Chapter 3
The History, Present and Future with IoT

Neha Sharma, Madhavi Shamkuwar and Inderjit Singh

Abstract Human beings quest for making comfortable life is due to their inquisitiveness about technical arena. Over the last few decades, mankind had experienced technical transformational journey with the inventions of new technology frontiers. These frontiers have interacted with human beings and performed every possible work in shorter period of time and with a much greater accuracy. With the advent of 'Smart Concepts', the world is now becoming more connected. Precisely termed as hyper-connected world. The smart concepts includes smart phones, smart devices, smart applications and smart cities. These smarter concepts forms an ecosystem of devices whose basic work is to connect various devices to send and receive data. Internet of Things is one the dominating technology that keeps eye on the connected smart devices. Internet of Things has bought applications from fiction to fact enabling fourth industrial revolution. It has laid an incredible impact on the technical, social, economic and on the lives of human and machines. Scientists claim that the potential benefit derived from this technology will sprout a foreseeable future where the smart objects sense, think and act. Internet of Things is the trending technology and embodies various concepts such as fog computing, edge computing, communication protocols, electronic devices, sensors, geo-location etc. The chapter presents the comprehensive information about the evolution of Internet of Things, its present developments to its futuristic applications.

N. Sharma (✉)
Society for Data Science, Pune, India
e-mail: nvsharma@rediffmail.com

M. Shamkuwar
Zeal Institute of Business Administration, Computer Application and Research, Savitribai Phule Pune University, Ganesh Khind, Pune 411007, Maharashtra, India
e-mail: madhavi.sh@gmail.com

I. Singh
BCL Secure Premises, Delhi, India
e-mail: Inderjit.barara@gmail.com

V. E. Balas et al. (eds.), *Internet of Things and Big Data Analytics for Smart Generation*, Intelligent Systems Reference Library 154,
https://doi.org/10.1007/978-3-030-04203-5_3

Keywords Internet of things · IoT history · IoT evolution · IoT definition
IoT trends · Sensors · Communication model · IoT architecture
IoT technologies · IoT applications · Future of IoT · IoT · Fog computing
Edge computing

3.1 Introduction

A huge rise in the number of objects connected to the internet, either by wire or wireless has made Internet of Things (IoT) an increasingly growing topic of conversation both in the industry and outside of it [1]. It is predicted that IoT will rival all the past scientific marvels, such as steam engine, printing press and electricity and will surpass all the previous industrial revolutions. The "Internet of things" along with robotics, artificial intelligence, nanotechnology, quantum computing, biotechnology, 3D printing and autonomous vehicles, mark the fourth industrial revolution [2]. In particular, IoT is a concept that not only has the potential to impact our lives but also the way we work [3]. It can dramatically improve security, energy efficiency, education, health, and many other aspects of daily life for consumers, through amazing solutions [4–9]. It can also improve decision-making and productivity of enterprises in retail, supply chain management, manufacturing, agriculture and other sectors by reinforcing solutions [4–9].

Now, all kinds of everyday objects can be connected to the internet including cars, thermostats, sporting equipment, microwave oven, fitbit, refrigerators, and even shoes. Internet of Things is an evolution of mobile, embedded application and everything that is connected to internet to integrate greater communication ability and use data analytics to extract meaningful information. The IoT device which is connected to the internet and placed in shoes collects the data like the step counts and can be viewed from another internet connected device like smart phone. All the metrics collected by the shoes can be analyzed like how many calories burnt and can provide personalized fitness advice. IoT is not limited to consumer products. There are city trash cans which sends an alert when it needs to be empty. Sensors on the bridges can check for stress or damage on its structure and many more examples extending to healthcare, manufacturing and agriculture [4–9]. Unfortunately, since the system is controlled by free market, the risk of data protection and data security cannot be excluded. For example, a hacker can easily unlock an internet connected door lock remotely. There would be issues of data privacy which will be a major concern. All these devices are collecting large amount of personal data that can capture our action and location throughout the day.

IoT is a technology wave that would be connecting billions of objects in coming years and its upsurge also indicates beginning of new data age with its benefits and challenges. Two main components of an "IoT object" are its ability to capture data via sensors and transmit data via the Internet [10, 11]. Internet connectivity allows object to have their own identities as well as receive and send valuable communication making them smart. This chapter is arranged as follows: the next section reviews the work done by researchers with similar interest; Sect. 3.3 presents various definition of Internet of Things, its history and evolution of technology trends; IoT communication models, architecture and technology prevalent in present day scenario is discussed Sect. 3.4 and future of IoT is discussed in Sect. 3.5. Finally, Sect. 3.6 summarizes the chapter with conclusion, followed by references which are mentioned in the last section.

3.2 Related Work

The following section provides literature review, which presents the evolution of Internet of Things (IoT) as well as highlights spectrum of possible applications that has potential to improve the human life drastically. Ibarra-Esquer et al. have systematically presented the evolution of concept of the Internet of Things and tracked it across various application domains [12]. Ideally, it is essential to have in place an IoT infrastructure comprised of sensing devices, communication link and user application, to create a smart environment. However, it is not at all essential to have the entire infrastructure in the beginning, it can be added phase wise on priority basis. Laya et al., in their research paper, highlighted multiple factors impeding the adoption of IoT paradigm [13]. As per them, single solution cannot cater to the applications in heterogeneous field. In addition, lack of backend network services and devices to realize IoT network and absence of clear as well as accepted business model are the main reasons behind not being able to attract investments for deploying these technologies [13]. Likewise, there are few more literatures, which has described number of hurdles in implementing IoT based smart solutions for smart cities [14–18]. The obstacle are mainly political (decision-making power to various stakeholders), financial (unclear business model and lack of investors) and technical (heterogeneous technologies and issues of interoperability).

Study by Bellavista et al. have suggested many applications of IoT in varied domains like smart grids, intelligent energy management, mobile health care, medical aids, industry automation, home automation, elderly assistance, smart vehicles, traffic management and many others [19]. Schaffers et al. and Cuff et al. have presented urban IoT paradigm to enhance the public services like maintenance, surveillance and security of public area; efficient parking, transportation, garbage collection and lighting; preservation of cultural heritage and services at schools and hospitals [20, 21]. As per the authors, the deployment of urban IoT has potential to optimize the management of traditional public services, mainly by analyzing the profuse amount of data generated to provide transparent and effective governance.

There are few literatures that have presented a specific areas where IoT can be implemented to enhance the performance. Lynch et al. have suggested the usage of IoT for maintenance of the building by installing different types of specialized IoT devices to monitor building stress due to deformation and vibration, to track environmental conditions due to temperature and humidity and to check pollution level

[22]. The data collected should reduce the periodic structural check by human and assist them in focused maintenance and restoration activity. The data collected from various IoTs will also help in understanding the impact of natural calamity like earthquake on the buildings. Nuortio et al. have presented smart waste management system by installing IoT devices on waste containers to assess the level of load and communicate the information with the garbage collector truck to optimize the route and minimize the cost of garbage collection [23]. Soliman et al. have evaluated the benefits of IoT in learning environment of physical as well as virtual types. They have also presented and discussed the experimental results [24]. Whereas, Elsaadany has worked on smart secure campus environment and smart student feedback using IoT [25]. Atzori and Mashal have attempted to combine social networks and Internet of Things for better user engagement and to promote education in real and virtual environment [26, 27]. Chandrahasan et al. have presented the smart parking to indicate the nearest available free parking space for the vehicle in order to save time and energy [28]. Likewise, IoT devices and sensors can be used to monitor the quality of the air or noise level [29, 30]. It can also be used to offer services like providing information on traffic congestion, energy consumption, smart parking, smart lighting etc. [31–33]. However, all the above applications require initial investment on installation of sensors and their interconnection to a control system.

3.3 Internet of Things (IoT): Evolution

A network connects devices like computers, printers, fax machines, etc. together either by cables or wirelessly by radio or infrared signals to transfer the information from one point to another. A network need not be only for computers, it can be also of analog telephone system and interconnection of such networks is known as internet. Nevertheless, the technological advancement in recent past has transformed the internet to the network where everything is linked and everyday objects can be recognized and controlled via RFID tags, sensors and smart phones. The Internet of Things (IoT) is the network of physical objects that can sense, communicate and accessed through the Internet and becomes its integral part. These objects are embedded with electronics (Microcontrollers and transceivers), software, sensors, actuators and network connectivity that enables them to collect and exchange the data using various protocols [10]. Therefore, IoT offers connectivity of devices, systems and services that goes beyond Machine-to-Machine (M2M) communication and caters to variety of application in different domains.

The quality of life is undergoing fast transformation and will be improved drastically in future. Only 500 million devices were connected to the internet and today it has grown above 25 billion. By 2020, 50 billion devices will be equipped with a unique identifier as shown in Fig. 3.1, so that they can be of great benefit in the field of energy, safety and security, industry, manufacturing, retail, healthcare, independence of elderly persons, people with reduced mobility, environment, transport, smart cities, entertainment and many more [34].

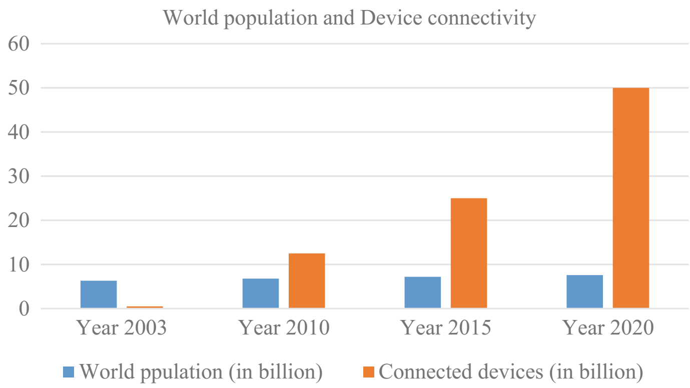

Fig. 3.1 Growth in connected devices as indicated by Cisco [34]

Such predictions regarding Internet of Things (IoT) has made a huge impact on the global economy. However, these estimates slightly vary from each other. As per McKinsey, the growth of IoT market would be from 4 trillion USD to 11 trillion USD by 2025 [35], whereas Gartner predicts it to be 2 trillion USD by 2025 [36] and IDC sees the benefit of 1.7 trillion in 2020 [37]. Therefore it is prudent to understand its evolution in this section. We present various definition of IoT proposed by different sections, its history and several technology trends that are driving it.

3.3.1 Definitions

Ashton coined the term Internet of Things in 1999 for the first time to highlight the power of connecting Radio Frequency Identification Tags to the internet for the domain of Supply Chain Management [38]. Multiple definitions of Internet of Things have evolved in the past decade based of latest technology of that time and the range of applications it caters [39]. However, there is no definition of Internet of Things which is universally accepted. The concept is almost the story of "The Blind Men and Elephant", it depends on the way we perceive and conceive the lucrative power of IoT. Different researchers, scientists define the term in their own way, some focus more objects, devices, Internet Protocols and Internet, while others focus on the communication processes involved. We present the following well known and well-accepted definitions of IoT:

1. Internet Architecture Board (IAB) defines IoT as a communication service [40]. According to them, the term "Internet of Things" (IoT) represents a set of large number of embedded devices, which provides communication services based on the Internet Protocols. The devices are popularly termed as "Objects" or "Smart Objects", these objects communicate with each other and often do not require human intervention.

2. The Internet Engineering Task Force (IETF) refers IoT as 'Smart Object' and were of opinion that it has limited power, memory, and processing resources, or bandwidth [41]. IETF focuses more on achieving network interoperability between several types of smart objects [42].
3. IEEE Communications Magazine relates Internet of Things to Cloud Services [43]. They define IoT as a framework in which each object is uniquely identified on the internet. More precisely, IoT targets to offer various applications and services to eliminate the gap in physical and virtual world using Machine-to-Machine (M2M) communications to enable interaction between objects and applications in the cloud.
4. The definition given by Oxford Dictionaries is very accurate and focuses on use of Internet as a connecting media between devices [44]. It defines IoT as "the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data" [44].
5. Atzori et al. defines Internet of Things as three key ideas i.e. Middleware, which is internet-oriented, Sensors which are things oriented and Knowledge which is semantic-oriented [10]. From definition point of view these three types are different from each other and seems to be an individual entity, however, in reality these three intersects with each other so that that potential benefits of IoT can be derived.
6. Forrester perceives IoT as a smart environment to offer services to various domain like education, administration, healthcare, and transportation etc. with the help of information and communications technology [45].

However, the distinct definitions is that the IoT is a constellations of objects, things, devices, technology, protocols that will change the whole communication process. This can be achieved by a unified framework which includes ubiquitous computing, cloud computing, data analytics and knowledge representation/visualization [46].

3.3.2 History

The first idea of IoT appeared almost two decades ago, but the technologies behind it had already existed and were under development since many years. Let us look at the history of evolution of IoT and its supporting and associated technologies in chronological order—

1. **1969**—Internet, the main technology behind IoT emerged as Advanced Research Project Agency Network (ARPANET) which was mainly used by academic and research fraternity to share research work, to develop new interconnection techniques and to link computers to many general purpose computer centers of defense department of United States and also in public and private sector [47].

2. **1973**—Another essential technology for IoT is RFID (Radio-Frequency Identification). Though the roots of RFID can be traced back to World War-II and the advances continued through 1950s and 1960s, but the first U.S. patent for RFID tag with rewritable memory was received by Mario W. Cardullo in 1973. However, a California based entrepreneur, Charles Walton also received a patent in the same year for passive transponder to unlock the door remotely.
3. **1974**—Embedded computer system was another important technology for IoT. These system are implemented using single board computers and microcontrollers and are embedded in the bigger system to form its integral part [48].
4. **1984**—Early use of IoT without it being christened. A coke machine was connected to internet to report the availability and temperature of the drink [49].
5. **1990**—Proliferation of internet in business and consumer markets. However, its use was still limited due to low performance of network connectivity.
6. **1991**—The concept of ubiquitous computing was proposed by Mark Weiser. The ubiquitous computing made use of advanced embedded computing as a computer to be present in everything, yet invisible. Later, it was known as pervasive computing [50].
7. **Mid 1990s**—Sensor nodes were developed to sense the data from uniquely identified embedded devices and seamlessly exchange the information to realize the basic idea of IoT [1, 12, 51].
8. **1999**—Device to Device communication was introduced by Bill Joy in his taxonomy of internet and the term 'Internet of Things' was used for the first time by Ashton [52, 53]. Besides, the RFID technology was boosted by an establishment of the Auto-ID Center at the Massachusetts Institute of Technology (MIT) to produce an inexpensive chip which can store information and can be used to link objects to the internet [54].
9. **2000 onwards**—As a result of digitalization, internet connectivity became the norm for many applications and all the business and products were expected to have presence on the internet and provide information on-line. However, these devices are still primarily things on the Internet that require more human interaction and monitoring through apps and interfaces. The roadmap of IoT from 2000 onwards is shown in the Fig. 3.2 [55].

The true potential of the IoT has just begun to realize—when imperceptible technology operates behind the scenes and dynamically respond to our expectation or need for the "things" to act and behave.

3.3.3 Trends in IoT

In 2011, Internet of Things has been identified as one of the emerging technologies in area of Information Technology and was added in the Gartner Hype Cycle [56]. A Hype Cycle is a curved graph representing the emergence of innovative technology, peak of inflated expectations, adoption, maturity and productivity [55].

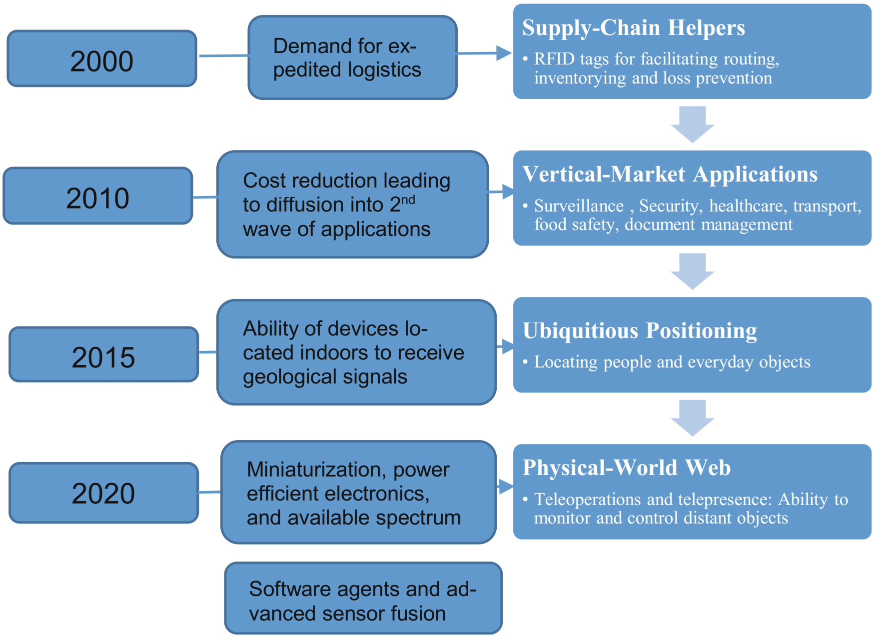

Fig. 3.2 Roadmap of internet of things from 2000 onwards [55]

According to the Gartner hype cycle 2017, it is estimated that IoT platforms will take 2 to 5 years for market adoption as shown in Fig. 3.3.

Google trends allows us to compare the trending patterns of various technologies by their web search popularity. Figure 3.4 compares three recent technologies i.e. Internet of Things, Big Data Analytics and Quantum Computing and shows that IoT is a technology trend setter in last three years [57].

A per the Accenture report 2018, covering 25 countries Tech Vision, 'Internet of Things' is one of the trending technology apart from Cloud, Artificial Intelligence, Blockchain, Augmented and Virtual Reality, Robotics, Quantum Computing [58].

3.4 Internet of Things: Present State

With the exponentially growing rate of the Internet of Things and lots of innovation happening around it in different verticals and technologies, the industries are highly motivated to invest in IoT with an objective of improving business processes, minimizing risks, and enhancing customer experiences. However, IoT is not just about installing sensors on objects and calling it "Smart". Comprehensive IoT solutions needs an appropriate infrastructure and supporting environment for data collection, data analysis and applications to trigger the action. The entire IoT

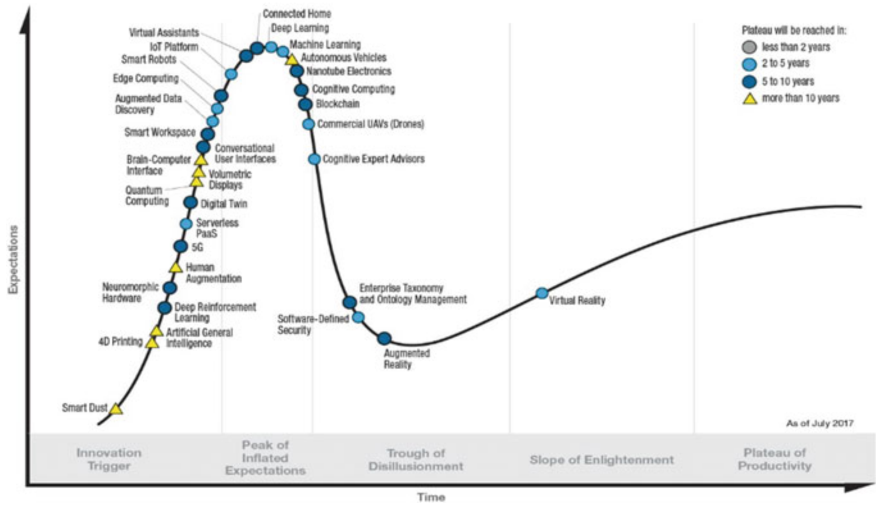

Fig. 3.3 Gartner 2017 hype cycle of emerging technologies (*Source* Gartner Inc.) [56]

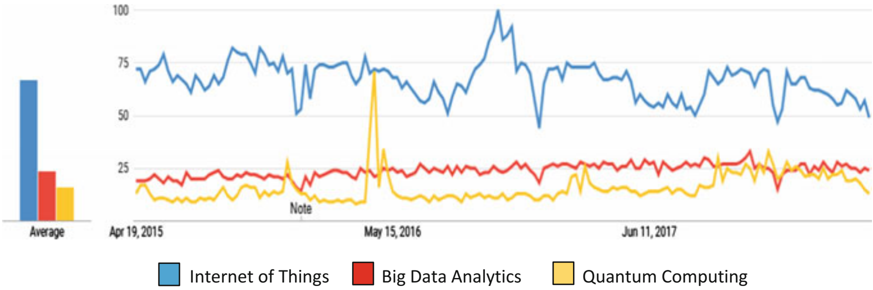

Fig. 3.4 Google search trends since 2015 for terms Internet of Things, Big Data Analytics, quantum computing [57]

ecosystem is driven by Government, Industry and Startups. Therefore, to set the stage properly for a shared vision of IoT in the complete ecosystem, we discuss the present state of IoT communication models, architecture, technologies and possible applications in this section.

3.4.1 Present Communication Models

The basic objective of IoT is to allow people to communicate with everything at anytime, anyplace, with anyone and anything, preferably using any network and any service. The speed with which IoT devices are growing, it's evident that in the future it will be found everywhere and will enable ambient intelligence. Hence, it is prudent to know about various communication models which allows IoT devices to connect and communicate. This section presents four communication models from a guiding architecture document released by Internet Architecture Board (IAB) for networking of smart objects (RFC 7452) in March 2015 [41].

(a) **Device-to-Device Communication Model**

- Communication is between two or more IoT devices as shown in Fig. 3.5.
- Devices does not need intermediary application server to connect and communicate with each other, they communicate directly.
- Communication takes place through Internet or IP networks or any other types of networks.
- Protocols used to establish direct communication can be Bluetooth [59], Zigbee [60], Z-Wave [61].
- Application are typically where small data packets are exchanged at a very low data rate, like home automation system which IoT devices are embedded in locks, bulbs, switches, thermostats etc.
- Limitation of device-to-device communication model- devices are incompatible due to different communication protocols being used by the manufacturers and can communicate only to the devices with same protocol.

(b) **Device-to-Cloud Communication Model**

- The communication is between IoT device and the internet cloud services (like application servers) for the data exchange and message traffic control as shown in Fig. 3.6.
- The communication takes place through traditional wired Ethernet or Wi-Fi connections to establish connection between the device and the IP network, which in turn connects to the cloud service.
- The device takes help of protocols such as HTTP, TCP/IP, TLS etc. to communicate with the cloud services.
- Samsung Smart TV [62] and Nest Labs leaning Thermostat [63] are the examples of IoT devices that have adopted device-to-cloud model.
- These IoT devices records the data, transmits it to the database in the cloud, where the data is analyzed for further use. The cloud technology provides a remote access to these devices, which can be obtained via a web interface or by a smartphone and also provides software updates to these devises.

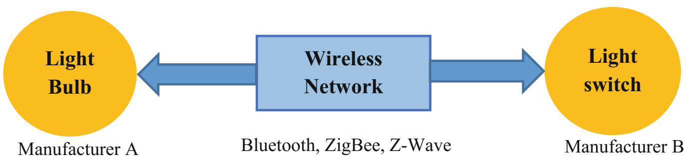

Fig. 3.5 Device-to-device communication model [41]

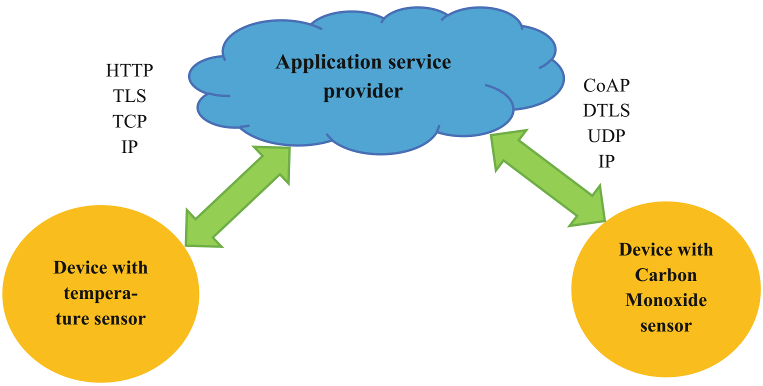

Fig. 3.6 Device-to-cloud communication model [41]

- In this model, the interoperability challenges are often faced when the devices developed by different manufacturers are attempted to integrate. In the present scenario, for this communication model to function properly, the device and the cloud should be from same vendor [64]. This vendor lock-in state prohibits the use of other service providers.

(c) **Device-to-Gateway Communication Model**

- The IoT device takes help of gateway device to communicate to the internet cloud services for the data exchange as shown in Fig. 3.7.
- The gateway device works on application layer and is known as application-layer-gateway. The gateway has an application software operating on it and acts as intermediary between IoT device and the cloud service, mainly supports data or protocol translation and provides security.
- Usually, the smart phones act as a gateway device with an App installed to communicate with an IoT device and transmit the data to a cloud service. An example of such application layer gateway is fitness App in a smartphone, which is connected to the fitness tracker device. This device cannot directly connect to the clouds service and hence depends on the smartphone App as a gateway device to connect.
- Besides smartphones, the hub devices also act as gateway device between IoT devices and cloud services, and are mainly used in home automation applications. Hub devices also bridge the interoperability gap between devices themselves.
- Advantage: This model integrates new smart devices into a legacy system which further facilitates interoperability between devices.
- The challenge is addition of application layer software which adds costs and design complexity to the system.

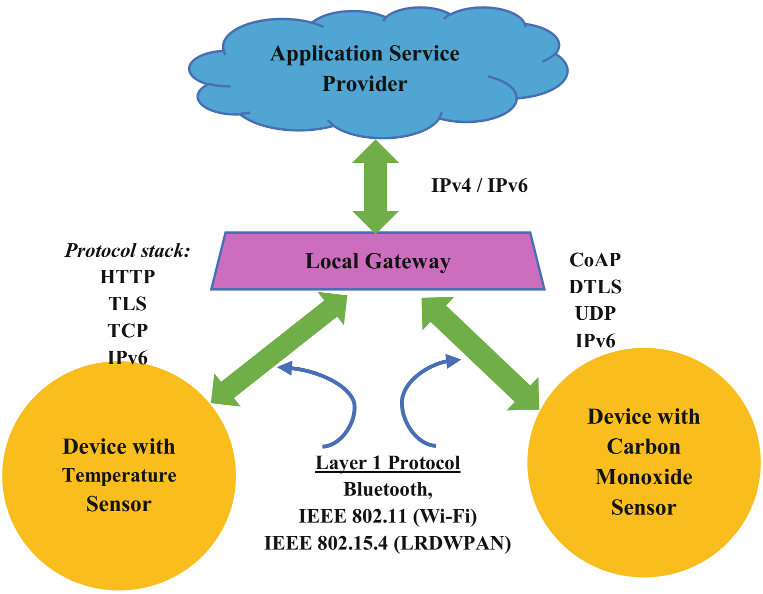

Fig. 3.7 Device-to-gateway communication model [41]

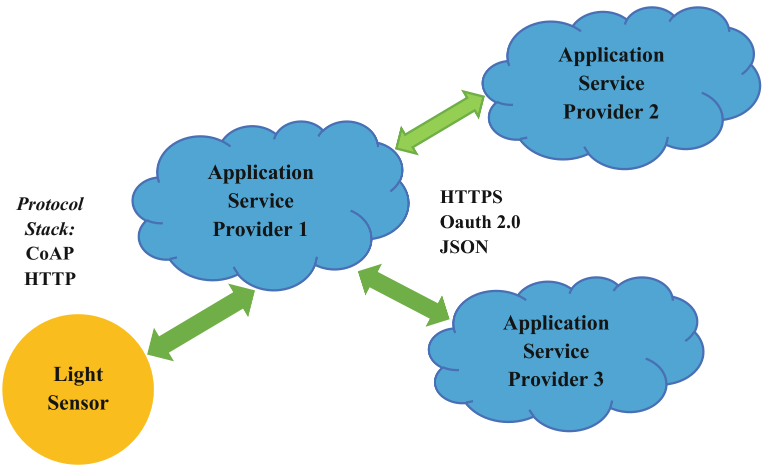

Fig. 3.8 Back-end data sharing communication model [41]

(d) **Back-End-Data-Sharing Communication Model**

- This communication model is driven by the users' wish to share the sensor data stored in the cloud with third parties [41]. Hence, the model empowers the users to export the smart object (IoT device) data from the cloud database and analyze it by integrating it with the data from other sources. The back-end data-sharing model is shown in Fig. 3.8.

- This model is an attempt to overcome the limitations of device-to-cloud model, where data from IoT devices are uploaded to single application service provider in the cloud creating data silos. A back-end sharing model permits to aggregate and analyze the data stream collected from multiple IoT devices.
- The model adopts a federated cloud services approach and achieves interoperability of IoT devices through cloud applications programmer interfaces.

The fundamental architecture used by IoT devices to communicate are divided into four categories of models. While selecting the right communication model for an IoT device being networked, one needs to understand its technical aspect as well as the type (open or proprietary). Right communication model adds value to the users' expectations from the IoT device. They provide a user to have better access to the device and the data generated so the values of device, app and data is augmented. The communication model also serves as a tool which allows to employ data aggregation, big data analytics, data visualization, and predictive analytics technologies to get value of IoT. Each of the communication model have their benefits and tradeoffs, the cloud services renders various applications, however, the costs incurred for the same must be affordable to the user in terms of connectivity of devices.

3.4.2 Present Architecture

The existing architecture of internet was adopted about four decades back in form of TCP/IP protocols, but today it is incompatible to serve the huge network of Internet of Things [65]. Hence, there is a need for a new architecture that can handle the network of over 25 billion connected objects, which is estimated to be available by 2020 [34]. This new architecture should use open source protocol to support existing network applications and provide security and Quality of Service (QoS) [66]. The key challenges for implementing IoT are data protection and data privacy [67, 68]. Therefore, various mutli-layered security architecture for IoT are proposed for its further enhancement. Wang Chen proposed the three layer architecture [69], Hui Sho et al. presented four layer architecture [70], MiaoWu et al. have referred architectures of Internet and Telecommunication management networks based on TCP/IP and TMN respectively to share the idea of five layer architecture [71] and Xu Cheng et al. proposed six layered architecture based on a hierarchical structure is shown in Fig. 3.9 [72].

The six layers of architecture of IoT is briefly discussed below:

- **First Layer—Coding**
  This is the base layer of the IoT architecture, where each object of interest is provided with a code for the sake of unique identification [72].

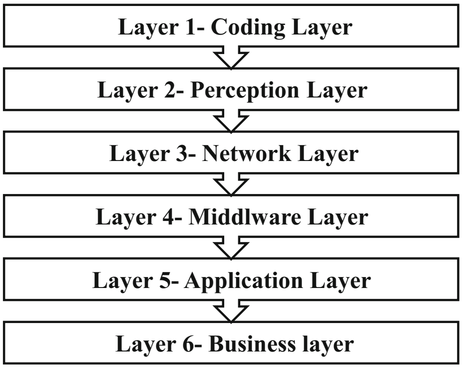

Fig. 3.9 Architecture of IoT proposed by Cheng [72]

- **Second Layer—Perception**
  The object of interest with the unique code is given a physical meaning by attaching an IoT devices to it, hence the layer is known as device layer or recognition layer or perception layer. The devices are usually sensors like RFID tags, IR sensors or other sensors and are responsible for sensing temperature, pressure, moisture, speed, location etc. [73]. In this layer, the data sensor gathers the information from the linked object, convert it into digital signal and transmits it for further action to the Network layer.
- **Third Layer—Network**
  The Network layers is responsible for secure data transmission between Perception layer and Middleware layer. This layer receives the information from the Perception layer in digital form and then further sends it to the Middleware layer for further processing. This layer uses various transmission mediums like Bluetooth, WiMaX, Zigbee, GSM, 3G etc. with protocols like IPv4, IPv6, MQTT, AMQP, CoAP, XMPP, DDS etc. [74], and is a convergence of internet and communication based network.
- **Fourth Layer—Middleware**
  This layer uses the advanced technologies like ubiquitous computing, cloud computing, fog computing, edge computing etc. to access the database directly and store the required information in it. This layer mainly processes the sensor data received from the Network layer, using Intelligent Processing Equipment, and performs a fully automated action based of the result [3].
- **Fifth Layer—Application**
  This layer provides the personalized service on the basis of user needs, using the result of the processed data. Various high-level intelligent applications of IoT is realized for all kinds of industry. The IoT related applications could be disaster monitoring, health monitoring, smart homes, smart transportation, smart planet etc. These applications encourage the expansion of IoT, and hence this layer is very vital in the development of large scale IoT network [71].

- **Sixth Layer—Business**
  The Business layer is the top layer of the IoT architecture, where various business models are generated for the effective business strategies. The applications and services provided by IoT is managed in this layer.

3.4.3 *Present Technologies*

The development of IoT network enables the object to be uniquely identified and be able to connect and communicate with other objects anytime and anywhere [75]. The seamless communication is achieved by three components of IoT that are mentioned below:

(a) Hardware—Sensors, Actuators, Embedded Communication Hardware
(b) Middleware—Storage tools, Computing tools
(c) Presentation—Visualization tool and Interpretation tool.

In this section, we present few technologies that make up the above components. These technologies help in realizing the entire IoT ecosystem.

Radio Frequency Identification (RFID)
Radio Frequency Identification is a key technology in the field of embedded communication, which aids the design of transceiver microchip for wireless communication [10]. RFID technology helps to identify and track objects in which it is implanted as a tag, that are of rice-grain size and very inexpensive, hence easy to integrate with any object [69]. There are mainly two types of tags i.e. active and passive. Active tags have their own battery, which helps them to be always active and emit the data signals, whereas passive tags are not powered by battery and needs to be triggered to fetch the data [3]. However, both the tags have wide range of application and can be implanted in living or non-living objects. RFID system comprise of tags that contains details of an object to which it is attached, and associated Readers [76]. The tags emit the data signals that contains the information like identification; location etc. regarding the object and that is transmitted using radio frequencies to the Readers, which then is shared with the processors for analysis.

Wireless Sensor Networks (WSN)
Wireless Sensor Networks is a breakthrough technology in remote sensing applications, which uses energy efficient, reliable, low cost, small size device based on integrated circuits and supports wireless communications. Hence, WSN is a sensor network that consists of many intelligent sensors, which collects, process, analyze and disseminates valuable information gathered over a network [51]. Each sensor is a communication, actuation and sensing unit, which is basically a transceiver that has micro-controller, antenna, a circuit which acts as an interface and a power source which could be battery or any other technology for energy harvesting [51,

77]. All of these put together forms the WSN hardware, which is known as a node, and are usually deployed in an adhoc manner for most of the applications. The deployed network is expected to have appropriate topology, MAC layer and routing to ensure the scalability and durability of the network, and be able to connect to the base station for data transmission in either single of multiple hop. The nodes may drop out and consequently the network may fail, hence a WSN communication stack at the sink node acts as a gateway between the Internet and WSN subnet so as to establish communication with the outer world [78].

WSN middleware provides access to sensor resources that are heterogeneous, by integrating cyber infrastructure with a sensor networks and Service Oriented Architecture (SOA) [78]. Open Sensor Web Architecture (OSWA) is a platform independent middleware which is used to develop sensor applications [79]. OSWA is based on Sensor Web Enablement Method (SWE) and Open Geospatial Consortium (OGC), which are the standard set of operations and data representations. Besides, WSN is expected to provide secure and efficient data aggregation method so as to ensure the authenticity of the collected sensor data and enhancing the life of the network [79]. Also, recovery process after the failure a node should be carried out without affecting the data transmission procedure.

Cloud Computing
Cloud Computing is an intelligent technology that is a convergence of many servers on to one cloud platform with an objective to share the resources and access them from anywhere and anytime [80]. Cloud technology is the integral part of IoT as it stores the aggregated data from various IoT devices, processes them and presents the analysis for future action [81]. With increasing number of IoT device interfacing with cloud, there is a need for more development of this technology to unleash its true power as IoT is be totally dependent on the Cloud Computing.

Data Storage and Analytics
Data is generated in profuse amount by IoT, the critical factors affecting the growth of data is its storage, data ownership and data expiry. Out of the total energy generated, 5% consumption is done by internet, which implies that the data centers needs to be energy efficient and reliable. The basic necessity is therefore data storage and its analysis. Algorithms making intelligent use of data should be designed which will be customized as per the need as centralized or distributed based algorithm. New genre of algorithm which are either evolutionary algorithms, genetic algorithms, neural networks are required for effective decision making. The systems thus created must possess characteristics such as interoperability, integration and adaptive communications. The system are based on modular architecture for hardware and software development.

Visualization
Visualization is one of the important aspect while dealing with IoT as it allows user interaction with the virtual environment. The visualization of the IoT application should be developed from layman perspective which is easy, simple and user friendly. This can be easily achieved through the advances in the touch screen and

speech recognition technologies. The change over from 2D to 3D screens implies that information is more organized and structured for the end used. The conversion of data into information to knowledge will lead to faster decision making process. The representation can be customized as the end user requirements and visualized further.

3.5 Discussion on Future of Internet of Things

As landscape of the Internet is growing at a very rapid pace, the entire world is migrating towards IOT which will have a huge impact on our lives in the coming few years. Computers, laptops, smartphones, and tablets are not the only things connecting with the internet, now there will be a multitude of smart devices connected to the internet and also to each other. Starting from home appliances such as refrigerator, microwave oven, doors to big industrial machinery. Everything will become smart. Some technology experts call it as the 'Next Digital Revolution' while others proclaim it as the 'Next Generation of Internet'.

There is a lot of scope for IoT in future. It has been estimated that there would be almost 50 billion connected devices by 2020. IoT is foreseen to touch every industry and people in every domain, optimizing businesses and simplifying people's lives. According to NASSCOM, global market size of IOT is expected to touch approximately USD 3 trillion by 2020. In this landscape, startups are playing a major role in enabling IOT services in the consumer as well as industrial segment. In India, there are more than 60% start-ups who are working in IOT solutions with their highly technical and technological skills.

IOT proves to have a huge scope as it provides a unique opportunity for businesses to turn data into insights. There are a number of contributing factors as well that drive the adoption of IOT such as improved sensors, device connections, the evolution of lifestyle and mobility. Following are some of the predictions about IoT that will see come true in the upcoming years.

3.5.1 Connected Devices

It is estimated that by 2020, the number of connected devices will increase at a much more rapid rate [34]. Commercial and Industrial sectors, powered by building automation, industrial automation and lighting, are expected to account for nearly 50% of all new connected devices between 2018 and 2030. This segment is the fastest-growing at 24.4%, with 5.4 billion IoT-enabled devices slated to hit the market by 2030 [82]. In absolute numbers, communication and consumer electronics account for the largest share of IoT connected devices. By 2030, there would be 22.7 billion such devices in these segments. Automotive and medical sectors follow, accounting for 928 million and 406 million IoT-enabled devices respectively. Figure 3.10 shows the number of connected devices (Internet of Things; IoT)

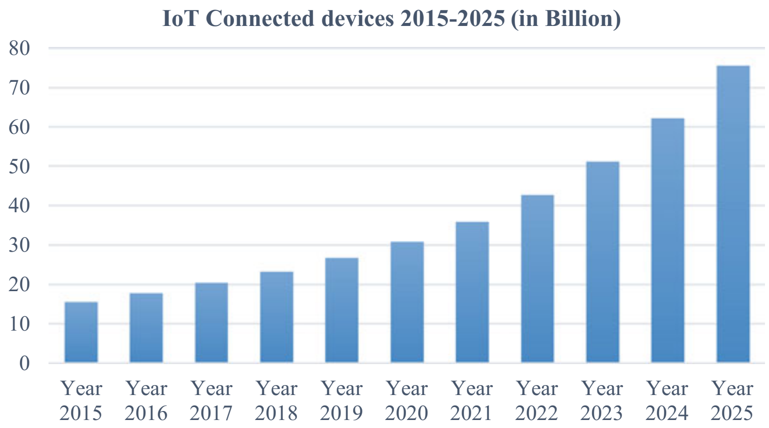

Fig. 3.10 IoTconnected devices installed base worldwide from 2015 to 2025 (in billions) [83]

worldwide from 2015 to 2025. For 2020, the installed base of Internet of Things devices is forecast to grow to almost 31 billion worldwide. The overall Internet of Things market is projected to be worth more than one billion U.S. dollars annually from 2017 onwards [83]. Moreover, for billions of smart connected devices to communicate via the Internet, there is a need of a robust naming architecture to be able to identify a smart object and to establish an access path to the object [84].

3.5.2 IoT for Hackers

Cyber security has emerged as a top concern for IoT adopters. Since IoT devices create a “Complex Management Environment” with multiple technology profiles, processing capabilities, use-cases, physical locations, etc. more data is potentially at risk. In case of IoT-enabled transportation, vehicles in motion could be compromised remotely to have a disastrous effect on passengers. IoT devices can also be embedded into systems that can affect physical health and safety [82].

In Oct 2016, first IoT malware was introduced. It had a strain of malware that has the ability to infect connected devices. This malware could easily access the devices using their default login (username and password). Then, it turns those devices into a Botnet that is then used for DDoS (Distributed Denial of Service) attacks. This attack brought many internet service websites to a screeching halt for hours. Many big hosting companies were also flooded in this attack. The code of this malware is available as open source for modification. As a result, after sometime after this attack, a modified version of this code was introduced that infected many other connected devices. Sadly, it is predicted that hackers will keep using IoT for DDoS in the future, too.

3.5.3 Smart Cities

Smart city devices are new Internet of things (IOT) applications that leverage ubiquitous connectivity, big data and analytics to enable smart city initiatives all over the world. These new applications introduce new capabilities such as the ability to remotely monitor, manage and control devices, and to create new insights and actionable information from massive streams of real-time data. Global smart city device shipments will increase from 202 million in 2017 to 1.4 billion in 2026 [82]. Using such technologies in cities would make it easier for cities to manage and collect data remotely. It will also be easier to automate different processes.

IHS Markit notes vertical applications related to physical infrastructure and mobility show particular potential for growth—in 2026 these applications are expected to comprise approximately 65 and 22% of total device shipments, respectively [83]. It believes the largest market will be Asia-Pacific with more than 700 million smart city device shipments by 2026. Other key regions will be North America and Europe, with more than 400 million and 200 million shipments, respectively.

3.5.4 Secured Routers

Many IoT devices would remain inside our homes and thus, it would be quite difficult to install any security software on them. Marketers are neglecting the security of the IoT products quite a bit. Here, a home router can play a very significant role. They are considered the data entry point of the Internet in your home. They can protect the data entrance to the internet. Today, routers do not have any security software installed on them. This means that the hackers can easily sneak malware through them. In the future, it is predicted that many secure routers will be made available for people to protect the internet from the entry point, too. Some of the features that such routers will have are:

- Data Encryption
- Secure DNS
- Automatic security updates.

3.5.5 Usage of Smart Products

As IoT has expands its reach into the home, businesses, and industrial environment. More and more devices would be connected to share data and for real-time communication and data analytics. From the consumer's point-of-view, following are some of the benefits of using smart products:

- Increased energy efficiency
- Improved safety
- Improved security
- Higher-quality product.

3.5.6 App-Specific Device Ecosystems

A model is put forward to create a semi-closed device vendor ecosystem for applications. The benefit of such a system is that with these services, it is possible for a multi-vendor ecosystem to certify different brands by their IoT gateways. The real issue is that most comprehensive device management is provided by IoT application vendors these days, which means that all the components, are bound together by a single vendor to work. For example, a smart briefcase tag device will work only with the vendor's briefcase tracking application but it is impossible to make it work with any other vendor's briefcase tracking application. In case you desire to switch to some other vendor, in that scenario you will have to buy a new tag to work with that vendor application. But with this solution, consumers can buy devices from different vendors and quickly make them work with an application.

Thus, the IoT industry needs an open device management standardization to ensure interoperability. Such efforts are already being made and will start to come to life shortly. In this way, IoT consumers will surely achieve a new maturity level, and they will then not fear losing their hardware investments.

3.5.7 IoT for Businesses

The business intelligence sector has been analyzing IoT growth for some years. It is predicted that almost USD 6 trillion will be spent on IoT solutions in the coming five years. Business will adopt IoT solutions at a bit faster rate than other sectors. The benefits they will get by following such strategies are:

- Increase in productivity
- lowering the costs of operations
- The government will also take a keen interest in such solutions to improve the quality of life of their people. They are believed to be the second-largest adopter of such solutions.

Consumers will also invest their money in the IoT ecosystems.

3.5.8 *Some Awesome Inventions*

Multi-application gas sensors are being developed that can detect bio-chemical threats and are able to recognize different diseases just by analyzing your breath. Such sensors are driving other new trends in technology.

Decrease in Air Pollution by Technology
Tired of the smog and air pollution these days? Infact, it may soon be a thing of the past and soon, the situation will be a bit different. There will be a spotlight with embedded video sensors that will be able to adjust the green and the red lights according to the traffic and the time. This solution will reduce congestion and smog, too.

Intelligent Parking System
The vehicles that we see idle at a red light in traffic burn up almost 17% of fuel consumption. The parking system will also be a bit different from what it is right now. Sensors embedded in parking systems will give real-time information about the empty spots through an app. In this way, drivers will be informed about those empty spots by the app. And do you know that almost 30% of congestion is due to drivers who keep carving the streets for hours in search an empty spot to park their vehicles?

3.6 Conclusion

Internet of Things has completely changed the way we live, communicate, play and work, however the potential is yet to be unleased. The sheer power of this technology giant will be fully utilized when the technology will impact the lives of people at every moment. It will change the way people look towards the use of technology and the ripple factor thus created will domesticate IoT. The corporate players are into the production of the devices, companies are into devising new applications, technocrats are designing new technology and protocols; and the users are using IoT solutions and services. Inspite of so much of work being done, the IoT paradigm will take more time to mature, as the technology and related concepts are still in the infant state. The economic and technology era will be helpful for the progress of IoT in the entire globe. However, we should not be blindfold by the power of this promising technology, there are many issues and challenges associated with it. More robust implementation strategies needs to be designed to maximize IoT opportunities and its exposure the world. In this paper, we have discussed past, present and future of IoT, as unless we know the technology evolution we cannot predict it future scope. The chapter is journey for the readers to understand tits and bits of IoT so that new horizons can be set by.

References

1. Khan, R., Khan, S.U., Zaheer, R., Khan, S.: Future internet: the internet of things architecture, possible applications and key challenges. In: Proceedings of Frontiers of Information Technology (FIT), pp. 257–260 (2012)
2. Alkhatib, H., Faraboschi, P., Frachtenberg, E., Kasahara, H., Lange, D., Laplante, P., Merchant, A., Milojicic, D., Schwan, K.: IEEE CS 2022 report; IEEE computer society: Washington. DC, USA (2014)
3. Shen, G., Liu, B.: The visions, technologies, applications and security issues of internet of things. E-Business and E -Government (ICEE), pp. 1–4
4. Pal, A., Mukherjee, A., Dey, S.: Future of Healthcare-Sensor Data-Driven Prognosis. International Publishing Switzerland, Springer Series in Wireless Technology (2016)
5. International Telecommunication Union—Telecommunication Standardization Sector (ITU-T). Recommendation ITU-T Y. 2060—Overview of the Internet of Things; ITU-T: Geneva, Switzerland (2012)
6. Hwang, J., Choe, Y.: Smart Cities—Seoul: A Case Study. ITU-T Technology Watch Report; International Telecommunication Union—Telecommunication Standardization Sector (ITU-T): Geneva, Switzerland (2013)
7. Cisco: The Internet of Things Reference Model; Cisco and/or its Affiliates: San Jose, CA, USA (2014)
8. OECD Committee for Digital Economy Policy: OECD Technology Foresight Forum 2014—The Internet of Things
9. Dutta, S., Geiger, T., Lanvin, B.: The Global Information Technology Report 2015—ICTs for Inclusive Growth. Geneva, Switzerland, World Economic Forum and INSEAD (2015)
10. Atzori, L., Iera, A., Morabito, G.: The internet of things: a survey. Comput. Netw.—Sci Direct **54**(15), 2787–2805 (2010)
11. Zeng, L.: A security framework for internet of things based on 4G Communication. In: Computer Science and Network Technology (ICCSNT), pp. 1715–1718 (2012)
12. Ibarra-Esquer, J.E., González-Navarro, F.F., Flores-Rios, B.L., Burtseva, L., Astorga-Vargas, M.A.: Tracking the evolution of the internet of things concept across different application Domains, Sensors **17**, 1379 (2017)
13. Laya, A., Bratu, V.I., Markendahl, J.: Who is investing in machine-to-machine communications? In: Processing 24th European registration ITS Conference, Florence, Italy, Oct. 2013, pp. 20–23 (2013)
14. Dohler, M., Vilajosana, I., Vilajosana, X., Llosa, J.: Smart Cities: An action plan. Proceedings Barcelona Smart Cities Congress, Barcelona, Spain, Dec. 2011, pp. 1–6 (2011)
15. Vilajosana, I., Llosa, J., Martinez, B., Domingo-Prieto, M., Angles, A., Vilajosana, X.: Bootstrapping smart cities through a self-sustainable model based on big data flows. IEEE Commun. Mag. **51**(6), 128–134 (2013)
16. Hernández-Muñoz, J.M., Vercher, J.B., Muñoz, L., Galache, J.A., Presser, M., Hernández Gómez, L.A., Pettersson, J.: Smart cities at the forefront of the future internet. the future internet. Lect. Notes Comput. Sci. **6656**, 447–462 (2011)
17. Mulligan, C.E.A., Olsson, M.: Architectural implications of smart city business models: an evolutionary perspective. IEEE Commun. Mag. 51(6):80–85 (2013)
18. Walravens, N., Ballon, P.: Platform business models for smart cities: From control and value to governance and public value. IEEE Commun. Mag. 51(6):72–79 (2013)
19. Bellavista, P., Cardone, G., Corradi, A., Foschini, L.: Convergence of MANET and WSN in IoT urban scenarios. IEEE Sens. J. 13(10), 3558–3567 (2013)
20. Schaffers, H., Komninos, N., Pallot, M., Trousse, B., Nilsson, M., Oliveira, A.: Smart cities and the future internet: towards cooperation frameworks for open innovation. The Future Internet. Lect. Notes Comput. Sci. **6656**, 431–446 (2011)
21. Cuff, D.; Hansen, M.; Kang, J.: Urban sensing: out of the woods. Commun. ACM, **51**(3), 24–33 (2008)

22. Lynch, J.P., Kenneth, J.L.: A summary review of wireless sensors and sensor networks for structural health monitoring. Shock Vibr. Digest **38**(2), 91–130 (2006)
23. Nuortio, T., Kytöjoki, J., Niska, H., Bräysy, O.: Improved route planning and scheduling of waste collection and transport. Expert Syst. Appl., **30**(2), 223–232 (2006)
24. Soliman, M., Elsaadany, A.: Experimental evaluation of internet of things in the educational environment. iJEP **7**(3), 50–60 (2017)
25. Elsaadany, A.: Campus crowd sensing platform using mobile computing for smart education environments. In: Proceedings of Fifth International Conference on Information Communications Technology, Alexandria (2015)
26. Atzori, L., et. al.: The social internet of things (SIoT)—when social networks meet the internet of things: concept, architecture and network characterization. Comput Netw **56**(16), 3594–3608 (2012)
27. Mashal, O.A., Chung, T.Y.: Analysis of recommendation algorithms for Internet of Things. In: IEEE Wireless Communications and Networking Conference Workshops (WCNCW), pp. 181–186 (2016)
28. Chandrahasan, M.: Survey on different smart parking techniques. Int. J. Comput. Appl. (0975–8887) **137**(13) (2016)
29. Al-Ali, A.R., Zualkernan, I., Aloul, F.: Amobile GPRS-sensors array for air pollution monitoring. IEEE Sens. J. **10**(10), 1666–1671 (2010)
30. Maisonneuve, N., Stevens, M., Niessen, M.E., Hanappe, P., Steels, L.: Citizen noise pollution monitoring. In: Proceedings of the 10th Annual International Conference on Digital Government Research: Social Networks: Making Connections between Citizens, Data and Government. Data Gov., pp. 96–103 (2009)
31. Li, X., Shu, W., Li, M., Huang, H.Y., Luo, P.E., Wu, M.Y.: Performance evaluation of vehicle-based mobile sensor networks for traffic monitoring. IEEE Trans. Veh. Technol., **58** (4), 1647–1653 (2009)
32. Lee, S., Yoon, D., Ghosh, A.: Intelligent parking lot application using wireless sensor networks. In: Proceeding International Symposium Collaborative Technologies and System Chicago, May 19–23, 2008, pp. 48–57 (2008)
33. Kastner, W., Neugschwandtner, G., Soucek, S., Newmann, H.M.: Communication systems for building automation and control. Proc. IEEE, Jun. 2005, vol. 93, no. 6, pp. 1178–1203 (2005)
34. Evans, D.: The internet of things—how the next evolution of the internet is changing everything. Cisco Internet Business Solution Group (IBSG) (2011)
35. McKinsey Global Institute, Unlocking the Potential of the Internet of Things, June 2015
36. Gartner Inc., The Internet of Things Is a Revolution Waiting to Happen, 30 April 2015
37. International Data Corporation (IDC) Explosive internet of things spending to reach $1.7 Trillion in 2020, According to IDC, 02 June 2015
38. Ashton, K.: That—Internet of things. Thing, RFiD J. (2009)
39. Sundmaeker, H., Guillemin, P., Friess, P., Woelfflé, S.: Vision and challenges for realising the internet of things. Cluster of European Research Projects on the Internet of Things—CERP IoT (2010)
40. RFC 7452: Architectural considerations in smart object networking (March 2015)
41. Thaler, D., Hannes, T., Barnes, M.: Architectural considerations in smart object networking. IETF 92 Technical Plenary—IAB RFC 7452. 6 Sept. 2015
42. Int Area Wiki—internet-of-things directorate. IOTDirWiki. IETF, n.d. Web. 06 Sept. 2015
43. http://www.comsoc.org/commag/cfp/internet-thingsm2m-research-standards-next-steps
44. Internet of Things. Oxford Dictionaries, n.d. Web. 6 Sept. 2015
45. Belissent, J.: Getting clever about smart cities: new opportunities require new business models. Forrester Res (2010)
46. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of things (IoT): a vision, architectural elements, and future directions. Future Gener. Comput. Syst. **29**, 1645–1660 (2013)

47. Bolt, R., Beranek, L., Newman, R.: A history of the ARPANET: the first decade; DARPA Report No. 4799; Bolt Beranek and Newman Inc.: Cambridge, MA, USA (1981)
48. Manley, J.H.: Embedded computers: software cost considerations. In: AFIPS '74 Proceedings of the May 6–10, 1974, National Computer Conference and Exposition; ACM Press: New York, NY, USA, pp. 343–347 (1974)
49. The "Only" Coke Machine on the Internet, Carnegie Mellon University, School of Computer Science
50. Weiser, M.: The computer for the 21st century. Sci. Am. **265**, 94–104 (1991)
51. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. Comput. Netw. **38**, 393–422 (2002)
52. Jason, P.: Bill joy's six webs. MIT Technology Review, 29 September 2005
53. Ashton, K.: That 'Internet of Things' Thing, RFID J. 22 June 2009
54. Roberti, M.: Jan. 16, 2005, "The History of RFID Technology"
55. Taso (2014) SRI consulting business intelligence—the internet of things roadmap
56. Gartner's hype cycle special report for 2017, Gartner Inc
57. Google trends, google. http://www.google.com/trends (n.d.)
58. Tech vision report https://www.accenture.com/t20180227T215953Z__w__/us-en/_acnmedia/Accenture/next-gen-7/tech-vision-2018/pdf/Accenture-TechVision-2018-Tech-Trends-Report.pdf
59. http://www.bluetooth.com and http://www.bluetooth.org
60. http://www.zigbee.org
61. http://www.z-wave.com
62. Samsung privacy policy—smart TV supplement, Samsung Corp. Web. 29 Sept. 2015
63. Meet the Nest Thermostat. Nest. Nest Labs. Web. 31 Aug. 2015
64. Marsan, D., Carolyn. (2015) IAB releases guidelines for internet-of-things developers. IETF J. 11.1: 6–8. Internet Engineering Task Force
65. From the ARPANET to the Internet by Ronda Hauben-TCP Digest (UUCP)
66. Jian, A., Xiao-Lin, G., Xin, H.: Study on the architecture and key technologies for internet of things. Adv. Biomed. Eng. **11**, IERI-2012, pp. 329–335 (2012)
67. Lan, L.: study of security architecture in the internet of things. Measur. Inf. Control (MIC), 2012, **1**, 374–377 (2012)
68. The Internet of Things, ITU Report, Nov 2005
69. Chen, W.: An IBE based security scheme of internet of things. Cloud Comput. Intell. Syst. (CCIS), pp. 1046, 1049 (2012)
70. Suo, H., Wan, J., Zou, C., Liu, J.: Security in the internet of things: a review. Comput. Sci. Electron. Eng. (ICCSEE), pp. 648–651 (2012)
71. Wu, M., Lu, T., Ling, F., Sun, L., Du, H.: Research on the architecture of Internet of things. Adv. Comput. Theory Eng. (ICACTE), pp. 484–487 (2010)
72. Cheng, X., Zhang, M., Sun, F.: Architecture of internet of things and its key technology integration based-on RFID. In: Fifth International Symposium on Computational Intelligence and Design, pp. 294–297 (2012)
73. Bandyopadhyay, D., Sen, J.: Internet of things-applications and challenges in technology and standardization. Wireless Pers. Commun. **58**(1), 49–69
74. Zhang, Y.: Technology framework of the internet of things and its application. Electr. Control Eng. (ICECE), pp. 4109–4112 (2011)
75. Khoo, B.: RFID as an enabler of the internet of things: issues of security and privacy. internet of things (iThings/CPSCom), pp. 709–712 (2011)
76. Zhang, H., Zhu, L.: Internet of things: key technology, architecture and challenging problems. Comput. Sci. Autom Eng. (CSAE), **4**, 507–512 (2011)
77. Sohraby, K., Minoli, D., Znati, T.: Wireless sensor networks: technology, protocols, and applications. Wiley, pp. 15–18 (2007)
78. Ghosh, A., Das, S.K.: Coverage and connectivity issues in wireless sensor networks: A survey. Pervasive Mobile Comput. **4**, 303–334 (2008)

79. Sang, Y., Shen, H., Inoguchi, Y., Tan, Y., Xiong, N.: Secure data aggregation in wireless sensor networks: a survey. In: 2006 Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06), pp. 315–320 (2006)
80. Rao, B.B.P., Saluia, P., Sharma, N., Mittal, A., Sharma, S.V.: Cloud computing for internet of things and sensing based applications. In: 2012 Sixth International Conference Sensing Technology (ICST), IEEE (2012)
81. Xiaohui, X.: Study on security problems and key technologies of the internet of things. In: Computational and Information Sciences (ICCIS), pp. 407–410 (2013)
82. Global business research and analytics provider IHS Markit https://cdn.ihs.com/www/pdf/enabling-IOT.pdf Accessed 09 Jun 2018
83. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/, Accessed 09 Jun 2018
84. Kopetz, H.: Internet of things. In: Real-Time Systems. Springer, Boston, MA, USA, pp. 307–323 (2011)