Impact of Internet of Things - A Review

Dr. B. Firdaus Begam[1], Dr. M. Sasikala[2]
Assistant Professor
Department of Computer Science
Karpagam Academy of Higher Education
PSGR Krishnammal College for Women

Abstract **- Internet of Things (IoT) has envisioned new paradigm where a network environment enabled to have interaction between machines and devices. IoT has lot of scope in wide range of industries, health care, agriculture and other application, as it is considered as future technology which can bring revolution in the fields. In this the basic concepts of IoT are discussed.**

Keywords: Internet of Things, architecture, security.

1. INTRODUCTION

The IoT environment which provides human to interact with machines, collect data, analyze and understand can be known as Internet of Everything. It can connect to various machine or devices and interact with heterogeneous technologies. Introduction of IoT has empowered objects to sense, hear, think and to analyse jobs it has to perform. It can also communicate with near by device and share information among them without human intervention. IoT is one of the revolutionary technologies expanding its scope of applications rapidly. Main advantage of IoT is that it can save time and resource utilization and reduces the work of human.[1][2]

The term Internet of Things was first coined by Kevin Ashton during 1999. Main element of IoT is Internet, which acts as heart and centre of Internet based IoT. According to S.Mandal, IoT is defined as "A network of physical objects or 'things' that can interact with each other to share information and take action." or: "The Internet of Things (IoT) is the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure." The International Telecommunication Union (ITU) has identified and released ITU annual report on Internet of Things.[4]

IoT has wide range of applications in various fields like in agriculture, forestry, health sector, transportation, traffic handling, smart cities, smart home, industry, logistic and environment as shown in figure 1. While designing IoT application for various fields some of the factors are to be taken into account like scalability, readability, topology, energy efficient, energy minimization, delay and throughput [5]. In section 2, various technologies used in IoT are discussed, section 3 and security threats are focused in section 4 and in section 5 conclusion.

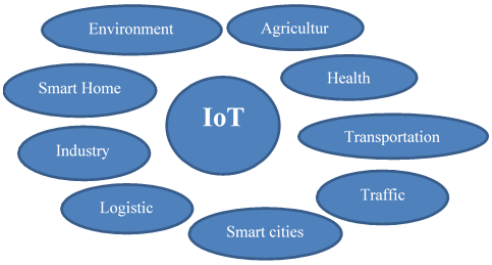

Figure 1: Applications of IoT

2. TECHNOLOGY AND PROTOCOLS USED IN IOT

There are many technologies are and protocols are used based on the application of field and requirements. Some of them are discussed below:

Radio Frequency Identification (RFID)

It is one of the most reliable and fastest method used to detect the objects, control and keep track of the object electronically. Components of RFID are RFID tags, reader and application system to which it is used. RFID tags are connected to various objects which has to be detected and tracked. They are also known as transponders. Transmitter of RFID is reader which contains interface module to handle radio frequency and control unit. Activation functions of RFID tags are done by reader to exchange information between tag and application system. Application system is where the data are collected through tags and transmitter for data processing.

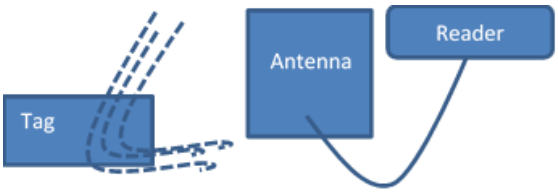

Figure 1: RFID

Machine-to-Machine Communication(M2M)

M2M is a communication technology used in IoT application to communicated with many devices without human intervention or process of communication. It can be considered as nerve system of IoT technology. Components of M2M communications are devices. Device domain, gateway, communication network and application system. It provides interconnection and interoperability between machines.

Figure 3: Machine-to-Machine Communication(M2M)

Wireless Sensor Network (WSN)

WSN consist of large number of sensor nodes which can self-organize and can develop a network in free space. The four main components of sensor networks are localized or distributed sensors, network which is interconnected, central clustering point for information and application system. Bluetooth, WiFi, Near Field Communication (NFC), Zigbee are some of the technologies used in IoT.

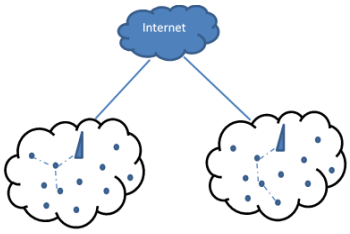

Figure 4: *Wireless Sensor Network (WSN)*

3. ARCHITECTURE OF IOT

As IoT is heterogenous there is no specific architecture defined, as it changes based on requirement and application system. Architecture of IoT are designed in a way that holds the capacity of connecting billions of heterogenous applications or objects over internet[5].

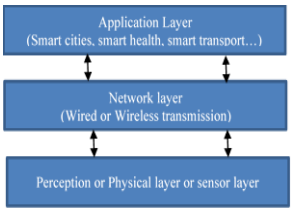

Figure 5: Three Layer Architecture

Three Layer Architecture and Five Layer Architecture

The basic structure of IoT consist of three layer, i) perception layer ii) network layer and iii) application layer. Five-layer architecture includes processing and application layer. Perception layer consist of sensor which collects information by sensing objects in the environment. Sensed information based on defined parameters are transported to processing layer through transport layer through various technologies like Bluetooth, RFID, NFC, 3G and LAN. The processing layer is also middleware layer. It is where the huge data collected from perception layer are analysed and processed. The Business layer manages whole IoT application system and user privacy[7].

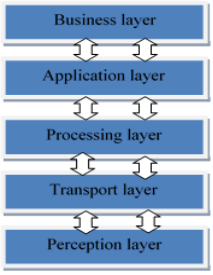

Figure 6: Five Layer Architecture

Cloud and Fog architecture

The data processing performed in central system is called Cloud architecture. It provides greater role in flexibility and scalability. Here the cloud resides in centre, controls and process the information collected from various different objects in environment. Cloud computing provides infrastructure, platform and software services to collect, store, analyze and visualize the processing result as per user requirements.[8][9]

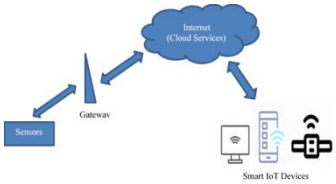

Figure 7: IoT-Cloud Computing Architecture

Fog architecture is similar to cloud architecture the difference is that here sensor and gateway also get involved in data processing and analysis. It is coined by CISCO and it is also known as edge computing architecture. The physical or perception layer collects the data and sends to transport layer.[8][9]

Before the data reaches to transport layer the

i) information are monitored for its power, resource consumption and services,
ii) pre-processing techniques are preformed over sensor data by filtering, reducing dimension and analysing,

iii) it provides sensor data to be stored temporally for performing data validation, data replication, analysing data and distribution,

iv) provides data security while transferring data from physical layer to transport layer by encrypting and decrypting data.

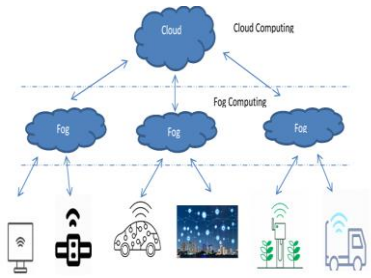

Figure 7: IoT-FogComputing Architecture

4. SECURITY ISSUES AND CHALLENGES IN IOT[7]

Device identity: Devices connected in IoT model has to be assigned with unique name.

Firmware issue:Installing and updating of security patches for the IoT devices is a challenging task.

Authentication and authorization: IoT devices have to be connected with internet all the time and the data handled by them may be more sensitive and confidential. It needs to be authenticated and authorization to be given before transferring or receiving the data.

Data privacy and integrity: It very challenging task as the person has to be authorized to access the user's personal data and to discard the data which is of no need.

Human factors: Mishandling of IoT devices by user are the challenging task.

Interoperability issue: Interoperability issues arise as when IoT devices of different technology (heterogenous nature) used for IoT development.

Quality of Service (QoS): The QoS has to measure on IoT devices, architecture and the service it provides based on metrics, cost, scalability, availability, security and consumption of energy.

CONCLUSION

Recent development of IoT has gain attention over world and it is showing grater impact when combine with cloud/fog technology. However, the security plays a vital role for data handling, various research is going on to overcome security issues. In this paper basic architecture and security issues are discussed.

REFERENCE

[1] S Mandal, "Internet of Things (part 1)," Introduction, [Online], source: http://www.csharpcorner.com/uploadfile/f88748/internet-of-things-iot-anintroduction/, 2015

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," Computer Networks, vol. 38, no. 4, pp. 393–422, 2002.

[3] Kramp T., van Kranenburg R., Lange S. (2013) Introduction to the Internet of Things. In: Bassi A. et al. (eds) Enabling Things to Talk. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-40403-0_1

[4] Shanzhi Chen, Senior Member, IEEE, Hui Xu, Dake Liu, Senior Member, IEEE, Bo Hu, and Hucheng Wang, A Vision of IoT: Applications, Challenges, and Opportunities with China Perspective, IEEE Internet Of Things Journal, Vol. 1, No. 4, August 2014.

[5] Harika Devi Kotha1, V Mnssvkr Gupta, International Journal of Engineering & Technology, 7 (2.7) (2018) 891-896

[6] Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao, A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications, IEEE INTERNET OF THINGS JOURNAL, VOL. 4, NO. 5, OCTOBER 2017

[7] F. Chen, T. Xiang, X. Fu, and W. Yu, "User differentiated verifiable file search on the cloud," IEEE Trans. Services Comput., to be published, doi: 10.1109/TSC.2016.2589245

[8] Z. Chen et al., "A cloud computing based network monitoring and threat detection system for critical infrastructures," Big Data Res., vol. 3, pp. 10–23, Apr. 2016