Chapter 6

Benefits and Challenges of Internet of Things for Telecommunication Networks

Asaad Ahmed Gad-Elrab Ahmed

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.81891

Abstract

Recently, Internet of things (IoTs) has become the main issue in designing monitoring systems such as smart environments, smart cars, and smart wearable devices. IoTs has transformed the life of people to be more adaptable and intelligent. For example, in a healthcare monitoring system, using smart devices will improve the performance of doctors, nurses, patients, and the healthcare industry. The IoTs revolution is known as the fourth industrial revolution and would change the way humans interact with machines and lead the way to a high-technology machine-to-machine interaction. In fact, almost every device around us would be connected to Internet, collecting and exchanging data with other devices on the cloud. In this chapter, we will introduce the benefits of IoTs on telecommunication networks and its challenges to give a complete overview for researchers to know how to improve our life and society by building smart IoTs systems.

Keywords: IoTs, smart things, smart environments, green IoT, Security and privacy, big IoT data

1. Overview of IoT

In recent decades, due to the developments in wireless and computer technologies, processors and sensors have been embedded into a lot of objects, which are used in our life. To build and design a real smart environment, these advancements are supported by huge developments in many research and industrial areas such as ubiquitous computing, wireless mobile communications, portable appliances and devices, wireless sensor networking, machine learning-based decision-making, agent technologies, IPv6 support, and human computer interfaces. A smart environment has sensor-enabled devices working collaboratively to build a small connected world for making the lives of people more comfortable and adaptable. The term smart refers to

the ability to autonomously obtain and apply knowledge, and the term environment refers to the surroundings. Therefore, a smart environment can be adapted by obtaining knowledge and applying it according to its users' requirements to improve their experience of that environment. In addition, the interconnection among different smart objects can enhance their functional capabilities [1]. In this context, IPv6 plays a vital role because of several features, including scalability in the case of billions of connected devices, better security mechanisms, and the elimination of network address translation (NAT) barriers. The "Internet of Things" (IoT) concept was first coined by Kevin Ashton, where smart objects are connected with the Internet.

Nowadays, IoT is receiving attention in many fields such as transport, agriculture, industry, and healthcare [2, 3]. Cisco reports that 50 billion devices and objects will be connected to the Internet by 2020. Also, the Internet of Things (IoT) will contribute $117 billion to the IoT-based healthcare industry and $1.9 trillion to the global economy according to Gartner and Forbes. In addition, according to Automotive News, the number of cars connected to the Internet worldwide will increase from 23 million in 2013 to 152 million in 2020. According to another report from Navigant Research, the number of installed smart meters around the world will grow to 1.1 billion by 2022. The prediction of such significant growth shows that IoT will become the umbrella of modern societies to realize the vision of smart environments. A lot of research efforts have been developed to integrate IoT with smart environments. To enable the user for monitoring the environment remotely or from remote sites, the integration of IoT with a smart environment is needed to extend the capabilities of smart objects. Based on the application requirements, IoT can be integrated with different smart environments. So, IoT-based smart environments can generally be classified into the following areas: (a) smart homes, (b) smart buildings, (c) smart cities, (d) smart grid, (e) smart health, (f) smart transportation, (g) smart industry, and (h) smart agriculture. **Figure 1** illustrates the IoT-based smart environments.

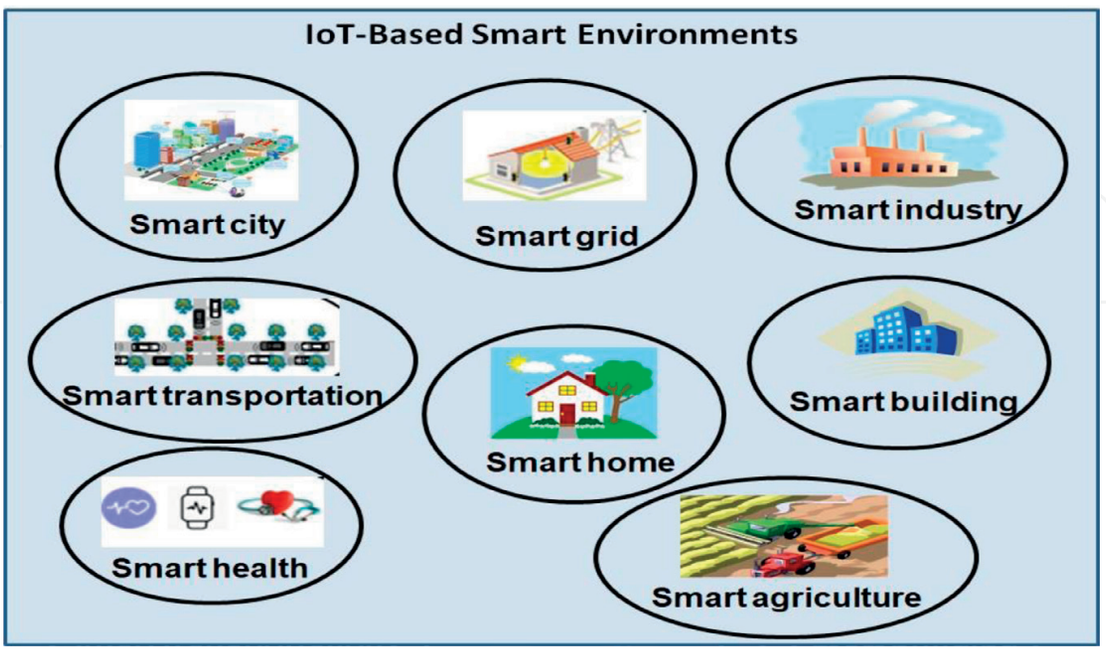

Figure 1. IoT-based smart environments.

2. Challenges of IoT

There are many open challenges that have been described by various researchers including those related to power supply, enabling a complex sensing environment, evolving architecture, multiple connectivity options, complexity of IoT, security of information exchange within IoT, and privacy [4–6]. Due to the lack of a clear and widely accepted business model that can engage investments to encourage the deployment of these technologies, there is difficulty in the adoption of the IoT paradigm [3].

To a certain extent, the above-mentioned challenges can be met, with the aid of a variety of wireless and wired connectivity options, such as radio frequency identification (RFID), near-field communication (NFC), Bluetooth, and Wi-Fi. These connectivity options are categorized into three broad types considering their geographical area coverage, that is, personal area network (PAN), local area network (LAN), and wide area network (WAN) [7]. **Figure 2** shows this categorization. The existing Wi-Fi networks should be modified to attain a wider coverage and to support mesh networks [8]. In addition, the confirmation on communication pathway of IoT is very important to understand the information exchange within IoT. It uses various standards, techniques, and protocols to disseminate information.

It is essential to support device-to-device (D2D), device-to-server (D2S), and server-to-server communications (S2S) to facilitate information sharing within the IoT [7, 9]. There are multiple standards and protocols involved with IoT communication. Some of these standards and

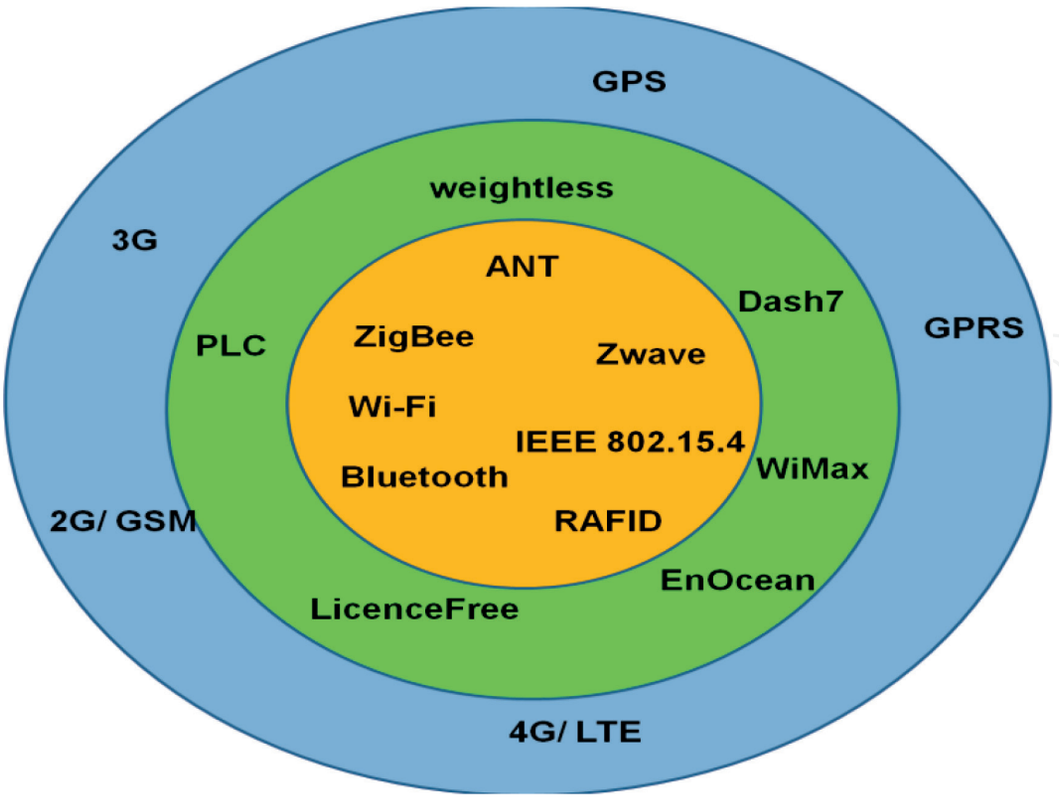

Figure 2. IoT communication technologies [7].

protocols take a higher priority, such as Internet Protocol version 4 (IPv4), Internet Protocol version 6 (IPv6), IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN), User Datagram Protocol (UDP) Constrained Application Protocol (CoAP), and Transmission Control Protocol (TCP). However, UDP is advantageous and cost-effective, due to its smaller size and performance according to constrained device developers [10]. To find a model for arranging these protocols into constrained and unconstrained stacks according to the TCP/IP network layer architecture, some efforts were made. The unconstrained stack contains Hypertext Transfer Protocol (HTTP), common standards Extensible Markup Language (XML), and IPv4, whereas the constrained stack contains Efficient XML Interchange (EXI), CoAP, and 6LoWPAN which are protocols with similar functionality but the complexity is reduced significantly [3]. In real life, the IoT has been rapidly developed and deployed with the enormous contribution from companies and research centers [11]. However, IEEE 802.11, IEEE 802.3, and IEEE 802.15.4 are the most common standards related to IoT [10], and the Internet Engineering Task Force (IETF) protocol suite has a vital contribution toward IoT for determining the challenges for IoT [12]. So, recently IoTs are widely accepted for using in practical application scenarios. Matrices are available to measure the cost, processing speed, and communication speed. However, there are few studies on application layer protocols and performance of 6LoWPAN [13, 14], IPv6 routing protocol for low power and lossy networks (RPL) [15–17], and IEEE 802.15.4 [18]; a complete evaluation of IoT has not taken place until now. Hence, this gap needs to be filled up in near future, considering a holistic view of IoT.

In this section, common major challenges of IoT and its future directions will be introduced. These challenges are *performance, availability*, *reliability, security and privacy*, *scalability*, *precision, interoperability*, *compatibility, Big IoT Data*, *mobility,* and *investment*. IoT is used to facilitate information and data anywhere, at any time for any person based on his request [19]. So, to realize IoT, availability is a highly critical issue. The IoT network requires the high availability guarantee of physical devices as well as IoT applications for achieving high availability. The feasible solution to this issue is using redundant maintenance of programs and hardware devices, so that the program or redundant device can be used to perform load balancing when the failure exists [20]. There are situations where simplicity is disclosed to achieve availability, even though redundancy increases complexity. Thus, to achieve availability, the feasible solution is redundant hardware components. In [20], two redundancy models are proposed: passive and active redundancy models. The active redundancy model performed bad compared to the passive redundancy model. Also, in the passive model, spare components are activated only when the primary component fails and these components will be at sleep mode or partially loaded during the other times. The reference provided claims a mathematical model based on Markov chain, which estimates availability and reliability. Since IoT depends on components and performance of involving technologies, its performance cannot be evaluated using a simple mechanism. Moreover, the other factors that influence the performance of IoT are network traffic, huge amounts of data, and heavy reliance on the cloud [21]. Cloud facilitates resource sharing, which is a vital requirement of IoT environments. In addition, users are enabled access to the services irrespective of the location via an Internet connection with the convergence of cloud and IoT. The convergence of cloud and IoT follows IoT-centric cloud approach or cloud-based IoT approach. In either way,

orchestration techniques, dynamic resource management, and dynamically offloading from clients/hosts to cloud are new challenges while overcoming existing individual challenges of IoT and cloud [22].

In critical applications, reliability is very important [23]. Reliability is not just sending reliable information, but being able to adapt to changing environmental conditions, be resistant to long-term usability and security problems [24]. In all aspects of software and hardware of IoT, reliability requires to be guaranteed. Attempts were made to explain clearly with the architecture considerations, the reliability consideration for transport, link, and application layers together [24]. Moreover, to describe and analyze reliability and cost-related properties of the service composition in IoT, a probabilistic approach was proposed [25].

Security and privacy are an essential requirement of most of the applications. In IoT, memory cards of a device have a limited storage capacity. So, only small amounts of data can be stored in them, and some of the data will be stored in other sites remotely. For these remote data, users do not want to disclose their information to others, so these data need high security and privacy. In terms of security, privacy, and governance rules, new technology is required to give users the ability to verify whether the company satisfies their service level agreement or not, dynamically. Therefore, they should adapt pertinent mechanisms for IoT, to meet the expected security level of a user. Privacy, communication, trusted sensing, computation, and digital forging are rarely addressed tasks in terms of security scope [26]. IoT does not adhere to common security standards and architecture; however, security has become a very important issue [27]. Traditional security architectures cannot fully satisfy the security requests of IoT, because of the existence of a huge number of heterogeneous devices that are connected together. As result, there is a large number of malware entry points, which increases vulnerability. By applying a biological immunology approach, a scheme has been proposed based on a dynamic defense security mechanism to alleviate these security issues in an IoT architecture [28]. In [26], attempts were done to secure IoT communications by ensuring the security of IoT devices. As the first step, computer-aided design (CAD) techniques have been proposed to design IoT devices, which are highly optimized in both energy and security. Importantly, compared to the expensive hardware-securing concepts proposed, CAD techniques can be used to implement strong and ample security with low cost. However, it is practically not in use until date.

In literature, there are several approaches for tackling the security issues in the current IoT paradigm. However, the authentication of devices and securing links in a dynamic mobility environment are still unresolved challenges. Thus, the authentication of IoT devices in real-world scenario still has unresolved issues. Researchers have warned of a realistic threat to the IoT community in the future in industries called "smart home hacking" to meet these challenges.

The increase in the number of smart devices and the advances of embedded technologies have increased the devices-to-person ratio up to 1.84 in 2010 [29]. In addition, the requirements from applications by a client increase over the time. So, the scalability of IoT, which is the ability to add more devices and services to IoT without degrading the Quality of service (QoS), must be considered. Due to the heterogeneity of devices and underlying technologies, scalability becomes a critical issue in IoT. To enable unified addition of new devices via a layered

architecture, a distributed, interoperable architecture was proposed for IoT to address the scalability issues without degrading the QoS for the realization of IoT notion [30]. In [30], the authors propose three layers of IoT infrastructure: (1) virtual object layer (VOL), (2) composite virtual object layer (CVOL), and (3) service layer (SL). The base structure "IoT daemon" of the distributed architecture consists of the functionalities of the three layers which are object virtualization, service composition and execution, and service creation and management. Based on the processing power and memory, every object hosts its own IoT daemon. Various applications are unified by using the three layers of IoT daemon. VOL digitally represents the properties and functionalities of each object. However, to perform a task, multiple objects work in collaboration. Thus, during runtime, composite virtual object (CVO) is created as a mash-up of VOs corresponding to the task. To create a mash-up, potential VOs should be identified, which is done at the CVOL. With the aid of uniform representation of objects (virtual object (VO)), addition of new objects to the IoT network does not degrade QoS because all the devices are connected with distributed architecture. Also, there are scalability issues due to the increase of network elements (NEs) in the Internet. Compensating the scalability issues with a service-oriented path computation element (S-PCE) instead of conventional host-oriented PCE was proposed by Barbosa C. Souza et al. in [31]. The performance evaluation confirmed that the proposed model supports more network elements than host-oriented PCE by comparing results obtained and the logs of DNS servers [31].

Interoperability is another major concern with regard to IoT, since various types of devices are connected to each other via IoT. Hence, IoT should facilitate services to all these devices regardless of the type, as interoperability is a necessity. By adhering to standardized protocols, this can be achieved to a certain level at the network and application levels. Due to ambiguous interpretations of the same protocol, achieving interoperability is challenging. So, by avoiding such ambiguities, interoperability of IoT would become more realistic. In [32], a solution to address IoT resources using Web protocols via IoT hubs has been proposed. Thus, the interoperability challenges are reduced to data formats and presenting hub catalogues.

In IoT, most of the devices are mobile devices, which make the IoT scenario more complex. So, IoT applications need to deliver services by considering the mobility factor as well. There are available standard management protocols, that is Mobile IPv6 (network layer) and TCP migrate (transport layer), to facilitate mobility issues in IoT. However, these standards are too complex to be used in IoT nodes. For constrained devices in IoT, a CoAP-based mobility protocol (CoMP) was proposed [33]. Moreover, to ensure mobility, a group mobility management (GMM) mechanism is shown to be promising [34]. In this context, the leader machine does mobility management for the group of machines that are grouped according to mobility patterns.

Precision is another one of the most important challenges that need to be addressed in many smart IoT environments such as transportation, healthcare, and unmanned aerial vehicular networks, where devices and systems are connected globally. Compliance with stringent requirements becomes central to the health and safety of the machine operators, machines, and related businesses when dealing with precision machines that can fail if the timing is 1 ms. Available bandwidth and network latency are the key factors that can affect the precision of distributed IoT delay-sensitive mission-critical environments. Therefore,

when deploying IoT in a smart environment, these parameters need to be considered. For example, longer network latencies can cause delays in applying car brakes and be very dangerous in the case of vehicle-to-vehicle communication in smart transportation environments. Successful IoT deployment in smart environments can be achieved by designing and developing high-precision systems.

Big data are another challenge in IoT because IoT is one of the largest sources of collecting large amounts of data. As mentioned earlier, by 2020 more than 50 billion devices will be connected with each other, which can lead to big data production. The performance of most IoT applications is based on the data management services. Therefore, due to big data generated by devices forming a smart IoT environment, managing the big IoT data in terms of processing, access, and storage requires highly scalable computing platforms that do not affect the performance of the application.

Compatibility is another challenge in an IoT-based smart environment, where various products are connected with each other. Due to the unavailability of a universal language, most of the products are unable to connect with each other and lead to compatibility issues. To connect devices with each other, collaboration among enterprises, such as LG, Philips, and Samsung, is required. People will be frustrated if these companies are not collaborated and they are only capable of using one brand, in this case. Therefore, the collaboration among these companies is demanded to obtain the infrastructure information of each product and design a universal coding language accordingly by developers. To ensure the success of IoT, a solution to compatibility issues is demanded.

Massive investment in IoT scenario is required for the investment decision to deploy an industrial IoT environment. In IoT, there is a difficulty for industries to adopt this technology where things are not open and interoperable in terms of hardware and software. Therefore, open and integrated hardware and software-based IoT solutions should be built for deployment in industries. In addition, instead of replacing these deployments with new systems, the solutions should be flexible enough for enabling industries to evolve and adapt to their changes. Expertise and investment are required for generating innovation within existing hardware and software architectures.

3. IoT-based smart environments

In this section, the state-of-the-art IoT-based smart systems are presented and categorized and classified according to application domain. The main categories are as follows: (a) smart homes, (b) smart building, (c) smart cities, (d) smart grid, (e) smart health, (f) smart transport, (g) smart industry, and (h) smart agriculture.

3.1. Smart homes

In [35], for detecting a fault in the software defined network (SDN)-based smart home environment, a cloud-based home solution was proposed. To find the faulty location in an

IoT-based smart home environment, four social relationships are defined, namely, IoTService, IoTphysical space, IoTNetwork, and IoTIoT. An SDN controller makes a status graph that contains information on each home IoT to resolve the dependencies by collecting information from the packets passing through SDN switches, and the stateless protocol is used by Web-based services, which are not made for long-term sessions.

3.2. Smart buildings

In terms of cost, accuracy, intrusiveness, and privacy, existing occupancy monitoring approaches were analyzed by Akkaya et al. in [36]. For improving the occupancy detection accuracy in a smart building, they used multi-modal data fusion. In the information fusion techniques, noisy measurements generated from IoT devices are filtered and occupancy status is predicted. To reduce the energy consumption of the smart building, they also investigated how occupancy monitoring techniques could be used with data fusion techniques. EUFP7 IoT is a project to devise authentication and authorization mechanisms for service access protection. To extend the security functionalities stated by the architectural reference model for EUFP7 IoT, the framework was proposed in [37]. In [37], the authors proposed this framework to utilize the available localization data and to implement the access control for services provided in smart building. The proposed framework is based on a service management platform which is a city explorer that implements the key security aspects.

3.3. Smart cities

For urban IoT, the authors in [3] presented a survey on the architectures, protocols, and enabling technologies. They describe link layer technologies, Web service-based IoT architecture, and devices suitable for the urban IoT architecture. To enable various IoT applications, a generic top-down IoT architecture for smart cities was proposed in [38]. The integrated information center run by the IoT service provider is the core element of this architecture. This information center is connected to a set of services, such as water, electrical energy, central gas supply, provided in smart cities. Several technologies that are essential for the realization of smart cities, such as IoT co-building, openness, and convergence, are facilitated by this architecture.

In [39], Al-Hader et al. proposed a five-level pyramid architecture for smart cities as shown in **Figure 3**. The bottom layer is the smart infrastructure layer including water, electronics, fire protection, natural gas, electronic communications, and network. The next layer is the smart database resources layer including database server, data resources, and databases. The next layer is the smart building management system layer including building automation, control network, and HVAC. The next layer is the smart interface layer including dashboard, common operational platform, and integrated Web services. The top layer is the smart city. Some of the major functionalities that can be included in smart cities are street lighting, maintenance, waste management, surveillance, building, and emergency health monitoring.

3.4. Smart grid

In [40], an IoT-based real-time monitoring system was proposed for power transmission lines to avoid disasters. In the proposed system, conductor galloping, wind deviation, conductor

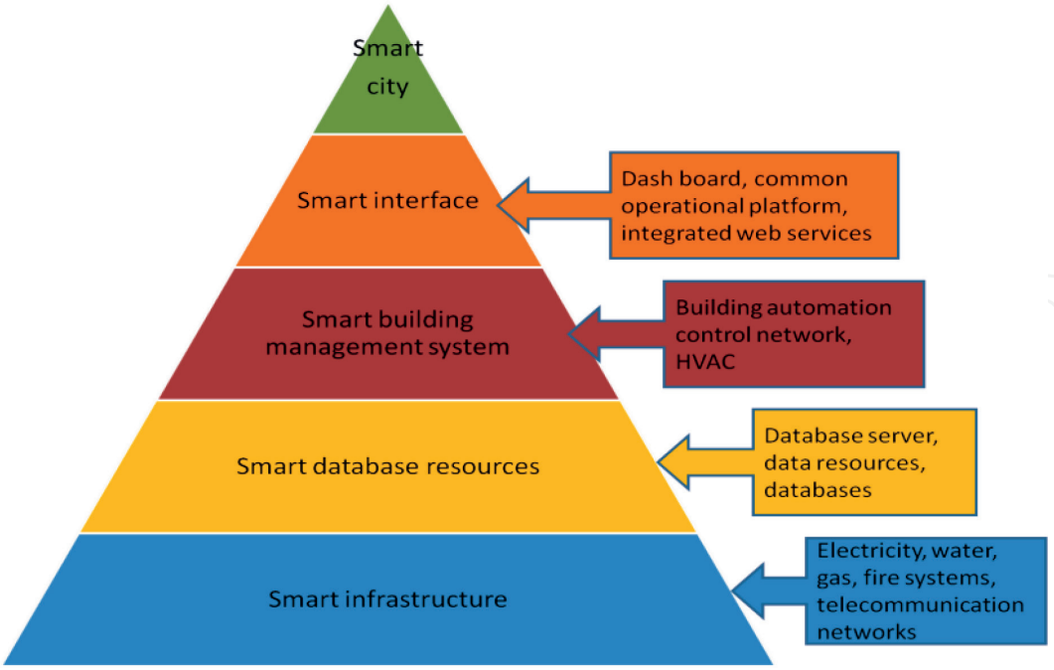

Figure 3. A pyramid architecture for smart cities [39].

temperature, icing, and tower leaning are visually displayed at the monitoring center. These parameters represent the power transmission lines and operational parameters of the tower. So, the system can implement real-time monitoring and early warnings of disaster for minimizing the damage of smart grid caused by natural disasters. In [41], IoT-based smart grid applications were classified into three types: (a) key equipment state monitoring, (b) information collection, and (c) smart grid control. It also describes the types and characteristics of IoT-based smart grids. As a result, a reference architecture for smart grid IoT based on the characteristics was proposed. There are three layers in this reference architecture: perception layer, transport layer, and application layer. For security protection of IoT-based smart grids, a secure access control system is proposed for ensuring that IoT-based smart grid devices can securely access the Internet.

3.5. Smart health

In [42], to monitor, collect, and transmit remote healthcare data, a system architecture based on IoT was proposed. To transfer data to a gateway, IEEE 802.15.4 standard was used and static and adaptive rule engines were developed as well. Through transmitting data based on important parameters extracted from the collected data, these two rules are involved in the decision-making process. As a result, these developed rule engines can minimize network traffic and save energy consumption. To solve issues such as reliability, interoperability, performance, energy efficiency, scalability, and security, the authors in [43] presented a smart e-Health gateway based on IoT. Based on taking responsibility of handling the sensor networks implemented in the remote healthcare center, this smart gateway can address these issues. The authors presented a case study called UTGATE for this smart e-Health gateway. Based on the achieved results from this case study, the smart

e-Health gateway can provide services such as fast data processing, storage, and embedded data mining.

3.6. Smart transportation

The IoT can be used in all aspects of transportation such as geo services, collection of data related to passenger counting, communication, and smart ticketing. In [44], Eurotech provides IT solutions that can help in connecting every public transport element and use the technical tools to connect IT infrastructure with sensors and other devices. To enhance the traffic conditions in cities, the Kapsch Group in [45] investigated how Internet technologies can be leveraged.

3.7. Smart industry

In [46], the authors presented smart factory based on IoT architecture and defined issues such as optimized decision-making, flexibility, remote monitoring, and mass customization, with respect to energy management. By using the proposed mechanism, energy consumption is improved in a smart factory by incorporating energy data into production management.

3.8. Smart agriculture

Water utilization and irrigation can be improved by leveraging weather forecast and farm data, key trends and anomalies, and evapotranspiration index. Building IoT-based smart farming will enable farmers and growers to reduce waste and enhance productivity ranging from the number of journeys the farm vehicles have made to the quantity of fertilizer utilized. In IoT-based smart farming, with the help of sensors such as light, humidity, temperature, soil moisture sensors, a system is built for monitoring the crop field and automating the irrigation system. This system is highly efficient when compared with the conventional approach, and it gives farmers the ability to monitor the field conditions from anywhere.

4. Green IoT

Because of the increasing awareness of environmental issues all over the world, green IoT technology initiatives should be taken into consideration. The concept of greening IoT refers to the technologies that make the IoT environment more healthy in a friendly way by making use of facilities and storages that enable subscribers to gather, store, access, and manage various information. The enabling technologies for green IoT are called information and communication technologies (ICTs) [47]. ICTs can cause climate change in the world [48–52] because with the growing application of ICT much more energy has been consumed. The consideration for sustainability of ICTs has concentrated on data centers optimization through techniques of sharing infrastructure, which leads to increasing the energy efficiency, reducing CO_2 emissions and e-waste of material disposals [53]. Greening ICT is enabling technologies for green IoT, which includes green wireless sensor networks (GWSNs), green machine-to-machine

communication (GM2M), green RFID, green data center (GDC) [5], green cloud computing (GCC), green Internet, and green communication network as shown in **Figure 4**. Therefore, green ICT technologies play an essential role in green IoT and provide many benefits to the society such as decreasing the energy used for designing, manufacturing, and distributing ICT devices and equipment.

Greening IoT is the practice of designing, manufacturing, disposing of computers, servers, and associated subsystems (i.e., monitors, printers, communications equipment, and storage devices) efficiently and more frequently but with reduced effect on the society and the environment [54]. The aim of using green IoT is to look for new resources and minimize IoT devices' negative impact on the health of humans and its disturbance to the environment. The main objective of greening IoT is to reduce pollution and Co_2 emission, exploit environmental conservation, and minimize the costs of things operating and power consumption [55–57]. Details about industrial emissions are analyzed and provided in [58]. These emissions influence environmental change in different regions and over time. Reducing the energy consumption of IoT devices is needed to make the environment healthier [59]. Due to the continuous development of green ICT technologies, green IoT provides a high possibility to support environmental sustainability and economic growth [57]. These valuable and emerging technologies make the world greener and smarter. Therefore, this section reviews the core of green IoT technologies that demonstrate efforts for constructing a green and smart world.

Green IoT consists of designing and leveraging aspects. Green IoT focuses on reducing IoT energy usage and CO_2 emissions, a necessity for building a smart world with the sustainability of intelligent everything. As shown in **Figure 5**, design elements of green IoT refer to developing computing devices, energy efficiency, communication protocols, and networking architectures [57].

The IoT element can be used to eliminate CO_2 emissions, reduce the pollutions and enhance the energy efficiency. Uddin et al. [60] introduced techniques for enhancing the energy efficiency and reducing CO_2 emission for enabling green information technology. Since M2M is equipped with sensors and communication add-ons, these devices can communicate with each other and sense the world. However, sensors will consume high power for executing the tasks. In networking, green IoT aims to identify the location of the relay and number of nodes which satisfy budget constraints and energy saving. To achieve a smart and sustainable world, green IoT plays a significant role in deploying IoT to reduce energy consumption [47], CO_2 emission [61] and pollution [61–63]; exploit environmental conservation [64];

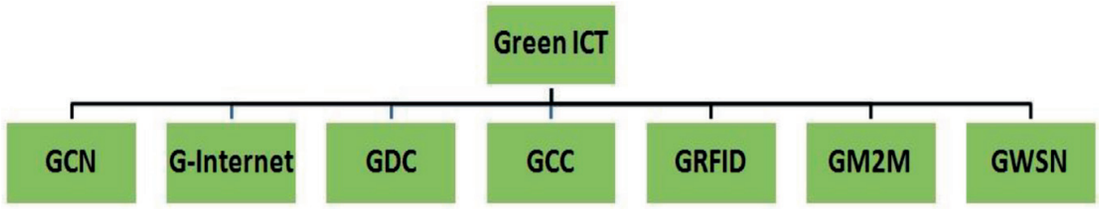

Figure 4. Green ICT technologies.

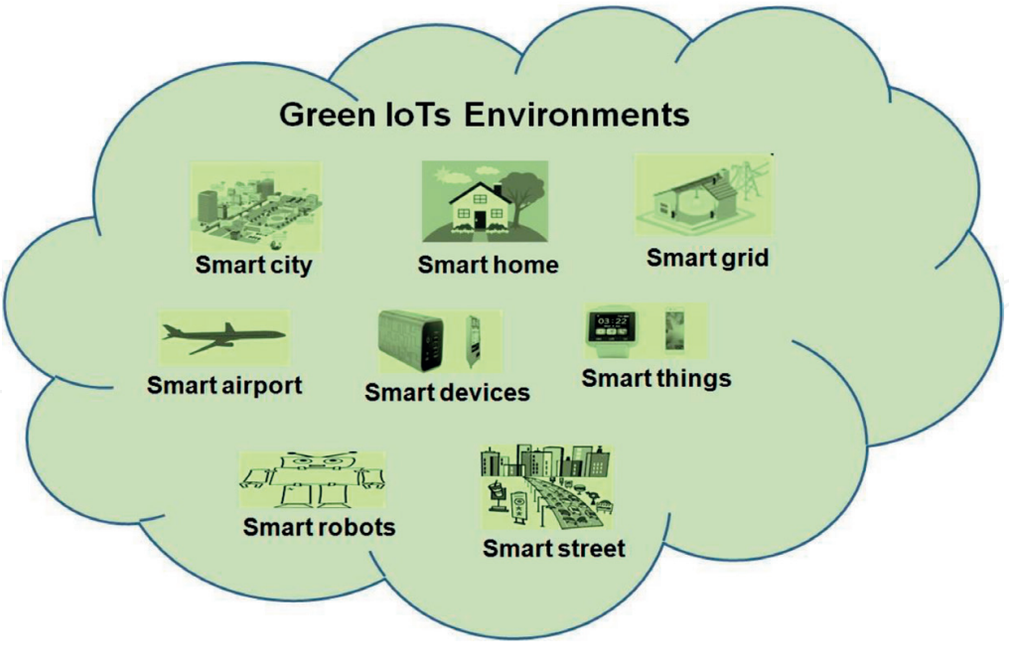

Figure 5. Green IoT environments.

and minimize power consumption [65]. Also, green IoT in [66] is defined as "the study and practice of designing, using, manufacturing, and disposing of servers, computers, and associated subsystems such as monitors, storage devices, printers, and communication network systems efficiently and effectively with minimal or no impact on the environment." There are three concepts for achieving green IoT, namely, design technologies, leverage technologies, and enabling technologies. Design technologies refer to the energy efficiency of devices, communication protocols, network architectures, and interconnections. Leverage technologies refer to cutting carbon emissions and enhancing energy efficiency. Due to green ICT technologies, green IoT has become more efficient through reducing energy, hazardous emissions, resources consumption, and pollution. Consequently, green IoT leads to preserving natural resources, minimizing technology's impact on the environment and human health, and reducing the cost significantly. Therefore, green IoT is indeed focusing on green manufacturing, green utilization, green design, and green disposal [67]. These issues are described as follows.

1. **Green use**: minimizing power consumption of computers and other information systems as well as using them in an environmentally sound manner.

2. **Green design**: designing energy efficient for green IoT sound components, computers, and servers, and cooling equipment.

3. **Green disposal**: refurbishing and reusing old computers and recycling unwanted computers and other electronic equipment.

4. **Green manufacturing**: producing electronic components and computers and other associated subsystems with minimal or no impact on the environment.

http://dx.doi.org/10.5772/intechopen.81891

5. Applications and services for IoT in smart environments

The integration of IoT with smart environments has brought about unprecedented opportunities. This section highlights the main opportunities offered by this environment.

5.1. Real-time information

In an IoT-based smart environment, organizations can collect data about processes and products for analysis in a real-time manner and provide the analyzed information to make appropriate decisions. Based on the decisions taken, the smart environment can rapidly adapt itself and improve operational efficiency that results in higher customer satisfaction.

5.2. Cost-effective cloud-based applications

Cost-effective, flexible, and secure cloud-based applications can transform a smart environment into a decision-making platform by collecting data from the environment and transferring them to the cloud through IoT. The key tasks performed in the cloud server are the analysis of these collected data, decision-making, and prediction of environment parameters.

5.3. New business models

IoT gives companies the ability to build new business models and revenue streams that can create many new business opportunities. IoT has the capability to change the way consumers and businesses follow the world. Therefore, consumers and businesses will require new services that can assist them to explore this ultra-connected, changing landscape. In addition, IoT can enable companies to create new revenue streams and services on top of traditional services, for example, vending machine vendors offering inventory management to those who supply the goods in the machine.

5.4. Intelligent operations

With rapid growth in IoT devices, the data produced by the IoT also grow exponentially. The management of such huge amounts of data will be a challenge in terms of performance. Designing intelligent cloud operation management solutions that can ensure the working of a cloud infrastructure at an optimal level will also be necessary.

6. Future of IoT

Due to the integration of novel concepts as well as the adaption of existing technologies, IoT is still evolving. Thereby, it supports the development of more competitive, realistic, and advanced IoT-based applications. The development of IoT applications based on the client requirements evolves according to the requirements of the users. Moreover, many organizations and interest groups are prepared to standardize IoT-related technologies to ensure more effective and secure applications.

The bright future of green IoT will change our future environment to become healthy, green, very high QoS, and sustainable socially, environmentally, and economically. Recently, the most exciting areas have focused on greening things such as green design and implementations, green communication and networking, integrated RFIDs and sensor networks, green IoT services and applications, energy-saving strategies, mobility and network management, smart objects, the cooperation of homogeneous and heterogeneous networks, and green localization. The following research fields need to be researched to develop optimal and efficient solutions for greening IoT:

1. There is a need for unmanned aerial vehicle (UAV) to replace a massive number of IoT devices, especially in agriculture, traffic and monitoring, which will help to reduce power consumption and pollution. UAV is a promising technology that will lead to green IoT with low cost and high efficiency.
2. Transmission data from the sensor to the mobile cloud must be more useful. Sensor-cloud is integrating the wireless sensor network and mobile cloud. It is a very hot and promising technology for greening IoT. A green social network such as a service (SNaaS) may investigate the energy efficiency of the system, service, WSN, and cloud management.
3. M2M communication plays a critical role to reduce energy use and hazardous emissions. Smart machines must be smarter to enable automated systems. Machine automation delay must be minimized in case of traffic and taking necessary and immediate action.
4. Design Green IoT may be introduced from two perspectives which are achieving excellent performance and high QoS. Finding suitable techniques for enhancing QoS parameters (i.e., bandwidth, delay, and throughput) will contribute effectively and efficiently to greening IoT.
5. While going toward greening IoT, it will be required to use less energy, looking for new resources, minimizing IoT's negative impact on the health of humans and disturbance to the environment. Then, green IoT can contribute significantly to sustainable, smart, and green environment.
6. To achieve energy-balancing for supporting green communication between IoT devices, the radio frequency energy harvest should be taken into consideration.
7. More research is needed to develop the design of IoT devices which helps to reduce CO_2 emission and energy usage. The critical task for smart and green environmental life is saving energy and decreasing the CO_2 emission.

7. Conclusion

In this chapter, the overview and benefits of IoT on telecommunication networks and their challenges were introduced to know how to improve our life and society by building smart IoT systems. In addition, the concept of green IoT and its related services and applications were described in detail. Finally, many research fields, which are needed to develop optimal and efficient solutions for greening IoT, were introduced.

Acknowledgements

This research was supported by the Department of Mathematics, Faculty of Science, Al-Azhar University, Cairo, Egypt. In addition, it was partially supported by King Abdul-Aziz University, Jeddah, Saudi Arabia. I thank both of them for providing guidance to finish this research. I also thank IntechOpen Limited for giving the opportunity for publishing this research work as a book chapter in Telecommunications Networks.

Author details

Asaad Ahmed Gad-Elrab Ahmed[1,2]*

*Address all correspondence to: asaadgad@azhar.edu.eg and aaahmad4@kau.edu.sa

1 King Abdul-Aziz University, Jeddah, Saudi Arabia

2 Department of Mathematics, Faculty of Science, Al-Azhar University, Cairo, Egypt

References

[1] Hayajneh T, Almashaqbeh G, Ullah S, Vasilakos AV. A survey of wireless technologies coexistence in WBAN: Analysis and open research issues. Wireless Networks. 2014; **20**(8):2165-2199

[2] Almashaqbeh G, Hayajneh T, Vasilakos AV, Mohd BJ. QoS-aware health monitoring system using cloud-based WBANs. Journal of Medical Systems. 2014;**38**(10):1-20

[3] Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M. Internet of things for smart cities. IEEE Internet of Things Journal. 2014;**1**(1):22-32

[4] Atzori L, Iera A, Morabito G. The Internet of things: A survey. Computer Networks. 2010; **54**(15):2787-2805

[5] Gluhak A, Krco S, Nati M, Pfisterer D, Mitton N, Razafindralambo T. A survey on facilities for experimental Internet of things research. IEEE Communications Magazine. 2011; **49**(11):58-67

[6] Texas Instrument Organization. The Internet of things: Opportunities & challenges [Online]. 2014. Available from: http://www.ti.com/ww/en/internet_of_things/pdf/14-09-17-IoTforCap.pdf

[7] Internet of Things Technologies. Postscapes [Online]. Available from: http://postscapes.com/internet-of-things-technologies%20#communication

[8] Kasznik E. Internet of things: The third wave of revolution. World Intellect. Property Rev. [Online]. 2015. Available from: http://www.worldipreview.com/contributed-article/semiconductor-focus-the-third-wave-of-revolution

[9] Schneider S. Understanding the protocols behind the Internet of things. Electronic-design [Online]. 2013. Available from: http://electronicdesign.com/iot/understanding-protocols-behind-internet-things

[10] Internet of things protocols & standards. Postscapes [Online]. Available from: http://postscapes.com/internet-of things-protocols

[11] Ganchev I, Ji Z, O'Droma M. A generic IoT architecture for smart cities. In: ISSC 2014/CIICT 2014, Limerick; 2014

[12] Sheng Z, Yang S, Yu Y, Vasilakos A, McCann J, Leung K. A survey on the IETF protocol suite for the Internet of things: Standards, challenges, and opportunities. IEEE Wireless Communications. 2013;**20**(6):91-98

[13] Enjian B, Xiaokui Z. Performance evaluation of 6LoWPAN gateway used in actual network environment. In: International Conference on Control Engineering and Communication Technology (ICCECT), Liaoning; 2012

[14] Khoshdelniat R, Sinniah G, Bakar K, Shaharil M, Suryady Z, Sarwar U. Performance evaluation of IEEE802.15.4 6LoWPAN gateway. In: 17th Asia-Pacific Conference on Communications (APCC), Sabah; 2011

[15] Long N, De Caro N, Colitti W, Touhafi A, Steenhaut K. Comparative performance study of RPL in wireless sensor networks. In: IEEE 19th Symposium on Communications and Vehicular Technology in the Benelux (SCVT), Eindhoven; 2012

[16] Yushev A, Lehmann P, Sikora A. 6LoWPAN with RPL performance measurements in an Automated Physical Testbed. In: 2nd IEEE International Symposium on Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems, Offenburg; 2014

[17] Xie H, Zhang G, Su D, Wang P, Zeng F. Performance evaluation of RPL routing protocol in 6LoWPAN. In: 5th IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing; 2014

[18] Cheng X, Liang Q, He J. Analysis of IEEE802.15.4 network performance comprehensive evaluation and prediction. In: International Conference on Measurement, Information and Control (ICMIC), Harbin; 2013

[19] Marshal I, Alsaryraha O, Chung T, Yang C, Kuob W, Agrawal D. Choices for interaction with things on Internet and underlying issues. Ad Hoc Networks. 2015;**28**:68-90

[20] Macedo D, Guedes L, Silva I. A dependability evaluation for Internet of things incorporating redundancy aspects. In: ICNSC, Miami, FL; 2014

[21] Sevone. How will the Internet of things disrupt your performance monitoring strategy? – White paper [Online]. 2015. Available from: https://www.sevone.com/white-paper/how-will-internetthings-disrupt-your-performance-monitoring-strategy

[22] Biswas AR, Giaffreda R. IoT and cloud convergence: Opportunities and challenges. In: IEEE World Forum on Internet of Things (WF-IoT), Seoul; 2014

[23] Maalel N, Natalizio E, Bouabdallah A, Roux P, Kellil M. Reliability for emergency applications in Internet of things. In: IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS), Cambridge, MA; 2013

[24] Kempf J, Arkko J, Beheshti N, Yedavalli K. Thoughts on reliability in the Internet of things [Online]. Available from: https://www.iab.org/wp-content/IAB-uploads/2011/03/Kempf.pdf

[25] Li L, Jin Z, Li G, Zheng L, Wei Q. Modeling and analyzing the reliability and cost of service composition in the IoT: A probabilistic approach. In: IEEE 19th International Conference on Web Services (ICWS), Honolulu, HI; 2012

[26] Xu T, Wendt J, Potkonjak M. Security of IoT systems: Design challenges and opportunities. In: IEEE/ACM International Conference on Computer-Aided Design (ICCAD), San Jose, CA; 2014

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

[28] Liu C, Zhang Y, Zhang H. A novel approach to IoT security based on immunology. In: 2013 9th International Conference on Computational Intelligence and Security (CIS), Leshan; 2013

[29] Evans D. The Internet of things – cisco Whitepaper [Online]. 2011. Available from: http://www.iotsworldcongress.com/documents/4643185/3e968a44-2d12-4b73-9691-17ec508ff67b

[30] Sarkar C, Nambi S, Prasad R, Rahim A. A scalable distributed architecture towards unifying IoT applications. In: IEEE World Forum on Internet of Things (WF-IoT), Seoul; 2014

[31] Barbosa V, Souza C, Masip-Bruin X, Marin-Tordera E, Ramirez W, Sanchez-Lopez S. Towards the scalability of a service-oriented PCE architecture for IoT scenarios. In: 20th European Conference on Networks and Optical Communications – (NOC), London; 2015

[32] Ishaq I, Carels D, Teklemariam G, Hoebeke J, Vanden Abeele F, De Poorter E, et al. IETF standardization in the field of the Internet of things (IoT): A survey. Journal of Sensor and Actuator Networks. 2013;**2**(2):235-287

[33] Chun SM, Park JT. Mobile CoAP for IoT mobility management. In: 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV; 2015

[34] Fu H-L, Lin P, Yue H, Huang G-M, Lee C-P. Group mobility management for large-scale machine-to-machine mobile networking. IEEE Transactions on Vehicular Technology. 2013;**63**(3):1296-1305

[35] Kim Y, Lee Y. Automatic generation of social relationships between Internet of things in smart home using SDN-based home cloud. In: IEEE 29th International Conference

on Advanced Information Networking and Applications Workshops (WAINA); 2015. pp. 662-667

[36] Akkaya K, Guvenc I, Aygun R, Pala N, Kadri A. IoT-based occupancy monitoring techniques for energy-efficient smart buildings. In: IEEE Wireless Communications and Networking Conference Workshops (WCNCW). IEEE; 2015. pp. 58-63

[37] Herńandez-Ramos JL, Moreno MV, Bernabè JB, Carrillo DG, Skarmeta AF. Safir: Secure access framework for IoT-enabled services on smart buildings. Journal of Computer and System Sciences. 2014

[38] Ganchev I, Ji Z, O'Droma M. A generic IoT architecture for smart cities. In: 25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC'14/CIICT'14). IET; 2014. p. 196199

[39] Al-Hader M, Rodzi A, Sharif AR, Ahmad N. Smart city components architecture. In: International Conference on Computational Intelligence, Modelling and Simulation, Brno; 2009

[40] Ou Q, Zhen Y, Li X, Zhang Y, Zeng L. Application of Internet of things in smart grid power transmission. In: Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing (MUSIC). IEEE; 2012, pp. 96-100

[41] Wang Y, Lin W, Zhang T, Ma Y. Research on application and security protection of Internet of things in smart grid; 2012. pp. 1-5

[42] Kiran M, Rajalakshmi P, Bharadwaj K, Acharyya A. Adaptive rule engine based IoT enabled remote healthcare data acquisition and smart transmission system. In: IEEE World Forum on Internet of Things (WF-IoT'14); March 2014. pp. 253-258

[43] Rahmani AM, Thanigaivelan N, Gia TN, Granados J, Negash B, Liljeberg P, et al. Smart e-health gateway: Bringing intelligence to internet-of-things based ubiquitous healthcare systems. In: Consumer Communications and Networking Conference (CCNC), 2015 12th Annual IEEE; Jan 2015. pp. 826-834

[44] EuroTech. Smart Mobility with IoT/M2M Solutions. [Online]. Available from: https://www.eurotech.com/en/ [Accessed: 28 September, 2015]

[45] Kapsch. Driving the future. Powered by kapsch. [Online]. Available from: https://www.kapsch.net/ [Accessed: 28 September, 2015]

[46] Shrouf F, Ordieres J, Miragliotta G. Smart factories in industry 4.0: A review of the concept and of energy management approached in production based on the Internet of things paradigm. In: IEEE International Conference on Industrial Engineering and Engineering Management (IEEM). IEEE; 2014. pp. 697-701

[47] Zhu C, Leung VC, Shu L, Ngai EC-H. Green Internet of things for the smart world. IEEE Access. 2015;**3**:2151-2162

[48] Sala S. Information and communication technologies for climate change adaptation, with a focus on the agricultural sector. In: Thinkpiece for CGIAR Science Forum Workshop

on ICTs Transforming Agricultural Science, Research, And Technology Generation, Wageningen, Netherlands; 2009. pp. 16-17

[49] Eakin H, Wightman PM, Hsu D, Gil Ramón VR, Fuentes-Contreras E, Cox MP, et al. Information and communication technologies and climate change adaptation in Latin America and the Caribbean: A framework for action. Climate and Development. 2015; **7**:208-222

[50] Upadhyay AP, Bijalwan A. Climate change adaptation: Services and role of information communication technology (ICT) in India. American Journal of Environmental Protection. 2015;**4**:70-74

[51] Zanamwe N, Okunoye A. Role of information and communication technologies (ICTs) in mitigating, adapting to and monitoring climate change in developing countries. In: International conference on ICT for Africa; 2013

[52] Mickoleit A. Greener and Smarter: ICTs, the Environment and Climate Change. OECD Publishing; 2010

[53] Di Salvo AL, Agostinho F, Almeida CM, Giannetti BF. Can cloud computing be labeled as "green"? Insights under an environmental accounting perspective. Renewable and Sustainable Energy Reviews. 2017;**69**:514-526

[54] Murugesan S, Harnessing green IT: Principles and practices, IT professional;10; 2008

[55] Rani S, Talwar R, Malhotra J, Ahmed SH, Sarkar M, Song H. A novel scheme for an energy efficient Internet of things based on wireless sensor networks. Sensors. 2015; **15**:28603-28626

[56] Huang J, Meng Y, Gong X, Liu Y, Duan Q. A novel deployment scheme for green Internet of things. IEEE Internet of Things Journal. 2014;**1**:196-205

[57] Gapchup A, Wani A, Wadghule A, Jadhav S. Emerging trends of green IoT for smart world. International Journal of Innovative Research in Computer and Communication Engineering. 2017;**5**:2139-2148

[58] Lü Y-L, Geng J, He G-Z. Industrial transformation and green production to reduce environmental emissions: Taking cement industry as a case. Advances in Climate Change Research. 2015;**6**:202-209

[59] Arshad R, Zahoor S, Shah MA, Wahid A, Yu H. Green IoT: An investigation on energy saving practices for 2020 and beyond. IEEE Access. 2017;**5**:15667-15681

[60] Uddin M, Rahman AA. Energy efficiency and low carbon enabler green IT framework for data centers considering green metrics. Renewable and Sustainable Energy Reviews. 2012;**16**:4078-4094

[61] Xiaojun C, Xianpeng L, Peng X. IOT-based air pollution monitoring and forecasting system. In: 2015 International Conference on Computer and Computational Sciences (ICCCS), IEEE; 2015. pp. 257-260

[62] Manna S, Bhunia SS, Mukherjee N. Vehicular Pollution Monitoring using IoT, Recent Advances and Innovations in Engineering (ICRAIE). IEEE; 2014. pp. 1-5

[63] Zupancic T, Westmacott C, Bulthuis M. The impact of green space on heat and air pollution in urban communities: A meta-narrative systematic review. Vancouver, BC, Canada: David Suzuki Foundation; 2015

[64] Bandyopadhyay D, Sen J. Internet of things: Applications and challenges in technology and standardization. Wireless Personal Communications. 2011;**58**:49-69

[65] Shaikh FK, Zeadally S, Exposito E. Enabling technologies for green Internet of things. IEEE Systems Journal. 2015;**11**:983-994

[66] Murugesan S, Gangadharan G. Harnessing Green IT: Principles and Practices. Chichester, West Sussex, United Kingdom: John Wiley & Sons Ltd; 2012

[67] Nandyala CS, Kim H-K. Green IoT agriculture and healthcare application (GAHA). International Journal of Smart Home. 2016;**10**:289-300