1

Internet of Things (IoT) Fundamentals

LEARNING OBJECTIVES

After studying this chapter, students will be able to:

- describe the evolution of the IoT concept.
- state the vision and definition of IoT.
- explain the basic characteristics of IoT.
- distinguish the IoT from other related technologies.
- elaborate the IoT enablers.
- explain the IoT architectures.
- articulate the pros and cons of IoT.
- apply the IoT architecture concepts for specific IoT applications.
- understand the implementation aspect of IoT architecture.

1.1 Introduction

In our daily lives, the augmented practice of Information and Communication Technologies (ICT) plays a paramount role in the development of emerging information societies. In developed countries, ICT is being employed to develop various innovative applications and services to address the challenges of sustainable societies, thus improving the quality of human lives. In the modern era, a plethora of things are being connected to each other using underlying network technologies with an aim to promote the paradigm of the Internet of Things (IoT). IoT is a network of uniquely identifiable connected *things* (also known as devices, objects, and items) offering intelligent computing services [1]. Things in IoT are also known as Smart Things that provide feasibility in performing the execution of daily life operations in a rational way. Moreover, IoT also positively assists the communication process among human beings. IoT comprises diversified technologies including pervasive computing, sensor technology, embedded system, communication technologies, sensor networking, Internet protocols, etc. which eventually underpin the economic growth of modern societies. The fundamental notion behind IoT is the provision of seamless ubiquitous connectivity among things and human beings. The basic idea of IoT

Enabling the Internet of Things: Fundamentals, Design, and Applications, First Edition.
Muhammad Azhar Iqbal, Sajjad Hussain, Huanlai Xing, and Muhammad Ali Imran.

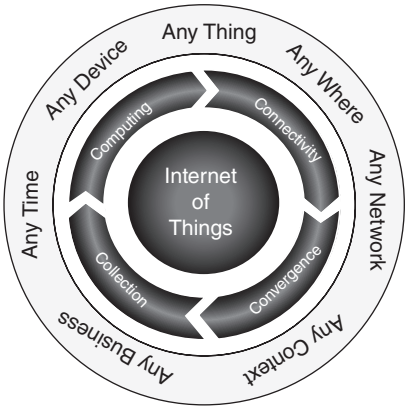


Figure 1.1 The concept of As and Cs in the IoT.

can be conceived as a representation of various As and Cs, as shown in Figure 1.1 [2]. In Figure 1.1, the As reflect the concept of ubiquity or globalization (i.e. any device, anywhere, anytime, any network etc.) and the Cs mirror the main characteristics of IoT (i.e. connectivity, computing, convergence, etc.). IoT, in essence, can be seen as an addition of the third dimension named "Thing" to the plane of ICT world, which is fundamentally based on two dimensions of Place and Time as shown in Figure 1.2. This "anything" dimension ultimately boosts the ubiquity by enabling new forms of communication of humans and things and between things themselves [3].

1.2 Evolution of IoT Concept

The concept of ubiquitous computing through smart devices dates back to the early 1980s when a Coke machine at Carnegie Mellon University was connected to the Internet and able to report its inventory of cold drinks [4, 5]. Similarly, Mark Weiser in 1991 [6] provided the contemporary vision of IoT through the terminologies of ubiquitous computing and pervasive computing. Raji in 1994 elaborated the concept of home appliance automation to entire factories [7]. In 1999, Bill Joy presented *six web* frameworks wherein device-to-device communication could be formed [8]. Neil Gershenfeld in 1999 used a similar notion in his popular book *When Things Start to Think* [9]. In the same year, the term "Internet of Things" was promoted by Kevin Ashton during his work on Radio Frequency Identification (RFID) infrastructure at the Auto-ID Center of Massachusetts Institute of Technology (MIT) [10]. In 2002, Kevin was quoted in Forbes Magazine with his saying "We need an *Internet for things*, a standardized way for computers to understand the real world" [11]. The article was entitled as *The Internet of Things*, which was the first-ever official document with the use of this term in a literal sense.

The evolution of IoT with reference to the technological progress in Internet conception is shown in Figure 1.3. The typical Internet introduced in the early 1990s was only concerned with the generation of static and dynamic contents on the World Wide Web (WWW). Later on, large-scale production and enterprise-level business

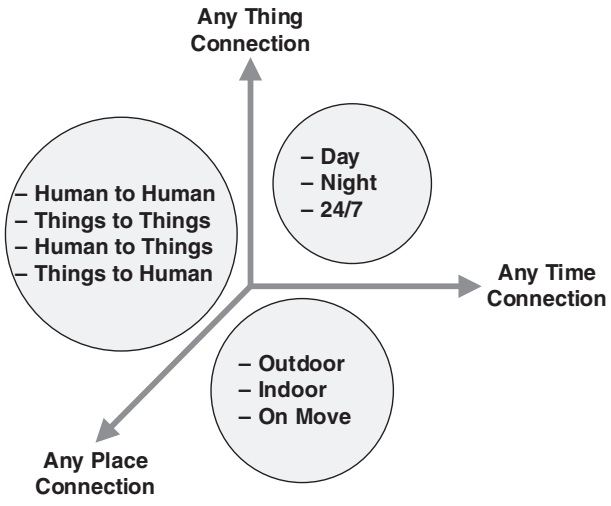


Figure 1.2 Thing as a new dimension to endorse IoT. Source: Peña-López [3].

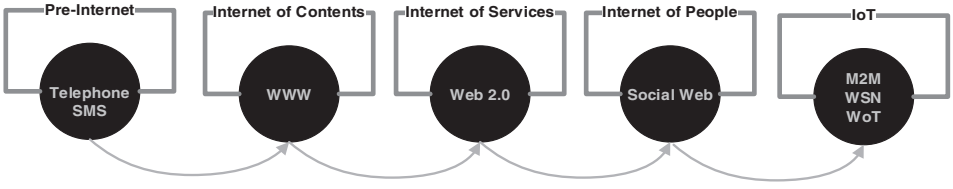


Figure 1.3 Technological progression in IoT.

collaborations initiated the creation of web services which laid the foundation of Web 2.0. Nevertheless, with the proliferation of affordable smartphones and tablets, social network apps become dominant on the Internet. In current situation, advancements in embedded system, Machine-to-Machine (M2M) communication, Cyber Physical Systems (CPS), Wireless Sensor Network (WSN), and Web of Things (WoT) technology enabled the communication of things over the Internet. The overall technological progression related to IoT is shown in Figure 1.3.

1.3 IoT Vision

The conventional WWW offers the convenience of information searching, e-mail conversation, and social networking. The emerging trend of IoT comes up with a vision of expanding these abilities through interactions with a wide spectrum of electronic appliances. In general, the IoT vision can be seen in terms of things centric and Internet centric. The things-centric vision encompasses the advancements of all technologies related to the notion of "Smart Things." On the other hand, the Internet-centric vision involves the advancement of network technologies to establish the connection of interactive smart things with the storage, integration, and management of generated data. Based on these

views, the IoT system can be seen as a dynamic distributed network of smart things to produce, store, and consume the required information [12]. The IoT vision demands significant advances in different fields of ICT (i.e. digital identification technology, communication technology, networking technology, computing technology, and distribution system technology), which are in fact the enabling technologies or fundamental elements of IoT [13, 14]. More specifically, the IoT paradigm can be envisioned as the convergence of three elementary visions, i.e. Things-oriented vision, Network-oriented vision, and Semantic-oriented vision [15, 16]. This convergence of three visions with abilities and technologies is shown in Figure 1.4.

Things-oriented vision at the initial level promotes the idea of things network through unique identifiable Electronic Product Code (EPC). Things-oriented vision in the present form is evolved into smart sensor networks. In Internet-oriented vision, Internet Protocol for Smart Object (IPSO) communities is formed to realize the challenging task of smart sensor communication. Considering unique identification through Internet Protocol (IP) addressing, IPSO communities are working for the interoperability of smart things (having sensors) to IP protocol technologies. Finally, the Semantic-oriented vision provides the solution to deal with the huge amount of data generated by the IoT devices. IoT architectural layers and associated protocols have been structured in these three envisions [17].

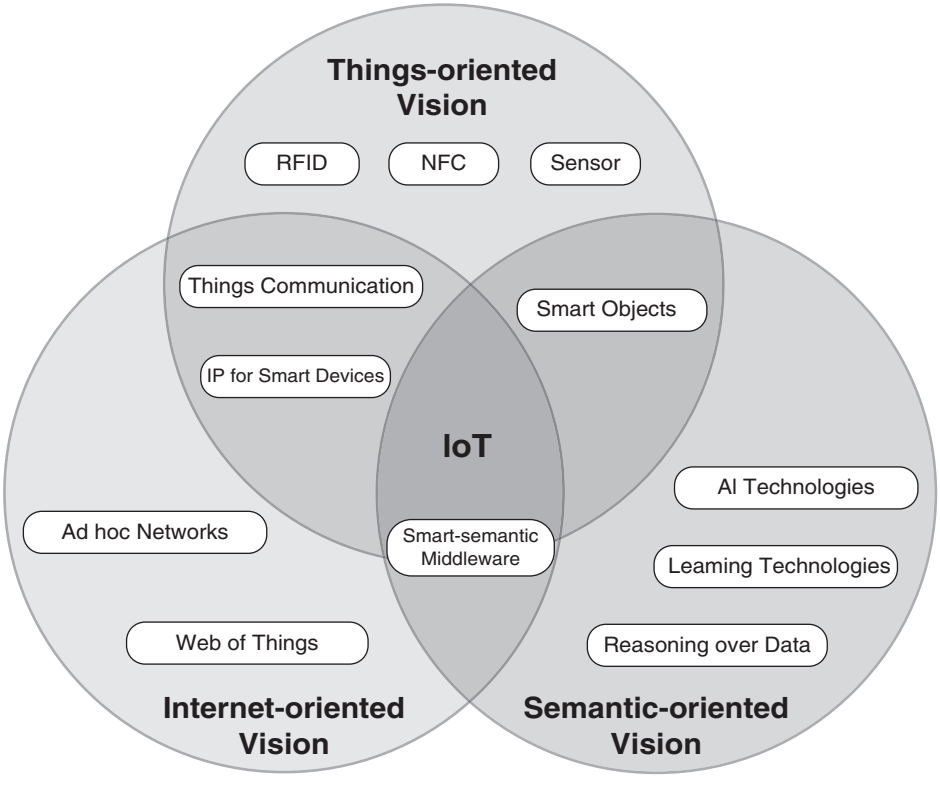


Figure 1.4 IoT as convergence of three visions. Source: Adapted from Atzori et al. [15].

1.4 IoT Definition

Considering the facts of similarity with peer technologies and envision the convergence of three different visions, it is not an easy job to provide a precise definition of IoT. In simple words, IoT could be deemed as a system wherein things are connected in such a manner that they can intelligently interact with each other as well as to humans. However, to better comprehend IoT, a number of standard organization and development bodies have provided their own definitions [13, 15, 18, 19]. A few IoT definitions presented by different standard organizations are illustrated in Table 1.1 [20].

Table 1.1 IoT definitions by standard organizations.

Standard organization	IoT definition
Institute of Electronic and Electric Engineering (IEEE)	"The Internet of Things (IoT) is a framework in which all things have a representation and a presence in the Internet. More specifically, the IoT aims at offering new applications and services bridging the physical and virtual worlds, in which Machine-to-Machine (M2M) communications represents the baseline communication that enables the interactions between Things and applications in the Cloud."
Organization for the Advancement of Structured Information Standards (OASIS)	"System where the Internet is connected to the physical world via ubiquitous sensors."
National Institute of Standards and Technology (NIST)	"Cyber Physical systems (CPS) – sometimes referred to as the Internet of Things (IoT) – involves connecting smart devices and systems in diverse sectors like transportation, energy, manufacturing, and healthcare in fundamentally new ways. Smart Cities/Communities are increasingly adopting CPS/IoT technologies to enhance the efficiency and sustainability of their operation and improve the quality of life."
International Standard Organization (ISO)	"It is an infrastructure of interconnected objects, people, systems, and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react."
Internet Engineering Task Force (IETF)	"In the vision of IoT, "things" are very various such as computers, sensors, people, actuators, refrigerators, TVs, vehicles, mobile phones, clothes, food, medicines, books, etc. These things are classified as three scopes: people, machines (for example, sensor, actuator, etc.) and information (for example, clothes, food, medicine, books, etc.). These 'things' should be identified at least by one unique way of identification for the capability of addressing and communicating with each other and verifying their identities. In here, if the 'thing' is identified, we call it the 'object'."
International Telecommunication Unit (ITU)	"IoT is type of network that is available anywhere, anytime, by anything and anyone."

1.5 IoT Basic Characteristics

Considering all perspectives of modern-day IoT systems, a few generic and vital characteristics are shown in Figure 1.5 and explained in Table 1.2 [21, 22].

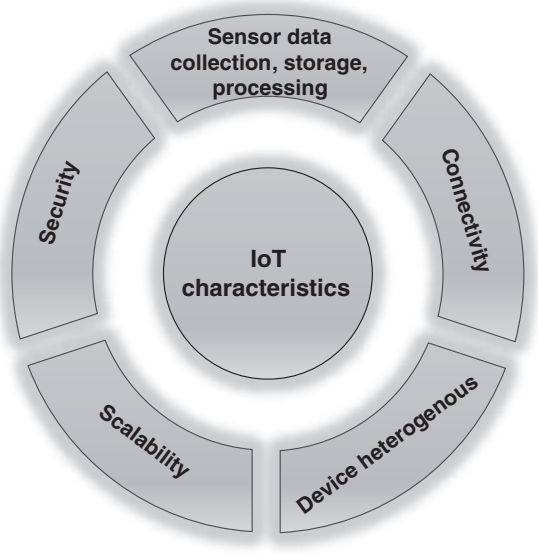


Figure 1.5 Fundamental IoT characteristics.

Table 1.2 Description of fundamental characteristics of IoT.

IoT characteristic	Description
Sensor Data Acquisition, Storage, Filtering and Analysis	The plethora of distributed Sensors (or smart things) gather observation of physical environment/entity and direct to Cloud for storage and analytics with an ultimate objective to improve business workflow
Connectivity	IoT has made possible the interconnectivity of Physical and Virtual things with the help of the Internet and global communication infrastructure (that is built using wired and wireless technologies)
Device Heterogeneity and Intelligence	The interoperability of devices (based on different hardware and network platforms) with the provisioning of ambient intelligence at the hardware/software level supports intelligent interactions
Scalability	The plethora of IoT devices connectivity shifts human interactions to device interactions
Security	The security paradigm is required to be implemented at the network level as well as the end-devices level to ensure the security of data

1.6 IoT Distinction

From the evolutionary perspective of IoT, it seems that IoT in different eras has been regarded as another name of a particular technology. Therefore, the term IoT is associated with other technologies in literature, i.e. embedded system, M2M communication, CPS, WSN, and WoT. However, the IoT concept is not attributable to any single technology.

1.6.1 IoT Versus Embedded Systems

Table 1.3 shows the differences between embedded systems and IoT.

1.6.2 IoT Versus M2M

Table 1.4 shows the differences between M2M and IoT.

1.6.3 IoT Versus CPS

CPS and IoT are highly overlapped; therefore, it is very difficult to demarcate the boundary between their differences. Both IoT and CPS encompass embedded devices that are able to transmit physically sensed data over the network. However, the use of these terms has been exploited by different communities on the basis of perceived criteria. Table 1.5 shows the differences between CPS and IoT.

Table 1.3 Difference between embedded systems and IoT.

Embedded system	IoT
Embedded systems include electronic devices that are usually standalone in nature and independently run on the Internet	IoT is a system that includes Internet connectivity-reliant devices for communication
Embedded systems are a combination of hardware and software (firmware)	IoT systems are a combination of computer hardware, software, and networking capabilities that are embedded into things of our daily lives
Embedded systems firmware mostly needs no modifications once the device is delivered to the clients	IoT requires continuous update
Example: ECG machine in a healthcare service that analyzes health parameters associated with humans is an example of embedded systems	Example: ECG machine connected to the Internet and able to transfer human health parameters on a remote server is an example of IoT devices
Embedded systems are a subset of IoT	IoT is a broader term including different technologies, i.e. embedded systems, networking, and information technology

Table 1.4 Difference between M2M and IoT.

M2M	IoT
In M2M, mostly communication type is point to point	In IoT, communication takes place at IP networks
Middleware not necessarily required for data delivery	Middleware is responsible for data delivery
Mostly, M2M devices do not rely on Internet Connection	In IoT, most of the devices require Internet connectivity
M2M devices have limited options to integrate with other devices due to corresponding communication standard requirements	In IoT, multiple communications demand unlimited integration options
M2M is a subset of IoT	IoT is a broader term which includes M2M as well as various other technologies

Table 1.5 Difference between CPS and IoT.

CPS	IoT
The term CPS is usually preferred over IoT by the engineering communities. The computer scientists working with an embedded system also used this term	The term IoT is frequently preferred over CPS by the network and telecommunications communities and the computer scientists doing research in the areas of next-generation networks and future Internet advancements
In the United States, the CPS term is preferred over IoT	In the European Union, the term IoT is preferred over CPS
CPS is considered as a system	IoT is considered as devices on the Internet
Development of effective, reliable, accurate, and real-time control system is the primary goal of CPS	BigData collection, storage, management, analysis, and sharing over Quality of Service (QoS) networks are primary goals of IoT

1.6.4 IoT Versus WSN

Table 1.6 shows the differences between WSN and IoT.

1.6.5 IoT Versus WoT

Table 1.7 shows the differences between WoT and IoT.

According to literature, the terms *embedded systems, M2M, CPS, WSNs,* and *WoT* are occasionally interchangeable with IoT; however, these are not synonyms of the term IoT. IoT is likely to be the prevailing term over all these terms. The conceptual relationship of IoT with other related technologies [23] is shown in Figure 1.6. Figure 1.6 illustrates that IoT is essentially the outcome of various existing technologies used for the collection, processing, inferring, and transmission of data.

Table 1.6 Difference between WSNs and IoT.

WSN	IoT
WSN refers to a set of dedicated sensors to monitor, record, and transmit physical parameters of an entity or environment to a central location	IoT system includes all uniquely identifiable physical things/devices (i.e. home appliances, vehicles, etc.) embedded with electronics, software, sensors, and actuators, with ubiquitous connectivity to each other over the Internet. Moreover, sensor data processing and analysis is also part of IoT
WSN is a subset of IoT	IoT is a broader term and includes various technologies other than WSNs
Example: A large collection of sensors (optionally connected) used to monitor the moisture in a field likely to be considered as WSNs	Example: A fridge having the capability of sensing and transmitting the temperature reading to the Internet is an example of a smart device in the IoT system

Table 1.7 Difference between WoT and IoT.

WoT	IoT
WoT system involves the incorporation of IoT entities over the web	IoT is a network of smart things/objects/devices, people, systems, and applications
WoT includes web-based applications over the network layer of IoT architecture	IoT applications include all sorts of applications such as web-based, android-based applications
Example: Embedded systems to connect objects over the web for communication with other objects	Example: Network of wireless devices and objects

1.7 IoT General Enablers

Mark Weiser in 1999 [13, 24] considered the general trends in technology and provided the imagination that future IT developments would not be dependent on a particular technology but would be based on the confluence of computing technologies, which ultimately results in Ubiquitous Computing. In his depiction, the world of ubiquitous computing consists of real-life objects which are capable to sense, communicate, analyze, and act according to the situation. In general, miniaturization, portability, ubiquitous connectivity, integration of a diverse range of emerging devices, and pervasive availability of digital ecosystems (i.e. Cloud) are the general enablers that play a significant role for enabling IoT systems [1, 25, 26]. Precisely, the five stages of IoT functional view or information value loop are related to data creation, data communication, data aggregation, and data analysis and are necessary actions to achieve set goals [14]. Each stage of the IoT information value loop is empowered by a specific technology. For example, an observed action in the environment creates data that is passed to different networks for communication. Communicated data is of heterogeneous nature and is required to follow standards before aggregated for the purpose of comprehensive analysis [27]. Considering this functional view, IoT systems

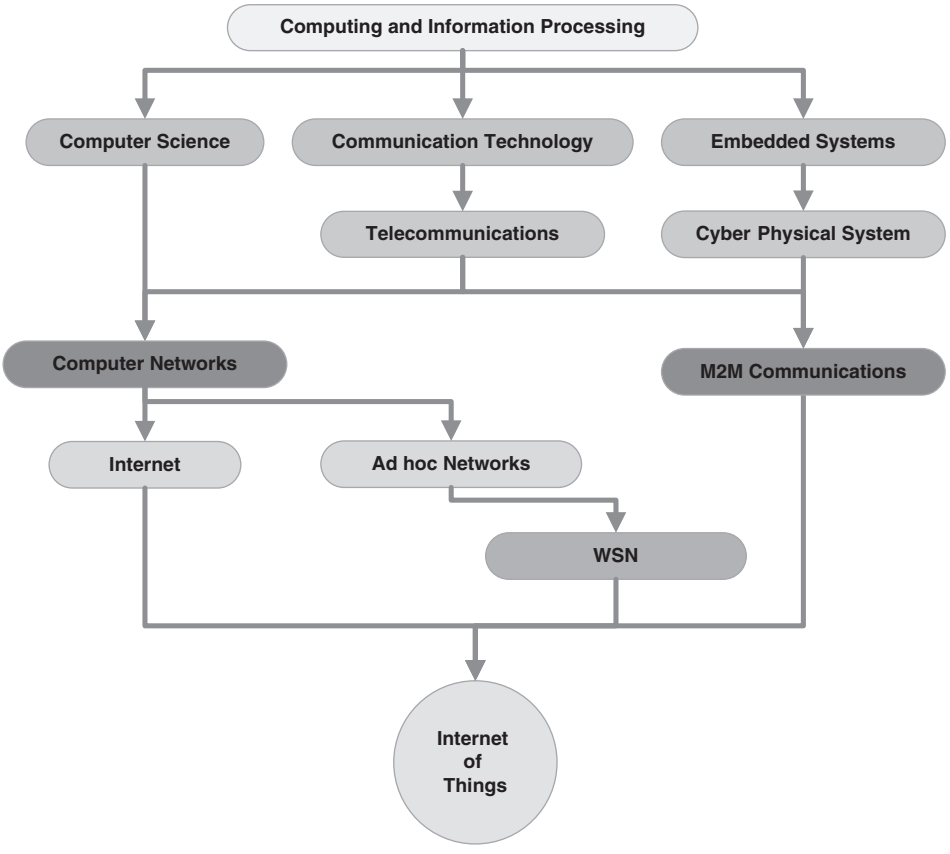


Figure 1.6 IoT relationship with peer technologies. Source: Adapted from Manrique et al. [23].

are technologically dependent upon the sensors, networks, standard aggregations, artificial intelligence, and augmented behavior as discussed in Table 1.8. Therefore, in terms of technological advancements, the following five technologies are the main reasons for the enabling of IoT [1, 13, 14, 25, 28].

The working of IoT systems revolves around the paradigm of identification, communication, interaction of anything along with the analysis on data originated from anything. Following this paradigm, details about these technologies are part of the next subsections.

1.7.1 Identification and Sensing Technologies

Nowadays, our living/working environment demands the use of electronics in various ways including computers, projectors, cameras, tags, and sensors/actuators. Smart identification of sensor/actuators and detection of physical sensation are two of the basic system-level characteristics of IoT systems [12, 26].

Identification in terms of naming and matching of smart things and services in IoT is essential, and a number of identification methods are in use (i.e. Ubiquitous Code [UCode], EPCs, Universal Product Code [UPC], Quick Response Code [QR Code], European Article

Table 1.8 IoT enabling technologies.

Technology	Description
Identification and Sensing Technologies	Include the development of devices (sensors) that converts any physical stimulus into an electronic signal
Wireless Communication and Networking	Include (network) devices that are able to communicate electronic signals
Aggregation Standardizations	Include technical standards that enable efficient data processing and allow interoperability of aggregated data sets
Augmented Intelligence	Include analytical tools that improve the ability to describe and predict relationships among sensed data
Augmented Behavior	Include technologies and techniques that improve compliance with prescribed action

Number [EAN], , etc.). Nevertheless, addressing (including IPv4 or IPv6) of IoT objects is also important to refer to its address in communication networks. Recognizing the difference between the object's identification and object's address is essential because identification methods are not globally unique. However, the addressing, in this case, is required to globally identify an object. Identification methods offer unique identity of objects within the network, and public IP addressing provides the unique identity to the smart things over the Internet [1].

Sensing in IoT involves the originating of data from interrelated smart things through the use of sensors and actuators. A sensor is basically an electronic device responsible to produce electrical, optical, and digital data deduced from the physical environment that further electronically transformed into useful information for intelligent devices or people [14]. Actuators are the technological complement of sensors that are responsible to convert an electric signal to nonelectric energy.

1.7.2 Wireless Communication and Networking

Wireless communication and wireless networking are the core of Wireless Identification and Sensing Technologies (WIST), which play a vital role in the IoT. WIST refers to RFID-based sensors and WSNs. RFID systems are the vital components of IoT. RFID stands for Radio Frequency IDentification, and it is a wireless communication technology, which uses electromagnetic fields to automatically identify tags that are attached to physical objects [29]. In general, it is stated that RFID technology has its roots in Identification of Friend or Foe (IFF) systems, used in the Second World War [30]. Basic digital identification codes have been used in IFF systems [31], which are transmitted between an interrogator and a responder to identify planes belonging to the enemy or allies. Similar to IFF technology, RFID systems utilize radio waves to identify physical objects in real-time through digital tag reading. Basically, a typical RFID consists of the following three components [29] (shown in Figure 1.7):

- An RFID Tag (also known as Transponder or Smart Label) composed of an antenna, (optional) battery, and semiconductor chip

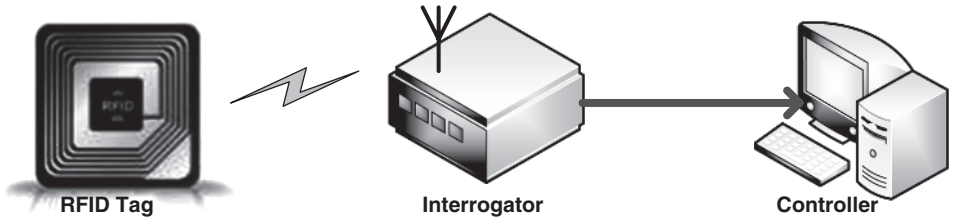


Figure 1.7 Building blocks of RFID system.

- An Interrogator (also known as Reader or read/write device) having RF module, control module, and an antenna
- A Controller (also known as Host or Workstation) to store required information in a database

The RFID tag and interrogator in the RFID system do not require line of sight and communicate with each other through radio waves. Within the transmission range, the Interrogator reads the required information (i.e. serial number, manufacturer, location, usage history, maintenance schedule, etc.) stored on the RFID tag and directs this information toward the Controller that ultimately uses this information for various purposes.

RFID tags can be of two types, i.e. Active Tags (Tags having on-board power source) and Passive Tags (Tags without an on-board power source). Active RFID Tags have greater capabilities (i.e. large memory, long read range, high data transmission rate, lower infrastructure cost, etc.) than Passive Tags but are more complex and expensive. Active Tags use battery power and are able to transmit information over a longer range. On the other hand, to transmit information, Passive RFID Tags are able to derive power from the signal received by the Interrogator. RFID usage covers a wide spectrum of application areas, i.e. object identification, asset tracking, manufacturing, supply chain management, payment systems, and location identification. Two basic power harvesting approaches, i.e. Electromagnetic Wave Capture and Magnetic Induction have been implemented [32]. (Internal details of RFID tags have been discussed in the chapter on Sensing Principles of Sensors.)

Contrary to the RFID devices, sensors in the WSN have cooperative capabilities to sense and transfer data [33]. In fact, sensed data is required to be collected to store it in a database, data warehouse, or Cloud for analysis to make in-time right decisions. These databases, data warehouses, or Cloud are located far from the place of actual data creation. Therefore, the information created by the sensors is required to be transmitted to these locations for aggregation and analysis. Typically, this kind of transmission of data in IoT involves multiple types of wireless communication and network technologies. Wireless communication in IoT emphasizes the way how heterogeneous devices are able to communicate with each other in a sustainable way that they can understand. On the other hand, wireless networking involves the interconnectivity of devices for the efficient transmission of sensed data. Various types of networks are involved in the transmission of data from the place of origination to the destination. WSN comprises many tiny sensors, which are distributed in an ad hoc manner but work in collaboration to measure and transfer

certain physical phenomena to the required destination (also known as a sink). Considering the requirements of different scenarios, Infrared (IR), Radio Frequency (RF), and optical (Laser) are three popular communication schemes used in WSNs. In addition, WSNs follow layered architecture and consists of protocols and algorithms with self-organizing capabilities. Generally, commercial WSNs technology is based on the IEEE 802.15.4 standard that ultimately provides the definition of Physical (PHY) and MAC layers for low-power communications. For the seamless connectivity to the Internet, upper layers of TCP/IP protocol stack have not been specified for WSNs. Therefore, a number of energy-efficient routing and transport layer solutions have been proposed in the literature for the efficient and reliable transmission of sensed data [34, 35].

Currently, the integration of RFID technology having sensing capabilities (Wireless Identification and Sensing Platform [WISP] project [36]) enables new types of IoT applications. WISP devices are able to sense different physical quantities (i.e. temperature, light, liquid level, acceleration, etc.) and are able to harvest energy through received reader's signal. This WISP technology permits the creation of RFID sensor networks that ultimately requires no batteries [37].

RFID, sensors, and RFID sensor are connected to the Internet through heterogeneous network devices, i.e. Bluetooth, Access Points (APs), Wi-Fi routers, Gateways, etc. Therefore, a unique IP address is required for all smart things on the Internet. IP is responsible for the provisioning of unique IP addressing over the Internet. Due to the greater scalability, IPv6 has been considered as one of the main enablers of IoT.

Smart things require continuous connectivity and need to be connected to various heterogeneous networks through switches, routers, gateways, etc. Therefore, the right choice of network technology is essential. Depending on the range and/or rate of data transmission, a number of network technologies are available, i.e. USB, Ethernet, Bluetooth, ZigBee, Near Field Communication (NFC), Wi-Fi, WiMax, 2G/3G/4G (Long Term Evolution [LTE]) [14, 28], etc. These technologies can be classified as Wired (including USB and Ethernet) and Wireless (including Bluetooth, NFC, Wi-Fi, WiMax, and 2G/3G/4G [LTE]). Connectivity type and network type of different communication technologies are given in Table 1.9.

Table 1.9 Wireless technologies.

Technology	Connectivity type	Network type
USB	Wired	Personal Area Network
Ethernet	Wired	Local Area Network
Bluetooth/Bluetooth Low Energy	Wireless	Personal Area Network
ZigBee	Wireless	Personal Area Network
Near Field Communication (NFC)	Wireless	Personal Area Network
Wi-Fi	Wireless	Local Area Network
WiMax	Wireless	Metropolitan Area Network
2G/3G/4G, LTE/LTE-Adv.	Wireless	Wide Area Network

Factors (other than Data Rate and Transmission Range) that drive the adoption of network technology for a particular IoT system includes Internet transit prices, IPv6 adoption, power efficiency, security/privacy [14, 15], etc.

1.7.3 Aggregation Standardization

Aggregation refers to the gathering of sensed data in a way that eases the process of handling, processing, and storage of data. Aggregation, besides providing the ease of handling, is also helpful to extract meaningful conclusions for future decision-making. Within the context of data aggregation in IoT, Standardization is one of the most important issues. So far, relational databases and SQL have been considered for storing and querying of structured data. However, no standard is available to handle unstructured data. IoT promises the scalability of billions of devices that ultimately demand common standards in order to communicate and aggregate the data of heterogeneous nature. The existing Internet standards had been developed without the consideration of IoT vision. Correspondingly, IoT systems have been developed using proprietary protocols that eventually make the communication problematic among IoT devices. Standardization is inevitable within the domain of IoT and is essential to guarantee interoperability, scalability, alike data semantics, security, and privacy [38, 39]. Several standards are required to be followed to realize data aggregation in IoT. However, Technology Standards and Regulatory Standards are two broad categories of standards, which are related to the process of aggregation [14].

Technology standards include network protocols (set of rules dealing with the identification and connectivity among devices), communication protocols (set of rules with the provision of a common language for devices' communication), and data-aggregation protocols (set of rules that assist the aggregation and processing of sensed data).

Hitherto, not a single or universal standardization body exists to make IoT technology standards. However, few standardization organizations are active at different level, i.e. international, regional, and national level (described in Table 1.10) [40].

On the other hand, regulatory standards are important in the evolution of IoT and deal with the ownership, use, and sale of the data. Envisioning the scale of emerging IoT application, the US Federal Trade Commission defined recommendations called Fair Information Practice Principles (FIPPs), which must be considered. For example, rules in FIPPs state that:

- Before data collection, concerned users must be notified and given options to choose about the usage of their personal information.
- After the usage of the required information, data must be deleted.
- Organizations must care about the security and privacy of collected data.

However, until now, it is undecided about the main organization which would be responsible for the implementation of regulatory standards for IoT applications [14].

1.7.4 Augmented Intelligence

Analysis of collected data demands the practice and advancements of different augmented cognitive technologies. Augmented intelligence enables the automation of systems to

Table 1.10 Standardization organizations at different levels.

Organization	Active at
NoSQL	International Level
MapReduce and Hadoop Distributed File System (HDFS)	International Level
Institute of Electric and Electronic Engineers (IEEE)	International Level
Internet Engineering Task Force (IETF)	International Level
International Telecommunication Unit (ITU-T)	International Level
One M2M	International Level
European Telecommunications Standards Institute (ETSI)	Regional Level
Korean Agency for Technology and Standards (KATS)	National Level
Telecommunication Standards Development Society, India	National Level
Global ICT Standardization Forum for India (GISFI)	National Level
Bureau of Indian Standards (BIS)	National Level

Source: Based on Pal et al. [40].

perform descriptive (amenable representation of data to recognize insights), predictive (to foresee future consequences), and prescriptive (related to optimization) analysis [41]. SAS Visual [42] and Tableau [43] are examples of tools that are helpful in (big) data analysis through visualization, which is an unavoidable aspect of business analytics. Predictive analysis performs analysis on historical data to find future trends through the use of machine learning approaches by avoiding explicit programming instructions. Hadoop, Spark, Neo4j, etc. are different tools that have been proposed to support predictive analysis on (big) data. However, these technologies need to be more matured because in many practical applications, it is very difficult to forecast a future trend even if there exists a strong correlation between entities. Prescriptive analysis techniques improve prescribed accuracy in decision optimizations. Computer vision, natural-language processing, and speech recognition are a few examples of cognitive technologies that are playing an important role in predictive and prescriptive analytics. Computer vision techniques are mostly used to process images for different types of diagnoses and predictions of medical diseases. Natural language processing and speech recognition techniques are preferred to perform analysis related to the expressions and transcription of words in text and accent in speech. Applications include voice control computer systems, spam e-mail detection, medical dictation, etc. Availability of BigData generated through IoT devices, high demands of crowdsourcing, advancements in analysis tools and real-time data processing are the main driving factors for augmented intelligence [14].

1.7.5 Augmented Behavior

Augmented behavior involves the actions that are required to perform while considering all phases of the information value loop, i.e. from sensing to data analysis. Following the

changes in people's behavior and organizational processes, augmented behavior supports the manifestation of suggestive actions with the use of advanced technologies (i.e. M2M and Machine to Human [M2H]). At this phase of the information loop, IoT concerns transferred from data science to behavioral sciences. Advancements in M2M and M2H are main driving forces that support the cognitive and actuation abilities of machines to understand the environment and act logically, respectively [14].

1.8 IoT Architectures

In the Internet, communication is based on a layering stack of TCP/IP protocols. Similarly, the IoT paradigm is a multilayer technology that supports meaningful communication of billions of smart things equipped with a processor, sensor/actuator, and communicator. Considering basic IoT elements (as shown in Figure 1.8), the IoT essentially connects a diverse range of hardware devices to a plethora of application domains. The heterogeneity of application and hardware domains imposes varied significant challenges that are essential to meet for the successful deployment of simple and complex IoT systems [44]. In addition to heterogeneity, considering all time ubiquitous connectivity, IoT needs to address a diverse range of issues including scalability, interoperability, security/privacy, and QoS for high traffic/storage needs that ultimately affect the architecture of IoT systems. A number

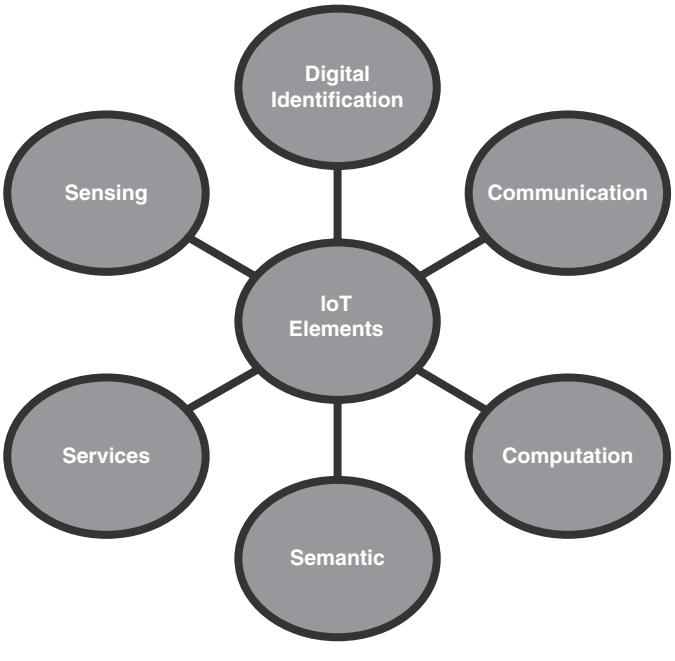


Figure 1.8 IoT elements.

of IoT architectures have been proposed in the literature. These architectures are varied not only with each other's functionalities but also in technical terminologies. Interoperability between different IoT systems is limited as the proposed architectures have not yet converged to a single reference architecture [44, 45]. Therefore, there is a need for a layered architecture that is central to all IoT projects. In this chapter, from the pool of proposed IoT architectures, the functionality of each layer of the following IoT architectures has been explicated:

- Three-layer IoT architecture
- Five-layer IoT architecture
- Six-layer IoT architecture
- Seven-layer architecture

1.8.1 Three-layer IoT Architecture

The simplest IoT architecture consists of three layers, i.e. perception, network, and application layers [1, 28, 46] as shown in Figure 1.9.

1.8.1.1 Perception Layer

The perception layer at the bottom of IoT architecture is responsible for the collection of various types of information through physical sensors or components of smart things (i.e. RFID, sensors, objects with RFID tags or sensors, etc.). Moreover, the perception layer transmits the processed information to the upper network layer via service interfaces. The main challenge at the perception layer is related to the recognition and perception of environmental factors through the use of low-power and nanoscale technology in

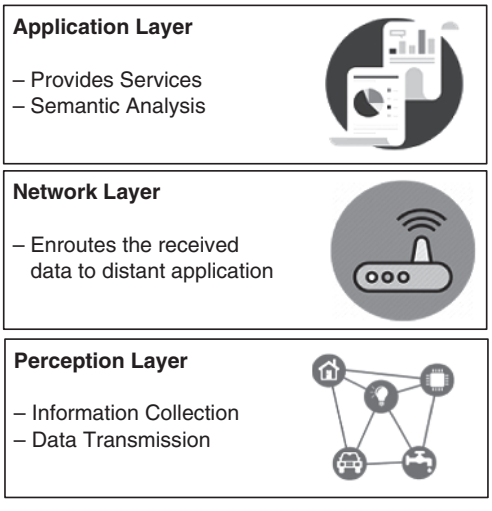


Figure 1.9 Three-layer IoT architecture.

smart things.

1.8.1.2 Network Layer

The middle layer in three-layer IoT architecture is Network (also known as transmission) layer. The network layer accepts processed information from the perception layer and forward the received data to distant application interface(s) by using integrated networks, the Internet and other communication technologies. A number of communication technologies (i.e. Wireless Local Area Networks (WLAN), Wi-Fi, LTE, Bluetooth Low Energy [BLE], Bluetooth, 3G/4G/5G, etc.) are integrated with IoT gateways that handle heterogeneous types of data to or from different things to applications and vice versa. In addition to network operations, the Network layer in some cases enhances to perform information operations within the Cloud.

1.8.1.3 Application Layer

The application layer at the top of the three-layer IoT architecture is responsible for the provisioning of services requested by the users, e.g. temperature, moisture, humidity, air pressure, light intensity measurements, etc. In addition to the user-requested services, the application layer provides data services (i.e. Data warehousing, BigData storage, data mining, etc.) to perform semantic data analysis. Smart health, intelligent transportation

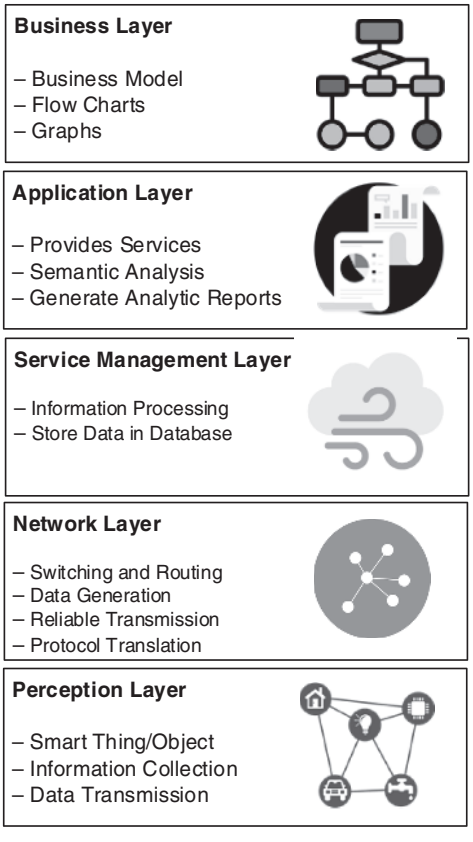


Figure 1.10 Five-layer IoT architecture.

system, smart building, smart industry, and smart city are some of the applications with smart user interfaces at the application layer.

1.8.2 Five-Layer IoT Architecture

Object (Perception), Object Abstraction (Network), Service Management (middleware), Application, and Business are the names of the five layers in five-layer IoT architecture [1, 47] as shown in Figure 1.10. Each layer is briefly explained in the following sections.

1.8.2.1 Object (Perception) Layer

The object layer primarily deals with the identification, collection, and processing of object-specific information (i.e. temperature, humidity, motion, chemical changes, etc.) through a diverse range of physical sensors. The object layer is also known as the perception layer or device layer. Physical sensors at this layer are based on different sensing principles (i.e. capacitance, induction, piezoelectric effect, etc.) and are responsible to digitize and transfer sensed data to Object Abstraction layer through secured channels. BigData is initialized at this layer.

1.8.2.2 Object Abstraction (Network) Layer

Object Abstraction Layer or Network layer is responsible for secure data transmission from physical sensors to information processing systems by using various technologies, i.e. Wi-Fi, Infrared, ZigBee, BLE, WiMax, GSM, 3G/4G/5G, etc. In other words, the Network layer transfers the sensed information from the perception layer to the Service Management layer of the IoT layering stack.

1.8.2.3 Service Management (Middleware) Layer

The smart things in IoT implement a diverse range of services, and each smart thing is connected and capable to communicate with smart objects that have implemented the same type of services. The service management layer provides pairing of services with its requesters' applications and enables IoT application programmers to deal with heterogeneous data created by smart things with different hardware specifications. This layer includes the processing of received data before transmitting to the application layer.

1.8.2.4 Application Layer

The application layer in five-layer IoT architecture is responsible for the provisioning of services requested by the users, e.g. temperature, moisture, humidity, air pressure, light intensity measurements, etc. In addition to the user-requested services, the application layer provides data services (i.e. Data warehousing, BigData storage, data mining, etc.) to perform semantic data analysis. Smart health, intelligent transportation system, smart building, smart industry, and smart city are some of the applications with smart user interfaces at application layers.

1.8.2.5 Business Layer

The business layer is responsible to manage overall activities/services of the IoT system through the creation of flowcharts, business models, and graphs on received processed

data from the application layer. In addition, based on BigData analysis, this layer supports automatic decision-making as well as the making of smart business strategies.

A few authors have suggested another five-layer SoA-based architecture consisting of Objects, Object Abstraction, Service Management, Service Composition, and Application layers [15].

1.8.3 Six-layer Architecture

The six-layer architecture comprises of Focus Layer, Cognizance Layer, Transmission Layer, Application Layer, Infrastructure Layer, and Competence Business Layer as shown in Figure 1.11. This architecture model is proposed to design the integration of more than one IoT system (focusing on different subject areas) and analyzing their implications on business value [48, 49].

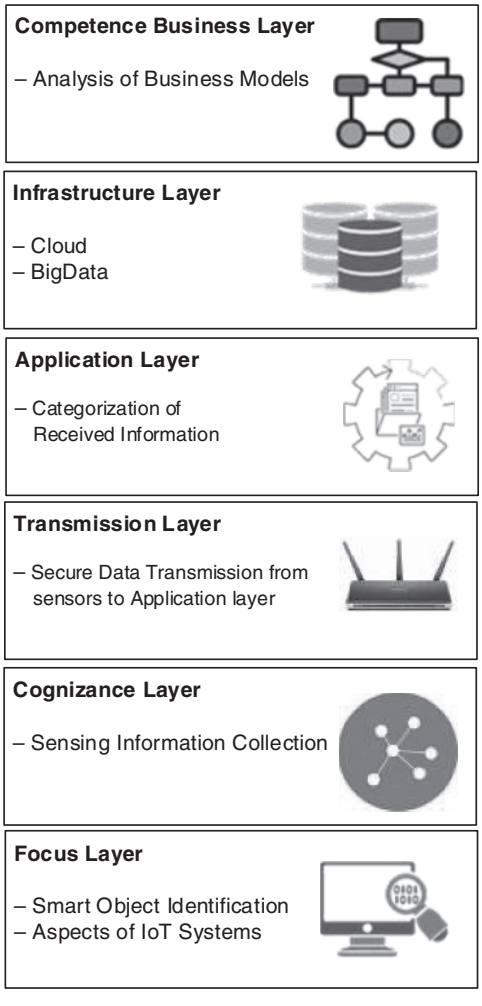


Figure 1.11 Six-layer IoT architecture.

1.8.3.1 Focus Layer

The modules at this layer are responsible for the identification of smart objects while focusing on the aspects of IoT systems under consideration.

1.8.3.2 Cognizance Layer

This layer consisting of sensors, actuators, and data monitoring modules is responsible for the collection of sensing information from smart objects (identified in the Focus layer).

1.8.3.3 Transmission Layer

This layer is responsible for the transmission of sensed data from the cognizance layer to the application layer.

1.8.3.4 Application Layer

This layer is responsible for the categorization of received information on the basis of application modes.

1.8.3.5 Infrastructure Layer

This deals with the availability of service-oriented technologies, i.e. Cloud, BigData, data mining, etc.

1.8.3.6 Competence Business Layer

This layer includes the analysis of business models of IoT systems.

1.8.4 Seven-layer Architecture

Seven-layer IoT architecture comprises seven layers including Things, Edge Computing, Data Accumulation, Data Abstraction, Application, People collaboration and processes layer (as shown in Figure 1.12). The architecture provides the simplest way to understand the functionality of IoT systems [50]. The functionality of each layer is described in the following:

1.8.4.1 Layer 1: Things Layer

The Things layer comprises endpoint devices of IoT systems including smart things (with sensors and controllers) and smart mobile devices (i.e. smartphones, tablets, Personal Digital Assistant [PDA], etc.) to send and receive information. The Things layer supports a diverse range of devices in terms of form, size, and sensing principles; the layer is capable to gather data and conversion of analog observations to digital signals.

1.8.4.2 Layer 2: Connectivity

Considering a diverse range of communication and networking protocols, the connectivity layer is responsible for the in-time transmission of observed data within and between smart things of level 1 and across different networks. In other words, horizontal communication between smart things of level 1 and switching/routing and secure data transmission at different network levels are the basic functionalities of this layer. Although, communication and connectivity through existing IP-enabled network standards is the main focus of IoT

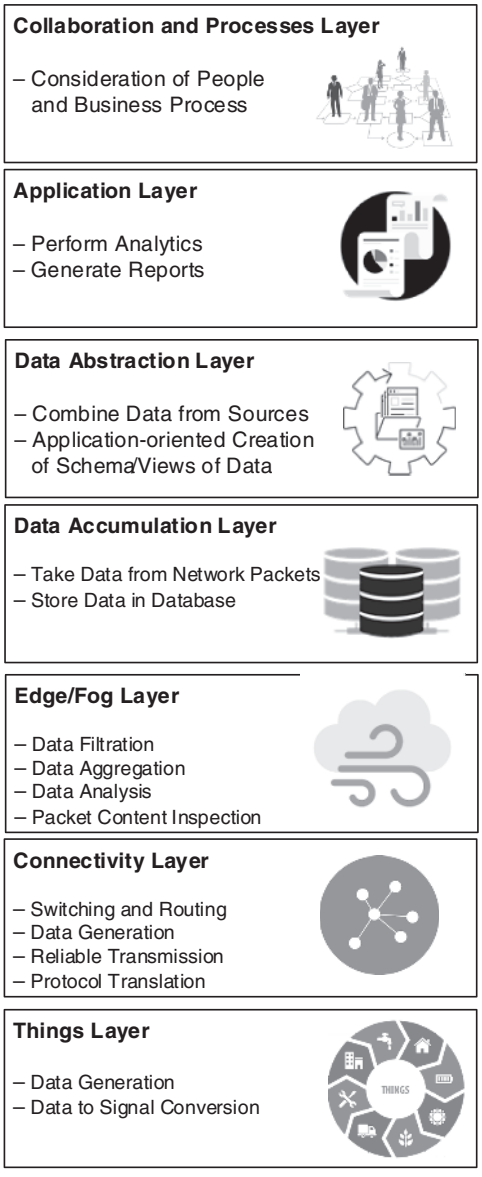


Figure 1.12 Seven layer IoT architecture.

reference architecture, however, the involvement of non-IP-enabled devices demands gateway standardization.

1.8.4.3 Layer 3: Edge/Fog Computing

Edge/Fog Computing layer is responsible for the conversion of heterogeneous network data flows into information that is appropriate in terms of storage and analysis. According to the notion of early information processing in intelligent IoT systems, this layer initiates

limited processing on the received data at the edge of the network, which is mostly referred to as Fog computing. Data formatting, reduction, decoding, and evaluation are the basic functionalities of this layer. The focus of this layer is vertical communication between level 1 and level 4. IoT gateway is an example device at this level.

1.8.4.4 Layer 4: Data Accumulation

Data accumulation or placement of moving data on disk is done at this layer. In other words, at this layer, event-based data is converted to query-based data for processing. Considering the interests of higher layers in available accumulated data, this layer performs filtering or selective storing to reduce data.

1.8.4.5 Layer 5: Data Abstraction Layer

The main focus at the data abstraction layer is related to the rendering and storage of data in such a way that reconciles all the differences in data formats and semantics for the development of simple and performance-enhanced applications.

1.8.4.6 Level 6: Application Layer

Considering the application requirements, the interpretation of level 5 data is done at this layer. Applications are diverse in nature (including system management and control applications, business applications, mission-critical applications, analytical applications, etc.); therefore, relevant data interpretation demands vary from application to application. If data is efficiently organized at layer 5, then information processing overhead gets reduced at this layer, which ultimately supports parallel activities at end devices.

1.8.4.7 Layer 7: Collaboration and Processes

In IoT, different people with different aims use the same application. Therefore, in IoT, the ultimate objective is not the creation of applications but the empowerment of people to do work in a better way. In collaboration and communication for business, processes mostly transcend multiple IoT applications.

1.9 Advantages and Disadvantages of IoT

The pros and cons associated with developed and upcoming IoT systems are described in Table 1.11.

Review Questions

1.1 How is IoT distinct from other peer technologies, i.e. M2M, CPS, and WSNs?

1.2 With the help of a diagram, explain the concept of the Information Value Loop. How is it related to IoT?

Table 1.11 Pros and cons of IoT.

Advantages	Disadvantages
Enhanced comfort and convenience through IoT-based ambient assisted living (AAL) applications improve the quality of life	Interoperability and compatibility of heterogeneous devices in IoT systems
In IoT-based systems, device-to-device interactions provide better efficiency in terms of fast reception of accurate results that ultimately save time	The complexity of IoT-based systems results in more failures
Automation of daily activities through IoT devices provides a better quality of services	There exist risks of increased unemployment in societies due to the adoption of IoT-based systems in the industrial sector
Optimum utilization of resources in IoT systems saves money	The ubiquitous and pervasive nature of IoT systems has increased the risks of losing security and privacy

1.3 Explain the difference between technology standards and regulatory standards.

1.4 Is it possible to differentiate Augmented Behavior from Augmented Intelligence? If Yes, then how?

1.5 Explain the driving factors that support the use of standardization and augmented intelligence.

1.6 What is the importance of layered architecture? Identify the components and functionality of each layer of the seven-layer IoT architecture.

1.7 A company launched an IoT-based application called *CureMe* for the monitoring and management of healthcare of chronic disease patients in a city. The *CureMe* application is designed for:

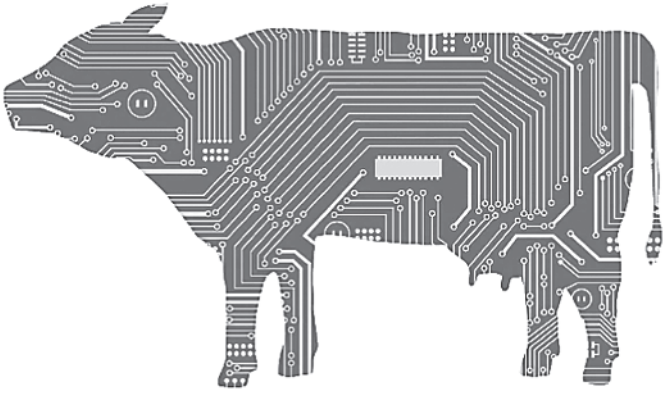
- **A** Personal usage as the mobile platform is capable to generate alerts for caregivers when something goes wrong about the vital sign readings of chronic disease patients
- **B** Government agencies with the provisioning of the web platform to analyze disease trends in the city

Considering the implementation perspective of an IoT system, provide a clear architecture diagram of *CureMe* application. All five IoT building blocks are required to be shown in this IoT-based healthcare architecture diagram. Moreover, working details of all involved components (for *CureMe* Application) are required to be explained.

1.8 For good quality milk production, monitoring cows' activity in the farm is one of the main factors that demand nonstop (24×7) monitoring of every single cow on the farm. To address this challenge, a company launched an IoT-based application

(called Ida – Intelligent Dairy Farmers Assistant) for dairy farmers. Ida combines sensor technology, machine learning, and Cloud computing to translate obtained cows' data from the farm into meaningful information that can be used to support decisions made by farmers every day. Therefore, Ida not only monitors the activities of all cows at the farm but also uses AI to learn the behavior of cows to generate information that is useful for the farmers. Thinking about the implementation perspective of an Ida-like IoT system, it is required from you to answer the following questions:

A Consider the following figure. Mark the boundary of any five parts of cow and label with respective five types of sensors that can be used to monitor cow activities that ultimately affect the quality of milk.



Source: Financial Times www.ft.com.

B Provide a clear IoT-based system architecture diagram of the Ida-like system.

References

1 Al-Fuqaha, A., Guizani, M., Mohammadi, M. et al. (2015). Internet of things: a survey on enabling technologies, protocols, and applications. *IEEE Communication Surveys and Tutorials* 17 (4): 2347–2376.

2 Gupta, R. and Gupta, R. (2016). ABC of Internet of Things: advancements, benefits, challenges, enablers and facilities of IoT. In: *IEEE Symposium on Colossal Data Analysis and Networking (CDAN)*, 1–5. IEEE.

3 Peña-López, I. (2005). *ITU Internet report 2005: the Internet of Things*.

4 Ornes, S. (2016). Core concept: the internet of things and the explosion of interconnectivity. *Proceedings of the National Academy of Sciences* 113 (40): 11059–11060.

5 *The "Only" Coke Machine on the Internet* (2018). Carnegie Mellon University, www.cs.cmu.edu/~coke/history_long.txt.

6 Weiser, M. (1999). The computer for the 21st century. *Mobile Computing and Communications Review* 3 (3): 3–11.

7 Raji, R.S. (1994). Smart networks for control. *IEEE Spectrum* 31 (6): 49–55.

8 Pontin, J. (2005). *ETC: Bill Joy's Six Webs*, MIT Technology Review.

9 Gershenfeld, N.A. and Gershenfeld, N. (2000). *When Things Start to Think*. Macmillan.

10 Mattern, F. and Floerkemeier, C. (2010). From the internet of computers to the internet of things. In: *From Active Data Management to Event-Based Systems and More*, 242–259. Springer.

11 Schoenberger, C.R. (2002). The internet of things. *Forbes*: 155160–155160.

12 Miorandi, D., Sicari, S., De Pellegrini, F. et al. (2012). Internet of things: vision, applications and research challenges. *Ad Hoc Networks* 10 (7): 1497–1516.

13 Gubbi, J., Buyya, R., Marusic, S. et al. (2013). Internet of things (IoT): a vision, architectural elements, and future directions. *Future Generation Computer Systems* 29 (7): 1645–1660.

14 Holdowsky, J., Mahto M., Raynor M.E. et al. (2015). *Inside the internet of things (IoT)*. Deloitte Insights. August, 2015.

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

16 Parnian, A.R., Parsaei, M.R., Javidan, R. et al. (2017). Smart objects presence facilitation in the internet of things. *International Journal of Computer Applications* 168 (4): 25–31.

17 Weyrich, M. and Ebert, C. (2016). Reference architectures for the internet of things. *IEEE Software* 1: 112–116.

18 Atzori, L., Iera, A., and Morabito, G. (2017). Understanding the internet of things: definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Networks* 56: 122–140.

19 Borgia, E. (2014). The internet of things vision: key features, applications and open issues. *Computer Communications* 54: 1–31.

20 Minerva, R., Biru, A., and Rotondi, D. (2015). Towards a definition of the internet of things (IoT). *IEEE Internet Initiative* 1: 1–86.

21 Rose, K., Eldridge, S., and Chapin, L. (2015). *The Internet of Things: An Overview–Understanding the Issues and Challenges of a More Connected World*. The Internet Society (ISOC).

22 Mukhopadhyay, S.C. and Suryadevara, N.K. (2014). Internet of things: challenges and opportunities. In: *Internet of Things*, 1–17. Springer.

23 Manrique, J.A., Rueda-Rueda, J.S., Portocarrero, J.M. (2016). Contrasting internet of things and wireless sensor network from a conceptual overview. IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 252–256.

24 Weiser, M., Gold, R., and Brown, J.S. (1999). The origins of ubiquitous computing research at PARC in the late 1980s. *IBM Systems Journal* 38 (4): 693–696.

25 Want, R., Schilit, B.N., and Jenson, S. (2015). Enabling the internet of things. *Computer* 1: 28–35.

26 Raj, P. and Raman, A.C. (2017). *The Internet of Things: Enabling Technologies, Platforms, and Use Cases*. Auerbach Publications.

27 Kejriwal, S. and Mahajan, S. (2016). *Smart Buildings: How IoT Technology Aims to Add Value for Real Estate Companies*. Deloitte Center for Financial Services.

28 Lin, J., Yu, W., Zhang, N. et al. (2017). A survey on internet of things: architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal* 4 (5): 1125–1142.

29 Hunt, V.D., Puglia, A., and Puglia, M. (2007). *RFID: A Guide to Radio Frequency Identification*. Wiley.

30 Violino, B. (2005). The history of RFID technology. *RFID Journal* 16.

31 Bowden, L. (1985). The story of IFF (identification friend or foe). *IEE Proceedings A (Physical Science, Measurement and Instrumentation, Management and Education, Reviews)* 132 (6): 435–437.

32 Kaur, M., Sandhu, M., Mohan, N. et al. (2011). RFID technology principles, advantages, limitations & its applications. *International Journal of Computer and Electrical Engineering* 3 (1): 151.

33 Ruiz-Garcia, L., Lunadei, L., Barreiro, P. et al. (2009). A review of wireless sensor technologies and applications in agriculture and food industry: state of the art and current trends. *Sensors* 9 (6): 4728–4750.

34 Akkaya, K. and Younis, M. (2005). A survey on routing protocols for wireless sensor networks. *Ad Hoc Networks* 3 (3): 325–349.

35 Jones, J. and Atiquzzaman, M. (2007). Transport protocols for wireless sensor networks: state-of-the-art and future directions. *International Journal of Distributed Sensor Networks* 3 (1): 119–133.

36 Radoslav, L. (2012). *Wireless Identification and Sensing Platform*. PON Press.

37 Philipose, M., Smith, J.R., Jiang, B. et al. (2005). Battery-free wireless identification and sensing. *IEEE Pervasive Computing* 4 (1): 37–45.

38 Sen, J. (2018). *Internet of Things: Technology, Applications and Standardization*. IntechOpen.

39 Pal, A. and Purushothaman, B. (2016). *IoT Technical Challenges and Solutions*. Artech House.

40 Pal, A., Rath, H.K., Shailendra, S. et al. (2018). *IoT Standardization: the Road Ahead. Internet of Things-Technology, Applications and Standardization*, 53–74. IntechOpen.

41 Davenport, T. and Harris, J. (2017). *Competing on Analytics: Updated, with a New Introduction: The New Science of Winning*. Harvard Business Press.

42 Abousalh-Neto, N.A. and Kazgan, S. (2012). Big data exploration through visual analytics. In: *2012 IEEE Conference on Visual Analytics Science and Technology (VAST)*, 285–286. IEEE.

43 Murray, D.G. (2013). *Tableau your Data!: Fast and Easy Visual Analysis with Tableau Software*. Wiley.

44 Krco, S., Pokric, B., and Carrez, F. (2014). Designing IoT architecture (s): a European perspective. In: *IEEE World Forum on Internet of Things (WF-IoT)*. IEEE.

45 Wang, W., De, S., Toenjes, R. et al. (2012). A comprehensive ontology for knowledge representation in the internet of things. In: *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, 1793–1798. IEEE.

46 Mahmoud, R., Yousuf, T., Aloul, F. et al. (2015). Internet of things (IoT) security: current status, challenges and prospective measures. In: *IEE 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, 336–341. IEEE.

47 Khan, R., Khan, S.U., Zaheer, R. et al. (2012). Future internet: the internet of things architecture, possible applications and key challenges. In: *IEEE 10th International Conference on Frontiers of Information Technology*, 257–260. IEEE.

48 Kumar, N.M., Dash, A., and Singh, N.K. (2018). Internet of Things (IoT): an opportunity for energy-food-water nexus. In: *IEEE International Conference on Power Energy, Environment and Intelligent Control (PEEIC)*, 68–72. IEEE.

49 Kumar, N.M. and Mallick, P.K. The Internet of Things: insights into the building blocks, component interactions, and architecture layers. *Procedia Computer Science 132*: 109–117.

50 CISCO Draft (2014). *The Internet of Things Reference Model*. (White Paper), Available at: http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf.