International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 04 | Apr 2021 www.irjet.net p-ISSN: 2395-0072

Need of security in IoT: A Review

Nikhil Pandey[1], Suniti Purbey[2]

[1]Student; Amity Institute of Information Technology, Amity University Chhattisgarh, Raipur, India
[2]Assistant Professor; Amity Institute of Information Technology, Amity University Chhattisgarh, Raipur, India

---

Abstract - The Internet of Things(IoT) is the next generation of communication. Using IoT we can encourage physical objects to create, receive, or exchange the data in a smooth manner. Various IoT application are used to automate the process and complete the task without any human interactions. The introduction to IoT significantly increased the comfort and efficiency and accuracy of doing a certain task in today's industry. But increase in the use of this technology also invited some major threats regarding security of IoT. So it is necessary to take care of high security, privacy, authentication, and recovery from attacks. So to accomplish the above task it is very necessary to make some important changes in the architecture of application in order to achieve maximum security possible. In this paper we have a descriptive review of many security challenges and source of threats in IoT is presented. After discussing the challenges, I have discussed various emerging and existing technology focused on achieving maximum security in IoT.

***Key Words*: Internet of Things(IoT), Threats, Security, Hacking, Measures**

1. INTRODUCTION

Internet of Things is uniting interconnected things, services, people and devices that can interchange, share the data to achieve objective in various areas and application. IoT can be executed in many fields including transportation, agriculture, medical, energy and many other fields that require objects to interact over internet to automate business projects efficiently without human interaction. Devices connected to IoT follows an Identity Management (IM) approach to be identified in group of different devices. A zone in IoT can be defined by an IP address, however within the zone each part has a specific ID by which it is recognized [1]. The IoT includes almost everything from smart home appliances to factory control devices and even automobiles. But unfortunately security has not been a very high concern until now. There has been a lot of conversation regarding hacking of devices and system to gain data etc. Unfortunately, many of these systems which are thought to be safe are still vulnerable. On daily basis the IoT devices are targeted by hackers and intruders, a study disclosed that 70% of the IoT devices are very vulnerable to attacks. Therefor a very strong mechanism is very much needed to secure the devices connected to internet [2].

2. DATA SURVEY ON INTERNET OF THINGS

The global market for IoT reached $100 billion in income for the first time in 2017, and predictions suggests that this figure will grow to around $1.6 trillion by 2025. With such a diagnosis, the technology is estimated to step far ahead than our imaginations. But with the increment in the popularity of IoT there will be a rise in security challenges too.

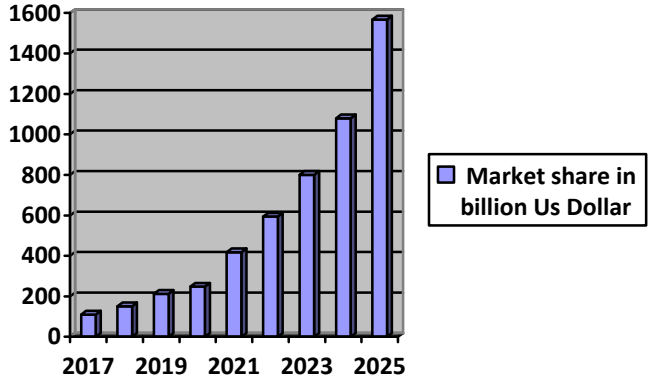

CHART 1 "Market Share of IOT" Source: Statista

In October 2016, a hacker found a breach in a particular model of security cameras. Nearly 3,00,000 IoT video recorder started to attack multiple social networks website and brought down twitter and other high profile platforms for almost two hours. This is an example of what can happen with device with poor security. [3]

3. TOP IOT SECURITY RISKS

The following security issues with IoT can be classified as a cause or effect:

3.1 Lack of Compliance on the part of IoT Producers

New Iot devices are launched almost every day, all with some unknown vulnerabilities, for example, many fitness trackers with Bluetooth remain visible after the first pairing, a smart refrigerator can expose our Gmail Login credentials. This is precisely one of the biggest security issues with IoT. While there is scarcity of universal IoT security Standards, Developers will continue to develop devices with bad security. [3]

The following are some security risks in IoT devices from manufacturers:

a. Weak, Easy to guess passwords
b. Hardware issues
c. Lack of a secure update mechanism
d. Old and unpatched embedded operating system and software
e. Insecure data transfer and shortage

3.2 Lack of user awareness

Over the time Internet user have learned how to avoid spam or phishing and perform virus scan on their PCs and securing accounts using strong Password, But IoT is a new technology, ad people still do not know much about it. While most of the risk are from manufacturer side, one of the biggest threat is user's ignorance and lack of awareness of the IoT functionality.

3.3 Lack of physical hardening

The lack of physical hardening can also cause IoT security issues. Even if Some IoT devices should be able to operate autonomously without any intervention from user, they need to be physically secured from outer threats. Many times these devices can be located in remote location for long stretch of time, and they could be physically tampered with, for example, Using USB flash drive with Malware. [3]

3.4 Botnet Attack

A single IoT device infected with malware does not pose any real threat; it is a collection of them that can bring down anything. To perform a botnet, attack a hacker creates an army of bots by infecting them with malwares and directs them to send thousands of request per second to bring down target. [3]

3.5 Hijacking Your IoT Devices

Ransomware has been names as one of the nastiest malware types ever existed. Ransomware does not destroy your sensitive files-it blocks access to them by way of encryption. Then the hacker who infected the device will demand a ransom fee for the decryption key unlocking the files. [3]

4. SECURITY MEASURES TO STOP SUCH ATTACKS

Some of the methods to secure the IoT devices are:

4.1 Run security tests on IoT source code

To generate a secure IoT devices, companies should start with the smallest part in their infrastructure. Security administrators can also bind cookies; these are randomized data string that application are coded to write into the stack just before the Instruction Pointer Register. [4]

4.2 Deploy access controls

Controlling access of IoT environment is one the most severe security challenges companies face when connection properties. Companies should first recognize the behaviors and activities that are deemed acceptable by connected things within the IoT environment, and then place controls that account for this but at the same time don't hinder process. [4]

4.3 Protect against IoT identifying spoofing

Hackers have become more dangerous than ever before and this can be a big threat to IoT. All IoT devices must have a unique identity. In the absence of a unique identity a company is at very high risk of being hacked from the microcontroller level.

5. CONCLUSIONS

So after many attacks in the past people realized that any device connected to internet are vulnerable to army of bots but that is the beginning. Still now Internet of things are not found in the same place, there are still many risks related to IoT now and more fill definitely emerge in coming times. We have seen a rapid growth in the industry of IoT, there are smart devices that we never thought will be available on internet. The world us transforming into a network of objects collecting our personal and sensitive information. So it is very necessary to take adequate steps regarding securing our devices to maintain security of IoT and protect the users and company's data from unwanted threats.

REFERENCES

[1] R. Vignesh and A. Samydurai, "Security on Internet of Things (IOT) with Challenges and Countermeasures", 2017 IJEDR | Volume 5, Issue 1 | ISSN: 2321-9939

[2] Mirza Abdur Razzaq, Muhammad Ali Qureshi, Sajid Habib Gill and Saleem Ullah, "Security Issues in the Internet of Things (IoT): A Comprehensive Study", International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017

[3]] Intellectsoft, "Top 10 biggest IoT security Issues", July 30, 2020

[4]] BOB Violino, "7 steps to enhance IoT security", 2019

[5] Ning Wang; Long Jiao; Pu Wang; Monireh Dabaghchian; Kai Zeng "Efficient Identity Spoofing Attack Detection for IoT in mm-Wave and Massive MIMO 5G Communication",