International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

A Survey on the Internet of Things

Akhilesh Kumar Singh#*, Archana Tandon! and Nidhi Rai#

#Dept. of Computer Science & Engineering, !M.C.A. Department, LDCITS Soraon, Prayagraj, India

Received 02 Feb 2020, Accepted 03 April 2020, Available online 06 April 2020, **Vol.10, No.2 (March/April 2020)**

Abstract

This paper describes the Internet of Things (IoT). Main enabling factor of these promising paradigms is the integration of several technologies, wired and wireless sensor and actuator networks. Internet of things (IoT) plays the role of an expert's technical tool by empowering physical resources into smart entities through existing network infrastructures. The main focus of Internet of things (IoT) is to provide smart and seamless services at the user end without any interruption. The IoT paradigm is formulating large and complex information system with the combination of sensor data acquisitions, efficient data exchange through networking, artificial intelligence, big data, machine learning and cloud computing, collecting information and maintaining the confidentiality of an independent entity and then running together with privacy and security provision in IoT is the main concerning issue. The main problem arises using the new advance technology such as new applications and policies, smart vehicular system, secure tools, analytics tools IoT generated data.

Keywords: *Internet of things (IoT), Architecture, Security and surveillance, challenges.*

1. Introduction

Internet of Things (IoT) is the networking of physical objects that contain electronics embedded within their architecture in order to communicate and sense interactions amongst each other or with respect to the external environment. In the upcoming years, IoT-based technology will offer advanced levels of services and practically change the way people lead their daily lives. Advancements in medicine, power, gene therapies, agriculture, smart cities, and smart homes are just a very few of the categorical examples where IoT is strongly established. The basic idea of this concept is the pervasive presence around us of a variety of things or objects-such as Radio-Frequency Identification (RFID) tags, sensors, actuators, mobile phones etc. Which through unique addressing schemes are able to interact with each other and cooperate with their neighbors to reach common goal (D.Giusto *et al*, 2010)? The number of connected devices is growing exponentially, forming the so-called Internet of Things (IoT), a large network of networks connecting smart devices such as sensors and actuators. Such devices are adopted in various domains such as public health, smart grids, smart transportation, waste management, smart homes, smart cities, agriculture, energy management, etc. (El-hajj, 2017; Atzori, 2010).

The IoT allows objects to be sensed or controlled remotely across existing network infrastructure (Harvard Business Review, 2014), creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention (Vermesan Ovidiu, 2013; Mattern Friedemann; Santucci Gerald; Lindner Tim, 2015).

2. Architecture of IoT

For the architecture of IoT, there is no single consensus. Different Architecture has been proposed by different researchers.

Three layer and five-layer Architecture

The most basic architecture is three-layer architecture as shown in figure-1.

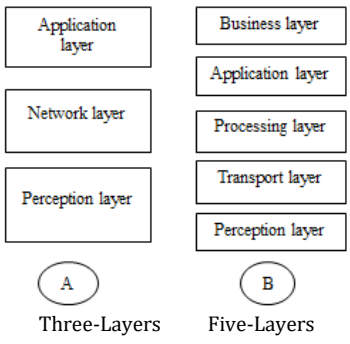

Figure1: Architecture of IoT

*Corresponding author's ORCID ID: 0000-0002-0096-7962
DOI: https://doi.org/10.14741/ijcet/v.10.2.11

It was introduced in the early stages of research in this area. It has three layers, namely, the perception, network, and application layers.

(i)The perception layer- is the physical layer, which has sensors for sensing and gathering information about the environment. It senses some physical parameters or identifies other smart objects in the environment.
(ii)The network layer- is responsible for connecting to other smart things, network devices, and servers. Its features are also used for transmitting and processing sensor data.
(iii)The application layer- is responsible for delivering application specific services to the user. It defines various applications in which the Internet of Things can be deployed, for example, smart homes, smart cities, and smart health. The three-layer architecture defines the main idea of the Internet of Things, but it is not sufficient for research on IoT because research often focuses on finer aspects of the Internet of Things. That is why, we have many more layered architectures proposed in the literature.

One is the five-layer architecture, which additionally includes the processing and business layers (I. Mashal, 2015; O. Said, 2013; M. Wu, 2010 R. Khan, 2012). The five layers are perception, transport, processing, application and business layers (see Figure-1).The role of the perception and application layers is the same as the architecture with three layers. We outline the function of the remaining three layers.

(i) The transport layer- transfers the sensor data from the perception layer to the processing layer and vice versa through networks such as wireless, 3G, LAN, Bluetooth, RFID, and NFC.
(ii) The processing layer- is also known as the middleware layer. It stores, analyzes, and processes huge amounts of data that comes from the transport layer. It can manage and provide a diverse set of services to the lower layers. It employs many technologies such as databases, cloud computing, and big data processing modules.
(iii) The business layer- manages the whole IoT system, including applications, business and profit models, and user's privacy. The business layer is out of the scope of this paper. Hence, we do not discuss it further.

Another architecture proposed by Ning and Wang (2011) is inspired by the layers of processing in the human brain. It is inspired by the intelligence and ability of human beings to think, feel, remember, make decisions, and react to the physical environment. It is constituted of three parts. First is the human brain, which is analogous to the processing and data management unit or the data center. Second is the spinal cord, which is analogous to the distributed network of data processing nodes and smart gateways. Third is the network of nerves, which corresponds to the networking components and sensors.

3. Security in IoT

The security of information and Network should be fitted with these properties such as identification, integrity, confidentiality and un-deniability. The IoT will be applied to the crucial area of national economy i.e. medical service and health care. So the security needs in the IoT will be higher in availability and dependability.

In general, the IoT can be divided into four levels (G. Yang, 2010). Figure-2 shows that the level architecture of the IoT. The most basic level is the perceptual layer (also known as recognition layer), which collects all kinds of information through physical equipment and identifies the physical world, the information includes object properties, environmental condition etc., and physical equipment's include RFID reader, all kinds of sensors, GPS and other equipment's. The key component in this layer is sensors for capturing and representing the physical world in the digital world.

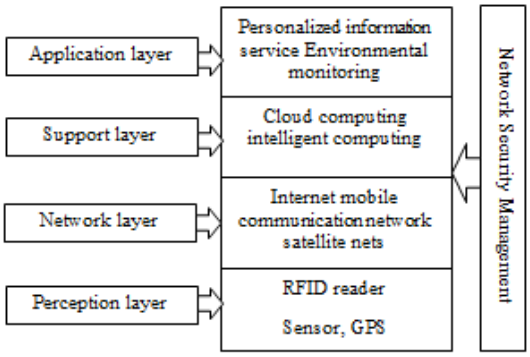

Figure 2 Security Architecture

The second level is network layer. Network layer is responsible for the reliable transmission of information from perceptual layer, initial processing of information, classification and polymerization. In this layer the information transmission is relied on several basic networks, which are the internet, mobile communication network, satellite nets, wireless network, network infrastructure and communication protocols are also essential to the information exchange between devices.

The third level is support layer. Support layer will set up a reliable support platform for the application layer, on this support platform all kind of intelligent computing powers will be organized through network grid and cloud computing. It plays the role of combining application layer upward and network layer downward. The application layer is the topmost and terminal level.

Application layer provides the personalized services according to the needs of the users. Users can access to the internet of thing through the application layer interface using of television, personal computer or mobile equipment and so on. Network security and management play an important role in above each level.

4. Security Features

a) Perceptual Layer- Usually perceptual nodes are short of computer power and storage capacity because they are simple and with less power. Therefore it is unable to apply frequency hopping communication and public key encryption algorithm to security protection. And it is very difficult to set up security protection system. Meanwhile attacks from the external network such as deny of service also bring new security problems. In the other hand sensor data still need the protection for integrity, authenticity and confidentiality.
b) Network Layer- Although the core network has relatively complete safety protection ability, but Man-in-the Middle Attack and counterfeit attack still exist, meanwhile junk mail and computer virus cannot be ignored, a large number of data sending cause congestion. Therefore security mechanism in this level is very important to the IoT.
c) Support Layer- Do the mass data processing and intelligent decision of network behavior in this layer, intelligent processing is limited for malicious information, so it is a challenge to improve the ability to recognize the malicious information.
d) Application Layer- In this level security needs for different application environment are different, and data sharing is that one of the characteristics of application layer, which creating problems of data privacy, access control and disclosure of information (G. Yang, 2010; C. Ding, 2011).

5. Challenges

IoT as a very active and new research field, a variety of questions need to be solved, at different layers of the architecture and from different aspects of information security, the following subsections analyze and summarize common challenges for security of IoT.
(i) Security Structure- In (C. Ding, 2011), the IoT will remain stable-persisting as a whole over time, putting together the security mechanism of each logical layer cannot implement the defense-in-depth of system, so it is a challenge and important research area to construct security structure with the combination of control and information.
(ii) Key Management- Because key management is the important basis of more security mechanism, it is always the hot research area. It is still the most difficult aspect of cryptographic security. Currently the researchers don't find ideal solutions. Lightweight cryptographic algorithm or higher performance of sensor node is still not applied. So far the real large-scale sensor network is always seldom put into practice. The problems of network security will be paid more attention to and become key points and difficulties of research in this network environment (T. Polk, 2010).
(iii)Security Law and Regulations- Currently security law and regulations is still not the main focus, and there is no technology standard about the IoT. The IoT is related to national security information, business secrets and personal privacy. Therefore, our country needs the legislative point of view to promote development of the IoT. Policies and regulations are urgently needed. In this aspect we have a long way to go.
(iv)Requirements for Burgeoning Applications- With the development of WSNs, radio frequency identification (RFID), pervasive computing technology, network communication technology, and distributed real-time control theory, CPS, an emerging form of IoT, is becoming a reality (J. F. Wan, 2011; J. H. Shi, 2011). In this system, the high security is necessary for guaranteeing system performance.

6. Advantages and Disadvantages

(A) Advantage

(i)Communication- Since IoT has communication between devices, in which physical devices are able to stay connected and hence the total transparency is available with lesser inefficiencies and greater quality.
(ii)Automation and Control- Without human involvement, machines are automating and controlling vast amount of information, which leads faster and timely output.
(iii)Monitoring saves money and time- Since IOT uses smart sensors to monitor various aspects in our daily life for various applications which saves money and time

(B) Disadvantage

(i)Compatibility- As devices from different manufacturers will be interconnected in IoT, presently; there is no international standard of compatibility for the tagging and monitoring equipment.
(ii)Complexity- The IoT is a diverse and complex network. Any failure or bugs will occurs in the software or hardware will have serious consequences.
(iii)Privacy/Security- IoT has involvement of multiple devices and technologies and multiple companies will be monitoring it. Since lot of data related to the context will be transmitted by the smart sensors, there is a high risk of losing private data.
(iv) Lesser employment of menial staff- With the advent of technology, daily activities are getting automated by using IoT with less human intervention, which in turn causes fewer requirements of human resources. This causes unemployment issue in the society.

Conclusion

The Internet has changed drastically the way we live, moving interactions between people at a virtual level in several contexts spanning from the professional life to social relationships. The IoT has the potential to add a new dimension to this process by enabling communications with and among smart objects, thus

leading to the vision of ‘‘anytime, anywhere, any media, anything” communications.

In this survey paper, we analyzed the IoT architecture, Security in IoT and its challenges. We observed that it covers large area it also has some advantage and disadvantage. We also observed that still IoT is not much used in the field of agriculture. So we find its very much necessary to improve the applications of IoT in this field and educate the same to the agriculturist, this will in turn reduces the dependency on man power and which leads to increase the economy.

References

D.Giusto, A.Iera, G.Morabito, L. Atzori (Ends) (2010), the Internet of Things, Springer, ISBN: 978-1-4419-16730.

El-hajj, M. Chamoun, M. Fadlallah, A. Serhrouchni (2017), Analysis of authentication techniques in Internet of Things (IoT). In Proceedings of the 1st Cyber Security in Networking Conference (CS Net), Rio de Janeiro, Brazil, pp.1-3.

El-hajj, M. Chamoun, M. Fadlallah, A. Serhrouchni (2017), A. Taxonomy of authentication techniques in Internet of Things (IoT). In Proceedings of the 2017 IEEE 15th Student Conference on Research and Development (SCOReD), Putrajaya, Malaysia, pp. 67–71.

Atzori, L. Iera, A. Morabito (2010), The Internet of Things: A survey, Comput. Netw, 54, 2787–2805.

Harvard Business Review (2014), Internet of Things: Science Fiction or Business Fact.

Vermesan Ovidiu, Friess Peter (2013), Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, Aalborg, Denmark: River Publishers.

Santucci Gerald, The Internet of Things: Between the Revolution of the Internet and the Metamorphosis of Objects, European Commission Community Research and Development Information Service.

Mattern Friedemann, Floerkemeier Christian, From the Internet of Computers to the Internet of Things, ETH Zurich.

Lindner Tim (2015), The Supply Chain: Changing at the Speed of Technology, Connected World.

I. Mashal, O. Alsaryrah, Y. Chung, C.-Z. Yang, W.-H. Kuo, and D. P. Agrawal (2015), Choices for interaction with things on Internet and underlying issues, Ad Hoc Networks, vol. 28, pp. 68– 90.

O. Said and M. Masud (2013), towards internet of things: survey and future vision, International Journal of Computer Networks, vol. 5, no. 1, pp. 1–17.

M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du (2010), Research on the architecture of internet of things, in Proceedings of the 3rd International Conference on Advanced Computer. Theory and Engineering (ICACTE ’10), IEEE, Chengdu, China, vol. 5, pp. V5-484–V5-487.

R. Khan, S. U. Khan, R. Zaheer, and S. Khan, (2012), Future internet: the internet of things architecture, possible applications and key challenges, in Proceedings of the 10th International Conference on Frontiers of Information Technology (FIT ’12), pp. 257–260.

H. Ning and Z. Wang (2011), Future internet of things architecture: like mankind neural system or social organization framework, IEEE Communications Letters, vol.15, no.4, pp. 461–463.

G. Yang, J. Xu, W. Chen, Z. H. Qi, and H. Y. Wang (2010), Security characteristic and technology in the internet of things, Journal of Nanjing University of Posts and Telecommunications (Natural Science), vol. 30, no. 4.

C. Ding, L. J. Yang, and M. Wu (2011), Security architecture and key technologies for IoT/CPS, ZTE Technology Journal, vol. 17, no. 1.

T. Polk and S. Turner (2010). Security challenges for the internet of things, http://www.iab.org/wp-content/IAB uploads/2011/03/Turner.pdf.

Z. H. Hu (2011), the research of several key question of internet of things, Conf. on Intelligence Science and Information Engineering, pp. 362-365.

J. F. Wan, H. Suo, H. Yan, and J. Q. Liu (2011), A general test platform for cyber-physical systems: unmanned vehicle with wireless sensor network navigation, Advances in Engineering, Nanjing, China.

J. H. Shi, J. F. Wan, H. H. Yan, and H. Suo (2011), A survey of cyber-physical systems, on Wireless Communications and Signal Processing, Nanjing, China, November.