the other hand predictive analytics is used to predict the future rainfall, future yield, future sales etc. The combination of precision agriculture and predictive analytics helps the agronomists not only to formulate the strategies but also in efficient decision making. The ultimate of agronomists is to increase the GDP of the country though agriculture.

Agricultural engineering deals with usage of machines in the field of agriculture. AgIoT make use of drones, robots, automated vehicles for seeding, ploughing and harvesting. M2M telemetry is used to communicate between two or more machines which are the part of an IoT system. With the help of IoT in agricultural engineering many solutions for the problems like disease identification intruder detection, conduction of smooth and fast harvesting has been proposed.

There are myriad applications of AgIoT in terms of crop production and livestock production which include health analytics where the health of crops and animals is monitored, identification of livestock using RFID tags, smart irrigation,

smart greenhouse using efficient methods such as MicaZ, sheep IT for monitoring of Sheep at vineyards etc. It also include water management, weed control, crop protection etc. Section 19.3 also reveals that the issues related to big data, communication and security can be resolved using cloud services and advanced communication technologies like LorWan, Zigbee, Sigfox etc.

This research identifies potential applications of AgIoT for sustainable agricultural growth. It also reveals the business benefits that can be derived from IoT. The survey reveals that business benefits can be reaped maximum by domains like floriculture, viticulture, apiculture, pomology etc., as these domains are more important at global market for exporting. AgIoT also contributes to various allied fields such as water management, weather forecasting, wildlife management, finance, forestry, plant and animal disease identification, transport and storage of agricultural produce, extension services, etc.

As the future directive the survey projects various applications of AgIoT adoption of which can contribute to rural development in emerging economies. The study can also be utilized by developers of new IoT technologies to build country-specific technologies based on the various identified applications. The strength and spread of IoT reveals that its contribution in various fields mainly in agriculture can contribute in fulfilling the basic needs and play a major role in poverty alleviation and uplifting the standards of the people.

References

Agrawal, H., Prieto, J., Ramos, C., & Corchado, J. M. (2016). Smart feeding in farming through IoT in silos. In J. Corchado Rodriguez, S. Mitra, S. Thampi, & E. S. El-Alfy (Eds.), *Intelligent systems technologies and applications 2016. ISTA 2016. Advances in intelligent systems and computing* (Vol. 530). Cham: Springer.

Akkaş, M. A., & Sokullu, R. (2017). An IoT-based greenhouse monitoring system with Micaz motes. *Procedia Computer Science, 113*, 603–608.

Alam, M. (2012a, October 26–28). Cloud algebra for cloud database management system. *The second international conference on Computational Science, Engineering and Information Technology* (CCSEIT-2012), Coimbatore, India, Proceeding published by ACM.

Alam, M. (2012b, December). Cloud Algebra for handling unstructured data in cloud database management system. *International Journal on Cloud Computing: Services and Architecture (IJCCSA)*, *2*(6), ISSN: 2231-5853 [Online]; 2231–6663 [Print], https://doi.org/10.5121/ijccsa.2012.2603, Taiwan.

Alam, M., & Shakil, K. A. (2013). Cloud database management system architecture. *International Journal of Advances in Computer Science and its Applications*, *3*(1), 27–31, Universal Association of Computer and Electronics Engineers (UACEE), ISSN:2250–3765, Australia.

Alam, B., Doja, M. N., Alam, M., & Malhotra, S. (2013). 5-layered architecture of cloud database management system. *AASRI Procedia Journal, 5*, 194–199, ISSN: 2212-6716, Elsevier.

Balachandar, S., & Chinnaiyan, R. (2018). Internet of Things based reliable real-time disease monitoring of poultry farming imagery analytics. In *Proceeding of the international conference on computer networks, Big data and IoT (ICCBI – 2018). ICCBI 2018. Lecture notes on data engineering and communications technologies* (Vol. 31). Cham: Springer.

Baruah, S., & Dutta, J. (2009). Nanotechnology applications in pollution sensing and degradation in agriculture: A review. *Environmental Chemistry Letters, 7*(3), 191–204.

Bo, Y., & Wang, H. (2011, May). The application of cloud computing and the internet of things in agriculture and forestry. In *Service Sciences (IJCSS), 2011 International Joint Conference on* (pp. 168–172). IEEE.

Channe, H., Kothari, S., & Kadam, D. (2015). Multidisciplinary model for smart agriculture using internet-of-things (IoT), sensors, cloud-computing, mobile-computing & big-data analysis. *International Journal of Computer Technology & Applications, 6*(3), 374–382.

Chen, X. Y., & Jin, Z. G. (2012). Research on key technology and applications for internet of things. *Physics Procedia, 33*, 561–566.

Cozzolino, D., Porker, K., & Laws, M. (2015). An overview on the use of infrared sensors for in field, proximal and at harvest monitoring of cereal crops. *Agriculture, 5*(3), 713–722.

Deksnys, V., Jaruevicius, I., Marcinkevicius, E., Ronkainen, A., Soumi, P., Nikander, J., ... & Andersen, B. (2015, September). Remote agriculture automation using wireless link and iot gateway infrastructure. In *Database and Expert Systems Applications (DEXA), 2015 26th international workshop on* (pp. 99–103). IEEE.

Dlodlo, N., & Kalezhi, J. (2015, May). The internet of things in agriculture for sustainable rural development. In *Emerging Trends in Networks and Computer Communications (ETNCC), 2015 International conference on* (pp. 13–18). IEEE.

Duhan, J. S., Kumar, R., Kumar, N., Kaur, P., Nehra, K., & Duhan, S. (2017). Nanotechnology: The new perspective in precision agriculture. *Biotechnology Reports, 15*, 11–23.

Gondchawar, N., & Kawitkar, R. S. (2016). IoT based smart agriculture. *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), 5*(6), 177–181.

Holland, K. H., Lamb, D. W., & Schepers, J. S. (2012). Radiometry of proximal active optical sensors (AOS) for agricultural sensing. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, 5*(6), 1793–1802.

Karim, F., & Karim, F. (2017). Monitoring system using web of things in precision agriculture. *Procedia Computer Science, 110*, 402–409.

Kassim, M. R. M., Mat, I., & Harun, A. N. (2014, July). Wireless sensor network in precision agriculture application. In *Computer, Information and Telecommunication Systems (CITS), 2014 International Conference on* (pp. 1–5). IEEE.

Khattab, A., Abdelgawad, A., & Yelmarthi, K. (2016, December). *Design and implementation of a cloud-based IoT scheme for precision agriculture*. In Microelectronics (ICM), 2016 28th International Conference on (pp. 201–204). IEEE.

Kothiya, R. H., Patel, K. L., & Jayswal, H. S. (2018). Smart farming using Internet of Things. *International Journal of Applied Engineering Research, 13*(12), 10164–10168.

Kushwaha, M., & Raghuveer, V. R. (2017). Survey of impact of technology on effective implementation of precision farming in India. *International Journal on Recent and Innovation Trends in Computing and Communication, 5*(6), 1300–1310.

Li, M., Imou, K., Wakabayashi, K., & Yokoyama, S. (2009). Review of research on agricultural vehicle autonomous guidance. *International Journal of Agricultural and Biological Engineering, 2*(3), 1–16.

Liqiang, Z., Shouyi, Y., Leibo, L., Zhen, Z., & Shaojun, W. (2011). A crop monitoring system based on wireless sensor network. *Procedia Environmental Sciences, 11*, 558–565.

Lobsey, C. R., Rossel, R. V., & Mcbratney, A. B. (2010). Proximal soil nutrient sensing using electrochemical sensors. In *Proximal soil sensing* (pp. 77–88). Dordrecht: Springer.

Majone, B., Viani, F., Filippi, E., Bellin, A., Massa, A., Toller, G., et al. (2013). Wireless sensor network deployment for monitoring soil moisture dynamics at the field scale. *Procedia Environmental Sciences, 19*, 426–435.

Mo, L. (2011, August). A study on modern agricultural products logistics supply chain management mode based on IOT. In *Digital Manufacturing and Automation (ICDMA), 2011 Second international conference on* (pp. 117–120). IEEE.

Mohanraj, I., Ashokumar, K., & Naren, J. (2016). Field monitoring and automation using IOT in agriculture domain. *Procedia Computer Science, 93*, 931–939.

N'obrega, L., Goncalves, P., Pedreiras, P., & Pereira, J. (2019). An IoT-based solution for intelligent farming, sensors, *19*(3), 603, 2019, Multidisciplinary Digital Publishing Institute.

Nóbrega, L., Pedreiras, P., & Gonçalves, P. (2019). SheepIT, an IoT-based weed control system. In M. Salampasis & T. Bournaris (Eds.), *Information and communication technologies in modern agricultural development. HAICTA 2017. Communications in computer and information science* (Vol. 953). Cham: Springer.

Parameswaran, G., & Sivaprasath, K. (2016). Arduino based smart drip irrigation system using Internet of Things. *International Journal of Engineering Science,* 5518–5521.

Parisi, C., Vigani, M., & Rodríguez-Cerezo, E. (2015). Agricultural nanotechnologies: What are the current possibilities? *Nano Today, 10*(2), 124–127.

Sasikumar, V., & Priya, S. (2017). IOT applications for Indian based farming and hospitality industry. *International Journal of Advance Research, Ideas and Innovations in Technology, 3*(4), 739–745.

Satyanarayana, G. V., & Mazaruddin, S. D. (2013). *Wireless sensor based remote monitoring system for agriculture using ZigBee and GPS*. In Conference on Advances in Communication and Control Systems (vol. 3, pp. 237–241).

Shakil, K. A., & Alam, M. (2016, December). Recent developments in cloud based systems: State of art. *International Journal of Computer Science and Information Security (IJCSIS)*, *14*(12), 242–258, ESCI, Thompson Reuter. ISSN: 1947-5500.

Shi, Y., Wang, Z., Wang, X., & Zhang, S. (2015, August). Internet of things application to monitoring plant disease and insect pests. In *International conference on Applied Science and Engineering Innovation* (ASEI 2015) (pp. 31–34).

TongKe, F. (2013). Smart agriculture based on cloud computing and IOT. *Journal of Convergence Information Technology, 8*(2).

UNICEF. (n.d.). https://www.unicef.org/publications/files/UNICEF_Humanitarian_Action_for_Children_2018_Overview_ENG.PDF

United Nations. (n.d.). https://www.un.org/en/sections/issues-depth/poverty/

Valin, H., Sands, R. D., Van der Mensbrugghe, D., Nelson, G. C., Ahammad, H., Blanc, E., Bodirsky, B., Fujimori, S., Hasegawa, T., & Havlik, P. (2014). The future of food demand: Understanding differences in global economic models. *Agricultural Economics, 45*(1), 51–67, Wiley Online Library.

Vani, P. D., & Rao, K. R. (2016). Measurement and monitoring of soil moisture using cloud IoT and android system. *Indian Journal of Science and Technology, 9*(31), 1–8.

Wójtowicz, M., Wójtowicz, A., & Piekarczyk, J. (2016). Application of remote sensing methods in agriculture. *Communications in Biometry and Crop Science, 11*, 31–50.

Yan-e, D. (2011, March). *Design of intelligent agriculture management information system based on IoT*. In Intelligent Computation Technology and Automation (ICICTA), 2011 International Conference on (vol. 1, pp. 1045–1049). IEEE.

Zhang, Q., Reid, J. F., & Noguchi, N. (1999, August). Agricultural vehicle navigation using multiple guidance sensors. In *Proceedings of the international conference on field and service robotics* (pp. 293–298).

Chapter 20
Intelligent Healthcare Solutions

Salman Basheer Ahmed and B. M. Jabarullah

Abstract IoT technology has been present for more than a decade but has shown rapid growth in recent years, a process catalysed by advancements in sensors, smartphone technology and application software. The impact of IoT in healthcare sector has been so huge that it has paved way to a new frontier, Internet of Medical Things (IOMT). IOMT aims at achieving an intelligent and collaborative model capable of independent and isolated work with minimum security risks. Rapid advancements in sensing technologies, data processing techniques and end user applications helped establish IoT as an effective and adaptive technology in PHS.

Keywords IoT · Healthcare · Intelligent heath · e-health · M-health

20.1 Introduction

The literature of IoT in healthcare introduces one to the architecture and workflow of IoT platforms in healthcare, a gist of which is presented in this chapter. Open source technologies are often assigned meaning with reference to context, a habit leading to misinterpretations. This chapter aims at understanding this multi layered and multi flavoured approach at a level that would encompass the literature, not at the cost of shifting focus from the foundations of this technology.

The flow of data at each stage of intelligent healthcare systems is researched upon as data and various intelligent models associated with data form a vital part of this field. Various approaches exist for processing the large amounts of real time data generated by multiple devices and applications. Diving deep into the actual mathematical models involved might deviate the work towards understanding algorithms devised for intelligent learning of systems. Hence this chapter would abstract itself and apply more focus on understanding the "centric" approaches.

S. B. Ahmed (✉)
Department of Computer Engineering, Faculty of Engineering and Technology, New Delhi, India

B. M. Jabarullah
Pusa Institute of Technology, New Delhi, India

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_20

The ultimate aim of healthcare services is to be able to cover a larger fraction of the population than the current extent with minimum usage of financial and human resources with no compromise on quality. “Pervasive Healthcare” has emerged to be one technology assisted solution to this problem. Personalised healthcare systems (PHS) present an inclusive picture for the potential and challenges of IoT technology in healthcare. This chapter understands these healthcare systems at a suitable depth taking it as a case study. The chapter concludes by taking a peek into the future of this decade long technology that involves introducing oneself to the modern half baked marvels like hearables, ingestible sensors and moodables.

Personalised healthcare systems (PHS) present a suitable application that brings out the potential and also the challenges of using IoT technology in healthcare. Pervasive healthcare in it’s true essence means to be able to provide healthcare to anyone, anywhere and anytime thereby overcoming any geographical, demographic and technological barriers. Personalised healthcare systems make a fitting case of the above.

20.2 IT Platforms in Healthcare

Internet of Things (IoT) in the healthcare sector, better described as Internet of Medical Things (IOMT), has shown an impressive growth accompanied by ample implementation and deployment of systems, which was possible due to the advancements in sensing technologies such as those obtaining physiologic data such as pulse rate, respiratory rate, blood pressure and body temperature and those obtaining other kinds of data such as geolocation, physical orientation etc., and due to advancements in end user applications, gateway devices and network devices. IoT has helped reduce the pressure on the healthcare sector to meet the demands of an ever-growing population to provide good healthcare services at the minimum possible cost.

IoT approach to healthcare makes use of a network of interconnected devices, which is said to form the IoT network, to provide healthcare related services. They harness the power of wireless technologies such as WiFi or Bluetooth technology to obtain data from medical devices as well as more non-conventional devices such as wearables. Current implementation include systems for continuous and remote monitoring of patient’s health, applying intelligent prediction models to patient’s data and also enable clinicians to provide healthcare guidance to patients in cases of chronic diseases. A more indirect application would be the use of face recognition technologies (Jabarullah et al. 2012; Saxena et al. 2018) to help identify accident patients using a cloud enabled storage facility.

This chapter aims at understanding the structure of the IoT based healthcare systems, considering the problem in a hollistic manner. It also aims at understanding the various models and approaches involved with handling, storing and processing the enormity of data generated in such applications. The chapter looks at the various centric approaches that exist and also the intelligent models that are

employed to develop a smart system. A branch of the healthcare industry i.e. Pervasive Healthcare is looked upon in this chapter as it is seen to be a typical example of such systems. Real world applications have also been considered to get a more clear understanding of the idea behind Pervasive Healthcare and also to provide the reader with an idea of such live implementations. The chapter concludes by looking at the various threats that exist to such systems. It also discusses some of the modern day marvels that are being extensively researched upon.

IoT enabled healthcare platforms are seen to confirm to the architectural trends seen in traditional IoT systems i.e. they tend to have a multi layered design to a system. The bottom layer is populated with physical systems that function as data hoarders that generate the mass of the data. The intermediate layer tries to strike a balance between the various heterogeneous devices that obtain data and the ones that perform network operations or may work on the network edge or close to an end user application. This layer also subjects the data to a rigorous data analytics routine to process and validate data. The top layer comprises of end user applications that are mainly concerned with information rendering and at times are also utilised for data processing due to computational advantages. The following paragraph aims at providing an overview of the workflow of an IoT enabled healthcare system to the reader before diving into the required specifics or detailing.

The literature of IoT systems in healthcare reveals that data is primarily obtained from sensing devices or applications running on smartphone devices, for example inertial sensors, physiological sensors, Global Positioning System (GPS), Electrocardiogram (ECG) and Electroencephalogram (EEG). The primary challenge at this stage is standardisation and interoperability of heterogeneous data generated from all these devices. These static and mobile devices are connected via a network, designing which takes into consideration the cost, pros and cons involved in mapping this inconsistent heterogeneous network onto a consistent and more meaningful hybrid computing grid. The raw data, that is now part of the IoT network, is digested to obtain meaning so that it may be fed to suitable end user applications.

As mentioned in Sect. 20.2 of this work, various intelligent models are put to use to obtain the same. Big data, learning methods such as supervised learning, unsupervised learning, knowledge based learning are tenacious research areas to name a few that are aiming at new frontiers and better solutions. For instance, Convolutional Neural Network (CNN) based model (Raza and Alam 2016) of Gene Regulatory Network (GRN) resulted in a powerful model which could be used for disease diagnosis, disease response and also to identify effective drug targets. The uniqueness of the Big Data problem (Khan et al. 2015), due to the 4Vs associated with it, was identified. This causes handling of such data a difficult task by using conventional methods. The author harnesses the power of cloud computing technologies to solve the Big Data problem. Cloud and Big Data are two important technologies utilised in any IoT based system. The unique problem presented by Big Data was analysed and cloud computing technology was used as the solution (Khan et al. 2017; Shakil and Alam 2017).

The data storage and processing that takes place at this stage of an IoT system makes use of all such technologies and implementations. This processed data is then fed to the applications that are responsible for user interfacing, implementing an alert system, enforcing authorisation at an application level and quality rendering of data. With the wide and diverse use of applications involved, the area is gaining more research attention leading to development of handy tools such as an application programming interface that would generalise the technology thereby enabling cross platform usage. This presented workflow summarises the operation of an IoT enabled personalised healthcare system. The observant reader would have noticed that this indicates a migration of healthcare centered around hospitals and healthcare centres, the traditional approach, to a personal level and thereby fulfilling the motives of pervasive healthcare to provide healthcare to anyone, anywhere and at any time.

The four tier architecture of a typical IoT based healthcare system (Qi et al. 2017) is shown in Fig. 20.1 which is quite complete and informative in its nature. Each layer is discussed in suitable depths below and the data processing layer is discussed as a separate section pertaining to its vastness in content.

20.2.1 Device Layer

As mentioned in the starting parts of this section, this layer is populated with sensor devices that are responsible for collecting the majority of data. These sensors form a set of key components to an IoT enabled healthcare system as they offer remote

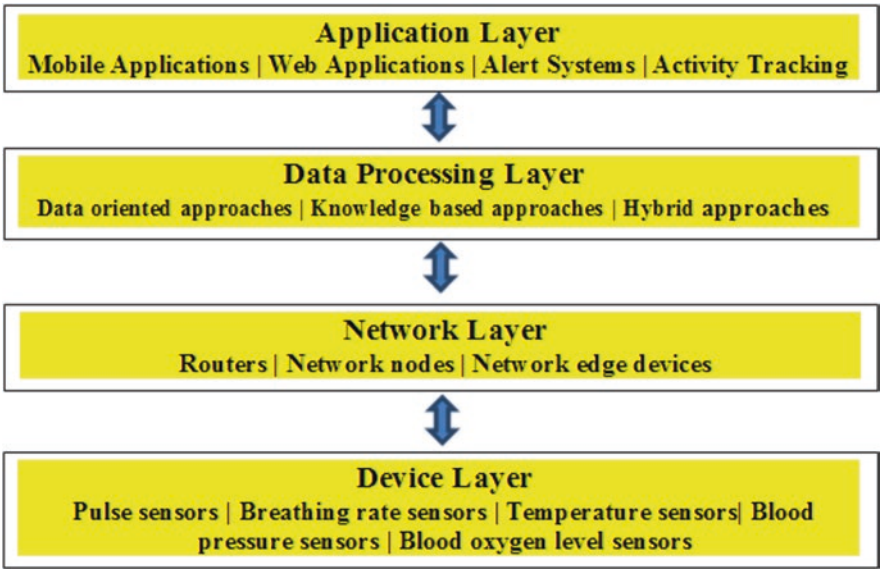


Fig. 20.1 IoT based healthcare system

gathering and transmission of data, a non compromisable asset to the IoT system. Though the data may be inconsistent pertaining to the variants of a natural environment (methods to handle which, have been discussed further in the chapter), these devices cannot be replaced or disposed off. This sub-section aims at looking at some of these sensing technologies (Baker et al. 2017), their functioning and use, that are widely used in healthcare environments.

Pulse Sensors: Pulse rate of an individual can be read off by making use of wearable devices such wrist watches or chest straps, both of which are used as commercial fitness products. The literature of such sensors reveals that these devices are being intensely researched and can be classified as pressure sensors, Photoplethysmographic (PPG) sensors, ultrasonic and radio frequency sensors. PPG sensors make use of an Light Emitting Diode(LED) light which is made incident on the blood stream and the amount of unabsorbed light is measured to detect the pulse rate.

Pressure sensors try and mimic the actual procedure of manual measurement of pulse i.e. by applying pressure on the wrist and the response to the pressure applied is taken for generating a pulse waveform. Both the sensors can be made part of a wearable device and as is the pitfall pertaining to any wearable device, both are sensitive to user movement and hence may produce somewhat inaccurate readings. Sensitization of the sensors results in increased presence of noise in the readings. Hence, these devices are being actively researched upon to produce more motion resistant and noiseless sensors.

Breathing Rate Sensors: A survey of breathing rate sensor technologies (Baker et al. 2017) reveals that several devices have been developed to measure the breathing rate of remote patients that make use of a wide array of parameters to arrive at a correct reading. Nasal sensors make use of thermally sensitive sensors that mainly detect the temperature changes caused when a person exhales. Breathing rate may also be obtained from the ECG readings of a patient.

Microphone based sensors are also used to measure respiration but as is evident are highly susceptible to external noise. Similarly optic fibre based vibration detection sensors are also used and these carry a disadvantage of generating incorrect readings when the user is in motion. In another example, capacitor plates were used, and the relative movements of which were used to measure the respiration rate.

While in another example, a ferroelectric polymer transducer was used which generated charge on application of tensile force, changes in which was used to measure the respiration rate. As the esteemed reader would agree, the major performance issue that arises in all of the above mentioned sensors is the accuracy of the reading when the device is used in a noiseful environment along with the user being in motion. Future scope of research would also be in developing such adaptable sensors.

Body Temperature Sensors: Recent studies show that body temperature sensors are mainly centered around thermistor based sensors (Baker et al. 2017), the scope of research in such sensors lies in making them as wearable as possible, as proximity to the human body results in a more accurate measurement of the body temperature.

Motion Sensors Devices that are used to monitor motion (Haghi et al. 2017) are also widely used in healthcare systems. Application of such sensors include remote patient monitoring in case of patients requiring exercise schedules which could be a part of their treatment. They are also used to monitor the amount of activity exercised by obese patients in order that guidelines by the clinician may be given accordingly.

Blood Pressure Sensors: Studies suggest that measurement of blood pressure using wearable sensors that would provide continuous data and also obtain the same in a non-invasive manner are somewhat of a challenge to researchers and technologists. On inspecting the work that has been performed, it would be somewhat suitable to say that the aforementioned difficulty may exist due to the absence of any direct way of measuring blood pressure. Pulse Transit Time (PTT), conventionally defined as the time it takes for a pulse measured at the heart to travel to another point in the body for example the earlobe, radial artery etc., is measured and processed to obtain the blood pressure readings of the individual.

This could be made possible by making use of an ECG chest-strap and a PPG sensor perhaps connected to the earlobe. But as pointed out by (Baker et al. 2017), this kind of a setup becomes obstructive as the connection between the devices will tend to be a wired one. Hence, modern and slightly different applications of the same have been to measure the PTT between the palm and the fingertip or between the ear and the wrist. But as is the case with all sensing technologies the readings have been seen to be reasonably accurate in the case of manually controlled environment. Developing sensors that are adaptable, accurate and are also less obstructive becomes the aim of further rigorous research in this sector.

Blood Oxygen Sensors: Blood oxygen level measurement sensors or pulse oximetry sensors are mainly based on the above mentioned PPG technology, using a pair of LEDs to measure the amount of light absorbed by the haemoglobin in the blood to determine the amount of oxygen content in the blood. Studies indicate that major work is being carried out on making the sensors more portable as conventional ones are seen to reduce the flexibility of the individual using them. The author of (Baker et al. 2017) provides an extensive survey of the various research implementations that exist for the same.

For example the author mentions about the development of a low power consumption sensor that continuously tracks the signal to noise ratio and also the peaks and troughs generated in the PPG reading, to try and moderate the intensity of the LED light accordingly. Another example proposes an in-ear based reflective oximetric sensor that stands out as it is seen to successfully obtain the readings in cases where the measuring the same from finger tips would be difficult such as when the patient suffers from conditions such as shock that lead to blood centralisation. The most mobile implementation was the design of a wrist wearable reflective oximetric sensor that would be least obstructive in nature.

20.2.2 Network Layer

Network layer performs the task of providing a means of communication to the various "things" in an IoT enabled healthcare system. The various devices, mainly sensing devices, need to be integrated to work together and as pointed out by various studies, IoT systems are seen to generate a requirement for protocols that facilitate machine-to-machine communication, instead of the conventional human-to-human communication in a network. The various tasks that may be performed as part of networking or connecting this wide array of devices would be to establish Quality of Service (QoS) management and standardisation that is specific to the end user applications or devices in the subsequent layers of the system. As mentioned in (Da Xu et al. 2014), these devices should be able to deploy, manage and schedule the behaviour of the "things" in the network, which may be the same device or some neighbouring device as coherence is expected of such a system.

As brought out by (Riazul Islam et al. 2015), IoT enabled healthcare systems are seen to utilise the IPv6 based 6LoWPAN (IPv6 based low power wireless personal area network) to form the basis of the network model. The various devices and applications operating in the network can be accommodated to separate layers of operation. The devices i.e. the sensors use the IPv6LoWPAN to transmit data over the 802.15.4 protocol, which forms the base layer of operation. The overlooking network layer makes use of the standard IPv6 and RPL (Routing Protocol for Low Power and Lossy Networks) protocols for communication.

The transport layer abstraction finally relays data by subjecting it to conventional TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) protocols. The end user applications have a relatively larger array of options presented to them, which are also seen to be convenient in terms of support to the applications, which contain HTTP, CoAP (Constrained Application Protocol) and SSL (Secure Socket Layer) as their prime constituents. Figure 20.2 shows 6LoWPAN protocol stack (Riazul Islam et al. 2015) which encompass the above mentioned layers. The CoAP protocol (Ali Khattak et al. 2014) would require special attention, in the interest of application developers, as it aims at handling all the work involved with data querying and response based on HTTP methods alone to be able to develop powerful REST (Representational State Transfer) based applications.

It can be said as a powerful protocol as it provides with features such as asynchronous communication, HTTP to CoAP and CoAP to HTTP translations. It also ensures reliable message exchange. As brought out by (Ali Khattak et al. 2014), CoAP is seen to provide with the ability to design and develop a very flexible and resource intensive (in terms of the end user application which takes up most of the interfacing and rendering tasks) system. The network layer is also subjected to rigorous research in the aim to develop more efficient networks in terms of latency, cost, real time and guaranteed delivery of data.

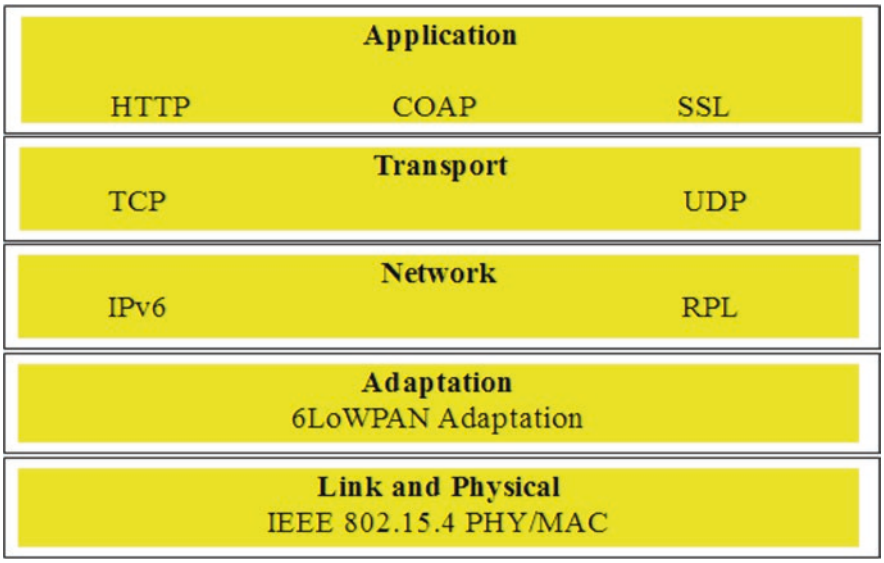


Fig. 20.2 6LoWPAN protocol stack

20.2.3 Application Layer

The final layer of a typical IoT enabled healthcare system, this layer is populated with the end user application that perform all the heawylifting related to rendering, interfacing and even data processing at times. This layer is mainly composed of powerful computing devices such as smartphones, tablets, PDAs and other such computing devices. Pertaining to the way the rest of the system has been implemented, this layer would be desgined to react in a dynamic sort of way. The logic associated with this layer would be mainly concerned with concepts that try and harness the power of data visualisation techniques.

Design implementations to tackle with security issues such as unauthorised access to sensitive data would be handled here. As suggested by the literature on IoT based healthcare implementations, these final applications could occur in various forms such as a website rendering data obtained either from the cloud or from a server that accumulates and processes data obtained from further below in the system, or in the form of a mobile application that may make use of some the computing powers of the mobile computing device to reduce the heawylifting of data processing performed by lower layers of the system or it could in the form alert based system that would simply work on a wearable such as smart watches. This layer is more under the eye of application developers to come up with better approaches to handling intelligent models, rendering data and providing even more secure ways of handling data.

20.3 Handling Data

As the reader would respond in affirmation that processed data (sometimes referred to as information in a few contexts) is more valuable than raw data. The enormous amount of data generated (also referred to as Big Data) thus needs to be processed and hence data processing is an important stage in the lifecycle of an IoT based intelligent system. As discussed in Sect. 20.1 of this chapter, the structure of an IoT based healthcare system can be seen as comprising multiple layers, each of which is capable of processing data with varied capacity and efficiency. Computation offloading (Samie et al. 2016) i.e. decentralising the computation process to the various layers of an IoT system is followed and the major design decision that accompanies it is, determining where the offloading should be done. Evaluation against various factors such as the availability of resources, network latency, capacity of data that can be handled with minimum deviation or error etc. needs to be done for a layer before arriving at a proposition. As described in (Samie et al. 2016), various 'centric approaches' exist for computation of data in an IoT system, which primarily outlines the various places in an IoT enabled system where data processing could be carried out.

20.3.1 Device Centric

Data computation can be performed at the base layer of an IoT system, the layer consisting of devices with embedded microcontrollers. As our esteemed reader would have realised that the major restriction with this approach is the minimum resource availability in terms of storage and computing power. The decision to perform computation at this stage could be pre-determined and in some cases could be determined at run time (Kim 2015).

20.3.2 Gateway Centric

Gateway devices bridge the communication gap between IoT devices, sensors and cloud. Due to the high extent of heterogeneity present in the devices, there may exist devices which may not support certain communication protocols and thus may require a translation medium. The various "things" in an IoT system communicate amongst themselves through a private network and with the external environment such as the cloud through a public network. Enforcing security and standardised protocols thus becomes a necessity, which can be achieved by making use of gateway devices. ARM Cortex-A, Cortex-M MCU and smartphones (Zachariah et al. 2015) are examples of gateway devices. They provide a computational processing

advantage over the device centric approach. As pointed out by (Samie et al. 2016), network latency, guaranteeing content delivery and entropy of the wireless technologies pose as major challenges to processing data at the gateway devices. An implementation of this scheme is presented in (Samie et al. 2015), which makes use of a smartphone as a gateway device that processes the medical data.

20.3.3 Fog Centric

Fogs provide more computing power in comparison to microcontroller embedded devices or gateway devices and are seen to have less delay in comparison to the cloud servers. Fog computing techniques have also shown to consume less power as compared to a cloud network. The fog computing paradigm performs the tasks of data storage, computation and control closer to the end user applications. As pointed out in (Chiang and Zhang 2016), fog computing technique is seen to have an upper hand in data processing when compared to the previous approaches.

Through migration of data processing tasks to the network edge, fog computing techniques help achieve a cyber-physical system with minimum latency, a problem that was majorly observed in the gateway centric approach. IoT enabled healthcare systems face a major hurdle in tackling latency as the aim is in developing and implementing a system that works with real time data and provides applications with miniature response times.

Fog computing takes the burden off from resource constrained devices by performing all the resource intensive tasks in scenarios where migration of these tasks to the cloud is not preferred due to various reasons which may be related to cost minimisation or technical constraints. Fogs also overcome network bandwidth constraints by achieving a balance between the end user application requirements and the availability of networking resources.

20.3.4 Cloud Centric

Cloud computing techniques may be used for storing, processing and visualising the huge volume of data i.e. Big Data, generated in an IoT enabled intelligent healthcare system. Cloud offers a rich set of features such as impressive computational power, immense storage capacity, extensive implementation of security features, etc. and has always been an active field of research. Major challenges to this approach are seen to be centered around cost minimisation, latency and scalability as the cloud approach tends to be a resource intensive approach when best results are desired.

As mentioned in (Zhang et al. 2015), the amount of data in the IoT space is expected to exceed the trillion objects in Amazon S3, and a centralised cloud architecture for such huge volumes is quite unimaginable. Residing on the network edge,

cloud computing may just add to the latency which is highly undesirable in a healthcare oriented application. Literature shows that the cloudlet architecture presents itself as a viable solution to the latency problem as it is seen to implement a direct communication between the data accumulator and the cloudlet, thereby avoiding all delays. IoT applications generate most of the data on the network edge thereby crowding network's upstream link bandwidth, which is one of the scalability challenges.

The author of (Zhang et al. 2015) also points out that durability of data, both acquired through sensors and data that is stored in the cloud, is also a major concern and needs to be ensured as part of an efficient model. Apart from processing, management of data is also vital as large amounts of data is not only processed but also stored in the cloud. The author of (Shakil and Alam 2014) presents a novel clustering approach towards data management in the cloud. The author presents the various places where data management tasks could be performed and proposes an efficient technique for the same.

20.3.5 Intelligent Approaches Towards Data Processing

IoT enabled healthcare systems harness the power of intelligent data processing models and approaches to perform data analytics (to try and obtain meaning from data), to indicate trends in data, to clean the heterogeneous data obtained and also to design and implement applications capable of performing predictions from patient legacy data for early diagnosis and treatment of disease. As brought out by (Qi et al. 2017), the decision of choosing the correct data processing approach from the wide array of available approaches cannot be done in an absolute manner as the size, type and format of data and the application that is going to digest the data, must be considered and the trade-off among time, space and cost must be evaluated before arriving at a proposition. This chapter aims at outlining the approaches (Qi et al. 2017), so that the reader gets a clear picture of the options that exist.

Data Oriented Approaches: Supervised and unsupervised learning algorithms drive the data oriented approach for data processing. In layman terms, supervised learning algorithms are made use of to generate prediction models which can be reliably arrived at by training the model with legacy data by providing the actual outcomes for a few (at times large) input measurements. This is popularly referred to as the training data set which forms the basis of prediction. As is common to any learning algorithm, cost minimisation i.e. variation between actual outcome and predicted outcome (tested by providing a smaller dataset, commonly referred to as the testing set) is the ultimate motive as it proves to be a direct indicator of the reliability of the prediction model.

Activity recognition, clinical decision making and symptom rehabilitation (Qi et al. 2017) are few implementations of supervised learning approaches made in IoT enabled healthcare systems. Artificial Neural Networks (ANN), Bayes Network (BN), Support Vector Machines (SVM) etc. are supervised learning approaches to

name a few. The literature of IoT enabled healthcare systems shows that these approaches have been used both individually and also in combinations, giving rise to a more hybrid sort of approach, with one another to derive suitable implementations. Unsupervised learning algorithms are mainly centered around clustering of the huge amount of raw data fed to these systems.

K-mean clustering algorithm and Gaussian mixture model are typical examples of the same. Clustering approaches find application deeper into the hierarchy by being utilised in laboratories for extensive research and diagnosis purposes thereby extending the reach of IoT systems. Clustering trends reported in genetic data of patients to indicate affinity trends in the genetic heredity and history of diseases in families of the patients, characterising the different types of physical activities using data generated from numerous wearables and sensors are examples of implementation of this approach.

Knowledge Based Approaches: Knowledge based approaches try and map the knowledge owned by individuals such as healthcare professionals or clinicians, to computer algorithms to achieve a system based on organisational knowledge model construction and inference rules. They can be simply understood as three module system.

The first module contains the interface that allows users to query the system, the second module interacts with the back-end knowledge base to arrive at decisions and the third module i.e. the knowledge base is loaded with expert knowledge as rules that are rigorously utilised to arrive at computerised decisions. These systems are applied as decision making systems and also utilised as tailor made software to act as a continuous aid to chronic disease patients and elderly patients living alone by providing services such as monitoring, day-to-day advice, clinical appointment reminder based on the condition of the patient etc.

The literature of implementations of this approach (Qi et al. 2017) shows various successful deployments that have incorporated this model. For example, an IoT enabled system has been proposed that supports home based care for breast cancer patients by providing structured advice to patients that are derived by the smart system. The author of (Kaur and Alam 2013) proposes an intelligent system that can be used to handle data related to atrial fibrillation, a disorder leading to irregular heat beat. The system makes use of a knowledge based approach that has been hybridised to emphasise the role of knowledge engineering in the development of such systems.

Other examples include a context based reasoning system for continuous monitoring of chronic patients, a smart system that generates disease assessment and recommendations of asthma patients to be made use by clinicians, etc. Knowledge based approaches can be subjected to further classification based on the idea behind the reasoning model that is used. Syntax based approaches contain two layers, the bottom layer being composed of Hidden Markov Model (HMM) and Bayes Network (BN) and the top layer being composed of Context Free Grammar (CFG), and it follows a language grammar based ruling to arrive at the structure of the reasoning model.

Logic based approaches define entities and a set of rules are inferred to achieve rationality. Ontology based approaches are seen to be the most bendable approach as it offers a more extensive control over specifying the tweaks of the organisational structure. It defines concepts, properties and relationships among the units of the organisational structure.

Hybrid Approach: Hybrid approaches are brought into the picture as both data oriented and knowledge based approaches are seen to have their own set of shortcomings. While it is difficult to deal with the heterogeneity present in the training samples prepared using data collected from a wide array of heterogeneous devices, the knowledge based approaches are seen to be less robust when dealing an uncontrolled environment such as that of a hospital or clinic.

Research suggests that adapting and interoping both of the above approaches to arrive at the hybrid approach proves to be beneficial and helps harness the power of both while ensuring that each approach complements the pitfalls of the other. The author of (Qi et al. 2017) mentions a few examples of the application of this approach such as the COASR, a suitable case which combines the two approaches to help elderly people at home with self-management.

20.3.6 Data Validation

Lifelogging data presents itself as one of the most important raw material to be fed into an intelligent system as it captures a satisfying extent of physiologic and geographic data of an individual. Obtaining individual specific information such as heart rate, body temperature, physical activity, geolocation etc. are examples of the same. But as is the major challenge to any IoT based system, the heterogeneity of the devices used and varied lifestyle patterns of individuals, the data so obtained is inconsitent and non standardised.

As a knowledgeable reader would understand that enforcing protocols or standards would not prove to be a good solution as an IoT based intelligent healthcare system is expected to work in an adaptive manner. Thus, validation of data so obtained from devices becomes an area of active research. LPAV-IoT model, is proposed by (Po et al. 2016) which validates the lifelogging data against a set of rules and provides a descriptive analysis of the reliability of data, noise introducing factors and errors causing uncertainty in the data.

It is seen as an adaptive model as it provides a dynamic standardised empirical analysis workflow that is capable of usage specific updation, IoT enabled Personalised Healthcare System being one. Legacy data is fed into the LPAV-IoT model to instantiate the validation rules. The model works as a dynamic recurrence, as is expected from any automated system, and the initial set of legacy data grows over time. The validation rules can be updated by replacing the initial set of legacy data with a new one. The model works on a four layer system of investigation, methodology, knowledge and action.

The uncertainty in data is categorised, based on the cause and frequency of occurrence, as irregular and regular. The investigation layer generates the uncertainty measurement matrix and a set of investigation approaches is proposed by the methodology layer. The knowledge layer establishes a set of validation rules and principles to effectively remove irregular uncertainty and try and minimise/manage regular uncertainties. The action layer provides with the set of actions, derived from the results of the previous layers that could be carried out. The proposed method in the LPAV-IoT model makes use of various descriptive statistical formulations for arriving at calculative conclusions to be able to propose the said model to eliminate irregular uncertainty and estimate the data reliability.

Rigorous research is being carried out in developing more models that can incorporate more impact factors, take into account more human specific diversities and error causing sources, so that one could increase the reliability and consistency of the huge volume of data generated.

20.4 Personalised Healthcare Systems

IoT enabled Personalised Healthcare Systems (PHS) present a befitting example for pervasive healthcare and aims at fulfilling its motive of being able to provide healthcare to anyone, anywhere and anytime (Varshney 2005) thereby overcoming any geographical, demographic and technological barriers. It makes use of the platform architecture and intelligent data processing models, discussed in above sections of this chapter, to perform various healthcare related activities such as realtime health monitoring, on demand availability of patient records, emergency assessment, remote surgeries, digital prescriptions and digital bill payment alternatives interoping.

ZigBee Based Monitoring: One such implementation is the system to monitor physiological parameters of patients admitted to a hospital which does not make use of the conventional WLAN or Bluetooth technologies, opting instead for ZigBee based implementation and deployment (Kodali et al. 2015). Making use of wireless technologies eliminates the need of a healthcare professional for periodic recording, a digital approach of Electronic Health Records (EHR).

The onset of IEEE 802.15.4 standard for physical and MAC layers of wireless communication paved way for a more rigorous implementation of the ZigBee protocol (Baronti et al. 2007), which proves to be a better alternative to conventional protocols that pose power consumption and scalability as challenges during implementation of a fully functional unit. As stated in (Kodali et al. 2015), this system makes use of LM35 temperature sensor to obtain physiological data (temperature data in this specific implementation), transmitted to the logic unit of the IoT enabled system.

This unit makes use of a gateway to collect data through a Universal Asynchronous Receiver and Transmitter (UART), at preconfigured periodic intervals, and relays the same after processing it to a web server. Once it reaches web servers, application developers may obtain the data easily and novel methods can be devised to render

data, not in an obsolete format, to be able to cover the diversity of the end user. Suitable authentication and sensitive data protection measures may also be enforced accordingly.

Sepsis Detection: Another such implementation is a prediction model for Severe Sepsis (SS) of patients admitted to ICU, incorporated with an electronic alert generation mechanism (Kamaleswaran et al. 2018). Sepsis is a serious clinical condition occurring in patients admitted to the ICU, which according to (Sepsis https://en.wikipedia.org/wiki/Sepsis) arises when the body's response to infection (inflammation) causes injury to its own tissues and organs. Severe sepsis is a heightened version of sepsis leading to multiple organ failure. It is one of the major conditions having high mortality rate for patients admitted to the ICU.

The implementation proposed in (Kamaleswaran et al. 2018) uses intelligent learning approaches such as Logistic Regression (LR), Random Forests (RF) and Convolutional Neural Network (CNN) to establish a prediction model for SS using the physiomarker data of patients and completes the versatile system by making use of an alert mechanism. In this specific implementation the study was performed on children admitted to the ICU, presenting a paediatric case, but the same model could be extended to a more general application as well. Five statistical values and seven Probabilistic Symbolic Pattern Recognition (PSPR) features were obtained for each of the five physiologic data to be used, which produced a total of 60 physiomarkers to be fed to the intelligent system. This information was obtained from the Electronic Health Records (EHR) of the patient.

Systemic Inflammatory Response Syndrome (SIRS), which was previously considered a sufficient enough marker for mortality prediction, was used as a criteria to determine the chances of SS and once the physiologic data met the pre determined conditions a flag was raised and an alert sent to the healthcare officials and teams on their smartphone with alert characteristics for immediate response and course of action. In addition a SS label was also recorded with a timestamp and added to the patient's EHR as part of a more standardised observation recording system for future use.

Etiobe: Apart from patient care, implementations have been devised to support and promote a healthy lifestyle, a variant system that is moderately active and distances from a manually controlled environment, as in the above applications. Etiobe (Baños et al. 2011), is an e-health platform comprising of three independent factions, coordinating in real time, to help prevent and treat obesity in children. It presents itself as an application that is well connected, in the sense that it establishes a routine between the healthcare official, the child and also the parents or guardians.

Clinical Support System (CSS), a tool used by the clinician to store and maintain patient records and also to provide digital prescriptions and routines to be followed by the kids. An alert system is also built into this tool to raise alarms towards trends that indicate severe cases obesity in the patient. Home Support System (HSS), a tool rich in user interface elements that is designed and implemented to resemble a smart electronic personal trainer. Data obtained from this is immediately sent to CSS for clinician monitoring and analysis. Mobile Support System (MSS) is comprised of a personal digital assistant and a sensor recognition platform called Therapy Intelligent Personal Sensor (TIPS).

TIPS is used to obtain the context based information (geoposition, posture, physical activity) and physiological information (heart rate, skin conductance, breathe frequency) that is relayed to the application enabling remote monitoring for the clinician. MSS tool is primarily used to track the dietary trends and physical activity of the individual. Each tool of the platform is equipped with an appropriate authentication system to prevent unauthorised access to sensitive data and is observed to follow the security patterns and conventions of a network enabled smart application that entertains a diverse set of users.

The Etiobe e-health platform, wraps around this three tools, and is seen as an implementation that is smarter, secure and robust than relative conventional applications as discussed above, in the sense that it presents a working model in the natural environment of the users, rather than a manually controlled environment of a clinic, and also is seen to align relatively more towards de-centralisation, features that are expected from an IoT enabled PHS.

20.5 Conclusion

Since its advent decades before, IoT enabled healthcare systems have been seen to undergo rapid and powerful changes. As mentioned at the beginning of this chapter, this process was catalysed by the growth in sensing technologies, storage facilities, processing capabilities and also in versatility and flexibility of end user applications. This chapter aimed at providing a comprehensive understanding of the architecture, devices, network implementations, data processing models and various deployments of IoT enabled healthcare systems to the esteemed reader. As the literature of such systems reveal, information security and ensuring privacy of users prevails to be a major concern in this domain. IoT enabled systems present an even more tougher case as the heterogeneity of devices involved is large and also the amount of data generated is massive.

Vulnerabilities may exist in the network where MiTM (Man in The Middle) attacks could be carried out to obtain the data that is being transmitted. Securing data in the cloud is seen to have emerged as a separate field of research pertaining to its vastness. Attacks may be carried out extensively at the application side. If the end user applications of the IoT based healthcare system are web based systems then they may be prone to various web based attacks such as injection, cross-site scripting, cross-site request forgery etc. Much of the data is stored and processed at the cloud, therefore having a secure cloud service becomes vital. Securing the cloud is an area being actively researched upon.

For instance (Bashir et al. 2013) presents an extensive coverage of the various threat models in cloud based services and also thereby presents novel solutions to a few. Another work done by (Alam and Sethi 2013) analyses the risk factors that a government organisation may face in migrating to the cloud and how to mitigate them. Such works can find application where government based healthcare systems are to be implemented which may involve processes like identification of users

based on some global identification repository. This tends to increase the risks as even more sensitive data gets involved. In another example, a particular but dangerous attack, Distributed Denial of Service (DDOS) (Alam et al. 2014) was introduced.

The author analyses the various reasons that make a cloud based system vulnerable to this attack and also proposes an intelligent system based on neural networks that would help mitigate the same. Hence developing, implementing and deploying a fully functional and highly secure IoT based healthcare system remains to be a big challenge and also an area that is being highly researched upon.

IoT based healthcare systems are continuously evolving to become more robust. This has given rise to a new range of healthcare devices that could be looked upon as modern day marvels. Ingestible sensors, which are nothing but pill sized electronic devices composed of biocompatible materials that provide with power, micro processing and control capabilities to the device, is one such example. Gut gas sensors and bacteria on a chip are a few actual implementations of the same. Moodables are another example of these modern day marvels. Head mounted, these mood altering devices send low intensity current to the brain to alter and in some cases replace the mood of the patient that is admitted to the hospital.

Hearables are devices that have been changing the scenario for patients with hearing problems. These small and portable devices are growing rapidly both in usage and also in features, to help patients with hearing problems. These marvels could be justly called as half baked as they lack complete implementation. But these devices have paved way to a new phase in the life of IoT enabled systems and it would be safe to say that these devices could change the landscape of such systems.

References

Alam, M., & Sethi, S. (2013). Security risks & migration strategy for cloudsourcing: A government perspective. *International Journal of Engineering and Innovative Technology, 2*(7), 205–209.

Alam, M., Shakil, K. A., Javed, M. S., Ansari, M., & Ambreen. (2014). Detect and filter traffic attack through cloud trace back and neural network. In *The 2014 international conference of Data Mining and Knowledge Engineering*, Imperial College, London, 2–4 July, 2014.

Ali Khattak, H., Ruta, M., & Di Sciascio, E. (2014). CoAP-based healthcare sensors network: A survey. In *Proceedings of 2014 11th international Bhurban conference on Applied Sciences & Technology (IBCAST)* Islamabad, Pakistan, 14th–18th January, 2014.

Baker, S., Xiang, W., & Atkinson, I. (2017). Internet of things for smart healthcare: Technologies, challenges, and opportunities. *IEEE Open Access, 5*, 26521–26544.

Baños, R. M., Cebolla, A., Botella, C., García-palacios, A., & Oliver, E. (2011). Improving childhood obesity treatment using new technologies: The ETIOBE system. *Clinical Practice and Epidemiology in Mental Health, 7*, 62–66.

Baronti, P., Pillai, P., Chook, V. W. C., Chessa, S., Alberto, G., & Fun Hu, Y. (2007). Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards. *Elsevier, Computer Communications, 30*, 1655–1695.

Bashir, A., Doja, M. N., Alam, M., & Malhotra, S. (2013). Security issues analysis for cloud computing. *International Journal of Computer Science and Information Security, 11*(9), 117–125.

Chiang, M., & Zhang, T. (2016). Fog and IoT: An overview of research opportunities. *IEEE Internet of Things Journal, 3*(6), 854–864.

Da Xu, L., He, W., & Li, S. (2014). Internet of things in industries: A survey. *IEEE Transactions on Industrial Informatics, 10*, 2233–2243.

Haghi, M., Thurow, K., & Stoll, R. (2017). Wearable devices in medical internet of things: Scientific research and commercially available devices. *The Korean Society of Medical Informatics*, (1), 4–15.

Jabarullah, B. M., Saxena, S., Kennedy Babu, C. N., & Alam, M. (2012). Hybrid approach of face recognition. *Cyber Times International Journal of Technology & Management, 6*(1), 6–12.

Kamaleswaran, R., Akbilgic, O., Hallman, M. A., West, A. N., Davis, R. L., & Shah, S. H. (2018). Applying artificial intelligence to identify physiomarkers predicting severe sepsis in the PICU. *Pediatric Clinical Care Medicine, 19*(10), 1.

Kaur, A., & Alam, M. (2013). Role of knowledge engineering in the development of a hybrid knowledge based medical information system for atrial fibrillation. *American Journal of Industrial and Business Management, 3*(1), 36–41.

Khan, I., Naqvi, S. K., & Alam, M. (2015). Data model for big data in cloud environment. In *Computing for sustainable global development (INDIACom), 2015 2nd international conference*, New Delhi, 11–13 March 2015.

Khan, S., Shakil, K. A., & Alam, M. (2017). *Cloud based big data analytics: A survey of current research and future directions*. Springer, Big Data Analytics.

Kim, S. (2015). Nested game-based computation offloading scheme for mobile cloud IoT systems. *EURASIP Journal on Wire-less Communications and Networking, 1*, 1–11.

Kodali, R. K., Swamy, G., & Lakshmi, B. (2015, December). An implementation of IoT for healthcare. In *IEEE Recent Advances in Intelligent Computational Systems (RAICS)* 10–12 December 2015.

Po, Y., Stankevicius, D., Marozas, V., Deng, Z. k., Lukosevicius, A., Dong, F., Liu, E., & Dali, X. (2016). Lifelogging data validation model for internet of things enabled personalized healthcare. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 48*, 50–64.

Qi, J., Po, Y., Min, G., Amft, O., Dong, F., & Xu e, L. (2017). Advanced internet of things for personalised healthcare systems: A survey. Elsevier. *Pervasive and Mobile Computing, 41*, 132–149.

Raza, K., & Alam, M. (2016). Recurrent neural network based hybrid model for reconstructing gene regulatory network. *Elsevier, Computational Biology and Chemistry, 64*, 322–334.

Riazul Islam, S. M., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K.-S. (2015). The internet of things for health care: A comprehensive survey. *IEEE Access, 3*, 678–708.

Samie, F., Bauer, L., & Henkel, J. (2015). An approximate compressor for wearable biomedical healthcare monitoring systems. In *Proceedings of the 10th international conference on Hardware/Software Codesign and System Synthesis*, Amsterdam, The Netherlands, October 04–09, 2015.

Samie, F., Bauer, L., & Henkel, J. (2016). IoT technologies for embedded computing: A Survey. In *IEEE international conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS)*, Pittsburg, PA.

Saxena, S., Alam, M., & Jabarullah, B. M. (2018). DS-HM model with DCT-HW features for face recognition. *International Journal of Scientific Research in Computer Science Applications and Management Studies, 7*(5).

Sepsis https://en.wikipedia.org/wiki/Sepsis

Shakil, K. A., & Alam, M. (2014). Data management in cloud based environment using k-median clustering technique. *IJCA Proceedings on 4th International IT Summit Confluence 2013- The Next Generation Information Technology Summit Confluence, 2013*(3), 8–13. Jan-14.

Shakil, K. A., & Alam, M. (2017). *Cloud computing in bioinformatics and big data analytics: Current status and future research*. Springer, Big Data Analytics.

Varshney, U. (2005). Pervasive healthcare: Applications, challenges and wireless solutions. *Communications of the Association for Information Systems, 16*(3), 57–72.

Zachariah, T., Klugman, N., Campbell, B., et al. (2015). The internet of things has a gateway problem. In *Proceedings of the 16th international Workshop on Mobile Computing Systems and Applications*, Santa Fe, New Mexico, USA, February 12–13, 2015.

Zhang, B., Mor, N., Kolb, J., et al. (2015). The cloud is not enough: Saving iot from the cloud. In *Proceedings of the 7th USENIX conference on hot topics in cloud computing*, Santa Clara, CA, July 06–07, 2015.

Chapter 21
Smart Car – Accident Detection and Notification Using Amazon Alexa

Lakshay Grover, V. B. Kirubanand, and Joy Paulose

Abstract The high demand for automobiles has increased traffic hazards and road accidents. Life of the people is under high risk. This is because of the lack of the best emergency facilities available in the country. The proposed system can detect accidents in significantly less time and sends the basic information first to aid center and relatives of the victim on mobile and Amazon Alexa within a few seconds covering geographical coordinates. Various devices like Arduino UNO for car movement demonstration, Arduino Mega for accident detection and Raspberry Pi 3B for internet services gateway, accelerometer and impact sensor working together to detect an accident. All connected over the internet to generate a huge amount of data which holds a lot of information about the occurrence of the accident based on the speed and location and can be used to detect accident hotspots. The system also focuses on the safety of pedestrians where a safety band is programmed to perform the notification services using an emergency push button. The ESP8266 NodeMCU invokes the same services using a button on the module. The data generated may be used for the prediction, analysis to prevent future accidents and contribute to future road safety.

Keywords Raspberry Pi · NodeMCU · Arduino mega · Arduino UNO · Amazon Alexa

21.1 Introduction

Nowadays, there is an increase in the number of accidents that happen in the world. As the population is increasing, there is a number of cars increasing on the road that contributes to severe accidents that happen daily. Around 80% of accidents contribute to the loss of many lives. Mostly, the growing countries are being targeted by the

L. Grover (✉) · V. B. Kirubanand · J. Paulose
Department of Computer Science, Christ University, Bangalore, India
e-mail: lakshay.grover@mca.christuniversity.in; kirubanand.vb@christuniversity.in; joy.paulose@christuniversity.in

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_21

day to day road accidents. The major reason is the lack of infrastructure, lack of traffic control, and accident management. Out of all the developing countries, India has been listed as the country with a higher number of accidents. The most prominent reason for the loss of life during an accident is the unavailability of immediate help that can save a person's life by a few seconds. The moment an accident has occurred, the life of all passengers traveling in the vehicle is at stake. It all depends on response time that can save their lives by a few minutes or seconds. According to the statistics, reducing accident delay time by even 1 min can save 6% of lives. Hence, this response time is very crucial, and it needs to be reduced or at least either improved to save their lives. In order to contribute to our society and reduce the number of accidents happening in our day to day life, there are several techniques and mechanisms that can drop down the rate of accidents and can save lot lives. Living in a tech world that is growing day by day with new technologies, we can apply these techniques in our society and help them overcome such problems.

The Vision of the Internet of Things (IoT) has come out to reach unexpected bounds of today's computing world. It is a concept that not only can impact human's life but also how they function. The heart of IoT is smart sensors without which it would not have existed. These sensors form a vast network for their communication. They capture minute details of their surroundings and pass this important information to each other. Based on the received information, relevant actions are performed accordingly. It is the latest communication model that imagines the proximate future, in which objects of day to day life will be incorporated with microcontrollers for digital communication with the help of appropriate protocol stacks that will make them capable of communication with one another. It is a technology that aims to impart intelligence to devices so that they can smartly connect and perform the necessary actions to eliminate human labor. It gives an image of the future where non-living objects will be communicating with each other and doing the needful work. In this way, human labor will be eliminated to an extent, and the devices will be performing necessary actions.

The significance of accident detection and notification system is very prominent for our society. Imagine a situation where an accident happened, and it is immediately notified of the emergency services. This will result in the rescue of injured people involved in the accident. For the IoT paradigm be effective, it should have the capability to track the location of the objects (i.e., cars in our case) which can serve to be useful for the ambulances to reach the location on time.

21.2 Related Work

Car accidents that happen daily are the major social problems towards which serious action must be taken. One of the solutions for this domain is the Internet of Things, which is the current trend in technology. For this purpose, many authors have worked in this domain by applying this technology.

Kim and Jeong (2014) proposed an algorithm for detecting crash using crash probabilities data in 2014. The proposed algorithm showed an improvement over Mote-Carlo simulation, which gave effective results of their model.

Raut and Sachdev (2014) proposed a call notification system that consists of XBee Wi-Fi Module, XBee Shield, GPS Module, and Seeeduino. The accident is detected using only crash sensors because of which it gives less accurate results.

Ali and Alwan (2015) proposed a system that consists of several cases to detect low speed and high-speed car accidents. In case of high speed, if the smartphone's acceleration > 4G, then there is an accident which is identified by the smartphone's application. However, it leads to triggering of false alarm in a few cases.

Chatrapathi et al. (2015) designed a framework that has two components. First one is accident detection and alerting system. The second one is traffic management for the ambulance. The efficient routing algorithm is used to route the ambulance. The technique is feasible for the road junctions with signals. However, it is not applicable to the segments without signals.

Pratiksha et al. (2015) developed a system which detects an accident, detects the condition of the car's engine about which user is informed if there is any flame or smoke is detected. The system effectively monitors the overall abnormalities that can be caused in a car. However, the system doesn't focus strongly on accident detection part.

Aishwarya et al. (2015) enhanced the driver's behavior by analyzing eye blinking with the help of IR sensors. The head movements of the driver are monitored by the accelerometer, which is fixed onto the forehead to measure the angles made by the head. This technique is not feasible since it would be uncomfortable for the driver to attach an accelerometer to the forehead every time. Moreover, driver behavior is the only factor that is considered for accident detection.

Namrata et al. (2017) detected the accident by a detection unit that is fitted in the car. The authors implemented this unit as a push on switches which senses any obstacles and triggers the microcontroller (AT8952) leading to turn on the buzzer immediately. However, this technique may not work every time because, in a few situations, the driver may not be able to turn on the switch.

Reddy and Rao (2016) developed a system which is used to detect calamities like fire in the car. The proposed methodology delivers good safety. It results in warnings that can be performed to trigger preventive measures in case of such incidents.

Kavya and Geetha (2016) suggested techniques to minimize the delay time caused by ambulance to reach the location of the accident and rather to provide a smooth flow of emergency vehicles using RF Technology. They have addressed an efficient routing algorithm to route vehicles.

Pallavi Agarwal (2017) focused on intelligently planning the transportation system based on RF technology to reduce overcrowding of vehicles in localities with smart control of signals and a proper path is planned with the help of an android application. Authors developed a real-time algorithm that makes use of VANET communication to avoid vehicles from traffic-related congestion. For some junctions, it is not feasible.

Singhal et al. (2016) found many tradeoffs while working with the accidental management system such as high cost, non-portability, false delivery, etc. The system faced many shortcomings due to lack of resources. In their technique, they used severity scale to measure the impact of an accident. This reduced load on the cloud server by 30%.

Khaliq et al. (2017) discussed techniques to detect the accident by using a few sensors and other hardware; they then verify the generated results. In their approach, they checked the severity of an accident.

Poorani et al. (2017) discussed the use of a jammer circuit which disables the keypad. It uses image processing techniques to detect driver behavior and sensors to detect the accident.

Sandeep and Kumar (2017) introduced a solution for the accidents that are majorly caused by drink and drive case. For this purpose, they used a few sensors like a touch sensor, heartbeat sensor, alcohol sensor interfaced with Raspberry Pi. In their work, they only considered the situation for the drink and drive cases.

Yadav and Kannan (2017) proposed to identify the accident and notify the cause to the registered number. In their work, they are reporting an accident to a specific number and not to an emergency service. However, the work is still unpolished due to lack of resources and implementation.

21.3 Proposed System

According to the survey, India has recorded a total of 4.61 lakh road accidents in 2018, leading to approximately 1.48 lakh deaths. This can be due to unconditional roads, over speeding, etc. An accident occurred approximately takes 10–15 min to be notified, and the authorities take a minimum of 30 min on an average to react upon it. The proposed system would make the notification and detection system smart and more efficient, which would take less than a few seconds to notify the victim's relatives and medical aid organization. The significance of defining the research problem is to address the gaps in the literature.

In our approach, we are addressing the problem by adding an accelerometer, vibration sensor, and most importantly, the heart rate sensor in the vehicle. These components contribute to the hardware setup of the system. Also, we would like to introduce an algorithm for general road accidents that is appropriate for this particular hardware setup. We have taken into account a few parameters which are helpful for accident detection and notification. These parameters are vehicle acceleration, retardation, crash impact, the value of heart rate sensor (embedded within the belt) and information of accident location, which is tracked by GPS. It is then sent to emergency services/family members through internet communication.

We implemented the system by designing an IOT based car. The car is embedded in Arduino as a development board which is interfaced with different sensors as listed above. It is controlled via Bluetooth module HC05. Also, the car is tested for different conditions to seek results. For this setup, the algorithm operates on the data gathered by accelerometer ADXL345, vibration sensor, heart rate sensor, GPS, and

GSM module. These sensors have their configurations and threshold range. The accelerometer's input range can be 2–200 g (negative and positive), and it can vary even more. Whereas, the vibration sensor has only two states, low and high. It is low for normal cases. On experiencing a large impact force from the environment, it becomes high. The heart rate sensor is an essential component since it keeps track of the driver's heartbeats during the journey. Normally, the heart rate for a person is between 75 and 170 bpm for the group of people between 20 and 50 years.

Following is the block diagram and a flow diagram for the system (Fig. 21.1).

The overall model includes various components. Arduino is the core unit of the entire system as it controls the flow of information between sensors. It is basically a development board which gives the flexibility of writing C programs for the sensors and later they can be deployed in the flash memory of Arduino in order to check the functioning of sensors.

The model uses many sensors. One of the sensors used is Impact Sensor. When a car is stopped abruptly by an impact, all bodies or objects that are not firmly fixed to the car will continue to move at the impact speed. This sensor measures this acceleration and relays it to the control unit as usable data. Vibration Sensor can recognize vibrations in a given area. It has two values as low and high. Usually, it remains low for the scenarios where vibration impact is not that powerful. It attains a high value on receiving high vibrations from the environment. A Global Positioning Sensor is used to get the position, speed, and timing information of an object. On installation of this sensor, any device can be tracked to locate its position. An accelerometer is another type of sensor which is designed to measure acceleration accu-

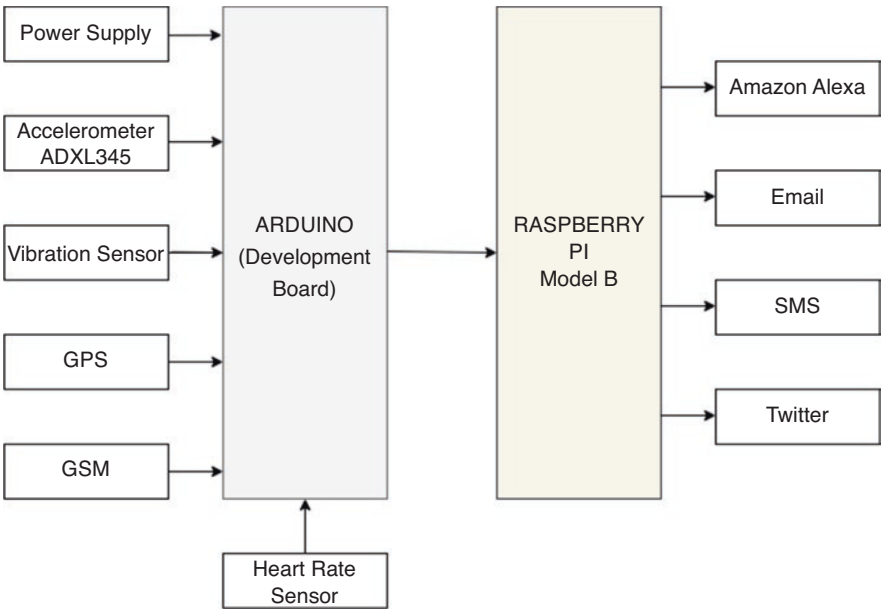


Fig. 21.1 Block diagram of proposed system

rately. It measures acceleration in three axes which are x-direction, and z-direction. The x-axis of the accelerometer gives the measure of positive acceleration, y-axis gives the measure of negative acceleration (retardation), and z-axis indicates the angle of turnover of the device in which it is installed. To measure the change in the volume of blood, Heart Rate Sensor is used. The heart rate sensor is based on the principle of photo plethysmography. It keeps track of the person's heartbeat.

GSM is used for mobile to mobile communication. It is responsible for sending SMS to the desired number or making a call whenever instructed.

The model also uses the Raspberry Pi Model B. The Raspberry Pi 3 Model B is a tiny credit card size computer. Just add a keyboard, mouse, display, power supply, micro SD card with installed Linux Distribution and you'll have a fully-fledged computer that can run applications from word processors and spreadsheets to games.

The model is able to send notifications via SMS, Email, Twitter, and Amazon Alexa. Amazon has a range of Echo devices, and Alexa is the brain behind them. We can ask Alexa any question, and it responds. Just like a human brain, Alexa is learning continuously, it updates through the cloud automatically and adds new functionality and skills.

The flow of the proposed system is given by the following flow diagram (Fig. 21.2).

The car used for the purpose is controlled by Android Application. After opening the application, it searches for the HC-05 Bluetooth module and pairs it with default passkey as 0000 or 1234. Once the pairing is done, the car can be controlled by the handset.

The Arduino Mega is used to process the sensors responsible for detecting an accident. The impact sensor and accelerometer perform the majority task of detecting the accident. The Arduino Mega is powered through Raspberry Pi through serial input. The same serial input can be used to send data to Raspberry Pi, which is used as a gateway to services like Amazon Alexa, Twitter, SMS, and Email.

Once the accident is detected, the serial data is passed from Arduino Mega to Raspberry Pi, which processes the incoming data and sends the relevant information to various services.

21.4 Proposed Algorithm

The main functioning behind the proposed system is the generalized accident detection and notification algorithm that takes different inputs into account and based on that it generates results that are helpful for determining the status of the proposed system.

In order to generate intended results, the following are taken into account:

Deployment of the hardware components in every car, the algorithm works only for the area which has strong networks, it is only applicable to cars, only cases for a possible crash are considered, the driver must wear seat belt each time to record the heartbeats since heart rate sensor is embedded in the seatbelt.

Following are the cases that are considered for an accident and its chances (Table 21.1):

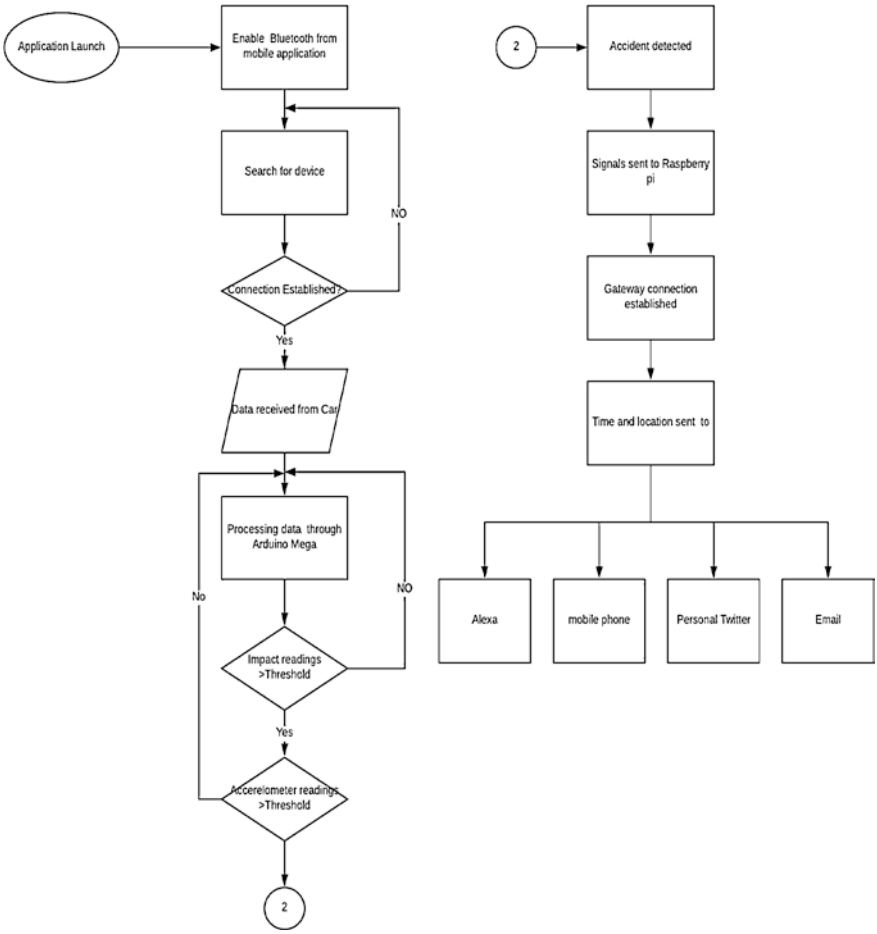


Fig. 21.2 Flow diagram of proposed system

Table 21.1 Shows the sensor ranges to determine an accident

Vibration sensor	Accelerometer (m/s^2)	Heart-rate sensor(bpm)	Inference
Low	Peak value	Normal range	Over speed
High	0	Peak value	Accident
High	0	0	Accident
High	Peak value	Peak value	Accident

- **Case 1: Warning to Avoid Accident**

  In this case, the driver is alerted for over-speeding

- **Case 2: When the car is static**

This case depicts a scenario for a possible crash when the car is at rest. The driver inside the car could be injured based on the value given by the heart rate sensor.

- **Case 3: When the car is static, and the driver is not inside**

  This case depicts a situation when the car is at rest, but the driver is not inside. This is also a case for an accident, but for such cases, emergency services need not be informed.

- **Case 4: When the car is moving**

  It is the most common case when a moving car gets hit by another vehicle. For such situations, emergency services must be prompted for rescue. It is the most common case when a moving car gets hit by another vehicle. For such situations, emergency services must be prompted for rescue.

In order to design the algorithm, the peak values of accelerometer and heart rate sensor are kept in mind.

According to the datasheets for the sensor, the peak value for the heart rate sensor is 170 bpm and above. The peak value of accelerometer is between −150 to −200 in case of retardation.

Let vibr, acc, and heartrate are the values of the vibration sensor, accelerometer, and heartbeat sensor.

Let hrSensor denote peak value for heart rate sensor, and accelSensor denote peak value accelerometer (Fig. 21.3).

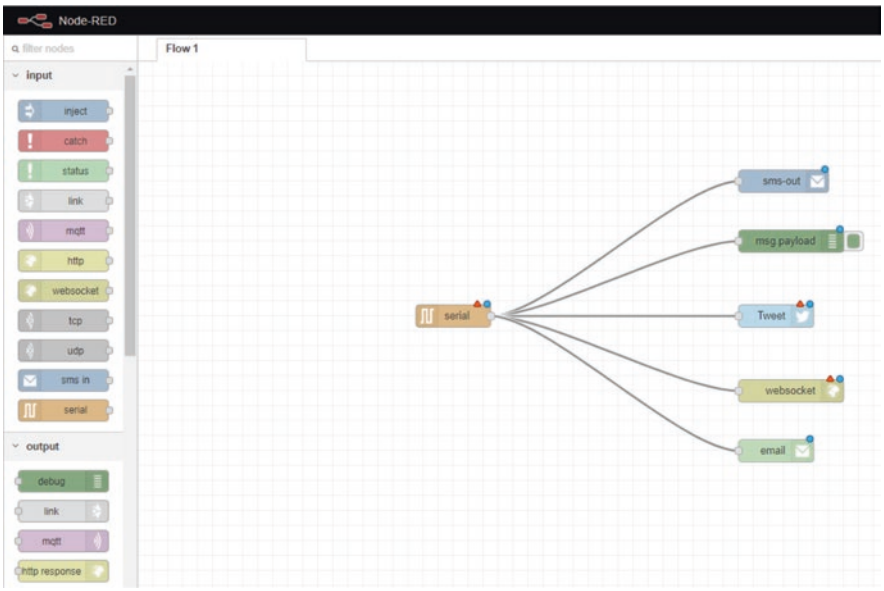


Fig. 21.3 Serial data to various services using NodeRED

```
                          1. Receive input from the sensors.
                           2. Process sensor input
\* Warning to avoid accident *\
                         3. While (vibr== LOW)
 {
If (acc == hrSensor)
{
         "Alert for over speeding of the vehicle."
}
                         }
/* When car has either high value for retardation or when car is
not moving and still there is a crash */
4. If (heartrate > =hrSensor)
{          /*for moving car (sudden crash results in retardation)
|| static car*/
            If (accelSensor == pt2 || accelSensor ==0)
 {
"Arduino Mega detects accident and sends data through serial"
                           "Data sent to various services through
Raspberry Pi Gateway."
            }
}
5. Exit
write your own algorithm
```

Node-RED is a programming tool for wiring together hardware devices, APIs, and online services which can be easily fit on most widely used devices like Raspberry Pi, BeagleBone Black, Arduino, Android-based devices, etc. It can be used for various purposes other than the Internet of Things, and it is very helpful for assembling flows of various services.

NODE-RED has replaced many low-level coding tasks and has enabled users to bind web services and hardware with a drag and drop interface. Most of the components are connected together to create a flow, and the code is generated automatically.

NODE-RED supports a lightweight runtime environment along with event-driven and non-blocking model as it is built on Node.js.

All the data flow created in NodeRED is using JSON format, which is easy to be imported or exported to any application API.

It can also be run locally (Docker support, etc.), and, it can run in a cloud environment like Bluemix, AWS, MS-Azure, etc.

The nodes used in the project are (Fig. 21.4):

1. SMS payload
2. Twitter
3. Email
4. HTTP Request
5. Debug

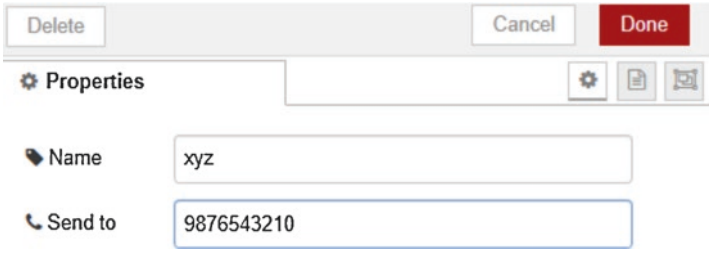


Fig. 21.4 SMS node configuration

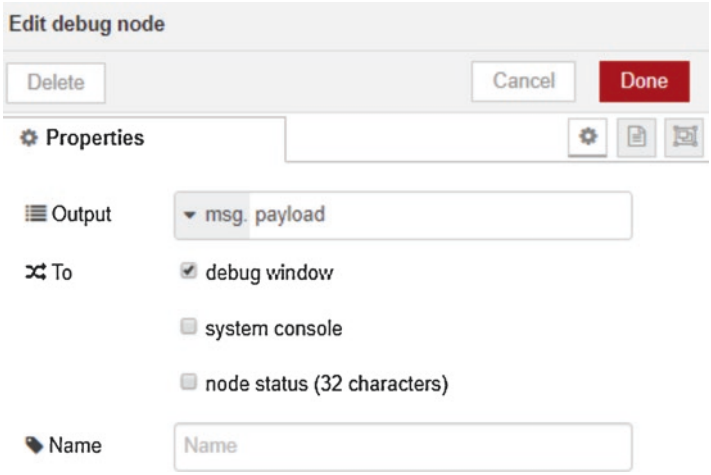


Fig. 21.5 Debug node configuration

To use the SMS service, the message topic is set to recipient's phone number, in international format.

ISO format will be used if the payload contains only Latin characters. Otherwise, the message will be sent in UCS2 encoding (Fig. 21.5).

Debug node displays selected message properties in the debug sidebar tab and optionally the runtime log. By default, it displays msg.payload, but can be configured to display any property, the full message, or the result of a JSON data expression (Fig. 21.6).

These nodes send a tweet for the authenticated user. If msg.media is set and contains a Buffer, it is attached as an image.

To send a Direct Message, the payload should be formatted as: D {username} {message} (Fig. 21.7).

Sends the msg.payload as an email, with a subject of msg.topic.

The default message recipient can be configured in the node; if it is left blank, it should be set using the msg.to property of the incoming message. If left blank you

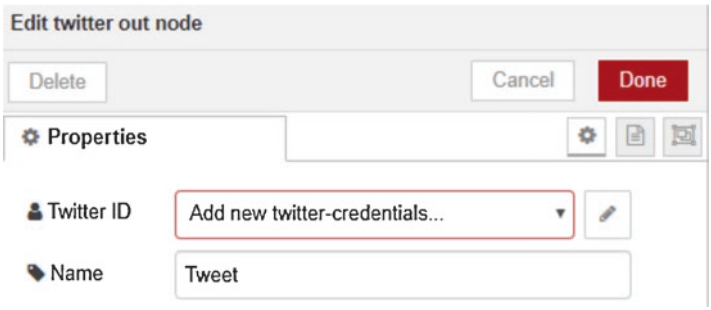


Fig. 21.6 Twitter node configuration

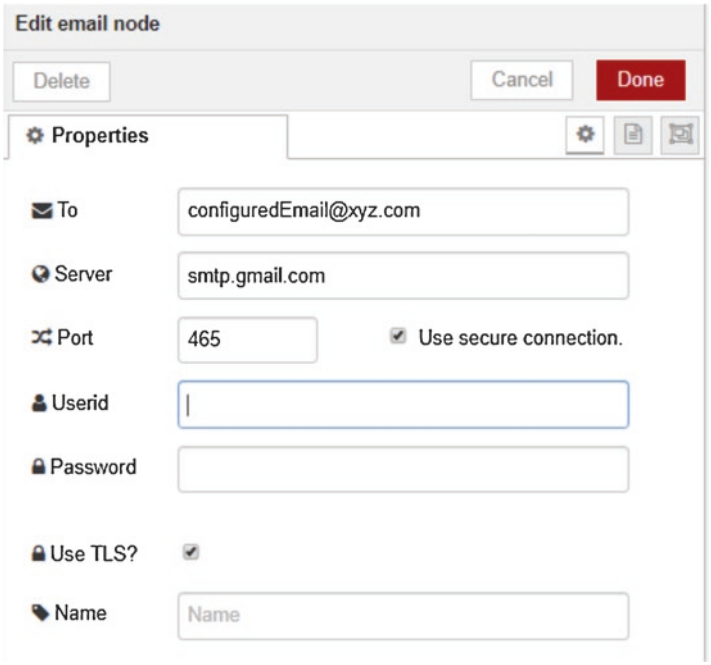


Fig. 21.7 Email node configuration

can also specify any or all of: msg.cc, msg.bcc, msg.replyTo, msg.inReplyTo, msg.referencesproperties.

You may optionally set msg.from in the payload which will override the userid-default value.

The payload can be HTML format (Fig. 21.8).

By default, msg.payload will be sent over the WebSocket. The socket can be configured to encode the entire msg object as a JSON string and send that over the WebSocket.

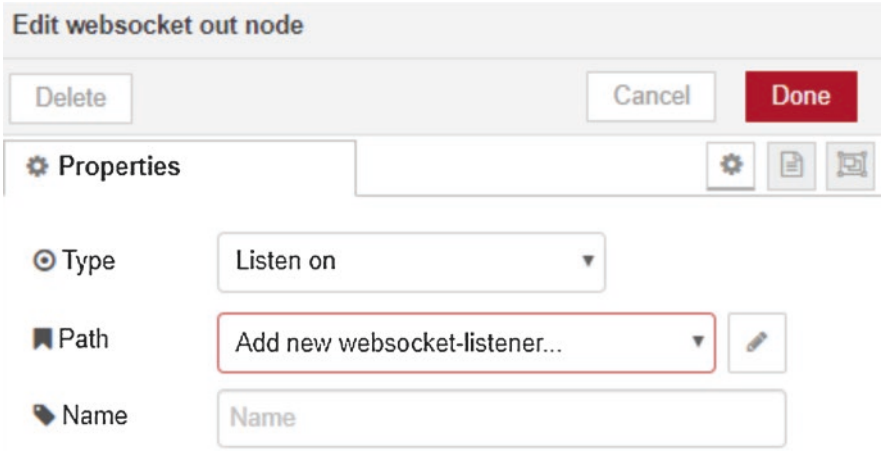


Fig. 21.8 API web socket node

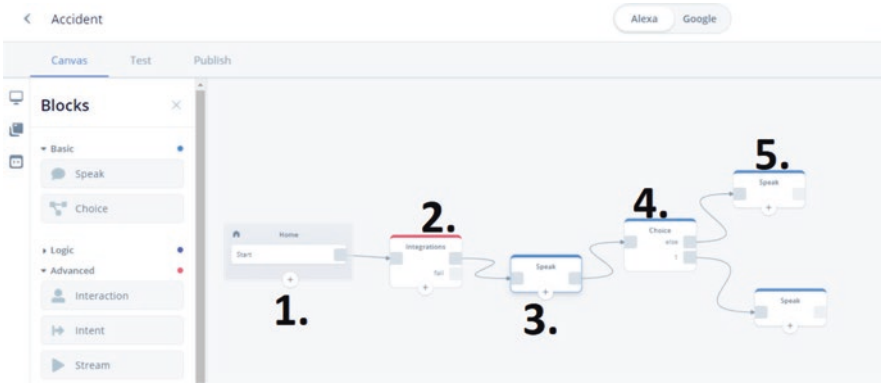


Fig. 21.9 Alexa App development using Voice Flow

If the message arriving at this node started at a WebSocket, in node, the message would be sent back to the client that triggered the flow. Otherwise, the message will be broadcast to all connected clients. To develop the Alexa Application, Voiceflow platform is used.

Voiceflow makes it faster & easier to build out a well-designed voice interface for your voice app. Using Voiceflow, you can:

Connect to APIs & 3rd party services using VF as your interface.

Build cross-platform (Alexa + Google) simultaneously (Fig. 21.9).

1. The initial node is the invocation name through which the Alexa skill can be activated.
2. The second node actually does the work of updating the skill with the latest knowledge of any accident that happened, with time and location.
3. The output from the second node, i.e., details of the accident (time, location) is passed to the third node where it is read and processed.

4. The fourth node asks the user whether to call the ambulance or not?
5. Based on the input received from the 4th node, the response is made (calling not included)

The last module of the project included an emergency push-button enabled ESP8266 NodeMCU module that intended to send an emergency mail to health organization of any accident that occurred. The device is intended for pedestrian safety and enabled with a programmed push button that is programmed to invoke the mail service as soon as it is pressed (Fig. 21.10).

SMTP is used to send messages. In this, we can only provide email and password using SMTP authentication. On the other hand, Google uses a more complex method for verification.

To send emails, we will need a Base64 encoded email address and password for Gmail account.

```
#ifndef G_SENDER
#define G_SENDER
#define GS_SERIAL_LOG_1          // Print to Serial only server
responce
//#define GS_SERIAL_LOG_2        //  Print to Serial client
commands and server responce
#include <WiFiClientSecure.h>

class Gsender
{
    protected:
        Gsender();
    private:
        const int SMTP_PORT = 465;
        const char* SMTP_SERVER = "smtp.gmail.com";
        const char* EMAILBASE64_LOGIN =
"[redacted]";
        const char* EMAILBASE64_PASSWORD = "c[redacted]=";
        const char* FROM = "pyushsingh27@gmail.com";
        const char* _error = nullptr;
        char* _subject = nullptr;
        String _serverResponce;
        static Gsender* _instance;
        bool AwaitSMTPResponse(WiFiClientSecure &client, const
String &resp = "", uint16_t timeOut = 10000);

    public:
        static Gsender* Instance();
        Gsender* Subject(const char* subject);
        Gsender* Subject(const String &subject);
        bool Send(const String &to, const String &message);
        String getLastResponce();
        const char* getError();
};
#endif // G_SENDER
```

Fig. 21.10 Block Diagram of Proposed System

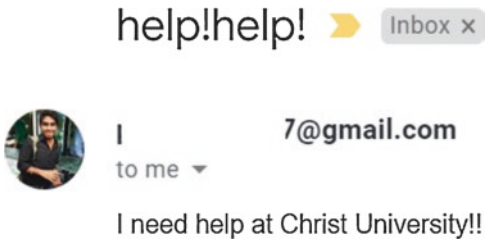


Fig. 21.11 Block Diagram of Proposed System

For encoding purpose, we can use base64encode.org and we will get results in the following manner -.

```
const char* EMAILBASE64_LOGIN = "Y2**********************b20=";
const char* EMAILBASE64_PASSWORD = "T*************I=";
Now set FROM field.
const char* FROM = "your_email@gmail.com";
That`s all for this part.
```

The Flash button on NodeMCU is connected between io 0 and ground. You can use it as a button. Set pinMode(0, INPUT_PULLUP) and you will read io 0 LOW if the button is pressed (Fig. 21.11).

21.5 Experimental Issues

During the execution of the experiments, we came across a few issues which were also resolved in due course of time with consistent efforts. The first problem we came across was the

(a) Amazon Notification Interrupt:
The Amazon Alexa development console doesn't provide the feature (as of January 2019) to interrupt the third party developed apps to notify the users directly. Hence, the user is required to trigger the apps using the invocation name to know the status of any notification by the Alexa Skill.

(b)Emergency Band size:
The Esp8266 NodeMCU module used to develop emergency band is small and can easily be accommodated on a wrist except when a precise location is needed. The precise location demands a GPS module that requires a relatively larger module to be integrated on the wrist. Hence, for demo purpose, the Wi-Fi ISP - location is sent as the accident location.

21.6 Results and Analysis

In this case, there can be a possible crash when the car is at rest, and the driver is inside. The accelerometer will give values low value or mostly 0 m/s^2. The vibration sensor will switch from low to high, the moment it experiences a crash with a larger impact. Table 21.2 depicts the numerical values responsible for an accident (Fig. 21.12).

From the above graph, it can be inferred that the heart rate sensor gives peak value for heartbeats when the acceleration is 0. This means that the driver is not in a healthy condition. Also, when both the sensor gives 0 value, then that means the driver is not inside the car, and that is why the heart rate sensor is 0.

21.6.1 Simulation for Moving Car Accident

This is a specific case depicted for a moving car. When the car meets with an accident, the accelerometer will experience a certain amount of retardation (negative acceleration). At this moment, the vibration sensor switches from low to high state. There are situations where the driver gets injured due to the impact of the crash because of which there will be a drastic change in the driver's heartbeat (Table 21.3).

Figure 21.13 represents the graph between accelerometer and heartrate sensor. According to the graph, when the car experiences high retardation due to crash, the driver's heartbeats raise up drastically indicating the cause of an injury. This situation calls for immediate help for an ambulance

Table 21.2 Sensor readings for static car accident

Vibration sensor	Accelerometer (m/s^2)	Heart-rate sensor(bpm)	Inference
1	0	190	Accident
1	0	170	Accident
1	0	195	Accident
1	0	185	Accident
1	0	0	Crash

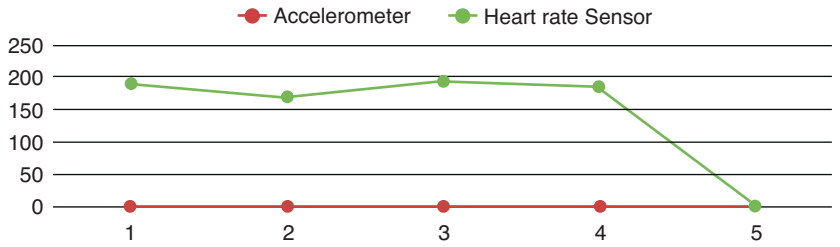


Fig. 21.12 Graph between Accelerometer and Heartrate Sensor

Table 21.3 Shows the sensor readings for moving car accident

Vibration sensor	Accelerometer (m/s^2)	Heart-rate sensor(bpm)	Inference
0	130	100	Over speed
1	−150	190	Accident
1	−180	170	Accident
1	−170	195	Accident
1	−200	185	Accident
1	−195	200	Accident

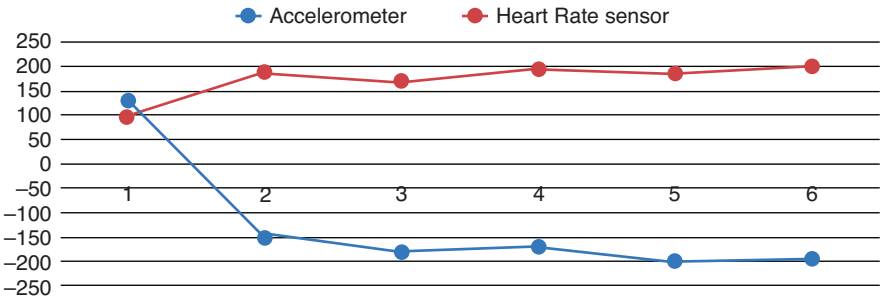


Fig. 21.13 Graph between Accelerometer and Heart Rate Sensor

Note that the values of the heart rate sensor vary according to the age of a person, and it has not been used for simulation. Only vibration sensor and accelerometer have been taken into account for testing.

However, in both the tables, only those cases are depicted that requires the need for a warning to the driver or emergency call to an ambulance.

21.7 Conclusion

Some studies have proposed the vehicle collision detection algorithm, which works well for T-intersection road design. The parameters that are considered for the design of the algorithm are, curvature area of T-intersection junctions and the predicted time for the two cars to meet at the junction. We feel that the algorithm is effective for the specific case of T-intersection and not for general road accidents. Therefore, there was a need for modifying the existing work done by authors to support general road accidents.

In our approach, addressing the gaps by adding an accelerometer, vibration sensor, and most importantly, heart rate sensor. These components contribute to the hardware setup of the system. Also, we introduced an algorithm for general road accidents. The main idea of this paper is to notify the concerned authorities about an accident only if the passengers are injured. This system can resolve most of the accident scenarios by detecting accidents on time and triggering immediate help from

emergency services without wasting any time. If implemented with proper planning and resources, this framework could serve to be a great help to society. Hence, there is a need for such systems that could save the lives involved with accidents.

References

Agarwal, P. (2017). *Technical Review on Different Applications, Challenges and Security in VANET Journal of Multimedia Technology & Recent Advancements*.

Aishwarya, S. R., et al. (2015). An IoT based accident prevention and tracking system for night drivers. *International Journal of Innovative Research in Computer and Communication Engineering, 3*(4), 3493–3499.

Ali, H. M., & Alwan, Z. S. (2015). Car accident detection and notification system using smartphone. *International Journal of Computer Science and Mobile Computing, 4*(4), 620–635.

Chatrapathi, C. et al. (2015). *Vanet based integrated framework for smart accident management system*. International conference on soft-computing and network security.

Kavya, K., & Geetha, C. R. (2016). Accident detection and ambulance rescue using raspberry Pi. *International Journal of Engineering and Techniques, 2*(2).

Khaliq, A. K., et al. (2017). *Prototype of automatic accident detection and management in vehicular environment using VANET and IoT*. 11th International conference on software, knowledge, information management and applications.

Kim, T., & Jeong, H. Y. (2014). A novel algorithm for crash detection under general road: Scenes using crash probabilities and an interactive multiple model particle filter 2014. *IEEE Transactions on Intelligent Transportation Systems, 15*, 2480–2490.

Namrata, H. S., et al. (2017). *Real time vehicle accident detection and tracking using GPS and GSM*.

Poorani, K., et al. (2017). IOT based live streaming of vehicle, position accident prevention and detection system. *International Journal of Recent Trends in Engineering and Research, 3*, 52–55.

Pratiksha, Kumar, V., & Gauns, R. (2015). Proposed model for the smart accident detection system for smart vehicles using Arduino board, smart sensors, GPS and GSM. *International Journal of Emerging Trends and Technology in Computer Science*.

Raut, P., & Sachdev, V. (2014). Car accident notification system based on Internet of Things. *International Journal of Computer Applications (0975 – 8887), 107*(17), 29–31.

Reddy, S., & Rao, R. (2016). Fire accident detection and prevention monitoring system using wireless sensor network enabled android application. *Indian Journal of Science and Technology, 9*(17), 1–5.

Sandeep, K., & Ravi Kumar, P. (2017). *Novel drunken driving detection and prevention models using internet of things*. International conference on recent trends in electrical, electronics and computing technologies.

Singhal, A., et al. (2016). *Intelligent accident management system using IoT and Cloud Computing*. 2nd International conference on next generation computing technologies.

Yadav, U., & Kannan, K. (2017). Smart vehicle monitoring system using IOT. *International Journal for Development of Computer Science and Technology, 5*(3).

Chapter 22
Prioritisation of Challenges Towards Development of Smart Manufacturing Using BWM Method

Shahbaz Khan, Mohd Imran Khan, and Abid Haleem

Abstract In the era of digitalisation, daily life is equipped with digital products and services. These smart products now become the necessity of everyday life. To fulfil the huge amount of demands of such product in a sustainable way, smart manufacturing is evolving. However, the development of smart manufacturing is facing many challenges from various perspective. These challenges need to overcome for the development of smart manufacturing. Therefore, the aim of this chapter is to identify and prioritise these challenges, which can be helpful to overcome these challenges. In this study, 16 challenges are identified towards the development of smart manufacturing from the literature review and experts' input. Additionally, these challenges are categorised in four dimensions. After that, these dimensions and their associated challenges are prioritised based on their importance using the best worst method (BWM). The result clearly shows that infrastructure-related challenges are the most significant while consumer related challenges are least significant. The identified challenges are helpful for the development of smart manufacturing. The prioritisation of these challenges assists the management and policymakers to formulate the strategies for the mitigation of these challenges. This study provides 16 challenges that can be evaluated by manufacturers/companies to realize the readiness for smart manufacturing transformation. This chapter provides an understanding of the smart manufacturing and associated challenges towards its development.

Keyword Challenges · Best Worst Method (BWM) · Smart product · Smart manufacturing · Big data

S. Khan · M. I. Khan · A. Haleem (✉)
Department of Mechanical Engineering, Faculty of Engineering and Technology, Jamia Millia Islamia, New Delhi, India
e-mail: ahaleem@jmi.ac.in

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_22

22.1 Introduction

In the last decade, there has been excessive advancement in manufacturing and its related fields such as mechanical automation, business analytics and cloud computing. These developments would offer the industries to enhance their conventional production system and adopt the concept of "smart manufacturing". Wang et al. (2018) refers the smart manufacturing as "… a new manufacturing paradigm where manufacturing machines are fully connected through wireless networks, monitored by sensors, and controlled by advanced computational intelligence to improve product quality, system productivity, and sustainability while reducing costs." In the context of this definition, the elements of "smart manufacturing" is a combination of the several advanced technologies such as industrial internet of things (IIoT), cyber-physical systems (CPS), IoT, cloud computing, additive manufacturing, industrial integration, virtual and augmented reality, big data analytics and others (Xu et al. 2018). Smart manufacturing collects real-time data through digital technologies and provides valuable information to the manufacturing system by analysing this data. These collected real-time data allows the manufacturer to improve the system and provide some after-sell services such as fault deduction, preventive maintenance and system update.

Smart manufacturing has the capabilities to bring substantial benefits to firms through reducing the wastage of material, processing time, operational expenses and capital expenditure. Moreover, smart manufacturing not only enhance the economic perspective, such as the reduction in cost and improved productivity but also create new values that can continuously contribute to societies. It is not only to construct an intelligent system through convergence with advanced technologies, but it also advances as a constant growth engine for manufacturing with human and society-oriented philosophy through 'sustainable development' (Kang et al. 2016).

However, the adoption of the advanced technologies to achieve the goal of smart manufacturing has made the manufacturing system more complex and led to many challenges related to the consumers, management and others. These challenges are the bottlenecks towards the development of smart manufacturing which needs to be addressed. Apart from the development of smart manufacturing, the transform the conventional manufacturing system into a smart manufacturing system is also facing similar challenges. This transformation requires a lot of efforts to overcome the challenges for the successful transformation of smart manufacturing which needs to be addressed. Therefore, this study has primary objectives as follows:

- Identify the major challenges towards the development of smart manufacturing
- Prioritise the major challenges using the BWM method

The remaining study is as follows: Sect. 22.2 provides the literature review related to smart manufacturing; Sect. 22.3 deals with the methodology adopted for this study; Sect. 22.4 identifies the major challenges of the development of smart manufacturing; Sect. 22.5 deals with the prioritisation of the identified challenges;

Sect. 22.6 provides the result and elaborate the finding Finally, section provides the conclusion, limitations and future scope of the study.

22.2 Literature Review

In order to develop the background for this study, a review and synthesis of the literature related to the concept of smart manufacturing had been undertaken. Additionally, some significant studies related to smart manufacturing is also discussed in this section.

22.2.1 Overview of Smart Manufacturing

Nowadays, 'smart' is the buzz word in various domain of life such a 'smart cities', 'smart technologies' and 'smart manufacturing'. The manufacturing industries going through a new revolution and paradigm named as 'smart industries.' The manufacturing processes are adopted in the smart industries are termed as 'smart manufacturing.' Smart manufacturing is rapidly developing in the context of technologies, application methods and integrated concept. Before the arrival of the smart manufacturing, contemporary manufacturing technologies ranging from digital manufacturing, virtual manufacturing, and advanced manufacturing to sustainable manufacturing have been converged with ICT (Khan et al. 2015a; Kang et al. 2016). As is the case with many emerging technologies, there is no single universally accepted definition of smart manufacturing. The widely accepted definition are presented by the National Institute of Standards and Technology (NIST), which defines Smart Manufacturing as systems that are "fully-integrated, collaborative manufacturing systems that respond in real-time to meet changing demands and conditions in the factory, in the supply network, and in customer needs (Kusiak 2017)."

In recent years, the organisation focuses to develop the cyber-physical system through the integration of the manufacturing assets (i.e. physical assets) with the cyberspace (Alam et al. 2015; Khan et al. 2017a). According to the Kusiak (2017), smart manufacturing having two layers 'cyber layer' and 'manufacturing equipment layer' and these layers are linked by the interface. The cyber layer provided the system intelligence while manufacturing equipment has its own intelligence.

Smart Manufacturing is the integration of a large number of advanced technologies which can be developed individually and/or combination with other technologies (Khan et al. 2020). For instance, IoT, big data analytics and smart sensors were studied mostly on machines or processes (Javaid et al. 2020). Kusiak (2017) identified the six significant pillars of smart manufacturing. These six pillars are manufacturing technology and processes, predictive engineering, big data, materials, resource sharing & networking and sustainability (please refer Fig. 22.1). These

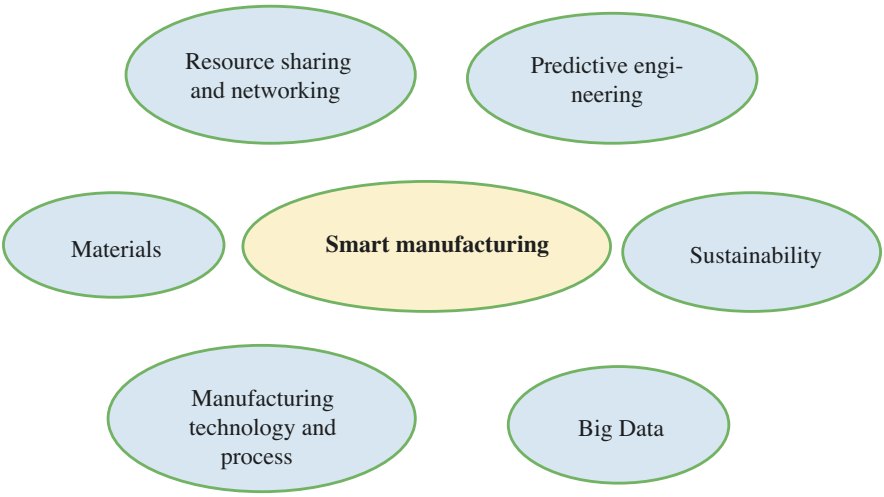


Fig. 22.1 Six pillars of smart manufacturing. (Adapted and modified from Kusiak)

pillars are always present around the manufacturing systems in different names and the different degree of importance. For example, data has been an essential part of traditional manufacturing system, and it has become big data in the context of smart manufacturing.

22.2.2 Smart Manufacturing Related Studies

The primary goal of smart manufacturing is the enhance the productivity, process improvement, sustainability and automation (Rajput and Singh 2018). Several studies are carried out in the context of smart manufacturing and its associated areas from various aspects. Kang et al. (2016) reviewed the literature of smart manufacturing as well as related areas and highlighted the major challenges and bottlenecks of smart manufacturing. Further, they suggested some valuable investigation for future research work in this emerging area. Siddiqui et al. (2016), discussed the other aspect of smart manufacturing such as the architecture of smart manufacturing, low latency setup of the latest 5G technology and new business ventures. Zhong et al. (2017) focuses on the technological aspect of smart manufacturing and overviewed the concept of smart manufacturing objects handled with wireless technologies and IoT. Some studies focus on the pillars of the smart manufacturing such as Khan et al. (2017b) have identified the major challenges towards the development of a big scholarly data platform. In this row. Khan et al. (2015b) has proposed a framework for the management of Big Data in cloud environment and further develop an outline for Big Data.

Kadera and Novák (2017) initially identified the value of the distributed and smart industrial systems of smart manufacturing. Further, they proposed some major points to handle the complications in communications among the interconnected devices. Cheng et al. (2017) proposed some smart cutting tools which can be used for the smart machining and further they also discussed the design, implementation, and application issues of these smart cutting tools. Li et al. (2017) studied the issue of big data in the context of smart manufacturing and optimised the load-balance of the devices. Smart manufacturing also utilised the 3D printing machine, in this regard major challenges are categorised into technical and managerial by Chen and Lin (2017). Kymäläinen et al. (2017) established a novel model for the user experience in the environment of smart industry. The issue of maintenance of the manufacturing system related to the big data is studied by Wan et al. (2017). They studied active preventive maintenance in smart manufacturing systems.

Kusiak (2017) provide an overview of the concept of the 'smart manufacturing' and addressed the issue of material handling. Further, they provide the ten conjectures of smart manufacturing. Tuptuk and Hailes (2018) addressed the security issues in the smart manufacturing system. They discuss the security of existing manufacturing systems and associated weakness and argue that security must play a key role in the development of smart manufacturing. Manavalan and Jayakrishna (2019) reviewed the several aspects of supply chain management, enterprise resource planning, IoT and Industry 4.0. Further, they explore the potential opportunities available in IoT embedded sustainable supply chain for smart manufacturing transformation.

22.3 Research Methodology

This study adopted two-phase methodology to fulfil the objective of the study. In the first stage, major challenges towards the development of smart manufacturing are identified through literature review and expert's input. The SCOPUS database is chosen for the selection of the articles to identify the major challenges towards the development of smart manufacturing. Initially, 22 challenges are identified through the literature review. These significant challenges are put in front of the expert panel and asked them to provide their responses based on the importance of the challenges. The expert's panel contains six members from the industry and academia. After the discussion with the experts' panel, six challenges are dropped and finally, 16 challenges are selected for further evaluation. Further, these finalised challenges are categorised into four major dimensions. In this manner, 16 major challenges and four dimensions of these challenges are finalised.

In the second phase of the study, these challenges are prioritised based on their importance. For serving this purpose, several multicriteria decision making (MCDM) technique are available in the literature such as AHP, ANP, TOPSIS, BWM and many more (Sufiyan et al. 2019; Khan et al. 2019a, b). Among these MCDM methods, BWM is selected for the prioritisation of the challenges. The

rationale behind the selection of this method is the capabilities of the BWM. This method required a smaller number of comparisons as compared to other methods such as AHP and ANP (Rezaei 2015; Khan et al. 2019b). Therefore, it takes less time of experts and less cost to take input from the experts. Additionally, the consistency ratio of this method is also high as compared to the other MCDM method. The application of this methodology is seen in several recent studies (Ahmadi et al. 2017; Pamučar et al. 2018; Rezaei et al. 2017; Cheraghalipour and Farsad 2018; Khan et al. 2019a, b). The adopted research framework is shown in the Fig. 22.2. The steps of the BWM method are provided as follows (Rezaei 2015):

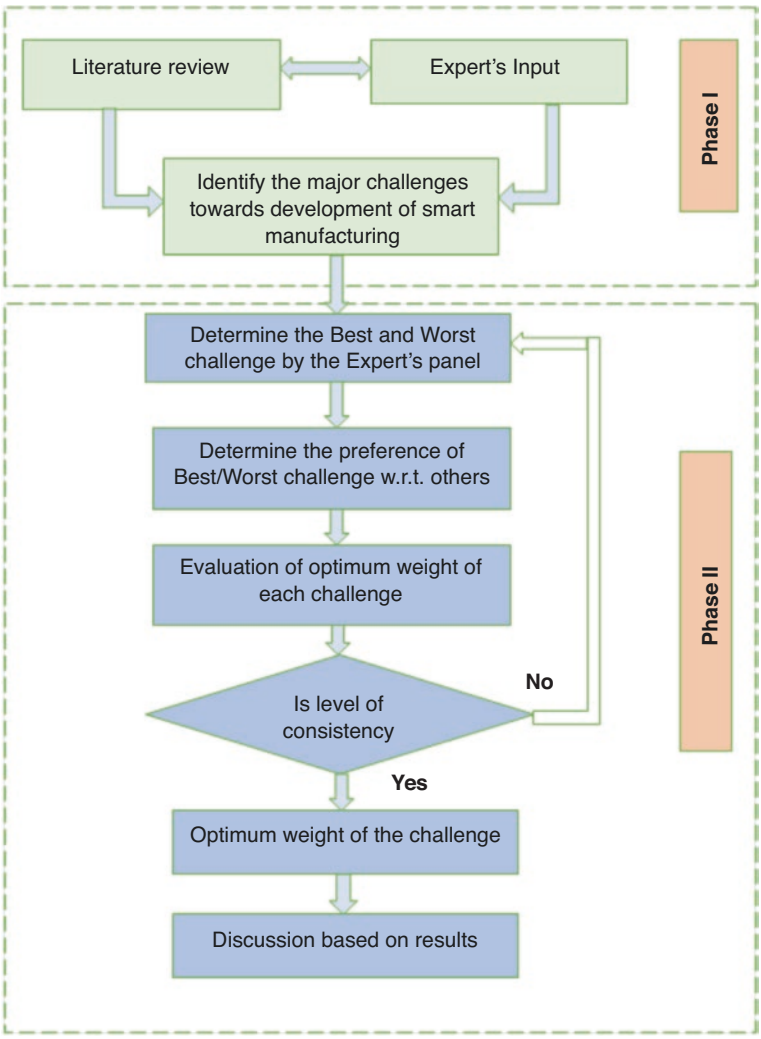


Fig. 22.2 Proposed research framework for this study

Step 1: Identification of decision criteria

In this step, literature review and expert's inputs are used to identify a certain set of criteria ("n" number of criterion: C_1, C_2, C_3,….C_n) which is important in decision making for the identified problem.

Step 2: Identify the best criterion (most significant) and the worst criterion (least significant)

In this step, the expert (decision maker) identifies the best and the worst criterion among the all identified criterion. The best criterion is represented as c_B, and the worst criterion is represented by c_W.

Step 3: Perform the reference comparisons for the best criterion.

The preference of the best criterion is determined over all the other criteria using 9-point scale (1–9) through expert input and represented by the vector as shown below:

$$A_B = \left(a_{B1}, a_{B2}, \ldots\ldots, a_{Bn}\right)$$

Where A_B the Best-to-Others (BO) vectors, a_{Bj} refers the preference of the best criteria B over criteria j and $a_{BB} = 1$

Step 4: Perform the reference comparisons for the worst criterion

The preference of the other criterion is determined over the worst criteria using 9-point scale (1–9) through expert input and represented by the vector as shown below:

$$A_W = \left(a_{1W}, a_{2W}, \ldots\ldots, a_{nW}\right)^T$$

Where A_B the Others-to-Worst vector, a_{jw} refers the preference of the criteria j over the worst criteria W and $a_{ww} = 1$

Step 5: Determine the optimal weights

The optimal weight for each criterion is the one where, for each pair w_B/w_j and w_j/w_W, it should have $w_B/w_j = a_{Bj}$ and $wj/w_W = a_{jW}$. To satisfy these conditions for all j, maximum absolute differences minimized of the set $\{|w_B - a_{Bj}w_j|, |w_j - a_{jW}w_W|\}$. This problem can be represented as following model:

$$\min \max \left\{ \left| w_B - a_{Bj} w_j \right|, \left| w_j - a_{jW} w_W \right| \right\}.$$

Subject to:

$$\sum_j w_j = 1 \tag{22.1}$$

$$w_j \geq 0; \forall \mathrm{j}$$

Model (22.1) can be transformed into following linear problem.
min ξ^Lsubject to:

$$\left|\frac{w_B}{w_j} - a_{Bj}\right| \xi^L \quad \forall \mathrm{j}$$

$$\left|\frac{w_j}{w_W} - a_{jW}\right| \xi^L \quad \forall \mathrm{j}$$

$$\sum_j w_j = 1$$

$$w_j \geq 0 \quad \forall \mathrm{j} \tag{22.2}$$

The optimal weights of each criterion $\left(w_1^*, w_2^*, w_3^* \ldots .. w_n^*\right)$and the optimal value of ξ^Lobtained by solving the linear problem (22.2). Consistency level of each comparison is checked through the value of ξ^L and the value of ξ^Lcloser to 0 indicates higher consistency and vice versa. (Rezaei 2016).

22.4 Result

In this section, the major challenges of smart manufacturing are identified through the literature review and expert opinion. These finalised challenges are prioritised using the BWM method.

22.4.1 Identification of Challenges in Smart Manufacturing

The major challenges are identified through the literature review of smart manufacturing, intelligent manufacturing system and industry 4.0. After identification of the 22 challenges, these challenges are put in front of experts for their approval. We have discussed these identified challenges with the expert's panel and finalised 16 major challenges which are further categorised into four dimensions. The identified 16 challenges with their brief description and associated references are shown in Table 22.1.

Table 22.1 Summary of challenges

Dimensions	Challenges	Description	References
Technological challenges (TC)	Data privacy and security issues (TC1)	Privacy and security of the industrial data (i.e. process details, maintenance schedule, customer details etc.) are the primary issue for the development of smart manufacturing in a sustainable manner	Elkhodr et al. (2016), and Kumari et al. (2018)
	Data quality (TC2)	Data acquisition and processed by different people/industries under special regimes and tainted with several types of imprecision, imperfection, uncertainty, and ambiguity	Alam and Alam (2013), d'Aquin et al. (2015), Ben Sta (2017), and Bibri (2018)
	Lack of advance materials and technologies (TC3)	New and upgraded materials are required for modern products and to manufacture these materials unconventional and complex manufacturing technologies are required. The scarcity of type of advance materials and technologies created a challenge towards the development of smart manufacturing	Yeh and Chen (2018) and Masood and Egger (2019)
	Lack of advanced research and development centres (TC4)	Advanced research centres are required for the design and development of smart product and processes which is essential to develop smart manufacturing. However, lack of these advance research centres is the major challenge	Hermann et al. (2016), and Luthra and Mangla (2018)
Infrastructure related challenges (IC)	Lack of capability to perform the supply chain analytics (IC1)	To be competitive in the market, the effectiveness of the supply chain can be enhanced through the business intelligence and supply chain analytics. Lack of these capabilities is the major challenge to develop smart manufacturing.	Wang et al. (2018) and Sun et al. (2016)
	High IT infrastructure and intelligence deficit (IC2)	Lack of IT infrastructure (e.g solar electrical systems, cloud computing, virtual reality) and artificial intelligence capabilities (e.g. smart communities, smart energy solutions, intelligent transport system, etc.) is set a challenge towards the adoption of smart manufacturing	Ahamd and Alam (2014), Zhou et al. (2016), and Rajput and Singh (2019)
	Lack of smart logistics infrastructure (IC3)	The internal logistics (within factories) and external logistics (inbound and outbound logistics) are needs to be at an advanced level for the successful survival of the smart factories. The development of the smart logistics infrastructure is the major challenge.	Qaiser et al. (2017) and Peraković et al. (2019)

(continued)

Table 22.1 (continued)

Dimensions	Challenges	Description	References
	Lack of global distribution network (IC4)	Global distribution network assists the supply chain partners to expand the range of targets which seems difficult due to the lack of knowledge regarding a recent technology.	Lee et al. (2013), Shakil and Alam (2016), and Masood and Egger (2019)
Consumers related challenges (CC)	Lack of access to technology (CC1)	Majority of consumers (especially developing economies) having lack of access to smart digital technologies that can be a challenge toward smart manufacturing development	Perales et al. (2018) and Rajput and Singh (2018)
	Low awareness of consumers (CC2)	Consumers are not very much aware about the concept of smart manufacturing, and its impact on their quality of life	Schuh et al. (2017) and Reyna et al. (2018)
	Health issues (CC3)	The smart manufacturing system might use 5G technologies for establishing communication with other smart factorises which causes an adverse effect on the human health	Expert opinion
	Issues of openness of data (CC4)	Consumers are also concerned about their openness of the data (for example-using pattern of appliances) which can be accessed by the several stakeholders.	Pereira et al. (2017), Kumar et al. (2018), and Rajput and Singh (2018)
Management related challenges (MC)	Cost of training and skills development (MC1)	Skill development can be achieved through the training of the working personnel, which needs a higher cost. This higher cost is one of the major challenges towards the smart manufacturing development	Zhou et al. (2016) and Wang et al. (2018)
	Unclear vision towards smart manufacturing (MC2)	Lack of vision on how management can be effectively imposed to develop and run the smart manufacturing	Chourabi et al. (2012), Hecklau et al. (2016), and Hofmann and Rüsch (2017)
	Organisational change/ Re-engineering (MC3)	To transform the conventional manufacturing system into a smart manufacturing system requires a lot of re-engineering in processes as well as culture, which is the major challenge for top management.	Khan et al. (2018) and Pacaux-Lemoine et al. (2019)
	Green technology management (MC4)	For the suitability of smart manufacturing, green technologies and green energy resources are adopted and managed. The adoption and management of green technology is also a challenge for top management.	Moktadir et al. (2018), Luthra and Mangla (2018), and Ali et al. (2019)

22.4.2 Prioritisation of the Challenges Towards Development of Smart Manufacturing

In this section, the identified challenges towards the development of smart manufacturing are prioritised. To accomplish this purpose, BWM is successfully applied using the expert's input. A brief overview of the BWM is provided to the expert's panel to revive the understanding about the adopted methodology. After that, the pairwise comparison matrices were provided for each dimension and their associated to the expert panel and asked them to identify the best challenge i.e. most significant challenge and worst challenge i.e. least significant challenge among the all identified challenges. Initially, there were different inputs comes from the experts but after exhaustive discussion by experts and moderator about each challenge, the panel were able to build a consensus on the comparative significance of each challenge.

Based on the expert panel decision, 'infrastructure related challenges' are the most significant challenge (best criteria) and 'consumer related challenge' are the least significant challenge (worst criteria). After identification of the best and worst dimension (criteria), experts rated the preferences of best dimension over other dimensions and similarly all the other dimensions were rate w.r.t the worst dimension on a scale of 1–9. In this manner, a pairwise comparison was obtained and shown in Table 22.2.

Table 22.3 shows the pairwise comparison of infrastructure-related challenges. Among the identified four challenges related to infrastructure, the most significant challenge is the 'lack of capability to perform the supply chain analytics (IC1)' and the 'least significant challenge is lack of global distribution network (IC4)'.

Table 22.2 Pairwise comparison of Technology related challenges

BO	TC1	TC2	TC3	TC4
Best criteria:TC1	1	2	5	4

OW	Worst criteria:TC3
TC1	5
TC2	4
TC3	1
TC4	3

Table 22.3 Pairwise comparison of Infrastructure related challenges

BO	IC1	IC2	IC3	IC4
Best criteria:IC1	1	2	3	6

OW	Worst criteria: IC4
IC1	6
IC2	5
IC3	4
IC4	1

Table 22.4 Pairwise comparison of consumers related challenges

BO	CC1	CC2	CC3	CC4
Best criteria:CC4	4	6	3	1

OW	Worst criteria:CC2
CC1	3
CC2	1
CC3	4
CC4	7

Table 22.5 Pairwise comparison of management related challenges (MC)

BO	MC1	MC2	MC3	MC4
Best criteria:MC2	3	1	2	3

OW	Worst criteria: MC4
MC1	2
MC2	4
MC3	3
MC4	1

Table 22.4 shows the pairwise comparison of consumers related challenges. The most significant challenge is the 'issues of openness of data (CC4)' and the least significant challenge is 'low awareness of consumers (CC2)'.

Table 22.5 shows the pairwise comparison of management-related challenges (MC). Among the identified four challenges related to management, the most significant challenge is the 'unclear vision towards smart manufacturing (MC2)' and the 'least significant challenge is 'green technology management (MC4)'.

Further, we have to find the optimal weight of each dimension and their associated challenges using the pairwise comparison score. This can be obtained by formulating a linear programming model as shown by the model (2) for dimensions and associated challenges. After the formulation of the model; these models are solved to calculate the weights of each dimension and their associated challenges and shown in Table 22.6. The consistency ratio of the dimension is 0.06504 which is acceptable because it is less than the 0.1. Similarly, the consistency ratio of the challenges is also less than 0.1 which is acceptable. Based on the optima weight of the dimensions and challenges, the dimensions and challenges are locally and globally ranked and shown in Table 22.6.

22.5 Discussion on Results

The result shows that the most significant dimension of challenge 'infrastructure-related challenges' having 0.471545 and the least significant challenge is 'consumers related challenges (CC)' having 0.081301. The infrastructure-related challenges

Table 22.6 Ranking of dimensions and challenges

Dimensions	Weights of dimensions	Consistency ratio of dimensions	Challenges	Weights of challenges	Consistency ratio of challenges	Local rank	Global weights	Rank
TC	0.268293	0.06504	TC1	0.486842	0.09210	1	0.130616	2
			TC2	0.289474		2	0.077664	6
			TC3	0.078947		4	0.021181	12
			TC4	0.144737		3	0.038832	9
IC	0.471545		IC1	0.473684	0.078947	1	0.223363	1
			IC2	0.276316		2	0.130295	3
			IC3	0.184211		3	0.086864	4
			IC4	0.065789		4	0.031022	11
CC	0.081301		CC1	0.160305	0.09160	3	0.013033	15
			CC2	0.076336		4	0.006206	16
			CC3	0.21374		2	0.017377	14
			CC4	0.549618		1	0.044684	8
MC	0.178862		MC1	0.176471	0.08823	3	0.031564	10
			MC2	0.441176		1	0.07891	5
			MC3	0.264706		2	0.047346	7
			MC4	0.117647		4	0.021043	13

need to be addressed to move a step forward in the direction of the develop a smart manufacturing system. Among the 'infrastructure relate challenges' the descending order of the infrastructure-related risk are: 'lack of capability to perform the supply chain analytics (IC1)'> 'high IT infrastructure and intelligence deficit (IC2)' > 'lack of smart logistics infrastructure (IC3)' > 'lack of global distribution network (IC4)'. To overcome these challenges, the government required an especial focus on the development of the IT infrastructure such as high-speed network connectivity. Utilising these infrastructures, the organisation can develop the skills and capability to perform supply chain analytics. At the same time, there a major challenge is the scarcity of smart logistics services. This challenge is more dominant in developing countries such as India. The least significant challenge among the infrastructure-related challenge is the 'lack of global distribution network' which needs to be addressed.

The next significant dimension of challenges is the 'technology-related challenges 'having the weight of 0.268293. This dimension having a technological challenge such as 'lack of advance materials and technologies' and 'data privacy and security which can hinder the development/transformation of smart manufacturing. The importance of the challenges in descending order are: 'data privacy and security issues (TC1)' > 'data quality (TC2)' 'lack of advanced research and development centres (TC4)' > 'lack of advance materials and technologies (TC3)'. Data privacy and security is a major challenge because it contains the confidential data about the materials, manufacturing process and details of the working/operating personnel. Data is collected from the different sources and these data are present in a different form so that the data quality is low. This data quality is a major challenge to develop

the predictive aspect of smart manufacturing. There is a lack of advanced research centres for the development of smart manufacturing process, data cleaning and analysing techniques. These advance research centre should be developed for the effective implementation of the smart manufacturing processes and techniques. In this row, the next major challenge is the lack of advance materials and technologies that can be a major hindrance towards the development of smart manufacturing.

The third significant dimension of the challenges related to the development of smart manufacturing is 'management related challenges' having the weight of 0.178862. The importance of the challenges in descending order are: 'unclear vision towards smart manufacturing (MC2)' > 'cost of training and skills development (MC1)' > 'organisational change/re-engineering (MC3)' > 'green technology management (MC4)'. The unclear vision of the management is a major challenge towards the development of smart manufacturing. To overcome this challenge, management should develop an understanding about the smart manufacturing process such as cyber-physical systems, big data analytics and interconnected machines. After developing a clear understanding of smart manufacturing, management has proposed a clear vision and achieve the goal of smart manufacturing. Next challenge is the cost of the training and skill development of the personnel. The environment of smart manufacturing is different from the conventional manufacturing system, so that, some training and skill development program is conducted for the personnel that will demand a high cost. Further, the third challenge in the context of the management related challenge is the 'organisational change/re-engineering (MC3)'. The current organisational and manufacturing structure should be re structured and redesigned as per the requirement of smart manufacturing. The least significant factor related to management is 'green technology management (MC4)'. Green technologies and their management are an essential component of the current business models. Therefore, to be competitive in the global business, green technologies should be adopted for the effective functioning of smart manufacturing.

Finally, the consumer-related challenges are having the least significant among the identified dimensions of the development of the smart manufacturing system. Consumer related challenges are ranked fourth and having the weight of 0.081301. Among the consumer-related factors, importance order of the challenges is: health issues (CC3) > issues of openness of data (CC4) > lack of access to technology (CC1) > Low awareness of consumers (CC2). The major challenge is health issues which are emerging from the utilisation of the advanced technologies such as 5G connections for the machine, eatable barcode and DNA barcoding on food products. These advanced technologies facilitate life but also have some bad effect on health. The next challenge is the issues of openness of data (CC4) which are related to the private information of the consumer. This information can be stored and transferred with other parties which are the major issue for consumers. Lack of access to technologies by consumers is one of the significant challenges towards the development of smart manufacturing. The smart devices are providing real-time data to the cloud. In this condition, if the consumer does not have access of advance technologies then it will lead to the failure of smart manufacturing. Finally, the least significant challenge is the low awareness of consumers that means consumers does not have an

explicit knowledge of the benefits or loss of the smart manufacturing system. Thus, they are having ambiguities in their perception towards the smart manufacturing and its related product. Therefore, there is a need to aware the consumers about the smart manufacturing and its benefits/cost through the awareness programs or other means.

22.6 Conclusion, Limitations and Future Scope

This chapter provides an overview of smart manufacturing and identified the challenges towards the development of smart manufacturing. Initially, this study identified the 16 major challenges towards the development of smart manufacturing and categorised them into four major dimensions using the literature review and expert's input. These identified challenges and their dimensions are prioritised using the BWM method for deeper insights. The result shows that the major dimension of the challenge is the infrastructure-related challenges among the identified dimensions. The least important challenge is consumer-related challenges. This study also provides some solution to mitigate these challenges.

This study also has some limitation which can be explored in future studies. The first limitation of this study is the scarcity of the literature in the area of smart manufacturing. Due to the limited access to the literature, there is a possibility to skip some challenges which can be included. Second limitation of this study is the sample size of the expert. We have only six experts in the panel and this sample size can be increased in the future studies. The prioritisation of the identified challenges can be validated through case studies. In term of the future scope, these identified challenges can be modelled using the other methods such as Interpretive Structural Modeling (ISM), Total Interpretive Structural Modelling (TISM) and DEMATEL. Further, the prioritisation of the challenges can be validated using other methods such as AHP, ANP, TOPSIS and many more.

References

Ahmad, S., & Alam, M. (2014). Balanced- ternary logic for improved and advanced computing. *International Journal of Computer Science and Information Technologies, 5*(4), 5157–5160.

Ahmadi, H. B., Kusi Sarpong, S., & Rezaei, J. (2017). Assessing the social sustainability of supply chains using best worst method. *Resources, Conservation and Recycling, 126*, 99.

Alam, M., & Alam, B. (2013). Cloud query language for cloud database. In: *Proceedings of the International conference on Recent Trends in Computing and Communication Engineering* – RTCCE 2013, Hamirpur, HP, pp. 108–112, ISBN: 978-981-07-6184-4 https://doi.org/10.3850/978-981-07-6184-4_24.

Alam, M., Sethi, S., & Shakil, K. A. (2015). Distributed machine learning based biocloud prototype. *International Journal of Applied Engineering Research, 10*(17), 37578–37583.

Ali, S., Affan, M., & Alam, M.. (2019). A study of efficient energy management techniques for cloud computing environment. 2019 9th international conference on cloud computing, Data Science & Engineering (Confluence).

Ben Sta, H. (2017). Quality and the efficiency of data in "smart cities". *Future Generation Computer Systems, 74*, 409–416.

Bibri, S. (2018). A foundational framework for smart sustainable city development: Theo-retical, disciplinary, and discursive dimensions and their synergies. *Sustainable Cities and Society, 38*, 758–794. https://doi.org/10.1016/j.scs.2017.12.032.

Chen, T., & Lin, Y. C. (2017). Feasibility evaluation and optimization of a smart manufacturing system based on 3D printing: A review. *International Journal of Intelligence Systems, 32*(4), 394–413.

Cheng, K., Niu, Z. C., Wang, R. C., Rakowski, R., & Bateman, R. (2017). Smart cutting tools and smart machining: Development approaches, and their implementation and application perspectives. *Chinese Journal of Mechanical Engineering, 30*(5), 1162–1176.

Cheraghalipour, A., & Farsad, S. (2018). A bi-objective sustainable supplier selection and order allocation considering quantity discounts under disruption risks: A case study in plastic industry. *Computers & Industrial Engineering, 118*, 237–250.

Chourabi, H., Nam, T., Walker, S., Gil-Garcia, J. R., Mellouli, S., Nahon, K., Pardo, T. A., & Scholl, H. J. (2012). Understanding smart cities: An integrative framework. 45th Hawaii international conference on system. *Science*, 2289–2297.

d'Aquin, M., Davies, J., & Motta, E. (2015). Smart cities' data: Challenges and opportuni-ties for semantic technologies. *IEEE Internet Computing, 19*(6), 66–70. https://doi.org/10.1109/mic.2015.130.

Elkhodr, M., Shahrestani, S., & Cheung, H. (2016). The internet of things: New interoperability, management and security challenges. *International Journal of Network Security & Its Applications, 8*(2), 85–102.

Hecklau, F., Galeitzke, M., Flachs, S., & Kohl, H. (2016). Holistic approach for human resource management in industry 4.0. *Procedia CIRP*, 1–6. https://doi.org/10.1016/j.procir.2016.05.102.

Hermann, M., Pentek, T., & Otto, B. (2016, January). *Design principles for industrie 4.0 scenarios*. In System Sciences (HICSS), 2016 49th Hawaii International Conference on (pp. 3928–3937). IEEE.

Hofmann, E., & Rüsch, M. (2017). Industry 4.0 and the current status as well as future prospects on logistics. *Computers in Industry, 89*, 23–34.

Javaid, M., Haleem, A., Khan, S., & Luthra, S. (2020). Different flexibilities of 3D scanners and their impact on distinctive applications. *International Journal of Business Analytics, 7*(1), 37–53. https://doi.org/10.4018/ijban.2020010103

Kadera, P., & Novák, P. (2017). Performance modeling extension of directory facilitator forenhancing communication in FIPA-compliant multiagent systems. *IEEE Transactions on Industrial Informatics, 13*(2), 688–695.

Kang, H. S., Lee, J. Y., Choi, S., Kim, H., Park, J. H., Son, J. Y., et al. (2016). Smart manufacturing: Past research, present findings, and future directions. *International Journal of Precision Engineering and Manufacturing-Green Technology, 3*(1), 111–128.

Khan, S., Asjad, M., & Ahmad, A. (2015a). Review of modern optimization techniques. *International Journal of Engineering Research And, V4*(04). https://doi.org/10.17577/ijertv4is041129

Khan, I., Naqvi, S. K., & Alam, M. (2015b). Data model for big data in cloud environment. computing for sustainable global development (INDIACom), 2015 2nd International conference on, 11–13 March 2015, New Delhi, India, IEEE (pp. 582–585).

Khan, S., Shakil, K., & Alam, M. (2017a). Cloud-based big data analytics—a survey of current research and future directions. *Advances in Intelligent Systems and Computing, 654*, 595–604.

Khan, S., Liu, X., Shakil, K., & Alam, M. (2017b). A survey on scholarly data: From big data perspective. *Information Processing & Management, 53*(4), 923–944.

Khan, S., Shakil, K., Arshad Ali, S., & Alam, M. (2018). On designing a generic framework for big data-as-a-service. In *2018 1st International conference on advanced research in engineering sciences (ARES)*. https://doi.org/10.1109/ARESX.2018.8723269.

Khan, S., Khan, M., Haleem, A., & Jami, A. (2019a). Prioritising the risks in halal food supply chain: An MCDM approach. Journal of Islamic Marketing, ahead-of-print(ahead-of-print).

Khan, M., Khan, S., & Haleem, A. (2019b). Analysing barriers towards management of Halal supply chain: A BWM approach. *Journal of Islamic Marketing*.

Khan, S., Khan, M. I., & Haleem. A. (2020). Blockchain enabled supply chain: An implementation perspective. *Our Heritage, 67*(5), 318–334.

Kumar, V., Kumar, R., Pandey, S. K., & Alam, M. (2018). Fully homomorphic encryption scheme with probabilistic encryption based on Euler's theorem and application in cloud computing. *Advances in Intelligent Systems and Computing, 654*, 605–611.

Kumari, A., Kumar, V., YahyaAbbasi, M., & Alam, M. (2018). The cryptanalysis of a secure authentication scheme based on elliptic curve cryptography for IOT and cloud servers. In *2018 international conference on advances in computing, Communication Control and Networking (ICACCCN)*

Kusiak, A. (2017). Smart manufacturing. *International Journal of Production Research, 56*(1–2), 508–517.

Kymäläinen, T., Kaasinen, E., Hakulinen, J., Heimonen, T., Mannonen, P., Aikala, M., & Lehtikunnas, L. (2017). A creative prototype illustrating the ambient user experience of an intelligent future factory. *Journal of Ambient Intelligence and Smart Environments, 9*(1), 41–57.

Lee, S. G., Chae, S. H., & Cho, K. M. (2013). Drivers and inhibitors of SaaS adoption in Korea. *International Journal of Information Management, 33*(3), 429–440.

Li, D., Tang, H., Wang, S., & Liu, C. (2017). A big data enabled load-balancing control for smart manufacturing of industry 4.0. *Cluster Computing, 20*, 1–10.

Luthra, S., & Mangla, S. (2018). Evaluating challenges to industry 4.0 initiatives for supply chain sustainability in emerging economies. *Process Safety and Environmental Protection, 117*, 168–179.

Manavalan, E., & Jayakrishna, K. (2019). A review of Internet of Things (IoT) embedded sustainable supply chain for industry 4.0 requirements. *Computers & Industrial Engineering, 127*, 925–953.

Masood, T., & Egger, J. (2019). Augmented reality in support of industry 4.0—Implementation challenges and success factors. *Robotics and Computer-Integrated Manufacturing, 58*, 181–195.

Moktadir, M., Ali, S., Kusi-Sarpong, S., & Shaikh, M. (2018). Assessing challenges for implementing industry 4.0: Implications for process safety and environmental protection. *Process Safety and Environmental Protection, 117*, 730–741.

Pacaux-Lemoine, M., Trentesaux, D., Zambrano Rey, G., & Millot, P. (2019). Designing intelligent manufacturing systems through human-machine cooperation principles: A human-centered approach. Available at: accessed 13 July 2019.

Pamučar, D., Petrović, I., & Ćirović, G. (2018). Modification of the best-worst and MABAC methods: A novel approach based on interval-valued fuzzy-rough numbers. *Expert Systems with Applications, 98*, 89–106.

Peraković, D., Periša, M., & Zorić, P. (2019). Challenges and issues of ICT in industry 4.0. *Lecture Notes in Mechanical Engineering*, 259–269.

Perales, D. P., Valero, F. A., & García, A. B. (2018). Industry 4.0: A classification scheme. In *Closing the gap between practice and research in industrial engineering* (pp. 343–350). Cham: Springer.

Pereira, T., Barreto, L., & Amaral, A. (2017). Network and information security challenges within industry 4.0 paradigm. *Procedia Manufacturing, 13*, 1253–1260.

Qaiser, F. H., Ahmed, K., Sykora, M., Choudhary, A., & Simpson, M. (2017). Decision support systems for sustainable logistics: A review and bibliometric analysis. *Industrial Management & Data Systems, 117*, 1376–1388.

Rajput, S., & Singh, S. (2018). Identifying industry 4.0 IoT enablers by integrated PCA-ISM-DEMATEL approach. *Management Decision*. https://doi.org/10.1108/md-04-2018-0378.

Rajput, S., & Singh, S. (2019). Industry 4.0 – challenges to implement circular economy. *Benchmarking: An International Journal*.

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems, 88*, 173–190.

Rezaei, J. (2015). Best-worst multi-criteria decision-making method. *Omega, 53*, 49–57.

Rezaei, J. (2016). Best-worst multi-criteria decision-making method: Some properties and a linear model. *Omega, 64*, 126–130.

Rezaei, J., Hemmes, A., & Tavasszy, L. (2017). Multi-criteria decision-making for complex bundling configurations in surface transportation of air freight. *Journal of Air Transport Management, 61*, 95–105.

Schuh, G., Anderl, R., Gausemeier, J., ten Hompel, M., & Wahlster, W. (2017). *Industrie 4.0 maturity index. Managing the digital transformation of companies*. Munich: Herbert Utz.

Shakil, K. A., & Alam, M. (2016). Recent developments in cloud based systems: State of art. *International Journal of Computer Science and Information Security (IJCSIS), 14*(12).

Siddiqui, M. S., Legarrea, A., Escalona, E., Parker, M. C., Koczian, G., Walker, S. D., & Ulbricht, M. (2016). Hierarchical, virtualised and distributed intelligence 5G architecture for low-latency and secure applications. *Transactions on Emerging Telecommunications Technologies, 27*(9), 1233–1241.

Sufiyan, M., Haleem, A., Khan, S., & Khan, M. (2019). Evaluating food supply chain performance using hybrid fuzzy MCDM technique. *Sustainable Production And Consumption, 20*, 40–57. https://doi.org/10.1016/j.spc.2019.03.004

Sun, S., Cegielski, C. G., Jia, L., et al. (2016). Understanding the factors affecting the organizational adoption of big data. *The Journal of Computer Information Systems, 58*, 193–203.

Tuptuk, N., & Hailes, S. (2018). Security of smart manufacturing systems. *Journal of Manufacturing Systems, 47*, 93–106. https://doi.org/10.1016/j.jmsy.2018.04.007.

Wan, J., Tang, S., Li, D., Wang, S., Liu, C., Abbas, H., & Vasilakos, A. V. (2017). A manufacturing big data solution for active preventive maintenance. *IEEE Transactions on Industrial Informatics, 13*, 2039–2047.

Wang, J., Ma, Y., Zhang, L., Gao, R., & Wu, D. (2018). Deep learning for smart manufacturing: Methods and applications. *Journal of Manufacturing Systems, 48*, 144–156.

Xu, L. D., Xu, E. L., & Li, L. (2018). Industry 4.0: State of the art and future trends. *International Journal of Production Research, 56*(8), 2941–2962.

Yeh, C.-C., & Chen, Y.-F. (2018). Critical success factors for adoption of 3D printing, Technol. Forecast.Soc. *Change, 132*, 209–216.

Zhong, R. Y., Xu, C., Chen, C., & Huang, G. Q. (2017). Big data analytics for physical internet-based intelligent manufacturing shop floors. *International Journal of Production Research, 55*(9), 2610–2621.

Zhou, K., Liu, T., & Zhou, L. (2016). Industry 4.0: Towards future industrial opportunitiesand challenges in: 2015 12th international conference on fuzzy systems andknowledge discovery. *FSKD, 2015*, 2147–2152. https://doi.org/10.1109/FSKD.2015.7382284.

Part VI
Next Generation Smart Applications

Chapter 23
Surveillance of Type –I & II Diabetic Subjects on Physical Characteristics: IoT and Big Data Perspective in Healthcare @ NCR, India

Rohit Rastogi, D. K. Chaturvedi, Santosh Satya, Navneet Arora, Parul Singhal, and Mayank Gupta

Abstract The Delhi and NCR healthcare systems are rapidly registering electronic health records, diagnostic information available electronically. Furthermore, clinical analysis is rapidly advancing-large quantities of information are examined and new insights are part of the analysis of this technology-experienced as Big Data. It provides tools for storing, managing, studying, and assimilating large amounts of robust, structured and unstructured data generated by existing medical organizations. Recently, data analysis data have been used to help provide care and diagnose disease. In the current era, systems need connected devices, people, time, places and networks that are fully integrated on the Internet (IoT). The Internet has become new in developing health monitoring systems. Diabetes is defined as a group of metabolic disorders affecting human health worldwide. Extensive research (diagnosis, path physiology, treatment, etc.) produces a great deal of data on all aspects of diabetes. The main purpose of this chapter is to provide a detailed analysis of healthcare using large amounts of data and analysis. From the Hospitals of Delhi and NCR, sample of 30 subjects has been collected in random fashion who has been suffering

R. Rastogi (✉) · P. Singhal
DEI Agra, Agra, India

ABESEC, Ghaziabad, Uttar Pradesh, India
e-mail: rohit.rastogi@abes.ac.in; parul.18mcs1004@abes.ac.in

D. K. Chaturvedi
Department of Electrical Engineering, DEI-Agra, Agra, Uttar Pradesh, India

S. Satya
Department of Rural Development, IIT-Delhi, New Delhi, India
e-mail: ssatya@rdat.iitd.ernet.in

N. Arora
Department of ME, IIT- Roorkee, Roorkee, Uttarakhand, India

M. Gupta
IT Consultant, TCS, Noida, Uttar Pradesh, India

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_23

from Diabetes from their Health Insurance Providers without disclosing any Personal Information (PI) or Sensitive Personal Information (SPI) by Law. The present study aimed to analyze diabetes with the latest IoT and Big Data analysis techniques and it's correlation with stress (TTH) on human health. Authors have tried to include age, gender & insulin factor and its correlation with diabetes. Overall, In conclusion, TTH cases increasing with age in case of males and not following the pattern of diabetes variation with age while in case of female TTH pattern variation is same as diabetes i.e. increasing trend up to age of 60 then decreasing.

Keywords AI · Machine learning · Diabetes mellitus · Depression · Obesity · Coronary artery disease

23.1 Introduction

23.1.1 Role of Big Data in Healthcare

Using Big Data analysis in the healthcare can be very positive and save lives. Large-scale data refers to massive data generated by digitizing all items referenced by integrating and analyzing a particular technology. For health care, it uses specific health information from the population (or specific people) to help prevent potential pandemic diseases, treat illness, reduce costs etc. (McAfee et al. 2012).

As we have lived for a long time, treatment models have changed, and many of these changes are based on data.

Physicians want to fully understand about the best possible about the patient and alerting the signs of serious illness early in life; treating the illness early is much easier and cheaper.

By analyzing health data, prevention is better than treatment, and managing a patient's perspective allows insurance to deliver the right package. This is an industry initiative to address silo issues with patient information. The bits and bytes are collected everywhere, archived in hospitals, clinics, surgery etc., there is no possibility of unreliable communication (McAfee et al. 2012).

23.1.1.1 Big Data Characteristics and Its Benefits in Healthcare

The concepts of Big Data are not new, but its definitions are constantly changing. In various efforts to define large-scale data, basically, A set of data elements complexity require the search, whose size, type, adoption and invention of new hardware and software mechanisms call analyze and visualize information (Rastogi et al. 2018b).

Health is a simple example that shows that three V data, speed (data generation speed), size, and volume are the essential aspects of the data generated. These data are distributed to various medical systems, insurance companies, researchers, researchers and government agencies. Furthermore, each of these data tanks is inherently unstable and cannot provide (Alam 2012).

A platform for global data transparency. In summation to the three V's, healthcare data are too essential for meaningful usage of it to develop translational research.

The potential data and Benet data in the development and implementation of large-scale data solutions in this area, despite the inherent complexity of healthcare (Alam 2012).

Benefits: Create 360° views of consumers, patients, and doctors.

- Improve personalization and care with a comprehensive patient profile.
- Follow your doctor's preferences, referrals, and clinical reservation data to let the doctor know how to manage your reservation.
- Improve healthcare marketing efforts with information about consumers, patients and physicians (McAfee et al. 2012) needs and preferences.
- Analyze trends in hospitals and larger healthcare networks to help research and care improve people's health.
- Identify health outcomes, patient satisfaction, and patient tissue patterns.
- Predict health outcomes by using data analysis and developing preventive care strategies.
- Optimization of growth by improving efficiency, efficiency and care compliance.

23.1.1.2 The Future of Healthcare Big Data

In the future, the healthcare providers will be adding significant amounts of data as they are critical to success. Healthy data continues to support smarter, more integrated touch marketing.

In addition, with the growth of wearable technology and Internet objects (IoT), a large amount of data will be available. Permanent monitoring of patients with wearable technology and IoT is the norm, adding more information to large data stores (As per Fig. 23.1).

23.1.1.3 Role of Big Data in IoT

Health Tracking: Big Data & analysis alongside the Internet of Things (IoT) are a revolution in that it can track user statistics and information. Aside from a wearable foundation that can help patients sleep, heart rate, exercise, walking distance etc., there are new medical innovations that can control the patient's blood pressure, pulse oximeter, glucose monitor etc.

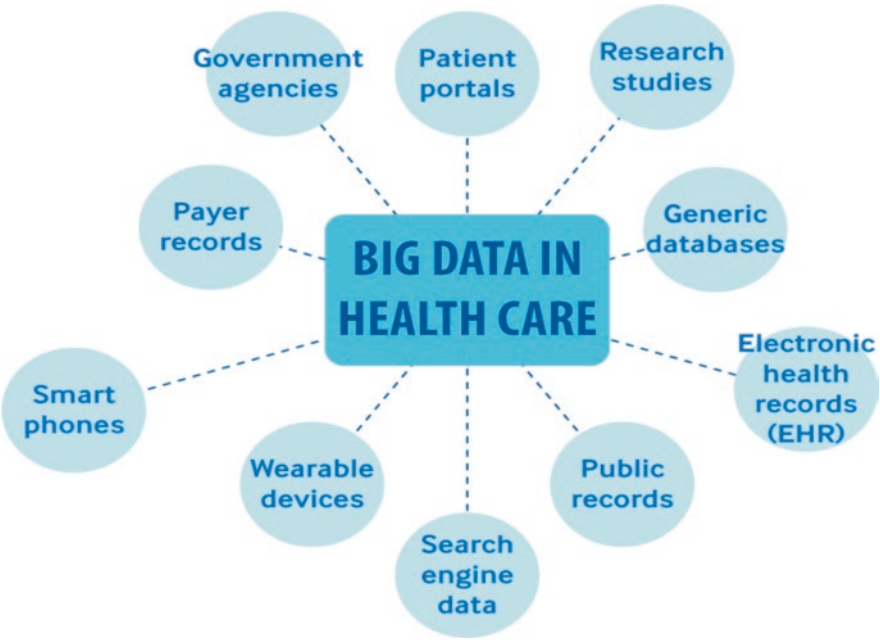


Fig. 23.1 Sources of big data in healthcare. (Ali et al. 2019)

Cost Savings: Large amounts of data are the best way to save the cost of hospitals that are more or less staffed by the book. Predictive analysis helps solve this problem by helping to predict acceptance rates and assigning employees. This reduces the amount of hospital investment and, in fact, helps maximize the investment potential.

The insurance industry can save money by guaranteeing wearable and hygienic trackers to keep patients from going to the hospital (Rastogi et al. 2018d; Bansal et al. 2018). High Risk Patient Support: If all hospital records are digitized, this is complete information that you can get to understand many patient patterns. This will bring patients back to the hospital and identify their chronic problems. Such understanding will help provide better care to such carers and will provide insight into corrective actions to reduce their frequent visits. This is a great way to maintain a list of at-risk patients and provide them with custom care (Singh et al. 2019).

Human Error Prevention: Experts are reported to believe that they are prescribing misleading drugs or sending different drugs misleadingly. In general, Big Data can be used to analyze user data and prescription drugs to reduce such errors. This can identify information and has great potential for prescribing alternatives to reduce errors and save lives. Such software can be a great tool for doctors exposed to many patients every day.

Healthcare Progress: Regardless of the current scenario, large-scale data can be a good benefit for science and technology advancements. For healthcare, artificial intelligence like Watson's IBM can use several data in a matter of seconds to find solutions to various illnesses. Such progress is ongoing and will continue with the

amount of research collected by Big Data. Not only can it provide an accurate solution, it will also provide a custom solution for a unique problem. The availability of predictable analysis of patients moving to a specific geographical location will help to study similar patients in the area.

23.1.1.4 Big Data Tools

The following ten open source tools were listed as the best open source Big Data tools in 2019, based on popularity and ease of use.

- Hadoop
- Apache Spark
- Apache Storm
- Cassandra
- RapidMiner
- MongoDB
- R programming tool
- Neo4j

23.1.1.5 Big Data Security

Analysis of Big Data processing security and security processes within the cloud and based on assumptions. Analysis of various factors that can compromise your own confidentiality. Large data security is a concern because great flexibility is a valuable target for potential failures.

23.1.2 IoT

Communication and measurement equipment, as well as their software, are highly diversified for IT solutions in different fields. A new technology called the Internet of Things (IoT) is helping practitioners and researchers design new healthcare solutions. Healthcare research sponsored by IoT is noteworthy for its beneficial implications, including high quality and low cost of reliable preventive care and care (Singh et al. 2019; Khan et al. 2019a).

23.1.2.1 Origin of IoT

The term IoT was first coined by the Massachusetts Institute of Technology Auto ID Center. Automatic IDs are used to describe any kind of action, such as work, to identify and improve the program.

In 2003, such as automation, productivity improvement, error reduction, it released the automatic ID electronic center.

Product Code (EPC) Network EPC passes objects from one place to another. It provides the idea of running IoT that can be used by microchip to create a network for business tools (Satya et al. 2018).

RFID (Radio Frequency Identification) offers more opportunities for developing IoT as a new IT paradigm in academic and industrial environments (Khan et al. 2019b; Saxena et al. 2018).

23.1.2.2 Applications of IoT

IoT has many uses and can be successfully implemented areas such as in the healthcare (Malhotra et al. 2018).

- Department,
- Event Management,
- Travel and Hypermarkets,
- Retail,
- Manufacturing,
- Environment Systems,
- Tourism,
- Logistics systems
- Hotels, restaurants etc.

This is the range of functional areas that explain it IoT plays an important role in the proper functioning of society (Williams and Woodward 2015).

23.1.2.3 Applying Internet of Things (IoT) for Healthcare

The main problem is that all patients, especially in remote areas, cannot receive medical attention or treatment in critical situations. It has had awful consequences on people's minds about hospital and doctor services. Today, these issues are largely addressed by implementing new technologies using IoT devices to monitor healthcare. In addition to maintaining healthy patients, IoT has the potential to improve the way doctors consult. IoT healthcare can also increase patient participation and satisfaction by deepening patient involvement with doctors.

Using the Internet of Things (IoT) in the healthcare are a vast ecosystem. General concept of healthcare & electronic health is more integrated with approaches & benefits (Shakil et al. 2018). Medical devices has changed the equipment of conventional devices (Rahmani et al. 2015). This improvement includes the emergency of IoT medical systems that can also be connected to mobile phones.

IoT drugs are basically a system of health management. Patient health parameters are recorded through the back system. It then analyzes the basis and provides reasonable data for recorded data and clinical staff. Feedback experts can help

experts determine the current health of the patient and respond to important situations.

Medical equipment can be used to monitor health parameters. Alternative devices such as smart watch and cell phones can be a good option (Malhotra et al. 2018).

23.1.2.4 Healthcare Applications of IoT

An important area of IoT is healthcare. IoT plays an important role in improving service quality and reducing costs (Malhotra et al. 2018). Using the wireless sensor, health parameters such as blood pressure, blood sugar and temperature can be feasible in real time. The development of advanced technologies for advanced sensor, advanced data processing technologies and wireless communication has increased the use of IoT in the medical field. Develop wearable body sensor system (WBSN) manages the patient's activities continuously. This is a landmark for implementing IoT (Yin et al. 2016).

23.1.2.5 Critical Issues and Challenges of IoT in Healthcare

The IoT-based healthcare sector is experiencing tremendous growth. The use of IoT devices and sensors in the medical sector forms the basis of the e-health system. People use these devices to monitor their daily health statistics. Simultaneously, the devices use transmission networks to send/receive the health-related data of patients. This results in a potential threat by hackers. Hence, it becomes necessary to completely secure the IoT-based healthcare system. The medical IoT systems face the following major threats (Sharma et al. 2018; Rastogi et al. 2018c):

- Scalability
- Security
- Mobility

23.1.2.6 Examples of IoT Services in Healthcare

The IoT-based healthcare architecture has three main layers. Layers of information recognition, network transmission and information recognition layer application services are mainly from sensors used to monitor health statistics (Williams and Woodward 2015).

The collected data are sent over the network and stored in cloud data center. Wireless technology such as Wi-Fi, ZigBee, EnOcean is used to transfer data through the network. The application service layer includes IoT applied at medical facilities to provide telemedicine. Blood glucose monitoring, ECG monitoring, blood pressure monitoring, body temperature monitoring, wheelchair management, heart rate (Khanna et al. 2016).

23.1.3 Artificial Intelligence (AI) & Machine Learning (ML)

The broad science theory with its origin in philosophy, mathematics & computer science aimed at understanding and developing systems that show the nature of intelligence (Malhotra et al. 2017).

An AI subsystem, in which a computer program (algorithm) learns the power of communication from data samples.

Machine (ML) is the simplest application of statistical data models using a computer. Learn devices using statistical methods that are wider than those commonly used in medicine. Modern technologies, such as detailed training, are based on models with few assumptions about initial data to manage complex information (Malhotra et al. 2017).

23.1.4 Tension Type and Chronic Headache

Episodic Tension Headaches: It can last from 30 min to about a week. It can also vary from 15 days in a month to about 3 months. It can also become chronic. One can have migraines if episodic headaches occur frequently.

Chronic Tension Headaches: If the headache last for 15–20 days out of a month continuing for about 3 months it becomes chronic. It occurs early in the morning and its symptoms include: poor appetite, restlessness, lack of concentration and depression (Chaturvedi et al. 2018; Satya et al. 2019).

TTH varies in intensity, duration and location. Use of alcohol, stress, caffeine, cold, dental problem, eye strain, excessive smoking, tiredness etc. are the triggers of tension headaches. However one must remember they are not a brain disease.

An individual may suffer with this TTH in any age group however they are normal in adult age and older teens. It generally runs in families and is common in women (as per Fig. 23.2).

Earlier reports which show the occurrence of tension type headaches is given below:

This graph shows various countries in which Episodic TTH and Chronic TTH is experienced by the people whether it is man or women. Around 71% and 3% people in Denmark are suffering, 39% & 2.5% in Germany and around 38.3% & 2.2% all are suffering by this disease (Saini et al. 2019; Singhal et al. 2019).

23.1.4.1 TTH Treatment

Massaging scalp, temples or bottom of your neck can help to relieve pain in a headache. Over the countries painkillers such as ibuprofen, aspirin, paracetamol and naproxen are mostly used by patients suffering from TTH. These painkillers are used when the condition of headache becomes uncontrollable and interferes with

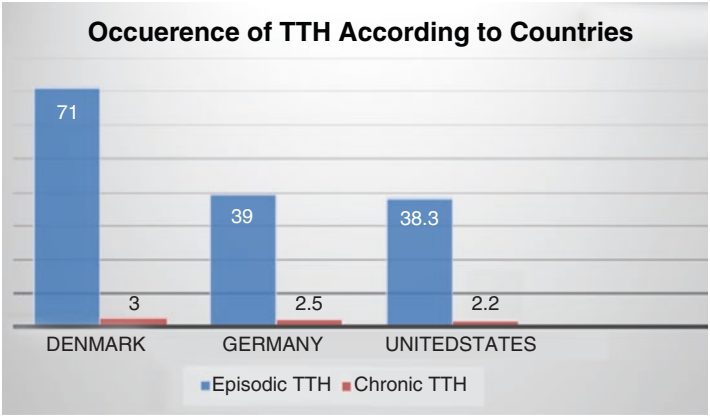


Fig. 23.2 States of occurrence of TTH as per different countries (Episodic vs. Chronic). (Chauhan et al. 2018)

your physical activities. However the treatment of TTH can vary according to the symptoms and triggers causing it (Chauhan et al. 2018).

Taking painkillers more than thrice a weak can be harmful and thus avoided by the patient. An individual is suggested to be in relaxation stage and tension free to avoid TTH. It is also suggested by experts to have a full sleep of 7–8 h a day in order to be away from headaches. Other way is the use of Tricyclic antidepressants. If your headache is caused due to psychological factors it may be hard to tackle. It is then advised to see a counselor or psychotherapist. If home remedies do not work then medical assistance may be needed by the doctor. Consumption of high quantity of acetaminophen can damage the liver. The heavy dose of analgesic like ibuprofen or aspirin can disturbance's stomach or damage the kidneys too (Arora et al. 2019).

23.1.4.2 TTH Preventions

Relaxation Techniques: Includes effective alternate therapies like deep breathing, yoga, meditation and progressive muscle relaxation etc.

As per different studies and reports, it has been found and established that TTH is directly correlated with demographical conditions, social culture across region as per age, gender of individual and stats analysis of data assessment. Large range of risk factors, new researches in genetic and neurobiological research have given a clear insight and in depth know how for TTH (Vyas et al. 2018; Saini et al. 2018).

A majority of people with TTH do not seek medical attention thus it has been proven to be difficult to completely diagnose the exact effects, causes and preventions of TTH. Even adults with new bodily changes are likely to go through TTH. This report thus proves that further research is very necessary on this particular topic and must be done by the medical associations (Yadav et al. 2018; Chaturvedi et al. 2017).

23.1.5 Diabetes Mellitus and Its Types

Diabetes mellitus (DM) is specified as a set of pancreas due to insulin cleaning and / or abnormal exercise. Due to insulin deficiency, blood sugar levels increase and hyperglycemia is caused by carbohydrate, fat and protein.

DM, who has affected over 200 one million people worldwide. The possibility of diabetes is expected to increase in the following few years. DM can be split into many different characters. Yet, according to the disease's disease, there is two main types of clinics, type-1 diabetes (T1D) and type-2 diabetes (T-2D).

The most common form of T2D diabetes is considered 95% of all diabetes patients, mainly due to insulin resistance T2D, lifestyle factors, physical activity, dietary habits and congenital heart disease (Imran Khan et al. 2018).

Due to the devastation of the T1D effective system, it is visible from planarians' pancreases beta cells intestlezes. T1D affects about 10% of diabetes patients worldwide, 10% of which eventually develop IDEpathic diabetes (Imran Khan et al. 2018; Kumar et al. 2017).

Gestational diabetes, endocrine disorders, type-2 diabetes mellitus, neuritis, mitochondria, and pregnancy are based on the specifications of other types of DM and the onset of insulin hygiene.

Symptoms of DM include polyuria, hirsute and especially weight loss. Detection depends on the degree of glucose (fasting blood glucose = 7.0 mmol / L).

The advancement of diabetes is linked up with many complications, mainly due to chronic hyperglycemia. It is well known that DM has a extensive range of hitherto physiological conditions. The most usual side effects of microangiopathy and macroangiopathy, including diabetic nephropathy, retinopathy, neuropathy, diabetic fatigue and cardiovascular disease (Chaturvedi 2004, 2012).

Prevention and treatment are one of the contributing cases of death from DM and related diseases. While insulin infusion is the primary treatment for T1D, insulin is also offered in the specific case of T2D patients who have hypoglycemia, diet, Weight loss, exercise and oral medicine.

Current medications are primarily targeted as

- Save people's lives and reduce symptoms.
- Prevention of long-term complications of diabetes and the elimination of some risk factors, resulting in longer life.

The most commonly used ant diabetic agents include sulfonylurea's, metformin, alpha-glycosidase inhibitors, peptide analogues, non-sulfonylurea secretions and the like. However, many of the current anti-diabetic drugs have a lot of side effects. Additionally, insulin therapy is associated with weight gain and hypoglycemia. So, although the design and discovery of anti-diabetic drugs is very important, the subject is also research (Yang et al. 2018; Chaturvedi and Arya 2013a).

Although extensive research on DM is ongoing for decades, the disease, therapy and disease screening and management has not yet been identified, has not been

identified, and is unknown. Through such processes, diagnosis, prognostic assessment of appropriate treatments, and clinical management can be important bases for reaching a medical disorder.

Likewise, data mining and machine learning are coming forth as important processes that potentially lead to physician decision-making (Chaturvedi and Satsangi 2013).

23.1.5.1 Facts for Diabetes Cause Tension Type Headache

Diabetes often does not cause headaches. However, although headaches are not usually at risk, it may be difficult to control the blood sugar of diabetics (Imran Khan et al. 2018). People with diabetes cannot control their blood sugar through insulin hormones.

Over time, the level of continuous or hyperglycemic can be serious and even life-threatening consequences like cardiovascular disease and kidney failure. Detecting headaches as a result of poor glycemic control is the first step in preventing serious health problems. This chapter examines the relationship between diabetes and headache and suggests ways to alleviate the headache associated with diabetes.

23.1.5.2 Diabetes and Headaches

Not everyone diabetic will experience a headache. Those who have recently been diagnosed with diabetes tend to have headaches because they are still trying to control their blood sugar and use a diet. For people with diabetes, headaches are usually due to changes in blood sugar levels. A headache can indicate that your blood sugar is high, and your doctor calls it hyperglycemia. Instead, blood sugar levels may be very low, a doctor called it hypoglycemia. Changes in blood sugar levels are more likely to cause headaches for diabetics (Marrie et al. 2019; Chaturvedi 2019).

23.1.6 Hypoglycemia (Low Blood Sugar)

Hypoglycemia means glucose or low levels of glucose. Although hypoglycemia is not a disease, it can be a health problem. All cells, including the trunk, need energy, the brain, including the glucose, provides energy to the body. Hormones absorb insulin and use cells (Nordqvist 2019a). The symptoms of hypoglycemia are:

- Hunger
- Shake
- Heart competition
- Nausea and sweat

In many cases, it causes back injuries and death. Hypoglycemia can occur under a variety of conditions, but often occurs as a response to drugs such as insulin. Diabetic patients use insulin to treat hyperglycemia.

23.1.6.1 Hypoglycemia and Diabetes

To prevent hypoglycemia in people with glucose, regular glycemic tests can help diabetic people to stop hypoglycemia.

Type-1 and type-2 diabetes are related to insulin problems (Nordqvist 2019a).

Type-1 diabetes: Normally damage to insulin-producing salmon means that the body cannot make insulin.

Type-2 diabetes: the somatic cells cannot respond to insulin, or the pancreas cannot leave enough insulin. In both types of diabetes, cells do not receive much energy.

Some people with type-1 diabetes and type-2 diabetes should use insulin or other medicines to reduce their blood sugar levels (Richa and Devendra Prakash 2016).

23.1.6.2 Hypoglycemia and Headaches

Doctors consider blood sugar levels below 70 mg / dl (mg / dl) as an indicator of hypoglycemia. This is a serious condition because glucose are a major fuel source for many body cells, including the brain.

Hypoglycemic symptoms are usually sudden and can be much faster than hyperglycemic symptoms. In addition to headache, there are some of the hypoglycemic symptoms:

- Anxiety
- Blurred eyes
- Shit
- Confusion
- Affair
- Hunger
- Hypersensitivity
- Nausea
- Heart competition
- Seizure
- Vulnerability
- Sweating
- Fatigue
- Unconscious
- Weakness

Hypoglycemia can increase if a diabetic patient gets too much insulin or carbohydrates. Careful treatment and quick treatment of hypoglycemic symptoms are

essential. This helps to prevent more serious headaches and compilers (Nordqvist 2019a).

23.1.6.3 Hyperglycemia and Its Causes

Most people experience hyperglycemia after drinking hyperglycemia, but people with stable hyperglycemia may have problems with insulin production and use.

Insulin is a hormone produced in pancreas that gives the cells the power to produce glucose, generates energy and generally works. If insulin is low or inefficient, diabetes can progress.

There are two types of diabetes. Type I diabetes occurs when the body does not produce insulin. Type-2 diabetes occurs when the body is not using insulin effectively as a result, glucose remains in the blood and burns the body. Exercise and exercise can increase hyperglycemia levels. It can improve the effectiveness of insulin by providing more glucose, which can improve the process (Liu et al. 2014).

Stress, life, and relationships in the work can release hormones that maintain high blood sugar levels. Stress associated with high blood pressure. Illnesses like flu may lead to stress that can increase your blood sugar (Felman 2019).

23.1.6.4 Hyperglycemia and Headaches

Hypoglycemia or hyperglycemia can cause headaches. Hyperglycemia is caused by excess glucose in the blood. In type-1 diabetes, insulin deficiency raises blood sugar levels. In type-2 diabetes, the body cannot use insulin properly.

The excess risk factors include:

- Weak and rich in sugar and fat
- Polite lifestyle
- Release the hormone cortisol, which increases stress, blood glucose levels (Felman 2019).

Symptoms of hyperglycemia often appear. However, a headache can be a sign of hyperglycemia.

Other symptoms include:

- Blurred eyes
- Confusion
- Dehydration
- Thirst
- Fatigue
- Hunger
- Urine Increase
- Recovery wounds gradually

Symptoms of hyperglycemia often appear. However, a headache can be a sign of hyperglycemia.

Hyperglycemia is a serious condition, which requires rapid management because high levels of glucose can harm blood vessels & nerves. Without treatment, hyperglycemia can oppose the effects of the body on insulin, a hormone, which allows the cells to absorb glucose (Chaturvedi and Lajwanti 2015; Chaturvedi et al. 2015).

Without glucose absorption into cells, the body is fatter instead. This process may lead to the production of ketones, a growing waste product when the body burns from fat and burns.

Production of ketones can lead to diabetic ketochonidosis, which can lead to coma & even death.

People can control hyperglycemia with changes in food &medicine. Keeping your blood sugar in your control reduces the risk of diabetes mellitus.

23.1.6.5 The Cases When to See a Doctor

Headaches can indicate up and down blood sugar levels that can occur without complications from life-threatening side effects. Therefore, patients with frequent headache should consult a physician. It is very important to contact your doctor after it becomes clear.

- Headaches can seriously affect everyday life.
- Blood sugar does not return to the required level.
- Severe or persistent symptoms with headache.

23.1.7 Depression

Grief, fatigue, loss of interest, enjoyment of everyday life-these are all familiar to us, but if we are still affected by our lives, we may be depressed (Ali and Alam 2016).

23.1.7.1 Depression: Sign and Symptoms

Symptoms of depression include:

- Depression mode
- Loss of sexual desire
- Lowering interest or
- Enjoying previously
- Enjoyed activities

  Unintended weight loss (without food)/loss of appetite

- Insomnia (difficulty sleep)/hypersomnia (hypersomnia)

- Psychological stimulation, e.g. restlessness, walking up and down
- For example, psychological skills delayed, moved and accelerated speech
- Fatigue or energy loss
- No value or guilt
- Disturb your thinking & concentration

23.1.7.2 Depression Causes

The causes of depression have not been fully understood and are not limited to only one reason. Due to the combination of many factors, depression can occur (Pramodkumar et al. 2019; Gulati et al. 2019).

- Genetics
- Biological changes in neurotransmitters levels
- Environment
- Psychology & society (psychology)

23.1.7.3 Depression Treatment

- People are listening to people in treatment or counseling groups
- Counseling and treatment will help people manage depression symptoms.
- Depression area treatable mental illness. There is three factors for managing depression.
- Help teach the family from discussions about practical solutions and tensions.
- Psychotherapy, also known as speech therapy, is known as cognitive behavioral therapy (CBT).
- Medications, especially antidepressants.
- My psychotherapy puts people at risk of depression (Ali and Alam 2016).

23.1.8 Obesity

Obesity is a medical condition that occurs when an individual increases their body's body fat or excess weight, which can affect their health. Doctors usually indicate that people with high obesity are obese.

Body Mass Index (BMI) is a device that is used to estimate doctors whether a person is eligible for their weight, age and height. Measurement is the combination of average and weight.

Between 25 and 29.9, BMI indicates that the person is overweight. More than 30 BMIs indicate that a person may be suffering from obesity (Chaturvedi and Satsangi 2014; Chatruvedi and Lajwanti 2014).

Other factors such as waist Percentage (WHR), waist-to-stature ratio (WtHR), body fat distribution and distribution help determine body weight. If you have obesity and overweight, it can increase the danger of several diseases, includes metabolic syndrome, arthritis, and some types of cancer.

Metabolic syndrome also includes severe serum publication such as high blood pressure, type-2 diabetes, and snap disease. To prevent or reduce obesity, a healthy weight or feeding is a way of deteriorating weight. In some cases, a person can call for an operation (Brazier 2018).

Study showing the factors to become obese now tells the reasons as

- Excess calorie intake
- A person holding an apple in one hand and a confection in the other hand.

If your diet is mainly from fruits, vegetables and fava beans, you have a lower risk of obesity. When people consume more calories, they apply their energy, and their bodies store additional calories as fatty. This can lead to overweight and obesity.

Likewise, the great unwashed who accept certain foods, particularly fats and sugars, are probable to help gain weight. Foods that tend to increase the danger of weight gain are (Chaturvedi and Arya 2013b):

- Fast food
- Fried foods such as French fries
- Fat and processed meat
- Many dairy products
- Cooked products, breakfast grains, foods with added sugar such as biscuits
- Hidden sugar foods such as ketchup and many other canned foods
- Freshwater, sodium, alcoholic beverages
- Processed foods containing carbohydrates such as bread and confectionery
- Some processed foods contain high-fructose corn syrup (including flavors such as ketchup) as a sweetener.

Eating too much of these foods and doing little exercise can result in weight gain and obesity.

People who use a diet that uses primarily whole grains, water fruit & vegetables, are also at risk of being overweight.

However, while maintaining a healthy weight, they are exposed to more diverse diets. Fresh foods and beans contain fiber, which can make others feel better and promote healthy digestion (Brazier 2018).

23.1.9 CAD

If coronary artery disease is too narrow, cardiovascular disease (CHD) or coronary artery disease will progress. The coronary arteries are the blood vessels that carry oxygen and blood to the heart (Nordqvist 2019b). CHD produces cholesterol in the

arterial wall. These plaques cause arterial stenosis and reduce blood flow to the heart. Thrombosis can sometimes disrupt the bloodstream and cause serious health problems.

The coronary arteries form a vascular network on the surface of the heart that is supplied with oxygen. If these arteries are narrow, the heart may not have received enough oxygen-rich blood, especially during physical activity. Sometimes CHD causes a heart attack. It is the most common type of heart disease in the US and kills more than 370,000 people annually (Nordqvist 2019b).

23.1.9.1 CAD Causes

Cardiovascular disease in healthy people damage to the coronary arteries causes CHD, which causes plaque formation. CHD results from damage or damage to lining of the coronary arteries. This injury causes the formation of plaque deposits at the injury site. These stores contain cholesterol from cells and other waste products. This structure is called atherosclerosis.

If the plaque is broken or broken, platelets in that area are being tested for revascularization. This cluster can stop ultrasound and reduce or stop blood flow, which may cause a heart attack (Richa et al. 2016).

23.1.9.2 CAD Symptoms

CHD can cause angina. This is a type of chest pain associated with heart disease. Angina can cause the following feelings across the chest (Gupta et al. 2019):

- Squeeze
- Pressure
- Weight
- Tightening
- Burn
- Painful.

Angina can also cause the following symptoms:

- Indigestion
- Heartburn
- Weakness
- Sweating
- Nausea
- Cramp

CHD also leads to breathlessness. If the heart and other organs do not get enough oxygen, any activity can be very annoying and it can make people tired.

Side effects: A heart attack occurs when there is insufficient blood and oxygen in the myocardium, such as when a thrombus is made of one plaque in a coronary artery.

The formation of a thrombus is called coronary artery thrombosis. This clot can stop blood supply in the heart if it is large enough.

The symptoms of heart attack are:

- Chest discomfort
- Chest pain or collapse
- Cough
- Dizzy
- Shortness of breath
- Gray blouse on the face
- General inconvenience
- Panic
- Nausea and vomiting
- Restless
- Sweating
- Greasy skin

The first symptom is usually chest pain, ears which spread, chin, to the neck, hands, wrist & possibly scapula, back or stomach. If you change situations, relax or lie down, then you cannot feel relief. The pain is often fixed, but it may fall. It can be from minute to hour.

Heart attack is a medical emergency that can lead to permanent damage to death or heart. If someone shows Signs of heart attack, it is necessary to call urgent emergency services. The foremost symptom is usually chest pain, which propagate to the neck, chin, ears, hands, wrist and possibly scapula, back or abdomen. If you change situations, slow down or lie down, then you cannot feel relief. The annoyance is often specified, simply it may come. It can be from minute to hour. The heart attack is a medical emergency that can guide to lasting damage to death or heart. If someone shows signs of heart attack, it is necessary to call urgent emergency services (Chaturvedi et al. 2012).

23.1.9.3 CAD Treatment

There is no cure for CHD. However, there are ways in which one can manage the situation. Treatment includes changing your lifestyle, including quitting smoking, eating a healthy diet, and regular exercise. However, there are people who need to receive medicine and treatment.

Medicine: Doctor talks about medicine. There are various drugs for the treatment of cardiovascular disease.

The following are the drugs that people can use to reduce the risk and impact of CHD:

Beta-blockers: Physicians may prescribe beta-blockers to lower blood pressure &heart rate, especially for people who have had a previous heart attack. Sprays, Nitroglycerin Patches or pills: This increases arteries, increases blood pressure in the heart, and relieves chest pain (Nordqvist 2019b).

23.1.10 Insulin

Insulin is essential for controlling your blood sugar and claiming the strength of your hormones. Insulin is a chemical messenger that allows cells to carry glucose and glucose from the origin. Pancreas is an abdominal stomach and is the main source of insulin in the body. The size of the pancreatic cells, called the hormone island, is found in the physical formation of blood sugar levels (Felman 2018).

Higher degrees of glucose are higher and more insulin is made in order to balance blood sugar levels. Insulin also helps to lower fat and protein levels. The delicate balance of insulin regulates blood sugar and many physical expeditions. If the level of insulin is too high, it can cause too much or hypoglycemic symptoms. If this level remains hypoglycaemic or hyperglycemic, then there may be serious health problems.

Insulin Problems: In some people, the immune system attacks the islets and does not produce insulin. When this happens, blood sugar in the blood remains in the blood and the cells cannot absorb it and cannot convert it into energy.

This is the introduction of T1D, and people with this type of diabetes need regular insulin to stay alive. In some people, especially overweight, obese or inactive people, insulin is not effective in transmitting glucose, and can not increase its effectiveness. Inhibition of insulin affects the tissue.

Type-2 diabetes occurs when islets do not develop insulin to remove insulin resistance. Because insulin is isolated in the early twentieth century and cannot be manufactured alone or as an insulin supplement, insulin cannot withstand it (Tsai et al. 2013).

23.2 Literature Survey

According to Yang et al. (2018), Diabetes is one of the most important pandemics in many countries, but many people with diabetes suffer from endless control, subsets or adherence results (Centers for Disease Control and Prevention).

They describe the purpose of the study to show the past US largest urban-related diabetes-related criteria, including diabetes and non-diabetic incidence, diabetes patient health, diabetes drug use and poor spread Managed diabetes.

Wenya Yang et al. (2018), revealed methods for estimating diabetes was calculated using practical factor monitoring systems, the American Statistical Society, national surveys of nurses, census population, and cross-sectional data from national health and nutrition surveys.

According to him, the analysis of health claims is based on regular databases, Medicare's standard analysis file, and Medicaid analysis extract (by geographical location, insurance type, treatment of men and women and age groups and diabetes management) be informed.

They found the following: In 2012, adults with type-2 diabetes were less than 79%, with a diagnosis of diabetes less than 100%. West Palm Beach Florida. Oklahoma City, Oklahoma. The proportion of patients treated with medical claims indicates that poor diabetes management in Austin, Minnesota, Minnesota and San Antonio, Houston, Texas, was very low.

They concluded that diabetes diagnosis and treatment in urban areas is often less than government estimates and non-ratings. Local diabetes management standards can help track local improvements over time.

The paper 'Diabetes and anxiety adversely affect cognition in multiple sclerosis' written by following authors as Marrie et al. (2019), for the Comorbidity and Cognition in Multiple Sclerosis (CCOMS) Study Group. According to their, Compound conditions may indicate such variables. Depression is linked with cognitive impairment in the MS.

Ruth Ann Marrie et al. (2019) have revealed the purpose of this study is to determine if diabetes is associated with hypertension associated with multiple sclerosis. They include structured psychographic interviews, in-hospital anxiety and depression scales (HADS), correlation and input test (SDMT), California language test (CVLT-II), international memory repeated test (BVMT-R) And fluorite language test scores were adjusted to z-scores based on age, gender, and pedagogy. Multivariate linear models are utilized to connect the relationship between diabetes and hypertension with four subjective cognitive criteria to determine anxiety disorders, psychotropic drugs, treatment, smoking status and depression related to BMI.

The author found the following result the more than hundred participants, most women with MS have an average, revival age for that year. There were general complications; no more than thirty in all patients with high blood pressure; ten in each were diabetic. There was current major depression and below twenty cases of current anxiety disorder.

They were connected with cognitive mapping. Diabetes is associated with BVMT-R concentrations and z-scores. Anxiety were associated with lower SDMT scores. Z scores increased anxiety symptoms in SDMT and CVLT-II (HADS-A 11 11). Finally, association with diabetes related diseases and anxiety with cognitive deterioration associated with MS. Their presence can contribute to the practice of disability heterogeneity among people and can lead to improved cognitive management.

The paper written by authors Liu et al. titled as 'Parabens exposure in early pregnancy and gestational diabetes mellitus' (Liu et al. 2014).

According to them, Gestational diabetes (GDM) is known for the first time during pregnancy to any degree of glucose intolerance (American Diabetes, 2011). Exposure to parabens should be warned, especially in Pregnant women. But one survey indicated that parabens were associated with blood glucose levels in pregnant women. Yet, written reports of exposure to parabens and gestational diabetes (GDM) are missing. Xiaojie and Yuan explained the aim of this survey.

This survey tested whether exposure to parabens during pregnancy was initially associated with GDM.They are conducting a prospective study on approximately 1300 pregnant women who came from a clinical medical center in Wuhan, China between past few years. The concentration GDM of paraben (methyl paraben (MeP), ethyl paraben (EtP), propyl parapen (PrP), butyl parapen (BuP) and benzyl paraben (BzP) in urine samples collected between 8 and 16 weeks of gestation Use Poisson Diversity, which has a strong error variance, determined according to the International Expediency Disclosure Board (IADPSG) recommendations of the International Diagnostic and Pregnancy Society, and by analyzing estimates of the generalized general equation (GEE) for evaluation. Communication between paraben exposure and GDM risk was used.

They received the results and in total more than 100 women were diagnosed with GDM. Although the relationship between GDM and MeP, EtP and PrPy risks was investigated, the relationship between UrPP and BzP for detection rate was relatively low. After adjusting for potential abnormalities, EtP urine was associated with GDM. Risk ratio to the least squares and the largest squares of the second and third apartments. There was no evidence that there was an association Between urinary MeP or PrP and GDM (Liu et al. 2014; Cox and Elelman 2009).

Thus, in their judgment, it was reasoned that this is the first account of the relationship between paraben concentrations during pregnancy and GDM. Our findings indicate that exposure to EtP can increase the risk of GDM.

The paper '1,5 Anhydroglucitol in gestational diabetes mellitus' by Pramodkumar et al. (2019). 1,5 anhydroglucitolis reported to be sensitive to several days of glucose changes and short-term glycemic control in type-1 and type-2 diabetic patients. However, the role of 1.5 gg in gestational diabetes (GDM) is unknown.

They also estimated serum levels of 1, 5 g in pregnant women with and without GDM.

The method used by the authors during their study is less than 100 pregnant women, less than 150, and almost none. Visiting GDM from a preschool clinic in Tamil Nadu in South India for 85 years. An oral glucose tolerance (OGTT) test was performed using 80 grams of oral glucose and GDM was determined based on the International Diabetes and Pregnancy Society standards. Serum levels of 1, 5 AG were measured using a laboratory enzyme kit, colorimeter (Glycomark®, New York, NY). The receiver function curve (ROC) was used to identify 1,5 GHz breakpoints for GDM detection.

The conclusion was taken as an average of 1,5 AG in women with GDM / μg / ml, Pb compared to non-GDM women. In the multiple regression analysis, 1,5 gigabytes were significantly correlated with GDM after adjusting the opponent candidates. 1, 5 DM was C 0.693 compared to fructosamine and HbA1c, detecting GDM. In general, according to him, 1,5 gg of pregnant women with GDM is lower than pregnant women without GDM (Pramodkumar et al. 2019).

23.3 Our Experimental Results, Interpretation and Discussion

23.3.1 Experimental Setup

It does not cause headache due to diabetes. However, although headaches are usually not at risk, they may show signs of diabetes management in diabetics. A tension headache can indicate that the level of hyperglycemia is higher. Instead, blood sugar levels can be very low this is called hypoglycemia. Stress is a natural response to different types. Body sensors, as well as the concept of Internet sensors, can supply a wealth of data about mental and physical health.

We have collected this big data and studied the people; we have studied their tension level and helped them to cure it. In this chapter, we did our best to analyse the correlation between diabetes and stressors. For the analysis, we have been collected sample of 30 subjects from hospitals of Delhi in random fashion who has been suffering from Diabetes from their Health Insurance Providers without disclosing any Personal Information (PI) or Sensitive Personal Information (SPI) by Law.

To identify each case sample ids like S1, S2 etc. has been allotted to the subjects. Sample Data has been collected for following parameters: gender, age, diabetes type, insulin dependency, obesity status, CAD status. We have used the Tableau s/w for this analysis.

The body sensors along with the concept of the Internet of Things can provide rich information about one's mental and sical health.

DM are a metabolic-metabolic disease syndrome identified by hyperglycemia that results in decreased insulin action, secretion, /(or) both. Hyperglycemia with DM causes long-term damage, abnormal function and multiple organ failure, especially the eye, kidney, nerves, heart and blood vessels.

Several data sources are used to diagnose DM and determine their own care activities. In this chapter, we discusses type-2 diabetes and its correlation with TTH, the role of emerging technologies in diabetes treatment, diabetes self care, and Big Data analysis in diabetes management.

Stress is a natural response to stressors that can cause physiological and behavioral changes. If it is longer than that, stress can adversely affect your body. Body sensors with the Internet of Things concept can provide rich information about their mental and physical health.

To identify each case sample ids like S1, S2 etc. has been allotted to the subjects. Sample big data has been collected for following parameters:

1. Gender
2. Age
3. Diabetes Type
4. Subject on Insulin
5. Subject having Obesity
6. Subject having CAD

7. Subject having HTN
8. Subject suffering from TTH (a.ka. headache)/Migraine.

Our area of interest is on TTH/ Migraine parameter. The study focuses on finding the role of diabetes in causing TTH and what are the peculiar probabilities/pattern which do/can lead subject to TTH. To find the pattern and relationship on different parameters, we first, analyzed the collected sample data with following parameters: TTH/Migraine parameter, Diabetes Type & Insulin.

23.3.2 About the Study and Analysis

In order to gain more in-sight and to know the role of diabetic type in causing the TTH, a stacked bar relationship of diabetes type and TTH is plotted and it has been observed that Type-I diabetic is almost no contribution in TTH. In other words subject suffering from Type-I is reported very less about TTH. It can be justified as Type-I subjects are of younger age groups so they are able to cope up with tense situation or it might be the case they do not have such significant level of tension that can cause the TTH. But the number increases significantly for type-II diabetes patient. The summary data of various are as: (As per Table 23.1) & (As per Fig. 23.3).

The respective chart is:

To gain the combined insight of TTH, Diabetes Type with Gender, a group stacked columnar chart is created in which Age group and Gender is plotted on axis

Table 23.1 Diabetes type & TTH distribution in the sample

Diabetes type	TTH	% of total number of subjects	% of total number of subjects within each diabetic type	Number of subjects
Type-I	Yes	3.333333333%	20%	1
Type-I	No	13.333333333%	80%	4
Type-II	Yes	23.333333333%	28%	7
Type-II	No	60%	72%	18
Type-II	No	60%	72%	18

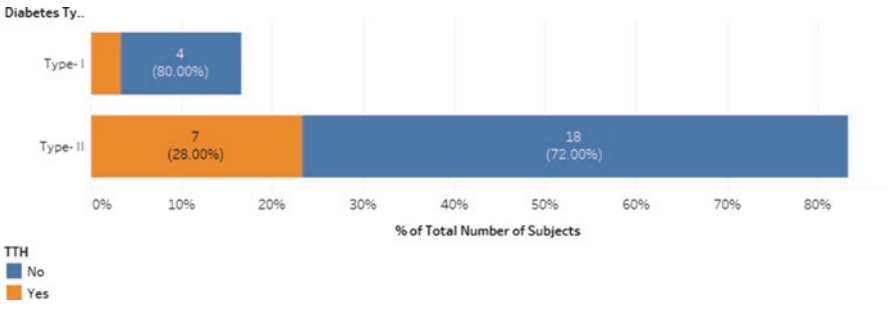


Fig. 23.3 Diabetes type & TTH distribution in the sample

with subject frequency on y-axis and Diabetes type is mapped with the color aesthetic feature there by helping in visualizing 4 different attributes on single graph and giving us very beautiful insight (As per Fig. 23.4).

The graph above is showing precisely that TTH to the subject having Type-I diabetes has been found only in 1 subject that too below 25 age. The subject may be demotivated and over thinking due to diabetes condition and leading to TTH. Other than this all reported cases are of Type-II diabetes following the same pattern with male and females as discussed above (As per Fig. 23.5).

In this it can be clearly seen that, middle aged male is not consuming insulin but is sufferer of TTH while the TTH suffering female is consuming insulin and non-insulin equally while the aged female is not consuming insulin but all the male reported TTH is necessarily consuming insulin. Observing this it can be stated that if old aged male is consuming external insulin then he must be having TTH. And for rest other group drawing a generic conclusion is difficult as the variation is peculiar for each group.Summary data of above graph is below: (As per Fig. 23.6) & (As per Table 23.2).

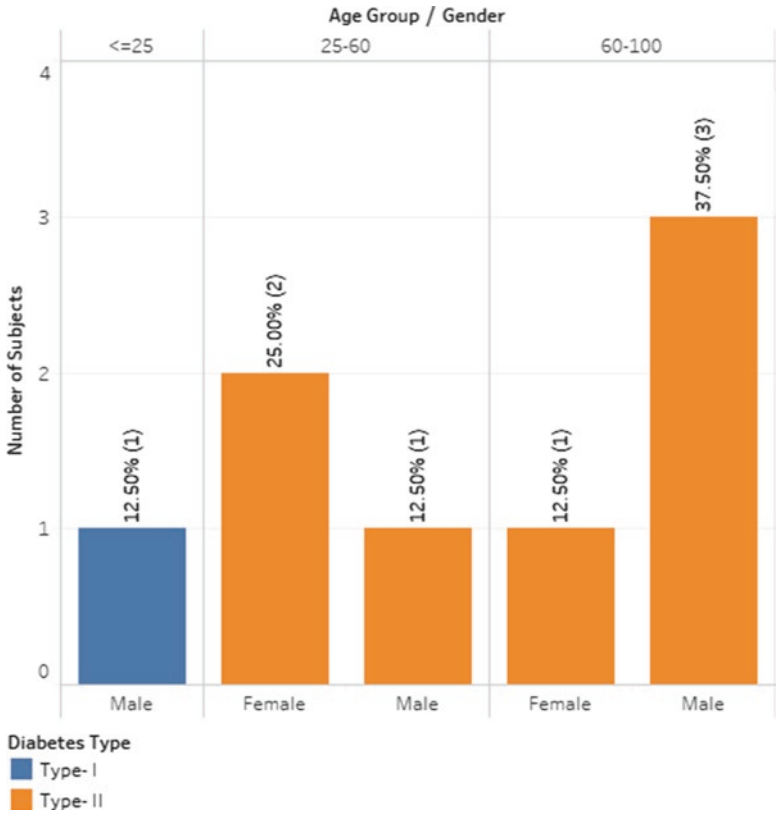


Fig. 23.4 Age group, gender & diabetes type-TTH distribution in the sample

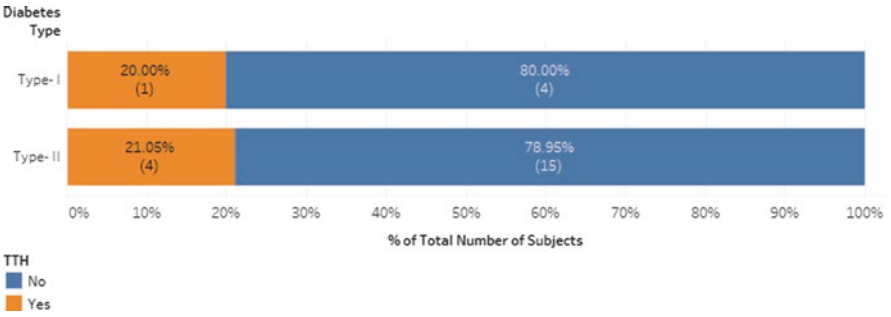


Fig. 23.5 Diabetes type & insulin consumption-TTH distribution in the sample

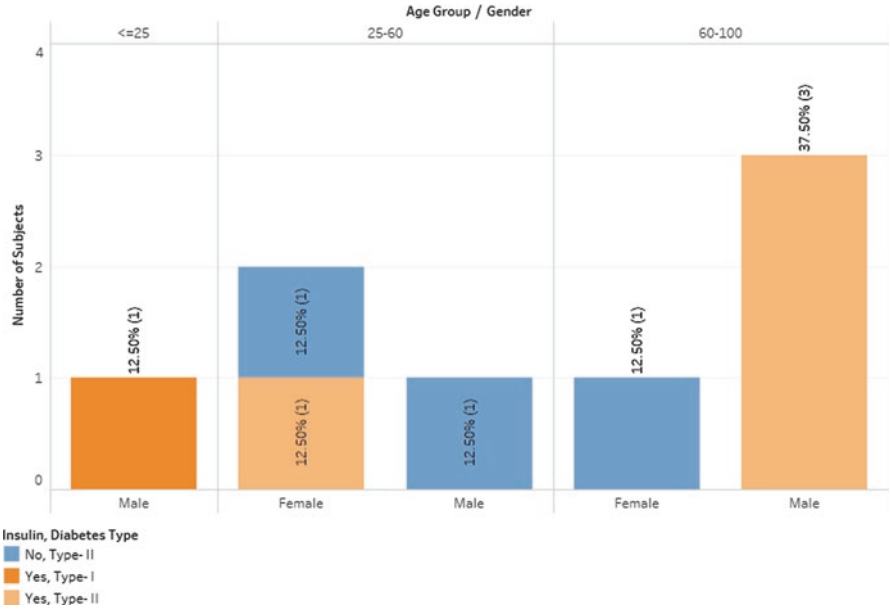


Fig. 23.6 Age group, gender & diabetes type for insulin consuming group –tth distribution as per type-1 & type-2 in the sample

23.4 Novelty in Presented Work

In the current scenario, the problem of diabetes and stress (<= 25, 25–60 and 60–100) are set up in the major issues of adult males and women of different age groups.

A people belonging to any class and society are now, and how the problem is affected by diabetes, and because of this, it catches stress and thus faces TTH or HTN (Chaturvedi et al. 2018; Satya et al. 2019; Rastogi et al. 2018a). In the initial stage such subject can control it by correcting their life style, doing yoga or exercises. Nutrition is the Fundamental part of treatment.

Table 23.2 Summary for the diabetes and correlation of stress on human health on various medical parameters

Summary data						
			Gender/TTH			
			Female		Male	
Diabetes type	Age group	Insulin	No	Yes	No	Yes
Type-I	<=25	Yes	4.55%		9.09%	12.50%
	25–60	Yes			4.55%	
Type-II	<=25	Yes			4.55%	
	25–60	No		12.50%	9.09%	12.50%
		Yes	40.91%	12.50%	9.09%	
	60–100	No	4.55%	12.50%		
		Yes	4.55%		9.09%	37.50%

Our research will be very helpful for diagnosing the both type of diabetes, insulin production and consumption and for reducing the headache level. We have used the Tableau s/w for the Analysis of Diabetes and Correlation of Stress on Human Health on Various Medical Parameters.

The tableau platform helps you to transform your Big Data into an action-driven insight. As it is said right, everywhere Big Data and tableau for everyone. Studies have shown that more systematic assessments are needed to increase the possibilities in many areas. Our research is particularly useful. There are studies to tailor solutions to predict high-risk patients and many data streams side effects and select treatment for ill patients, especially the use of sensor technology and several organ systems.

23.5 Future Scopes, Limitations and Possible Applications

We have found from our sample analysis our sample is not prone to Gender bias. Which can be used efficiently in future for analyzing large data sample (McAfee et al. 2012; Alam 2012; Ali et al. 2019; Singh et al. 2019). It is clearly shown by the donut chart that Type-II diabetes is most commonly found diabetes. This type of diabetes is mainly caused due to bad life styles – irregular sleeps wrong food habit. In this type of diabetes some cases may or may not require insulin (Felman 2018). In the initial stage such subject can control it by correcting their life style, doing yoga or exercises.

It can be seen clearly that the in Type-I category, male is having 80% of total type-I subjects that is indicating that males are more prone to hereditary diabetes transfer as compare to females (Imran Khan et al. 2018; Kumar et al. 2017). Since the sample size is less so to conclude it into final remark one should study larger sample size for type-I diabetes patient residing in various regions.

We can easily find TTH variation with the variation of other disease in subject apart from above mentioned diseases like Obesity, Cancer and heart attack etc. using Tableau s/w for the Big datasets (McAfee et al. 2012; Rastogi et al. 2018a). This TTH & both type of diabetes depends on various factors like age, gender, Diabetes Type, subject on Insulin, Subject having Obesity, subject having CAD, Subject having CAN & Subject suffering from TTH (a.ka. headache) / Migraine etc. (Chaturvedi et al. 2017; Gupta et al. 2019; Brazier 2018; Nordqvist 2019b; Felman 2018). Interesting observation during our research that none of our female subject having diabetes is below 25 years i.e. early age diabetes cases are very less comparative to males subjected to the case sampling should not be impacted for age group gender biasing.

Big Data analytics helps in the pursuit of healthcare, for example, using tools such as assessing the driver's overall cost and geocaching (coding data with geographic information) to diagnose epidemics you or identify "hot spots" etc. of expenses. Outcomes for both patients, such as high cost patients, may be re-established or suffer side effects, and patient management should lead to savings in medical costs. There are various healthcare devices available in the hospitals for the diabetic patient and for maintaining sugar level in human body. But proper diet plan and insulin therapy can be very useful for controlling diabetes.

23.6 Recommendations and Future Considerations

The authors have distributed the parameters in the sample for better analysis like: Gender, age and Gender & age group. We have found our sample is not bias. It contains equals number of males and females. The result were taken using analysis parameters as mentioned above type of Diabetes Type I & II with different age groups <=25, 25–60 and 60–100. It has been observed middle age (25–60) is having more diabetic cases than other ages. The study may be increase for larger subjects.

In the Type-I category, male is having 80% of total type-I subjects that is indicating that males are more prone to hereditary diabetes transfer as compare to females. It was seen that females of age group 25–60 are the highest in frequency in the collected sample. On studying articles related to diabetes it can be said that the possible cause can be the pregnancy in females, irregular sleeping and daily habits etc. This fact is supported by the big data when we look deeper into the details then we found that even in type-I case only female subject is of middle age while all male subjects are below 25 year of age group.

In type-II category female seems to dominate by 16% that indicates females are having more bad habits for food, life style etc. When we look into insight of gender with age group distribution it has been found that in every age group females are dominating. The overall age group with gender and number of subject having TTH or not is plotted in below grouped stacked columnar chart. It can be observed that very fewer cases are observed for TTH for the males below 60 but the number get increased dramatically as age goes beyond 60. This signifies old age men are having highest probability among all segregation having TTH.

23.7 Conclusions

Big data/ Massive data, including analytics, are a potent tool that will help with healthcare in other manufactures as well. The election of these specific uses discussed in this chapter is controversial. It was seen that with the starting of the sample analysis we had the sample From the Hospitals of Delhi and NCR, of 30 subjects in random fashion. Our sample is not prone to Gender bias.

We found that even in type-I case only female subject is of middle age while all male subjects are below 25 year of age group (Kumar et al. 2017). On seeing the result, It can be clearly observed from the donut chart study that the 25–60 age group is more prone towards diabetes (Imran Khan et al. 2018).

On analyzing the frequency stacked columnar graph, it can be easily seen that females of age group 25–60 are the highest in frequency in the collected sample. On studying articles related to diabetes it can be said that the possible cause can be the pregnancy in females, irregular sleeping and daily habits etc. It is clearly shown by the donut chart that Type-II diabetes is most commonly found diabetes. This type of diabetes is mainly caused due to bad life styles – irregular sleeps wrong food habit. In this type of diabetes some cases may or may not require insulin. In the initial stage such subject can control it by correcting their life style, doing yoga or exercises.

On analyzing this ratio distribution within the gender, it has been found that males are more prone to TTH than as compare to females. Twenty-five percent more males are reported having TTH than females. On detailed look into the data and subjected to discussion it has been found that sampled males are working while females are less working so there is possibility of work stress which is causing more frequent headache.

The overall age group with gender and number of subject having TTH very less cases are observed for TTH for the males below 60 but the number gets increased dramatically as age goes beyond 60. This signifies old age men are having highest probability among all segregation having TTH (Rastogi et al. 2018a; Chauhan et al. 2018).

Also, for females increasing trends of TTH can be observed up to age of 60 beyond that cases of TTH decreases. This is in line with the overall pattern of diabetic subject variation with age group.

In our research work it has been observed that Type-I diabetic is almost no contribution in TTH. In other words subject suffering from Type-I is reported very less about TTH. In conclusion, it can be said that TTH cases increasing with age in case of males and not following the pattern of Diabetes variation with age while in case of female TTH pattern variation is same as diabetes i.e. increasing trend up to age of 60 then decreasing.

In the overall scenario, Interesting observation during our research that none of our female subject having diabetes is below 25 years i.e. early age diabetes cases are very less comparative to males subjected to the case sampling should not be impacted for age group gender biasing. It can be said that TTH cases increasing with age in case of males and not following the pattern of Diabetes variation with

age while in case of female TTH pattern variation is same as diabetes i.e. increasing trend up to age of 60 then decreasing.

Acknowledgments We would like to thanks seniors of ABES Engineering College, Ghaziabad, Dayalbagh Educational Institute, Agra and experts from Tata Consultancy Services for their extraordinary support in this research process. The Infrastructure and research samples by different labs have been collected. We pay our sincere thanks to all direct and indirect supporters.

References

Alam, M. *Cloud algebra for cloud database management.* The second international Conference on Computational Science, Engineering and Information Technology (CCSEIT-2012), October 26~28, 2012, Coimbatore, India, Proceeding published by ACM.

Ali, S. A., & Alam, M. *A relative study of task scheduling algorithms in cloud computing environment.* In Proceedings of the 2016 2nd international conference on contemporary computing and informatics, IC3I 2016, 7917943, (pp. 105–111), (Scopus indexed).

Ali, S. A., Affan, M., & Alam, M. (2019). A study of efficient energy management techniques for cloud computing environment. *2019 9th international conference on cloud computing, data science & engineering (confluence)* (pp. 13–18), Noida, India. https://doi.org/10.1109/CONFLUENCE.2019.877697.

Arora, N., Rastogi, R., Chaturvedi, D. K., Satya, S., Gupta, M., Yadav, V., Chauhan, S., & Sharma, P. (2019). *Book chapter titled as 'Chronic TTH analysis by EMG & GSR biofeedback on various modes and various medical symptoms using IoT',* Paperback ISBN: 9780128181461, Chapter 5, (pp. 87–149), Advances in ubiquitous sensing applications for healthcare, Book-Big Data analytics for intelligent healthcare management. https://doi.org/10.1016/B978-0-12-818146-1.00005-2.

Bansal, I., Rastogi, R., Chaturvedi, D. K., Satya, S., Arora, N., & Yadav, V. (2018). *Intelligent analysis for detection of complex human personality by clinical reliable psychological surveys on various indicators.* In the national Conference on 3rd MDNCPDR-2018 at DEI, Agra On 06–07, September, 2018.

Brazier, Y. (2018). What is obesity and what causes it? *Medical News Today*, Retrieved November 2, 2018, from, https://www.medicalnewstoday.com/articles/323551.php.

Chatruvedi, D. K., & Lajwanti. (2014). *Correlation between energy distribution profile and level of consciousness*. *International Journal of Education, 4*(1), 1–9.

Chaturvedi, D. K. (2004). *Science, religion and spiritual quest* (pp. 15–17). DEI Press. Edited book on linkages between social service, agriculture and theology for the future of mankind.

Chaturvedi, D. K. (2012). *Human rights and consciousness.* International seminar on prominence of human rights in the criminal justice system (ISPUR 2012), Organized Ambedkar Chair, Department of Contemporary Social Studies & Law, Dr. B.R. Ambedkar University, Agra, 30–31 March 2012, pp. 33.

Chaturvedi, D. K. (2019). *Relationship between chakra energy and consciousness*. *Biomedical Journal of Scientific and Technical Research, 15*(3), 1–3. https://doi.org/10.26717/BJSTR.2019.15.002705, ISSN: 2574-1241.

Chaturvedi, D. K. & Arya, M. (2013a). *Correlation between human performance and consciousness.* IEEE-International conference on human computer interaction, 23–24 August 2013, Saveetha School of Engineering, Saveetha University, Thandalam, Chennai, IN, India.

Chaturvedi, D. K., & Arya, M. (2013b). A study of correlation between consciousness level and performance of worker. *Industrial Engineering Journal, 6*(8), 40–43.

Chaturvedi, D. K., & Lajwanti. (2015). *Dayalbagh way of life for better worldliness*. *Journal of Research in Humanities and Social Science, 3*(5), 16–23, ISSN(Online) : 2321-9467.

Chaturvedi, D. K., & Satsangi, R. (2013). *The correlation between student performance and consciousness level.* International Conference on Advanced Computing and Communication Technologies (ICACCT™-2013), 16 November 2013, Asia Pacific Institute of Information Technology SD India, Panipat (Hariyana), Souvenir – pp. 66, proc. pp. 200–203.

Chaturvedi, D. K., & Satsangi, R. (2014, January). The correlation between student performance and consciousness level. *International Journal of Computing Science and Communication Technologies*, *6*(2), 936–939. (ISSN 0974-3375).

Chaturvedi, D. K., Lajwanti, T. H. C., & Kohli, H. P. (2012). *Energy distribution profile of human influences the level of consciousness.* Towards a science of consciousness, Arizona conference proceeding, Tucson, Arizona.

Chaturvedi, D. K., Kumar Arora, J., & Bhardwaj, R. (2015, September). Effect of meditation on chakra energy and hemodynamic parameters. *International Journal of Computer Applications, 126*(12), 52–59.

Chaturvedi, D. K., Rastogi, R., Arora, N., Trivedi, P., & Mishra, V. (2017). *Swarm intelligent optimized method of development of noble life in the perspective of indian scientific philosophy and psychology.* In Proceedings of NSC-2017 (National System Conference), DEI Agra, December 1–3, 2017.

Chaturvedi, D. K., Rastogi, R., Satya, S., Arora, N., Saini, H., Verma, H., Mehlyan, K., & Varshney, Y. (2018). *Statistical analysis of EMG and GSR therapy on visual mode and SF-36 scores for chronic TTH.* In the proceedings of UPCON-2018 on 2–4 November 2018 MMMUT Gorakhpur, UP.

Chauhan, S., Rastogi, R., Chaturvedi, D. K., Satya, S., Arora, N., Yadav, V., & Sharma, P. (2018). *Analytical comparison of efficacy for electromyography and galvanic skin resistance biofeedback on audio-visual mode for chronic TTH on various attributes.* In the proceedings of the ICCIDA-2018 on 27 and 28th October 2018, CCIS Series, Springer at Gandhi Institute for Technology, Khordha, Bhubaneswar, Odisha, India.

Cox, E. M., & Elelman, D. (2009). Test for screening and diagnosis of type-2 diabetes. *Clinical Diabetes, 27*(4), 132–138.

Felman, A. (2018). An overview of insulin. *Medical News Today*. Retrieved November 2018, from https://www.medicalnewstoday.com/articles/323760.php.

Felman, A. (2019). What to know about hyperglycemia. *Medical News Today.* Retrieved May 7, 2019, from https://www.medicalnewstoday.com/articles/323699.php.

Gulati, M., Rastogi, R., Chaturvedi, D. K., Sharma, P., Yadav, V., Chauhan, S., Gupta, M., & Singhal, P. (2019).Statistical resultant analysis of psychosomatic survey on various human personality indicators: Statistical survey to map stress and mental health. *Handbook of Research on Learning in the Age of Transhumanism* (pp. 363–383). Hershey: IGI Global. ISSN: 2326-8905|EISSN: 2326–8913. https://doi.org/10.4018/978-1-5225-8431-5.ch022.

Gupta, M., Rastogi, R., Chaturvedi, D. K., Satya, S., Arora Verma, H., Singhal, P., & Singh, A. (2019). Comparative study of trends observed during different medications by subjects under EMG & GSR biofeedback. ICSMSIC-2019, ABESEC, Ghaziabad. 8–9 March 2019. IJITEE, *8*(6S), 748–756. https://www.ijitee.org/download/volume-8-issue-6S/.

Imran Khan, S., Naqvi, K., Alam, M., & Rizvi, S. N. A. (2018). *A framework for twitter data analysis, Big Data analytics* (pp. 297–303). Verlag: Springer Singapore, Print ISBN: 978-981-10-6619-1, Electronic ISBN: 978-981-10-6620-7.

Khan, S., Liu, X., Shakil, K. A., & Alam, M. (2019a). *Big data technology – enabled analytical solution for quality assessment of higher education systems*. International Journal of Advanced Computer Science and Applications (IJACSA), *10* (6). https://doi.org/10.14569/IJACSA.2019.0100640 [ESCI/Scopus].

Khan, S., Shakil, K. A., & Alam, M. (2019b). *PABED – a tool for Big education data analysis*. In 2019 20th IEEE International Conference on Industrial Technology (ICIT 2019), Melbourne, Australia, February 13–15, 2019. [Scopus/IEEE].

Khanna, A. L., Singh, S. N., & Alam, M. Educational data mining and its role in determining factors affecting students academic performance: A systematic review. *Conference Information Processing (IICIP), 2016 1st India International Conference* (pp. 1–7), 2016/8/12, IEEE.

Kumar, V., Kumar, R., Pandey, S. K., & Alam, M. (2017, October). *Fully homomorphic encryption scheme with probabilistic encryption based on Euler's theorem and application in Cloud Computing, Big Data Analytics* (pp. 605–611). Springer. Print ISBN: 978-981-10-6619-1, Electronic ISBN: 978-981-10-6620-7.

Liu, Z., Ao, D., Yang, H., & Wang, Y. (2014). Gestational weight gain and risk of gestational diabetes mellitus among Chinese women. *Chinese Medical Journal (Engl.), 127*(7), 1255–1260.

Malhotra, S, Doja, M. N, Alam, B., & Alam, M. Big data analysis and comparison of big data analytic approaches, Computing, Communication and Automation (ICCCA). 2017 International Conference, 2017/5/5 (pp. 309–314), IEEE.

Malhotra, S., Doja, M. N., Alam, B., & Alam, M. *Journal International Journal of Information Technology and Web Engineering (IJITWE)*, *13*(3), 1–13, 2018/7/1, IGI Global, (Scopus indexed).

Marrie, R. A., Patel, R., Figley, C. R.,Kornelsen, J., Bolton, J. M., Graff, L., Mazerolle, E. L., Marriott, J. J., Bernstein, C. N., & Fisk, J. D. (2019, January). Diabetes and anxiety adversely affect cognition in multiple sclerosis. *Multiple Sclerosis and Related Disorder Satellites*, *27*, 164–170.

McAfee, A., Brynjolfsson, E., Davenport, T. H., Patil, D. J., & Barton, D. (2012). Big data: The management revolution. *Harvard Business Review, 90*(10), 60–68.

Nordqvist, C. (2019a). All about hypoglycemia (low blood sugar). *Medical News Today.* Retrieved March 11, 2019, from https://www.medicalnewstoday.com/articles/166815.php.

Nordqvist, C. (2019b). What to know about coronary heart disease. *Medical News Today.* https://www.medicalnewstoday.com/articles/184130.php, 5th July 2019.

Pramodkumar, T. A., Jayashri, R., Gokulakrishnan, K., Velmurugan, K., Pradeepa, R., Venkatesan, U., Saravanan, P., Uma, R., Anjana, R. M., & Mohan, V. (2019, March). *1,5 An hydroglucitol in gestational diabetes mellitus*. *Journal of Diabetes and Its Complications, 33*(3), 231–235. https://doi.org/10.1016/j.jdiacomp.2018.11.010.

Rahmani, A.-M., Thanigaivelan, N. K., Gia, T. N., Granados, J., Negas, B., Liljeberg, P., & Tenhunen, H. (2015, January). Smart e-health gateway: bringing intelligence to Internet-of-Things-based ubiquitous healthcare systems. In *Proceedings of the annual IEEE consumer communications and networking conference*. NV, USA: IEEE.

Rastogi, R., Chaturvedi, D. K., Satya, S., Arora, N., & Chauhan, S. (2018a). *An optimized biofeedback therapy for chronic TTH between electromyography and galvanic skin resistance biofeedback on audio, visual and audio visual modes on various medical symptoms.* In the national conference on 3rd MDNCPDR-2018 at DEI, Agra On 06–07 September, 2018.

Rastogi, R., Chaturvedi, D. K., Satya, S., Arora, N., Yadav, V., Chauhan, S., & Sharma, P. (2018b). *SF-36 scores analysis for EMG and GSR therapy on audio, visual and audio visual modes for chronic TTH.* In the proceedings of the ICCIDA-2018 on 27 and 28th October 2018 CCIS Series, Springer at Gandhi Institute for Technology, Khordha, Bhubaneswar, Odisha, India.

Rastogi, R., Chaturvedi, D. K., Satya, S., Arora, N., Singhal, P., & Gulati, M. (2018c). *Statistical resultant analysis of spiritual & psychosomatic stress survey on various human personality indicators.* In the international conference proceedings of ICCI 2018. https://doi.org/10.1007/978-981-13-8222-2_25.

Rastogi, R., Chaturvedi, D. K., Satya, S., Arora, N., Sirohi, H., Singh, M., Verma, P., & Singh, V. (2018d). *Which one is best: Electromyography biofeedback efficacy analysis on audio, visual and audio-visual modes for chronic TTH on different characteristics.* In the proceedings of ICCIIoT- 2018, 14–15 December, 2018 at NIT Agartala, Tripura, ELSEVIER- SSRN Digital Library (ISSN 1556-5068).

Richa, K. C., & Devendra Prakash, S. (2016). *The consciousness in Mosquito*. *Journal of Mosquito Research, 6*(34), 1–9, ISSN 1927-646X.

Richa, Chaturvedi, D. K., & Prakash, S. (2016). *Role of electric and magnetic energy emission in intra and interspecies interaction in microbes*. *American Journal of Research Communication, 4*(12), 1–22, ISSN: 2325-4076.

Saini, H., Rastogi, R., Chaturvedi, D. K., Satya, S., Arora, N., Verma, H., & Mehlyan, K. (2018). *Comparative efficacy analysis of electromyography and galvanic skin resistance biofeedback*

on audio mode for chronic TTH on various indicators. In the proceedings of ICCIIoT- 2018, 14–15 December, 2018 at NIT Agartala, Tripura, ELSEVIER- SSRN Digital Library (ISSN 1556-5068).

Saini, H., Rastogi, R., Chaturvedi, D. K., Satya, S., Arora, N., Gupta, M., & Verma, H. (2019). *An optimized biofeedback EMG and GSR biofeedback therapy for chronic TTH on SF-36 scores of different MMBD modes on various medical symptoms.* ISBN:978-981-13-8929-0, Chapter 8 of hybrid machine intelligence for medical image analysis, studies Comp. intelligence, vol. 841, Springer Nature Singapore Pte Ltd. https://doi.org/10.1007/978-981-13-8930-6_8.

Satya, S., Rastogi, R., Chaturvedi, D. K., Arora, N., Singh, P., & Vyas, P. (2018). *Statistical analysis for effect of positive thinking on stress management and creative problem solving for adolescents.* In Proceedings of the 12th INDIA-Com; 2018 ISSN 0973–7529 and ISBN 978-93-80544-14-4, (pp. 245–251).

Satya, S., Arora, N., Trivedi, P., Singh, A., Sharma, A., Singh, A., Rastogi, R., & Chaturvedi, D. K. (2019). *Intelligent analysis for personality detection on various indicators by clinical reliable psychological TTH and stress surveys.* In the proceedings of CIPR 2019 at Indian Institute of Engineering Science and Technology, Shibpur on 19th–20th January 2019, Springer-AISC Series.

Saxena, S., Alam, M., & Jabarullah, B. M. (2018, September). DS-HM model with DCT-HW features for face recognition. *International Journal of Scientific Research in Computer Science Applications and Management Studies*, *7*(5), ISSN 2319–1953.

Shakil, R. K., Alam, M., Shakeel, S., Ora, A., & Khan, S. Exploiting data reduction principles in cloud-based data management for cryo-image data. In *Proceedings of the 2018 International conference on computers in management and business* (pp. 61–66), 2018/5/25, ACM.

Sharma, S., Rastogi, R., Chaturvedi, D. K., Bansal, A., & Agrawal, A. (2018). *Audio visual EMG & GSR biofeedback analysis for effect of spiritual techniques on human behavior and psychic challenges.* In Proceedings of the 12th INDIACom; 2018, ISSN 0973–7529 and ISBN 978-93-80544-14-4, (pp. 252–258).

Singh, A., Rastogi, R., Chaturvedi, D. K., Satya, S., Arora, N., Sharma, A., & Singh, A. (2019). Intelligent personality analysis on indicators in IoT-MMBD enabled environment. Chapter 7 of multimedia Big Data computing for IoT applications: Concepts, paradigms, and solutions, Springer Nature Singapore. https://doi.org/10.1007/978-981-13-8759-3_7.

Singhal, P., Rastogi, R., Chaturvedi, D. K., Satya, S., Arora, N., Gupta, M., Singhal, P., & Gulati, M. (2019). *Statistical analysis of exponential and polynomial models of EMG & GSR biofeedback for correlation between subjects medications movement & medication scores.* ICSMSIC-2019, ABESEC, Ghaziabad, 8–9 March 2019, IJITEE, *8*(6S), 625–635. https://www.ijitee.org/download/volume-8-issue-6S/

Tsai, H. C., Cohly, H., & Chaturvedi D. K. (2013). *Towards the consciousness of the mind.* Towards a science of consciousness, Dayalbagh conference proceeding, Agra, India.

Vyas, P., Rastogi, R., Chaturvedi, D. K., Arora, N., Trivedi, P., & Singh, P. (2018). *Study on efficacy of electromyography and electroencephalography biofeedback with mindful meditation on mental health of youths.* In Proceedings of the 12th INDIA-Com; 2018 ISSN 0973–7529 and ISBN 978-93-80544-14-4, (pp. 84–89).

Williams, P. A., & Woodward, A. J. (2015, July). *Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem.* Medical devices (Auckland), *8*, 305–316.

Yadav, V., Rastogi, R., Chaturvedi, D. K., Satya, S., Arora, N., Yadav, V., Sharma, P., & Chauhan, S. (2018). Statistical analysis of EMG & GSR biofeedback efficacy on different modes for chronic TTH on various indicators. *International Journal of Advanced Intelligence Paradigms, 13*(1), 251–275. https://doi.org/10.1504/IJAIP.2019.10021825.

Yang, W., Dall, M. T., Tan, E., Byrne, E., Iacobucci, W., Chakrabarti, R., & Loh, F. E. (2018). *Diabetes diagnosis and management among insured adults across metropolitan areas in the U.S.*. Preventive medicine reports, *10*, June 2018, pp. 227–233.

Yin, Y., Zeng, Y., Chen, X., & Fan, Y. (2016, March). *The internet of things in healthcare: an overview*. *Journal of Industrial Information Integration, 1*, 3–13.

Chapter 24
Monitoring System Based in Wireless Sensor Network for Precision Agriculture

Fekher Khelifi

Abstract The monitoring of various interest parameters in a culture was proven as a useful tool, which improve the agricultural production. The monitoring of crops in precision farming can be achieved through a multiplicity of technologies; however, using Wireless Sensor Networks results in low-power deployments, thus becoming a dominant option. Our research proposes the development of a new agricultural field monitoring system based on atmospheric sensors capable of measuring the different parameters of the air and soil sensors measuring the soil parameters. In this chapter, we propose a periodic hybrid routing algorithm sensitive to the threshold for the collection of environmental data. The proposed algorithm uses region-based cluster approaches for the deployment of sensor nodes, which provide effective coverage to the entire agricultural area. In addition, a proposed clustering protocol based on the combination of residual energy and distance between neighboring nodes, to obtain optimal Cluster-head and improve energy efficiency in the WSN. The results of the simulation show that the proposed routing algorithm exceeds other well-known algorithms based on packet delivery, energy consumption and network lifetime as a performance measure.

Keywords Monitoring system · WSN · Clustering · Precision agriculture

24.1 Introduction

The emergence of connected objects is considered by observers as a revolution in the twenty-first century (Tayeb et al. 2017). We speak of IoT and M2M to translate autonomous interaction and bidirectional or mono-directional transmission of data between networks of physical and virtual objects (Sánchez et al. 2015). IoT applications are increasingly present in everyday life from connected buildings (security control or energy consumption) to community projects to optimize infrastructure

F. Khelifi (✉)
Laboratory of Electronics and Microelectronics, University of Monastir, Monastir, Tunisia
e-mail: fakher.Khelifi@fsm.rnu.tn

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_24

management (transport, energy, water, etc.), including industry and automotive, agriculture and livestock.

Agriculture is perhaps the most successful sector in which IoT can benefit from its implementation (Jiang et al. 2016): its assets are scattered over long distances and difficult to monitor manually. By combining IoT and Big Data analysis, operators can obtain a wide range of data and use it to increase efficiency, increase productivity and monitor the quality of food products, from field to plate.

All specialties combined, agricultural production, dairy or livestock, the professionals of the sector must manage and monitor their productions and their equipment spread over surfaces of varying size: livestock, crops, tractors or even irrigation equipment (Maurya and Jain 2017). IoT solutions can help them greatly, to monitor the health of remote animals, for example, and track herd movements to better manage pastures and increase yields. As far as irrigation systems or agricultural equipment are concerned, analysis of the data collected by the IoT sensors gives an overall view of performance and better planning of maintenance operations to avoid any risk of failure which would penalize the performance. In the field of precision farming, real-time access to weather data, air quality, soil.

Hydration can help make better decisions when planting and harvesting (Cheng-Jun 2014). The innovative use of the Internet of Objects in the agricultural sector is today an excellent way to continue the development of precision agriculture.

The main advantage of using IoTs in agriculture is the lack of wiring, which considerably reduces the cost of installation. Another advantage is the flexibility of deployment and ease of maintenance (Gubbi et al. 2013). Indeed, the sensors are autonomous and require very little human intervention on the fields, especially in the case where the communication protocols are fault tolerant and support the mobility of the nodes.

The most widely used agricultural monitoring systems are based on low-cost technologies. However, the unique use of the sensor has certain disadvantages such as sensitivity to temperature's variations, sunlight and fluorescence. Hence the need to integrate other acquisition methods in order to improve detection accuracy (Ojha et al. 2015). This additional information can come from environmental sensors, such as temperature sensors, humidity sensors, pressure sensors, vibration sensors. To make the process more efficient and less costly, it collects data from sensors arranged around the installation and analyzes this information to better understand the water circuit as a whole, from the arrival of wastewater to their purification and from receiving the request to the distribution to the stations. By combining these data with cost, electricity consumption and water consumption information, the Agency also extracts real-time information that guides its decisions (Garcia-Sanchez et al. 2011). The organization can thus know which pumps to use, when and for what length of time, depending on supply and demand. The multimodal aspect of these different sensors leads to the implementation of data fusion algorithms in order to obtain reliable information. The fusion of multi-sensory data corresponds to the combination of data provided by several sensors of heterogeneous modalities in order to ensure a reliable and precise information (Khelifi et al. 2017). The main advantages of merging multimodal data are the redundancy and complementarity of

measurements. Merging redundant data can dramatically reduce uncertainty about the information sought and increase its accuracy (Khelifi et al. 2014). In agriculture, Wireless Sensor Networks (WSNs) have been deployed as a cost-effective communications technology that enables the acquisition and transmission of crop-specific data to end users at sites without prior telecommunications infrastructure or by implementing Wired Communications). A WSN consists of small non-intrusive communication devices to which one or more precision sensors for data collection are adapted (Garcia-Sanchez et al. 2011). Sensors typically measure parameters such as soil moisture, salinity or pH, among others. Once the information arrives at their operators, they are processed and studied in order to make an appropriate decision (e.g. additional watering if soil conditions indicate.

After the acquisition phase, the collected data are sent to a node which will be the point of collection of the information on the environment where the various nodes are deployed (Ojha et al. 2015). The routing then takes place, to allow all the nodes of the network to send their information considered vital to the collection point. The routing to the heavy task, to achieve the smooth flow of communications in a sensor network but also in the case of wireless sensor networks, to a compromise with excellent management of transmissions so as not to fall into an energy overconsumption (Liao et al. 2017).

In this chapter, we are interested in the problem of the transmission of data collected by different types of sensors and the energy consumption in the networks of wireless sensors. Thus, our study aims to analyze and model the energy behavior of a node, to study the distribution of energy throughout the network and the aggregation and transmission of data.

Our solution concerns the hierarchical organization of the nodes of the network. We have chosen to concentrate our study on the adaptation of cluster training methods. Therefore, our first contributions concern the clustering processes (Heinzelman et al. 2002; Kuila and Jana 2014; Fang et al. 2003). These avoid the periodic reconfiguration of clusters; and this by initially dividing the network into an optimal number of K equilibrium and disjoint clusters. These processes are based on the following properties:

Organize nodes that have similarities in the same cluster through the distance between a node and its neighbors, the residual energy of the node and its neighbors, and the distance between a node and the base station.
Define the optimum number that the sensor array may contain.
Maximize short-range communications to minimize power consumption and reduce radio interference.
Finally, an inter-cluster communication model is established in each cluster using the "Time Division Multiple Access (TDMA)" technique.

The rest of this chapter is organized like this. Section 24.2 gives the related work. In Sect. 24.3, we present our agricultural monitoring system. Section 24.5 evaluates the performance of the proposed algorithm in scenarios using the NS-3 simulator. On the basis of the results, we conclude this document.

24.2 Related Work

24.2.1 Agricultural Monitoring System

Agriculture is currently experiencing an intense technological change. Its tools evolve its practices also. Every year, many sketches materialize to form new connected objects, to facilitate the work of farmers stuck in the gear of ever more demanding productivity. In this context, a project developed by Irstea involving the use of connected sensors. Autonomous sensors placed in the heart of plots collecting data, transmitted by Internet and analyzed in order to predict possible risks encountered in the field (presence of pests, diseases or "hybrid stress"). Researchers are currently working on the design of these sensors to test them on a farm as quickly as possible (Maurya and Jain 2017).

The latter should be equipped with a control tool connected to a connection interface, a USB port and a wireless communication module (via Bluetooth or Wi-Fi). Once set up, they will communicate with each other before sending their reports to a central data collection platform. Another example of IoT within the farm is that of the measurement sensors. A company like the American Solum has specialized in the sale of grounded, geo-localization and internet-connected probes that measure soil moisture and mineral and nitrate levels (Nugroho et al. 2016). This allows the visualization of these parameters by superimposing them on satellite images and the adaptation of the irrigation and the fertilization by determining them in a targeted and differentiated way between the different plots.

In order to analyze whole hectares of agricultural land, the French start-up Airinov has developed an automatic GPS - guided agronomic mapping system that measures the threshold surface area, chlorophyll rate, nitrogen (Hwang et al. 2010; Khedo et al. 2010). Information-gathering and processing technologies offer prospects of savings of several tens of billions of dollars through the optimization, streamlining and targeting tools offered by ICT. Agriculture now aims to return to a more local and differentiated approach by taking into account data on the farm environment (Maurya and Jain 2017).

In more recent work, data acquisition and fusion (Khelifi et al. 2017) aim to improve decision-making with WSN, which reduces resource consumption and increases performance. Data fusion is a widely useful technique in several WSN, robotic domains. For example, Manjunatha et al. (2008) proposed a mechanism to merge the signals of different sensor types for a cluster to solve this problem. While (Hao et al. 2015), processing and merging of these data is done by a leader of the CH group using a fuzzy system. Detection and fusion are also obtained by multiple data. This article only deals with heterogeneous intra-cluster data fusion, but the merger at the inter-cluster decision level has not yet been mentioned. The fuzzy logic uses a degree of adhesion to normalize the partial data and combine them with fuzzy rules to give a fuzzy output. Therefore, this solution is powerful to cope with the uncertainty of the data. The cluster architecture is used in WSN to optimize data processing from different types of sensors simply by organizing the cluster network.

In the literature, the formation of a cluster begins with the detection of certain events. Heinzelman et al. developed (Heinzelman et al. 2002) a classical clustering protocol that combines energy-efficient clusters, Routing based on application-centric data aggregation, and provides a better lifetime for a WSN. LEACH introduces an algorithm for cluster adaptation and rotation of CH positions to distribute uniformly the energy load among all nodes, allowing for self-organization in the WSN. Another clustering approach proposed by Kuila and Jana (2014). This algorithm presents a linear/nonlinear formulation (LP/NLP) of energy clustering and routing problems in WSN, followed by two algorithms for the same based on particle gas optimization (PSO). In (Fang et al. 2003) Fang et al., Developed a dynamic clustering algorithm. As more than one sensor can detect an event, several volunteers probably existed. Therefore, a decentralized approach must be applied to ensure that only CH is active in close proximity with a highly probable target to follow. The sensors in the active CH proximity are invited to be members of the cluster and to report their sensor data to the CH. In this way, a cluster is not constituted in a zone with a high concentration of events.

24.3 Wireless Sensor Network for Precision Agriculture Application

24.3.1 System Overview

Internet of Things Precision Agriculture uses natural resources more efficiently by collecting real-time data on crop development, soil, weather and air quality, to help farmers make intelligent decisions in planting, fertilizing and harvesting. Using this technology, farmers can use information efficiently to obtain higher yields and, therefore, earn higher profits. To extinguish this objective, we propose a sensitive system to the periodic threshold to measure environmental parameters. The data acquisition network is consisting of the various sensor nodes deployed in the field and the data distribution network composed of a collector node connected to the base station which in turn can be connected to a more extensive network. In order to collect the necessary parameters for decision-making in agriculture, we have chosen a hybrid architecture of the acquisition network that includes two types of nodes: atmospheric nodes capable of measuring the different parameters of the air and Soil nodes measuring the soil parameters. Given that users need information from all of the agricultural field, the routing protocol must provide effective coverage over the entire agricultural field. Thus, the sensors must measure each part of the field, presented on Fig. 24.1. To provide efficient coverage over the entire network field, the region-based clustering approach is used, where the entire zone is divided into different fixed regions and different types of nodes are deployed in the fixed regions according to their Task and their energy level.

Fig. 24.1 Scenario for data collection

In order to ensure effective data routing and effective coverage across the entire field, we propose a hierarchical routing protocol based on the partitioning of the network into a set of clusters. The proposed cost function considers the residual energy within the nodes as the main metric, the distance between a node and its neighbors and the distance between a node and the base station. Our choice is based on the strong constraint Energy in the WSN. Moreover, we will weigh the costs of the links near the base station more than the others, which allows better load balancing between neighboring nodes of the base station. Indeed, these nodes are the most critical because they are more solicited by the routing process and their energies are depleted faster than the other nodes. In order to maintain the structure of the routing constructed, we propose an adaptive approach with a mechanism of implicit acknowledgment of the packets.

24.3.2 Routing Protocol

In a first step, the nodes are deployed in an agricultural field. The base station broadcasts an announcement message to all nodes on the network. Each node can determine the distance between the base station and its neighbors. Subsequently, it broadcasts its parameters in the network with its identifier. By collecting the received packets, each node maintains a list for neighbors. Initially, no nodes belong to the cluster structure and all nodes are in the ordinary state. Each node must then broadcast the message (E_i, d_{ij}, d_i, BS) to its neighbors to a jump. This message will allow neighboring nodes to discover the presence of the sender's node and add it to their neighbor lists. After exchanging the message, each node extracts the information

from the message, calculates the cost function P, by the following Eq. (24.1) and compares it with that of its neighbors:

$$P_{(i,j)} = \left[1 - \sum_{i=j=1}^{n} \left(1 - \frac{d_{BS,i}}{d_{BS,j}} \right), \left(1 - \frac{E_i}{E_j} \right), \left(1 - \frac{d_i}{d_j} \right) \right] \tag{24.1}$$

Where: d is the distance between the node and the base station and E is the residual energy of the node. If the latter is below a defined threshold, the node declares CH and then informs its neighbors of its election. Thus, a warning message containing its identifier as CH is broadcast via a CSMA protocol to avoid probable collisions and interferences between adjacent CHs. The nodes decide to belong to CHs taking into account the distance d_{ij}. Thus, the CH having a higher amplitude cost will have a greater probability of being chosen relative to other CHs. Once the clusters are formed, each CH moves from a simple member node role to a cluster-head role for the transmission of information within its cluster.

Based on the task scheduling method, it implements the TDMA protocol and assigns to each of its member nodes a time interval during which the node can communicate its information. The set of these time intervals constitute a frame, the duration of which differs according to the number of nodes of the cluster. Later, the nodes can start sending and receiving data to the CHs. After a predetermined time, the network will enter a new cycle by returning to the first phase.

When a signal measured by the sensors exceeds a predefined threshold or the collection period is exceeded, the data detected by the member nodes is sent to the cluster head. The data collected at each CH is aggregated and then transmitted directly to the SB. Outside the time allowed for transmission, each node has the ability to standby to save its resources. In this protocol, the processing of the data at the level of each cluster is done locally and the role of each CH is to coordinate the exchanges with the other member nodes. The network has the capacity to self-reorganize during the election phase of the CHs. Each node has the possibility of being elected CH and vis versa, each CH can become a single NM that can belong to a cluster. The election of an HC is based on the cost function. The more the node has an important cost the more it can become CH.

24.4 Experimental Results and Discussion

In the following part, we analyze the costs and the performances of the simulations and the experiments obtained during the implementation of two routing scenarios by measuring and comparing three metrics: end-to-end delay, energy consumption and service life network. We use the NS-3 simulator. Table 24.1 summarizes the simulation parameters used for both scenarios. Several experiments are executed out taking into account the density of the network. We consider four networks with densities of 100, 200 and 800 nodes. As the experimental times are identical for

Table 24.1 Simulation parameters

Parameter	Values
Number of nodes	100–800
Mac protocol	802.11
Number of rounds	500
Field size	150 m × 150 m
Data packet size	5000 bits
Control packet size (l)	300 bits
Electronics energy (Eelec)	50 nJ/bit
εfs	8 pJ/bit/m
εmp	0.0015 pj/bit/m4

each network, they are of the order of 10,000 s. The obtained results for each of the networks in terms of energy consumption are illustrated in the Table. 24.1.

24.4.1 Packet Delivery Ratio: PDR

We evaluate the performance of the four routing algorithms in relation to the increasing number of nodes by measuring their packet delivery rates. The packet delivery rate is given by the following Eq. (24.2):

$$\text{PDR} = \frac{\sum \text{Number of packets received}}{\sum \text{Number of packets sent}} * 100 \tag{24.2}$$

The rate of delivery decreases slightly when the number of nodes in the network also increases with the two activity rates (98% to 96.3%). There is also an increase in the number of collisions which cause the retransmission of the packets several times. Therefore, this reduces the packet delivery rate. Figure 24.2 shows that proposed algorithm provides the greatest number of packets per second, even the largest number of nodes deployed in both scenarios. LEACH provides the smallest number of packets because it is a conventional protocol and does not use any optimization algorithm.

24.4.2 Average Energy Consumption per Node

We evaluate the performance of the four routing algorithms as the number of nodes increases by measuring their energy consumption.

In Fig. 24.3, we find that the Average energy consumed by the four routing algorithms is increased with the increase in the number of nodes. This is, in fact, explained by the higher number of nodes which send different data and induce a

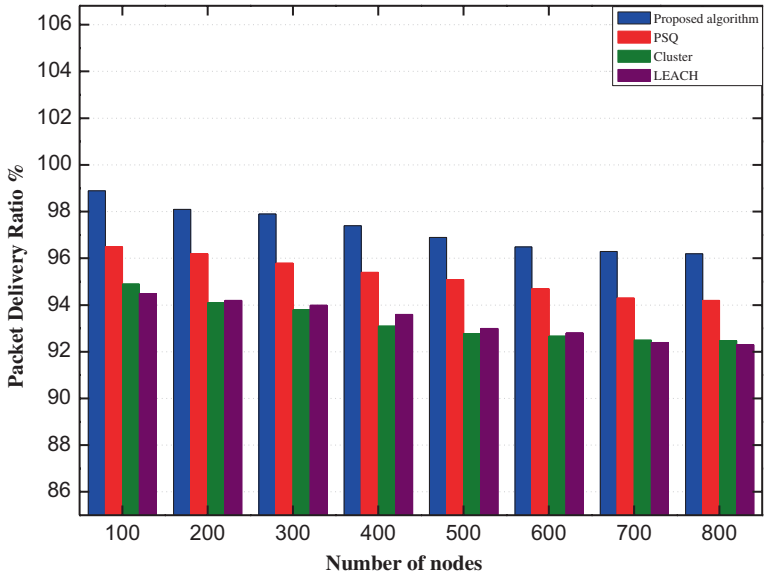


Fig. 24.2 Packet delivery ratio in WSN

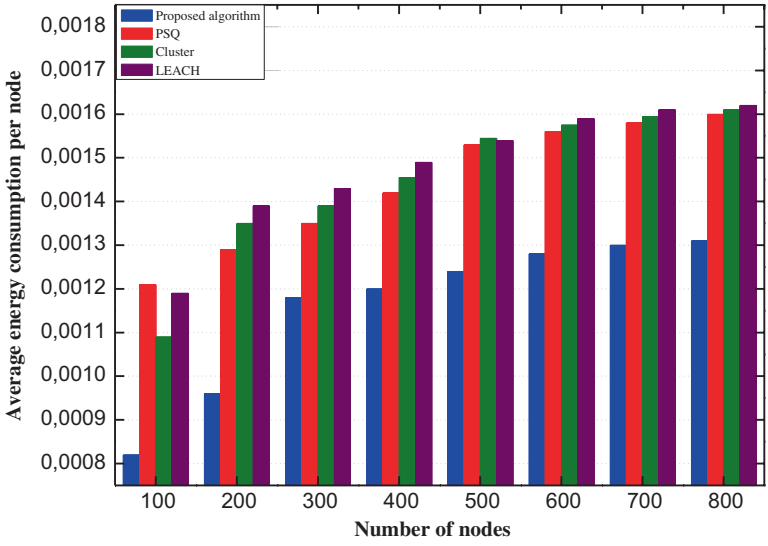


Fig. 24.3 Average energy consumption per node

multiplication of the transmitted data packets. Figure 24.3 shows that proposed algorithm consumes less average energy compared to the three algorithms. LEACH consumes more energy because all CHs are inevitably used as a relay node to transmit the data packets to the BS, thus consumes more power.

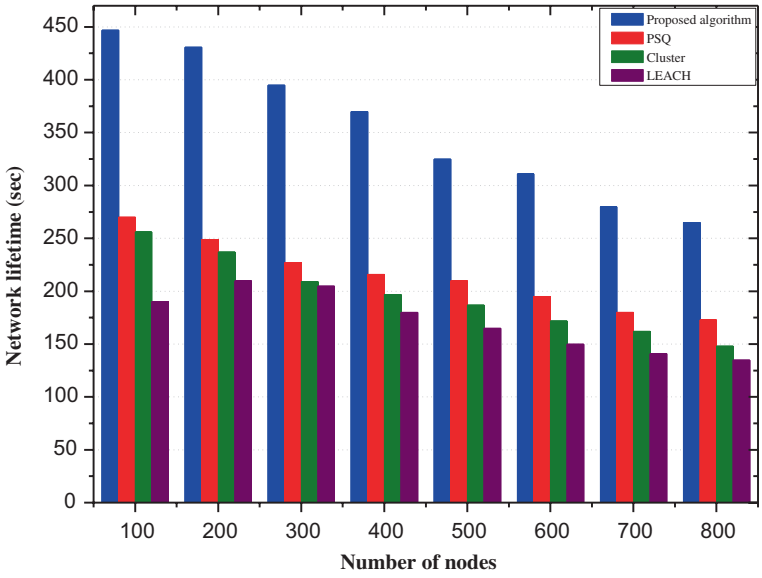


Fig. 24.4 Network lifetime in WSN

24.4.3 Network Lifetime

We evaluate the performance of four routing algorithms when the number of nodes increases by measuring their node lifetime. We consider a network of variable size from 100 to 800 nodes and each second collects data and sends it to the BS. Figure 24.4 shows the service life of the different routing scenarios.

Figure 24.4 shows that proposed algorithm extends the network lifetime from approximately 445 s to 270 s. When the number of nodes varies from 100 nodes to 800 nodes with respect to LEACH, which is the effect of the availability of excess node energy due to a lower calculation and optimal selection of CH proposed. LEACH has the smallest lifespan of the network among its peers due to the lack of a clear aggregate of data.

24.5 Conclusion

In this chapter, a new agricultural monitoring mechanism is proposed for wireless sensor networks. We propose a clustering-based routing algorithm that provides efficient coverage to the entire agricultural area. As a result, a proposed clustering protocol based on the combination of residual energy and distance between neighboring nodes, to obtain optimal Cluster-head and improve energy efficiency in the WSN. Sensor nodes deployed in the network collect the environmental parameters

continuously, but the detected data is transmitted to the base station (BS) only when the periodic value defined by the user or the value of the detected attributes exceeds Threshold.

The performance analysis of our proposal is carried out via the NS-3 network simulator. The simulation results show that proposed algorithm consumes less energy compared to other protocols and provides the greatest number of packets and extends the network lifetime in various WSN scenarios. In the future, we want to implement the network scenarios on a real sensor test bench.

References

Cheng-Jun, Z. (2014). Research and implementation of agricultural environment monitoring based on internet of things. In *2014 fifth international conference on intelligent systems design and engineering applications*. IEEE, pp. 748–752.

Fang, Q., Zhao, F., & Guibas, L. (2003). Lightweight sensing and communication protocols for target enumeration and aggregation. In *Proceedings of the 4th ACM international symposium on mobile ad hoc networking & computing*. ACM, pp. 165–176.

Garcia-Sanchez, A.-J., Garcia-Sanchez, F., & Garcia-Haro, J. (2011). Wireless sensor network deployment for integrating video-surveillance and data-monitoring in precision agriculture over distributed crops. *Computers and Electronics in Agriculture, 75*(2), 288–303.

Gubbi, J., Buyya, R., Marusic, S., et al. (2013). Internet of things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660.

Hao, Z., Zhang, Z., & Chao, H.-C. (2015). A cluster-based fuzzy fusion algorithm for event detection in heterogeneous wireless sensor networks. *Journal of Sensors, 2015*, 1.

Heinzelman, W. B., Chandrakasan, A. P., Balakrishnan, H., et al. (2002). An application-specific protocol architecture for wireless microsensor networks. *IEEE Transactions on Wireless Communications, 1*(4), 660–670.

Hwang, J., Shin, C., & Yoe, H. (2010). Study on an agricultural environment monitoring server system using wireless sensor networks. *Sensors, 10*(12), 11189–11211.

Jiang, J.-A., Wang, C.-H., Liao, M.-S., et al. (2016). A wireless sensor network-based monitoring system with dynamic convergecast tree algorithm for precision cultivation management in orchid greenhouses. *Precision Agriculture, 17*(6), 766–785.

Khedo, K. K., Perseedoss, R., Mungur, A., et al. (2010). A wireless sensor network air pollution monitoring system. *International Journal of Wireless & Mobile Networks, 2*(2), 31–45.

Khelifi, F., Kaddachi, M. L., Bouallegue, B., et al. (2014). Fuzzy logic-based hardware architecture for event detection in wireless sensor networks. In *2014 world symposium on computer applications & research (WSCAR)*. IEEE, pp. 1–4.

Khelifi, F., Bradai, A., Kaddachi, M. L., et al. (2017). A novel intelligent mechanism for monitoring in wireless sensor networks. In: *2017 IEEE international conference on consumer electronics (ICCE)*. IEEE, pp. 170–171.

Kuila, P., & Jana, P. K. (2014). Energy efficient clustering and routing algorithms for wireless sensor networks: Particle swarm optimization approach. *Engineering Applications of Artificial Intelligence, 33*, 127–140.

Liao, M.-S., Chen, S.-F., Chou, C.-Y., et al. (2017). On precisely relating the growth of phalaenopsis leaves to greenhouse environmental factors by using an IoT-based monitoring system. *Computers and Electronics in Agriculture, 136*, 125–139.

Manjunatha, P., Verma, A. K., & Srividya, A. (2008). Multi-sensor data fusion in cluster based wireless sensor networks using fuzzy logic method. In *2008 IEEE region 10 and the third international conference on industrial and information systems*. IEEE, pp. 1–6.

Maurya, S., & Jain, V. K. (2017). Energy-efficient network protocol for precision agriculture: Using threshold sensitive sensors for optimal performance. *IEEE Consumer Electronics Magazine, 6*(3), 42–51.

Nugroho, A. P., Okayasu, T., Hoshi, T., et al. (2016). Development of a remote environmental monitoring and control framework for tropical horticulture and verification of its validity under unstable network connection in rural area. *Computers and Electronics in Agriculture, 124*, 325–339.

Ojha, T., Misra, S., & Raghuwanshi, N. S. (2015). Wireless sensor networks for agriculture: The state-of-the-art in practice and future challenges. *Computers and Electronics in Agriculture, 118*, 66–84.

Sánchez, V., Gil, S., Flores, J. M., et al. (2015). Implementation of an electronic system to monitor the thermoregulatory capacity of honeybee colonies in hives with open-screened bottom boards. *Computers and Electronics in Agriculture, 119*, 209–216.

Tayeb, S., Latifi, S., & Kim, Y. (2017). A survey on IoT communication and computation frameworks: An industrial perspective. In *2017 IEEE 7th annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, pp. 1–6.

Chapter 25
Securing E-Health IoT Data on Cloud Systems Using Novel Extended Role Based Access Control Model

Mamoon Rashid, Shabir Ahmad Parah, Aabid Rashid Wani, and Sachin Kumar Gupta

Abstract As lot of data is getting generated and captured in Internet of Things (IoT) based devices related to Health Care Systems. This data is real time, unstructured in nature and its storage and processing in IoT applications is still a big challenge. Due to the popularity of cloud computing, many health care providers are storing these Electronic Health Records (EHR) in public cloud systems. However unauthorized access of this medical data is always a concern. Many access control models along with cryptographic techniques are used to prevent an unauthorized access of this medical data stored in public cloud systems. In this chapter, an Enhanced Role Based Access Control (ERBAC) is proposed for securing IoT medical data in Health Care Systems in terms of its storage on public cloud systems. The authors believe that proposed system will greatly help in efficient storage of IoT application medical data and provide secure storage of medical data in the cloud systems based on these role based access policies.

Keywords Internet of Things · Health · Access control

M. Rashid (✉)
School of Computer Science & Engineering, Lovely Professional University, Jalandhar, India

S. A. Parah
Department of Electronics and Instrumentation Technology, University of Kashmir, Srinagar, India

A. R. Wani · S. K. Gupta
Department of Electronics & Communication, Shri Mata Vaishno Devi University, Katra, Jammu, India

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_25

25.1 Introduction to Internet of Things

25.1.1 Internet of Things

The Internet of Things (IoT) is a computing paradigm which has changed the ways in our daily livelihood and functioning. IoT focuses on the interconnection of all the sensor based devices like smart meters, coffee machines, cell phones etc. enabling these devices to exchange data with each other during human interactions (Ray 2018). With easy connectivity among humans & devices, speed of data generation is getting multi-fold, increasing exponentially in volume and is getting more complex in nature. The message of IoT is the direct integration of computer based systems to that of physical world where the objects can be controlled remotely by using the existing network infrastructure. With the use of IoT technology, human intervention is minimized and this technology also leads to greater accuracy and efficiency as well.

IoT is connectedness of various physical devices through internet for the exchange of data. Various researchers have defined IoT formally in different perspectives. IoT is defined in research in terms of three A's- anywhere, anytime and any media resulting into the balance between man and radio in the ratio of one: one (Srivastava 2006). The measures to bring security in data storage on public clouds is discussed by providing the extended model of Role Based Access Control where the authenticated users can only access the data in terms of roles with assigned permissions and restricts the unknown users from accessing data by adding variable constraints (Rashid and Chawla 2013). IoT is defined as a global network infrastructure based on interoperating protocols where the virtual and physical things are having attributes and identities with capabilities that are self-configuring in nature (Van Kranenburg 2008). IoT have been defined as the novel paradigm in wireless communications where the things like mobile phones, sensors, RFID's, actuators are interacting with each other and its surroundings to achieve desired common goals (Atzori et al. 2010). The outline of IoT paradigm is shown in Fig. 25.1.

25.1.2 Key Fundamentals of Internet of Things

The basic fundamentals used in IoT are shown in Fig. 25.2.

Hardware The various hardware devices interconnected to sensors and actuators are important part of IoT which are responsible for the connectivity of physical world. These devices must have the storage capabilities for collecting the transmitted data from various sensors in terms of Integrated Circuits or Microcontrollers.

Embedded Programming Devices in IoT are embedded ones and need programs in terms of languages using C, C++ or Python. In addition to this, various communication protocols are required to establish the connections between sensors

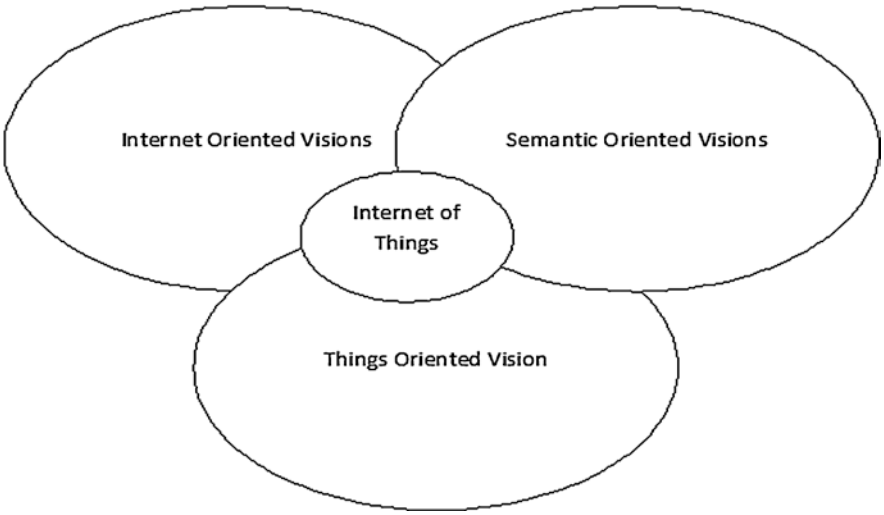


Fig. 25.1 Internet of Things paradigm

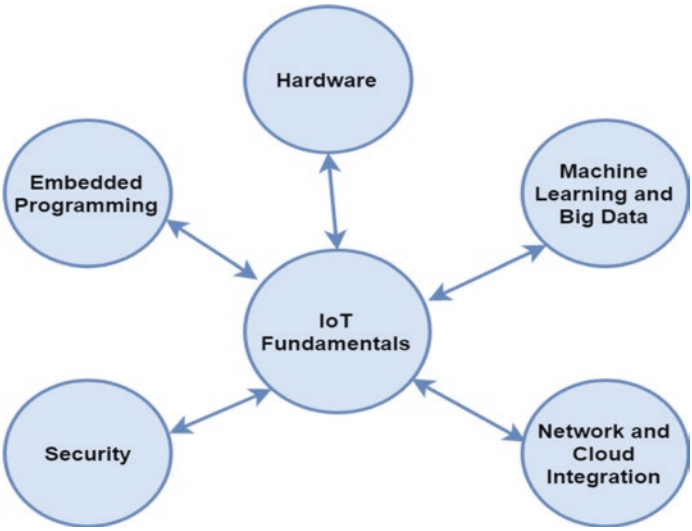


Fig. 25.2 Key fundamentals of IoT

and microcontroller. Use of Printed Circuit Boards (PCBs) and microcontroller platforms is required for prototyping IoT devices as well.

Security In IoT Systems, millions of devices are getting connected on daily basis which brings threats to the system due to the possibility of new attacks. So it is the quite important to have IoT system which will make it quite reliable and secure in terms of data integrity with encryption and challenges related to ethical hacking.

Machine Learning and Big Data: To bring the value for the huge amounts of data generated using IoT based system, Big Data pipelines are used for computing data at faster rates and Machine Learning techniques are required to compute this sensor data in real time environments for effective predictive analysis or identification in data patterns.

Networks and Cloud Integration As the number of devices connected in IoT system is large, design of good network along with its management is essential. Network connectivity helps various devices in IoT system to communicate with each other and use various cloud services. Cloud Integration with IoT system is done for data storage and real time data streaming of IoT based data.

25.1.3 Architecture of IoT

The IoT is defined as Internet of Everything which is dynamic network of machines capable of interacting with each other (Lee and Lee 2015). The essence of IoT is realized when communication is taking place in connecting devices and its integration with customer support systems, business analytics and business intelligence applications. The stage wise architecture of IoT is given by (Boyes et al. 2018). The various things are inputted to stage of architecture where the presence of sensors remain in wired or wireless manner. The Internet Gateways and Data Acquisition Systems are used in next stage for data aggregation and its control (Singh and Rashid 2015). The pre-processing and various analytics are performed in next stage for which services in terms Data Centre or cloud is to be used. The whole process is explained in IoT architecture given in Fig. 25.3.

25.1.4 Standards of IoT Applications

There is no clear line for classifying IoT Standards, however the major standard Protocols in use are based on IOT Data Link Protocols (Salman and Jain 2017). Physical layer and MAC layer protocols are mostly used by various IoT standards.

IEEE 802.15.4 This standard is used in MAC layer and specifies source and destination addresses, headers, format of frames, identification in communication between the nodes. Low cost communication and high reliability is enabled in IoT by the use channel hopping and synchronization in terms of time.

IEEE 802.11ah This kind of standard is used in traditional networking as Wi-Fi for IoT applications. This standard is used for friendly communication of power in sensors and supports lower overhead. This standard covers features of Synchronization Frame, Shorter MAC Frames and Efficient Bidirectional Packet Exchange.

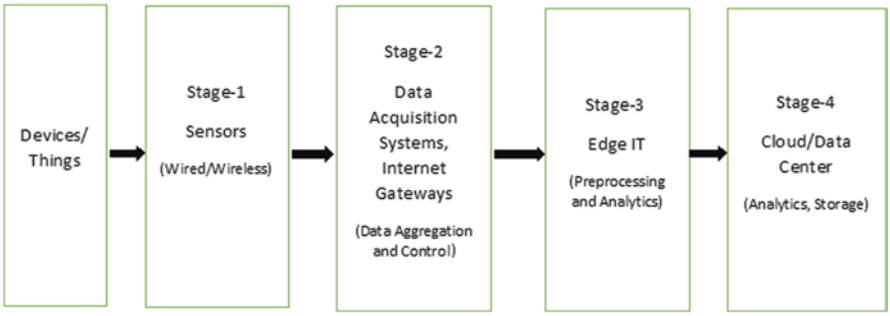


Fig. 25.3 Stage-wise architecture of IoT

WirelessHART This standard works on MAC layer and uses time division multiple access. This standard is more secure and reliable than other standards as it uses efficient algorithms for encryption purposes.

Z-Wave: This standard works on MAC layer and was designed specifically for automation of homes. This standard works on Master Slave Configuration where the master sends small messages to slaves and is used for point to point short distances.

ZigBee This standard is common one and is used for communication in Health Care Systems and Remote Controls. This standard is meant for medium level communications.

DASH7: This standard is used on MAC layer and is used in RFID devices. This standard supports master slave architecture and is very suitable for IoT applications and is designed for IPv6 addressing.

HomePlug This standard is MAC based and is used in smart grid applications. The beauty of this standard lies in its power saving mode where it allows nodes to sleep when not required and wakes them only whenever required.

25.2 Role of IoT in Health Care Systems

In the era of E-Health systems, the inclusion of IoT has brought a greater change in the health care paradigms by promising the availability and accessibility of data with quite easiness (Bhatt et al. 2017). Industry specialists like Gartner predicts the possibility of connecting 25 billion devices by year 2025 to IoT (Gartner 2014). It will include medical devices for measuring heart rates, blood sugar, heart rates, mood swings and body masses at various levels. All such data generated will be generated using efficient IoT systems which will be later processed with Big Data pipelines for meaningful insights (Manogaran et al. 2018).

At present, amount of data generated in Healthcare systems is growing exponentially due to the use of technologies like mHealth and biosensors. This includes the data coming from various software's, Electronic Health Records (EHR) and Electronic Patient Record Outcomes (ePRO). The role of Big Data in Healthcare systems is to process the amount of bigger data within small time intervals and thus to minimize computation time (Dey et al. 2018). Big data can predict diseases and thus avoid deaths which are preventable. The flow of processing in a big data pipeline is to take data from various kinds of sources like insurance and medical records and then to outline detailed picture of an individuals within less times (Dimitrov 2016).

Big Data together with IoT healthcare becomes quite valuable where the patients data will be received by cloud platforms as a part of IoT and then later processed with the help of Big Data processing tools (Rashid et al. 2019a). IoT systems with Big data pipelines provide platforms where applications are managed and then to run analytics, to store and secure medical data (Rashid and Chawla 2013). The role of IoT and Big Data in Healthcare systems is shown in Fig. 25.4.

25.3 Background

Security reference model related to Electronic Health Records (EHRs) and their integration with Healthcare Clouds is proposed. Core components for security EHR data on cloud is outlined in this research. The model proposed in this research covers security based on use-case scenario and addresses all measures related to security of data (Zhang and Liu 2010). Novel hybrid security model is implemented for securing text data in medical images. This research has worked on the integration proposed encryption scheme with that of 2-D Discrete Wavelet Transforms Level 1 or 2 technique of steganography. This research claims for better results in hiding data in medical images with acceptable imperceptibility (Elhoseny et al. 2018).

Novel authentication and access control model has been implemented for securing data on cloud systems. This research extended the authentication model of RBAC by imposing certain constraints on users in terms of permissions along with using encryption technique for securing data on public cloud system. Encryption keys which are used for converting data into cypher text before stored on cloud platform are stored locally and sent to users based on requirements when they need to access the data on cloud system (Rashid and Chawla 2013). Hybrid privacy model is proposed for preserving medical data in cloud systems. In this research, medical data has been partitioned vertically to achieve the objectives of data preservation. This research claims the effectiveness of this implemented model in terms of privacy in comparison to other models in state-of-art (Yang et al. 2015).

An attempt is made for securing sensitive data storage on cloud systems before its uploading. In this research, individual users are enforced for all privacy requirements before data which is sensitive in nature is uploaded on cloud system for its storage (Henze et al. 2016). Various kinds of research challenges and their

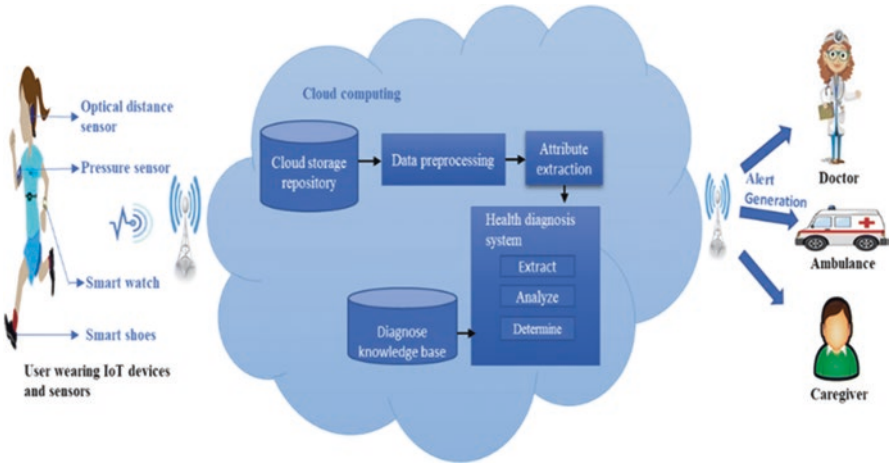


Fig. 25.4 Role of IoT and Big Data in Healthcare systems

solutions for providing security of IoT systems is discussed. The security issues in IoT systems are identified and possible solutions where the researchers in future will work are highlighted as well (Sicari et al. 2015). Various security issues which arise while working with cloud systems are discussed. Security vulnerabilities arising in cloud systems are identified and later possible solutions are presented as well (Ali et al. 2015).

Access control schemes in fog computing environment are identified for the security of data storage systems. Different requirements of access control for these schemes are also highlighted (Zhang et al. 2018). Secure IoT based healthcare system is proposed and then deployed on cloud system. This research used fog computing environment to run this framework. Edge devices are used for the storage of healthcare based data which is later transferred to the cloud system where from various healthcare professionals will make use of it.

This research makes use of asynchronous communication between data servers and applications related to healthcare on cloud platform (Thota et al. 2018). Linking of medical records related to patients on IoT systems in secure and preserved ways is addressed. This research identified and highlighted various security challenges in IoT data systems (Iyengar et al. 2018). The efficient storage of data in cloud systems is proposed in (Rashid et al. 2019b). The authors in this research have used techniques based on IP and geographic locations for the efficient access of stored data. For providing the security of data in cloud systems, efficient encryption technique has been proposed based on the Homographic Encryption Scheme (Kumar et al. 2018). This encryption technique ensured the confidentiality of data stored on cloud systems. Authentication model is discussed for securing data in IoT and Cloud based systems (Kumari et al. 2018). Issues of security are discussed in this research covering stolen verifier in terms of identity and password attack.

25.4 Access Control and Authorization Using Role Based Access Control (RBAC)

Security of data storage in cloud platforms is one of the most challenging issue. Authentication and Authorization are two key mechanisms which impart security in data storage systems. Authentication is the mechanism to get access of any data in system after proper validation of proof identities. Authentication is a way for matching of credentials in terms of username, password or some other kind of user validity. The accessibility of stored data is granted only if user identity is verified based on authentication factors. In present times, authentication is done at two or three levels to grant access for anyone inside the system. Authorization, on the other hand, are the permissions for using resources of system once the user is authenticated with proof identity.

Authorization basically provides the extent to which the intended user can access your system after proper authentication. Authorization usually comes for any system after proper authentication and provides user privileges for accessing system. In computer systems, Role Based Access Control (RBAC) is a model which provides limited access based on privileges for users after proper authentication. This model works on a mechanism which is revolving around roles and permissions which are applicable for users.

25.4.1 Rules for Defining RBAC

The basic rules which are used in RBAC model are shown in Fig. 25.5.

Assignment of Roles for Users: Role is a job function which is getting assigned to users and users can exercise permissions only after the assignment of roles.

Authorization of Roles: Users are authorized for active roles only which means that users will be able to access only assigned roles for which authorization is already done.

Authorization of Permissions: Users are authorized for permissions only for roles, which are active ones.

25.4.2 RBAC Reference Models

RBAC basically consists of four reference models as shown in Fig. 25.6.

RBAC0 This type of RBAC model is basic with basic requirements of security in terms of access control. Roles, Users and Permissions are defined in terms of this model based on assignments based on Role to Permission and User to Permission (Sandhu et al. 1996). RBAC0 is based on rules where any user can act as member of many roles and each role in turn can have many users. A user is having access to

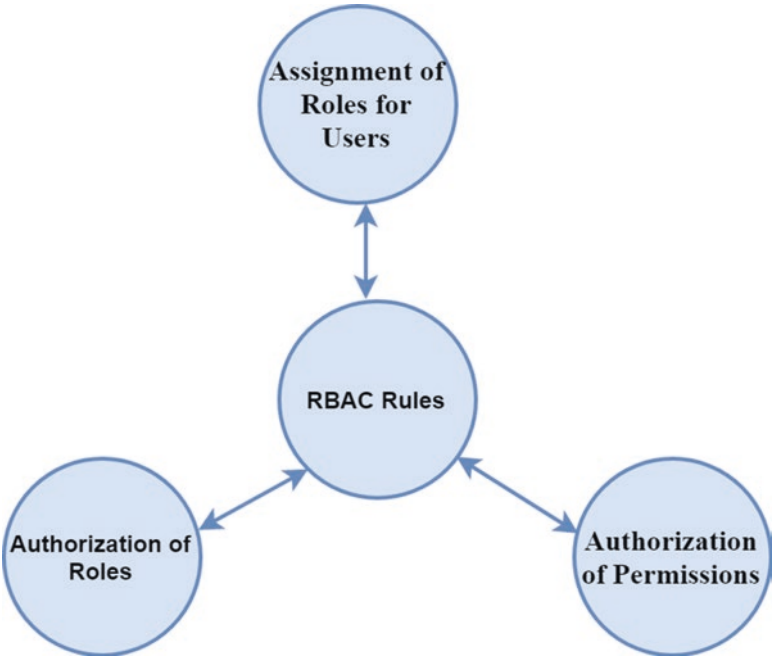


Fig. 25.5 Rules in RBAC model

invoke many sessions and each session is governed by single user. Many permissions can be assigned to single role and permissions can be assigned to multiple roles as well.

RBAC1 The addition of Role Hierarchy is done in RBAC1 with all the rules of RBAC0. This access control model has been introduced to increase efficiency of system at administration level. Role Hierarchy is quite helpful when one is assigning roles to senior and junior users in any organization. Role Hierarchy helps senior role to access all kinds of information which is related to junior role but junior role is not having power to do it on other side. Role hierarchies are important in systems where degree of authority and responsibility varies among users.

RBAC2 This access control model is also using all rules of RBAC0 with the addition of constraints for enhancing security of systems. This kind of model is used in systems where cardinality is of importance. In RBAC2, permissions are added for roles for bringing separation among such roles.

RBAC3 RBAC3 is often called as Unified model as it works on all rules of RBAC0, RBAC1 and RBAC2. RBAC3 supports addition of constraints and Role Hierarchies as well. This model is suitable for systems where sensitive interactions need to take place.

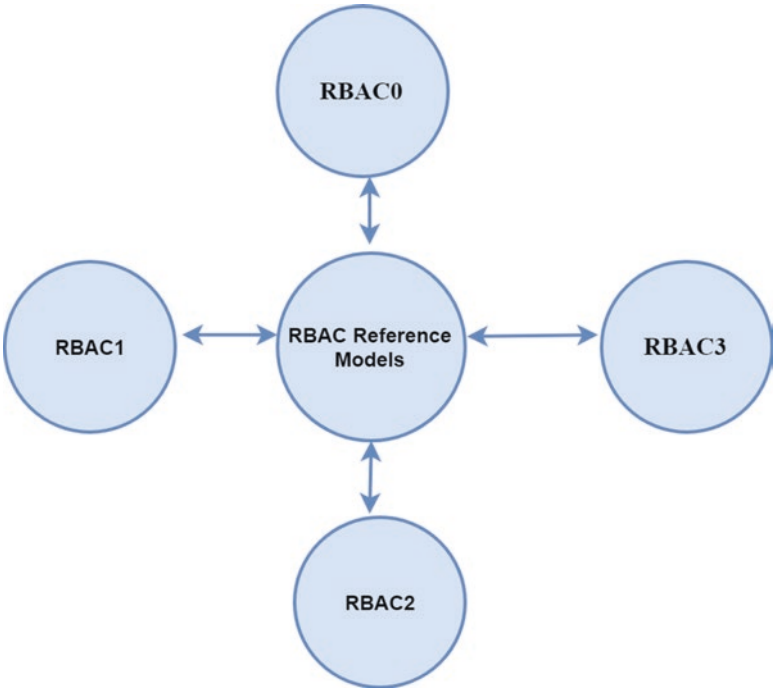


Fig. 25.6 RBAC reference models

25.5 Security Healthcare Model Based on Extended RBAC

25.5.1 Extended Role Based Model (ERBAC)

Although core reference models of RBAC prove to be better models in terms of authentication and access control, however there are few issues where these models turn to be ordinary. As RBAC reference models allow to create multiple users for a role, however there is no criteria for restricting number of users for a particular role. Also as permissions are assigned to roles, users under one role cannot get different accesses based on requirements. Also limits for accessing data are not applied anywhere which make any user. Keeping these loopholes under consideration, RBAC model need to be extend to fulfill all these requirements.

In Extended RBAC, the following steps are proposed to fulfill the limitation in base reference models.

1. Constraint in terms of limit of users for particular role is added.
2. Limit on data accessibility will be added for users based on active roles.
3. Membership Status is added on particular role.

In step 1, constraint is added for limiting users for particular roles. Only such users are added for role which are supposed to use data under such role. In step 2,

permissions are imposed on data storage for users so that sensitive based data will be accessed with limits and minimize the chances of data breaching for invalid users. In step 3, Membership status will be added for different user under one role so that data will be accessed based on positional hierarchy.

25.5.2 Proposed Security Model for Storage of Medical IoT Data Using ERBAC

Extended Role Based Access Control with steps mentioned in Sect. 25.5.1 is proposed and applied to IoT medical data for secure storage as shown in Fig. 25.7. The authors have implemented this access control model for securing storage of data on cloud systems. The model is implemented by using Model View Controller Framework (MVC) of Microsoft. For testing purpose, Cloud storage is used for storing IoT medical data on Microsoft Azure Platform. All details related to users supposed to use this application is stored on SQL database on Azure itself. Role and Permission information related to roles is also put in SQL database on Azure. IoT sensors with gateway are used for the storage of medical data on cloud system and stored in containers of storage account. The same data is encrypted to get converted into cypher text and then allowed to store on storage account of Microsoft Azure. The keys for encryption and decryption are kept on database to be stored locally.

In Fig. 25.7, administrator portal has been designed for healthcare organization for managing users and roles along with permissions. Administrator can sign in on with credentials to get redirected on main dashboard. On dashboard, administrator can create roles and impose permissions over roles for particular users. The organization is having provision to decide the user base for this model to access and can put constraints on users for accessibility of patient data records. Credentials for different hierarchy of users is created on dashboard as well. Model is based on two way authentication for user's i.e. if successful login will occur, the key for decoding data records on cloud platform will be emailed on registered mailbox. In case of authentic credentials, the single user will be given 3 attempts to validate credentials and on fourth attempt, the user in any hierarchy will not be allowed to sign in for next 24 h.

The dashboard showing the creation of roles is shown in Fig. 25.8. New Roles will get created on this page with required constraints. The user limit for one particular role is assigned on this page as well.

The dashboard showing the creation of users is shown in Fig. 25.9. New users will get created on this page for roles. The security aspect of users for accessing medical data in terms user hierarchy is assigned on this page.

The IoT Healthcare data using gateway is stored in blobs inside containers on Microsoft Azure and its page layout is shown in Fig. 25.10. Data Records are stored in the form of Blobs which are kept in containers of storage account. The capacity of storage is limited to 200TB on Microsoft Azure.

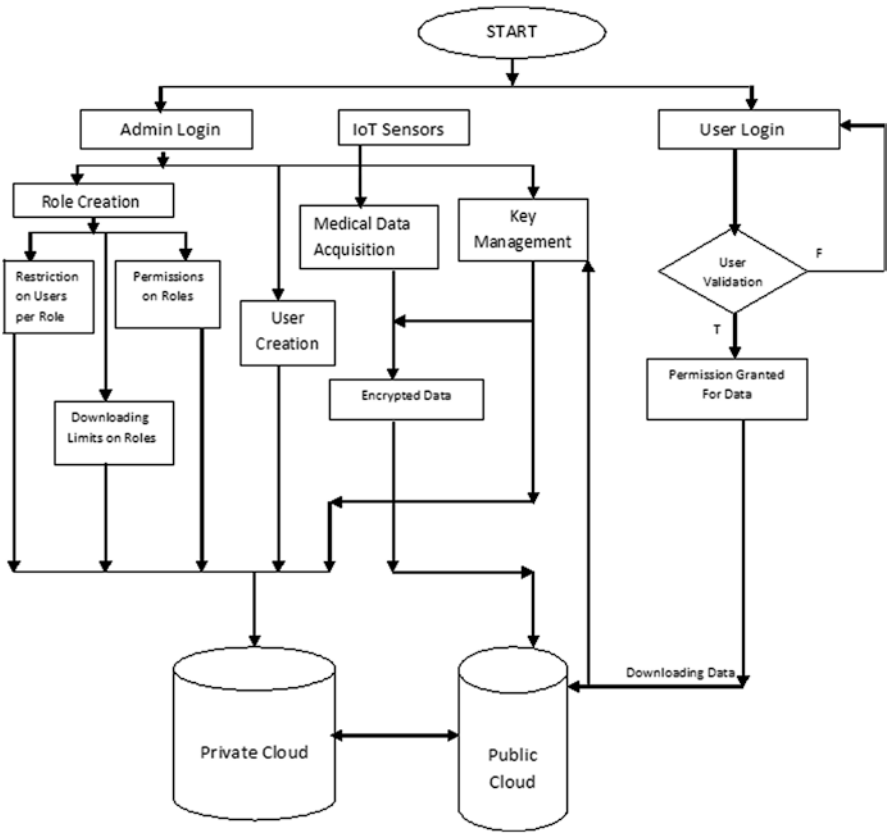


Fig. 25.7 Proposed extended RBAC for securing storage of medical data on cloud systems

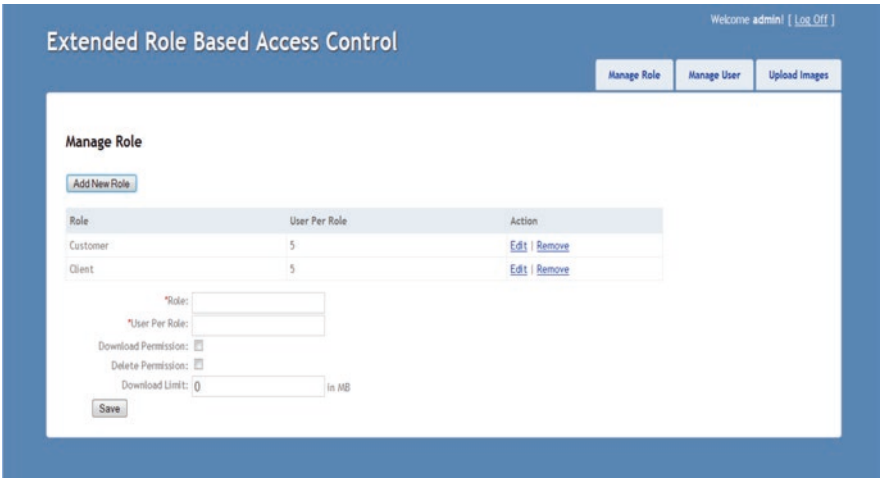


Fig. 25.8 Interface for role creation with user limts

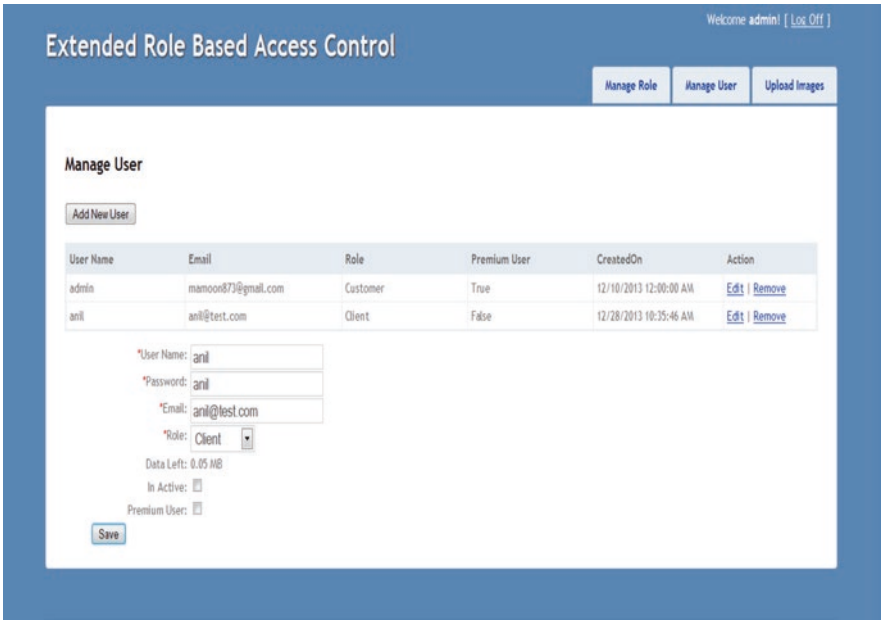


Fig. 25.9 Interface for user creation for roles

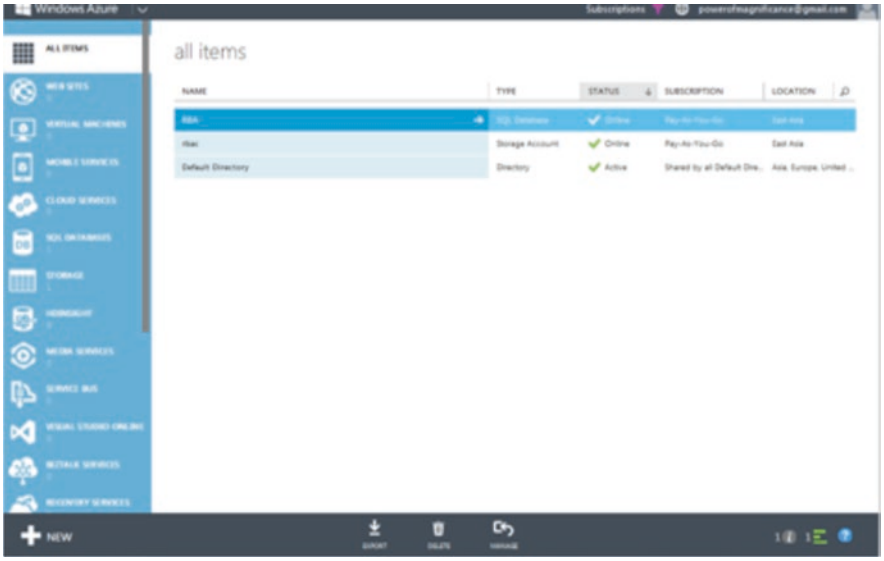


Fig. 25.10 Storage account on Microsoft Azure for storage of medical data

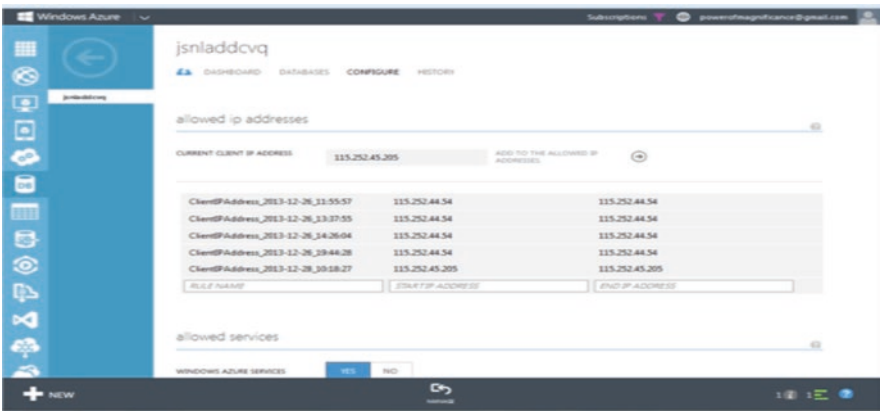


Fig. 25.11 Azure interface for adding IP address of client machines

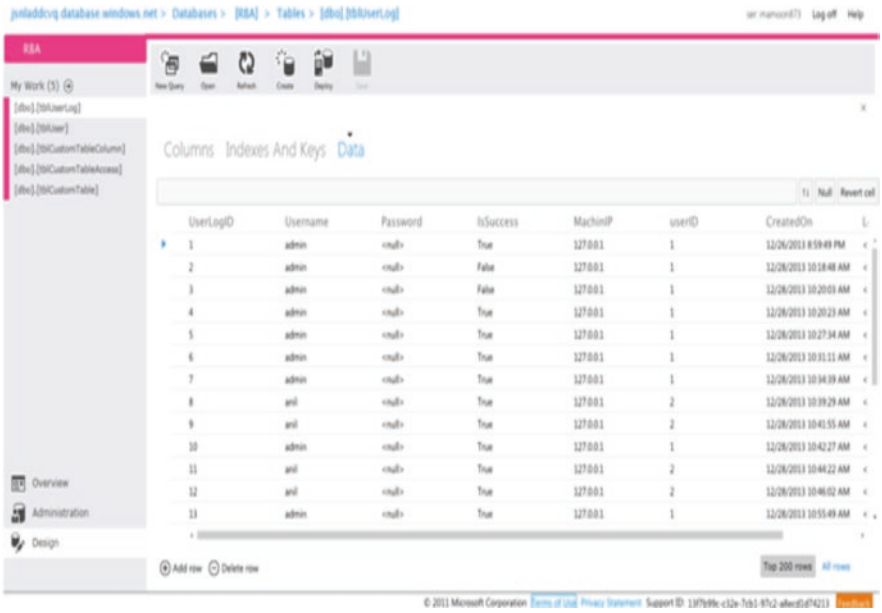


Fig. 25.12 Log table of users in Microsoft Azure for healthcare model

Addition of IP addresses of various client machines in Azure is shown in Fig. 25.11. It is only because of this client machine address, database on Microsoft Azure will get connected to MVC based application on client machine.

The various users which are added in this model in various hierarchies can use this system on need basis. The log details of various users for health care system is shown in terms of SQL database of Microsoft Azure in Fig. 25.12.

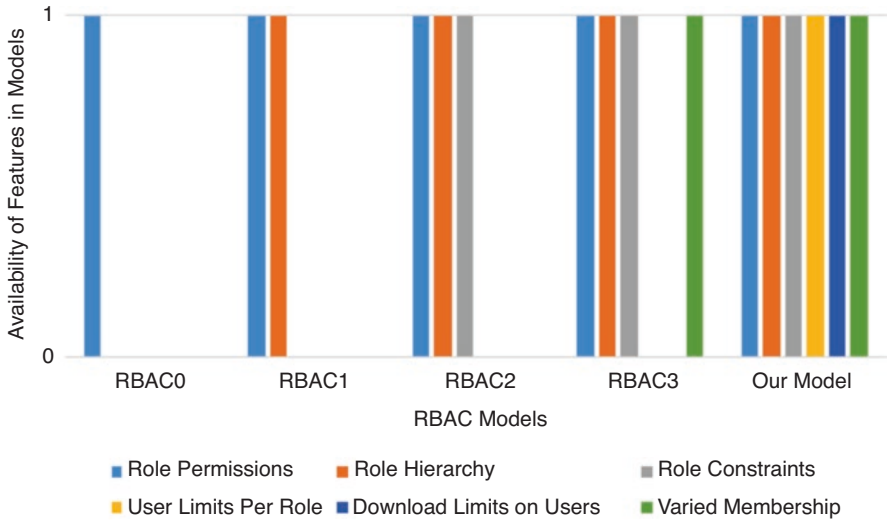


Fig. 25.13 Comparison of proposed model with state-of-art

The results achieved for authenticating and providing access in healthcare data storage with the help of proposed extended role based control model proved better and comparison with state-of-art is shown in Fig. 25.13. Clearly this extended new model shows more presence of constraints and features in terms of Permissions assigned to roles, Role Hierarchy, Constraints imposed on roles, limits applied on users per role, data downloading limits on users and nature of varying data accesses of users based on their membership in comparison to existing models. The scale of 0 and 1 in Fig. 25.13 shows the absence or presence of features in different models.

25.6 Conclusion

In this chapter, new extended Role Based Access Control model is proposed for addressing the various security features in Healthcare applications. This model guarantees security of medical data stored on cloud systems by providing necessary constraints on roles and users. This model added a feature in RBAC where a single role with multiple users will be able to access the stored records on need basis. Two way authentications has been used in this model along with cryptographic technique for securing data on cloud system. Although an attempt in this work might not be an exhaustive but it is believed that this proposed model will definitely add new dimension in RBAC models for securing data by providing better authentication and access control.

References

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences, 305*, 357–383.

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787–2805.

Bhatt, C., Dey, N., & Ashour, A. S. (Eds.). (2017). *Internet of Things and big data technologies for next generation healthcare*. Cham: Springer.

Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial Internet of Things (IIoT): An analysis framework. *Computers in Industry, 101*, 1–12.

Dey, N., Hassanien, A. E., Bhatt, C., Ashour, A. S., & Satapathy, S. C. (Eds.). (2018). *Internet of Things and big data analytics toward next-generation intelligence*. Berlin: Springer.

Dimitrov, D. V. (2016). Medical Internet of Things and Big Data in healthcare. *Healthcare Informatics Research, 22*(3), 156–163.

Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O. M., Shawkat, S. A., Arunkumar, N., & Farouk, A. (2018). Secure medical data transmission model for IoT-based healthcare systems. *IEEE Access, 6*, 20596–20608.

Gartner. (2014, March 19). *Gartner says the Internet of Things will transform the data center*. Retrieved from http://www.gartner.com/newsroom/id/2684616

Henze, M., Hermerschmidt, L., Kerpen, D., Häußling, R., Rumpe, B., & Wehrle, K. (2016). A comprehensive approach to privacy in the cloud-based Internet of Things. *Future Generation Computer Systems, 56*, 701–718.

Iyengar, A., Kundu, A., & Pallis, G. (2018). Healthcare informatics and privacy. *IEEE Internet Computing, 22*(2), 29–31.

Kumar, V., Kumar, R., Pandey, S. K., & Alam, M. (2018). Fully homomorphic encryption scheme with probabilistic encryption based on Euler's theorem and application in cloud computing. In *Big Data Analytics* (pp. 605–611). Singapore: Springer.

Kumari, A., Kumar, V., YahyaAbbasi, M., & Alam, M. (2018, October). The cryptanalysis of a secure authentication scheme based on elliptic curve cryptography for IOT and cloud servers. In *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)* (pp. 321–325). Piscataway: IEEE.

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons, 58*(4), 431–440.

Manogaran, G., Varatharajan, R., Lopez, D., Kumar, P. M., Sundarasekar, R., & Thota, C. (2018). A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system. *Future Generation Computer Systems, 82*, 375–387.

Rashid, M., & Chawla, E. R. (2013). Securing data storage by extending role-based access control. *International Journal of Cloud Applications and Computing (IJCAC), 3*(4), 28–37.

Rashid, M., Goyal, V., Parah, S. A., & Singh, H. (2019a). Drug prediction in healthcare using big data and machine learning. In *Hidden link prediction in stochastic social networks* (pp. 79–92). Hershey: IGI Global.

Rashid, M., Singh, H., & Goyal, V. (2019b). Cloud storage privacy in health care systems based on IP and geo-location validation using K-mean clustering technique. *International Journal of E-Health and Medical Communications (IJEHMC), 10*(4), 54–65.

Ray, P. P. (2018). A survey on Internet of Things architectures. *Journal of King Saud University-Computer and Information Sciences, 30*(3), 291–319.

Salman, T., & Jain, R. (2017). A survey of protocols and standards for Internet of Things. *Advanced Computing and Communications, 1*(1).

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *Computer, 29*(2), 38–47.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks, 76*, 146–164.

Singh, P., & Rashid, E. (2015). Smart home automation deployment on third party cloud using Internet of Things. *Journal of Bioinformatics and Intelligent Control, 4*(1), 31–34.

Srivastava, L. (2006, March). *Pervasive, ambient, ubiquitous: The magic of radio*. In European Commission Conference. From RFID to the Internet of Things, Bruxelles, Belgium.

Thota, C., Sundarasekar, R., Manogaran, G., Varatharajan, R., & Priyan, M. K. (2018). Centralized fog computing security platform for IoT and cloud in healthcare system. In *Fog computing: Breakthroughs in research and practice* (pp. 365–378). Hershey: IGI Global.

Van Kranenburg, R. (2008). *The Internet of Things: A critique of ambient technology and the all-seeing network of RFID*. Amsterdam: Institute of Network Cultures.

Yang, J. J., Li, J. Q., & Niu, Y. (2015). A hybrid solution for privacy preserving medical data sharing in the cloud environment. *Future Generation Computer Systems, 43*, 74–86.

Zhang, R., & Liu, L. (2010, July). Security models and requirements for healthcare application clouds. In *2010 IEEE 3rd international conference on cloud computing* (pp. 268–275). Piscataway: IEEE.

Zhang, P., Liu, J. K., Yu, F. R., Sookhak, M., Au, M. H., & Luo, X. (2018). A survey on access control in fog computing. *IEEE Communications Magazine, 56*(2), 144–149.

Chapter 26
An Efficient Approach towards Enhancing the Performance of m-Health Using Sensor Networks and Cloud Technologies

Kamta Nath Mishra

Abstract Mobile health technology has great prospective to increase healthcare quality, expand access to services, reduce costs, and improve personal wellness and public health. The online m-health monitoring and control is one of most the promising areas for mobile computing technologies. The online health management and control by using medical sensors, environmental sensors, clouds, Internet of Things (IoT), and fuzzy logic based approaches for establishing unbreakable and endless communication between medical professionals and patients is the need of current hospitals. Wireless Medical Sensor Networks and Radio Frequency Identification have been widely adopted in both the medical and healthcare industry. However, mobile health monitoring systems also raise significant privacy and security challenges. The early day's experimentation outcomes have recommended a strong potential for using wireless sensor networks (WSNs) to which can efficiently use low-cost medical sensors and environmental sensors for improving the quality of online patient diagnosis and health monitoring in the hospitals. It is tremendously desirable to merge ubiquitous computing with m-health system and use wireless medical sensors & smart phones to observe the wellness of chronic patients continuously. Here, the monitoring of patients can be either with the consent of patients or with the consent patient's family members. The patients can be monitored and their activities can be tracked using wearable or non-wearable sensors. The most modern advancements in WSN technologies have created a new pitch of Wireless Body Area Networks (WBAN) whose integration with m-health system is creating a new dimension of patient friendly online health monitoring, advice and control system. Since, the physiological data obtained from medical sensors of a patient are very receptive. Therefore, maintaining the confidentiality of patient' data is a highly responsible task. Hence, the security is an essential research concern of m-health applications especially for the cases where patients have upsetting diseases. The healthcare services have been further expanded to become mobile healthcare service with the help of global mobile communication systems and broad radio

K. N. Mishra (✉)
Department of Computer Science & Engineering, Birla Institute of Technology, Ranchi, Jharkhand, India

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_26

frequency services. In this research work, the author has tried to raise and discuss the issues related to mobile health systems and try to find suitable solutions for these problems using sensors, clouds, Internet of Things (IoT) and soft computing technologies. In the proposed m-health system a central cloud server enabled with IoT and fuzzy sets based technologies is being used to read medical sensors data of patients. This obtained data will further be transmitted to mobile applications for sending alert SMS (Short Message Service) on a regular interval in case of emergency situations.

Keywords Message alerts · Performance enhancement · Mobile health monitoring system · Remote health management system · Wireless biomedical sensor network · Wireless body area network

26.1 Introduction

The Internet of Things (IoT) is an active system of inter-communicative computing devices, digital and mechanical machines which are classified with the help of unique identifiers and interconnects different object/things with the Internet technology. The IoT performs interchange of information/data and can track or manage the real-life related objects (Five Reasons Healthcare Data Is Unique and Di cult to Measure 2017; Abbas and Khan 2014). The integration of IoT with information technology offers solutions for different day-to-day related problems and it can store, transmit, retrieve, & manipulate global data without the help of human-to-human or human-to-computer interfaces. Therefore, the IoT can be redefined as a dynamic and globally networked universally available infrastructure based on standard and interoperable communication protocols which have self-configuring capabilities (Acampora et al. 2013; Aceto et al. 2012).

The IoT integrates physical and virtual things of this earth. Therefore, the realization physical and virtual things are easily possible by integrating IoT with several new and forthcoming sensing and communication technologies of mobile health systems. The radio frequency identification technology (RFID) tags can communicate with IoT and it can further be characterized by a unique identifier for the purpose monitoring objects in a real-time system. Hence, it is sure that the RFID technology can be efficiently used in advanced healthcare systems (Aceto et al. 2016; Ahuja et al. 2012). The wireless sensor networks are integrated with IoT for further improving the easiness and accessibility of healthcare communication systems. Therefore, it is very clear and true that IoT can be applied to identify sensors and it can further improve the efficiency of healthcare systems. Therefore, in this research work, the author has adopted IoT based sensing technologies to collect data for a smart healthcare system (Al Yami et al. 2016; Alaba et al. 2017; Alemdar and Ersoy 2010).

The internet of things (IoT) has a wide scope in improving the smartness of healthcare systems. Here, service-oriented architecture (SOA) is being used as the middleware which is interposed between the technology and application layers. In middleware architecture, the IoT can be used to develop any particular application. Although, many researchers and scientists have developed a middleware in the sphere of IoT, unfortunately, no broad middleware is available which can be used across all possible smart devices of healthcare systems (Allen 2016; Alpay et al. 2004).

The cloud computing system is an extended business model of computing and communicating resources which provide scalability and economic benefits to its end users over the internet. It acts as a software product and provides data storage, data access facilities where knowledge of end users physical location configuration of the system are not required. In cloud computing systems, the end users make use of the web browsers as an interface, whereas the data software products are stored on far-flung servers. Therefore, it is considered as device independent system (Amazon Lex n.d.; Andriopoulou et al. 2017). In the last few years, many healthcare organizations have started deploying wireless senor networks for monitoring patients of remote locations. Further, many insurance companies and healthcare organizations have started deploying electronic medical record system (ERMS) by using which the medical records can be updated and maintained in the form of electronic records in a centralized database system using cloud computing environment (Angiuoli et al. 2011; Archenaa and Anita 2015).

This research paper presents a model where the medical health status of a patient is obtained and healthcare promoting messages are delivered from time to time the persons in a smooth way through a wireless network system (WNS). Here, the WNS can help in communicating with medical services (Armbrust et al. 2010). The application software products are installed on the clouds for updating electronic records for medical data. The most generalized scope of our proposed work is to develop an architecture which can integrate the healthcare clouds with wireless sensor network based technologies via smart devices including fourth or fifth generation mobile phones. The healthcare applications installed on smart devices including smart mobile phones will supervise patients' health in a wireless environment and will provide real-time updates of patients health condition on a regular interval to the doctors & other medical staff members by using the cloud (Atzori et al. 2010; Elfouly 2017).

The Fig. 26.1 describes a paradigm of a healthcare system in an ideal condition. The main high level technologies used for managing ideal healthcare system are sensor networks based technologies and information processing technologies. Here, the information processing technologies include digitized imaging processing, electronic health recording systems, and diagnostic systems (Farheen Pathan and Jadhav n.d.). Most recently researches in the field of IoT have offered more possibilities of mobile healthcare systems than the researchers of medical sciences where it is possible to improve the quality of healthcare systems with the help of cloud computing technologies and other wireless computing systems (Bahga and Madisetti 2013; Balter et al. 2017).

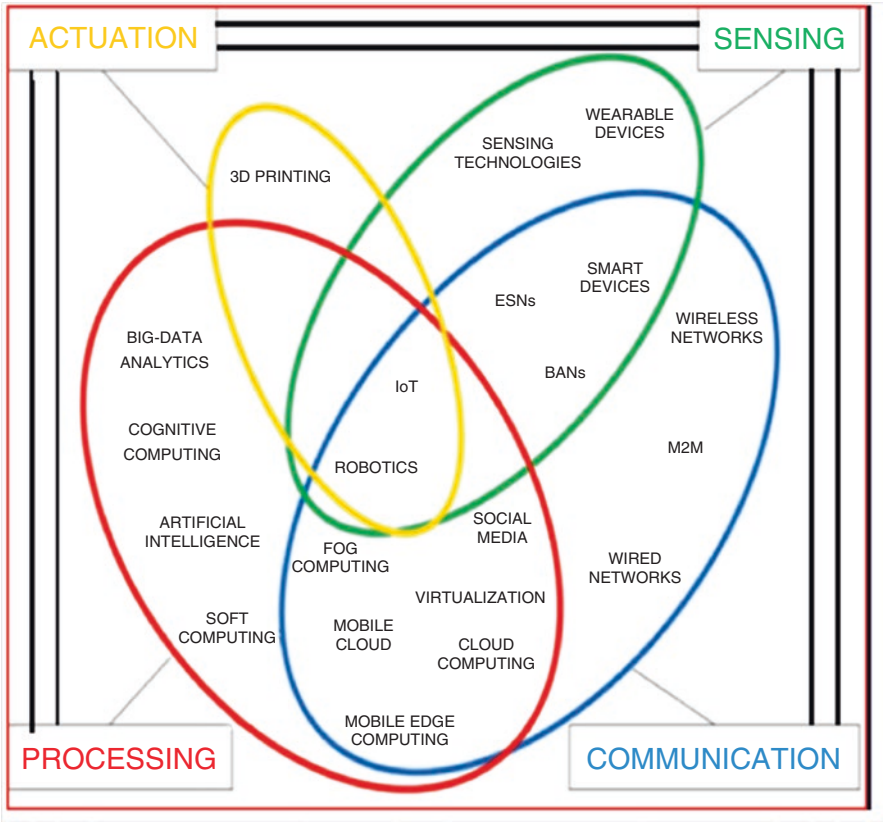


Fig. 26.1 The Paradigms of ideal healthcare system in cloud computing and sensor network's environment

Few researchers have developed IoT sensor devices which can be integrated with the healthcare systems for bringing patients data in clouds whereas some researchers have expanded and linked the thought of IoT with the several potential components of the healthcare system. Here, the IoT provides day-to-day care and monitoring of remotely located patients and sends a meaningful data stream continuously for making better decisions which can be flawlessly accepted in favor of patients. In the recent researches, the micro wireless physiological sensors are combined with smart mobile technologies and other smart devices because of which it is possible to monitor patients continuously in a 24×7 domain (Bamiah et al. 2012; Bardram and Christensen 2001; Barua et al. 2011).

Many elderly people are suffering from chronic and degenerative diseases. These respected people of our society also need better healthcare services. The cardio vascular disorders, high/low blood pressure and high/low sugar levels are some of the examples of chronic and degenerative diseases which border elderly people from executing their day-to-day outdoor deeds. Hence, the accessibility of enhanced

emergency healthcare services for remote patients is the real-time technological challenge which can permit people to survive in a safe and independent way (Bazzani et al. 2012).

Health monitoring is one of the important methods to advance emergency healthcare services. It enables the early detection of mass killing diseases and the timely medical care under urgencies results into the reduction of long-term distress and medicinal costs. The implementation of sensors for monitoring and transmitting the patient's data is very much helpful for risk identification of patients. The medical personnel can decide the actions to be taken to safeguard the patient's health using the sensor based information monitoring system (Beam and Kohane 2016; Benharref and Serhani 2014).

The deliverance of appropriate medical care could create a significant difference between life and death casualties. The Advancements in mobile health services integrate different platforms which are based on wireless body sensor networks (WBSN) that is a central aid for remote coverage of data to a hospital under the medical emergencies (Bernhard et al. 2016). The WBSN will collect data from installed biomedical sensors and cameras with the help of user-friendly graphical user interfaces. The WBSN will transmit physical signals, images, and videos. The Emergency Remote Pre-Hospital Assistance platform will enable medical observations in real time system from hospitals to accident locations (Biswas et al. 2010; Blobel and Holena 1997).

An effective and readily accessible modern healthcare system is a prerequisite for keeping individuals healthy. An efficient healthcare system must provide improved healthcare services to the people round the clock and from everywhere in a cost-effective and patient welcoming manner. Currently, the healthcare system is passing through a paradigm and cultural shift from a conventional approach to a modern approach which is patient centered (Chen et al. 2016; Darshan and Anandakumar 2015). In the traditional healthcare approach, the whole system is dependent on healthcare professionals' abilities and attitude. These professionals need to visit the patients every time for necessary medical diagnosis and further advise. But, this approach suffers from two basic problems which include the 24×7 presence of healthcare professionals in the hospital and hospitalization of patients for a specific period of time. In order to solve these two problems of traditional approach a new method called patient-oriented approach has come into existence (Datta et al. 2015; Duarte et al. 2015).

In the patient-oriented approach the patients have enough knowledge and information to play an active role in disease prevention and diagnosis. The requirement of a real-time notification and recording of vital signs of a patient is of leading importance for developing and managing patient-oriented approach efficiently (Fang et al. 2016). A modern patient management system (PMS) should obtain, record, display, and broadcast the physiological data from the patient body to a remote place at any time by encapsulating the advantages of modern bio-instrumentation, telecommunication, and computational technologies. The PMS must be able to incorporate with an alarm system for an efficient, opportune, and emergency medical care (Aceto et al. 2018; Ermakova et al. 2013).

The PMS should not only observe and analyze the severely ill patient's data but it should also be able to send alarming messages in the cases where the observed data go exterior to the normal range. Therefore, a dynamic database system must be linked with the PMS for executing these alarms. Most of the projected PMS is based centralized allocation of all data on a single server. But, by using necessary cloud computing and IoT based technologies the data of patients can store at different locations and could ease the transmission, update and monitoring of patients data via an open communication network of TCP/IP protocol (Pino and Di Salvo 2013; Calabrese and Cannataro 2015). Hence, a patient can be easily and efficiently monitored from distant locations. The existing widespread mobile phone networks can play a vital role in this regard.

The gigantic acceptance of advanced information and communication technologies is considerably changing the m-health sector parameters and originating new opportunities & introducing new domains of applications. The co-ordination and cooperation among medical health practitioners are improving rapidly because of ICTs. And the healthcare professionals are sharing their knowledge about the patients with other colleagues which is finally helping the existing and forthcoming patients of the hospitals (Abbas and Khan 2014; Laplante and Laplante 2015).

In general, it can be said that the acceptance of the most recent technologies will help governments to present value-added services to citizens of our country and opens a number of multidimensional opportunities. Therefore, the chronic and panic creating diseases can now be better faced because of advancements in m-health technologies. Hence, the resulting health systems facilitate the citizens to have better control over their own wellness, by using personalized and competent health monitoring and control system from their houses.

26.2 Literature Review

In the technical narratives, a huge number of surveys can be seen which are dealing with the acceptance of the identified information and communication technology pillars in the domain of healthcare. The existence of these studies is an indication of interest which the scientific community is having in the topics of mobile healthcare monitoring and control system. This paradigm shift requires the unified adoption of all the pillars of ICT based healthcare systems. Therefore, unfair views of ICTs applications to the domain of mobile healthcare systems fall diminutive of providing the required holistic knowledge. This approach has motivated us to using sensor networks and cloud computing for enhancing the performance of mobile healthcare systems.

In this part of the chapter, the author has reported the relevant surveys of m-health applications according to ICT pillars, cloud computing, and IoT. The exhaustive use of cloud technologies in the m-health domain has been surveyed in numerous research works. Ermakova et al. (2013) aimed at identify the status of research work associated with the inclusion of cloud computing in the mobile healthcare systems.

The researchers Pino and Di Salvo (2013) proposed a literature review regarding the existing models of cloud-based healthcare systems. The authors Calabrese and Cannataro (2015) reviewed the foremost cloud-based m-healthcare and biomedicine applications. Abbas and Khan (2014) intended to cover the state-of-art privacy-preserving techniques used in the electronic and mobile health cloud systems. Several literature reviews discussed the implementation of IoT in m-health systems. The researchers Laplante and Laplante (2015) described a structured and controlled approach for unfolding IoT for m-health systems. The authors Islam et al. (2015) reviewed the advances in IoT-based health monitoring and control technologies which include current trends in implementing and developing IoT-based healthcare solutions. Yeole and Kalbande (2016) illustrated various applications which and IoT can enable in the area of mobile healthcare systems.

The researchers Darshan and Anandakumar (2015) addressed the employment of IoT in healthcare systems and discussed its challenges. Wu et al. (2011) presented a new idea of machine-to-machine (MTM) concept and analyzed the forthcoming directions and network architecture evolutions which can make possible the mass deployment of MTM services in the field wireless communications based healthcare systems. The different uses of wireless communication systems provide us with information about how wireless sensor networks have become boon for healthcare systems in the last few years. Alemdar and Ersoy (2010) described numerous state-of-art examples about the acceptance of wireless sensor networks in healthcare for improving security, scalability and energy efficiency. The authors Chen et al. (2011) and Latrâe et al. (2011) outlined the perception of Wireless Body Area Networks (WBAN) and described types of WBAN communication systems. The authors Cao et al. (2009) reviewed and analyzed pioneer WBAN research projects. Filipe et al. (2015) compared the existing technologies and network protocols available in the most modern researches. They also described the WBAN issues of medical monitoring systems.

26.3 The Pillars and Paradigms of Mobile Health Systems

The core ICTs building blocks and paradigms which can hold the mobile healthcare domain were described by scientists and researchers in their research papers. The ICTs pillars which the author has taken into considerations are presented in Fig. 26.2. In this figure, the author has divided the overall information and communication systems into four components which are actuation, communication, processing, and sensing. The Fig. 26.2 provides a functional guidance to develop and use mobile healthcare systems efficiently. The ICT pillars and paradigms described in the order of communication, processing, sensing, and actuation (Taylor and Stoianovici 2003; Taylor 2006; Haux et al. 2008; Ko et al. 2010).

The union of communication systems and Network Technologies describes an important part of m-health care system. The communication system encompasses different phases and forms of interactions between patients and medical professionals

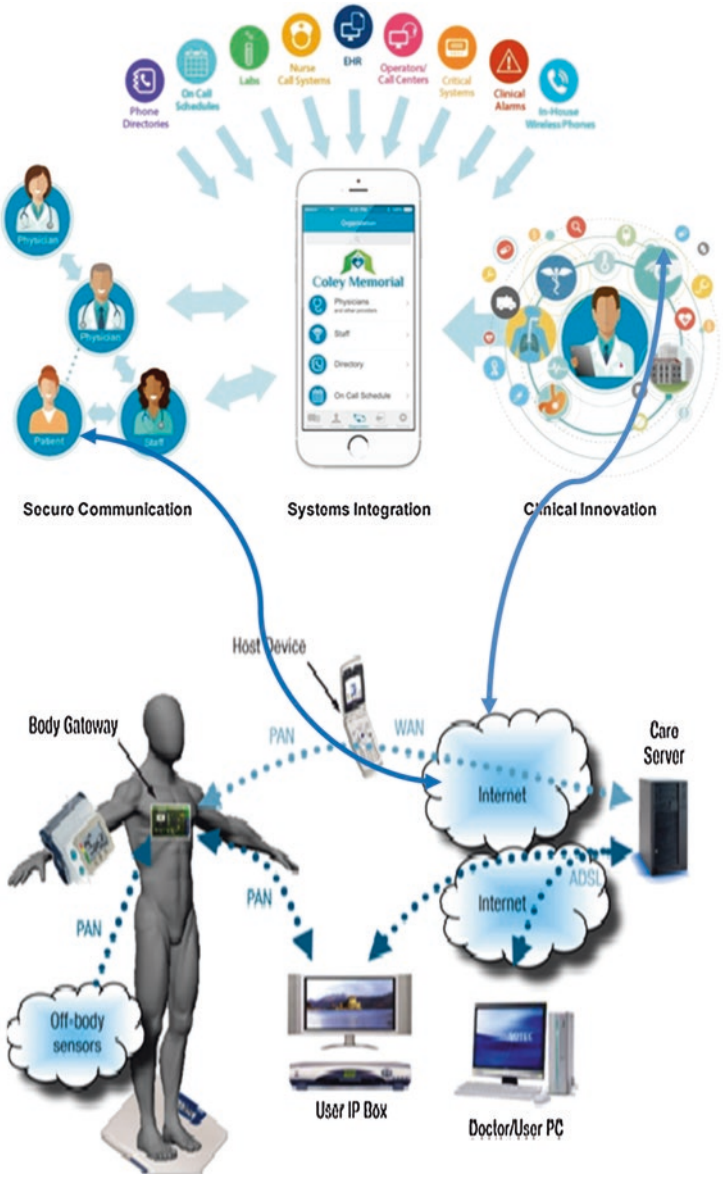


Fig. 26.2 Representing the main pillars of mobile healthcare systems

in a mobile healthcare system. The ICT in the healthcare domain offers a practical means to increase user-friendliness, sharing, and exchanging information for overall quality enhancement of mobile healthcare services (Yoo et al. 2012; Griffiths et al. 2012; Pino and Di Salvo 2013; Sun and Reddy 2013; Zou et al. 2013).

With swift changes in mobile healthcare systems and technology, the online m-health information systems are becoming the center of our concerns. The huge and easily accessible internet infrastructure is definitely the component with the utmost potential to further improve the broadcasting of secured information and to transform the way m-healthcare facilities. The extensive accessibility of medical and technical information in the world of internet is having a deep impact on the connection between medical professionals and patients. The large numbers of patients are efficiently using the internet for getting medical advice. Therefore, the available mobile health systems can be integrated with IoT for getting numerous benefits (Malik et al. 2015; Archenaa and Anita 2015; BurgerKahrs et al. 2015; Ramesh et al. 2016; Kassahun et al. 2016).

The augmentation and integration of wireless communications with healthcare systems using local and wide Wi-Fi networks will be considered as a golden step for patients and medical professionals of mobile healthcare systems. In actual sense, the Wi-Fi networks are the main source for researchers to think about implementing mobile health concept. This approach also fulfills the dream of the omnipresent nature of the healthcare system by removing time and location constraints. The interconnection of mobile devices with the internet of things and broadband networks permits the patients of remote geographical locations to access m-health systems for getting advice without visiting the hospital physically. Thus, the healthcare services can be expanded to rural and underserved areas which still exist worldwide (Ciuti et al. 2016; Kaur and Alam 2013; Alam and Alam 2013; Alam et al. 2013).

The mobile communication and m-health sectors have traveled a long path from 2G to 5G because of which it has become possible to almost all types of electronic devices with each other. The descriptions of 5G include high data transfer rate, low transmission latency, and high capability to support diversified challenging applications. However, still, a lot of improvements are required for providing interconnection between multi-input multi-output technology, and device-to-device communication. In addition to it, the interference control and monitoring, spectrum chipping with multi-radio frequency access technology, cloud computing technologies, and other necessary software-defined networks are becoming attractions of mobile health communities. The 5G networks are providing interconnection between wireless and wired networks with any hindrance and enabling us to execute many exigent applications. Therefore, the author has very high expectations for running massive multidimensional data processing tasks using clouds and mobile health systems (Khan et al. 2015, 2017, 2019).

26.4 Proposed Architecture of Mobile Health System

In this section, the author has proposed the architecture of mobile health system which uses clouds and sensor networks for further improving the performance of mobile health systems. The proposed architecture enables a healthcare organization e.g. a clinic or a hospital to administer the data collected by wireless sensor networks

for supervising patients. The proposed architecture is scalable and it is able to able to store the huge amount of data originated by sensors of the proposed m-health system. Since the obtained patient's data are extremely sensitive. Therefore, the author has proposed a novel security mechanism which guarantees data confidentiality, integrity, and access controls. The safety configurations and key issues management in the proposed solution are completely translucent to the end users including doctors and patients and it does not need any type of external or internal interventions.

In order to attain the aforesaid objectives, the author has proposed the architecture described in Fig. 26.3. This proposed architecture considers two types of users namely patients and healthcare professionals. The proposed architecture includes the following four components:

(i) Wireless Sensor Networks (WSN): The WSN gathers health-related data and information from patients.
(ii) Monitoring Applications: The monitoring applications permit healthcare professionals including doctors, nurses and others to access and to store the collected data.
(iii) HealthCare Authority (HCA): The HCA specifies and enforces the concerns of security issues of the healthcare organizations.
(iv) Cloud Servers: The cloud servers ensure data storage in a scattered way. After storing data on the clouds, the proposed architecture provides almost infinite storage facility with high scalability. In an actual sense, the proposed architecture increases its storage capabilities by using on-demand service providing the feature of the clouds as per the requirements.

In order to obtain tuned access control, the author has used attribute dependent encryption (ADE) to encode data before storing in the clouds. In ADE, the patient's data is being encoded with the help of an access structure which is the logical representation of access policy. Therefore, the data can be easily accessed by physicians in different divisions of the health institution. The encoded text can be decoded by any end user if his/her undisclosed key has attributes which assure the access policy.

The supremacy of ADE is defined by the way where we don't need to depend on the storage server for preventing unlawful data access. Nevertheless, this particular characteristic becomes problematic at the time of changing access policy. In order to apply to apply an innovative access policy for a file, we must download it, re-encode it with the help of a novel access & control structure and upload it once more to the cloud. But, certain questions should be handled carefully like who should generate the access structure which will control the security policy and who should originate & and allocate the keys which are necessary to access the data are actual tests in mobile healthcare systems. The ADE based system which is based on patient-centric approach may not be suitable to answer these questions.

In order to handle the first challenge of ADE integration, the author has advised using symmetric cryptography and ADE to encode data. Furthermore, the author has proposed to encode each medical data file with a randomly generated symmetric

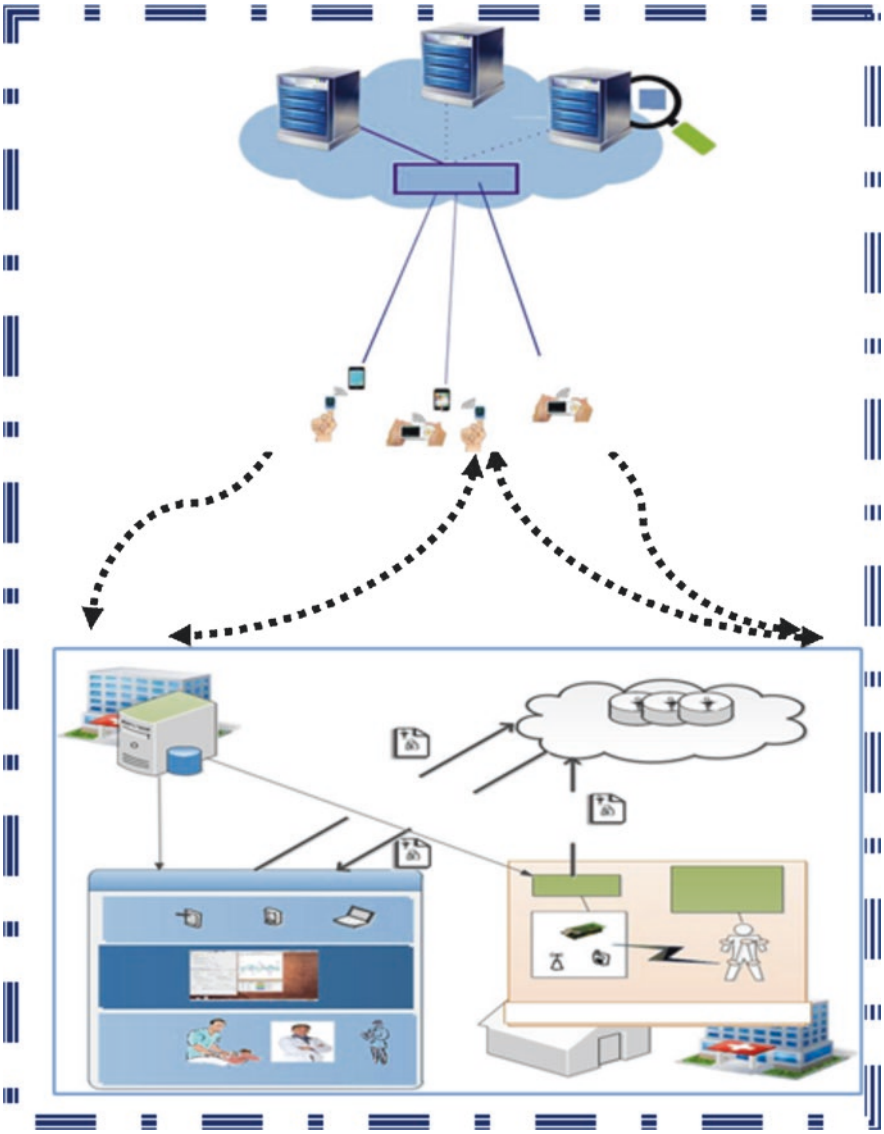


Fig. 26.3 The ADE based proposed architecture of mobile health care system using cloud computing and sensor networks

key (RGSK) and encode the RGSK with ADE. Here, the encoded file and the encoded RGSK are transmitted to the clouds for storage. If a user has a secret key which satisfies the ADE access mechanism then he/she will be able to decode the RGSK and hence it will be possible to decode the file. This approach leads to a momentous gain in data communication and encoding operations. In fact, the author

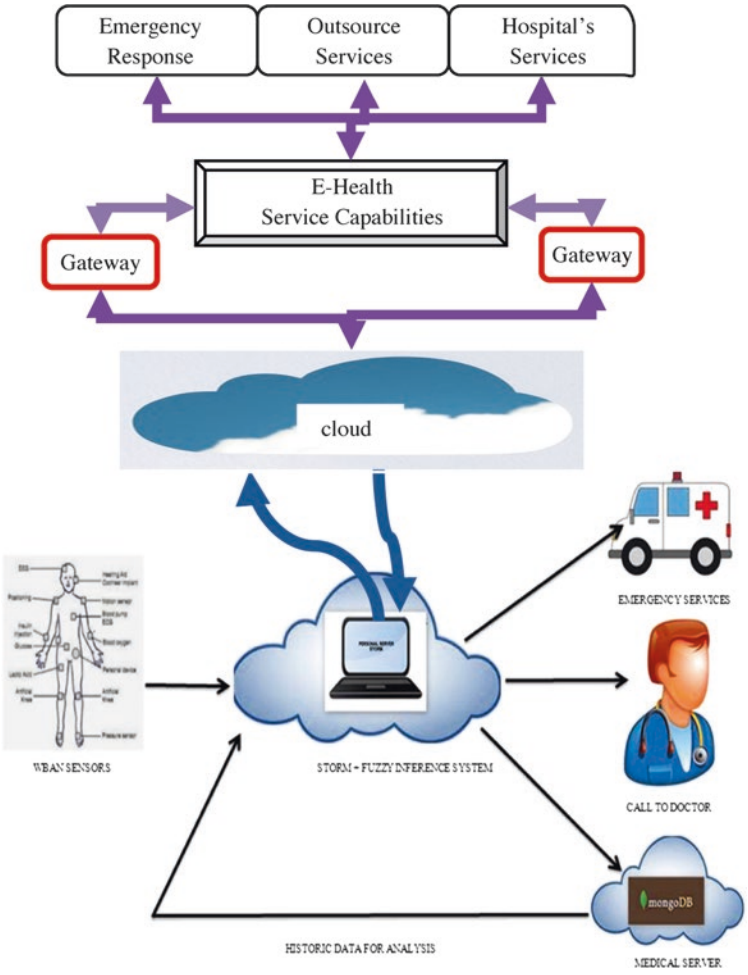


Fig. 26.4 Interaction between mobile healthcare systems with different layers of clouds

has observed that the ADE takes much processing power than symmetric cryptography at the time of handling complex access policies of mobile health management systems. In order to handle the second dispute, the author has used healthcare authority based complex security management systems.

The proposed architecture of Fig. 26.3 consists of three main layers which are acting as the moral fiber for our proposed system. The Fig. 26.4 describes the three layers of our proposed architecture and its interaction with mobile healthcare systems using sensor networks.

26.4.1 Awareness Layer

The initial layer at the bottom of the pecking order includes a variety of sensors which are used in the proposed system for collecting real-time medical data. These sensors are wearable and are fixed in and around the environment neighboring the patient and also in the body of the patient. These sensors are mainly classified into two types namely environmental sensors and medical sensors. The environmental sensors measure and control parameters of the room like room temperature, and oxygen level whereas the medical sensors measure very important parameters of the patient blood pressure, electrocardiogram (ECG) and body temperature etc. The data related to the patients collected using sensors are transmitted to medical healthcare professionals through IoT and cloud computing systems. Here, a unique identification number is attached to each data which represents the corresponding patient. The gateway is used for transmitting data from one layer to another layer.

26.4.2 Middleware and Application Programme Interface Layer

This particular layer is the crucial layer of the proposed system which consists of numerous Application Programming Interfaces (APIs). The clouds will store the patient's medical history and current medical records of parameters obtained through medical sensors. The storage will play a key role in the case of urgent response which may be needed by the hospital management system. At the time of patient's registration in the mobile healthcare system, an API creates the profile of the patient. The APIs maintain the profile creation, storage space, and queries about the patient's history in the system.

26.4.3 E-Mobile Health Application and Service Layer

This layer of the proposed m-healthcare management system offers outsourcing services. Therefore, it will provide E-health related advises to all the patients. The duties of the E-mobile healthcare application layer are to prescribe medicines to the patients and analyze the values of parameters obtained from medical sensors. The e-health service layer offers suggestions with the help of sensors data and parameters. Further, the response team may take necessary actions on urgent basis as per the information of sensors data. The mobile healthcare system monitors and controls the patients who are contacting from remote locations.

The most basic functionalities of a smart mobile healthcare management system comprise of electrocardiogram display in the form of waves, showing pulse rates and displaying the levels of gases in the blood flowing in the body. The proposed model has the multi-level diagnostic capability. Therefore, it is very much helpful for medical professionals including doctors. In the proposed model the network sockets are created using a wireless network communication system and occupied network protocols to perform their day-to-day activities including emergency services. The right to use the Bluetooth or Wi-Fi technologies permits the specific users/applications to configure the locally available device. The proposed mobile healthcare network permits specific users/applications to view and observe information about network connection status (not connected/connected).

26.5 Results and Discussions

26.5.1 Services Provided by Proposed Cloud and IoT Based Healthcare System

On the basis of processing, monitoring, messaging, viewing, and storage capabilities proposed cloud and IoT based mobile healthcare system the author can say that the proposed system offers services like Cloud Data Storage Services, Hospitals Services, Emergency Response Services, Patient Monitoring Services, and Health Advice with Necessary Action Services.

26.5.1.1 Cloud Data Management and Storage Services

In this section, the proposed mobile healthcare system has offered a unique set of services in the form of storing patient's data in the cloud and its corresponding management. Here, the storage capacity of the cloud is used to store a patient's medical history and it can further be correlated with the current medical sensors data of the same patient.

The storage capacity of the cloud can be utilized by the mobile healthcare system to store the medical reports, prescriptions, and illness healing patterns with allergic medicines. These patterns will be stored in the form of Microsoft Excel files or XML files.

26.5.1.2 Hospital Services

In the proposed approach each patient is being observed and examined by comparing the values of specific parameters obtained from the medical sensors embedded on the patient's body and in the surrounding atmosphere. To minimize the risks

these values are also being monitored by attendants who are physically present in the premises of mobile healthcare centers. If any anomaly exists then the corresponding message will be sent to the concerned authorities and further corrective actions will be taken. Hence, the corrected data will further be stored in the cloud and IoT of the proposed system. The same type of services can be provided by the proposed system to the patients who are opting for private monitoring at their houses. In this situation, a nurse should be provided to the premises of the patient and correspondingly a fixed amount of additional charge may be taken by the m-healthcare system.

26.5.1.3 Emergency and Urgent Response Services

In any mobile healthcare system, there may arise situations where instant attention is required on an urgent basis from the caregivers for certain circumstances in which the life the patient is in danger. Here, a situation may arise where the threat of life may be far beyond the control of the caregiver. Therefore, these urgent cases need immediate intervention from the medical experts of that particular medical science field. The proposed system is also able to tackle this situation.

26.5.1.4 Online Health Advice and Necessary Action Services

The online health advice service is designed to function in the cases where emergency response system failed and the patient struggling hard to get a life is unattended. In this situation, the online health advice based necessary action services are activated and used. Here, the server of the proposed m-healthcare system will execute an artificial intelligence based pattern detection program to find whether such type of urgent situation has been reported earlier or not? If such type of pattern matching is reported then the system will try to find out its history and the corresponding medicines which were given at that time with the help of clouds storage and IoT based technologies of the proposed system. This approach based medical treatment can help the doctors of the m-health system in curing chronic diseases.

26.5.1.5 Online Patient Monitoring Services

Nowadays the younger generation is working in different cities and they are changing their cities frequently. Therefore, many parents of these younger generations are staying away from their sons and daughters. Hence, in these situations, if sudden health problems arise with these parents who are staying at remote locations and away from their younger generation family members then the proposed patient monitoring approach of the m-healthcare system will be very much useful.

This model is developed in such a way that the doctors and medical professionals can monitor the parameters of the patient's medical sensors from the hospital and

the values of these parameters can be seen by the sons and daughters using their smart mobile phones because the proposed m-healthcare system will transmit the parameter values of medical sensors to the sons and daughters of these old age patients using IoT and cloud-based API technologies. The current location old age parents are monitored and managed using global positioning system.

26.5.2 Online Monitoring the Performance of Cloud and IoT Based Healthcare Systems

The design and infrastructure of mobile Healthcare systems depend on the way of deployment of wireless sensors for handling emergency and urgent cases of remotely located patients. After analyzing many research papers the author came to the conclusion that the majority of developed mobile healthcare systems are developed for handing epilepsy, dementia, cardiac arrest, and paralysis deceases. Therefore, while designing and developing the proposed mobile healthcare system the author concentrated on almost all types of deceases. The evaluation of our proposed system was analyzed for indoor and outdoor patients. In our proposed mobile healthcare system the sensors of wireless body sensor networks are successfully handling decision making processes of emergency and urgent cases of patients in odd hours.

Since sensors deployed on the patient's body and surrounding atmosphere are generating a large amount of data. Therefore, the clouds are used to store these data and updates are provided for sensors data every twenty seconds. In order to handle these critical data items of patients, the author has divided the critical cases into different categories namely brain strokes, brain hemorrhage, cardiac arrests, heart attacks, severe respiratory arrests, epilepsy, and severe accidents etc. In the proposed system the most appropriate scheduling approach is used to deploy medical professionals for handling urgent and emergency cases of patients.

The fuzzy logic and soft computing based algorithms are used in the proposed system to define when and how much data should be transmitted that decide the best time to start a data transmission. Since the physicians have better compatibility with video technology based patient examination and monitoring system. Therefore, the online IoT and Cloud technologies based video communication approaches are used in this research work to visualize and monitor patients. Hence, the proposed m-healthcare system works with better accuracy in the cases of patient illness diagnosis and online patients monitoring. The data sampling strategy used in this research work is very much helpful in reducing the size of data gathered from sensors deployed on the patient's body. The interaction between segments of proposed cloud and IoT based m-health system is presented in Fig. 26.5. The structure of Fig. 26.5 shows that the patients and medical professionals can register and perform different medical related activities online.

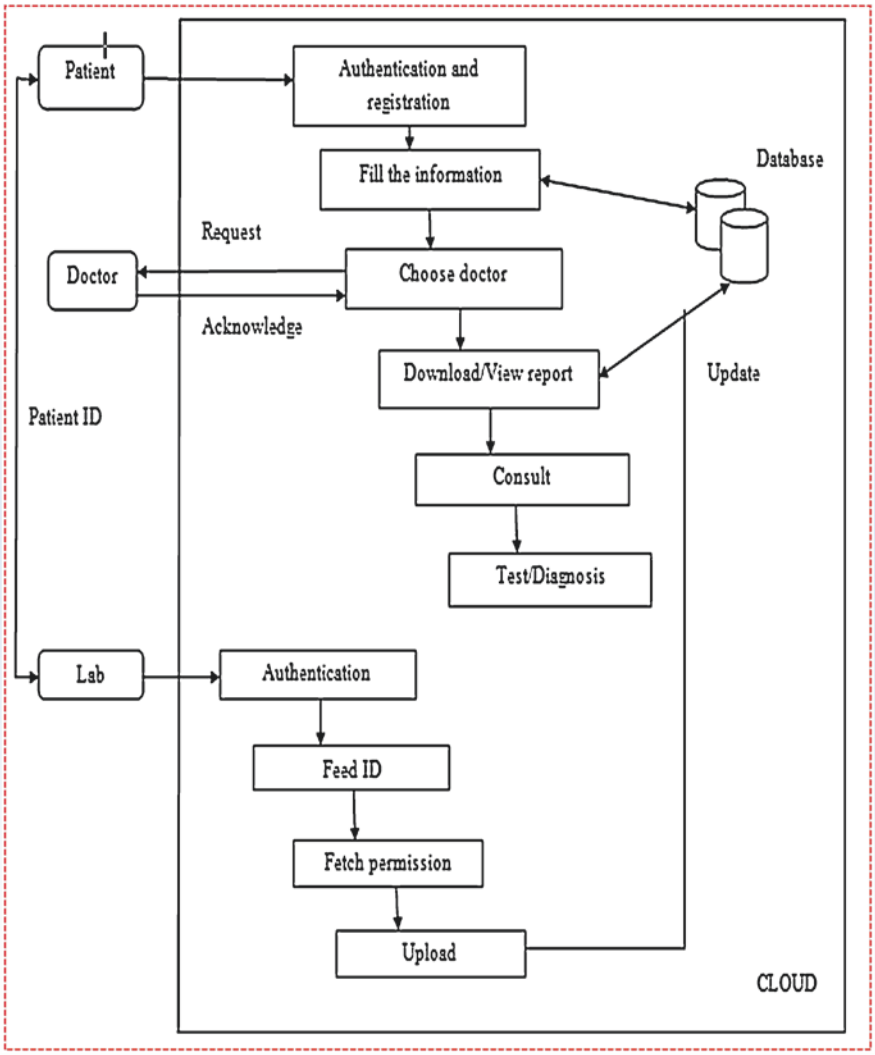


Fig. 26.5 The day-to-day activities performed by patients and medical professionals in an online m-health system

The features provided by the proposed mobile healthcare system which uses sensor networks, soft computing, fuzzy set concepts, clouds & IoT based technologies and its comparisons with other existing m-health systems is presented in Table 26.1.

Table 26.1 The characteristics provided by the proposed mobile healthcare system and its comparison with other existing smart m-health systems

Authors	Year	Cloud	IoT	WBAN	Big Data	WSN	MTM	Networking Technologies	3D Printing	Robotics	Fog and Mobile Cloud	Social Networks	cialArti Intelligence
Taylor and Stoianovici (2003)	2003	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Taylor (2006)	2006	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Haux et al. (2008)	2009	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cao et al. (2009)	2009	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Ko et al. (2010)	2010	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Alemdar and Ersoy (2010)	2010	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Latrâe et al. (2011)	2011	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Chen et al. (2011)	2011	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Wu et al. (2011)	2011	Yes	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Yoo et al. (2012)	2012	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Griffiths et al. (2012)	2012	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Ermakova et al. (2013)	2013	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Pino and Di Salvo (2013)	2013	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Sun and Reddy (2013)	2013	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Zou et al. (2013)	2013	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Abbas and Khan (2014)	2014	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Malik et al. (2015)	2015	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Calabrese and Cannataro (2015)	2015	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Laplante and Laplante (2015)	2015	Yes	X	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Islam et al. (2015)	2015	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Darshan and Anandakumar (2015)	2015	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Filipe et al. (2015)	2015	Yes	Yes	X	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Archenaa and Anita (2015)	2015	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Burgner-Kahrs et al. (2015)	2015	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Yeole and Kalbande (2016)	2016	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Ramesh et al. (2016)	2016	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Kassahun et al. (2016)	2016	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
Ciuti et al. (2016)	2016	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Proposed sensor networks, clouds, and IoT based Healthcare system	2019	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

26.6 Conclusions

Regardless of increasing the presence of remotely managed health monitoring in houses, multi-specialty hospital, and emergency scenarios, the expansion of WBSN based mobile healthcare management systems is still at a progressing stage particularly for outdoor urgent and emergency cases. The proposed research work of this chapter highlights the urgent requirement of mobile healthcare management and control system which can be integrated with clouds, internet of things, sensor networks and soft computing technologies. The proposed mobile healthcare management system of this research work fulfills this dream of integrating various 4G and 5G technologies and tools with m-health systems.

The sprouting technologies e.g. cloud services, medical sensors and Internet-of-things signify new paradigms for providing communication among specified layers which are established in mobile healthcare systems. The fuzzy logic and soft computing based algorithms help the proposed system in reducing the data size which is obtained from sensors of the proposed mobile healthcare system. The integration of video technologies with clouds and IoT technologies reduce the complexity level of online patient monitoring and health examination process. Hence, the proposed m-healthcare system works with high accuracy in the cases of patient illness diagnosis and online patients monitoring. The data sampling strategy used in this research work is very much helpful in reducing the size of data gathered from sensors deployed on the patient's body. The proposed mobile healthcare system uses the most appropriate sampling strategy to reduce the volume of data obtained from medical sensors and atmospheric sensors. Hence, the channels of WBSN have relatively lower traffic load.

References

Abbas, A., & Khan, S. U. (2014). A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. *IEEE Journal of Biomedical and Health Informatics, 18*(4), 1431–1441.

Acampora, G., Cook, D. J., Rashidi, P., & Vasi-lakos, A. V. (2013). A survey on ambient intelligence in health-care. *Proceedings of the IEEE, 101*(12), 2470–2494.

Aceto, G., Botta, A., de Donato, W., & Pescap, A. (2012). Cloud monitoring: Definitions, issues and future directions. In *1st IEEE international conference on cloud networking*, CLOUDNET 2012, Paris, France, November 28–30, 2012, pp. 63–67.

Aceto, G., Montieri, A., Persico, V., Pescape, A., D'Argenio, V., Salvatore, F., & Pastore, L. (2016). *A first look at an automated pipeline for NGS-based breast-cancer diagnosis: the cardigan approach*. In 3rd workshop on computational intelligence techniques for industrial and medical applications, December 2016.

Aceto, G., Persico, V., & Pescap, A. (2018). The role of information and communication technologies in healthcare: Taxonomies, perspective and challenges. *Journal of Network and Computer Sciences, 1*, 1–48.

Ahuja, S. P., Mani, S., & Zambrano, J. (2012). A survey of the state of cloud computing in healthcare. *Network and Communication Technologies, 1*(2), 12.

Al Yami, A., Atkins, A. S., & Campion, R. (2016). *Performance improvement in hospital management using RFID and ZigBee technologies for tracking and monitoring patients and assets in Saudi Arabia*. In Proceedings of IIER 64th International Conference on Science, Innovation and Management (ICSIM) Performance, 2016.

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of things security: A survey. *Journal of Network and Computer Applications, 88*, 10–28.

Alam, M, & Alam, B. (2013). Cloud query language for cloud database. In *Proceedings of the international conference on Recent Trends in Computing and Communication Engineering – RTCCE 2013*, Hamirpur, HP, pp. 108–112.

Alam, B., Doja, M. N., Alam, M., & Malhotra, S. (2013). 5-layered architecture of cloud database management system. *AASRI Procedia Journal, 5*, 194–199.

Alemdar, H., & Ersoy, C. (2010). Wireless sensor net-works for healthcare: A survey. *Computer Networks, 54*(15), 2688–2710.

Allen, S. (2016). New prostheses and outhouses step up their game: Motorized knees, robotic hands, and exosuits mark advances in rehabilitation technology. *IEEE Pulse, 7*(3), 6. https://doi.org/10.1109/MPUL.2016.2539759. ISSN:2154-2287.

Alpay, L., Toussaint, P., & Zwetsloot-Schonk, B. (2004). Supporting healthcare communication enabled by information and communication technology: Can HCI and related cognitive aspects help? In *Proceedings of the conference on Dutch Directions in HCI*, Dutch HCI '04, New York, USA, pp. 1–12.

Amazon Lex, Conversational interfaces for your applications. Powered by the same deep learning technologies. https://aws.amazon.com/lex/

Andriopoulou, F., Dagiuklas, T., & Orphanoudakis, T.. (2017). Integrating IoT and fog computing for healthcare service delivery. In *Components and services for IoT platforms*, pp. 213–232.

Angiuoli, S. V., White, J. R., Matalka, M., White, O., & Fricke, W. F. (2011). Resources and costs for microbial sequence analysis evaluated using virtual machines and cloud computing. *PLoS One, 6*(10), 1–10.

Archenaa, J., & Anita, E. M. (2015). A survey of big data analytics in healthcare and government. *Procedia Computer Science, 50*, 408–413.

Armbrust, M., Fox, A., Grith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM, 53*(4), 50–58.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks, 54*(15), 2787–2805.

Bahga, A., & Madisetti, V. K. (2013). A cloud-based approach for interoperable electronic health records. *IEEE Journal of Biomedical and Health Informatics, 17*(5), 894–906.

Balter, M. L., Chen, A. I., Maguire, T. J., & Yarmush, M. L. (2017). Adaptive kinematic control of a robotic venipuncture device based on stereo vision, ultra-sound, and force guidance. *IEEE Transactions on Industrial Electronics, 64*(2), 1626–1635.

Bamiah, M., Brohi, S., Chuprat, S., et al. (2012). A study on significance of adopting cloud computing paradigm in healthcare sector. In *Cloud Computing Technologies, Applications and Management (ICCCTAM)*, 2012 international conference on IEEE, pp. 65–68.

Bardram, J. E., & Christensen, H. B. (2001). Middleware for pervasive healthcare. In *Advanced topic workshop: Middleware for mobile computing*.

Barua, M., Liang, X., Lu, R., & Shen, X. (2011). ESPAC: Enabling security and patient-centric access control for e-health in cloud computing. *International Journal of Security and Networks, 6*(2–3), 67–76.

Bazzani, M., Conzon, D., Scalera, A., Spirito, M. A., & Trainito, C. I. (2012). Enabling the IoT paradigm in e-health solutions through the virtual middleware. In *2012 IEEE 11th international conference on trust, security and privacy in computing and communications*, pp. 1954–1959.

Beam, A. L., & Kohane, I. S. (2016). Translating arterial intelligence into clinical care. *JAMA, 316*(22), 2368–2369.

Benharref, A., & Serhani, M. A. (2014). Novel cloud and SOA-based framework for e-health monitoring using wireless biosensors. *IEEE Journal of Biomedical and Health Informatics, 18*(1), 46–55.

Bernhard, J.-C., Isotani, S., Matsugasumi, T., Duddalwar, V., Hung, A. J., Suer, E., Baco, E., Satkunasivam, R., Djaladat, H., Metcalfe, C., Hu, B., Wong, K., Park, D., Nguyen, M., Hwang, D., Bazargani, S. T., de Castro Abreu, A. L., Aron, M., Ukimura, O., & Gill, I. S. (2016). Personalized 3d printed model of kidney and tumor anatomy: A useful tool for patient education. *World Journal of Urology, 34*(3), 337–345.

Biswas, J., Maniyeri, J., Gopalakrishnan, K., Shue, L., Phua, J. E., Palit, H. N., Foo, Y. S., Lau, L. S., & Li, X.. (2010). Processing of wearable sensor data on the cloud – A step towards scaling of continuous monitoring of health and well-being. In *2010 annual international conference of the IEEE engineering in medicine and biology*, IEEE, pp. 3860–3863.

Blobel, B., & Holena, M. (1997). Comparing middleware concepts for advanced healthcare system architectures. *International Journal of Medical Informatics, 46*(2), 69–85.

BurgerKahrs, J., Rucker, D. C., & Choset, H. (2015). Continuum robots for medical applications: A survey. *IEEE Transactions on Robotics, 31*(6), 1261–1280.

Calabrese, B., & Cannataro, M. (2015). Cloud computing in healthcare and biomedicine. *Scalable Computing Practice and Exercise, 16*(1), 1–18.

Cao, H., Leung, V., Chow, C., & Chan, H. (2009). Enabling technologies for wireless body area networks: A survey and outlook. *IEEE Communication Magazine, 47*(12), 84–93.

Chen, M., Gonzalez, S., Vasilakos, A., Cao, H., & Leung, V. C. (2011). Body area networks: A survey. *Mobile Networks and Applications, 62*(2), 171–193.

Chen, Y., Argentinis, J. E., & Weber, G. (2016). IBM: Watson: How cognitive computing can be applied to big data challenges in life sciences research. *Clinical Therapeutics, 38*(4), 688–701.

Ciuti, G., Calio, R., Camboni, D., Neri, L., Bianchi, F., Arezzo, A., Koulaouzidis, A., Schostek, S., Stoyanov, D., & Oddo, C. (2016). Frontiers of robotic endoscopic capsules: A review. *Journal of Micro-Bio Robotics, 11*(1–4), 1–18.

Darshan, K., & Anandakumar, K. (2015). A comprehensive review on usage of internet of things (IoT) in health-care system. In *Emerging Research in Electronics, Computer Science and Technology (ICERECT)*, 2015 International Conference on IEEE, pp. 132–136.

Datta, S. K., Bonnet, C., Gyrard, A., da Costa, R. P. F., & Boudaoud, K. (2015). Applying Internet of Things for personalized healthcare in smart homes. In *Wireless and Optical Communication Conference (WOCC)*, IEEE, pp. 164–169.

Duarte, J. M., Cerqueira, E., & Villas, L. A. (2015). Indoor patient monitoring through Wi-Fi and mobile computing. In *2015 7th international conference on New Technologies, Mobility and Security (NTMS)*, IEEE, pp. 1–5.

Elfouly, T. (2017). Distributed in network processing and resource optimization over mobile-health systems. *Journal of Network and Computer Applications, 82*, 65–76.

Ermakova, T., Huenges, J., Erek, K., & Zarnekow, R. (2013). Cloud computing in healthcare – A literature review on current state of research. In *Proceedings of the nineteenth Americas conference on Information Systems, Chicago, Illinois* (pp. 1–5). Seattle: AMCIS.

Fang, L., Chen, T., Li, R., & Liu, S. (2016). Application of embedded FBG sensors in monitoring health to 3D printing structures. *IEEE Sensors Journal, 16*(17), 6604–6610.

Farheen Pathan, & Jadhav, H. B. (n.d.). Patient privacy control for healthcare system in cloud computing environment. *International Research Journal of Engineering and Technology, 4*(7), 674–676.

Filipe, L., Fdez-Riverola, F., Costa, N., & Pereira, A. (2015). Wireless body area networks for healthcare applications: Protocol stack review. *International Journal of Distributed Sensor Networks, 11*(10), 21–37.

Five Reasons Healthcare Data Is Unique and Di cult to Measure. Health Catalyst, 2017. https://www.healthcatalyst.com/5-reasons-healthcare-data-is-difficult-to-measure. Accessed April 2017.

Griffiths, F., Cave, J., Boardman, F., Ren, J., Pawlikowska, T., Ball, R., Clarke, A., & Cohen, A. (2012). Social networks the future for network delivery. *Social Sciences and Medicines, 75*(12), 2223–2241.

Haux, R., Howe, J., Marschollek, M., Plischke, M., & Wolf, K.-H. (2008). Health-enabling technologies for pervasive health care: On services and ICT architecture paradigms. *Informatics for Health and Social Care, 33*(2), 77–89.

Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The internet of things for health care: A comprehensive survey. *IEEE Access, 3*, 678–708.

Kassahun, Y., Yu, B., Tibebu, A. T., Stoyanov, D., Giannarou, S., Metzen, J. H., & Vander Poorten, E. (2016). Surgical robotics beyond enhanced dexterity instrumentation: A survey of machine learning techniques and their role in intelligent and autonomous surgical actions. *International Journal of Computer Assisted Radiology and Surgery, 11*(4), 553–568.

Kaur, A., & Alam, M. (2013). Role of knowledge engineering in the development of a hybrid knowledge based medical information system for atrial fibrillation. *American Journal of Industrial and Business Management, 3*(1), 36–41.

Khan, I., Naqvi, S. K., & Alam, M. (2015). Data model for big data in cloud environment. In *Computing for Sustainable Global Development (INDIACom), 2015 2nd IEEE international conference on*, March 11–13, pp. 582–585.

Khan, S., Shakil, K. A., & Alam, M. (2017). Cloud based big data analytics: A survey of current research and future directions. *Advances in Intelligent Systems and Computing, 654*, 595–604. ISBN:978-981-10-6619-1, Electronic, Springer, 629–640.

Khan, S., Ali, S. A., Hasan, N., Shakil, K. A., & Alam, M. (2019). *Cloud computing for geospatial big data analytics* (pp. 1–28). Cham: Springer.

Ko, J., Lu, C., Srivastava, M. B., Stankovic, J. A., Terzis, A., & Welsh, M. (2010). Wireless sensor networks for healthcare. *Proceedings of the IEEE, 98*(11), 1947–1960.

Laplante, P. A., & Laplante, N. L. (2015). A structured approach for describing healthcare applications for the internet of things. In *Internet of Things (WF-IoT), 2015 IEEE 2nd world forum on IEEE*, pp. 621–625.

Latrâe, B., Braem, B., Moerman, I., Blondia, C., & Demeester, P. (2011). A survey on wireless body area networks. *Wireless Networks, 17*(1), 1–18.

Malik, H. H., Darwood, A. R., Shaunak, S., Kulatilake, P., El-Hilly, A. A., Mulki, O., & Baskaradas, A. (2015). Three-dimensional printing in surgery: A review of current surgical applications. *Journal of Surgical Research, 199*(2), 512–522.

Pino, C., & Di Salvo, R. (2013). A survey of cloud computing architecture and applications in health. In *International conference on Computer Science and Electronics Engineering*, pp. 1–6.

Ramesh, D., Suraj, P., & Saini, L. (2016). Big data analytics in healthcare: A survey approach. In *Microelectronics, Computing and Communications (MicroCom), 2016 international conference on IEEE*, pp. 1–6.

Sun, J., & Reddy, C. K. (2013). Big data analytics for health-care. In *Proceedings of the 19th ACM SIGKDD international conference on Knowledge Discovery and Data Mining*, pp. 1525–1525.

Taylor, R. H. (2006). A perspective on medical robotics. *Proceedings of the IEEE, 94*(9), 1652–1664.

Taylor, R. H., & Stoianovici, D. (2003). Medical robotics in computer-integrated surgery. *IEEE Transactions on Robotics and Automation, 19*(5), 65–81.

Wu, G., Talwar, S., Johnsson, K., Himayat, N., & Johnson, K. D. (2011). M2M: From mobile to embedded internet. *IEEE Communications Magazine, 49*(4), 36–43.

Yeole, A. S., & Kalbande, D. (2016). Use of Internet of Things (IoT) in healthcare: A survey. *Proceedings of the ACM Symposium on Women in Research, 2016*, 71–76.

Yoo, I., Alafaireet, P., Marinov, M., Pena-Hernandez, K., Gopidi, R., Chang, J.-F., & Hua, L. (2012). Data mining in healthcare and biomedicine: A survey of the literature. *Journal of Medical Systems, 36*(4), 2431–2448.

Zou, Q., Li, X.-B., Jiang, W.-R., Lin, Z.-Y., Li, G.-L., & Chen, K. (2013). Survey of map reduce frame operation in bioinformatics. *Briefings in Bioinformatics, 15*(4), 637.

Chapter 27
Future Internet of Things (IOT) from Cloud Perspective: Aspects, Applications and Challenges

Nahid Sami, Tabish Mufti, Shahab Saquib Sohail, Jamshed Siddiqui, Deepak Kumar, and Neha

Abstract The technological development has changed the way we live. With the fast pace by which technology is advancing to an ultra-era of computerization, the perception and behavior of our daily life has also got a new direction. With early days of advancement when desktop computers had been perceived as a revolution, people started to rely upon digital transformation. But as the Internet has grown exponentially, desktop is considered as 'gone are the days'. In the recent emergence of cloud services and Internet of Things (IoT), the various services and applications are applied without having any physical resources at one's hand. Since, Internet of Things is proved to be very influencing and has become fastest growing technology which is very evident as it is reported that IoT Devices will cross 21 billion by 2025. IoT provides infrastructure for real time objects and also help in keeping track about these objects by connecting devices smartly so that they can share data and resources with other machines. IoT uses various types of sensors embedded in various devices which emit data. These sensors share data using IoT common platform. This chapter aimed at studying different aspects of IoT. With the help of the detail discussion carried out in the work, the researchers can get a clear insight of how IoT can be perceived in future; also what could be the possible ways of utilizing cloud resources in the application of IoT. The study is believed to be useful for the researchers especially seeking research dimension in the field of cloud computing and IoT.

N. Sami · S. S. Sohail (✉) · Neha
Department of Computer Science and Engineering, School of Engineering Sciences and Technology, Jamia Hamdard, New Delhi, India

T. Mufti
Department of Computer Applications, Faculty of Computer Science and System Studies, Mewar University, Chittorgarh, Rajasthan, India

J. Siddiqui
Department of Computer Science, Aligarh Muslim University, Aligarh, India

D. Kumar
Amity Institute of Information Technology, Amity University, Noida, India

M. Alam et al. (eds.), *Internet of Things (IoT)*, S.M.A.R.T. Environments,
https://doi.org/10.1007/978-3-030-37468-6_27

Keywords IoT · Cloud computing · Cloud services · Smart devices · Radio frequency identification

27.1 Introduction

The extraordinary growth in the technological devices and the proliferation of Internet has made the things very different from what they were perceived few years back. The recent advancements in the technology has given birth to Internet of Things (IoT) and cloud computing. The various techniques have been suggested by the researchers to incorporate these two techniques together to make use of the features of the duo in a more effective way (Zhang et al. 2015; Munir et al. 2017; Rindos and Wang 2016). In the recent emergence of cloud services and Internet of Things (IoT), the various services and applications are applied without having any physical resources at one's hand. Since, Internet of Things is proved to be very influencing and has become fastest growing technology which is very evident as it is reported that IoT Devices will cross 21 billion by 2025 (Främling et al. 2014; Kobayashi et al. 2014). IoT provides infrastructure for real time objects and also help in keeping track about these objects by connecting devices smartly so that they can share data and resources with other machines. IoT uses various types of sensors embedded in various devices which emit data. These sensors share data using IoT common platform. These platforms collect data from various sources and then further analytics are performed on data and essential information is extracted before the result is concluded. Since, these resources is not easily available at every place, further, the cost is not affordable for all the research communities (Sohail et al. 2012). Hence, the cloud based services for IoT technologies would not only enhance the research performance but also it may reduce the cost and complexities in the implementation of several experiments. In future the devices can be implemented in smart farming, pulse oximeter, air pressure detection, smart eye and many more. It can also be used to figure DDoS (Distributed Denial of Service) attack by cyber criminals (Elkhatib et al. 2017; Abdelshkour 2015). These devices will be fueled with 5G network that will connect the 5G IoT devices directly with the network without using Wi-Fi router (Alam and Shakil 2013; Alam et al. 2013). But for using the smart devices, human need to be smarter as the rapid growth of these IoT devices give rise to privacy and security concern. These devices can be weaponized which in result may give adverse effect. This chapter aimed at studying different aspects of IoT. The chapter is organized as follows: the Sect. 27.2 deals with the background of the paper and illustrates how different sections are related. Section 27.3 gives the applications of the IoT from the perspectives of the cloud as reported in the literature, whereas Sect. 27.4 has a great insight of what IoT may look like in future. Finally the chapter is concluded in Sect. 27.5.

27.2 Background

27.2.1 Understanding IoT

In our daily life we have often come across modern and digitally equipped infrastructure where we find real objects which are connected to the internet. These real objects are electronic products that span over varieties of electronic gadgets, modern systems, intelligent sensors or smart devices. When these systems are connected to Internet, they are usually referred as "IoT-enabled" devices (Kim et al. 2015; Singh et al. 2015). The simple inference of the term IoT enabled is that the device is connected to the internet. These IoT enabled products can communicate data and able to be operated remotely which gives sense of an automated system. The exponential growth in the field of IoT can be understood by the truth that it has grown the attraction of the market and almost in all sectors of daily life it has received huge investments recently (Ahuja and Deval 2018; De Cremer et al. 2017; Karimi and Atkinson 2013; Sohail et al. 2014; Fleisch 2010). Figure 27.1 shows the details of IoT expenses in different sectors (https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/; https://www.pocket-lint.com/apps/news/126559-internet-of-things-explained-your-complete-guide-to-understanding-iot).

27.2.2 IoT and Its Relation with Cloud

The Internet of Things facilitates the users to use the connected devices for their use with the modern and updated equipped technology. Below in Fig. 27.2, we have shown a diagrammatic representation of how the different cloud based ToT services can be provided to users for better facilities (Yassine et al. 2019; Sohail et al. 2018a; Cui 2016).

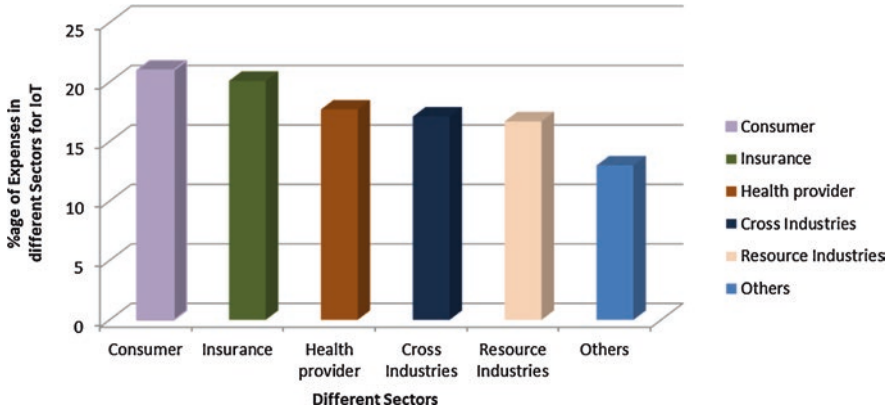


Fig. 27.1 IoT expenses in different sectors

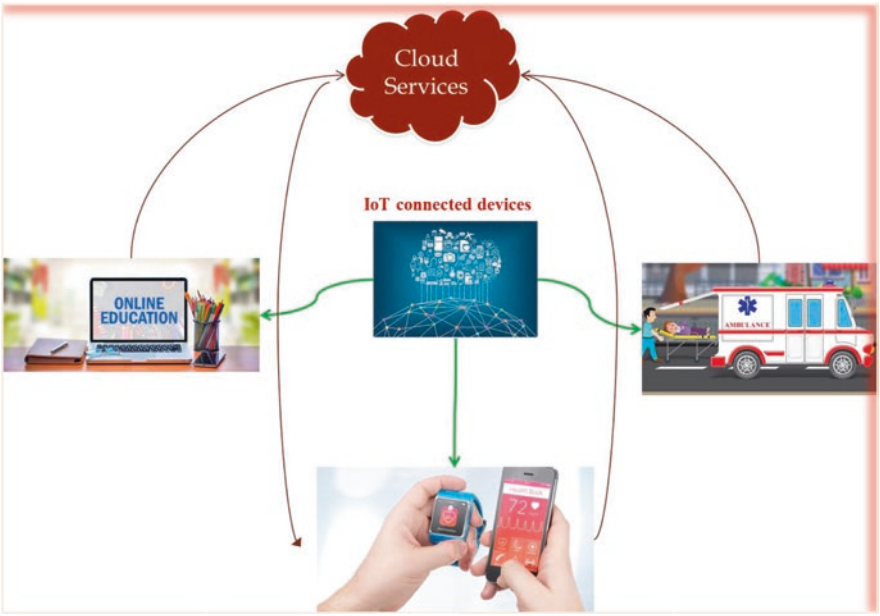


Fig. 27.2 IoT services at cloud

In this chapter we have tried to simplify the futuristic opportunities of IoT and highlights the advantages of the cloud computing and IoT when combined together. The chapter presents cloud aspects of IoT, applications of IoT and their cloud importance, and future IoT. These contents are provided in the Fig. 27.3 below for the readers.

27.3 Application of IoT

The emergence of IoT has introduced new technologies and has successfully explored several areas of research. On a keen observation of several online trends, we have come to know three trends of online social media behaviors i.e. the Google search, the twitter and the Linkedin feeds, an approximate score of 100 percent will be achieved as per a study conducted wherein the other applications using IoT ranked with a correspondingly relative percentage to the highest score. IoT offers many applications, uses and solutions but the major solutions directly related to our day to day life as well as economic usage of resources are enumerated below (Kodali et al. 2016; Alam et al. 2012; Gram-Hanssen and Darby 2018; Ashton 2009).

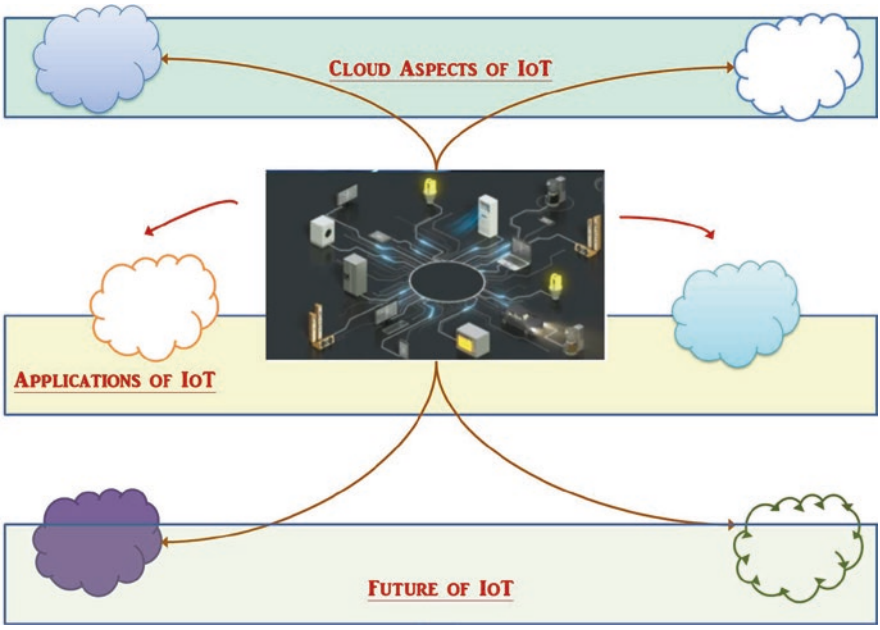


Fig. 27.3 The different aspects of IoT from cloud perspectives which have been discussed in the chapter.

27.3.1 Smart Home

Creating a smart home what does it mean, 100 years ago smart was able to turn lights on-off with the switch on the wall (Ashton 2009; Wijaya et al. 2014). The term smart means we can take control of your home with smart phones, tablets or another digital devices. By making things smart the things able to do work them self without you have to do anything at all like the lights turn on – off when the sun goes up and down or the lights turn on automatically when you arrive home or you turn on car through smart phone while having breakfast in the morning for better to save time (Alam et al. 2012; Gram-Hanssen and Darby 2018) According to the same study, approx. 60,000 people look for the term "smart home" every month which is quite believable because the IoT analytics company database preserves a database of 256 companies and startups for smart homes. The funding received to the startups for smart homes is above $ 2.5bn which includes multinationals like Haier, Phiilips and startups like Nest, AlertMe etc. (Främling et al. 2014; Sohail et al. 2012)With increase in need of innovation IoT provides the way to easily operate smart devices from a single touch. Allen Pan's Home Automation System used string of musical notes for the functions done (Mardacany 2014; Fig. 27.4).

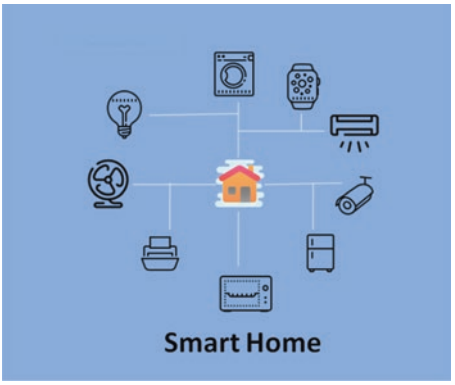


Fig. 27.4 Smart home

Fig. 27.5 Smart watch

27.3.2 Wearables Technologies

Another hot topic of IoT searches is Accessories like smart watches, trainers, smart bracelets and the like. Although Apple's smart watches leaded the race in 2015. However since then, plethora of other devices has gained customer's attention like the Sony Smart B trainer, Myo control LookSee bracelet. The startup by the name of Jawbone has received a record funding of more than half a million dollars in IoT wearables market. Wearable technology has a variety of applications being incorporated into navigation systems, quick trackers and healthcare (Repko and DeBroux 2012). In 2004, fashion design label invention called Hugshirt won the grand prize at the Cyber Art Festival in Bilbao, Spain. Fitbit released its first wearable around 2009 they basically works on active tracking (Fig. 27.5).

Fig. 27.6 Smart city

27.3.3 Smart City

In today's overpopulated metropolitans, citizens can only dream of cities which provide solutions to the day to day challenges they face in their lives (Abdelshkour 2015). Smart city is one such term which has gained popularity over the internet because of smart solutions to traffic woes, reduced noise and environmental pollutions and safety promise of such smart cities which are very few in the world but definitely possible due to the given level of technology and science (Ejaz and Anpalagan 2019). IoT is drastically used by the engineers and government for solving the issues faced globally for the better water management, (Ahuja and Deval 2018)increasing urban density, clean drinking water, analyzing air quality and often complex factors of town planning specifically to aid the problems facing by them. Palo Alto, San Francisco, is the first smart city which used new approach for traffic management (Gassmann et al. 2019; Fig. 27.6).

27.3.4 Smart Grids

A conceptualized Smart Grid of future resolves to use the supply and demand of electricity based on usage and consumption patterns in order to increase the efficiency, reliability and economics of electricity. Every month approx 40,000

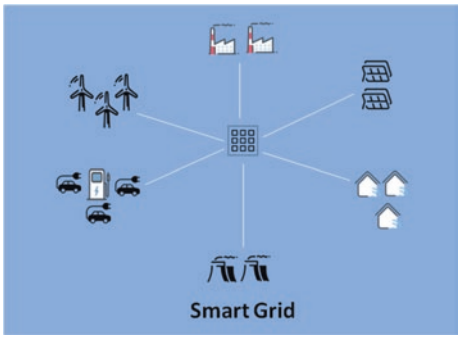


Fig. 27.7 Smart grids

searches on Google highlight the popularity of this concept. However because of the lack of technical and conceptual knowledge reduces the number of tweets on this topic. With more than half of the world population using IoT for making the cities ready for tomorrow's needs so that they can explore new opportunities, solutions and mechanisms to digitalized by creating a smart grid (Khatiwada 2018; Tsiatsis et al. 2019; Wang et al. 2010; Nogueira and Carnaz 2019; Fig. 27.7).

27.3.5 Industrial Internet

Unlike the consumer oriented IoT concepts, an upcoming industrial IoT concept that has been on a rage on internet both on Google and twitter as well as LinkedIn feeds is "Industrial Internet". Market research companies like Garter, Cisco etc. see Industrial internet as a potential promise but due to its lack of popularity among the masses it lags behind other consumer related IoT solutions. However, Industrial Internet gets the biggest word on twitter with approximately 1700 tweets per month. By connecting the machines, turbines, tools and devices in industries to a central Internet connection which has the capacity to collect, store and utilize data in instances of unplanned downtimes or system failures. This will not only boost as well as stabilize the production cycle but also ensures regulated growth and improvisation. The products quality is one of the major factor for a higher return on investment, by using IoT one can re-innovate product for better performance to create a table turning point in both cost and customer experience. In just 1-year internet connected devices reaches from 5 million to billions. Business Insider Intelligence estimates that 24 billion IoT devices increases over 300 billion as they grow over time (Pantano and Timmermans 2014; Fig. 27.8).

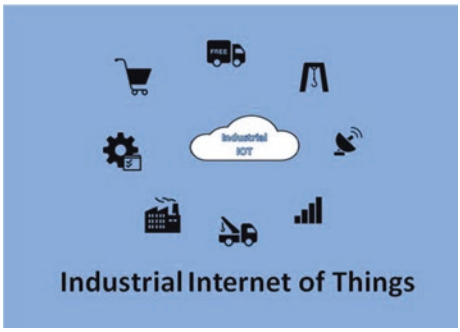


Fig. 27.8 Industrial IoT

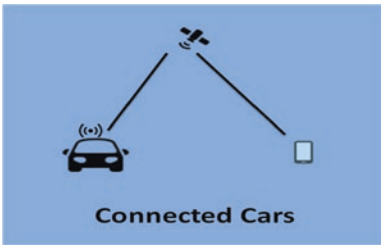


Fig. 27.9 Smart cars

27.3.6 Connected Car

Most of the innovative and ambitious automakers and some brave startups are working rigorously on the concept of Connected Cars. Apart from the auto giants like Ford and BMW, the techno giants like Apple, Google and Microsoft have announced the platforms for connected cars. Since the development cycle takes anything between 2 and 5 years, there is not much buzz yet in the masses yet. Still this concept occupies some margin on the internet especially Google (Kodali et al. 2016; Repko and DeBroux 2012; Kanchana 2018). Connected Car technology includes a network of antennas, sensors and embedded software's inside the car to enable it to deal with our complex world. It enables an automobile to use a mass of information it has gathered overtime to make consistent and accurate decisions and manage speed. This set of data and its IoT management will be crucial especially when the human lose all control on the steering and brakes to the autonomous controls of the smart car. Connected cars innovated in the way so that they can reach the peak to solve the current needs as the engineers working on it to made them self-authenticating and analyzing the problems while driving as they can easily analyze the defects on the way like pit holes, reasons of blockage etc. The first automobile invented by Carl Benz which patent his "vehicle powered by a gas engine" (Nogueira and Carnaz 2019; Fig. 27.9).

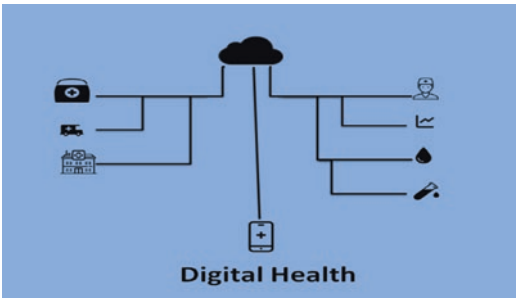


Fig. 27.10 Digital health

27.3.7 Connected Health (Digital Health/Tele Health/Tele Medicine)

The notion of Connected Health Care System and Smart Medical devices stands massive potential still remain the sleeping giants of the IoT (Jayaram 2017). Not just for the industry sector but also for the national well-being this concept should get push from the government and hopefully the few startups working in this area receive some push. By increasing the connectivity between the doctors and their patients, IoT may boost the relationship and satisfaction into the industry. IoT has brought new tools in the health industry ranging from fitness sensors to robotic surgery equipments. Thus it is a great way offer pocket friendly solutions in healthcare. It basically uses leftover data, controlled environments for medical advices. IoT basically works in the way to makes something important into something essential as they creates systems rather than just equipments (Bhavani Shanker and Shanmugam 2016; Fig. 27.10).

27.3.8 Smart Retail

Smart Retail or Proximity Advertising is slowly gaining popularity but the search trend still seems to be low as per a study only 430 feeds are coming on LinkedIn for this upcoming trend. Most of the real life and online retail giants as well as startups are already using some applications of IoT to improve their Store operations, Purchase momentum and theft control, inventory management and enhanced consumer experience (Sohail et al. 2017). Through IoT Physical retailers can beat the threats faced by the online retailing and regain the losing consumer base back to store. Such smart in store applications will also save the time and increases the efficiency of the consumer too (Sheela et al. 2019). It is an adverse need of smart retail in this competitive world to survive in the market. As Paytm is going to bring a first-of-its-kind cloud –based store to empowers the smart retail t increase profitability with ease (SR 2015; Fig. 27.11).

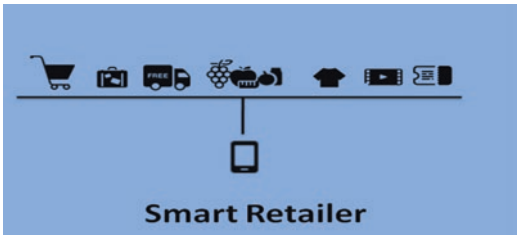


Fig. 27.11 Smart retailer

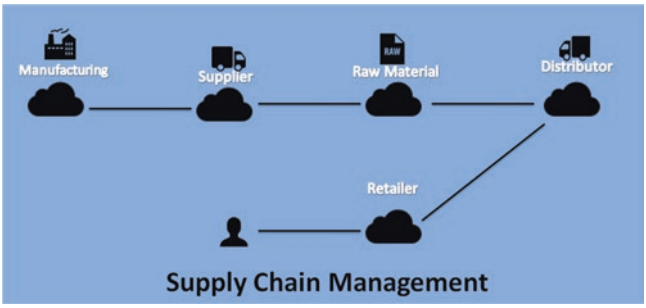


Fig. 27.12 Smart supply chain management

27.3.9 Smart Supply Chain

The supply chain has already induced the solutions like tracking of supplies and exchanging inventory information before and during delivery line since many years. This area will also require smarter logic but so far its popularity is confined and supply chain seems to be happy with the current achievements. With the help of IoT enabled systems, embedded sensors in the Factory could send and receive data based on arrange of parameters like pressure, temperature and utilization of machines while processing workflow information, equipment change settings and optimum performance. Industries need an intelligent supply chain for being responsive and flexible working. Tech Mahindra used a cloud based solution which provides end- to- end information visibility (WijerathnaYapa 2019; Fig. 27.12).

27.3.10 Smart Farming

Smart Farming can be a smart idea for agrarian economies and agricultural- export countries (Ahuja and Deval 2018; Gram-Hanssen and Darby 2018; SR 2015). The IoT is often overlooked when it comes to this category unlike the rapid adoptions at the industrial and consumer goods segment. Although it has the potential to revolu-

Fig. 27.13 Smart farming

tionize the way farming is done from maintaining the Livestock information to the agricultural cycles and other farming operations can be drastically supported (SR 2015; Mufti et al. 2019). As an emerging concept that defines managing farms using modern technologies like IoT to increase the quantity with quality. Statistics estimate the grows at world population to reach nearly 10 billion by the year 2050. Smart greenhouse is the need for future feed (Fig. 27.13).

27.3.11 Smart Factories

Smart factory is a flexible system which is a broad concepts consist the functioning of a factory to self-adopt, optimize and learn from the new conditions to produce more effectively in real-time conditions, IoT helps the plants, factories to transform to use new ideas to prevent the losses and expand the profitability. Schneider, which entered India in 1963, now has 24 manufacturing facilities provides over employment for 20,000 people. Although with smart solutions Panasonic aims to be the one stop solution for all welding, SMT and digital marketing needs (WijerathnaYapa 2019; Gubbi et al. 2013; https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html; Mufti et al. 2019). The Indian Institute of Science(IISC) is building India's first smart factory in Bengaluru. Due to rise of IoT in manufacturing industries Indian companies are being competitive to each other for achieving the tag of smart factory (Fig. 27.14).

27.3.12 Smart Food Industry

With IoT food industries are smarting up as they are using it for processing, tracking and quality check of food. The precise quantity of nutrients can be listed within a second and the freshness of food can be stored for a longer period of time. Different

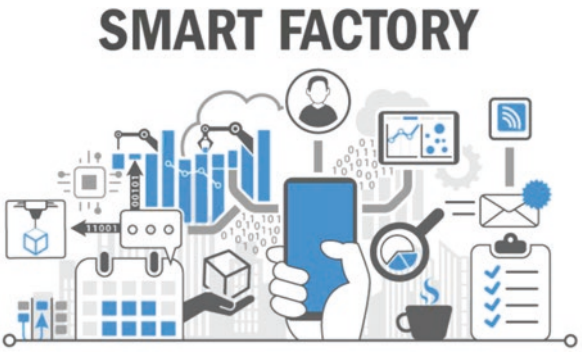


Fig. 27.14 Smart factory

kinds of sensors are used to monitor essential production state, temperature and so on (Gram-Hanssen and Darby 2018). The Indian food industry is worth US$13.56 billion & is growing at 17%. The food services sector touched upto US$24.77 billion by 2015. The first of series of India-wide smart food culinary symposia was organized by chefs from major dining chains and food representatives in Bangalore (Abdelshkour 2015; Wang et al. 2010).

27.4 Future of IoT

IoT is gathering enormous popularity all around the world for its huge demand in the field of technology. In IoT objects are present around us in one or another form. This new technology will give rise to Wireless Sensor Network (WSN) for its implementation (Gubbi et al. 2013). As the devices need to be connected ubiquitously for its smart functioning which will eventually increase its demand and usage? looking at its existing demand and potential, we can conclude that it has a great future ahead.

Looking at the present scenario of IoT, we wonder what the future technology is going to provide us. Going through an intense research led us say that the devices will make use technology in the most efficient way.

The above Fig. 27.15 shows the rapid growth of IoT devices over years in different sectors. The future seems to be more smart and ubiquitous with the emerging technology. Some of the futuristic predictions made about IoT includes (https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html).

- It has been roughly calculated that by 2025 IoT devices will cross 50 billion. The estimation made by the analytics of IoT shows that in 2016 4.7 billion devices were connected through the internet which may increase to 11.6 billion by 2021 and so on.

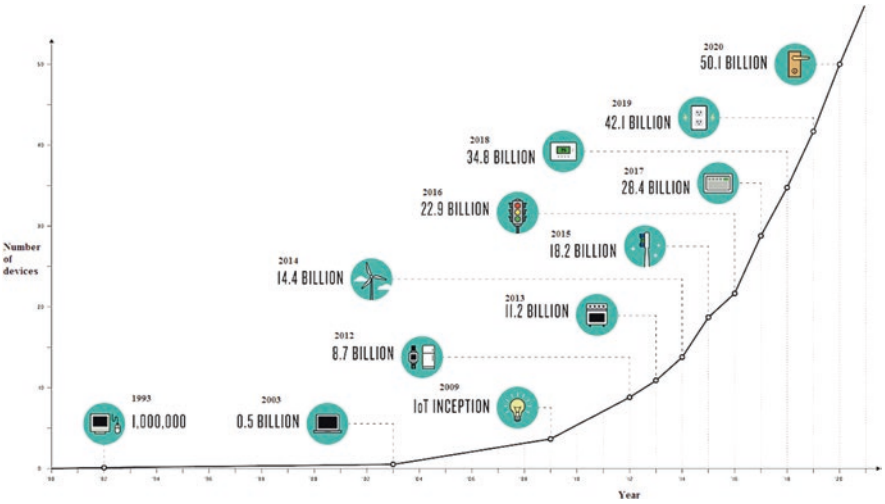


Fig. 27.15 Growth of IoT devices over years

- The advancement in technology will led to smart city development. The usage of IoT is not limited to people. Now a day companies and cities are adopting the smart technologies very frequently to save more money as well as time (Mufti et al. 2019). This will result in automated city which can be remotely managed and the data will be collected through IoT devices using various technologies.
- The increasing demand of IoT will give rise to artificial intelligence as the smart devices will collect data and that will be stored at cloud. Machine learning will help the system to understand things without using programming concept (Wang et al. 2016). Systems are designed such that data is given priority as it is received which later on make the machine smarter by giving preferences and work on the basis of need of the system.
- More intelligent and secure routers need to be used in case the IoT devices are installed in private places as they are not highly secure. While manufacturing IoT devices the focus is more upon their efficiency and less upon security. Routers need to be secure enough to prevent the connected devices at entry level. So, the manufacturers should look after the different technologies to enhance the security of the system.
- IoT growth will be boosted with the use of 5G network. The 5G(fifth generation) network will enhance the speed as well as efficiency in terms of connecting more smart devices simultaneously. This will also give rise to recent products based on the demand of costumer.
- Security and privacy will also become the area to be concerned about with the arrival of new 5G technology. The devices will be connected within the network through routers which will directly affect them with several attacks. The data will be stored on cloud and make easier for the attackers to aim them.

27.4.1 IoT Network in Future

This part explains a deep understanding about the IoT network in coming future. The given figure below describes different components in the network and how they are interconnected. The working of each component is explained further. The below architecture uses the concept of SDN(Software Defined Network) which is a prominent architecture in network (Reitblatt et al. 2013). It supervises the network control directly rather than using the forwarding concept (Sohail et al. 2018b). The working of SDN is done through different layers mostly infrastructure/physical, control/middle and the application layer (Kobayashi et al. 2014; Nunes et al. 2014; McKeown et al. 2008) (Kumar and Mufti 2017; Fig. 27.16).

- All the network devices required within is connected at the infrastructure layer which includes the routers, switching equipment etc.
- At the control layer the different mechanism works regarding providing essential protocols required for the network. Open flow plays a vital role here by providing the specification required for the network devices and controllers within the network.
- Application layer is basically concerned with the data regarding statistics, state, and the topology of the network.

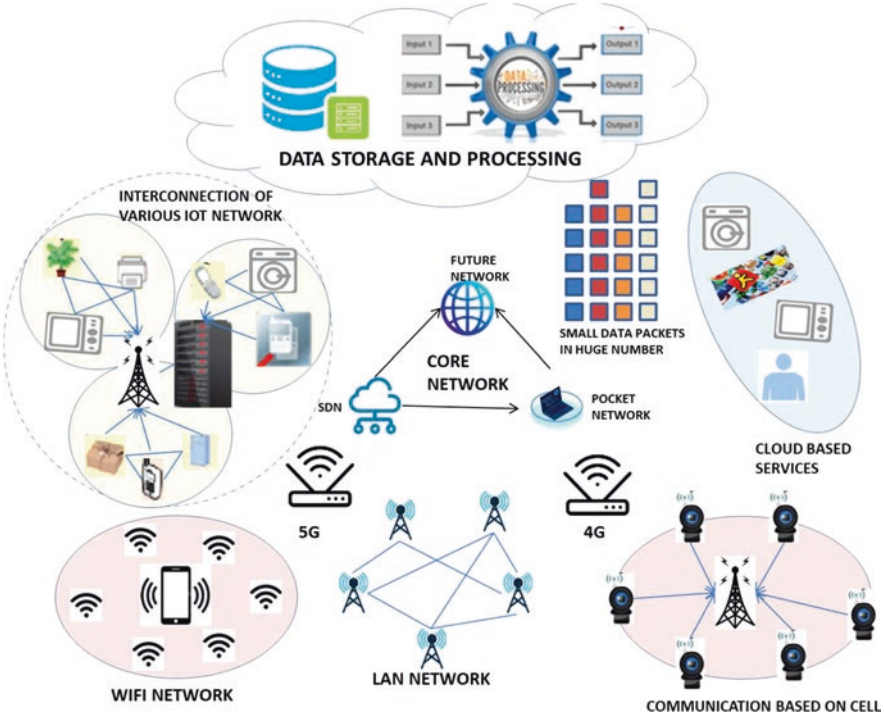


Fig. 27.16 Future IoT network

The use of SDN makes the working of devices smoother. And the use of open flow protocol provides the controller and network devices to communicate with each other (Wang et al. 2016; Patil et al. 2012). It helps in multiple packets simultaneously within the network and improves the quality of service being provided (Ishimori et al. 2013). And the fastest growing 5G technology in the future provides a high speed communication within the architecture (Patil et al. 2012). The IoT provides association such that everything can be tracked individually and easily. The most important right in such network is the privacy of an individual. It provides a trustable environment which should not have any negative impact over society. Technology should be standardized for better performance by reducing barriers (Coetzee and Eksteen 2011).

27.5 Conclusion

We intend to present a prospective idea of how IoT can influence our daily life and how the cloud computing can enhance the IoT services in future. The idea is explained and demonstrated using proper diagrams and explanations. The main contribution in the chapter is its inclusion of those unimaginable areas where the researcher may focus which in turn shall prove a milestone for the research community.

Further, there are the area where a lot of exploration is required which is yet to be answered. Hence, the study tries to reveal those areas and would be very helpful for the new researcher to explore the field of research in the related domain.

References

Abdelshkour, M. (2015). *IoT, from cloud to fog computing*. Cisco Blog.

Ahuja, S. P., & Deval, N. (2018). From cloud computing to fog computing: Platforms for the internet of things (IoT). *International Journal of Fog Computing (IJFC), 1*(1), 1–14.

Alam, M., & Shakil, K. A. (2013). Cloud database management system architecture. *International Journal of Advances in Computer Science and Its Applications, 3*(1), 27–31. Universal Association of Computer and Electronics Engineers(UACEE), ISSN:2250 – 3765, 2013, Australia.

Alam, M. R., Reaz, M. B. I., & Ali, M. A. M. (2012). A review of smart homes—Past, present, and future. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 42*(6), 1190–1203.

Alam, B., Doja, M. N., Alam, M., & Malhotra, S. (2013). 5-layered architecture of cloud database management system. *AASRI Procedia Journal, Elsevier, 5*, 194–199.

Ashton, K. (2009). That 'internet of things' thing. *RFID Journal, 22*(7), 97–114.

Bhavani Shanker, K., & Shanmugam, V. (2016). *Smart retailing in unison with supply chain in IoT eco-system*.

Coetzee, L., & Eksteen, J. (2011). *Internet of things–promise for the future? An Introduction*.

Cui, X. (2016). The internet of things. In *Ethical ripples of creativity and innovation* (pp. 61–68). Springer.

De Cremer, D., Nguyen, B., & Simkin, L. (2017). The integrity challenge of the internet-of-things (IoT): On understanding its dark side. *Journal of Marketing Management, 33*(1–2), 145–158.

Ejaz, W., & Anpalagan, A. (2019). Internet of things for smart cities: Overview and key challenges. In *Internet of Things for Smart Cities* (pp. 1–15). Springer.

Elkhatib, Y., Porter, B., Ribeiro, H. B., Zhani, M. F., Qadir, J., & Rivière, E. (2017). On using micro-clouds to deliver the fog. *IEEE Internet Computing, 21*(2), 8–15.

Fleisch, E. (2010). What is the internet of things? An economic perspective. *Economics, Management, and Financial Markets, 5*(2), 125–157.

Främling, K., Kubler, S., & Buda, A. (2014). Universal messaging standards for the IoT from a lifecycle management perspective. *IEEE Internet of Things Journal, 1*(4), 319–327.

Gassmann, O., Böhm, J., & Palmié, M. (2019). *Smart cities* (pp. 25–66).

Gram-Hanssen, K., & Darby, S. J. (2018). "Home is where the smart is"? Evaluating smart home research and approaches against the concept of home. *Energy Research & Social Science, 37*, 94–101.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660.

https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html. Accessed on 22 Aug 2019.

https://www.ericsson.com/en/future-technologies/future-iot. Accessed on 22 Aug 2019.

https://www.pocket-lint.com/apps/news/126559-internet-of-things-explained-your-complete-guide-to-understanding-iot. Accessed on 25 Aug 2019.

https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/. Accessed on 25 Aug 2019.

Ishimori, A., Farias, F., Cerqueira, E., & Abelém, A. (2013, October). Control of multiple packet schedulers for improving QoS on OpenFlow/SDN networking. In *2013 Second European Workshop on Software Defined Networks* (pp. 81–86). IEEE.

Jayaram, A. (2017). *Smart retail 4.0 IoT consumer retailer model for retail intelligence and strategic marketing of in-store products*.

Kanchana, S. (2018). IoT in Agriculture: Smart farming. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 181–184.

Karimi, K., & Atkinson, G. (2013). *What the Internet of Things (IoT) needs to become a reality*. White Paper, FreeScale and ARM, pp. 1–16.

Khatiwada, A. (2018, August). *Smart Grid*.

Kim, O. T. T., Tri, N. D., Tran, N. H., & Hong, C. S. (2015, August). A shared parking model in vehicular network using fog and cloud environment. In *2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS)* (pp. 321–326). IEEE.

Kobayashi, M., Seetharaman, S., Parulkar, G., Appenzeller, G., Little, J., Van Reijendam, J., Weissmann, P., & McKeown, N. (2014). Maturing of OpenFlow and software-defined networking through deployments. *Computer Networks, 61*, 151–175.

Kodali, R. K., Jain, V., Bose, S., & Boppana, L. (2016, April). IoT based smart security and home automation system. In *2016 international conference on computing, communication and automation (ICCCA)* (pp. 1286–1289). IEEE.

Kumar, D., & Mufti, T. (2017). On line learning: Worth knowledge base or just money waste. *Review of Business and Technology Research, 14*(2), 174–178.

Mardacany, E. (2014). *Smart cities characteristics: importance of built environments components*. In IET Conference on Future Intelligent Cities, pp. 1–6.

McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., Shenker, S., & Turner, J. (2008). OpenFlow: Enabling innovation in campus networks. *ACM SIGCOMM Computer Communication Review, 38*(2), 69–74.

Mufti, T., Sami, N., & Sohail, S. S. (2019). A review paper on Internet of Things (IOT). *Indian Journal of Applied Research, 9*(8).

Munir, A., Kansakar, P., & Khan, S. U. (2017). IFCIoT: Integrated fog cloud IoT: A novel architectural paradigm for the future internet of things. *IEEE Consumer Electronics Magazine, 6*(3), 74–82.

Nogueira, V., & Carnaz, G. (2019). *An overview of IoT and healthcare*.

Nunes, B. A. A., Mendonca, M., Nguyen, X. N., Obraczka, K., & Turletti, T. (2014). A survey of software-defined networking: Past, present, and future of programmable networks. *IEEE Communications Surveys & Tutorials, 16*(3), 1617–1634.

Pantano, E., & Timmermans, H. (Dec. 2014). What is smart for retailing? *Procedia Environmental Sciences, 22*, 101–107.

Patil, S., Patil, V., & Bhat, P. (2012). A review on 5G technology. *International Journal of Engineering and Innovative Technology (IJEIT), 1*(1), 26–30.

Reitblatt, M., Canini, M., Guha, A., & Foster, N. (2013, August). Fattire: Declarative fault tolerance for software-defined networks. In *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking* (pp. 109–114). ACM.

Repko, J., & DeBroux, S. (2012). *Smart cities literature review and analysis*.

Rindos, A., & Wang, Y. (2016, October). Dew computing: The complementary piece of cloud computing. In *2016 IEEE International Conferences on Big Data and Cloud Computing (BDCloud), Social Computing and Networking (SocialCom), Sustainable Computing and Communications (SustainCom) (BDCloud-SocialCom-SustainCom)* (pp. 15–20). IEEE.

Sheela, K. S., Sheela, A., & Chakravarthi, D. (2019). *Smart farming with e: Technology* (pp. 32–35).

Singh, J., Pasquier, T., Bacon, J., Ko, H., & Eyers, D. (2015). Twenty security considerations for cloud-supported internet of things. *IEEE Internet of Things Journal, 3*(3), 269–284.

Sohail, S. S., Siddiqui, J., & Ali, R. (2012). Product Recommendation Techniques for Ecommerce-past, present and future. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 1*(9), 219.

Sohail, S. S., Siddiqui, J., & Ali, R. (2014, December). Ordered ranked weighted aggregation based book recommendation technique: A link mining approach. In *2014 14th international conference on hybrid intelligent systems* (pp. 309–314). IEEE.

Sohail, S. S., Siddiqui, J., & Ali, R. (2017). A novel approach for book recommendation using fuzzy based aggregation. *Indian Journal of Science and Technology, 8*, 1–30.

Sohail, S. S., Siddiqui, J., & Ali, R. (2018a). An OWA-based ranking approach for university books recommendation. *International Journal of Intelligent Systems, 33*(2), 396–416.

Sohail, S. S., Siddiqui, J., & Ali, R. (2018b). Feature-Based Opinion Mining Approach (FOMA) for improved book recommendation. *Arabian Journal for Science and Engineering, 43*(12), 8029–8048.

SR, M. B. (2015). Automatic smart parking system using internet of things (IOT). *International Journal of Scientific and Research Publications*, 628.

Tsiatsis, V., Karnouskos, S., Höller, J., Boyle, D., & Mulligan, C. (2019). *Smart Grid* (pp. 257–268).

Wang, L., et al. (Apr. 2010). Cloud computing: A perspective study. *New Generation Computing, 28*, 137–146.

Wang, Y., Zhang, Y., & Chen, J. (2016). SDNPS: A load-balanced topic-based publish/subscribe system in software-defined networking. *Applied Sciences, 6*(4), 91.

Wijaya, R., Setijadi, A., Mengko, T. L., & Mengko, R. K. L. (2014). Heart rate data collecting using smart watch. In *2014 IEEE 4th International Conference on System Engineering and Technology (ICSET), 2014* (Vol. 4, pp. 1–3).

WijerathnaYapa, A. (2019). *The rise of smart foods* (p. 168).

Yassine, S., Singh, M. S. H., & Muhammad, G. (2019). IoT big data analytics for smart homes with fog and cloud computing. *Future Generation Computer Systems, 91*, 563–573.

Zhang, B., Mor, N., Kolb, J., Chan, D. S., Lutz, K., Allman, E., Wawrzynek, J., Lee, E., & Kubiatowicz, J. (2015). *The cloud is not enough: Saving IoT from the cloud*. In 7th {USENIX} Workshop on Hot Topics in Cloud Computing (HotCloud 15).