Internet of Things (IoT) Security Challenges

Prof.Swami Shashikant Virbhandra
Dayanand College of Commerce, Latur

Abstract-

The Internet of Things (IoT) developed the global network containing of people, smart devices, intelligent objects, information, and data. It is no secret that as more and more devices connect to the internet, the challenges of safeguarding the data that they transfer and the communications that they initiate are becoming more reflective. Over the years, we have seen a surge in IoT devices, broadly in two areas – in homes and in manufacturing. With the former, we have seen an entire ecosystem built around Amazon's Echo devices using the Alexa Voice Service. Google, Microsoft, and Apple have followed suit as well. Since these are self-determining and closed platforms, the responsibilities of securing the devices rest with the platform providers. In this paper, we highlights cyber security in manufacturing and related industries. Industries such as manufacturing, oil & gas, refining, pharmaceuticals, food & beverage, water treatment, and many more are constantly looking to add the right layers of security, as they bring an increasing number of equipment and devices online. Device manufacturers and plant operations managers constantly face pressure to protect their physical assets from cyber threats. Moreover, for each of these industries, the nature of the data, topologies of IoT devices, and complexities of threat management and ensuring compliance vary widely.

Keywords-- Internet of Things, Cyber-attack, Security threats.

Introduction

The modern rapid development of the Internet of Things (IoT) and its ability to offer different types of services have made it the fastest growing technology, with massive impact on social life and business environments. Internet of Things (IoT) devices are rapidly becoming universal while IoT services are becoming persistent. Their success has not gone unnoticed and the number of threats and attacks against IoT devices and services are on the increase as well. The Internet of Things (IoT) is an idea that could radically alter our relationship with technology. The promise of a world in which all of the electronic devices around us are part of a single, interconnected network was once a thing of science fiction. But IoT has not only entered the world of nonfiction; it's taking the world by storm. IoT devices are no longer a niche market. They have started to move from our workspaces into our homes, where IoT devices are expected to have the most important impact on our daily lives. Most smart home devices will be benign, everyday appliances like kettles and toasters. Even if these devices are hacked and co-operated, short of ruining your breakfast, there's not a lot a hacker can do to cause you grief. The market is currently focusing on the vertical domains of IoT since it is in relatively early phases of development. But IoT cannot be treated as a single thing, or single platform, or even a single technology. In order to achieve the expected rapid growth from IoT opportunities, more focus needs to be put on interfaces, platforms, mobile applications and common/dominant standards. IoT in the education sector has already started to make the conventional education system more automated — interactive smart classrooms are helping students learn and participate more, whilst automatic attendance and various student tracking systems could help to make schools more secure. Internet-enabled remote classrooms will be a milestone for developing countries, making deep penetration in areas where setting up a traditional school infrastructure is not possible. Internet-enabled manufacturing and industrial units are giving differentiating results, making them safer and more efficient through automated process controls. Plant and energy optimization, health and safety control and security management are now increasingly being provided by advanced sensors, networked with sophisticated microcomputers. Financial services are already leveraging the internet for many of their services. Exponential improvement in digital infrastructure and the next generation of IoT enabled products could further lead the growth of the financial sector, with innovations, such as smart wearable and smart monitoring devices, helping customers to keep better track of their money and investments. Telcos could face a surge in data usage due to IoT-enabled devices, thus raising their ARPU (average revenue per user), while on the other hand, they will also have to deal with some concerns, such as privacy and infrastructure security. While the possibilities of these new technologies are mind-boggling, they also reveal severe IoTcybersecurity challenges. During the last few years, we've seen a dramatic increase in the number and the sophistication of attacks targeting IoT devices. The interconnectivity of people, devices and organizations in today's digital world, opens up a whole new playing field of vulnerabilities — access points where the cyber criminals can get in.

Internet of Things (IOT)

The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to - computer interaction A thing in the internet of things can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has builtin sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an IP address and is able to transfer data over a network. The internet of things (IoT) is a computing concept that describes the idea of everyday physical objects being connected to the internet and being able to identify themselves to other devices. The term is closely identified with RFID as the method of communication, although it also may include other sensor technologies, wireless technologies or QR codes.

Features Of Internet Of Things (IOT)

Some most popular characteristics of Internet of things are:

i. Intelligence: IoT comes with the combination of algorithms and computation, software & hardware that makes it smart. Ambient intelligence in IoT enhances its capabilities which facilitate the things to respond in an intelligent way to a particular situation and supports them in carrying out specific tasks. In spite of all the popularity of smart technologies, intelligence in IoT is only concerned as means of interaction between devices, while user and device interaction is achieved by standard input methods and graphical user interface [8]. Together algorithms and compute (i.e. software & hardware) provide the "intelligent spark" that makes a product experience smart. Consider Misfit Shine, a fitness tracker, compared to Nest's intelligent thermostat. The Shine experience distributes compute tasks between a smartphone and the cloud. The Nest thermostat has more compute horsepower for the AI that make them smart.

ii. Connectivity : Connectivity empowers Internet of Things by bringing together everyday objects. Connectivity of these objects is pivotal because simple object level interactions contribute towards collective intelligence in IoT network. It enables network accessibility and compatibility in the things. With this connectivity, new market opportunities for Internet of things can be created by the networking of smart things and applications. Connectivity in the IoT is more than slapping on a WiFi module and calling it a day. Connectivity enables network accessibility and compatibility.

iii. Dynamic Nature : The primary activity of Internet of Things is to collect data from its environment, this is achieved with the dynamic changes that take place around the devices. The state of these devices change dynamically, example sleeping and waking up, connected and/or disconnected as well as the context of devices including temperature, location and speed. In addition to the state of the device, the number of devices also changes dynamically with a person, place and time. The state of devices change dynamically, e.g., sleeping and waking up, connected and/or disconnected as well as the context of devices including location and speed.

iv. Enormous scale: The number of devices that need to be managed and that communicate with each other will be much larger than the devices connected to the current Internet. The management of data generated from these devices and their interpretation for application purposes becomes more critical. Gartner (2015) confirms the enormous scale of IoT in the estimated report where it stated that 5.5 million new things will get connected every day and 6.4 billion connected things will be in use worldwide in 2016, which is up by 30 percent from 2015. The report also forecasts that the number of connected devices will reach 20.8 billion by 2020.

v. Sensing: IoT wouldn't be possible without sensors which will detect or measure any changes in the environment to generate data that can report on their status or even interact with the environment. Sensing technologies provide the means to create capabilities that reflect a true awareness of the physical world and the people in it. The sensing information is simply the analogue input from the physical world, but it can provide the rich understanding of our complex world. We tend to take for granted our senses and ability to understand the physical world and people around us. Sensing technologies provide us with the means to create experiences that reflect a true awareness of the physical world and the people in it. This is simply the analog input from the physical world, but it can provide rich understanding of our complex world.

vi. Heterogeneity: Heterogeneity in Internet of Things as one of the key characteristics. Devices in IoT are based on different hardware platforms and networks and can interact with other devices

or service platforms through different networks. IoT architecture should support direct network connectivity between heterogeneous networks.

vii. Security: IoT devices are naturally vulnerable to security threats. As we gain efficiencies, novel experiences, and other benefits from the IoT, it would be a mistake to forget about security concerns associated with it. There is a high level of transparency and privacy issues with IoT. It is important to secure the endpoints, the networks, and the data that is transferred across all of it means creating a security paradigm

Applications Of Internet Of Things (IOT)

Some useful applications of Internet of Things (IOT) are:

- Connected Health- IoT has various applications in healthcare, which are from remote monitoring equipment to advance & smart sensors to equipment integration. It has the potential to improve how physicians deliver care and also keep patients safe and healthy.
- Smart City-IoT will solve major problems faced by the people living in cities like pollution, traffic congestion and shortage of energy supplies etc. Products like cellular communication enabled Smart Belly trash will send alerts to municipal services when a bin needs to be emptied
- Connected Cars - Most large auto makers as well as some brave startups are working on connected car solutions. Major brands like Tesla, BMW, Apple, and Google are working on bringing the next revolution in automobiles
- Smart Retail- Retailers have started adopting IoT solutions and using IoT embedded systems across a number of applications that improve store operations such as increasing purchases, reducing theft, enabling inventory management, and enhancing the consumer's shopping experience. Through IoT physical retailers can compete against online challengers more strongly.

Smart Farming -The potential of IoT in the retail sector is enormous. IoT provides an opportunity to retailers to connect with the customers to enhance the in-store experience. Smartphones will be the way for retailers to remain connected with their consumers even out of store. Interacting through Smartphones and using Beacon technology can help retailers serve their consumers better.

Security Challenges Facing IOT

IoT security is the safeguard of Internet of Things devices from attack. While many business owners are aware that they need to protect computers and phones with antivirus, the security risks related to IoT devices are less well known and their protection is too often neglected. Internet of Things devices are everywhere. From cars and fridges to monitoring devices on assembly lines, objects around us are increasingly being connected to the internet. The speed at which the IoT market is growing is staggering - Juniper research estimates that the number of IoT sensors and devices is set to exceed 50 billion by 2022.While consumer IoT devices allow lifestyle benefits, businesses are quickly adopting IoT devices due to high potential for savings. For example, after Harley-Davidson turned their York, Pennsylvania plant to a 'smart factory' using IoT devices in every step of the production process, they reduced costs by 7% and increased net margin by 19%. Data Integrity Billions of devices come under the umbrella of an interlinked ecosystem that is connected through IoT. Manipulating even a single data point will result in manipulation of the entire data which is exchanged and shared back and forth from the sensor to the main server. Decentralized distributed ledger and digital signatures should be implemented in order to ensure integrity Encryption Capabilities Data encryption and decryption is a continuous process. The IoT network's sensors still lack the capability to process. Privacy Issues IoT is all about the exchange of data among various platforms, devices, and consumers. The smart devices gather data for a number of reasons, like, improving efficiency and experience, decision making, providing better service, etc.; thus, the end point of data shall be completely secured and safeguarded. Common Framework There is an absence of a common framework and so all the manufacturers have to manage the security and retain the privacy on their own. Once a common standardized framework is implemented, the individual efforts will then collectively be utilized in an expandable manner and so reusability of code can be achieved

Conclusion

The IoT framework is helpless to attacks at each layer. Therefore, there are many security threats and requirements that need to be dispatched. Current state of research in IoT is mainly concentrated on confirmation and access control protocols, but with the rapid growth of technology it is essential to combine new networking protocols like IPv6 and 5G to achieve the progressive mash

up of IoT topology The main importance of this chapter was to highlight major security issues of IoT particularly, focusing the security attacks and their countermeasures. Due to lack of security mechanism in IoT devices, many IoT devices become soft targets and even this is not in the victim's knowledge of being infected. In this chapter, the security requirements are discussed such as confidentiality, integrity, and authentication, etc

References

1. Y. Xie and D. Wang, "An Item-Level Access Control Framework for Inter-System Security in the Internet of Things," in Applied Mechanics and Materials, 1430-1432, 2014.
2B. Anggorojati, P. N. Mahalle, N. R. Prasad, and R. Prasad, "Capability-based access control delegation model on the federated IoT network," in Int'l Symposium on Wireless Personal Multimedia Communications (WPMC), 604-608, 2012.
3 M. K. Saini and R. K.SainiInternational Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Published by, www.ijert.org NCRIETS – 2019 Conference Proceedings
4. MirzaAbdurRazzaq and Muhammad Ali Qureshi "Security Issues in the Internet of Things (IoT): A Comprehensive Study" by (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017.
5. A. Mohan, "Cyber security for personal medical devices internet of things," in Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on. IEEE, 2014, pp. 372–374