GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

IOT, ITS PROTOCOLS & CHALLENGES

Anshul
Asst. Prof. of Computer Science and Engineering, Ganga Technical Campus, Soldha

ABSTRACT

IoT i.e. Internet of things is based on networking of thing. It is a technology that allows communication between objects, machines and everything together with peoples. In this every objects have network connectivity which allow them to send and receive data. The most important thing is connectivity. So IoT use various types of protocols from cell phone connectivity to wide area connectivity like satellite, Bluetooth, WiFi and many more. The world will become smart by the use of this technology. It has many applications like smart cities, smart highways, smart parking, and smart lightning etc. Apart from these applications, IoT has some challenges also. In this paper we review a concept of IoT, its communication protocols and some challenges that that are faced by the IoT developers.

Keywords: *IoT, WiFi, Zigbee, LoRa, GSM.*

I. INTRODUCTION

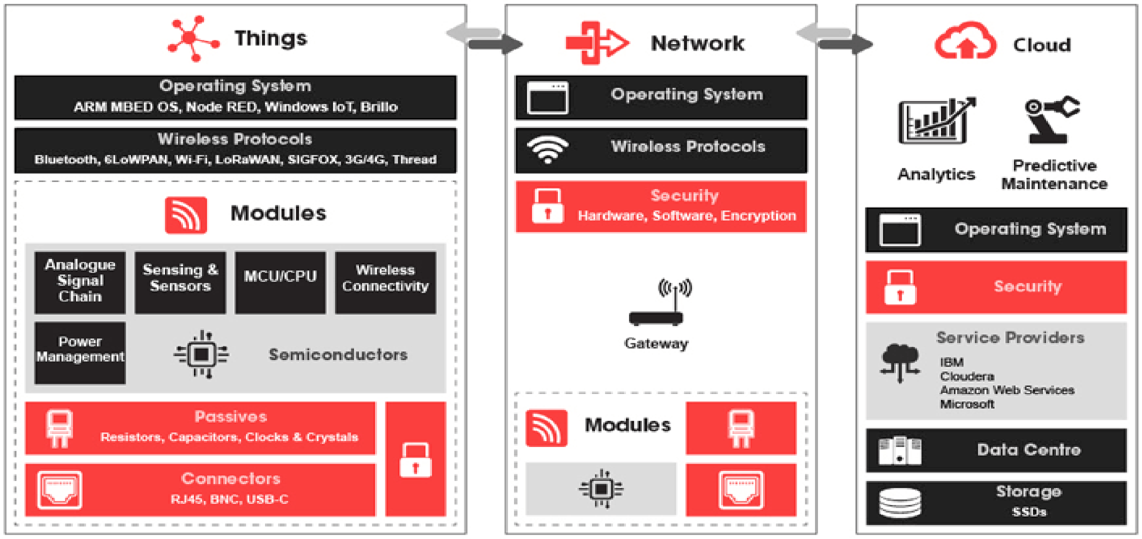
The Internet of Things is made up of two parts i.e. Internet and Things. Internet is for connectivity and things means objects or devices. So, IoT is a network of connected devices which is used to collect and exchange the information. In simple words, things that sense and collect data and send it to the internet. [1] The devices have range from home automation which can include lighting, heating, air conditioning, media, security systems too many more. These can be implemented with various software and electronic devices. All these devices fall into three categories:

a) Devices that collect information and then send it.
b) Devices that receive information and then act on it.
c) Devices that do both things. [2]

The System operates on three levels:

a) Hardware
b) Infrastructure
c) Apps. [3]

IoT High-level Architecture



Source: ie.rs-online.com

II. PROTOCOLS

50 to 100 billion things will be connected by internet by 2020. [4] IOT communicates and transfer different types of information from one machine to another. [5] This depends on standardization, which provides interoperability, compatibility, reliability, and effective operations on a global scale. [6]Today more than 60 companies for leading technology, in communications and energy, working with standards, such as IETF, IEEE and ITU to specify new IP based technologies for the Internet of Things. [7] Some Protocols are:

- **ZigBee** = Low range, meshed net, low speed.
- **Wi-Fi** = Medium range, pear to pear, high speed.
- **GSM/GPRS** = World wide range, pear to pear, medium speed.
- **LTE** = World wide range, pear to pear, high speed.
- **Bluetooth** = Medium range, pear to pear, high speed.

III. CHALLENGES

Despite the benefits of IoT, it has some challenges also which are as follows:

1. **Security:** The greatest threat to IoT is Security. Acc. to the Global Risk Report 2018, the cyber-attacks is the weakness of Internet. The Annual Economic cost of cybercrime is estimated to be around 1 trillion US dollars, which supersedes costs of natural disasters such as Hurricane Sandy and Katrina. [8]
2. **Privacy:** It is another issue for users with IoT. Privacy is the personal thing and this simple fact gets complex because IoT is the network of connected devices and data is shared between people, companies, government and ecosystems. All devices highly depend on trust relationships. Connecting more devices, increases the threat which in turn increases the security risk. It is difficult to build trust with IoT without these privacy settings. [9] According to the recent study of Glasgow University, consumers are highly unsatisfied with the lack of privacy the IoT allows them.
3. **Internet Walls:** The risk of losing important data via hacks is a dangerous not just for corporations, but also for nations. Acc. to the World Economic Forum, this hacking limits the activity of the IoT to particular regions. This become the barrier and prevents the exchange of data. This is also serving as an obstacle to technological advancement by substantially slowing it down. [10]
4. **Cloud attacks:** The next potential threat to IoT is cloud network because it has the biggest data stocks to run the IoT. According to recent study, the annual economic cost of cybercrime was estimated around $1

trillion in 2017, which is a multiple of 2017's record-year aggregate cost of almost $300 billion from natural disasters. the World Economic Forum report quotes a study that put forward the takedown of just one cloud provider could cause $50 billion to $120 billion of financial damage.[10]

5. **Understanding IoT:** Rapid growth in technology has resulted in a limited understanding of the IoT. For consumers to make use of the internet and all that the IoT has to offer, it is essential to work upon their awareness of the changes taking place within IoT to make it more efficient. Not only will the comprehension empower them, it will prepare them mentally and they will possibly be able to find solutions on how to take caution from any of the mentioned problems.[10]
6. **Lack of Confidence:** According to the latest research report shared by the State of IoT Security, which was released at the end of October, showed that:

a) 96 percent of companies and 90 percent of consumers believe that IoT IoT should be more secure.

b) 54 percent of consumers possess an average of four IoT devices, but then again only 14 percent consider that they are familiar with IoT device security.

c) 65 percent of consumers are petrified about a hacker monitoring their IoT device, whereas around 60 percent are fretful of their personal or professional data being leaked.[11]

IV. CONCLUSION

IoT is the network of interconnected devices. It has many protocols or communication technologies such as WiFi, Zigbee, LoRa, GSM, and Bluetooth. It's quite evident that organizations all over the world are boarding onto IoT and in addition to better meet the demands of their customers and citizens. With all these advantages of IoT, there might be risks to these ventures, but, nonetheless, if coped appropriately, organizations could be further assured and the road to IoT victory and efficiency should be impartially smooth.

REFERENCES

1. *https://www.quora.com/What-is-the-simple-meaning-of-Internet-of-Things*
2. *https://www.iotforall.com/what-is-iot-simple-explanation/*
3. *https://r-stylelab.com/company/blog/iot/internet-of-things-how-much-does-it-cost-to-build-iot-solution*
4. *Jayavardhana Gubbia, Rajkumar Buyyab, Slaven Marusic, Marimuthu Palaniswami. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems 29 (2013) 1645-1660.*
5. *https://dupress.deloitte.com/dup-us-en/focus/internet-of-things/iot-commercial-real-estate-intelligent-building-systems.html*
6. *Grandinetti, Lucio. Pervasive Cloud Computing Technologies: Future Outlooks and*
7. *Interdisciplinary Perspectives: Future Outlooks and Interdisciplinary Perspectives. IGI*
8. *Global, 2013.*
9. *http://standardsinsight.com/iot/iotworkshop*
10. *https://dzone.com/articles/problems-with-internet-of-things-you-need-to-know*
11. *https://www.iotforall.com/protecting-privacy-in-iot/*
12. *https://dzone.com/articles/problems-with-internet-of-things-you-need-to-know*
13. *https://www.cmswire.com/cms/internet-of-things/7-big-problems-with-the-internet-of-things-024571.php*