Future Aspects and Challenges of the Internet of Things for the Smart Generation

Chander Diwaker, Pradeep Tomar and Atul Sharma

Abstract The internet is now a basic necessity for human beings, especially in modern cities and metropolitan areas. Without the internet, an educated person feels helpless and unable to understand and follow events. At present, most people depend on machines. The field of computer engineering has helped the process of automation and the control of software as well as hardware devices. The internet of things (IoT) is a field of computer engineering that presents a synchronous behavior of components in a real-time system. Every piece of hardware and software that assists in accessing the internet or is used by the internet constitutes a main part of the IoT. The IoT includes the applications used in every field, e.g., healthcare, engineering, designing, inventory control, machine control, selling-purchasing, and the export-import of goods etc. In modern cities almost everyone uses the internet with individuals being linked to it through variable bandwidths and network ranges. People can access internet easily but they are not aware of the various issues, problems, and challenges of providing data to everyone at the same time on an unlimited number of topics. In this paper, the architecture of the IoT, the functioning of the IoT, the applications of the IoT in different fields, along with the research challenges and problems relating to the IoT are discussed.

Keywords IoT · Cloud computing · Applications · Security
Future aspects

C. Diwaker (✉) · A. Sharma
Department of CSE, UIET, Kurukshetra University, Kurukshetra, Haryana, India
e-mail: chander_cd@rediffmail.com

A. Sharma
e-mail: atulsharma2204@gmail.com

P. Tomar
Department of CSE, School of ICT, Gautam Buddha University, Greater Noida, Uttar Pradesh, India
e-mail: parry.tomar@gmail.com

A. Kumar and S. Mozar (eds.), *ICCCE 2018*,
Lecture Notes in Electrical Engineering 500,
https://doi.org/10.1007/978-981-13-0212-1_61

1 Introduction

The basis of the IoT is networking. The main components of networking are sensors; a finite set of heterogeneous devices that supports networking, storage devices, variable size of files, service providing, distributed system, and maintenance of networks etc. It is a collection of a heterogeneous system that is connected in a distributed manner to provide service to a customer for a particular query. Cloud computing also plays an important role in the IoT [1].

The revolution of the IoT started in 1970. At that time, there were low-speed processors, less RAM and cache memories, and low stage space. Currently, the speed of the processor, the capacity of RAM, the large data storage space, and small size of components help to perform high-speed data communication. The IoT helps in sending, receiving, and sharing information using the internet.

The IoT has applications in every field of engineering: from agriculture to flight systems, car manufacturing, education systems, software development, and real-time systems etc. The IoT includes the entire field in which software is used to manage and control things.

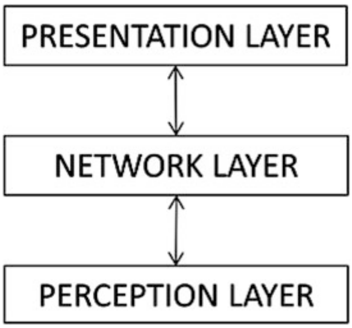
2 Architecture of the IoT

The IoT's architecture consists of three layers, i.e. perception layer, network layer, and application layer. The working of each layer is equivalent to an OSI model. Figure 1 shows the architecture for the IoT [2]:

(i) *Perception layer*: This is equivalent to the physical layer. It includes different types of sensors. Different sensors are used for different types of sensing information. The hardware components used are sensors, IP cameras, actuators, embedded communication and closed-circuit Television (CCTV), bluetooth, radio-frequency identification (RFID), and near-field Communication (NFC) etc.

(ii) *Network layer*: This uses a network device to find the optimal route for sending data packets. The network devices used are routers, bridges,

Fig. 1 Architecture of the IoT



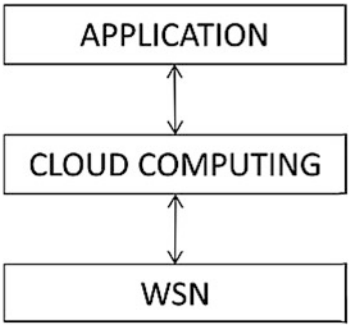


Fig. 2 Equivalent layers of the architecture of the IoT

gateways, hubs, and switches. The techniques used are 2G, 3G, 4G, and local area network (LAN) etc. Cloud computing and big data strategies are used to store and manage data.

(iii) *Presentation layer*: This uses different protocols for data transmission and to present that data in an understating and meaningful manner. This layer assists in monitoring and providing services to users.

The use of the IoT and its applications can be used based on the concept of 5As, i.e. anything, anytime, anywhere, anyhow, and anyway [3].

An equivalent layer architecture of the IoT is shown in Fig. 2. It includes the same layers as shown in Fig. 1 [4].

(i) *WSN*: WSN use set of protocols that provide the location of data, quality of service, and security to the network.

(ii) *Cloud Computing*: The architecture of cloud computing has three types: Software as a service (SaaS), infrastructure as a service (IaaS) and platform as a service (PaaS). These are responsible for data analytics, data storage, data visualization, and data computation.

(iii) *Application Layer*: The information provided by cloud computing is helpful in monitoring different activities at end users, such as building design monitoring, health monitoring, surveillance for security purpose, environmental monitoring, and transportation system monitoring etc.

3 Applications of the IoT

The IoT helps in developing smart devices, smart cars, smart cities, smart homes, and smartphones etc. The main research areas of the IoT are ad hoc networks, wireless sensor networks (WSN), cyber-physical systems (CPS), mobile computing (MC), and pervasive computing (PC) [5]. The interaction in these area helps in growing the IoT and helps its better utilization. Table 1 shows the general applications of the IoT.

Table 1 General applications of the IoT [4]

Healthcare services	Monitoring health activities
Emergency services, defence	Remote control, resource management, resource distribution, monitoring future and current disaster information
Crowd monitoring services	Monitoring crowds in public and private places
Traffic management services	Managing and monitoring real-time traffic conditions on the road air, in the air, and on the water, smart parking
Infrastructure services	Monitoring structural faults, accident monitoring
Water services	Quality, usage, waste management distribution, leakage, usage
Building management services	Temperature, activities for monitoring energy usage management, humidity control, heating, ventilation, and air conditioning (HVAC)
Environmental services	Waterways, air pollution, industry monitoring, noise monitoring

4 Challenges Facing the IoT

For successful implementation of the IoT, the prerequisites are [6]:

(i) *Dynamic demand*: The demand of accessing resources is increasing dynamically on the internet. Systems should be set up in a manner that enables them to handle and manage heavy load if resource demand increases.
(ii) *Real-time Systems*: A system should have the capability to tolerate faults and automatically repair faults.
(iii) Access to an open and interoperable cloud system.
(iv) Power usage of applications.
(v) Carrying out of the applications close to end users.
(vi) *Scalability*: Scalability is a concern with providing data as soon as possible and with minimum error. The addition of storage devices, processors, and low power consumption is a challenge.
(vii) *Multi-tenancy*: Multi-tenancy is a concern with shared IoT devices. Multi-tenancy minimizes faults as it uses shared machines. If one machine is not working properly or shows an error, the same work can be completed by another machine.
Multi-tenancy is necessary for monitoring health activities via pacemakers, MRI machines, ECG, CT Scans and other real-time systems.
(viii) *Network security*: This includes cryptography mechanisms, along with detection, prevention, and avoidance of attacks and intruders, and cyber crime etc.
(ix) *Low-power communication*: The addition of more memory, storage devices, and processors speeds up the whole system, but it consumes a lot of power and energy. The use of a greater number of electronic devices leads to an increase in electronic pollution.

(x) *Security Challenges*: Security in the non-real environment has a varied nature, i.e. the problem can be repaired or corrected after a period of time. However, in real time, high security must be implemented that can detect and avoid any mishaps while achieving a particular target, as observed in military operations, flight systems and healthcare systems [2]. The key factors of security are trust in another system, data privacy, and data confidentiality. Data Privacy and data protection are important factors that should be addressed with a high priority.

(xi) *Radio spectrum*: The use of different radio frequencies and spectra influence data transmission and reception. As the number of user increases, the demand also increases. The available frequency spectrum becomes less as demand rises. There is a need to increase the number of spectra for data transmission and receiving so that the demand of users can be fulfilled within an appropriate time period.

5 Related Work

Researchers and practitioners are focusing on sensors and energy generation mechanisms with reduced costs and less time-consuming mechanisms. The most recent work on the IoT found as follows.

Vyas et al. [7] discussed the applications, various application areas, challenges facing the IoT, and future aspects of the IoT. This paper focuses on open issues like naming, traffic characterization, QoS support, data integrity and data forgetting, security, and data management etc. It also looked at how big data can be used to manage a large database.

Perera et al. [8] discussed the necessity of IoT for a human body like of use of IoT-based wristwatches, socks, footwear, bands, gloves, helmets, and rings. This study included some of the trends in the IoT solutions based on domains, functionalities, and value. A survey compared approximately 70 different products with respect to variability, unit subscription, and service provided, such as Xively, PROJECT GRIZZLY, Smart Pile, NFC ring, SIGMO, Smart Things, and Where Dial etc. This survey took place during 2011–2103.

Ziegeldorf et al. [9] analyzed privacy issues in the IoT. Various privacy threats were classified and examined for identification, profiling, and tracking of known threats. The major threats to privacy were identified, i.e. violating interactions and presentations, inventory attacks, lifecycle transitions, and information linkage arise. As data accessing and storage demand increases, various threats make the management of big data a challenge.

Rad and Ahmada [10] focused on various applications of the IOT in different areas and explored the challenges and opportunities facing global industries. This study discussed the implementation and usability of the IoT on a global scale.

The application of the IoT in ways that are useful for both humans and traffic was also discussed.

Kaur and Kaur [11] focused on driver technologies and system design of the IoT. The relation of big data with IoT was also discussed. The use of the IoT was surveyed based on person to person (P2P), person to machine (P2M), and machine to machine (M2M) criteria. It was observed that 1% of the IoT is used for retail purposes and 41% of IoT-based applications are used for medical systems. A comparison of different protocols used in the application layer was also discussed. Parametric analysis was used in resolving challenges encountered in the IoT.

Gubbi et al. [4] presented a cloud-centric vision for the IoT. An implementation of cloud used Aneka based on the interaction of public and private clouds. It concluded that there is a need for convergence of the internet, WSNs, and distributed computing. This study presented the evolution of the IoT using a hype cycle of emerging technologies. The study focused on different groups in the city of Melbourne. Future technology will depend on machines rather than human beings.

Zeinab and Elmustafa [12] reviewed IoT applications and future possibilities relating to new technologies. The challenges and problems faced at the time of implementation were also discussed. The applications included smart cities, smart environments, smart energy and smart grids, smart manufacturing, and smart healthcare. The main issues in managing the IoT data are cloud computing, big data, security, privacy, distributed computing, and fog computing etc.

6 Future Aspects of the IoT

The future work is going on, How to use heat/energy released by different components, the vibration of components, movement of components, radio/other frequencies, wind energy, the temperature for providing high-speed networking, energy to hardware components, reusable electronic waste (e-waste), and other scratched material to generate energy and new products. Figure 3 shows, How the energy can be generated by using different resources that are easily available on earth. The main focus is on generating energy that can be sensed by a particular sensor through utilizing the following aspects:

- **Heat Energy**: Every machine that runs, with either a high speed or a low speed, consumes and exhausts heat energy. This heat can be used to increase the lifetime and to charge, or fulfill the requirement of energy to a particular machine. Those machines in which the engine/machine uses more displacement or horsepower release a huge amount of heat that can be used by applying a feedback mechanism to provide extra power to the machine. Alternatively this heat energy can be stored for the further use of the machine. The heart energy realized by a human being can also be used to power small machines, such as mobiles or watches.

Fig. 3 Different ways of energy generation by different aspects

- **Vibration or Movement**: Energy can be generated by moving objects and vibration in objects. More vibrations and movement provide a greater generation of heat and energy.
- **Frequency**: High speed and high capacity frequency can be used for the generation of energy. However, these frequencies can only be used in particular ranges that don't affect human life.
- **Natural Resources**: Wind energy and solar energy can be major sources of energy. People need to be more aware of these natural resources in order to reduce pollution and increase economic wealth.
  Natural energy is a big source of energy production. It includes heat released by volcanos and the energy in deep layers of the earth. Other research is also stated: "How the plants survive in a different environment". If a plant can produce food using photosynthesis for survival, then a plant can be used to generate energy that can be used to run different kinds of applications.
- **Pollution/Smoke**: Researchers have experimented with using gases generated by the pollution of vehicles and industries to generate energy that can be used in different fields.

- **Other Components**: In computer networking there are a number of servers, client systems, and other hardware devices running for 24 h a day that release a lot of harmful gases and heat. These gases and heat can be used to generate and store energy that can then be used later.
- **Recycling of E-waste and others wastes**: E-waste is increasing daily. E-waste can be utilized to make/produce new products that will save time and money.

7 Conclusion

The IoT is becoming a part of human life. Without IT, it is difficult to live in the modern era or in a developing country. It has become a basic necessity of life. In this paper, an attempt has been made to present the highlights of the IoT, and the various research issues and challenges relating to it. The IoT in growing at an increasing rate every day and it is becoming a challenge to manage and provides services to end users. These challenges and problems can be minimized through the use of natural resources and the application of some logical mechanisms.

References

1. Alsaadi E, Tubaishat A (2015) Internet of things: features, challenges, and vulnerabilities. Int J Adv Comput Sci Inf Tech 4(1):1–13
2. Kumar JS, Patel DR (2014) A survey on internet of things: security and privacy issues. Int J Comput Appl 90(11):20–26
3. Madakam S, Ramaswamy R, Tripathi S (2015) Internet of things (IoT): a literature review. J Comput Commun 3(5):164–173
4. Gubbi J, Buyya R, Marusic S, Palaniswami M (2013) Internet of things (IoT): a vision, architectural elements, and future directions. Future Gener Comput Syst 29(7):1645–1660
5. Stankovic JA (2014) Research directions for the internet of things. IEEE Internet Things J 1 (1):3–9
6. Rose K, Eldridge S, Chapin L (2015) The internet of things: an overview. Internet Society, 1–50
7. Vyas DA, Bhatt D, Jha D (2016) IoT: trends, challenges and future scope. Int J Comput Commun 7(1):186–197
8. Perera C, Liu CH, Jayawardena S (2015) The emerging internet of things marketplace from an industrial perspective: a survey. IEEE Trans Emerg Top Comput 3(4):585–598
9. Ziegeldorf JH, Morchon OG, Wehrle K (2014) Privacy in the internet of things: threats and challenges. Secur Commun Netw 7(12):2728–2742
10. Rad BB, Ahmada HA (2017) Internet of things: trends, opportunities, and challenges. Int J Comput Sci Netw Secur 17(7):89–95
11. Kaur J, Kaur K (2017) Internet of things: a review on technologies, architecture, challenges, applications, future trends. Int J Comput Netw Info Secur 4:57–70
12. Zeinab KAM, Elmustafa SAA (2017) Internet of things applications, challenges and related future technologies. World Sci News 2(67):126–148