

Challenges in Internet of Things Applications

Priyankar R. Tiwari

M.E. Scholar, Department of Computer Engineering,
Thakur College of Engineering & Technology,
Mumbai, India
priyankartiwari@gmail.com

Loukik S. Salvi

M.E. Scholar, Department of Computer Engineering,
Thakur College of Engineering & Technology,
Mumbai, India
Loukiksalvi96@gmail.com

Abstract— IoT (Internet of Things) is a system where objects are embedded with sensor technology to interact with each other over a wireless communication medium to generate, exchange and transfer data without human interaction. Now Internet of Things(IoT) is getting so much popular than any other trending topic. Up to our best knowledge, it is the first study about vulnerabilities in the application of the Internet of Things. IoT is also getting industrialized using sensors in a simple work also for sake of ease of working and computation but no one thinks about its vulnerabilities and drawback which can affect in future and may result in a leak of private details breaking privacy of the whole world. In this paper, we will talk about all these vulnerabilities and drawbacks of the Internet of Things with a lot of examples.

Keywords-Issues, Challenges, Vulnerabilities, Internet of Things, IoT, Application, Drawback, Security

I. INTRODUCTION

IoT (Internet of Things) is a system where objects are embedded with sensor technology to interact with each other over a wireless communication medium to generate, exchange and transfer data without human interaction. IoT is getting involved in our day to day life by with machine-readable or radio frequency identification tag or wireless operating devices. These sensors may couple with the devices to collect the data about the condition of the objects that we use every day and those presents around them. The time is not far that you are out of town and your tube light at home contact you to tell you that you forgot it to turn off and turn it off by itself. Your fridge at home reminds you to get the milk from the market. This isn't just a fantasy but soon to be a reality due to the amazing possibilities of the Internet of Things (IoT).

The first time the term —Internet of Things: the word was used by Kevin Ashton in a presentation during 1998. [2]. He has mentioned —The Internet of Things has the potential to change the world, just as the Internet did maybe even more so. Later during 2001, MIT AutoID Lab center presented their view on IoT.

With the help of the communication technologies such as wireless sensor networks (WSN) and Radio frequency identification (RFID), sharing of information takes place. So, in general we can say IoT allows people and things to be connected Anytime, Anyplace, with anything and anyone using any network and any service as shown in figure 1.

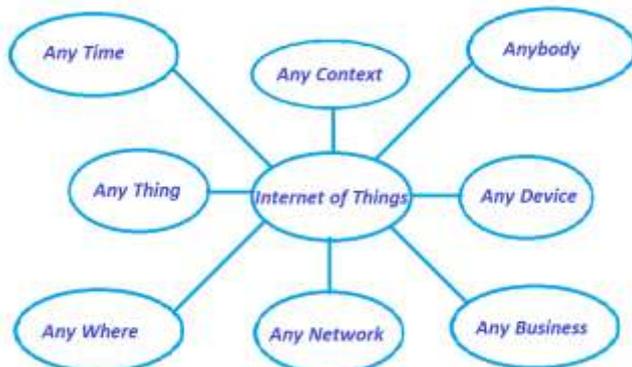


Figure 1: Introduction of IoT

II. ARCHITECTURE

Stage 1 of an IoT architecture consists of your networked things, typically wireless sensors and actuators. Stage 2 includes sensor data transmission systems and analog-to-digital data conversion. In Stage 2, edge IT systems perform preprocessing of the data before it moves on to the data center or cloud. In Stage 3, the data is analyzed, managed, and stored on traditional back-end data center systems. Finally, in stage 4, all the three stage is applied to the application. Clearly, the sensor/actuator state is the province of operations technology (OT) professionals. So is Stage 2, Stage 3 are typically controlled by IT, although the location of edge IT processing may be at a remote site or nearer to the data center.

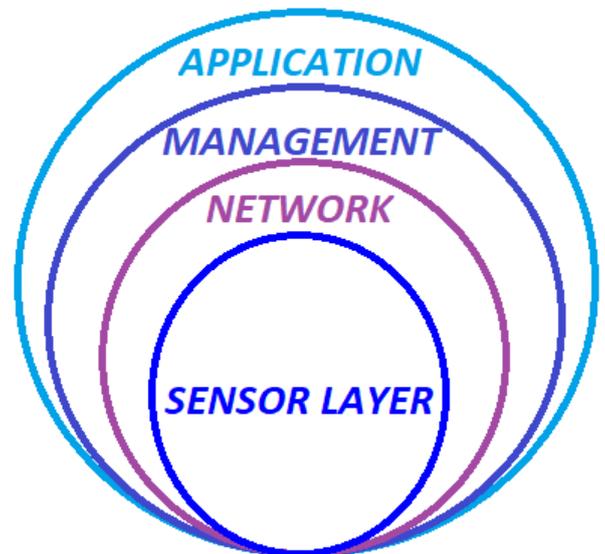


Figure 2: Architecture of IoT

III. APPLICATIONS

IoT have a lot of application in daily life. It can start from wake up in morning to do the daily routine till the time you go to the bed. Following are some areas where IoT can be used to leverage the day to day life.

Smart Clock

Smart clock can be the best example of IoT. The clock alarm when rings up in morning to wake you up in morning and you woke up to switch it off, it sends a notification to geyser to warm water of the temperature you want. At the same time it notifies Coffee machine to brew coffee while you get a refresh.

Smart Fridge

Smart Fridge is the fridge that orders milk automatically when you run out of the milk. It sends a reminder on your smartphone to carry the vegetable and fruits. It automatically detects the vegetable or fruit which is not usable or getting useless.

Air Quality Monitoring

By embedding sensors which collects context information such as the amount of carbon monoxide (CO), nitrogen dioxide (NO₂) in the air, sound levels, temperature, humidity levels in the environment. This provides continuous information about the context, which helps to take the precaution if it exceeds the normal level.

Natural Disaster Monitoring

Natural disasters such as an earthquake, landslides, forest fire, volcanoes, flood, etc. can be predicted by using wireless detection sensors. These detections intimate the respective authorities to take the precautions before the disaster occurs.

Supply-chains

Internet of Things monitors every stage of the supply chain from purchasing of raw materials from the suppliers by the manufactures, production, distribution, storage, product sales and after-sales services. This will help to maintain the stock required for continuous sale, which in turn results in customer satisfaction and increased sales. According to Cisco's economic analysis, IoT will generate \$1.9 trillion from the supply chain and logistics over the next decade. By using this we can also diagnose if the machines require repair and maintenance.

Food sustainability

Packed Food that we eat has to go through various stages of food cycle such as production, harvesting, transportation, and distribution. Sensors are used to detect context like temperature, humidity, light, heat etc. which precisely notifies the variation and intimates the concerned persons to prevent the food from spoiling.

Health tracking

The IoT is used in healthcare domain to improve the quality of human life by assisting basic tasks that humans must perform through the application. Sensors can be placed on health monitoring equipment used by patients. The information collected by these sensors is made available on the Internet to doctors, family members, and other interested parties in order to improve treatment and responsiveness. Additionally, IoT devices can be used to monitor a patient's current medicines and evaluate the risk of new medications in terms of allergic reactions and adverse interactions. With the use of sensors and the technology stated above, we can track the person's body temperature, heartbeat rate, blood pressure, etc. In case of emergency, the individual and their personal doctor will be notified of all the data collected by the sensors. This system will be very useful to senior citizens and disabled people who live independently

IV. CHALLENGES

All the applications of this technology culminate in increased comfort, convenience, and better management, thereby improving the quality of life, but as it is rightly said that a coin has two sides. Similarly, it also has some challenges.

A. Compatibility

As the devices from a different manufacturer are used to be interconnected, the issue of compatibility of tagging and monitoring is increased. Although this challenge can be solved if all the manufacturer agrees to a common standard and an international standard is set up for the equipment to be used. Today, we have Bluetooth-enabled devices and compatibility problems exist even in this technology! Compatibility issues may result in people buying appliances from a certain manufacturer, leading to its monopoly in the market.

B. Complexity

IoT is a combination of diverse devices and complex network. There are a lot of chances of failure with a complex system. Any failure or bug in software or hardware will have a serious consequence. For example, a bug in printer ink ordering system may order multiple ink tank for the printer due to the bug or hardware failure.

C. Lesser Employment of Menial Staff[3]

The unskilled workers and helpers may end up losing their jobs in the effect of automation of daily activities. This can lead to unemployment issues in the society. This is a problem with the advent of any technology and can be overcome with education

D. Technology Takes Control of Life

Our lives will be increasingly controlled by technology and will be dependent on it. The younger generation is already addicted to technology for every little thing. We have to decide how much of our daily lives are we willing to mechanize and be controlled by technology.

E. Privacy

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.

F. Security

Security is a crucial issue on the Internet, and it is probably the most significant challenge for the IoT. When you increase the number of connected devices, the number of opportunities to exploit vulnerabilities through poorly designed devices can expose user's data to theft, especially when the data streams are left with inadequate protection. In certain cases, it may even harm the safety and health of people. The Zika virus is not the only threat out there! There are a number of IoT deployments that also have collections of nearly identical or identical devices. This magnifies the impact of any one security vulnerability by the number of devices that all have similar characteristics. To deal with all

these unique challenges, there is a need for a collaborative approach to security. A lot of users are ultimately going to have to compare the cost against the security, which is related to the mass scale deployment of the Internet of Things devices.

V. CONCLUSION

If IoT devices are deployed without proper forethought, there will be plenty of too-late afterthoughts when they cause unintended havoc. Having a scalable IoT network that can connect servers and devices is critical for any large-scale IoT apps. It is vital to not only consider the above challenges but to solve them. As long as these issues are addressed before

setting up the infrastructure, everything should be fine. If they aren't get ready for a rough ride.

REFERENCES

- [1] Jinesh Ahamed; Amala V. Rajan, "Internet of Things (IoT): Application systems and security vulnerabilities" IEEE Xplore 10.1109/ICEDSA.2016.7818534
- [2] Jayavardhana Gubbia, Rajkumar Buyyab, Slaven Marusic a, Marimuthu Palaniswami, — Internet of Things (IoT): A vision, architectural elements, and future directions", Future Generation Computer Systems, Elsevier,2013.
- [3] <https://www.buzzle.com/articles/pros-and-cons-of-internet-of-things-iot.htm>