IoT and its Issues

Yanish Sahu
Ajeenkya D Y Patil University, Pune

Lalit Kumar
Ajeenkya D Y Patil University, Pune

Shabnam Sharma
iNurture Education Solutions, Bangalore

ABSTRACT
Moving into the future world, life will be getting more easier and easier. Everything will be connected like interconnected smart homes, smart hospitals, smart cities, smart wearables, smart supply chain, and a variety of other smart environments. These systems use a technology known as Internet of things or also known as internet of everything. Nowadays with increased need for surveillance, monitoring and data collection IoT has become more important. This paper describes about internet of things and its issues. It also discusses the hardware required by a basic IoT system, privacy concerns, security issues and data handling issues. It also includes problems faced due to the hardware.

Keywords
Internet of Things, RFID

1. INTRODUCTION
The ongoing decade has witnessed a lot of change/modification of the devices and the increase in popularity of the internet a lot of internet-capable devices have went through a revolution. While the internet is global computer network consisting of interconnected devices using standardized communication protocols, IoT is interconnected ecosystem of physically addressable/smart objects which have multiple capabilities like sensing, observation, automation using internet as their medium.

In a 1999 article for the RFID Journal Ashton wrote: If people had computers that knew everything there was to know about things—using data they gathered without any help from us -- one would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best. Every people need to empower computers with their own means of gathering information, so people can see, hear and smell the world for themselves, in all its random glory. RFID and sensor technology enable computers to observe, identify and understand the world—without the limitations of human-entered data.

This innovative idea had a long way to go with the technology and hardware available at that time. With the betterment of Wi-Fi abilities and introduction of IPv6 which allows millions of devices at a time, IoT is more than just a vision and is getting popular day by day.

In simple words, IoT is a system in which all physical devices with or without sensors but are able to connect to a network are connected together in a network maybe for monitoring purpose or to automate things.

Hardware requirements for a system may vary according to the needs. But there are 5 basic components of an IoT system:

- **Power source and power management:** IoT is interconnection of autonomous device to the internet and every device need a power for operate. You must be understanding which kind of power source need to IoT device and how to manage it.
- **Sensor/actuator:** If you collect any data then how to know the data is accurate or not? Sensor and actuator can be used to find accuracy of data. People can say sensor is source of IoT data. Sensor is converts one form of energy to another.
- **Processor and memory storage:** Processor are most necessary for configuration of software, for right balance of performance and power, processor is very necessary. Memory storage is also very important for IoT applications. If someone collect data by IoT then whom need to store that data and manage that data. Hence memory storage is most in IoT applications.
- **Wireless communication:** In IoT, wireless communication is very useful. It is a standard way to connect two or more system to each other. Wi-Fi, Wi-Fi direct, Zigbee, Z Wave, Bluetooth, RF, 6LowPAN, GPRS/LTE, and NFC are protocols for wireless communication.
- **UI/UX:** There are a lot of IoT device that is controlled by smart phone and web app, due to only help of user interface. If you get any visibility then and then you can control that. User interface (UI) provide screen and the help of that screen people can control any IoT device.

2. LITERATURE REVIEW
The internet of thing is a technology which is more than capable the way to live. The growth in the number of devices and the speed of that growth presents challenges to people's security and freedoms as person battle to develop policies, standards, and governance that shape this development without stifling innovation. [1] IoT promises the interconnection of multitude of things demonstrate services to humans and machines. It is expected that by 2020 tens of billions of things will be deployed worldwide. For scalable and trusted platform underpinning the growth of IoT, a new kind of architecture is needed. [2] If someone want to develop fog/edge computing-based IoT infrastructure, the architecture, enabling techniques, and issues related to IoT should be researched first, and then the integration of fog/edge computing and IoT should be explored. [3] Nowadays Internet of Things (IoT) attract much more to researchers, because it becomes a principle technology that make a smart human being life, by providing a communication between objects, machines and everything together with peoples. [4] The IoT sensor may include wi-fi, Bluetooth, RFID, ZigBee etc. Internet of thing is technology in which physical system is connected with internet and they communicate with each other. Internet is providing the instruction to physical system and physical system is work according to instruction. [5] IoT applications are widely using in many fields of social living such as healthcare, energy and industrial automation. While people are enjoying the convenience and efficiency that IoT brings to peoples, always a new threat from IoT also have raised. [6] There are increasing a lot of researcher on works to ease these threats, but many problems remain open. Internet

of things (IoT) is hugely interconnected global network which connected to everyone's life, expand business productivity, improve government efficiency, and the list just goes on. [7] Therefore, this new reality (IoT) built on the basis of Internet, and always raised new kind of challenges from a security and privacy perspective. The Internet of Things (IoT) is the most optimistic area which use the advantages of Wireless Sensor and Actuator Networks (WSAN) and Computing domains. [8] Different applications of IoT have been developed and researchers investigate the opportunities, problems, challenges and the technology used in IoT such as Radio-Frequency Identification (RFID) tags, sensors, actuators, mobile phones, etc. Modern societies are finding modern way to live life and IoT is making it more possible day by day. A huge number of IoT devices will be continuously making the data they generate available on internet. [9] The Internet of Things (IoT) can deliver a lot of services in different areas such as health, fitness and wellbeing, manufacturing, transportation and logistics, disaster coordination, sustainability environment, and human development. The Internet of Things (IoT) make easy to live life due to IoT provides facilitates the interconnection and data exchange of modern objects across every aspect of people's lives, it may be people's homes, cars, and even living bodies. [10] According to few researchers the IoT will consist of nearly 30 billion objects by 2020. Therefore, due to the open Internet connectivity, IoT contain a huge number of threats, hackers may exploit critical vulnerabilities in a wide range of IoT applications and devices for carrying out their nefarious activities.

3. BENEFITS AND ISSUES

3.1 Benefits

Some of the basic benefits are:

- **Communication:** IoT communicates people about the status and conditions of their devices and system. Before IoT, people had to collect all these data themselves. For example, in a health care system track of everything can be kept i.e. all their apparatus used, empty beds, available doctors and medicines.
- **Control and Automation:** 20 years earlier who would have that one can control his/her house by using just his voice. All this is possible now by using IoT enabled - connected smart homes. Everything can be controlled starting from turning off/on lights or to drop-in from a remote location and have a look at the house.
- **Cost Savings:** When it comes to a business point of view, organizations spend or lose a lot of money where their devices fail. IoT helps them overcome this problem by giving prior information about the device's performance.

3.2 Issues of IoT

Apart from having lots of benefits IoT also has some issues which can be concerning.

Some of the basic ones are:

- **Security Issues**: It may look good and or everyone may find living in a smart home easier since all the devices are connected to a same network but this thing is also the biggest concern. Getting access to companion devices on a network is not a big task neither is getting into a network. The hacking of baby monitors, smart fridges, Barbie dolls, drug infusion pumps, cameras and even assault rifles are a security nightmare being caused by the future of IoT. So many new nodes being added to networks and the internet will provide a massive number of hackers and enormous number of attack possibilities. This is also concerning as we looking forward towards smart cities, and if system is compromised critical areas can be targeted. Scalability issues also contribute to the creation insecure IoT products. The fact is that many security solutions being used today have been created with generic computing devices in mind. IoT devices often lack the computational power, storage capacity and even proper operating system to be able to deploy such solutions.
- **Privacy Issues**: IoT devices handle a lot of very sensitive data. Some smart homes devices such as ones inbuilt with Alexa have access to amazon accounts which contain user's personal details and even credit cards. The data is protected by legislations such as the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. and are fundamentally different from our browsing and clicking habits. Yet the necessary precautions aren't taken when storing the data or sharing it with other service providers. Vendors and manufacturers must either discard this data or remove the Personally Identifiable Information (PII) to make sure that consumers aren't damaged in case of data breaches. Even though devices such as smart bathroom system, smart toasters may not reveal any sensitive data but when embedded with other devices may give some information about an individual's life pattern.
- **Connectivity issues**: IoT requires a number of devices to be connected in a system at once. This is now becoming possible and easier with the introduction of IPv6. IoT systems need to defy the current communication models and used hardware/technologies. At present we rely on the centralized, server/client model to authenticate, authorize and connect different nodes in a network. The server client model is capable enough to handle when hundred or a couple of devices are connected. But for a system in which millions or may be billion devices can connect the server client model fails. Such systems will require a huge setup cost on cloud services which can handle such an enormous amount of information exchange.
- **Compatibility and longevity issues**: IoT is growing in many different directions, with many different technologies competing to become the standard. For example, we currently have ZigBee, Z-Wave, Wi-Fi, Bluetooth and Bluetooth Low Energy (BTLE) all trying to become the dominant transport medium between devices and hubs. This will have its own issues and extra hardware will be needed to connect the devices or to make them compatible with each other. Some more issues will be the difference in clouds, operating systems and firmware. Some of these technologies may not be used after some years and that will make their devices eventually useless. IoT devices last for a long time but generic computing devices may not.

3.3 Some security issues of IoT

- **Vulnerable Constrained Devices**:
  Many IoT devices have limited amounts of storage, memory, and processing capability and they often need to be able to operate on lower power, for example, when running on power backup. Security approaches that rely heavily on encryption are not a good fit for these constrained devices, because devices are not capable of performing complex encryption and decryption quickly enough to be able to transmit data securely in real-time. These devices are often vulnerable to side channel attacks, such as power analysis attacks, that can be used

to reverse engineer these algorithms. Instead, constrained devices typically only employ fast, lightweight encryption algorithms.

- **Authorize and authenticate devices:**

Authentication and authorization are extremely important parts of basic security processes and are hardly needed in the Internet of Things. Devices must establish their identity before they can access gateways and upstream services and apps. However, there are many IoT devices that fall down when it comes to device authentication, for example, by using weak basic password authentication, or using passwords unchanged from their default values.

- **Manage device updates:**

Device updates in IoT are an essential task for service providers & manufacturers. manufacturers. Applying updates, including security patches, to software that runs on IoT devices and gateways presents a number of challenges. For example, you need to keep track of which updates are available apply updates consistently across distributed environments with heterogeneous devices that communicate through a range of different networking protocols.

- **Secured communication:**

In IoT, secured communication is one kind of challenge to ensure that communication over the network between device and other services such as cloud service or apps is secure. To ensure, whenever IoT device send any message over network, message should be encrypted. And using private (separate) network is also help to communicate securely to each other and data transmitted remains confidential.

- **Data privacy and integrity:**

It is also important that the data ends up after it has been transmitted across the network, it is stored and processed securely. Implementing data privacy includes anonymizing sensitive data before it is stored or using data separation to decouple personally identifiable information from IoT data payloads. Ensure data integrity, which may include digital signature and other that ensure data has not been changed.

- **Secured service:**

In the terms of IoT, service may be web mobile and cloud application and these services are used to manage, access, and process of IoT device and data so you must be secured the services of IoT. When installing IoT application, you must be sure to install secure system to avoid vulnerabilities.

- **Ensure high availability:**

High Availability is a characteristic of a system, which aims to ensure an agreed level of operational performance, generally uptime, for a higher than normal period. It is measured as a percentage of uptime in a given year. The potential for disruption as a result of connectivity outages or device failures, or arising as a result of attacks like denial of service attacks, is more than just inconvenience.

- **Detect vulnerabilities:**

One of the most security issues of IoT is detection of vulnerability. How do you know if your IoT system has been compromised? In large scale IoT systems, the complexity of the system in terms of the number of devices connected, and the variety of devices, apps, services, and communication protocols involved, can make it difficult to identify when an incident has occurred. While IoT is expected to improve life for many by enabling smart living spaces, the number of security risks that consumers and businesses face is also increasing. A high number of vulnerable IoT devices are prone to attacks and easy exploit. So, it is very important thing to always detect vulnerability in IoT device.

- **Manage vulnerabilities:**

The complexity of IoT systems also makes it challenging to assess the repercussions of a vulnerability or the extent of a breach in order to manage its impact. Challenges include identifying which devices were affected, what data or services were accessed or compromised and which users were impacted, and then taking actions to resolve the situation.

- **Predict security issues:**

A longer-term IoT security challenge is to apply security intelligence not only for detecting and mitigating issues as they occur, but also to predict and proactively protect against potential security threats. Threat modelling is one approach used to predict security issues.

3.4 Prevention

There is plenty that you can do to help protect your network when implementing IoT solutions.

- **Proper device Selection:** Ask yourself first if you really need that device to be connected. Think will the device help me enough in my daily routine or will help my organization in collecting important data.

- **Use strong passwords:** Always use strong and complicated passwords which consists of multiple characters and special symbols. Many of these devices include factory set passwords which are relatively easy to figure out for the smart hacker. Ensure you change them to something safe. Use different passwords for different devices.

- **Disable play functionality and Universal plug:** These attributes make it effortless for devices to recognize one another, that is useful for quick configuration, but also for hackers to identify and target your own network. By disabling universal plug and play, yes people will need to configure his/her devices to his/her network manually, but people will also get the reassurance it will be more difficult for people with ill intentions to target his/her own network too.

- **Keep Observing:** One should always visit and keep checking your device and apparatus to make sure they are working fine and they are not compromised. For business purposes, outsourcing this service can also be feasible and, believe me, it is well worth the expense. If your network is compromised, you are going to wish you had not saved the money up front, since it's extremely costly to recoup from a cyber assault.

4. CONCLUSION

IoT is a hot topic nowadays both in business sector and even for small homes/organizations. As people getting more and more devices generating enormous amount of data which leads to a lot of security concerns and privacy concerns. There are some basic hardware requirements which is needed by an IoT system are discussed in the paper. Even though IoT is not a new concept there are multiple issues like the security

issues, privacy concerns, compatibility issues and connectivity & longevity issues. The security issue also has some more divisions like manging the devices, communication channels, data privacy and integrity, exploitation of the limitations of a IoT device. And some more.

5. REFERENCES

[1] Maple, C. (2017). Security and privacy in the internet of things. Journal of Cyber Policy, 2(2), 155-184.

[2] Gazis, V., Goertz, M., Huber, M., Leonardi, A., Mathioudakis, K., Wiesmaier, A., & Zeiger, F. (2015, February). Short paper: IoT: Challenges, projects, architectures. In Intelligence in Next Generation Networks (ICIN), 2015 18th International Conference on (pp. 145-147). IEEE.

[3] Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5), 1125-1142.

[4] Zeinab, K. A. M., & Elmustafa, S. A. A. (2017). Internet of Things applications, challenges and related future technologies. World Scientific News, 2(67), 126-148.

[5] Suchitra., Vandana. Internet of Things and Security Issues. IJCSMC, Vol. 5, Issue. 1, January 2016, pg.133 – 139.

[6] Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2018). The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. IEEE Internet of Things Journal.

[7] Iqbal, M. A., Olaleye, O. G., & Bayoumi, M. A. (2017). A review on Internet of Things (IoT): security and privacy requirements and the solution approaches. Global Journal of Computer Science and Technology.

[8] [Porkodi, R., & Bhuvaneswari, V. (2014, March). The internet of things (IOT) applications and communication enabling technology standards: An overview. In Intelligent Computing Applications (ICICA), 2014 International Conference on (pp. 324-329). IEEE.

[9] Sheth, A. P., Srivastava, B., & Michahelles, F. (2018). IoT-Enhanced Human Experience. IEEE Internet Computing, 22(1), 4.

[10] Chen, Y. K. (2012, January). Challenges and opportunities of internet of things. In Design Automation Conference (ASP-DAC), 2012 17th Asia and South Pacific (pp. 383-388). IEEE.