Wireless Personal Communications (2019) 108:363–388
https://doi.org/10.1007/s11277-019-06407-w

IoT Technology, Applications and Challenges: A Contemporary Survey

S. Balaji[1] · **Karan Nathani**[1] · **R. Santhakumar**[1]

Published online: 25 April 2019

Abstract
Internet of things (IoT) is a very unique platform which is getting very popular day by day. The very reason for this to happen is the advancement in technology and its ability to get linked to everything. This feature of getting linked has in itself provided multiple opportunities and a vast scope of development. The fact that technology in various fields has evolved through the years, is the reason why we observe a rapid change in the shape, size and capacity of various instruments, components and the products used in daily life. And this benefit of simplified technology when accompanied by a platform like IoT eases the work as well as benefits both the manufacturer and the end user. The Internet of Things gives us an opportunity to construct effective administrations, applications for manufacturing, lifesaving solutions, proper cultivation and more. This paper proposes an extensive overview of the IoT technology and its varied applications in life saving, smart cities, agricultural, industrial etc. by reviewing the recent research works and its related technologies. It also accounts the comparison of IoT with M2M, points out some disadvantages of IoT. Furthermore, a detailed exploration of the existing protocols and security issues that would enable such applications is elaborated. Potential future research directions, open areas and challenges faced in the IoT framework are also summarized.

Keywords IoT · Smart cities · Agriculture · Life saver · Industry · Protocols · Security

1 Introduction

IoT is a dynamic network framework which intends to coalesce the physical and the virtual domains by utilizing the internet as the medium for communication and transmission of data between them [1]. Physical and virtual worlds are perfectly amalgamated into one big data network with the usage of communication protocols in the self-configuring IoT infrastructure. It has been characterized as an arrangement of interrelated computing gadgets, mechanical and electronic machines, articles, creatures or individuals that are furnished

✉ S. Balaji
sbalaji@vit.ac.in

Karan Nathani
karannathani22@gmail.com

[1] School of Electrical Engineering, VIT University, Vellore, India

with one of a kind identifiers and the ability to exchange information over a system without requiring human -human or human–machine interaction. IoT is a coming of age revolution affecting millions of lives worldwide which aims at autonomously operating devices without human intervention while establishing the machine to machine (M2M) communication. The interconnection of objects at anytime, anyplace for anything by usage of any smart network has always been the vision of IoT [2].

The label "Internet of Things" was formulated in 1999 by Kevin Ashton and since then this ubiquitous connectivity network has paved its way into our day-to-day lives and have been vividly used in real world applications like defence, medicine, industry, agriculture, energy and for the making of smart cities, homes and devices. With the use of internet and artificial intelligence it is making our world smarter while minimizing the manual efforts and being more and more human-friendly. The fundamental idea of an IoT system is the trade of data between machines which are elicited by cutting edge technologies like WSN (Wireless Sensor Networks) and RFID (Radio Frequency Identification) with usage of sensing devices with effective decision making skills and intelligent algorithms after which an action is performed accordingly. IoT systems are deployed successfully by enabling telecommunication interfaces with the internet in devices like sensors and actuators with storage and processing sections for successful interactions between machines. With the comfort it offers, this new paradigm also comes with some privacy and security issues which needs to be rectified for its proper utilization and functioning [3]. The Internet of Things (IoT) forms a processing idea that portrays a future where regular physical items will be associated with the Internet and will be capable to recognize themselves to different devices.

RFID which was first introduced in 1945 is a prerequisite of IoT. It is a programmed innovation which helps machines and digital devices to recognize objects, record metadata and control singular target through radio waves [4]. Normally, a RFID framework comprises of tags and readers [5]. The tag is a microchip associated with a receiving wire, which can be connected to any object as a unique identifier. With the utilization of radiowaves, there is a phase of communication between the RFID's reader and its tag which helps in the autonomous identification and classification of the object. Other than RFID, there are varied types of technologies used in IoT like WSN, Electronic Product Code (EPC), Bar Code, ZigBee as well as Bluetooth which uses low energy source and its one of the most convenient and popular IoT enabling technology. Currently, there are about 25 billion devices interconnected by the IoT which would ragingly grow to about 60 billion by the year 2025.

IoT forms a cyclic phenomenon which combines the usage of sensors to create a connection and sense the user and a network to communicate with a person as it further aggregates the standards and provides a machine with augmented intelligence which helps it to analyse, behave and act according to the situation. The action, creation, communication, aggregation and the analysis of a device are the combined functions which makes it interconnected to IoT by establishing an augmented intelligence for it and making it a Smart device. This IoT process operates in a cycle with everything interdependent on one another for its successful execution. Brief IoT Constituents elements are shown in Fig. 1.

The motive of our research is to identify the breadth, depth and diversity of present research in IoT. As a result, enormous number of research publications in journals and conferences are found associated with IoT. To illustrate the ongoing research work, we filtered the number of publications from 2013 to 2018 through scopus database. Figure 2 displays the number of publications in emerging applications of IoT. It indicates a trend towards popular research in IoT. The explosive growth of IoT technology opens many engineering

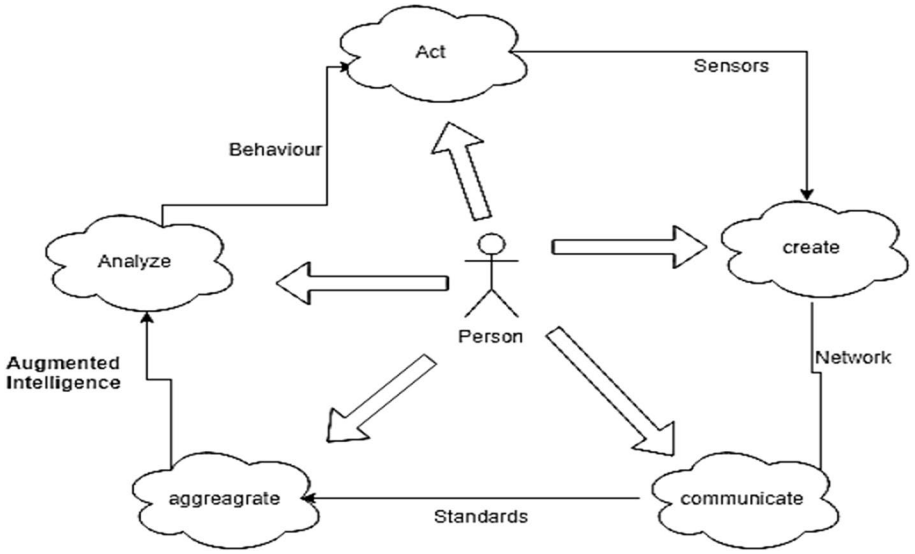

Fig. 1 Constituent elements of IoT

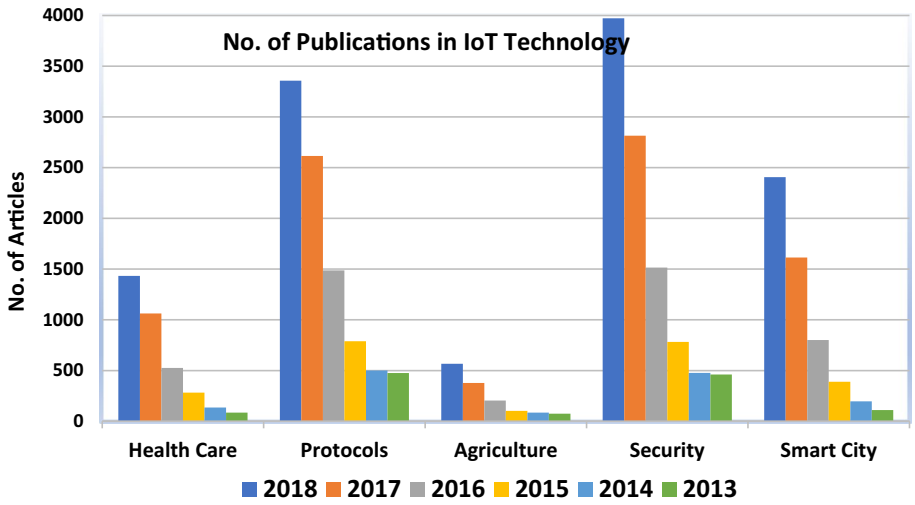

Fig. 2 Number of publications in IoT protocols, security and emerging applications

and scientific opportunities and problems. It calls for greater research efforts from various sectors like academic, industry, etc. The combined efforts of these sectors should necessarily advent new protocols, architectures, and services which are in dire needs to take up the challenges of IoT. The scopus data base contain large number of publications that use IoT technology for various applications. Figure 3 displays the distribution of articles by year wise. It is found from the Fig. 3 that the number of publications has increased over the recent years and the number rises almost exponentially from 2013 to 2018.

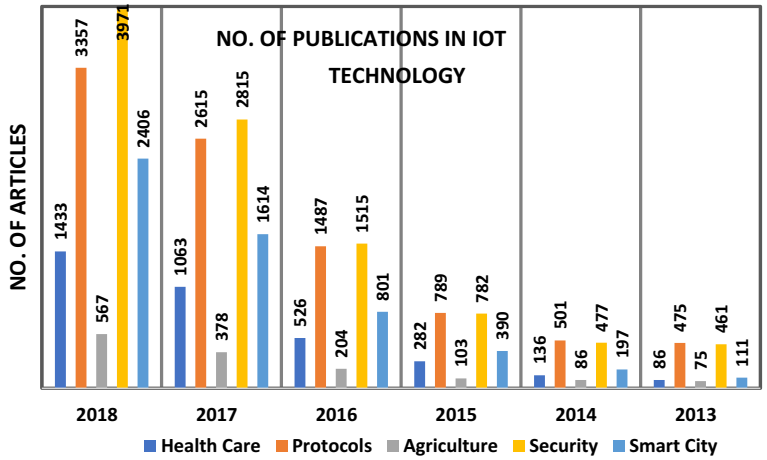

Fig. 3 Distribution of articles by publication year wise

Having recognized the advances in IoT technology and emerging applications, our motivation in this research review is to explore the benefits, disadvantages, opportunities, challenges present in IoT technology, protocols and its applications. In the past many studies were conducted to review the IoT. Benefits and challenges of IoT in agriculture has been presented by Elijah et al. [1]. This survey does not detail on the types of protocols and implementation challenges faced in agricultural domain. In an effort to understand the progress of IoT in industries, key enabling technologies for IoT applications in industry were discussed in [4]. But M2M has not been addressed in the survey. Lin et al. [6] overviewed IoT with respect to system architecture, technologies, and security and privacy issues. However, the technologies for important applications like healthcare, agriculture has not been addressed in this survey. Goudos et al. [7] reviewed IoT technology starting from physical layer to application layer for smart city, transportation and healthcare applications. However security aspects present in these IoT protocols has not been addressed. In [8] healthcare technologies and healthcare solutions were discussed. But complete end to end healthcare application solution and IoT life save tools has not been explored. Highlighted the achievements in realizing various aspects of smart cities were presented in [9]. Moreover this survey address smart health management in smart cities but smart structural health management which equally important in smart cities has not addressed. Table 1 summarizes the survey efforts of above mentioned research works.

Our survey is different from the above listed survey. We have selected large number of research works and this article basically outlines and gives an overview on the life-changing phenomenon of IoT and varied technologies, challenges and real-world applications adhered to it which has revolutionized our world with its raging outlook. The contributions of paper are summarized as follows. In particular, first this paper conduct a comprehensive overview of IoT Technology with respect to RFID, enabling wireless sensor network technologies, antennas for IoT technology. Particularly, the difference between Machine to Machine (M2M) and IoT is explored first. Second, comprehensive survey on emerging protocols and contributions from the past works along with limitations are explored. This helps to provide legacy solutions for existing standards to emerging technologies. IoT security issues are explored and then security issues involved in various applications are

Table 1 Comparison of past surveys

References	Technology	Protocols	Security	IOT Life saver/health care	Applications		
					Smart city	Industry	Agriculture
[1]	✓		✓				✓
[4]	✓	✓	✓				
[6]	✓	✓	✓		✓		
[7]	✓	✓		✓	✓		
[8]	✓	✓	✓	✓		✓	
[9]	✓	✓	✓	✓	✓		

reviewed. Most importantly in-depth review of IoT life saver tools along with protocols, issues are presented. State of the art framework for several applications including Smart City, Agriculture, and Industry etc. from the conception phase to the deployment presenting their supported features and limitations are illustrated. Finally open issues, challenges and disadvantages of IoT related to the emerging applications scenarios are presented. The methodology of this survey is to illustrate the IoT technology, protocols, security issues and open issues for important applications of IoT.

The paper is divided as follows, it presents various technologies used in IoT in Sect. 2. Section 3 provides review of IoT protocols and in Sect. 4 security issues are reviewed in detail. It explicates multiple IoT- based lifesaver tools in Sect. 5. Further, it discusses various real time applications in Sect. 6 while the disadvantages and eventual challenges are furthermore explored in Sect. 7. Finally Sect. 8 summarizes the research paper which concludes this paper.

2 Technology in IoT

In IoT applications, it is mandatory to transmit the data generated by the devices or sources to the internet. Proving connectivity and coverage is a daunting task for IoT applications. The users or vendors always wanted to collect data and analyse it for further processing for better enhancement of their devices. It is necessary to properly advent new technologies for communicating and processing the data. Rather than going to other network, a better privileged network especially for its own applications would be a good choice. Nowadays, the industries are actively involved developing wired or wireless communication channels or protocols. But the cost and infrastructure development plays a vital role in developing technology for IoT. The technology embedded in IoT is shown in the Fig. 4. The brief description of each of these items are described next.

2.1 RFID

RFID mainly focusses on Near field communication and Radio-Frequency identification. In last 2 decades' different companies are desperately working on Internet of things. At the time of 2nd World War, Radio-Frequency identification originated. It was impressive around Second World War. Radio frequency identification was helpful to determine if whether the fighters were "friend or foe". Radio-Frequency Identification

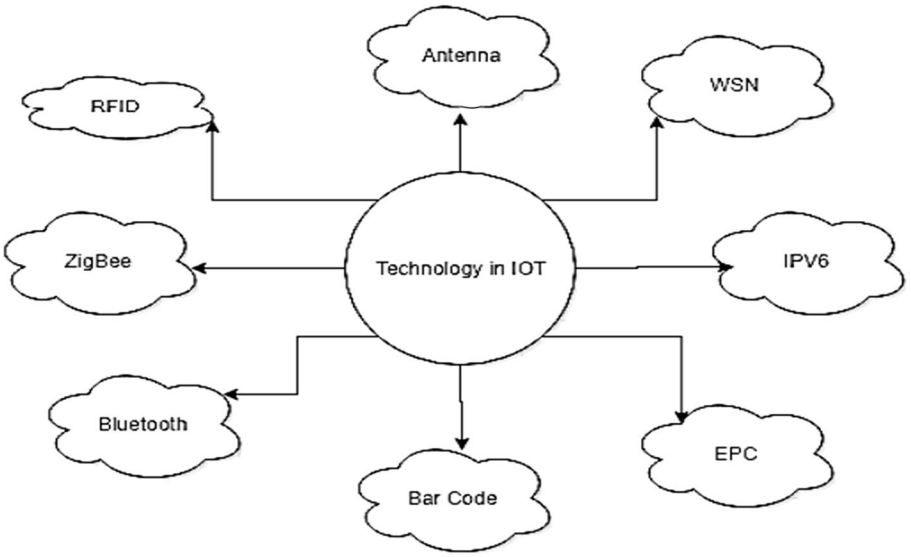

Fig. 4 Technology embedded in IoT

(RFID) is the utilization and identification of radio waves and exploitation of the same to pursue and catch the data [10]. A tag can be chased, followed or pursued from up to a small distance and does not need to be inside direct viewable pathway for the information to be exploited by the pursuer.

The main component of RFID is RFID tag. The transducer also plays a role of RFID tag. An antenna, a chip and some memory is comprised in this tag. The transducer includes transmitter and responder, and we can identify tags in two forms. The two forms are active and passive RFID. The Active and Passive RFID which are differentiated on the basis of power source.

Active RFID frameworks utilize battery-controlled RFID tag that ceaselessly communicates their own particular signal. Active RFID tag is regularly utilized as "reference points" to precisely track the constant area of advantages or in rapid conditions. The read range of active RFID tag is much longer than uninvolved tags [11] the reason being the extra power given by the battery, however, they are more costly.

Passive RFID frameworks utilize tags with no inward power source and are rather fuelled by the electromagnetic energy transmitted from an RFID per user [12]. These tags are further utilized for applications like to control, record following, race timing, brilliant marks, and the sky is the limit from there on. The lower value point per tag makes utilizing the inactive RFID frameworks more efficient for many such ventures.

Electronic Product Code (EPC) is also used in RFID. EPC can be recorded on RFID tag for an improvement in barcode system. It generates the unique code number which specifies the product's specification or information. In MIT University, at around 1999 Auto ID centre developed EPC. Some systems are developed with barcode. Its combination of bars spaces with the difference of some width, in 1995 for trademark the QR (quick response) created, for the very first time in Japan automotive industry matrix barcode designed which records the information related to products. It can read by camera or scanner.

Table 2 Frequency ranges for RFID antenna

Particulars	Low-frequency Type	High frequency	Ultra-high frequency
Frequency range	125–134 Hz	13.56 MHZ	865–960 MHZ
Distance range	1–10 cm	1–100 cm	About 1-m
Important uses	Use in animal tracking, it does not get affected water or metal	It uses in access control applications, data transmission and for passport security	In asset tracking and in laundry management

2.2 RFID Antenna

The RFID apparatus engenders the wave in both vertical and flat measurements. The field scope of the wave and furthermore its signal quality is in part controlled by the quantity of degrees. While the higher number of degrees implies a greater wave scope design, it eventually bring down the quality of the signal. By giving an empowering RF signal, a person can speak with a remotely found device that has no outside power source, for example, a battery. The RFID radio wires can be divided into two classes: the tag and the reader antenna.

First tag antenna is described. It has a tendency to collect energy for turn it on the channel. It consists of a property which advances on the fact that the collection of energy is greater if the area of the respective tag antenna is larger and vice versa. Tag antenna can be produced using an assortment of materials. They can be printed, scratched, or stamped with conductive ink, or even vapor kept onto labels. The tag antenna not only transmits the wave conveying the data put away in the tag, yet in addition to that it also needs to get the wave from the person to supply vitality for the tag operation. Tag antenna ought to be little in size, minimal in effort, and simpler to manufacture for large-scale manufacturing. By and large, the tag reception apparatus ought to have omnidirectional radiation or hemispherical scope. For the most part, the impedance of the label chip isn't 50 ohm, and the radio wire ought to understand the conjugate match with the label chip straightforwardly, so as to supply the greatest energy to the label chip. Tag antenna apparatus might be a signal turn or numerous turns as appeared here.

Like tag antenna, the reader antenna must also work properly. For changing from electric current into electromagnetic waves the reader antenna is used. Where into space, the tag antenna receives the waves and converts them back into electric current. Radio frequency identification uses different frequency for different purposes which are listed in Table 2.

2.3 Problems with RFID Standards

RFID Standards can be effectively disrupted. Since RFID frameworks influence utilization of the electromagnetic range (like Wi-Fi systems or cell phones), they are moderately simpler for utilizing energy at the correct frequency despite the fact that this would just be a burden for consumers in stores (longer holds up at the checkout). They could be deplorable in some different times and situations. RFID is used and progressively utilized in the likes of hospital facilities as well as in the military and defence field [13]. Common problems with RFID-Reader collision is the Tag collision. The first thought of the Auto-ID Centre depends on RFID tags and interesting recognizable proof by the Electronic Product Code

(EPC) [14], however, this has developed into objects having an IP address. On another hand, the universe of the Semantic Web concentrates rather on making all things (not only those electronic, brilliant, or RFID-empowered) addressable by the current naming conventions, for example, URI. The coming generation of internet technology would be able to communicate virtually by using the Internet protocol vision 6(IPV6) as it contains large address space. For identify objects in our industry in logistic transportation by IPV6.

2.4 Wireless Sensor Network

The advancement of wireless sensor networks (WSN) was inspired by military applications, today, they comprise of appropriated free gadgets that utilizes the sensor to screen the physical conditions with their applications stretched out to the industrial infrastructure, robotization, wellbeing, activity, and numerous customer regions. Wireless sensor network is part of the IoT class. Reconfigurable homogeneous or heterogeneous network scenarios like automatic network management is the need of the hour for IoT [15].

For IoT and wireless sensor networks short range communication Bluetooth is most preferred. This is one of the effective wireless technologies which allows to the transfer the data in a short range around 10–100 m, between devices such as mobiles, PCs, cameras etc. and generally the communication speed is less than 1 Mbps. In 1994 one mobile communication company invented this Bluetooth. It was created for personal area network, and later piconet was invented which was a set of 2–8 Bluetooth devices. When it comes to the enhancement of the features of wireless sensor network and IoT, the protocol which was created was named as ZigBee. It was founded in the year 2001. ZigBee has a flexible protocol design and is used in short transmission ranges. ZigBee covers the distance of 100 m and a bandwidth of 250 kbps.

2.5 Machine to Machine

IoT and Machine to Machine (M2M) are often considering as identical but their lies a huge difference between them. IoT is also equally plays huge role in today's integration of machine and man like M2M. The detailed difference between IoT and M2M is depicted in Table 3.

3 Protocols Used in IoT

Many IoT standards are proposed to facilitate and simplify application programmers' and service providers' jobs. Different groups have been created to provide protocols in support of the IoT including efforts led by the World Wide Web Consortium (W3C), Internet Engineering Task Force (IETF), EPC global, Institute of Electrical and Electronics Engineers (IEEE) and the European Telecommunications Standards Institute (ETSI) [10]. IoT protocols are used based on the application area and not all protocols are used everywhere. In fact, most protocols are not used for WSN's where the main idea is to have a protocol that can allow for energy efficient data transmission and communication between sensor nodes.

These protocols are different and are varied by the layer in which they are used. Each layer in the OSI model uses different protocols to achieve a different purpose in an IoT enabled network. Application layer protocols range from Constrained Application

Table 3 Difference between IoT and M2M

IoT	M2M
IoT connects a computer with "things", systems and people. Things include-machine, sensors, products and many more	It connects "things" to a computer [16]
IoT is generally connected to cloud which makes it a scalable and flexible solution	M2M communications which require an installation of SIM cards or drawing a fixed line
IoT support a variety of devices, passive sensors, and sensors with less strength and cheap devices that may or may not be supported by M2M	M2M only supports devices
IoT focus towards software solution or IP network	M2M communication is primarily oriented towards an embedded hardware [17]
IoT is considered a broader concept as it might point towards company's success [18]	M2M in this example points towards maintenance
Horizontal connection IoT uses. The connection of objects/devices to a cloud or user platform	Point-to-point communication (vertical)

Protocol (CoAP), Message Queuing Telemetry Transport (MQTT) and Hypertext Transfer Protocol (HTTP) REST protocols to enable energy efficient communication between devices. Bluetooth Low-Energy (BLE) [19] can also be used to transfer data over short ranges. These protocols use a variety of Communication models and these protocols are used mainly for user-centric applications like Home Automation or for WSN's where energy is scarce.

A main challenge in IoT protocols are those used for messaging purposes [20]. Messaging purposes can be used to communicate between devices and to send/receive messages between sensor nodes in a WSN. Many protocols have been developed over the years for messaging purposes but a single protocol has not met the needs and requirements for an IoT system. These protocols like MQTT, CoAP are mainly used in energy efficient networks and work based on different Communication models. There are various advantages and disadvantages to these protocols and each protocol can be applied in a different area. But, these protocols have not been combined and moreover, cannot be combined due to the difference in standards between them. If these protocols were combined in some way to reduce the shortcomings of each and account for the disadvantages each protocol faces, then we would have a protocol which can potentially satisfy the needs of an average IoT system.

Protocols used frequently are the messaging protocols used for low power devices [21] like MQTT, CoAP and IPv6 over Low Power Wireless Personal Area Network (6LoWPAN). The focus of previous research works on MQTT and CoAP protocols along with limitations and gaps are given in Table 4. These protocols are frequently used in IoT networks for devices with low energy and bandwidth. With an increasing number of connected devices, IoT systems are expected to handle the communication between these devices [22].

Therefore, state of the art systems are required to allow for these communications. Industrial IoT is one of the concepts that will rise in the next decade. The ability for devices to be connected in an industry is one of the main concepts in Industry 4.0 [23]. Industry 4.0 is the next industrial revolution which involves automation and IoT as one of the main concepts. It aims at automating the entire manufacturing process with

Table 4 Comparative analysis of MQTT and CoAP protocols

Protocol	Focus	References	Contribution/Methodology	Limitations/Gaps
MQTT	Security	[24]	Proposed AugPAKE algorithm for authentication and authorization	Energy consumption and latency of message exchange to be analysed
	Quality of service (QoS)	[25]	Authorization and authentication using OAug 2.0 and HMAC with one time password	Static tokens are used
		[26]	Enhanced MQTT with hybrid architecture for M2M, M2S and S2S	Enhanced MQTT in different deployment scenarios to be investigated
	Power aware implementation	[27]	Strong crypto algorithms in MQTT	Strong overhead in the usage of RAM memory
		[28]	Resource consumption experiment for MQTT	Participating devices trust each other which is not in real time
CoAP	QoS	[29]	Dynamic mode selection scheme that extends battery life time	Latency is not taken into account
		[30]	Capacity limits of a single IoT domain against cluster size, inter observation time etc.	Freshness of data is a major concern
		[31]	Performance analysis of CoreCoAP for congestion control	More memory per CoAP client
	Implementation	[32]	Possible design approaches for IoT domains that run CoAP and interface to the internet through a proxy containing a data cache	Optimal choice of protocol parameters under different application scenarios
		[33]	Functionality of CoAP are modified for better IoT (CoAP 2.0)	Implemented with integers and floating point systems

almost no human intervention. This leads to faster and more productive manufacturing with large volumes of products being manufactured every single day.

One of the major risks in IoT protocols remains that of security. Next we discuss the challenges present in the IoT security.

4 Challenges in IoT Security

As the basic principle of IoT involves connecting devices, it makes everything addressable and locatable which in turn makes our life easier [34]. However, making everything connected to internet opens the door for hackers. Without proper confidence about privacy and security, user will not be attracted towards IoT [3]. So, it must have a strong infrastructure dealing with security and some of the issues that IoT might face are listed below.

The primary issue the IoT facing is unauthorized Access to RFID. The RFID tags can contain any sort of information and as RFID tag can be easily modified or read by the reader. This opens a whole bunch of threat for the user as the data can be easily accessed by a miscreant reader [35]. Wireless sensor networks security breach sensors node in IoT are bidirectional. Acquisition of data is also possible other than transmission. In this scenario, some of the possible attacks include tampering where the data in the node can be extracted or altered. Next flooding creates a whole lot of problems in IoT.

Flooding the name suggests, it explains when traffic amount is high and exhaustion of memory takes place. Sybil attack wherein multiple pseudo identities are claimed for a node in order for it to give big influence. Security issues from Android where once when we connect IoT to an android, unlike IOS android it is an open source network which means it can easily be discovered. Once the front end devices are compromised, the IoT network is exposed. Software updating problem is usually faced by the developers because of high cost and memory, they do not update their software and devices. Once the hackers discover the devices, they can be easily accessed. Cloud Computing in IoT is a big network that allows sharing of resources and some of the security threats faced by shared resources are listed below.

Data loss happens when any miscreant user having unauthorized access can modify or delete the data. Cloud computing can also be used for controlling other devices, once the hackers get hold of an account it can upload certain software's which will give him control of any devices that come in contact. The Man-in-the-middle (MITM) the hacker works as a third person and can intercept or alter any message.

5 IoT Lifesaver Tools

These are the tools that have proved to be saving a lot of lives related to the road safety as well as many other major issues. Bumblebee is an IoT system particularly aiming for road safety. Primarily, it autonomously detects the danger and communicates with the nearby cars to give way to the driver with reference to the issue. Also a message is sent to traffic control centre about the position and the threat related issues, it works on the priority system, i.e. in case of multiple threats or victims the one whose priority is high will be sent first. It will help in passing the way to ambulance, notifying people about any mad driver or thief and many more. HAPIfork is an electronic fork designed as a health aid. Basically, it keeps tracks of how you eat rather then what you eat, it notifies the user whenever

the user's eating rate is too fast with the help of vibration, after the completion of food, the data is uploaded online for the user to compare or for sending it to the coach. It also assesses and tracks progress of daily workout targets.

BigBelly is a platform deployed in public, it offers many services such as smart waste and recycling. Alerts authority when the bin is full or when the waste in particular area is high than the set limit. Airqualityegg is an application that monitors the air pollution and notifies the authority when it crosses a certain threshold value. Air casting Platform dedicated to sharing health and environment data. Heat Watch IoT does not only aims to help rich people but this solution monitors and record the activity of animal which in term help farmers to decide over breeding and many critical issues. iGlucose furnishes individuals living with diabetes an advantageous and inexpensive diabetes care solution, and medicinal services experts with an ongoing perspective of blood glucose information and patterns. ADAMM is an IoT device for people suffering from asthma. Its fundamental aim is to quantify breath patterns, cough rate, heartbeat, temperature and other body information. The gadget issues warning if any of the parameters go above normal. Moreover, it reminds to take medicine and guarantees that the inhaler is used routinely.

There is a new IoT lifesaver tool Proteus Discover which is a mix of a cell phone application and an edible sensor that patients swallow together with their medicines. Utilizing edible sensors into which pills can be embedded, can give specialists full perception into their patients' restorative consumption schedules and issue fitting warnings at whatever point the recommended routine is broken. Insight robotics21 is a forest fire detection system. Smart Traffic ParkSight is an application which guides the driver towards the available parking slots. Vigo Smart Headster is an IoT tool which is used to prevent driver fatigue accidents. As soon as it senses that the driver is sluggish, it vibrates, makes sounds, flickers light, and even call a friend with the end goal of increasing alertness and expanding brain activity. There are some other tools includes smart lightening, Smart A/C, Smart Washing machines, Smart garbage cans etc. works as IoT life save tools. Some of the recent works of life saving areas of IoT in health care systems are reviewed in the Fig. 5.

6 Applications

The only thing that separate human from other living being is curiosity. We humans are curious and we question a lot which results in advancement in every field that connects or affects our life in any way. IoT which is also considered as fourth industrial revolution brings a whole lot of application and promises to reshape industries into next level. Some of the recent works in important areas of wellbeing of people are tabulated in the Table 5.

6.1 Medical Field

IoT health care is still considered as the sleepiest or least developed, researchers have shown that in coming years the giant will get awaken. It will not only be affecting companies but will also change the life of people. Some of the present applications in the medical field are listed below.

Ultraviolet Radiation monitors the level of UV radiation in different areas and notifies the people about the area having high radiations [57]. Medical freezers monitors the things kept under it, for example, monitor the temperature of the medicines and adjusting its temperature accordingly. All detection tracks the activity of people with disabilities or

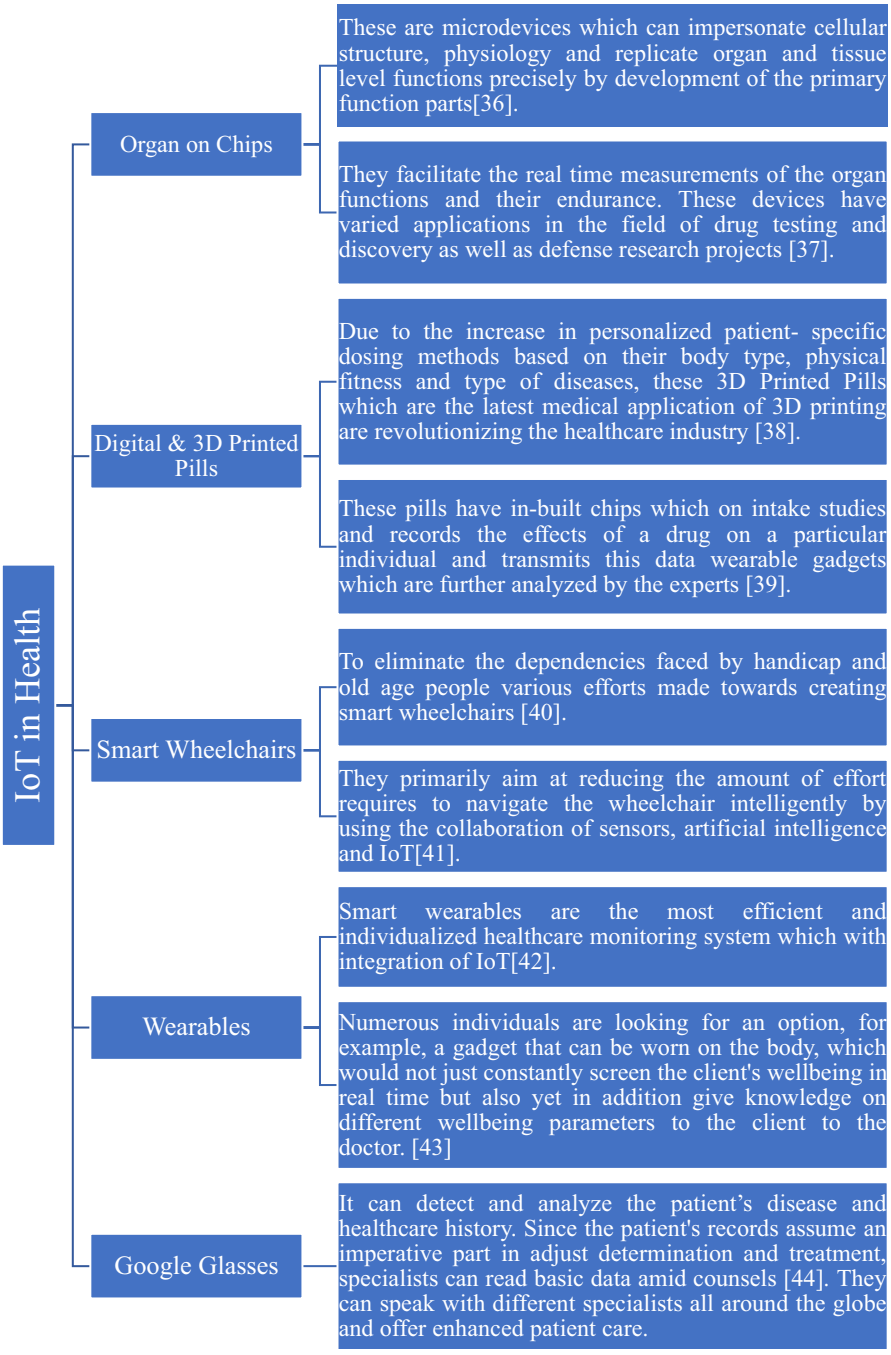

Fig. 5 Some important IoT lifesaver works in health

Table 5 Review of some recent works in smart applications

Safety	Pollution/Air Quality	Waste Management
Path planning and mapping model for mobile robot applications. Stereo vision strategy using bumblebee camera for optimization [45]	Low cost air, particulate matter, and metrological sensor based pollution monitoring in IoT environment is proposed [53]	Dynamic routing algorithm for solid waste disposal is proposed. Reduces the operational cost [49]
Channel allocation optimization in connected vehicle networks [46]	Real time high quality of air monitoring maps of indoor and outdoor of buildings using zigbee protocol was presented [54]	Genetic algorithm based route management for waste collection system is presented [50]
Wheelchair movement selection between landmark positions for patients [47]	Pollution aware approach by switching between electric and conventional propulsion system was described. Switching is optimized based on pollution information and pollution zones [55]	Smart and Green System (SGS) was proposed to integrate sensors, vehicles and crews in sustainable waste management environment [51]
Bumblebee based control area bus is adopted to connect LED display modules in flight arena systems [48]	Characterized the fog computing network in terms of CO_2 emissions for IoT environment [56]	Waste bin monitoring with ultrasonic sensors and RFID technology is used [52]

old age people living independently. Sportsmen Care monitors the activity of a sportsman and notify when seeing any fall in performance and patients surveillance. To reduce the respiratory problems of citizens and emerging privacy issues while adopting smart health management was discussed [58].

6.2 Industrial Control

Indoor Air Quality monitors the amount of oxygen present in air as well as the presence of toxic gases. Ozone Presence monitors the presence of ozone in food industry while the process of drying meat. Safety systems are machines involving large blades or high-pressure compression are covered by curtains with sensors if worker hand by mistake enter the area the whole system will stop. RFID tags system are employed in assemble branch where the container containing part to be assembled next is indicated with the help of bulb over the container. These systems help to keep track whether the parts are assembled in the right order or not. Tracking is employed for the tracking of goods and updation with the real-time data.

6.3 Domestic and Home Automation

With IoT being a hot topic and creating buss smart home is the most searched or user interested topic. The reason being the love and comfort of people towards their home and we all have experienced the irritation we feel after we are in bed to go to the switch and switch off the light. Well IoT solves this problem for you. Here are some IoT's application aiming toward home automation. Intrusion Detection Systems detects the condition of the window and doors and violations to prevent the user from any intruders. Remote Control Appliances controls the appliances with sensors to save energy and accidents [59]. Temperature and music control can feed the data of temperature and music preference of the members and you just have to say play songs or make me comfortable or something and it is all set. Energy and Water Use monitors the daily consumption of water and energy and suggests different ways to save them. Art and Goods Preservation monitors the condition inside warehouses and museum and suggest ideal conditions for better preservation.

6.4 Smart Cities

People continue to move towards cities the reason being good opportunities offered [60], this increases the population and in order to manage the increased population and the problems comes with that city needs to be smart. We all have experienced the irritation we feel when we spend hours waiting in jams [61]. The smell of improper disposal of waste in neighbourhood etc. All this problem will be solved with IoT. Some of the potential applications of IoT in smart cities are shown in the Fig. 6.

6.5 Security and Emergencies

We see a lot of news reading about the people who suffered in emergencies condition what if someone notifies you before it actually happened, won't it be nice? Well IoT will play the role of that someone in coming years. Here we discuss some of its application in securities and emergencies. Perimeter Access Control detects and controls the people activity inside

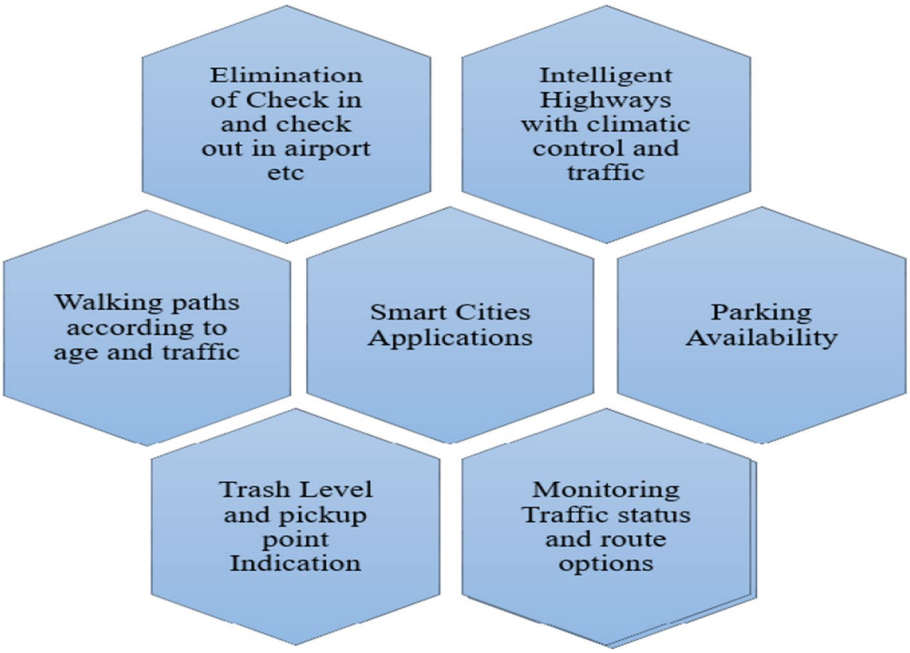

Fig. 6 Applications of IoT in smart cities

an unauthorized and restricted area. Radiation Levels are generally used in nuclear power plants or station to monitor the level of radiation in order to notify as soon as there is a leakage in the plant. Explosive and Hazardous Gases detects the level of gas in a chemical industry and notify as soon as a leakage is detected. Earthquake People suffer a loss of life and money when an earthquake hits, the system cannot save your money but it can save your life, it notifies as soon as it detects the presence of earthquake and guides you the safest and quickest way to exit. Definitely IoT plays a vital role in controlling these applications.

6.6 Smart Agriculture

With the continuous increase in the world population the production of the food has to be raised proportionally in order to provide basic food for each individual [62]. But from past years we have seen farmers committing suicide due to damage to their crop or loan. The government is doing everything in its power to help farmers. But with the help of IoT many problems can be solved. This is the main reason that's is why the government is more interested in advancement of smart agriculture using IoT [1]. Summary of certain important research contributions are compared in Table 6. Moreover in the summary, key performance indicators for different IoT domains are presented. The key performance indicators are vital for designing, deploying and commissioning the applications of IoT. More importantly the key performance indicators are usually measured and used to quantify the performance across the IoT domains.

Table 6 Comparison of some reviewed important research contributions

Topic/Area	IoT Domain	References	Key Performance Indicators
IoT technology	RFID	[10–12]	Scalability, Reliability, Roaming and mobility support, Large coverage, etc.
	WSN	[14, 15]	
	M2M	[16–18]	
Protocols	MQTT	[24–28]	Latency, Throughput, Congestion control, etc.
	CoAP	[29–33]	
Life saver tools	Organ on chips	[36, 37]	Memory, Security, Data freshness, Interoperability, etc.
	Wheelchairs	[40, 41]	
	Wearables	[42, 43]	
Applications	Waste management	[49–52]	Fault recovery, Routing, Energy and power, Safety, etc.
	Pollution/air quality	[53–56]	
	Smart cities	[60, 61]	
	Agriculture	[1, 62]	

Compost controls the level of temperature and humidity inside etc. to prevent any unwanted cause. Green Houses controls the climate condition in order to maximise the production. Meteorological Station Network studies or analyses the past atmospheric condition of whether to predict or forecast the future conditions. The security issues, protocols used and the enabling IoT technology for emerging application are tabulated in Table 7.

7 Challenges and Future Scope of IoT

Over the few decades, we have seen a lot of technical development, technologies change our lives. It has been responsible for making our lives full of resources available at our fingertip [65]. Out of the many technologies under development, IoT also known as M2M has successfully attracted a lot of audience towards it (here smart sensors collect real-time data and communicative with each other or with the internet to take necessary action), IoT being a technology offers both opportunities and challenges. M2M is generally broken down into four layers. First is sensor which collect real-time data and next the communication unit which is responsible for the transmission of data. The third computing unit is responsible for analysing the data and the service layer take necessary action after analysing the data [66]. This four components are essentially inherited in IoT also. The immediate important challenges IoT facing is listed in the Table 8.

But regardless of all the challenges faced, IoT is an innovation revolution with a predictive extravagant growth rate of 20.8 billion by 2020, it interconnects variegated gadgets, systems and people with its pervasive internet networking. The upcoming research, developments and projects in the field of IoT would boost up the standard of human lives and bring about substantial changes in areas of industrial, medical, defence, agriculture, homes as well as corporate world and businesses. For example, in India, about 120 organizations and 70% of the new companies are putting forth IoT empowered arrangements. From 2015 till now, around 60 million dollars has been devoted to resources into the IoT which has

Table 7 Illustration of IoT, protocol and security issue for emerging applications

Application	IoT Technology	Protocol	Security Issues
Life-saver	Bluetooth (high) WSN (high)	CoAP MQTT	Bluejacking, Warnibbling attack, Bluesnarfing, interoperability, high energy consumption, privacy threats
Healthcare	RFID (high) Bluetooth (very high) WSN (very high)	HTTP MQTT	Wireless network eavesdropping Bluejacking, car whisperer, Bluesnarfing energy issues, jamming, security attacks
Smart city	ZigBee (high) Bluetooth (high) Wi-Fi (very high)	MQTT CoAP	Bus pirate, sniffing attack and DoS attacks, Bluejacking, car whisperer, Bluesnarfing, wireless network eavesdropping
Industry	WSN (high) IPv6 (high) RFID (very high)	PROFINET OPC UA	Clandestine scanning, tracking, skimming and cloning, energy issues, ad-hoc networks, security attacks
M2M	ZigBee (high) Wi-Fi (very high) [2]	MQTT CoAP	Bus pirate, replay attacks and DoS attacks, energy issues and security attacks, interoperability
Structural health management	RFID (high) WSN (high)	Z-Wave [63] CoAP	Clandestine scanning, tracking, skimming and cloning, energy issues, ad-hoc networks, security attacks, interoperability
Agriculture	RFID (high) WSN (very high)	CoAP	Clandestine scanning, tracking, skimming and cloning, energy issues and security attacks, interoperability [64]

Table 8 The challenges faced by IoT

S. No.	Challenges Faced by IoT
1	As the customer and business demands of IoT change daily, the technology itself involve extensively connected devices because of which huge number of devices are involved here due to which the cost of servicing and maintenance will increase rapidly which will further position itself while causing imbalance in the economy of a country. One solution to this problem is to develop sensors or devices that require very less or no maintenance. This will reduce the cost of servicing and prevent certain economic situations
2	Also, most of the devices employed over here uses battery and as once the sensor is in the field, it is almost impossible to replace its battery which will lead to heavy power consumption and ultimately global energy crisis. Therefore, another challenge is designing sensors that do not require any battery change over lifetime which can be achieved by producing more devices which run on renewable sources of energy. One of the most recent one is integration of IoT with solar energy
3	As, internet is the soul of IoT and problems in internet connections would lead to poor service and inadequate performance of an IoT device. Almost all base station/gateways are designed with some limit of users that can access simultaneously when the count exceeds the limit, some user will not receive service. So, for IoT to be implemented successfully, fast, cheap and hassle-free internet should be established in a country
4	Self-configuration: IoT devices should be programmed in a way to suit a particular environment with user configuring it manually
5	The common communication standard stills remain a question to its development. As the aim of IoT is to be more user-friendly and also communicate easily with other connected devices. Due to this some common communication protocols which supports heterogeneity of networks and interoperability need to be established which are significantly easier for its user for its substantial development
6	Also, one of the major challenges faced by IoT is security, privacy and management of personal data. As, IoT is an interconnected platform all of the personal data is out there uploaded in the cloud which is highly vulnerable. If there is a glitch in security of IoT it will evidently compromise a person's privacy as well as security. This could be fixed by leveraging a safe gateway and developing protected algorithms and cryptographies for more secure environment

brought forth another method for working and living. It has changed the current market and business trends to more customer friendly and personalized services.

With the incorporation of IoT- consumers, businesses and industries are booming together and contributing each other by refining the productivity as IoT. The IoT services have made everything more user friendly with prefixing "SMART" in every intricate essence of our lives like SMART wearables, automobiles, homes and cities with efficient energy and money saving. It is provided by a cheaper and a healthier environment to the users. IoT is a vast concept as it not only helps in the tangible growth of an individual but of a country as a whole as booming industries help in a nation's economic growth. Moreover, advancements in healthcare services are cheaper, easier and patient-friendly, varied IoT defence schemes expands a country's security and sustainability. Development of smart cities which includes controlling of traffic using IoT, concepts like SMART wastage management and also effective energy and resources savings. But IoT is currently suffering from certain implementation issues like security, data management etc. which must be ameliorated for its full-fledged expansion and growth in the future. Some of the open issues for emerging applications is listed in Table 9.

Computational limitations, fog computing, security, deployment, scalability, signal acquisition and processing, memory management, interoperability and integration,

Table 9 Some open issues for emerging applications of IoT

S. No	Application	Some Open Issues/Areas
1	Agriculture	Health status of agricultural stocks, crops Supply chain management to bridge between demand and supply Forecasting weather conditions and protection of fields Integration of machinery with technology, protocols, communication etc.
2	Industry	Product life cycle and production control Smart sensing Solutions for latency and reliability mechanism Energy consumption and bandwidth
3	Smart city	Crowd monitoring and Guidance Threats, security and methodology for resilience to faults and Waste management and transportation Mobility management
4	Health	IoT for new diseases and disorders Nutrition management systems and devices Flexible electronics and mechanical devices Ambient assisted living

bandwidth efficiency, energy saving, communication technology, coverage and protocols etc. are still open issues/areas in IoT technology for various applications of today's world.

7.1 Disadvantages

Though IoT is having a large scope in almost all areas of our day to day applications. There are some disadvantages which hinders further implementation of the IoT systems at a faster pace. The main disadvantages of the IoT are listed in Table 10. The internet of things makes the physical objects in the real environment to be seen in cyber globe and offers the formation of smart systems and applications.

Networks of sensors, middlewares, digital communication and computing, protocols etc. led to expansion of interconnected devices. The advancement in communication, connection and integration helps to have lot of choices to choose devices and services. The variety of services and devices that provides similar functions lead to lookup and discovery. The discovery and categorization of similar devices and services causes the system to become more costlier and error prone. Addressing the disadvantages will allow next generation IoT to recognize and satisfy the information needs.

8 Conclusion

In this review, the technological standard required for implementation of IoT is discussed. Moreover, basic communication entities and networks which support IoT are also reviewed in such a way to foresee the problems of ideal implementation of IoT. IoT is also pitted against M2M to illustrate the similarities and difference between the technologies. Most importantly, recent advancements and potential applications in smart

Table 10 Disadvantages of IoT

S. No.	Disadvantages	Cause
1	Security and privacy can be greatly compromised	Since, large chunks of personal data relating to health, home, cars etc. are shared across varied devices and uploaded in the Cloud. The mis-management and leakage of this data could make the security and privacy of its user vulnerable as well as lead to various cybercrimes [67]
2	Excess power consumption and energy usage	As billions of devices are connected in IoT which are battery-operated and huge data transfers takes place between them, due to this there is an abundant consumption of power and energy which should be optimized for further expansion [68]
3	Unemployment of menial staff	In IoT, most of the work is done by fully-automated 'SMART' devices and there is minimal requirement of human resources which leads to unemployment of menial staff and on the long-run it can affect the economy of a country
4	Complexity	IoT is a complex concept. Any improper functioning or a bug in the software or hardware will create a lot of fuzz due to which its implementation, working and proper maintenance is quite toilsome [69]
5	Internet Bandwidth	IoT is nothing without a good internet bandwidth as for proper functioning a SMART device would require internet connectivity and lack of bandwidth would hinder the working of the device and affect the Quality of Service [67, 68]
6	Lack of flexibility and interoperability	Interoperability is characterized as the capacity of frameworks, applications, and services to work in a combined and predictable way but sometimes due to huge collection of data, there are some errors faced as well as many devices are not able to interconnect with one another which leads to inflexibility and flaws in the system [70, 71]

cities, agricultural environment and industrial control areas are also presented. Detailed review of IoT environment in life saver applications, protocols used for various applications, security issues involved in implementing the IoT is also demonstrated in this research. Future research directions, the implementation challenges and open issues are also reviewed for real time scenarios.

References

1. Elijah, O., Rahman, T. A., Orikumhi, I., Leow, C. Y., & Hindia, M. N. (2018). An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges. *IEEE Internet of Things Journal, 5,* 3758–3773.
2. Porkodi, R., & Bhuvaneswari, V. (2014). The Internet of Things (IoT) applications and communication enabling technology standards: An overview. In *2014 International conference on intelligent computing applications (ICICA)*, IEEE, pp. 324–329.
3. 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.
4. Amendola, S., Lodato, R., Manzari, S., Occhiuzzi, C., & Marrocco, G. (2014). RFID technology for IoT-based personal healthcare in smart spaces. *IEEE Internet of Things Journal, 1*(2), 144–152.
5. Da Xu, L., He, W., & Li, S. (2014). Internet of Things in industries: A survey. *IEEE Transactions on Industrial Informatics, 10*(4), 2233–2243.
6. 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*(5), 1125–1142.
7. Goudos, S. K., Dallas, P. I., Chatziefthymiou, S., & Kyriazakos, S. (2017). A survey of IoT key enabling and future technologies: 5G, mobile IoT, sematic web and applications. *Wireless Personal Communications, 97*(2), 1645–1675.
8. Alam, M. M., Malik, H., Khan, M. I., Pardy, T., Kuusik, A., & Le Moullec, Y. (2018). A survey on the roles of communication technologies in IoT-based personalized healthcare applications. *IEEE Access, 6,* 36611–36631.
9. Gharaibeh, A., Salahuddin, M. A., Hussini, S. J., Khreishah, A., Khalil, I., Guizani, M., et al. (2017). Smart cities: A survey on data management, security, and enabling technologies. *IEEE Communications Surveys & Tutorials, 19*(4), 2456–2501.
10. 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.
11. Singh, N., Bhatt, J., & Purohit, K. C. (2017). A survey on IoT and security issues of RFID. *International Journal of Engineering and Computer Science, 6*(4), 21061–21066.
12. Grosinger, J., & Bösch, W. (2014). A passive RFID sensor tag antenna transducer. In *2014 8th European conference on antennas and propagation (EuCAP)*, IEEE, pp. 3638–3639.
13. Suresh, P., Daniel, J. V., Parthasarathy, V., & Aswathy, R. H. (2014). A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment. In *2014 International conference on science engineering and management research (ICSEMR)*, IEEE, pp. 1–8.
14. Nie, X., & Zhong, X. (2013). Security in the internet of things based on RFID: Issues and current countermeasures. In *Proceedings of 2nd international conference on computer science and electronics engineering*, Vol. 162, No. 7.
15. Kazmi, A., Jan, Z., Zappa, A., & Serrano, M. (2016). Overcoming the heterogeneity in the internet of things for smart cities. In *International workshop on interoperability and open-source solutions*, Springer, Cham, pp. 20–35.
16. Kubo. (2014). The research of IoT based on RFID technology. In *2014 7th international conference on intelligent computation technology and automation*, Changsha, pp. 832–835.
17. Bhatia, S., Chauhan, A., & Nigam, V. K. (2016). The Internet of Things: A survey on technology and trends. *Information Systems Frontiers, 17,* 261–274.

18. Khalid, A. (2016). Internet of Thing architecture and research agenda. *Computer Science and Mobile Computing, 5*(3), 351–356.
19. Al-Sarawi, S., Anbar, M., Alieyan, K., & Alzubaidi, M. (2017). Internet of Things (IoT) communication protocols. In *2017 8th International conference on information technology (ICIT)*, IEEE, pp. 685–690.
20. Naik, N. (2017). Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. In *2017 IEEE international systems engineering symposium (ISSE)*, IEEE, pp. 1–7.
21. Kumar, S., Poddar, S., Marimuthu, R., Balamurugan, S., & Balaji, S. (2017). A review on communication protocols using internet of things. In *2017 International conference on microelectronic devices, circuits and systems* (ICMDCS), IEEE, pp. 1–6.
22. Sanchez-Iborra, R., & Cano, M. D. (2016). State of the art in LP-WAN solutions for industrial IoT services. *Sensors, 16*(5), 708.
23. 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.
24. Calabretta, M., Pecori, R., & Velti, L. (2018). A token-based protocol for securing MQTT communications. In *2018 26th International conference on software, telecommunications and computer networks (SoftCOM)*, IEEE, pp. 1–6.
25. Dalkiltc, G. (2018). Authentication and authorization mechanism on message queue telemetry transport protocol. In *2018 3rd International conference on computer science and engineering (UBMK)*, IEEE, pp. 145–150.
26. Al-Fuqaha, A., Khreishah, A., Guizani, M., Rayes, A., & Mohammadi, M. (2015). Toward better horizontal integration among IoT services. *IEEE Communications Magazine, 53*(9), 72–79.
27. Kaedi, S., Doostari, M. A., & Ghaznavi-Ghoushchi, M. B. (2018). Low-complexity and differential power analysis (DPA)-resistant two-folded power-aware Rivest–Shamir–Adleman (RSA) security schema implementation for IoT-connected devices. *IET Computers and Digital Techniques, 12*(6), 279–288.
28. Luoto, A., & Systä, K. (2018). Fighting network restrictions of request-response pattern with MQTT. *IET Software, 12,* 410–417.
29. Herrero, R. (2018). *Dynamic CoAP mode control in real time wireless IoT networks*. IEEE Internet of Things Journal: DOI. https://doi.org/10.1109/JIOT.2018.2857701.
30. Mišić, J., Ali, M. Z., & Mišić, V. B. (2018). Architecture for IoT domain With CoAP observe feature. *IEEE Internet of Things Journal, 5*(2), 1196–1205.
31. Betzler, A., Gomez, C., Demirkol, I., & Paradells, J. (2016). CoAP congestion control for the internet of things. *IEEE Communications Magazine, 54*(7), 154–160.
32. Misic, J., Ali, M. Z., & Misic, V. B. (2018). *Protocol architectures for IoT domains*. arXiv preprint arXiv:1803.08179.
33. Kome, M. L., Cuppens, F., Cuppens-Boulahia, N., & Frey, V. (2018). CoAP enhancement for a better IoT centric protocol: CoAP 2.0. In *2018 Fifth international conference on internet of things: systems, management and security*, IEEE, pp. 139–146.
34. Maple, C. (2017). Security and privacy in the internet of things. *Journal of Cyber Policy, 2*(2), 155–184.
35. Weber, M., & Boban, M. (2016). Security challenges of the internet of things. In *2016 39th International convention on information and communication technology, electronics and microelectronics (MIPRO)*, IEEE, pp. 638–643.
36. Beißner, N., Lorenz, T., & Reichl, S. (2016). Organ on chip. In *Microsystems for pharmatechnology*, Springer, Cham, pp. 299–339.
37. Balijepalli, A., & Sivaramakrishan, V. (2017). Organs-on-chips: Research and commercial perspectives. *Drug Discovery Today, 22*(2), 397–403.
38. Alhnan, M. A., Okwuosa, T. C., Sadia, M., Wan, K. W., Ahmed, W., & Arafat, B. (2016). Emergence of 3D printed dosage forms: Opportunities and challenges. *Pharmaceutical Research, 33*(8), 1817–1832.
39. Ventola, C. L. (2014). Medical applications for 3D printing: current and projected uses. *Pharmacy and Therapeutics, 39*(10), 704.
40. Akash, S. A., Menon, A., Gupta, A., Wakeel, M. W., Praveen, M. N., & Meena, P. (2014). A novel strategy for controlling the movement of a smart wheelchair using internet of things. In *2014 IEEE global humanitarian technology conference-South Asia satellite (GHTC-SAS)*, IEEE, pp. 154–158.
41. Desai, S., Mantha, S. S., & Phalle, V. M. (2017). Advances in smart wheelchair technology. In 2017 *International conference on nascent technologies in engineering (ICNTE)*, IEEE, pp. 1–7.

42. Baker, S. B., Xiang, W., & Atkinson, I. (2017). Internet of Things for smart healthcare: Technologies, challenges, and opportunities. *IEEE Access, 5,* 26521–26544.
43. Haghi, M., Thurow, K., & Stoll, R. (2017). Wearable devices in medical internet of things: Scientific research and commercially available devices. *Healthcare Informatics Research, 23*(1), 4–15.
44. Mann, S. (2017). Big Data is a big lie without little data: Humanistic intelligence as a human right. *Big Data & Society, 4*(1), 2053951717691550.
45. Aeschimann, R., & Borges, P. V. K. (2015). Ground or obstacles? Detecting clear paths in vehicle navigation. In *2015 IEEE international conference on robotics and automation (ICRA)*, IEEE, pp. 3927–3934.
46. Gill, K., Heath, K. N., Gegear, R. J., Ryder, E. F., & Wyglinski, A.M. (2018). On the capacity bounds for bumblebee-inspired connected vehicle networks via queuing theory. In *2018 IEEE 87th vehicular technology conference (VTC spring)*, IEEE, pp. 1–6.
47. Viet, N. B., Hai, N. T., & Hung, N. V. (2013). Tracking landmarks for control of an electric wheelchair using a stereoscopic camera system. In *2013 International conference on advanced technologies for communications (ATC)*, IEEE, pp. 339–344.
48. Gong, F., Zheng, N., Xue, L., Xu, K., & Zheng, X. (2014). RICA: A reliable and image configurable arena for cyborg bumblebee based on CAN bus. In *2014 36th Annual international conference of the IEEE engineering in medicine and biology society (EMBC)*, IEEE, pp. 860–863.
49. Anagnostopoulos, T., Zaslavsky, A., & Medvedev, A. (2015). Robust waste collection exploiting cost efficiency of IoT potentiality in smart cities. In *2015 International conference on recent advances in Internet of Things (RIoT)*, IEEE, pp. 1–6.
50. Fujdiak, R., Masek, P., Mlynek, P., Misurec, J., & Olshannikova, E. (2016). Using genetic algorithm for advanced municipal waste collection in smart city. In *2016 10th International symposium on communication systems, networks and digital signal processing (CSNDSP)*, IEEE, pp. 1–6.
51. Karadimas, D., Papalambrou, A., Gialelis, J., & Koubias, S. (2016). An integrated node for Smart-City applications based on active RFID tags; use case on waste-bins. In *2016 IEEE 21st international conference on emerging technologies and factory automation (ETFA)*, IEEE, pp. 1–7.
52. Lu, J. W., Chang, N. B., Zhu, F., Hai, J., & Liao, L. (2018). Smart and green urban solid waste collection system for differentiated collection with integrated sensor networks. In *2018 IEEE 15th international conference on networking, sensing and control (ICNSC)*, IEEE, pp. 1–5.
53. Pokric, B., Kreo, S., Drajic, D., Pokric, M., Jokic, I., & Stojanovic, M. J. (2014). ekoNET-environmental monitoring using low-cost sensors for detecting gases, particulate matter, and meteorological parameters. In *2014 Eighth international conference on innovative mobile and internet services in ubiquitous computing (IMIS)*, IEEE, pp. 421–426.
54. Ma, Y., Yang, S., Huang, Z., Hou, Y., Cui, L., & Yang, D. (2014). Hierarchical air quality monitoring system design. In *2014 14th International symposium on integrated circuits (ISIC)*, IEEE, pp. 284–287.
55. Tesanovic, M., & Vadgama, S. (2014). Short paper: Vehicle emission control in Smart Cities. In *2014 IEEE world forum on Internet of Things (WF-IoT)*, IEEE, pp. 163–164.
56. Sarkar, S., Chatterjee, S., & Misra, S. (2015). Assessment of the suitability of fog computing in the context of Internet of Things. *IEEE Transactions on Cloud Computing, 6,* 46–59.
57. Soumyalatha, S. G. H. (2016). Study of IoT: Understanding IoT architecture, applications, is-sues and challenges. In *1st International conference on innovations in computing and net-working (ICICN16), CSE, RRCE. International journal of advanced networking and applications*.
58. Liu, Y., Seet, B. C., & Al-Anbuky, A. (2013). An ontology-based context model for wireless sensor network (WSN) management in the Internet of Things. *Journal of Sensor and Actuator Networks, 2*(4), 653–674.
59. Rghioui, A., & Oumnad, A. (2017). Internet of Things: Visions, technologies, and areas of application. *Technology, 6,* 7.
60. Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things Journal, 1*(1), 22–32.
61. Gaur, A., Scotney, B., Parr, G., & McClean, S. (2015). Smart city architecture and its applications based on IoT. *Procedia Computer Science, 52,* 1089–1094.
62. Lee, M., Hwang, J., & Yoe, H. (2013). Agricultural production system based on IoT. In *2013 IEEE 16th international conference on computational science and engineering (CSE)*, IEEE, pp. 833–837.
63. Triantafyllou, A., Sarigiannidis, P., & Lagkas, T. D. (2018). Network protocols, schemes, and mechanisms for Internet of Things (IoT): Features, open challenges, and trends. In *Wireless communications and mobile computing*.
64. Tzounis, A., Katsoulas, N., Bartzanas, T., & Kittas, C. (2017). Internet of things in agriculture, recent advances and future challenges. *Biosystems Engineering, 164,* 31–48.

65. Parashar, R., Khan, A., & Neha, (2016). A survey: The Internet of Things. *International Journal of Technical Research and Applications, 4,* 251–257.
66. Zhang, Z. K., Cho, M. C. Y., Wang, C. W., Hsu, C. W., Chen, C. K., & Shieh, S. (2014). IoT security: Ongoing challenges and research opportunities. In *2014 IEEE 7th International conference on service-oriented computing and applications (SOCA)*, IEEE, pp. 230–234.
67. Farhan, L., Kharel, R., Kaiwartya, O., Quiroz-Castellanos, M., Alissa, A., & Abdulsalam, M. (2018). A concise review on Internet of Things (IoT)-problems, challenges and opportunities. In *2018 11th International symposium on communication systems, networks and digital signal processing (CSNDSP)*, IEEE, pp. 1–6.
68. Javed, F., Afzal, M. K., Sharif, M., & Kim, B. S. (2018). Internet of Things (IoTs) operating systems support, networking technologies, applications, and challenges: A comparative review. *IEEE Communications Surveys & Tutorials, 20,* 2062–2100.
69. Tiwary, A., Mahato, M., & Chandrol, M. K. (2018). Internet of Things (IoT): Research, architectures and applications. *International Journal on Future Revolution in Computer Science & Communication Engineering, ISSN, 4,* 2454–4248.
70. Samuel, S. S. I. (2016). A review of connectivity challenges in IoT-smart home. In *2016 3rd MEC International conference on big data and smart city (ICBDSC)*, IEEE, pp. 1–4.
71. Udoh, I. S., & Kotonya, G. (2018). Developing IoT applications: Challenges and frameworks. *IET Cyber-Physical Systems: Theory & Applications, 3*(2), 65–72.

Dr. S. Balaji received Master of Technology from National Institute of Technology, Tiruchirappalli, and Ph.D. in Electrical Engineering from VIT University, Vellore, India. Currently he is working as Associate Professor in the School of Electrical Engineering (SELECT), VIT University, India. He has published more than 25 research papers in the area of wireless communication in International Journals, National Level Journals and Conferences. His areas of interest include MIMO, OFDM, IoT and Wireless Communication with emphasis on Signal Processing.

Karan Nathani was born in Gwalior, India in 1997. He is a 3rd year B.Tech student currently pursuing Electronics and Instrumentation from Vellore Institute of Technology, Vellore from the year 2015–2019. He has written an intriguing paper on the topic "Cubic SVM Classifier Based Feature Extraction and Actor Dependent Emotion Detection of Speech Signals in noisy Environment" which will be sent to a respected Journal for its awaiting publication. His main areas of research interest are Machine Learning and IoT Technologies. He has been awarded a scholarship by VIT University in the academic year 2017–2018 for his excellent performance in the academics.

Prof. R. Santhakumar received Master of Engineering from Madras Institute of Technology, Chennai, and pursuing Ph.D. in Electrical Engineering from VIT University, Vellore, India. Currently he is working as Assistant Professor (Senior) in the School of Electrical Engineering (SELECT), VIT University, India. He has published more than 20 research papers in the area of wireless communication in International Journals, National Level Journals and Conferences. His areas of interest include MIMO, OFDM, and Wireless Communication.