International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)
ISSN: 2456-236X
Vol. **05** Special Issue **01** | **2020**

Internet of Things: Broad Overview and Major Security Challenges

[1]Pradnya A. Vikhar, [2]Ashish D Vikhar

[1]Department of Computer Engineering, KCES's College Of Engineering and I T Jalgaon
[2]Department of Mechanical Engineering, Government Polytechnic, Jalgaon

ABSTRACT

In recent years,IoT (Internet of Things)becomes huge field of research and attracts many researchers. IOT has become an inseparable part of our regular life.In day-to-day world, its main use is to secure our device from unknown person who can try to access device and try to misuse that the device. IoT is the extension of Internet connectivity, includes embedded systems, various devices and other different forms of hardwareare connected through Internet connectivity.All these devices can communicate with each other using interaction over the Internet, and user can be remotely monitored and controlled various devices at a time.

Many IoT devices come with the old operating system and software therefore it is difficult for users to change the default passwords and if they do so,the password is not so strong. Now days, some of the IoT devices come with the operating system and inbuilt software which doesn't allows user to change default passwords. Therefore security becomes major challenge in front of IoT. Numbers of IoT devices are directly connected to the internet so that it can be directly monitored and if anyone try to hack or attacked the device then action can be taken. This paper focuses on the concept of IoT. Further it covers the security and challenges in the area of IoT.

KEYWORDS: IoT, IoT security, IoT challenges, solutions.

1. INTRODUCTION

IoT devices are becoming a part of the mainstream electronics culture and people are adopting smart devices into their homes, offices faster than ever [1]. According to researches the number of **IoT devices** that are active is expected to grow to 25 billion by 2020.Security is the area of effort as number of devices gets connected, connected devices and network in the IoT.The concept of a network of smart devices was discussed as early as 1982, with a modified Coke vending machine at Carnegie Mellon University becoming the first web connected gadget wasable to report whether newly loaded drinks were cold or not [1].

When in 1990's the wave of ideaIoT was again introduced, the number of security experts said there is a potential risk of unsecured device connected to internet [1]. The concept ofIoT become popular in 1999's,by Kevin Asthon, through Auto-ID center at MIT and related market-analysis publication. He thought Radio-frequency identification (RFID) as an essential thing for IoT at that time. In 2016, IoT developed when the customary field of implanted system, wireless sensor network, control framework, home and building robotization empowered to IoT. That is the merging of numerous organizations including continuous investigation, machine learning, group sensor and inserted framework [1].

2. CHALLENGES IN IOT SECURITY

As IoT is an growing and developing technology and is connected to internet, there is a possibility of being attacked. To secure devices it is very important. It is necessary have a good kind of simple security for all the IoT devices.Most of the time it is difficult for users to change the default password of devices which is given by product manufacturer and if they can some are not able to set a very strong password as it have a some default restriction measures applied on it.It is a major challenge to secure the IoT devices.There are too many fields, yet the security is still a big major issue. Building and home motorization, vehicle to vehicle correspondence, wearable gadgets and other preparing contraptions speak to most of the IoT correspondence that happens.

Most gadgets are little and are proposed for low power consumption use with confined accessibility. Thus the dealing with the farthest point and memory required to work out their assignments is similarly to a great degree compelled notwithstanding, some are ease and essentially unimportant. To make more security based and attack proof IoT enabled gadgets and applications, following things needs to be consider

Figure 1: IoT Major Security Challenges

2.1 **Testing and Updating**

Currently there are 23 billion IoT connected devices are available worldwide. This number will further rise up to reach 25 billion by 2020 and may be over 60 billion by the end of 2025. This emerging technology wave of new gadgets doesn't come without a cost. Actually one of the main problems that companies building these devices is that they are working too careless when it comes to handling of device-related security risks. Most of the devices and IoT products don't get enough updates,while some don't get updates at all. It means customer buy a product for become secure but actually when he first time buy it becomes insecure and eventually prone to hackers and other security issues related to the product. Unfortunately, most manufacturers offer firmware updates only for a short period of time or for single time, only to stop the moment they start working on the next headline-grabbing gadget[5][6].

2.2. IoT Malware and Ransomware

As the number of IoT connected devices continuously connected in the network, so there are number of malware and ransomware used to exploit them. Once traditional ransomware identify that while encryption they able completely lock out the user to acess the different devices and platform, so by doing hybridization of malware and ransomware that aim together different type of attack. The ransomware attacks mostly to focus on limiting and/or disabling device functionality and stealing user secure data at the same time. So as we need to increase the number of IoT devices we give chance to unpredictability in the regard of possible future attacks.

2.3 Data protection and privacy

Data privacy and security is largest issues in today's IoT interconnected world. Huge amount of data is constantly being used , transmitted, stored and processed by IT companies and various service provider by using a number of IoT devices, such as a for various home appliances and entertainment devices like smart TVs, speakers and lighting systems, connected printers, HVAC systems, and smart thermostats.

As IoT is based on strategies which respect users personal data privacy choices across a broad spectrum of expectations[2]. Butcommonly, all this user-data is shared between various companies also some time sold to other these things are violating user's rights for privacy and data security and further driving public distrust.While this is an important challenge, so strategies need to set dedicated compliance and privacy rules that redact and anonymize sensitive data before storing, transferring and disassociating IoT data payloads from information that can be used to personally identify us.

2.4 Hardware and Device Compatibility

While set up full-fledged IoT network, various hardware elements to be made use of; such as sensors, development boards, gateways, and more. Hence, user need purchase their hardware from the same manufacturer to avoid compatibility issues. Besides, most of the ttimeIoT solutions are integrated into legacy systems, this becomes a challenge due to different firmware and non-standard M2M protocols. This can especially be a significant barrier for a large scale IoT implementation, While working with several IoTstartups when a device failure happens, it becomes very difficult to get it replaced and this is especially a problem in places where IoT has began at starting point. Also devices should be able to function even when manufacturers discontinue their device or hardware support which means that the systems need to be upgraded regularly.

2.5 Data Authentication

In IoTdata authentication is the process of confirming the origin and integrity of data. Data authentication related to communication, messaging and integration. Data authentication has two more important elements i.e authenticating that you're getting data from the correct entity and validating the integrity of that data. IoT, enables a constant data transfer and sharing of data among various devicesandusers in order to achieve specified goals. In this type of sharing environment, authentication, authorization, access control and

non-repudiation are important to ensure secure communication. Sometime more than one user uses the IoT device that we need to provide proper authorization rights along with anonymity ,Secure session key establishment, Mutual authentication ,need to check certificates provided to the smart device is legal.For example suppose we have purchased an IoT device to regulate parking. Sometime the data might pop-up wrong and that making you believe there were only vehicles parked in the parking. The actual number might have been 15 vehicles. The No.10 Car driver might misuse the data and included in any wrong activities in your building[1].

3. CONCLUSION

Challenges prevent the securing of IoT devices and ensuring end-to-end security in an IoT environment. As the idea of networking appliances and other objects or in various devices is relatively new, while set up the IoT network still security, has not always been considered top priority during a product's design phase. As IoThas a nascent market, many product designers and manufacturers are more interested in getting their products to market quickly, rather than taking the necessary steps to build security in from the start. A major challenging issue with IoT security is the use of default passwords or sometime hardcoded, which can lead to security breaches.

4. REFERENCES

[1] S. Sicari, A. Rizzardi, L.A Grieco and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead”,Comput. Netw.76, 146–164, 2015
[2] Pradnya A. Vikhar “Internet of Things: Introduction, Issues and Challenges”, International Journal on Future Revolution in Computer Science & Communication Engineering ISSN: 2454-4248 Volume: 4 Issue: 10 113 – 116
[3] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac,“Internet of things: Vision, applications and research challenges,” Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, 2012
[4] https://securityintelligence.com/
[5] https://www.peerbits.com/blog/biggest-iot-security-challenges.html
[6] https://www.iotforall.com/challenges-in-iot-development/