Parichay Maharaja Surajmal Institute Journal of Applied Research

IoT Risk and Security Challenges

Dr. Menal Dahiya*, Itisha Gupta, Sharmon Chahal**

Abstract: In today's world there are so many new technologies and because of that there are so many smart devices surrounding us. These new technologies are making our lives easier and simpler. As the technology evolves, threats and cyber-attacks are also increasing. And there is always a risk to our confidentiality. In the research paper, we are going to talk about the uses of IoT and the security risk in it.

Privacy and security are the biggest challenges in IoT. Improper device upgrades, e-customer shortages and robust security systems, user ignorance, and device preferences are some of the challenges facing IoT. IoT has three layers: Perception layer, Network layer, and Application layer. This paper addresses problems related to security inside and outside of these layers.

1. INTRODUCTION

The IoT collects connected devices, services, objects and people that can work together, sharing information and knowledge to achieve targets in a variety of regions. Internet of Things can be done in a variety of areas like health, traffic monitoring, hospitality, water supply, agriculture, smart grid and energy saving and other areas also that require Internet collaboration to do business intelligently without personal participation. Devices connecting to IoT usually follow the Identity Management (IM) method which will be identified in a group of comparable and different devices. The IoT areas can be explained with the help of an IP address, but inside that area every business has a different identity. Approximately 26.67 billion of IoT devices are present in this world [1].

The best part of IoT is that all visuals can be communicated and accessed online. Due to the high cost of the Internet, a large amount of devices is united to the Internet. In 2008, the number of devices which were united to the Internet was higher than the number of people in the world. According to research, there were around 4.49 billion devices which were connected to the Internet and hike in 2016 is likely to be increased by 30%. By 2020 to hit 50 billion. These devices lead to the location of the attackers. There are various characteristics of IoT given below:

1. **Connectivity:** Everything that happens on IoT and hardware, with sensors and other technologies and systems needed to connect and control must be interconnected at different levels.

2. **Items:** Anything marked or connected as it is designed to connect. From sensors and markers to livestock. Devices that may contain sensors or sensors may be connected to devices and objects.

3. **Communication:** Connected devices are able to communicate data and that data can be analyzed. Communication can be short distance or long distance or very long distance. Examples: Wi-Fi technology, LPWA network like LoRa or NB-IoT.

4. **The power of intelligence:** Sensing on IoT devices and intelligence collected from big data analytics / machine learning.

5. **Action:** The result of ingenuity. This can be a hands-on activity, an event-based conversation (Example: In smart factory decisions) and automation, often the most important part.

2. APPLICATIONS OF IOT

The IoT has many applications and many of them can be seen in our surrounding also. And few are following:

A. Environmental Monitoring

The environmental protection is done with the help of sensors and observing the atmospheric conditions such as quality of air and quality of water is also done with the help of sensors. Flora-and-fauna is also being observed to find out where they live.

B. Infrastructure Management

The process of observing and controlling the operation of infrastructure such as bridges, railway tracks, and roads etc. is the main application. Modification of structural conditions can put security at risk and increase risk, which is why IO infrastructure management can be considered.

**Associate Professor, Department of Computer Applications, Maharaja Surajmal Institute, Affiliated College of GGSIP University, New Delhi, menaldahiya@msijanakpuri.com*
***Student, Department of Computer Applications, Maharaja Surajmal Institute*
Sharmon Chahal, Student, Department of Computer Applications, Maharaja Surajmal Institute

C. Production

The effectiveness of actual production can be achieved. With the help of sensors and control systems the supply and production can be controlled. This can lead to faster production of new items.

D. Home Automation

Gas, water and energy information is directly conveyed to their respective service companies. Efficiency of resources can be increased using this process. Devices like AC, iron, windows, fans, TV, lights, refrigerator and washing machine can be controlled with the help of home automation process.

E. Transportation

IoT technology has been used for the first time in this field. It is using the combination of GPS, GSM and light sensors. The vehicle can operate as an organization and be connected to road infrastructure. Sensors in cars can also be used for avoiding collisions and to control vehicles to provide the parking.

3. ARCHITECTURE OF IOT

In Internet of Things (IoT) structure, each and every layer is illustrated with their purpose and the devices present in the layer. There is a different belief regarding the layers present in the Internet of Things. But after many researches it is found that IoT actually have three layers only: Perception layer, Network layer, and Application layer. Each IoT layer has its own internal security problems [6]. The diagram below shows the basic structure of the three IoT layers with the technologies and devices used in them.

Perception layer: This layer is also called as the "Sensors" layer. Perception layer is used to gather data of the surrounding with the support of nerves. Perception layer monitors, gather, and uses data from the sensors and transfers the data to the next layer that is network layer. The perception layer can also create a combination of IoT nodes for local and short-distance networks [2].

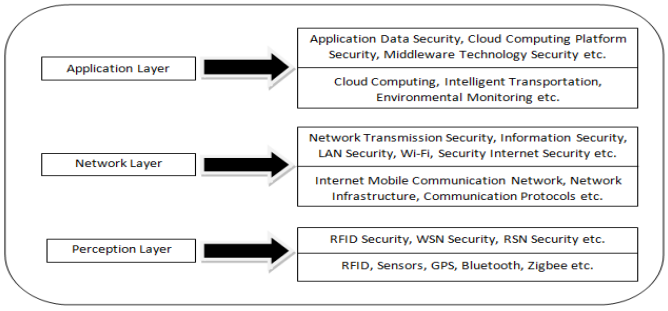

Fig. 1. Architecture of IoT

Network layer: This IoT layer accomplish the function of data transfer and conversation on various IoT ports and devices via the Internet. In network layer, internet gates, switches, and routes etc. works and operate practicing other technologies such as Bluetooth, Zigbee, 3G, Wi-Fi etc. to supply scattered network services. Network gates present as a link in the middle of various IoT sites for compiling, cleaning, and sending data to various sensors [3].

Application layer: This layer ensures the confidentiality, authenticity and integrity of the data. Creating intelligent environments is the main goal of this layer.

4. SAFETY VULNERABILITIES IN EACH LAYER IN IOT

Each IoT layer is controlled by security risks and attacks. This may work, or may be, and may be obtained from external sources or from an internal network attacked by an insider. Active attacks cause them to stop the service / application while the partition type looks at the IoT data network without blocking their service. In each layer, IoT devices and services are highly sensitive to Denial of Service (DoS) attacks, making the application, service or network inaccessible to the authorized users. The security issues for each layer are described below given a brief overview of these types of problems related to each layer in IoT.

Perception Layer:

In the IoT perception layer there are three types of security issues. Influence of wireless signals is the first issue in this layer. With the help of wireless technology significant signals are transmitted between the IoT sensors whose performance can be weakened by vibrating waves. Second issue is that the attack can easily happen not only by the owner but it can be done by the attackers also on the sensor node on the IoT devices because IoT nodes often operate on external surfaces, leading to physical attacks on sensory and IoT systems where the attacker may touch hardware components of the device. Next

problem is the status of the dynamic network model as IoT nodes are often installed in different locations. The visual field of IoT in particular has sensors and RFIDs, due to its lethal storage, power consumption, and limited calculation capabilities that make it responsive to a variety of risks and attacks.

Perception layer encryption can be misused by Replay Attack which can be done by spraying, changing or copying the details of one of the devices on IoT. Or by updating the time required to execute the encryption the attacker can get the encryption key, this is called as Timing Attack. Another secret attack is when the attacker takes the space below and takes all

the details and data from the real Node Capture. An attacker can attach new node to a network that threatens the visibility of the information in the detection layer by sending harmful data. This can lead to DoS attacks, by exploiting the existing nodes in the system and removing them from sleep mode used by energy saving sites. The security issues listed above in the acquisition layer can also be treated with encryption (either point or end point), authentication (sender authentication) and access control [5].

Network layer:

This IoT layer is also controlled by DoS attacks. In addition to the DoS attack, the enemy may attack the privacy and confidentiality of network installations by checking traffic, listening, and monitoring. This attack is most likely due to remote access to data exchange devices. The network layer is largely controlled by the Man-in-the-Middle invasion. And if device key tools are removed, the secure connection will be completely weakened. The IoT key exchange system should be protected to prevent anyone from entering the hearing, and then stealing identity information.

Application layer:

As IoT still has comprehensive policies and standards for communication and performance improvements, so there are many safety-related issues. Different applications and software have different authentication methods, making their integration more difficult to ensure data privacy and identity verification. A large number of data sharing devices will create a huge increase in data analytics applications, which can have a significant impact on service proximity.

5. IOT SAFETY CHALLENGES

IoT has brought great benefits to users. However, there are other challenges as well. The dangers of cyber security and secrecy are the main concerns of identified researchers and security experts. The two create a major problem for many business organizations and community organizations. The most prominent cyber security attacks have proven to be a threat to IoT technology. This danger is due to the fact that network communication with the Internet of Things (IoT) brings access to an anonymous and unreliable Internet that requires security solutions to this novel.

And the important thing is that of all the known challenges, none has a greater impact on IoT compliance, such as privacy and security. However, it is unfortunate that users often do not have the necessary acknowledgment of the security consequences until such time as the violation occurs, causing serious damage such as loss of important information. As a result of ongoing security violations that endanger user's privacy, consumers desire for less security has now diminished. In a recent review of security and privacy, the level of Internet consumers did not work well. There have been many defects in modern automotive systems.

Challenges in security of IoT are broadly divided into two categories: Technical and security resistance [3]. The technical challenges come as a result of the unique and widespread nature of IoT devices, while security breaches are related to ethics and usefulness that should be used to protect a secure network.

Keeping private: The most important thing is to make sure that the information is secured and protected and can be accessed by authorized users only.

Integrity: IoT is based on the sending and receiving of data and information among many devices connected to each other, that's why it is very important to make sure the correctness of data and the data received must be correct and data should not get changed during the transfer process.

Availability: The idea of IoT is to make many smart devices to join as possible. IoT users should have the access to view the data whenever it is needed. However, in IoT data is not only the single module used in it. And also, the devices and services should have the accessibility in a timely manner to fulfill the requirements.

Proof of Authenticity: Everything in the IoT should be smart to verify certain things clearly. However, this process can be tested due to the behavior of IoT, several organizations are assorted like services, people, devices, service providers and processing units. And sometimes things are needed to interact with each other for the first time. [4] In view of all of this, there is a need for more corporate governance in all IoT communications.

Data Integrity: The correctness of the data and the information transferred between the sender and receiver is the main problem. Therefore, it is important to make sure the correctness of the data.

6. ATTACKS ON IOTTECHNOLOGIES

1. Wireless Sensor Networks

It contains many small cells called sensor nodes and computer programs called actuators. Key features that help you hear, process data and communicate. The health care system, housing rent, military use, resource management, environmental monitoring and forecasting etc. are few WSN applications in IoT. WSNs have been attacked due to broadcast transmission. The main threats to WSN are:

Physical Attacks: Everything should have a sense of accomplishment. It is very difficult to stop physical access for unauthorized users. The signal can modify the node / sensor data, so that the entire network's performance sensor is compromised.

Replication of nodes: In this type of attack, the existing location is duplicated to the sensor network. And because of duplicate packets of incorrectly transmitted nodes, incorrect sensor readings are detected or network cuts occur. Therefore, the network performance of the sensor is interrupted.

Selected Forwarding: In WSN, referral sites receive messages / notifications on the go. A dangerous node transmits packets to this attack. Some messages can be discarded without continuing to send them. Package conversion from certain nodes is done and the message is transmitted to other nodes. Therefore, it is not easy to know who the attacker is.

Wormhole Attack: It is a censorious attack where the packets are recorded in a particular network area and then returned to the any other location. This process can be done particularly.

2. *Radio Frequency Identification Technology:*

Radio-frequency identification (RFID) has multiple RFID tags and one or more RFID readers. The tags are specified with an address and this is added to the items. These tags serve as a distinctive identifier for that object. These RFID Tags are used to know the production, monitor food and moisture quality, monitor patient health parameters, purchase, track animal movements etc [7]. There are various types of attacks on RFID technology. Some of them are following :

Modification of physical data: Tags are physically available and details are subject to change. Error inserting or writing memory is used for modification. The process of converting the data when the data is processed or written is known as error importing. Recording of memory can also be done with the help of some tools such as a small charged needle or laser cutting microscopes. This attack leads to the incorrect marking information. For example, a manufactured product with the RFID tag attached to it gives incorrect information for that product. Additionally, the tag cannot be tracked.

Tag Cloning: Tag cloning is the process of putting the first marker in a new location and copying the first id to it. Software and tags are accessible in the market. An attacker can easily insert a real marker and insert a new one, if the RFID tags do not use any physical access protection.

Tag Swapping: Marking is bringing out by marking two products that are different from one another. In the retail stores, these types of attacks can be easily occurred where an expensive tag is swapped for a lower price. The most expensive item is bought at a lower price.

Denial of Service Attack: If data is required of the RFID reader from the mark, then the id identification tag is accepted. Then compare it with the database stored id. If the tag failed to transfer ownership to the reader during the DOS attack, the connection between the reader and the tag will be unstable and the service will get suspended.

7. CASE STUDY

Amnesia:33 — Critical TCP/IP Flaws

Cybersecurity investigators have identified a number of widely used TCP / IP errors affecting more than a million devices from communications and medical services in an industry control system that an attacker can use to manage a targeted system.

The term "AMNESIA: 33" by Forescout investigators, a collection of 33 risks affecting four opensource TCP / IP sources - IP, FNET, pico TCP, and Nut / Net - widely used on the Internet - IoT and embedded devices.

As a result of improper memory control, active exploitation of errors can damage memory, and allow attackers to access devices, create malicious codes, attack DoS, leak important and sensitive information, and damage DNS cache.

These types of attacks can be played out in a variety of ways: disrupting the power of the power station leading to the extinguishing or switching of smoke alarms and offline temperature monitoring systems using any DoS threat. Errors, which will be clarified at the Black Hat Europe security

conference, are identified as part of Project Memoria's Forescout program to study the security of TCP / IP stacks.

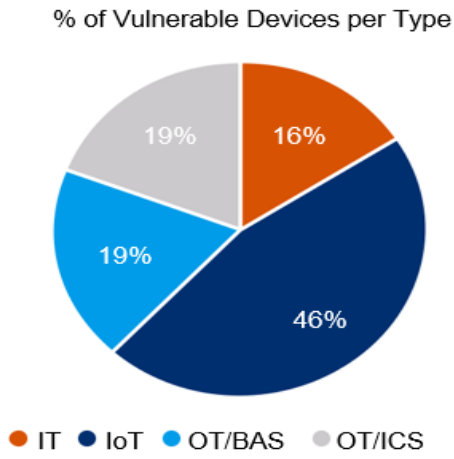

Fig. 2. Percentage of Vulnerable Devices per Type

Forescout Device Cloud and online devices for devices have also shown potential impact on many industrial processes, where government, health care, services and manufacturing have the greatest exposure. The increase in this risk means that more organizations around the world could be affected by AMNESIA: 33. Failing organizations minimizing this risk leaves the door open for attackers to use IoT, OT and IT devices across their organization [8].

8. THE FUTURE OF IOT

Currently, objects and programs are enabled for network communication and are enabled on computers to communicate with the same connected devices. Increasing the capacity of the network in all potential areas will give our lives purpose and helping us in saving money and time. However, connecting to the internet also leads to potential cyber threats. Products allowed on the Internet become victims of cybercrimes.

Over the next decade, from 2020 to 2030, IoT devices will grow from 75 billion to more than 100 billion, and improvements from 4G to 5G and IoT expansion are crucial. Today's 4G network can support up to 5500 to 6000 NB-IoT devices in a single cell. With a 5G network, up to a million devices can be controlled by a single cell.

9. CONCLUSION

This paper aims to provide the reader with an overview of the basics of IoT security challenges. It has major security and privacy challenges due to its apparent growth. The IoT framework is in at risk and each layer is under attack. There are many threats and security requirements that are needed to be addressed. Researchers at IoT are very focused on ensuring and controlling access for unauthorized users, but as the technologies are speedily growing it is important to integrate new communication rules such as IPv6 and 5G to achieve continuous development of IoT topology. While we continue to focus on safety and prevent major accidents.

IoT is turning out as an important technology. Data sent from sensors or RFID tags may contain important data that should be saved from the users who are not authorized. IoT connection between nodes are not protected and security for IoT devices should not be limited to supply and capture. To secure communications, IoT should provide services such as access control for real-time infrastructure protection, end-to-end encryption and sensitivity. It is a challenge for researchers to be in advance of the attackers. In the coming years,more security for smart devices will be needed and the IoT communication's privacy process will grow which will permit the users to use these technologies and can easily perform the tasks. The data protection strategies, ethical practices and high confidentiality will help in gaining the trust of the users.

REFERENCES

[1] Khvoynitskaya, S. The History and Future of the Internet of Things. 2020.https://www.itransition.com/blog/iot-history.

[2] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization," Computer Networks, vol. 56, 3594-3608, 2012.

[3] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (iacac) for the internet of things," J. of Cyber Security and Mobility, vol. 1, 309-348, 2013.

[4] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, 2266-2279, 2013.

[5] M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," Perception, vol. 111, 2015.

[6] Shaikh, Eman, (2019), *Internet of Things (IoT): Security and Privacy Threats,*https://ieeexplore.ieee.org/abstract/document/8769539

[7] Rohe, R.C., (1997), *The Spatially-variant backprojection point kernelfunction of an energy- substraction Compton scatter camera for medical imaging*,https://ieeexplore.ieee.org/abstract/document/65645

[8] Jose, San, (2020), *Identify and Mitigate the Risk from VulnerabilitiesLurking in Millions of IoT, OT and IT Devices*https://www.forescout.com/research-labs/amnesia33/