The Internet of Things Architecture, Feasible Applications and Fundamental challenges

Muhammad Saad
Computer Engineering Department
Sir Syed University, Pakistan

Muhammad Shahid
Computer Engineering Department
Sir Syed University, Pakistan

ABSTRACT

The Internet has evolved in ways that we could never have imagined. In the beginning, advancements occurred slowly. Today, innovation and communication are happening at a remarkable rate. Now days, Internet has become the most important aspect of our life. Starting from desktop late 90s when one use to go to the device to resolve the problem to the era of smart devices early 20s when everybody carry the devices in its pocket to the new emerging era of internet of everything where we are going to connect each and every non connected device present on the planet. To make this dream come true, we have to face a lot of challenges. In this paper I have given the brief description about the internet of things, elaborate its complicated architecture, highlighted few feasible application and alert about the fundamental issues which we are going to face while deploying internet of things in to live environment.

General Terms

Prototype, Security, Encryption, Algorithm, Threats.

Keywords

Cloud computing, Radio frequency identification (RFID), Internet of Things (IOT), Internet Protocol (IP).

1. INTRODUCTION

In order to understand the working of internet of thing we have to first understand how things and internet work together. According to the survey only 34% people are using internet service and only 1% things present in the world is connected to the internet. 99% things on the earth are still unconnected.

Alarm clocks, micro wave oven, lightning system, toaster, washing machine, vacuum cleaner etc. are still not the part of internet. In order to connect them we have to make use of complex circuits which includes smart sensors and controllers as well as Radio frequency identification (RFID) tags to make communication possible over the wireless medium as internet of things mainly use wireless medium to connect the things how far they are placed. These sensors are programmed with the high level prototype that supports all specific devices. As the numbers of devices on the internet are increasing their data is also increasing. To handle that data we are making use of cloud computing technology. Due to this all the data is stored in to the secured datacenters which can be easily accessible when required. As the quantity of data increases the problem to process and analyze the data also increases, which was resolved by making use of big data technology. It allows us to process and analyze the big data easily.

Finally, the main entity which is commonly known as the backbone of internet of things and which makes communication possible over the internet is the use of ipv6 concept. It is truly said that through the use of ipv6 we can easily assign IPs to other planet present in this universe as well.

2. THE EVOLUTION OF INTERNET

With the evolution of time, the use of internet becomes common and with the development of many advanced devices such as smart phones, tablets etc. the importance of internet went to its peak as shown in Fig 1. Starting from desktop late 90s when one use to go to the device to resolve the problem to the era of smart devices early 20s when everybody carry the devices in its pocket to the new emerging era of internet of everything where we are going to connect each and every non connected device present on the planet [1].

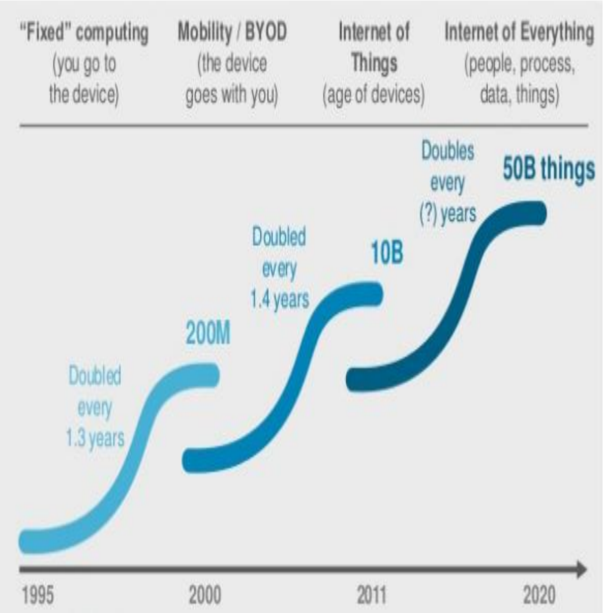

Fig. 1 Internet of Things Prediction Graph

At the starting we make use of ipv4 protocol to full fill our devices IP requirement but with the increasing growth of devices it is impossible to fulfill the requirement of bulk of IPs and in order to achieve this task we make use of the new ipv6 protocol through which we can easily assign IP to make it connected to the world [2]. The main difference between both IP version is that in IPv4 we can only get 32 bit of IPs range whereas in ipv6 we can get approximately 3.4x10^38 IP addresses which is a very big number.

3. GENERIC ARCHITECTURE

Every network architecture follows the TCP/IP layers standard as its base. Internet of things is commonly divided in to five layers which include physical layer, network layer, middle ware layer, application layer and business layer as shown in Fig 2. All layers are interconnected with each other in a particular sequence. All these layers are briefly described below:

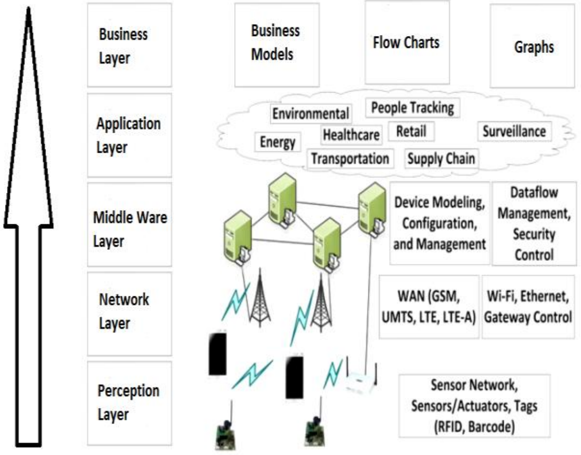
Business Layer
Application Layer
Middle Ware Layer
Network Layer
Perception Layer
Business Models
Flow Charts
Graphs
Environmental
People Tracking
Energy
Healthcare
Retail
Surveillance
Transportation
Supply Chain
Device Modeling, Configuration, and Management
Dataflow Management, Security Control
WAN (GSM, UMTS, LTE, LTE-A)
Wi-Fi, Ethernet, Gateway Control
Sensor Network, Sensors/Actuators, Tags (RFID, Barcode)

Fig.2 Internet of Things Architecture Layers

3.1 Physical Layer

In this layer all the devices are connected with each other through a particular medium to transfer the data to the next layer devices. Medium can be wired or wireless depending upon the situation but mostly wireless medium is used in Internet of things concept such as Radio frequency identification (RFID) tags, sensors and controllers as shown in Fig 3. All these tiny sensors and controller are embedded in to the device circuitry to make it smart and to take necessary decision when required. This layer connects to the next layer that is network layer.

3.2 Network Layer

To transfer the collected data from one hop to another hop we use network layer [3]. This layer make use of the latest advanced technologies such as Wi-Fi access points, RFID, Bluetooth, 3G, 4G etc. that make communication possible and to transfer the data securely. This layer connects to the next layer that is Middle ware layer.

3.3 Middle Ware Layer

Then, we go into the Middle Ware Layer. And in here, device modeling configuring and management is a major focus. Dataflow management and security control needs to be provided at the middle ware layer. This layer connects to the next layer that is Application layer.

3.4 Application Layer

In this layer we have energy, environment, healthcare, transportation, supply chain, smart farming, retail, people tracking, surveillance, and many, many more endless applications. This layer finally connects to the next layer that is Business layer.

3.5 Business Layer

In this layer all the data collected from different devices are gathered in a secure location that is data centers. After that deep analysis of each device data is done here according to different parameters and case testing to get the required results. This analysis of data would be in the form of Gantt chart, Pie chart or any other performance measuring tools. This layer help to improve the quality of service of a particular organization that will help him to achieve its goals successfully in the future endeavors.

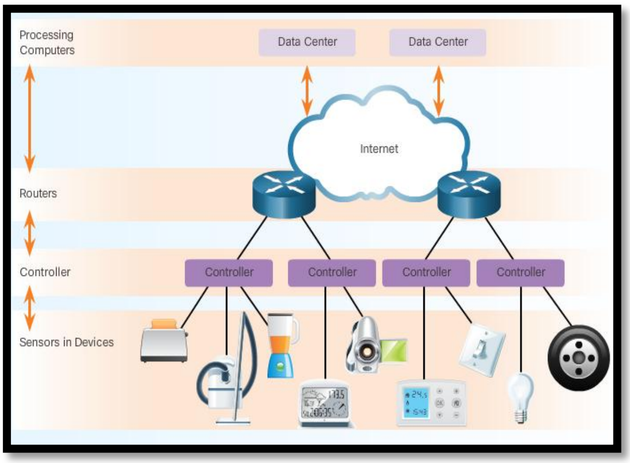

Fig.3 Controllers and Sensors

4. FEASIBLE FUTURE APPLICATIONS

Internet of things examples extend from smart connected homes to wearable's to healthcare. It is not wrong to suggest that IOT is now becoming part of every aspect of our lives. Below are some of the examples listed.

4.1 Smart Air ports

Airports can be more smartly operated if some changes in future are made. The ticketing system can be made more efficient by providing an app that contains all the journey transaction along with the arrival and departure timing notification. Through IOT we can also monitor the flow and volume of people in the airport. We can also improve the luggage delivery system by placing trackers on them such as RFID tag or make use of smart sensors to make sure that luggage should be delivered to the right person on the right time [4]. By making of this technology we can improve the whole operational structure of the airport.

4.2 Smart Health Tracking System

In this busy and stressful life, people have no time to pay attention to their health which cause disturbance in their body hormones which lead them to some serious disease [5]. This problem can be overcome by the use of this latest technology that is IOT by inventing some human friendly sensors that can be placed on different parts of our body with the ability to detect the behavior of all the internal parts of our body such as heart, kidney and stomach etc. and send a daily or weekly report to the concerned family doctor so that any possible disease can be cured before it cause damage.

4.3 Smart houses

From the kitchen related accessories which include refrigerator, microwave oven, smoke detector, toaster, coffee maker etc. [6] to the normal rooms related accessories such as Air Conditioner, Door lock and garage doors, trash cans, washers, dryers, lighting system etc. all can be made more efficient and smart by implementing the use of new technology that is internet of things.

4.4 Smart farming system

The secret behind every successful and growing country is due to its agriculture performance [7]. The more you grow the more you export and the more you earn. By making use of intelligent sensors that alert all the weather related reports to the farmers, tell the nature of their soil according to which they should use fertilizer and most important thing alerting them against the big disasters such as dam water overflow etc. By implementing all these things we can easily make our economy strong.

4.5 Smart Car

A lot of work has been done on this concept but it hasn't got common. Due to internet of things all the cars can talk to other cars in this car. We should design such prototypes which can be easily adopted by all the different vendors' cars. By doing this we can easily decrease the ratio of accidents which occurs normally on daily in the whole world.

5. FUNDAMENTAL CHALLENGES

While the deployment of this new technology we have to face a lot of hurdles and problems. Some of them are discussed below:

5.1 Power Deficiency

We are making use of thousands of small smart sensors and controllers to control all the unconnected things and to make them alive and in working condition a lot of power is required. In order to overcome this deficiency, we have to make use of solar panels and solar winds energy systems [8]. By using this green energy technology we can easily achieve our future goals.

5.2 Lack of Security

Security is one of the major issues while deploying IOT. If a patient health report is hacked by the hacker this would cause a great security breach and will cause many people to do suicide [9]. This problem can be overcome by deploying cyber threat techniques in our network to avoid this type of security breach [10].

5.3 Data confidentiality and encryption

As the numbers of device are becoming part of the internet, the size of the data is also getting big day by day. To avoid any leakage or damage to this data, a company should adopt the efficient cloud storage facilities and should do penetration testing to their network. In this way, we can easily protect data of millions of people.

5.4 Software Updates

The software's and prototype which the developer has embedded in the circuitry, to make sensors and controllers work accordingly should be updated on time when required.

5.5 Data confidentiality and encryption

As data becomes the currency of the future, vendors must finance in meeting critical end user data storage, management, analytics and ownership requirements [11]. The IOT service decides who can see the data, thus, it is necessary to protect the data from externals.

6. MOTIVATION

As Internet of things is a very popular topic now days and many well-known technical companies such as Cisco, Juniper, and Microsoft etc. are working on this technology trying to embed this prototype in the live environment. All these things motivate me to keep my research on this topic and to give some precious and useful suggestions regarding the deployment of this technology.

7. PROPOSED PLAN

While writing this research paper I proposed many ideas on different steps like if we talk about the security lacking, I proposed to embed cyber security techniques in our network such as make use of new security devices such as (Antivirus, Firewalls etc.), make use of effective packet capture appliances e.g. (packet shark) which has the ability to capture packet at any point of the network. It is equivalent to security camera which has no blind spot. Packet capture appliances provide detail report about what was taken in/out, when and how, perform 24/7 surveillance of the network which includes recording and time stamping all network activities, in order to identify any suspicious activity in the network. By doing this we can easily overcome the unauthorized access and malware attacks. Basically cyber security is a reactionary and by implementing all these techniques it allows the administrator to detect the hacker quickly and to react effectively to protect the organization valuable data. Penetration testing techniques is one of the important method through which we can easily get aware regarding any back doors in our network. Besides this I have also suggested the plan regarding the lacking of power efficiency issue. To keep our device in a workable condition that contains thousands of small sensors and controller, a lot of power is required. In order to overcome this deficiency, we have to make use of solar panels and solar winds energy systems. By using this green energy technology we can easily achieve our future goals. I have also proposed the plan regarding the software update which the developer has embedded in the circuitry, to make sensors and controllers work accordingly should be updated on time when required. This can be made possible by using different advance algorithm at the initial phase. In short, this technology is in development phase and besides all these known hurdles we still have to face a lot of unseen obstacles at the live environment.

8. CONCLUSION

In this paper I have given the brief description about the internet of things, elaborate its complicated architecture, highlighted few feasible application and alert about the fundamental issues which we are going to face while deploying internet of things in to real environment. Moreover I have suggested the proposed plan to how to get rid of those highlighted issues. While adopting all these physical and logical techniques we can easily avail the benefits of internet of things in our daily life.

9. REFERENCES

[1] V. G. Cerf, "On the evolution of Internet technologies," in *Proceedings of the IEEE*, vol. 92, no. 9, pp.1360-1370

[2] J. Govil, J. Govil, N. Kaur and H. Kaur, "An examination of IPv4 and IPv6 networks: Constraints and various transition mechanisms," *IEEE SoutheastCon 2008*, Huntsville, AL, 2008, pp. 178-185.

[3] R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, London, 2015, pp. 336-341.

[4] A. P. Renold and R. J. Rani, "An internet based RFID library management system," *2013 IEEE Conference on Information & Communication Technologies*, JeJu Island, 2013, pp. 932-936.

[5] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain and K. S. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," in *IEEE Access*, vol. 3, pp. 678-708, 2015.

[6] M. Darianian and M. P. Michael, "Smart Home Mobile RFID-Based Internet-of-Things Systems and Services," *2008 International Conference on Advanced Computer Theory and Engineering*, Phuket, 2008, pp. 116-120.

[7] Ji-chun Zhao, Jun-feng Zhang, Yu Feng and Jian-xin Guo, "The study and application of the IOT technology in agriculture," *2010 3rd International Conference on Computer Science and Information Technology*, Chengdu, 2010, pp. 462-465.

[8] S. F. Abedin, M. G. R. Alam, R. Haw and C. S. Hong, "A system model for energy efficient green-IoT network," *2015 International Conference on Information Networking (ICOIN)*, Cambodia, 2015, pp. 177-182.

[9] Muhammad Saad. Fog Computing and Its Role in the Internet of Things: Concept, Security and Privacy Issues. International Journal of Computer Applications 180(32):7-9, April 2018.

[10] Ali, Bako and Awad, Ali Ismail, "Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes," Sensors 18(3), 2018.

[11] H. Suo, J. Wan, C. Zou and J. Liu, "Security in the Internet of Things: A Review," 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, 2012, pp. 648-651.

10.