Internet of Things and Cyber Security

Shahab Ghalib [1], Namit Gupta [2]

[1] *Student, College of Computing Science & Information Technology TMU Moradabad 244001, Uttar Pradesh, INDIA*

[2] *Asst. Professors, College of Computing Science & Information Technology TMU Moradabad 244001, Uttar Pradesh, INDIA*

[1]shahabghalib222@gmail.com

[2]namit.k.gupta@gmail.com

Abstract—

Internet of Things (IoT) devices are rapidly exist everywhere while IoT services are becoming pervasive. The Cyber Attacks are not new in the field of Iot, but it will be deeply interwoven in our lives and societies, it is becoming important to step up an take cyber defence seriously. Hence, there is a real need to secure IoT basically in the field of Cyber Security, which has consequently resulted in a need to comprehensively understand the threats and attacks on IoT infrastructure. This paper is written to classify the various type of threats, besides analyse and characterize intruders and attack facing IoT devices and services.

Keywords - Internet of Things, Background, Cyber-Security, Cyber-Attacks, Security Threats.

Fig.1. IoT Cyber Security

INTRODUCTION

Attackers are now using more sophisticated techniques to gain unethical access or we can say to target the victim's systems. Individually, the small scale businesses or large scale businesses are being impacted. So, all these firms whether IT (Information Technology) or non-IT firms have to understood the importance of Cyber Security and focusing on adopting all the possible measure to deal with the various cyber threats.

With the game up for cyber threats and hackers wo are trying to attack on a victim, organizations and their employees should take a step head to deal with them. As we would like to connect everything to the internet, this also increases the chances of various Vulnerabilities, Breaches and Flaws.

BACKGROUND

The Internet of Things (IoT) is an extension of the Internet into the physical world for the interaction with the various physical entities from our surroundings. Entities, devices and the services are the key concepts within the IoT domain, as depicted in the Figure 1. There are much type of meanings and definitions among various projects.

Therefore, it is necessary to have a good understanding of what IoT entities, an entity in the IoT could be a human, animal, car, logistic chain item, electronic device or a closed or open environment. Interaction among entities is made possible by hardware components called devices such as mobile phones, various sensors, actuators or RFID's tags which are able to allow the entities to connect to the digital world.

In the current state of technology, Machine-to-Machine (M2M) is the most popular application form of IoT. M2M is now widely employees in power, transportation, retail, public service management, health, water, oil and other industries to monitor and control the user, machinery and the

production processes in the global industry and so on.

According to the estimates M2M applications will reach 12 billion connections by 2020 and generate approximately 714 billion euros in revenue.

Besides all the IoT application benefits, several security threats are observed. The connected devices or machines are extremely valuable to cyber-attackers for several reasons:

i. Most IoT devices operate unattended by human, thus it is easy for an attacker to physically gain the access to them.
ii. Most IoT components communicate over wireless networks where an attacker could obtain critical data and information by eavesdropping.
iii. Most IoT components cannot support the complex security scheme due to low power and computing resource capabilities.

I. UNDERSTANDING IOT DEVICES AND SERVICES

We all know that IoT devices is changing industries across the board - from agriculture to healthcare to manufacturing and everything in between – but what is Iot, in a proper manner?

We can give a technical explanation of IoT in this way like "**The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction**." The Internet of Things is actually a pretty simple concept; it means taking all the things in the world and connecting them to the internet.

To be smart, a thing doesn't need to have a super storage or a supercomputer inside of it. All a thing has to do is to connect to super storage or to a supercomputer.

In the Internet of Things (IoT), all the things are being connected to the internet can be put into three categories:

i. Things that collected information and then sent it.
ii. Things that receive information and then act on it.
iii. Things that do both.

And these above all three categories have enormous benefits that feed on each other.

1. Collecting and Sending Information

This means the sensors. The sensors could be temperature sensors, motion sensors, moisture sensors, air quality sensors, light sensors etc. These sensors, along with a connection, allow us to automatically collect information from the environment which, in turn, allows us to make more intelligent decisions.

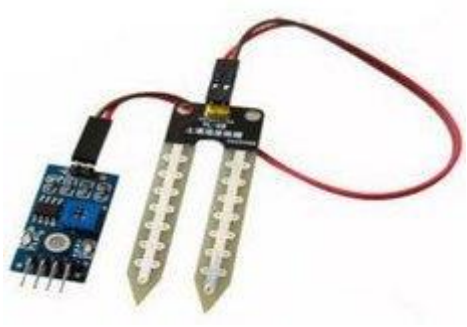

Fig.2. (Soil moisture sensor)

2. Receiving and Acting on Information

We all are familiar with machines that are getting information and then performing the task properly. Your printer receives a document and it prints it. Your vehicle (car) receives a signal from your car keys and doors open.

3. Doing Both

The sensors can be able to collect the data and information about the soil moisture to tell the farmer that how much need the water for a crop, but you don't actually need the farmer. Instead, the irrigation system can automatically turn on s needed, based on how much moisture is in the soil.

II. SECURITY IN IOT DEVICES AND SERVICES

Ensuring the security entails protecting both IoT devices and services from unauthorized access from within the devices and externally. Security should be securing our service which can be in any form, hardware resources, information and data, both in transition and storage. In this section, we identified three main key problems with IoT devices and services: Data confidentiality, Privacy and Trust.

Data confidentiality represents a basic problem in IoT devices and the services. In the IoT context not only user may access to data but also authorized objects. This requires addressing of two important aspects:

First, access control and authorization mechanism second authentication and identity management (IdM) mechanism. The IoT device needs to be able to verify that the entity is authorized to access the service.

Privacy is a major issue in IoT devices and service on the account of the ubiquitous character of the IoT environment. Entities are connected, and data is communicated and exchanges over the Internet on a network, rendering user privacy a sensitive subject in many research works. Privacy in data collection, as well as data sharing and management, and data security matters remain open research issue to be fulfilled.

Trust plays a vital role in establishing a secure communication when a number of things are communicating in an uncertain IoT environment. Two dimensions of trust should be considered in IoT. The trust in the interaction between the entities, and trust in the system from the user's perspective.

A) Attacks

There are five types of attacks in IoT which are as follows:

i) Physical attacks
ii) Reconnaissance attacks
iii) Denial-of-service attacks
iv) Access attacks
v) Attacks on privacy

B) Vulnerabilities

Vulnerabilities are the weaknesses which are exist in the system or its design that allow an intruder to execute commands, access unauthorized data, or conduct the Denial-of-Service attack.

The vulnerabilities can be found in a variety of areas in the IoT systems. In particular, we can say that it is a weakness in the system's hardware or software, weaknesses in policies and the procedures used in the systems and weaknesses of the system users themselves.

C) Exposure

Exposure is a problem or mistake in the particular system's configuration that allows an attacker to conduct information gathering activities. The one of the most challenging issues in IoT is resiliency against exposure to physical attacks.

D) Threats

A threat is an action that takes an advantage of security weaknesses in a system and has a negative impact on it. This can be originating from primary sources which are: humans and nature. Natural threats, like earthquakes, hurricanes, flood, and a fire could cause severe damage to the computer system.

III. PRIMARY SECURITY AND PRIVACY GOALS

Fig.3. IoT Security Targets

To succeed with the implementation of the efficient IoT security and the privacy, we must be aware of the primary security goals which are as follows:

i) Confidentiality

Confidentiality is an important aspect in the terms of security feature in IoT, but it may not be compulsory in some scenarios, where the data is presented publically, in the most cases that sensitive data and information must not be disclose or read by unauthorized entities which can be a human or a computer system, for example- it may be a patient data, private business critical information, government authorities data as well as security credentials and secret key, that are must be hidden from the unauthorized entities (Human or a machine).

ii) Integrity

The term integrity means to provide reliable services to IoT users; it is a mandatory aspect in the security property in most scenarios.

iii) Availability

A user of a device (or itself) must be able to accessing services anything, anywhere, whenever needed. There are much type of systems available which have different availability requirements.

iv) Accountability

When we want develop a security techniques to be a secure network, accountability add the redundancy and the responsibilities of certain actions, duties and the planning of implementation of network security policies.

CONCLUSION

Internet-of-Things (IoT) faces a number of threats that must be recognizes for the protected and the secures actions within the tasks. In this paper, IoT and Cyber Security we have discussed the various types of attacks, uses of the IoT technology in our day-to-day life also the security challenges and the security threats to IoT were introduced. The overall goal was to identify assets and the potential threats, attacks, vulnerabilities which we face by the IoT devices.

It's an overview which is the most important IoT security problems was provided, with the particular focus on the security challenges and the various aspects of the cyber security and the IoT devices implementations. Security challenges, like Confidentiality, integrity, availability, privacy and entity trust were identified.

REFERENCES

1) L. Atzori, A. Iera, and G. Morabito, "The internet of things: survey of the computer networks 2010.
2) S. Andreev and Y. Koucheryavy, internet of Things,2012.

3) https://elinux.org/images/f/f8/Common-Attacks-on-IoT-Devices-Christina-Quast.pdf.
4) https://geekflare.com/understanding-cybersecurity/
5) https://www.researchgate.net/publication/277718176_Cyber_Security_and_the_Internet_of_Things_Vulnerabilities_Threats_Intruders_and_Attacks
6) https://www.coursera.org/specializations/intro-cyber-security
7) https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4
8) https://blogs.harvard.edu/cybersecurity/2017/01/11/cybersecurity-and-the-internet-of-things/
9) YouTube
10) Book: Internet of Things.