Security Issues In IoT

Sreelakshmi Nair[1] ,
Asst. Professor, Department Of IT/ CS
Pillai HOC College of Arts, Science and and Commerce, Rasayani

Priyanka Sorte[2] ,
Asst. Professor, Department Of IT/ CS
Pillai HOC College of Arts, Science and Commerce, Rasayani

Babitha Kurup[3]
Asst. Professor, Department Of IT/ CS
Pillai HOC College of Arts, Science and Commerce, Rasayani

Abstract— — — Internet of Things is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that has the ability to transfer data over a network without requiring human or computer interaction. The Internet of Things (IoT) involves the rapid adoption of smart, adaptive and connected devices. IoT is rapidly being used in areas like health, utility, homes, transportation, industries etc. It brings benefits and reliability to consumers. The haste and its large scale connection however poses serious risks to consumers. These risks give rise to new attack vectors, new vulnerabilities and physical *destruction through remote access. The IOT brings implications on cyber security as these devices are connected through the internet.* In this paper, we review literature related to threats in the IoT and analyze the various models that could be used to overcome these threats.

Index Terms— computing devices, human interaction, vulnerabilities, attck vectors, cyber security

1 Introduction

In 1990 Kevin Ashton created the term the Internet of Things which is a worldwide dispersed network of objects that has the capability to connect with themselves and other computing devices.The concept of Internet of Things (IoT) has not been around for very long. However, there have been visions of machines communicating with one another since the early 1800s. The Internet of Things, as a concept, wasn't officially named until 1999[1]. One of the first examples of an Internet of Things is from the early 1980s, and was a Coca Cola machine, located at the Carnegie Melon University. The concept introduced was that the local programmers would connect to the refrigerator by Internet and can check if there was a drink available, and if it was cold, before making the trip.

Critical areas like temperature detection, security, home appliances, transportation and healthcare have seen an upsurge in the deployment of IoT enabled devices. Life has become much smarter by the adoption of IoT devices. It ensures that consumers acquire highly efficient services from the IoT devices that they deploy. Traffic signals, street lighting and public transport have become more efficient by the use IoT [2]. If we had computers that knew everything it would have made things much easier, we could easily use data they gathered without any help from us, we would be able to track and count everything and greatly reduce waste of time and cost. We could know when things need to be replaced or need to be repaired. Kevin Ashton believed Radio Frequency Identification (RFID) was a prerequisite for the Internet of Things. He concluded if all devices were "tagged," computers could manage, track, and inventory them. To some extent, the tagging of things has been achieved through technologies such as digital watermarking, barcodes, and QR codes.

However, evidence acquisition is very difficult as a sizable number of literature perused could not prescribe a comprehensive model that ensures the timely acquisition and reliability of evidence which is very critical for prosecution.

Security Issuues in IOT devices

Internet of Things (IoT) has made tremendous changes in user's expectation of a device. We demand for smart televisions, connected devices, and we need everything at our fingertips. But without proper security measures we are allowing intruders to take advantage of the weak points in our system[3]. Recent advancements in cloud computing, intelligent edge, artificial intelligence, and data analytics create many new opportunities for Internet of Things (IoT) devices to improve public safety. Recently, there were cases of smart televisions being used to spy on the users. *Are you watching TV or is your TV watching you?* There are a number of cybercrimes occurring on a daily basis in the field of IoT, among the various reasons one of the main reason for increase in cybercrime in this field is lack of security and privacy measures as well as lack of awareness among consumers to protect their devices from the threats and ambiguities related to IoT.

Types of Attacks on IoT Devices:

- ***UDP flood*** : As the name itself suggests this is a type of DDos attack where the user datagram protocol (UDP) packet is attacked. The main aim of this attack is to flood random ports on remote hosts which tend the host to repeatedly inspect the application listening at that port, and on finding no application reply with IPCM *destination unreachable* packet undermining the host resources which leads to the inaccessibility of the website. UDP flooding on one host leads to inferior performance of the host , at the same time if this attack takes place on two hosts it leads to extreme network snarl-up again affecting its performance. This attack can however not enable the party any additional access. Any person connected to the internet can cause denial of services[3].

- Malicious Code Injection Attack: The attack in-
- **Malicious Code Injection attack**: In this attack the attacker inserts some baleful code in the memory of the node. Generally, the firmware or software of IoT nodes are upgraded on the air, and this gives a gateway to the attackers to inject malicious code. Using such malicious code, the attackers may force the nodes to perform some unexpected functions or may even try to access all the data stored in IoT system.
- **False Data Injection Attack:** In this attack the attacker tries to capture a node in the IoT device and may use it to inject imprecise data in to the IoT system. This may lead to the generation of inaccurate results and may result in malfunctioning of the IoT application.The attacker may also use this method to cause a DDoS attack.
- Side-Channel Attacks (SCA): Apart from direct at-
- **Side Channel Attacks:** Other than the direct attacks on the nodes there are various side-channel attacks that may take place on IoT devices. This type of attacks can lead to leakage of sensitive data. The micro architectures of processors, electromagnetic emanation and their power consumption reveal sensitive information to adversaries. Side channel attacks may be based on power consumption, laser-based attacks, timing attacks or electromagnetic attacks.
- Eavesdropping and Interference: IoT applications
- **Eavesdropping and Interference:** IOT applications often consist of various nodes deployed in open environments due to which many IoT applications are susceptible to eavesdroppers. The attackers may eaves-drop and capture the data during different phases like data conveyance or authentication.
- Sleep Deprivation Attacks: In such type of attacks the
- **Sleep Deprivation Attacks**: In this type of attack the attacker tries to drain the battery of the IoT devices. This leads to a denial of service from the nodes in the IoT application due to a dead battery. This can be done by running infinite loops in the devices using malicious code or by artificially increasing the power consumption of the edge devices
- **DDoS/DoS Attack:** In this kind of attacks, the attacker floods the target servers with a large number of unwanted requests. This debilitate the target server, thereby restricting services to the legitimate users. If the attacker uses numerous sources to flood the target server, then such an attack is termed as DDoS or distributed denial of service attack. Such attacks are not specific to IoT applications, but due to the heterogeneity and complexity of IoT networks, the network layer of the IoT is prone to such attacks.

2 LITERATURE REVIEW

In the world of Internet of Things, millions of devices such as automobiles, smoke detectors, watches, glasses and webcams has the ability to get connected to the Internet to satisfy the users demands. Day by day the number of devices that has the capability to monitor and gather data is ceaselessly increasing. No doubt, the Internet of Things elevates human comfort and convenience, but it also raises serious issues related to security and privacy. It also creates significant challenges for digital investigators when they encounter Internet of Things devices in criminal scenes[4].

Due to the diverse nature of the IoT devices, the ways in which data is dispersed, aggregated and processed presents challenges to digital forensics investigators. New techniques are required to overcome these challenges and leverage the architectures and processes employed in IoT in order to gain access to this rich source of potential evidence. In coming years the growth of IoT can be accelerating but at the same time there is a need to take strong security measures of user's data.

The results of IoT device failures can be severe, therefore, the study and research in security issues in the IoT is of extreme significance. The main objective of IoT security is to preserve privacy, confidentiality, ensure the security of the users, infrastructures, data, and devices of the IoT, and guarantee the availability of the services offered by an IoT ecosystem.

3 IMPROVEMENTS AND ENHANCEMENTS REQUIRED FOR UPCOMING IOT APPLICATIONS

Personal computers (PC) and smart phones have a various security features built into them, e.g., firewalls, antivirus softwares, address space randomization, etc. These safety measures are not present in various IoT devices. There are various security challenges that the IoT applications are facing currently[4]. Some of the technologies which could help to improve the IoT devices are as follows.

Blockchain and IoT has a high impact on the IT and communication industry. These two technologies focus on ameliorating the overall transparency, visibility, level of comfort and level of trust in the users[5]. The IoT devices collects real-time data from sensors and blockchain yields the key for data security using a distributed, decentralized and shared ledger. The entries in the blockchain are chronological and time-stamped. Each entry in the ledger is tightly coupled with the previous entry using cryptographic hash keys.The key benefits of using blockchain in IoT applications are secure data storage,data encryption using Hash key and prevents data loss and spoofing attack. It also prevents unauthorized access of data.

Another technology called FOG computing could also be used for better management of IOT devices.
Fog computing allows computing, decision-making and action-taking to happen via IoT devices and **only pushes relevant data to the cloud.** Fog nodes make the communication in IoT application secure by providing cryptographic computations. Fog computing helps to prevent attacks like Man-in-the-middle attack, data transit attack and Eaves dropping.

Another technology that could be used as protection in IoT is Edge computing. Edge and FOG both are extensions of cloud computing. Edge computing brings computation and data storage closer to the devices where it's being gathered, rather than relying on a central location that can be thousands of miles away. This is done so that data, especially real-time data, does not suffer latency issues that can affect an application's performance. Edge computing provides security from data breaches, bandwidth and other safety issues.

4 Conclusion

In this survey we have discussed about the various threats in IoT based applications. We have also discussed about the different solutions that could be used by the upcoming IoT devices which may help to improve the security issues in existing IOT based devices.

secure future in cyber space. This study focuses on various technologies and tools used to minimize the cyber attacks on this digital world.

REFERENCES

[1]. https://www.dataversity.net/brief-history-internet-thing/

[2]. Davies, R (2015) The Internet of Things Opportunities and challenges, European Parliamentary Research Service, PE 557.012(), pp. [Online]. Available at:http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf(Accessed: 15th September 2015).

[3]. https://www.communicationstoday.co.in/services/cyber-crime-in-internet-of-things/

[4] https://link.springer.com/chapter/10.1007/978-3-319-99277-8_3

[5] Fardapaper-Blockchains-roles-in-strengthening-cybersecurity-and-protecting-privacy.