IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

THE SECURITY CHALLENGES IN IOT

Mrs. Ashwini Satkar, **Mrs. Rohini Bhoware, Mrs. Ashwini Patil**, **Mrs. Nikita Deore**

Asst. Professor, Asst. Professor, Asst. Professor, Asst. Professor,
Computer Science Department,
Dr. D. Y. Patil ACS College, Pimpri,Pune-18, India

Abstract: From past decades the world is undergoing a extreme rapid transformation from isolated systems to Internet based enabled things capable of interacting with each other and after analysing this data extracting valuable information. Due to Internet of things there are creation of new connecting devices, which have implemented smart cities, smart homes etc. With this new approach of Internet of things it contains new kind of challenges from a security and privacy perspective. In this paper, we present major security issues for IOT.

***Index Terms* - Internet of things (IOT), Security Challenges and Security Solutions**

I. INTRODUCTION

The Internet of Things is modifying our physical world into a complex and robust system of connected devices on an unusual scale. Now a day's concept of IOT has become popular through some agent applications such as smart electric meter reading, intelligent transportation greenhouse monitoring and telemedicine monitoring. Generally IOT has major characteristics including intelligence, connectivity, dynamic nature, sensing, heterogeneous access, information processing, applications and services and additional components such as security and privacy.

IOT is becoming well-known concept in markets with its various applications such as Location Sensing and Sharing of Location Information, Remote Controlling, Environment Sensing, etc.

From the security point of view, the IOT is facing many more challenges. There are some securities issues which arise at the time of using IOT such as botnet attack, Firmware Hijacking, Encryption Attacks, ransom ware, lack of physical hardening etc. so, the new security and privacy problems are arising. We should focus on the research issues for confidentiality, authenticity, and integrity of data in the IOT.

II. SECURITY CHALLENGES IN IOT

The security of information and network should be equipped with properties like identification, confidentiality, integrality and undesirability. Different from internet, the IOT will be applied to the important areas of national economy e.g. intelligent transportation, medical service and health care etc. thus security needs in the IOT will be higher in availability and dependability.

Things interact with the Internet using IOT without our intervention. Such "things" are communicating with the Internet, update sent by a fridge regarding the food inside or our vehicle transmitting messages to the mechanic to inform its oil levels. T**echnology has not yet matured and it is not completely safe.** The entire IOT environment, from manufacturers to users, still has many security challenges of IOT to overcome such as:

- Manufacturing standards
- Update management
- Physical hardening
- Users knowledge and awareness

Lack of Manufacturing Standards

In market daily new IOT devices come out with new features, all with undiscovered vulnerabilities. Manufacturers do not spend more amounts of time & resources in checking security.

For example, after first pairing most fitness trackers with Bluetooth remain visible, Gmail login credentials can be exposed by smart refrigerator. This is one of the major security issues with IOT. Manufacturers will continue creating devices with poor security due to lack of universal IOT security standards. Manufacturers do not always have the "security" concept as the critical element in their product design process when they started to add Internet connection to their devices.

Some of security risks in IOT devices from manufacturers are listed below:

1. Weak, guessable, or hard-coded passwords
2. Hardware issues
3. Lack of a secure update mechanism
4. Old and unpatched embedded operating systems and software
5. Insecure data transfer and storage

IOT Security Problems In Device Update Management

Another risk is insecure software or firmware. Even though a manufacturer deliver a device with the latest software update, it is certain that new vulnerabilities will come out.

For maintaining security on IOT devices updates are critical. Once **new vulnerabilities are discovered, it should be updated** quickly. Unlike smart phones or computers that get automatic updates, some IOT devices continue being used without the necessary updates.

During backing up data to cloud, meanwhile device may suffer a short downtime. If the connection is not encrypted and the update files are unprotected, a hacker could steal sensitive information.

Lack of Physical Hardening

It also causes IOT security issues. Some IOT devices need to be secured from outer threats when it should be able to operate autonomously without any intervention from a user. Sometimes, these **devices can be located in remote locations** and can be tampered for example, using a USB flash drive with Malware. Users are also responsible for maintaining the security of IOT devices. If we do not provide adequate protection to a smart motion sensor or a video camera that sits outside a house, it could be tampered.

Users knowledge and awareness

Peoples have learned about how to avoid spam, phishing emails, virus scans on their PCs, and secure their Wi-Fi networks with strong passwords while using Internet. IOT is a latest technology & people are not aware of it. Still most of the risks of IOT security issues are on the manufacturing side, users and business processes can create bigger threats due to lack of user knowledge & awareness about security issues.

Botnet Attacks

If a single IOT device gets infected with malware it results in breakdown of system still it is not a big threat. In a botnet attack, a hacker infects IOT devices with malware & creates an army of bots. Hacker takes control over it and directs them to send thousands of requests per second to bring down the target.

For example a hacker could activate a cooling and heating system at the same time, so it creates spikes on the power grid, hackers can create a nation-wide power outage in case of a big-scale attack.

IOT Devices Highjacking

Ransomware is named as one of the most terrible malware types existed. It does not destroy your sensitive files but blocks access to them by encryption. Then, the hacker will demand a ransom fee for the decryption key for unlocking the files.

Data Integrity Risks In Healthcare

With IOT data is always moving which is being transmitted, stored and processed. It gets collected or extracted from external environment. It can be in the form of medical devices, smart thermostat, HVAC, TVs. These devices send the collected data to the cloud without using any encryption method. Using this hacker can **gain access to a medical IOT device, gaining control over it and being able to alter the data it collects.** A controlled device can be used to send false signals which in turn can make health practitioners take actions that may damage the health of their patients.

III. IOT SECURITY SOLUTIONS

Keep tabs on mobile devices

we must be sure about mobile devices like tablets are checked in and locked up at the end of every business transaction. If tablets are lost or misplaced then data and information kept on it can be accessed and compromised. We must ensure that a strong access password or biometric can be used, so that no one can get into a lost or stolen device. Use a security application that restrict certain apps that will run on the device, separate dealing and personal data and wipe dealing data if a device is stolen.

Implement automatic antivirus updates

We need to install software on all devices to protect against viruses so that hackers will not be able to access our system and data. We set up automatic antivirus updates to protect devices from a cyberattack.

Require strong login credentials

Most of people use the same login and password for every device which they use because it's easier for them to remember, easier for cybercriminals to hack as well. We must be sure that every login is unique for every employee and passwords must be strong enough. Always change the default password on new devices. Never re-use the same password across devices.

Deploy end-to-end encryption

Connected devices may share & transfer data from one point to another. So we need to encrypt data at every intersection.

Update & Install software on time

At the time of buying a device, always make sure that the seller provides updates and always apply them as soon as they become available. Implement automatic updates when possible.

Keep track of device available features and disable the unused features

Check the available features on our devices and switch off any that we don’t intend to use to reduce the potential attack opportunities.

Choose an expert cyber security provider

we want IOT to increase our business, not to hurt it. To help, many businesses rely on a reputable cyber security and antivirus provider to access vulnerabilities and provide unique solutions that prevent cyber attacks.

IV. RESULTS AND DISCUSSION

We have seen the emergence of IOT as a trend in the last few years. There are smart devices coming out that we never thought needed an Internet connection: smart toothbrushes, beauty mirrors, tables, pillows, beds, and the list continue to grow. The world is turning into a network of objects collecting our personal, sensitive information. If we do not have proper security, data hackers could steal information from these IOT devices. If we want our devices smart, we need them to be secure as well. As discussed above, we have covered many issues & its solutions of IOT devices.

REFERENCES

[1] https://www.intellectsoft.net/blog/biggest-iot-security-issues/
[2] https://www.kaspersky.com/resource-center/definitions/what-is-iot
[3] https://www.google.com/