

Internet of Things: State-of-the-art, Challenges, Applications, and Open Issues

Hany F. Atlam^{1,2*}, Robert J. Walters¹, Gary B. Wills¹

¹University of Southampton, Southampton, ²Menoufia University, Menoufia, Egypt

Abstract

The Internet of Things (IoT) has become one of the unprecedented research trends for both academic and commercial organizations. Every day, the publicity of the IoT is increased. This is because the unlimited benefits that the IoT can bring to our environment. The IoT has the ability to connect almost all objects of real-world to communicate and cooperate with each other over the Internet to facilitate generating new applications and services that can improve our quality of life. This paper provides an overview of the IoT system with highlighting its applications, challenges, and open issues. It starts with discussing the state-of-the-art of the IoT system and its layered architecture. This is followed by discussing different characteristics of the IoT with presenting a comparison between common IoT communication technologies. Different IoT applications and challenges are also discussed. At the end, open research directions related to the IoT are also presented.

1. Introduction

Currently, the Internet of Things (IoT) becomes a broadly examined subject among researchers, specialists and experts. It is considered as the next stage of the evolution of the Internet. Although the Internet has passed several stages since it was invented in the mid 1980s, as it switched from a couple of PCs communicating with each other to billions of computational devices and billions of cell phones over the time. With the IoT, we are moving towards a phase where all items in our environment will be connected to the Internet and will have the ability to communicate with each other with minimum human efforts [1]. The IoT is considered as a universal presence in the environment that contains variety of things that can be connected whether using wireless and wired connections. These objects have a unique addressing scheme that allow things to interact and cooperate with other to create new IoT applications and services such as smart homes, smart cities, smart energy and the smart grids, smart transportation and traffic management

and control and others [2]. The IoT attracts the attention of both academic and commercial organizations. The main reasons behind this massive interest are unlimited capabilities that the IoT can provide [3]. For instance, it has the ability to provide a real-world intelligent platform for the collaboration of distributed smart objects through wireless or wired networks [4]. The main objective of this paper is to provide a review of IoT system with highlighting its applications, challenges, and open issues. This paper starts with providing an overview of the IoT system and its layered architecture. This is followed by discussing different characteristics of the IoT with presenting a comparison between common IoT communication technologies. Different IoT applications, challenges, and open research directions are also discussed. The rest of this paper is organized as follows: Section II presents the state-of-the-art of the IoT; Section III discusses IoT layered architecture; Section IV introduces the essential characteristics of the IoT; Section V discusses common IoT communication technologies; Section VI presents applications of the IoT; Section VII discusses challenges standing in the way of IoT deployments; Section VIII discusses future research directions of the IoT, and Section IX is the conclusion.

2. State of The Art IoT

The IoT can be considered both a dynamic and global networked infrastructure that manages self-configuring objects in a highly intelligent way. This, in turn, allows the interconnection of IoT devices that share their information to create new applications and services which can improve human lives [1]. Originally, the concept of the IoT was first introduced by Kevin Ashton, who is the founder of MIT autoidentification centre in 1999 [5], [6]. Ashton has said, "The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so" [5]. Later, the IoT was officially presented by the International Telecommunication Union (ITU) in 2005 [7]. The IoT has many definitions suggested by many organizations and researchers. However, the definition provided by ITU in 2012 is the most

common. It stated: “a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies” [8]. In addition, Guillemin and Friess in [9] have suggested one of the simplest definitions that describe the IoT in a smooth manner. It stated: “The Internet of Things allows people and things to be connected Anytime, Anyplace, with anything and anyone, ideally using any path/network and any service”. Several definitions were suggested by many researchers describing the IoT system from different perspectives but the important thing that majority or researchers have agreed on is the IoT is created for a better world for all the human beings.



Figure 1. The IoT can connect anything in anywhere using any path

The IoT is a promising technology that starts to grow significantly [10]. There were already more objects/things connected to the Internet than people from 2008, as shown in Figure 2. Predictions are made that by 2020; the number of Internet-connected devices will reach or even exceed 50 billion [11]. In addition, the IoT becomes the most massive device market that enables companies to save billions of dollars. It will add \$1.7 trillion in value to the global economy in 2019. This involves hardware, software, management services, installation costs, and economic value from realized IoT efficiencies [12].

Nowadays, the IoT notion has evolved to include the perception of realizing a global infrastructure of interconnected networks of physical and virtual objects. The huge technological development has expanded the idea of the IoT to involve other technologies such as Cloud computing and Wireless Sensor Networks (WSNs). The IoT has become able

to connect both humans and things anywhere, and anytime, ideally using any path/network [9].

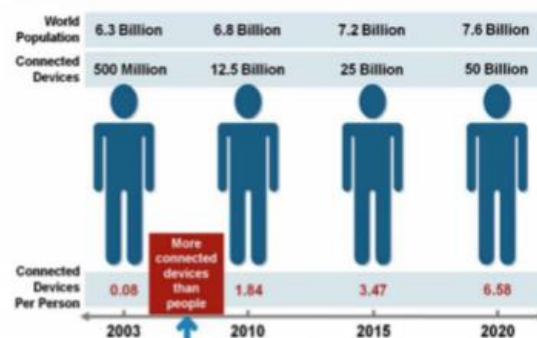


Figure 2. Growing number of things connected to the internet [13]

The IoT has become one of the interesting topics to many researchers. According to Google, the number of IoT journal and conference papers has almost doubled from 2004 to 2010. From 2010, the IoT articles are dramatically increased to reach about 985 article in 2015. Till the first of November of this year, there is about 845 article. Figure 3 shows the number of IoT journal and conference papers per year from 2004 till now.

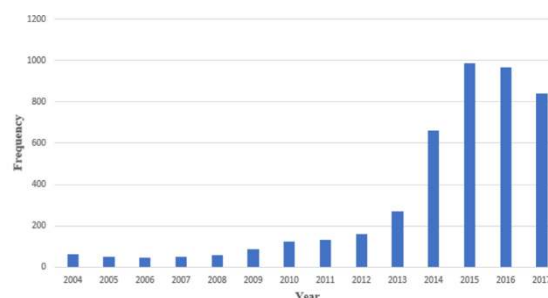


Figure 3. Number of IoT journal papers per year from 2004 to present

3. IoT Architecture

IoT World Forum (IWF) architecture committee released an IoT reference model in October 2014 [14]. This model works as a common framework to help the industry to accelerate IoT deployments. This reference model is intended to consolidate and encourage the collaboration and development of IoT deployment models. Figure 4 shows the seven-level architecture model of the IoT. This reference model is designed as seven-layers so that each layer provides additional information for establishing a common terminology. It also identifies where specific types of processing are optimized across different levels of the system and provides the first step to enable vendors to create IoT products that are compatible and can work

with each other. In addition, this model made the IoT as a real and approachable system, instead of simply conceptual [13].

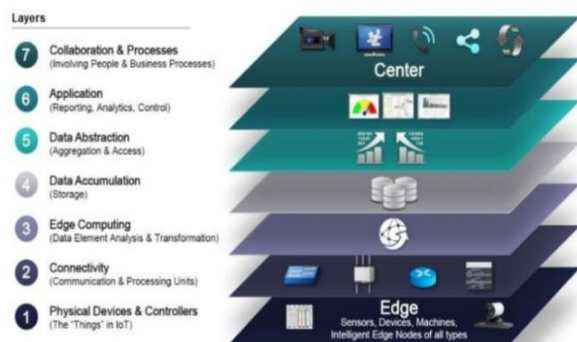


Figure 4. The IoT World Forum Reference Model [14]

Layer 1 is similar to the physical layer of the Open System Interconnection (OSI) model of the network architecture. It is composed of physical devices and controllers that control objects. These objects represent things in the IoT that include a wide range of devices that send and receive information. For instance, sensors that collect a variety of information about the surrounding environment [13].

Communications and connectivity are in layer 2. This layer includes devices such as routers, switches, gateways, and firewalls that are used to construct local and wide-area networks to enable Internet connectivity. In addition, this layer enables devices to communicate with one another and to communicate with application platforms such as computers, remote-control devices, and smartphones [14].

The purpose of the edge computing layer is to convert network data flows into information suitable for storage and higher-level processing. Processing elements at this layer might deal with high volumes of data and perform data transformation operations, resulting in storage of much lower volumes of data [15].

Layer 4 is the data accumulation. This layer is concerned with storing data coming from different IoT devices. This data is filtered and processed by the edge computing layer that absorbs large quantities of data and placed them in storage so as to be accessible by higher levels [14], [16]. Different types of data in different formats and from heterogeneous processors may be coming up from the edge computing layer for storage. While the data abstraction layer aggregates and formats stored data in ways that make it accessible by applications in more manageable and efficient way.

Layer 6 is the application layer where information interpretation occurs. This layer encompasses a variety of applications that use IoT input data or control IoT devices [13], [14]. The collaboration and processes layer identify individuals who can

communicate and collaborate to make the IoT system more useful. This layer involves different applications to exchange data and control information across the Internet [16], [17]. Table 1 provides a summary of IoT architecture layers and the function of each layer.

Table 1. A summary of IoT architecture layers with its functions

IoT Layer	Function
Collaboration and processes layer	This layer allows different IoT applications to communicate and collaborate with each other to make the IoT data more useful
Application layer	This layer includes different IoT applications such healthcare, smart home, and others
Data abstraction layer	This layer aggregates and formats the IoT stored data to make it accessible to different IoT applications
Data accumulation layer	This layer is used to store data coming from different IoT devices
Edge computing layer	This layer converts network data into information suitable for storage and higher-level processing
Connectivity layer	This layer allows different IoT devices to communicate with one another using different internetworking devices
Physical layer	This layer consists of physical devices and controllers that control IoT objects/devices

4. Characteristics of The IoT

The IoT represents a promising future technology that shows some common features as follows:

- Large scale: IoT devices are increased in billions. These devices need to be managed to be able to communicate with each other. The management of data generated from these devices and their interpretation for application purposes becomes critical [18].
- Intelligence: With the integration of software algorithms and hardware, IoT devices become smart. These intelligence capabilities make IoT devices interact in an intelligent way in certain situations. Although the popularity of smart technologies, intelligence in the IoT is only means of interaction between devices, while user and device interactions are achieved by usual input methods and graphical user interfaces [19].
- Sensing: IoT could not be realized without sensors. Sensors are used to perceive any changes in the environment

to generate data that reflect their status or even interact with the environment. Sensing technologies provide capabilities that reflect the awareness of humans and physical world. Although the sensing information is simply the analogue input from the physical world, it can provide a good understanding of our complex environment [8].

- **Complex system:** IoT has billions of devices. Performing operations with this large scale of objects/things make the coordination process very complex due to constraints associated with memory, energy and time [3].
- **Dynamic environment:** IoT is a dynamic network in nature where objects are continually deployed; some new items joining the network while others leaving without determining network boundaries [20]. The IoT devices can dynamically adapt to changing situations based on their operating conditions. For example, surveillance cameras can adapt their modes based on whether it is day or night. Cameras could switch from lower resolution to higher resolution modes when any motion is detected and alert nearby cameras to do the same [21].
- **Massive amount of data:** As IoT devices are in billions. These devices create a large amount of data which raises many issues including those related to security and privacy [19].
- **Heterogeneity:** The IoT system involves different devices, platforms, operating systems, and services which are connected with each other using different protocols [8].
- **Limited energy:** Most IoT devices are small and lightweight with limited resources, so they are designed to work with minimal energy consumption [20].
- **Connectivity:** Connectivity enables network accessibility and compatibility. It empowers the IoT by bringing together everyday objects. It also provides new market opportunities for IoT that can be created by the networking of smart things and applications [22].
- **Self-configuring:** IoT devices have the capability of self-configuring that enable many IoT devices to work together to provide certain functionality. These devices could configure themselves, setup the networking, and fetch latest software upgrades in association with the device manufacturer with minimal

manual or user intervention [21], [23].

- **Unique identity:** Each IoT device has a unique identity and unique identifier (such as IP address). These identities are provided by IoT manufactures to use it to upgrade devices to the appropriate platforms. In addition, these devices have interfaces that allow users to query devices, monitor their status, and control them remotely [21], [24].
- **Context-awareness:** There are many sensors that collect information about the physical and environmental features, therefore, sensor nodes get knowledge about the surrounding context, so it considered as context-aware [25].

5. IoT Communication Technologies

The IoT is a heterogeneous network that involves different devices such as electronic devices, mobile devices, and industrial equipment and others. Different devices may have different communication platforms, networking, data processing, data storage capacities, and transmission power. All these devices have to be connected by networking and communication protocols that enable them to communicate and cooperate together to share their data [24].

Communication protocols play a vital role in the IoT system. They represent the backbone of the IoT system by allowing IoT devices to exchange their data over the network. These protocols specify the format of data exchange, data encoding, addressing schemes for devices and routing of packets from source to destination. Furthermore, they provide other functions such as sequence control, flow control, and retransmission of lost packets [23], [24].

The IoT system uses various types of communication protocols and standards. The most common IoT communication protocols are ZigBee, Bluetooth, ZWave, 6LOWPAN, and NFC. The next section provides an overview of each protocol.

5.1. ZigBee

ZigBee protocol was invented by ZigBee Alliance that is based on low-power wireless IEEE802.15.4 networks standard [26]. The purpose of this protocol is to establish a standard that provides low-cost communication protocol to create personal area networks (PANs).

ZigBee is the suitable communication protocol for applications that need a low data rate, longer battery life, and secure networking devices. Furthermore, ZigBee can work with different network topologies such as mesh, star and tree [26].

5.2. Bluetooth

Bluetooth is a short-range communication protocol that is considered as the key element for wearable products. The new version of Bluetooth which is called Bluetooth Smart or Bluetooth Low-Energy (BLE) is a significant protocol for different IoT applications as it supports reduced power consumption and can be integrated with smartphones and other mobile devices [27].

5.3. Z-Wave

Z-Wave is a low-power radio frequency communication protocol that mainly built for home automation. It provides reliable and low-latency communication of small data packets with data rates up to 100kbit/s. in addition, it is a scalable protocol and supports full mesh network topology. Z-Wave is a simpler protocol which enables faster and simpler development [27], [28].

5.4. NFC

Near Field Communication (NFC) is a very short range wireless communication protocol that provides a simple and safe two-way communication protocol between electronic devices especially for smartphones. It also allows users to perform contactless payment transactions, access digital content and connect electronic devices. Basically, NFC makes it easier to connect and control IoT

devices to share information at a distance that is less than 4cm [29].

5.5. 6LoWPAN

IPv6 over Low Power Wireless Personal Area Network (6LoWPAN) is the first and most common communication protocol for the IoT. It efficiently encapsulates IPv6 long headers in IEEE802.15.4 small packets, which cannot exceed 128 bytes. It also supports different length addresses, low bandwidth, different topologies including star or mesh, power consumption, low cost, scalable networks, mobility, unreliability and long sleep time. Since it is an IP-based standard, it can be connected directly to another IP network without intermediate entities such as translation gateways or proxies [27], [28].

Table 2 provides a comparison between common IoT communication protocols in terms of protocol standard, network type, frequency band, supported range, data rate, power, topology supported by each protocol, security standard, and common applications that use the protocol. It is obvious that all communication protocols support Advanced Encryption Standard (AES) platform and belong to Wireless Personal Area Network (WPAN) except NFC which is a Peer-to-Peer (P2P) network. We can conclude that 6LoWPAN will be the future protocol as it allows an enormous number of IoT devices to be deployed over the internet easily by using the huge address space of IPv6.

Table 2. Comparison between common IoT communication protocols

Characteristics	ZigBee	Bluetooth	Z-Wave	NFC	6LoWPAN
Standard	IEEE 802.15.4	IEEE 802.15.1	Z-Wave	ISO/IEC 18000-3	IEEE 802.15.4
Network type	WPAN	WPAN	WPAN	P2P Network	WPAN
Frequency Band	2.4 GHz	2.4 GHz	900 MHz	13.56MHz	2.4 GHz
Range	Short Range 10-100 m	Short Range 15-30 m	Short Range 30 - 100 m	Short Range Up to 200 m	Short Range 10-100 m
Data Rate	250 kbps	1Mbps	100kbps	100 – 420kbps	250 kbps
Power	30 mA Low power	30 mA Low Power	2.5 mA Low power	50 mA low power	Very low power consumption
Supported Topology	Star, Mesh	Star and Bus	Mesh	P2P Network	Star Mesh
Security	AES	AES	AES	RSA and AES	AES
Common applications	Home control and monitoring	Wireless headsets and audio applications	Home control and monitoring	Payment and access	Monitor and control via internet

6. IoT Applications

The IoT has the capability to connect everyday objects. It has introduced several applications and smart services, which have affected users' daily lives. This section presents a brief discussion of some of IoT applications, as shown in Figure 5.

6.1. Healthcare

The IoT has brought many benefits and opportunities to the field of healthcare. It helps to develop and improve healthcare services and keep the field innovative. For instance, intelligent drug/medicine control and hospital management. In addition, the IoT add more benefits by monitoring the individual health in real-time. Also, ambulances can

be immediately dispatched to accident scenes and patients can be monitored at their homes just as effectively as in hospitals. For example, a doctor can immediately be informed if the patient suffers a heart attack [30].



Figure 5. Some of IoT applications

6.2. Smart City

The concept of the smart city is used to describe the better use of public resources, increasing the quality of service presented to the citizens, and at the same time reducing operational costs of public administrations [30]. The IoT provides several benefits in the management and optimization of public services, such as transport and parking, lighting, surveillance and maintenance of public areas, preservation of cultural heritage, and garbage collection. Furthermore, the availability of different types of data collected by IoT devices can be used to enhance the awareness of people about the status of their city and stimulate the active participation of the citizens in the management of public administration [31].

6.3. Smart Home

People always try to find new approaches to increase their luxury. Currently, people can install smart appliances inside their homes to control many of the house tasks. These intelligent devices have the option of remote control, which eliminates the need of being near the device [32]. Therefore, these devices have enabled the automation of home activities by the adoption of various embedded devices [33].

6.4. Connected Industry

The connected industry is the vision of a manufacturing environment where every machine can communicate with all other machines across the plant. The connected industry with IoT will connect, monitor and control virtually anything, anywhere to provide operational productivity and profitability [24]. In addition, the integration of IoT with sensor networks, wireless connectivity, innovative hardware and machine-to-machine communication will completely transform the conventional automation process of industries [32].

6.5. Smart Retail

For retailers, the IoT offers unlimited opportunities to increase supply chain efficiencies, develop new services, and reshape the customer experiences. For instance, applications for tracking goods, real-time inventory, information exchange among suppliers and retailers, and automated delivery capabilities will improve the retail sector [34], [35].

6.6. Connected Car

Connected cars are equipped with Internet access and can share their access with others, just like connecting to a wireless network in a home or office. More vehicles are starting to come equipped with this functionality, so be prepared to see more apps included in future cars [36]. The connected car is considered as the best way to minimize accidents such that a pilot can operate the car remotely to minimize car accidents and reduce human errors. These driverless cars can provide functions more than just safety such as they can save valuable time, reduce the stress of driving etc. Some studies reveal that by 2040, driverless cars will account for up to 75 percent of cars on the road worldwide [24].

6.7. Smart Parking

In recent time, smart parking sensors are attached in parking space to detect the arrival and departure of vehicles. It provides an efficient management solution to help drivers to save time and fuel. It provides the drivers with the accurate information about parking spaces and keeps the traffic system smooth. It also enables the facility of deployment to book parking space directly from the vehicle [30].

6.8. Smart Energy and Smart Grid

The IoT provides more information about the behaviours of electricity suppliers and consumers in an automated way to improve the energy efficiency. It also provides consumers with smart management of

energy consumption such as smart meters, smart appliances, renewable energy resources [30].

6.9. Environmental Monitoring

The key element of the IoT system is sensors which collect information about the surrounding environment. Therefore, with the IoT, a high-speed information system can be provided. This allows the entity that monitors wide-area environments and sensors deployed in the area to convey a huge amount of data easily such as pollution source monitoring, water quality monitoring, air quality monitoring [2].

6.10. Smart Agriculture

With the presence of sensors in everywhere, farmers can use the huge collected information to yield a better return on investment. Sensing for soil moisture and nutrients, controlling water usage for plant growth and determining custom fertilizer are some simple uses of IoT in the agriculture. In addition, many wireless technologies were used in the agriculture such as remote sensing, global positioning system and geographical information system. This in turn will replace human labour with automatic machinery which will increase the productivity [37].

6.11. Wearables

Watches are no longer just for telling time. Smartwatches have turned our wrists into a smartphone by enabling text messaging, phone calls, and more. Many other devices are used to give us more information about our workouts such as Fitbit, Jawbone and others [38].

7. Challenges of the IoT

There are many challenges that stand in the way of the successful deployment of IoT applications. These challenges include:

7.1. Big data

As said earlier, the IoT system involves billions of devices which generate a huge amount of data. This data is variable in term of structure and often arrive in realtime. The volume, velocity and variety make the storing and analytics process, which is used to generate meaningful information, a very complex task [39]. It is obvious that the IoT is one of the main sources of big data. Using the Cloud computing can facilitate storing this data for a long period of time. However, handling this massive amount of data is a substantial issue, as the whole performance of different applications is heavily reliant on the properties of this data management service [40].

Moreover, one of the important factors that related to big data is the data integrity. This is because it affects the quality of service and its security and privacy aspects [41].

7.2. Networking

The IoT system has different devices which use different communication networking protocols. IoT networking protocols can be divided into smart device networks and traditional networks, which is used to increase data rates. Smart networking protocols are expected to adopt the protocols already established in WSNs and Machine-to-Machine (M2M) communications [42]. Building a networking protocol is not an easy task as it should satisfy the requirements of ease-of-use, cost and performance of the whole system. In addition, choosing the suitable network topology for the protocol is another issue. However, the mesh topology is the most suitable choice for wireless communication in smart environments [33]. Therefore, different communication protocols and different network topologies create a significant challenge that needs to be handled.

7.3. Heterogeneity

The IoT interconnects large numbers of devices/objects to provide new applications that improve our quality of life. However, one of the important challenges faced by the IoT system is the wide heterogeneity of devices, platforms, operating systems, and services that exist and might be used to create new applications [43]. As the IoT continues to grow, the need for services that work with multiple IoT application will continue to increase to realize the promised efficiency gain of the IoT. In addition, the IoT system uses a wide variety of devices with different features which make the connectivity and coordination process very difficult task [44].

7.4. Interoperability

The IoT provides a common network that connects almost every object in our environment. The interconnectivity between IoT devices increases system productivity by generating new applications and services. This interconnectivity comes at a price, as the popularity increases, and the number of devices and networks increase, the lack of interoperability between them becomes a critical issue [45]. Although there are many suggested solutions to solve the interoperability issue such as data-over-sound technology which encodes data into several tones to produce a sonic barcode, which can then be transmitted and decoded by IoT devices [46], the

interoperability is still a big issue for the IoT system.

7.5. Scalability

The number of IoT devices grows rapidly. Predictions are made that by 2020; the number of IoT devices will reach or even exceed 50 billion [11]. The IoT system should meet scalability issue to adapt to environment changing condition. Scalability means that the system is able to handle the specific needs as they arise. The main purpose of making the IoT system scalable is to meet the changing demands as the interest of people changes with time as well as the environmental conditions [47]. In addition, scalability helps the system to work efficiently without any performance issues that may arise due to system expansion.

7.6. Security and privacy

One of the most difficult issues that face most of the new technologies is the security and privacy. As the IoT system relies on sensors that installed in our surrounding environment. These sensors collect not only environment data but also our habits, financial records and other sensitive information. Therefore, providing a secure IoT system is a compulsory task to continue its successful deployments in our environment [48]. The IoT is intrinsically vulnerable to most of the wireless common attacks because of most IoT devices are connected through wireless networks that are hard to protect against different attacks such as man-in-the-middle attack and other attacks.

7.7. Maintenance

Maintenance is a serious challenge to recognize as billions of new devices flood the Internet. These devices may belong to different vendors who have already gone out of business, and their devices may be full of bugs that nobody will ever be able to fix. In addition, many vendors do not care about upgrading their devices to the latest platforms and fix security and other problems in their devices which create a big challenge not only in overall performance but also it is considered as a weak point that can be attacked easily and affect the whole IoT network.

8. Open Research Directions

This section provides future research directions that related to the IoT.

8.1. Standardization

Standardization plays a key role in the development of the IoT. The IoT standardization aims

to lower the entry barrier of new service providers and users. In addition, standardization can improve the interoperability and allow products or services to compete better at a higher level [49]. However, the rapid growth of IoT makes the standardization difficult. There many issues related to IoT standardization such as interoperability, radio access level, semantic interoperability, and security and privacy. The open standards of IoT such as security standards, communication standards and identification standards, might be several key enablers for the expansion of the IoT technologies [50]. Researchers should pay their attention to build industry-specific guidelines and specify required architectural standards for efficient implementation of IoT.

8.2. Security and privacy

The social acceptance of IoT applications and services will strongly rely on the trustworthiness of information and protection of private data. Although a number of projects have been developed for security and privacy protection, a reliable security protection mechanism for the IoT is still in demand to satisfy the requirements of data confidentiality, integrity, privacy, and trust [51].

The widespread applicability of the IoT and its associated technologies are largely depend on the information security and data privacy protection. Being highly complex and heterogeneous in nature, IoT always faces severe security and privacy issues. A reliable, effective and powerful security protection mechanism for IoT is on the topmost priority at the moment, therefore, more research is needed to improve the security and privacy of the IoT system [50], [58].

8.3. Heterogeneity

IoT is a very complex heterogeneous network, which includes different connections among various types of networks through various communication technologies. The devices and methodologies for addressing things management is still a challenge [52]. The management of IoT connected objects by facilitating collaborative work between different things such as hardware components or software services and administering them after providing addressing, identification, and optimization at the architectural and protocol levels is a serious research gap that needs to be addressed.

8.4. Fog Computing

The Fog computing is a paradigm which provides limited capabilities such as computing, storing and networking services in a distributed manner between different end devices and classical Cloud computing.

It provides a good solution for IoT applications that are latency-sensitive [53]. To increase IoT system efficiency, most of the data generated by IoT objects/devices must be processed and analysed in real-time. The Fog computing will bring Cloud networking, computing, and storage capabilities down to the edge of the network, which will address the real-time issue of IoT devices and provide secure and efficient IoT applications [54].

Although the Integration of Fog computing with IoT will bring many benefits to different IoT applications, it also brings many challenges that need to be addressed. How to integrate Fog computing with IoT is a hot topic that needs more research studies to get all fog benefits to the IoT system.

8.5. Blockchain

Current IoT systems are built on centralized server/client model, which requires all devices to be connected and authenticated through the server. This model would not be able to provide the needs to outspread the IoT system in the future [55]. Therefore, moving the IoT system into the decentralized path may be the right decision. One of the popular decentralization platforms is blockchain.

A blockchain is a distributed database of records that contains all transactions that have been executed and shared among participating parties in the network. This distributed database is called distributed ledger [56].

Integrating IoT with blockchain will have many benefits. The decentralization model of the blockchain will have the ability to handle processing of billions of transactions between IoT devices, which will significantly reduce the costs associated with installing and maintaining large centralized data centres and will distribute computation and storage needs across the billions of devices that form IoT networks. In addition, working with the blockchain technology will eliminate the single point of failure associated with the centralized IoT architecture [57]. Integration IoT with blockchain needs more research to get the benefits of decentralization to the IoT field.

9. Conclusion

The IoT is considered as the next stage toward the evolution of the Internet. It has the capability to connect and communicate almost all real-world objects over the Internet to increase information sharing. With the help of sensors, the IoT has the ability to collect, analyses, and deploy a huge amount of data which in turn will be converted into meaningful information and knowledge that can be used to create new application and services that can improve our quality of life. This paper has provided a review of the IoT system. The state-of-the-art and layered architecture of the IoT are discussed. In

addition, IoT essential features and different communication technologies are presented. A comparison between common IoT communication technologies and IoT applications are also discussed. Finally, IoT challenges and future research directions are discussed.

10. Acknowledgment

We acknowledge Egyptian cultural affairs and mission sector and Menoufia University for their scholarship to Hany Atlam that allows the research to be funded and undertaken

11. References

- [1] R. Shanbhag and R. Shankarmani, "Architecture for Internet of Things to minimize human intervention," 2015 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2015, pp. 2348–2353, 2015.
- [2] M. Ibrahim, A. Elgamri, S. Babiker, and A. Mohamed, "Internet of things based smart environmental monitoring using the Raspberry-Pi computer," 2015 Fifth Int. Conf. Digit. Inf. Process. Commun., pp. 159–164, 2015.
- [3] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the internet of things: A survey," IEEE Commun. Surv. Tutorials, vol. 16, no. 1, pp. 414–454, 2014.
- [4] M. Elkhodr, S. Shahrestani, and H. Cheung, "The Internet of Things: Vision & challenges," IEEE 2013 Tencon - Spring, TENCONSpring 2013 - Conf. Proc., pp. 218–222, 2013.
- [5] K. Ashton, "That 'Internet of Things' Thing," RFID J., p. 4986, 2009.
- [6] G. Joshi and S. Kim, "Survey, Nomenclature and Comparison of Reader Anti-Collision Protocols in RFID," IETE Tech. Rev., vol. 25, no. 5, p. 285, 2013.
- [7] ITU, "The Internet of Things," Itu Internet Rep. 2005, p. 212, 2005.
- [8] ITU, "Overview of the Internet of things," Ser. Y Glob. Inf. infrastructure, internet Protoc. Asp. nextgeneration networks - Fram. Funct. Archit. Model., p. 22, 2012.
- [9] P. Guillemin and P. Friess, "Internet of Things Strategic Research Roadmap," Eur. Comm. Inf. Soc. Media, Luxemb., 2009.
- [10] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," Inf. Syst. Front., vol. 17, no. 2, pp. 243–259, 2015.
- [11] D. Evans, "The Internet of Things - How the Next Evolution of the Internet is Changing Everything," Cisco white Pap., no. April, pp. 1–11, 2011.
- [12] H. Gusmeroli, S., Haller, S., Vision and challenges for realizing the internet of things, vol. 1, no. APRIL. 2009.

- [13] Cisco, "The Internet of Things Reference Model," White Pap., pp. 1–12, 2014.
- [14] W. Stallings, "The Internet of Things: Network and Security Architecture," *Internet Protoc. J.*, vol. 18, no. 4, pp. 2–24, 2015.
- [15] S. Kraijak and P. Tuwanut, "a survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends," *Commun. Technol. (ICCT)*, 2015 IEEE 16th Int. Conf., pp. 26–31, 2015.
- [16] R. Sutaria, "Making sense of interoperability: Protocols and Standardization initiatives in IoT," *Int. Conf. Recent Trends Commun. Comput. Networks*, pp. 2–5, 2013.
- [17] R. H. Weber, "Internet of Things – New security and privacy challenges," *Comput. Law Secur. Rev.*, vol. 26, no. 1, pp. 23–30, 2010.
- [18] M. S. A. Carlo, "An Overview of Privacy and Security Issues in the Internet of Things," *McKinsey Q.*, vol. 2, p. 6, 2013.
- [19] D. Chen, G. Chang, L. Jin, X. Ren, and F. Li, "A Novel Secure Architecture for the Internet of Things," 2011 Fifth Int. Conf. Genet. Evol. Comput., pp. 311–314, 2011.
- [20] M. Adda, J. Abdelaziz, H. Mcheick, and R. Saad, "Toward an Access Control Model for IOTCollab," 6th Int. Conf. Ambient Syst. Networks Technol., vol. 52, no. Ant, pp. 428–435, 2015.
- [21] P. P. Ray, "A survey on Internet of Things architectures," *J. King Saud Univ. - Comput. Inf. Sci.*, 2016.
- [22] K. K. S. M. P. Patel, "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges," *Int. J. Eng. Sci. Comput.*, vol. 6, no. 5, 2016.
- [23] H. F. Atlam, G. Attiya, and N. El-Fishawy, "Comparative Study on CBIR based on Color Feature," *Int. J. Comput. Appl.*, vol. 78, no. 16, pp. 975–8887, 2013.
- [24] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Trans. Ind. Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.
- [25] G. Yang et al., "A Health-IoT platform based on the integration of intelligent packaging, unobtrusive biosensor, and intelligent medicine box," *IEEE Trans. Ind. Informatics*, vol. 10, no. 4, pp. 2180–2191, 2014.
- [26] F. Samie, L. Bauer, and J. Henkel, "IoT technologies for embedded computing: A survey," in 2016 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS), 2016, pp. 1–10.
- [27] S. Kuzlu, M. Pipattanasomporn, M. Rahman, "Review of communication technologies for smart homes/building applications," in 2015 IEEE Innovative Smart Grid Technologies - Asia (ISGT ASIA), 2015, pp. 1–6.
- [28] S. Al-sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of Things (IoT) Communication Protocols: Review," in 2017 8th International Conference on Information Technology (ICIT) Internet, 2017, pp. 685–690.
- [29] G. Cerruela García, I. Luque Ruiz, and M. GómezNieto, "State of the Art, Trends and Future of Bluetooth Low Energy, Near Field Communication and Visible Light Communication in the Development of Smart Cities," *Sensors*, vol. 16, no. 11, p. 1968, 2016.
- [30] M. Chen, J. Wan, and F. Li, "Machine-to-machine communications: Architectures, standards and applications," *KSII Trans. Internet Inf. Syst.*, vol. 6, no. 2, pp. 480–497, 2012.
- [31] a Zanella, N. Bui, a Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, 2014.
- [32] I. I. Pătru, M. Carabaş, M. Bărbulescu, and L. Gheorghe, "Smart home IoT system," *Netw. Educ. Res. RoEduNet Int. Conf. 15th Ed. RoEduNet 2016 - Proc.*, pp. 365–370, 2016.
- [33] B. L. Risteska Stojkoska and K. V. Trivodaliev, "A review of Internet of Things for smart home: Challenges and solutions," *J. Clean. Prod.*, vol. 140, pp. 1454–1464, 2017.
- [34] VMware, "smart retail solution: convert customer insights into dollars," 2017.
- [35] Z. Guo, Z. Zhang, and W. Li, "Establishment of intelligent identification management platform in railway logistics system by means of the Internet of Things," *Procedia Eng.*, vol. 29, pp. 726–730, 2012.
- [36] M. Kalmeshwar and N. Prasad, "Internet Of Things: Architecture, Issues and Applications," *Int. J. Eng. Res. Appl.*, vol. 7, no. 6, pp. 85–88, 2017.
- [37] K. L. Krishna, O. Silver, W. F. Malende, and K. Anuradha, "Internet of Things application for implementation of smart agriculture system," 2017 Int. Conf. I-SMAC (IoT Soc. Mobile, Anal. Cloud), vol. 25, no. 15, pp. 54–59, 2017.
- [38] H. R. Inc, "Wearable Technology Market Analysis, Market Size, Application, Analysis, Regional Outlook, Competitive Strategies and Forecasts, 2014 To 202," 2017.
- [39] A. Zaslavsky, C. Perera, and D. Georgakopoulos, "Sensing as a Service and Big Data," *Proc. Int. Conf. Adv. Cloud Comput.*, pp. 21–29, 2012.
- [40] H. F. Atlam, A. Alenezi, A. Alharthi, R. Walters, and G. Wills, "Integration of cloud computing with internet of things: challenges and open issues," in 2017 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), 2017, no. June, pp. 670–675.
- [41] C. Liu, C. Yang, X. Zhang, and J. Chen, "External integrity verification for outsourced big data in cloud and IoT: A big picture," *Futur. Gener. Comput. Syst.*, vol. 49, pp. 58–67, 2015.

- [42] M. Chen, J. Wan, and F. Li, "Machine-to-Machine Communications: Architectures, Standards and Applications.," KSII Trans. Internet Inf. Syst., pp. 480–497, 2012.
- [43] K. Xu, Y. Qu, and K. Yang, "A tutorial on the internet of things: From a heterogeneous network integration perspective," IEEE Netw., vol. 30, no. 2, pp. 102–108, 2016.
- [44] H. F. Atlam, G. Attiya, and N. El-Fishawy, "Integration of Color and Texture Features in CBIR System," Int. J. Comput. Appl., vol. 164, no. April, pp. 23–28, 2017.
- [45] H. F. Atlam, A. Alenezi, R. K. Hussein, and G. B. Wills, "Validation of an Adaptive Risk-based Access Control Model for the Internet of Things," I.J. Comput. Netw. Inf. Secur., 2017.
- [46] D. Bubley, "Data over Sound Technology : Device-to-device communications & pairing without wireless radio networks," 2017.
- [47] A. Gupta, R. Christie, and P. R. Manjula, "Scalability in Internet of Things : Features , Techniques and Research Challenges," Int. J. Comput. Intell. Res., vol. 13, no. 7, pp. 1617–1627, 2017.
- [48] H. F. Atlam, A. Alenezi, R. J. Walters, and G. B. Wills, "An Overview of Risk Estimation Techniques in Riskbased Access Control for the Internet of Things," in Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDs 2017), 2017, pp. 254–260.
- [49] H. Jiang, S. Zhao, Y. Zhang, and Y. Chen, "The cooperative effect between technology standardization and industrial technology innovation based on Newtonian mechanics," Inf. Technol. Manag., vol. 13, no. 4, pp. 251–262, 2012.
- [50] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," Inf. Syst. Front., vol. 17, no. 2, pp. 243–259, 2015.
- [51] P. Martin and K. Brohman, "CLOUDQUAL: A Quality Model for Cloud Services," IEEE Trans. Ind. Informatics, vol. 10, no. 2, pp. 1527–1536, 2014.
- [52] H. F. Atlam, A. Alenezi, R. J. Walters, G. B. Wills, and J. Daniel, "Developing an adaptive Risk-based access control model for the Internet of Things," in 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017, no. June, pp. 655–661.
- [53] M. Aazam and E. N. Huh, "Fog computing and smart gateway based communication for cloud of things," Proc. - 2014 Int. Conf. Futur. Internet Things Cloud, FiCloud 2014, pp. 464–470, 2014.
- [54] M. Ketel, "Fog-Cloud Services for IoT," Proc. SouthEast Conf. - ACM SE '17, pp. 262–264, 2017.
- [55] E. Karafiloski, "Blockchain Solutions for Big Data Challenges A Literature Review," in IEEE EUROCON 2017 -17th International Conference on Smart Technologies, 2017, no. July, pp. 6–8.
- [56] Nir Kshetri, "Can blockchain Strengthen the Internet of Things?," IEEE Computer Society, no. August, pp. 68–72, 2017.
- [57] A. Banafa, "IoT and Blockchain Convergence: Benefits and Challenges," IEEE IoT Newsletter, 2017.
- [58] Jaideep Kaur, Kamaljit Kaur, "Internet of Things: A Review on Technologies, Architecture, Challenges, Applications, Future Trends", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.4, pp. 57-70, 2017.