International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 06 | June 2019 www.irjet.net p-ISSN: 2395-0072

Internet of Things (IoT), and the Security Issues Surrounding It: A Study

Pratik Vaity[1], Anushree Goud[2]

[1]Pratik Vaity (Student) & BVIMIT, Navi Mumbai
[2]Anushree Goud (Prof) & BVIMIT, Navi Mumbai

Abstract - *The Internet of Things (IoT) concept has gained popularity in modern years. At a theoretical level, IoT is the interconnectivity among our day to day devices. While various researchers have identified security challenges and problems in IOT, there is a lack a precise study of security issues in IOT. In this paper we focus on bridging the gap by giving attention to the challenges and problems of IOT Security.*

Key Words: Internet of Things, Security Issues, IOT Hardware, IOT Software**.**

1. INTRODUCTION

Internet of things (IoT) is referred as uniquely identified objects, and their virtual representation in an internet-based arrangement. This was proposed in 1998 [1]. The Internet of Things (IoT) concept has gained popularity in modern years. At a conceptual level, IoT refers to the interconnectivity among our everyday devices, along with device autonomy, sensing capability, and contextual awareness. IoT devices include personal computers, laptops, tablets, smartphones, PDAs, and other hand-held embedded devices. Device scan communicate smartly to each other or to us in today's world. Connected devices are equipped with sensors and actuators perceive their surroundings, understand what is going on and perform accordingly [2]

Fig.1 shows smart home with inter-connected things.

We cannot say that the IOT is the future of Internet because of various security it has. Till the Internet of Things has these security issues, it cannot be the future of internet.[3].

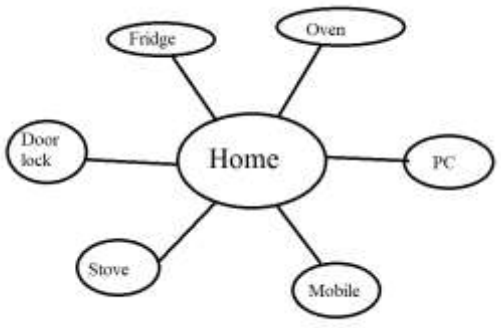

Fig.1 Smart home with inter-connected things

2. Encouragement:

To understand the importance of security and privacy issues in IoT, we first take a look at the present state of the IoT device in the world.[4]

Attackers have used household "smart" appliances to launch an IoT based attack, where everyday consumer gadgets such as connected multi-media centres, televisions, and refrigerators had been negotiated and used as a platform to send thousands of spam emails [5].

We argue that the incidents coupled with the insecurity of IoT device systems show a threat to the success of the emerging IoT. Hence, it is important to examine and understand the serious security issues in IoT. In this paper, we motivate and educate researchers about the multiple security issues and threats.

3. Background:

Prior to understanding IoT security issues, firstly we need to examine what are the components of the IoT network& how they work together. The IOT system comprises of five components.

Fig.2 shows connection between the following components.

-IOTDevices
-SensorBridge
-Controller
-IOTService
-Coordinator.

IOT Device. It consists of actuators, sensors, communication interface, OS, system software and pre-loaded applications. The main work of a smart device is to collect information using sensors and to carry out actions using actuators.

IoT services. Mainly, IoT services are hosted on cloud i.e. online that users can use IoT things anytime. The work of these include IoT process automation, device management, etc.

Sensor bridge. It acts as a bridge between the local IoT network and cloud services. It also works as a joiner between local IoT networks.

Controllers. IoT devices are controlled using the controllers.

Coordinator. A coordinator device behaves as a device manager. The main work of a coordinator is to keep an eye on health and work of the smart things.

4. Security Problems:

1. Hardware Based Limitations.
    a. Energy Constraint.

IoT devices are battery directed and are using CPUs which have less clock rate. Therefore, expensive algorithms that require very fast computational power, cannot be attached directly to such less powered devices.

b. Memory Constraint.

IoT devices are built with RAM that is limited and Flash memory compared to the old digital system (e.g. PC.), and make use of Real Time Operating System. They also run system software's. Therefore, security ideas must be memory active. However, old security algorithms are not made considering the memory efficiency, because the old digital system uses much more RAM and hard drive.

2. Software Based Limitations.
    a. Dynamic security patch:

Remote reprogramming is not totally possible for the IoT devices, as the operating system or protocol stack may not have the ability receiving and attaching new code or library.

b. Embedded software constraint:

IoT operating systems, have thin network protocol stacks and may lack enough security. Therefore, the security module designed for the protocol stack should be thin, but tough and should tolerate any fault.

3. Limitations based on network:
    a. Mobility:

Mobility is one of the main attributes of the IoT devices, where the devices join network without previous configuration. This mobility nature raises the need to produce mobility flexible security algorithms for the IoT devices.

b. Scalability:

The number of IoT devices is growing day by day and more devices are getting connected with. The global information networks. Latest security schemes don't have scalability property; therefore, such schemes are not proper for IoT devices.

c. Multi-Protocol Networking:

IoT devices might use a proprietary network protocol for communication in vast networks. At the same moment, it may communicate with an IoT service provider on the IP network. These multi-protocol communication characteristics make traditional security schemes not suitable for IoT devices.

5. Security Requirements:

There are many factors which need to be taken care of while computing a security solution for the IoT devices. The Security requirements that are expected to be met by the IoT security as given below.

1. Information security requirements.
a. Integrity:
Any condition can change the data and change the integrity of an IoT system. Thus, integrity ensures that the received data has not been tampered in transit.

b. Information protection:
The confidentiality of the stored information should be conserved. For example, an IoT network should not disclose the sensor readings to its neighbours.

C. Non-repudiation:
Non-repudiation is the guarantee that someone cannot rule out the validity of something. An IoT node cannot refuse sending a message it sends previously.

d. Freshness:
It is necessary to ensure the freshness of each message. Freshness assures that the data is recent and no old messages have been replayed.

2. Access level security requirements.

a. Authentication:

It enables an IoT device to ensure the identity of the node with which it communicates. It also requires to ensure that valid users get access to the IoT devices for administrative tasks.

b. Access control:

It is the act of ensuring that an authenticated IoT node accesses only what it is authorized to, and nothing else.

3. Functional security requirements.
    a. Exception handling:

Exception handling confirms that network is alive and keeps on serving even in the not so good situations like node compromise, malfunctioning hardware, software glitches etc. Hence it assures robustness.

b. Availability:

Availability ensures the survivability of IoT services to authorized parties when needed despite DOS attacks. It also ensures that it has the ability to provide a minimum level of service in the presence of power loss and failures.

6. Different types of attacks making IoT assets as targets.:

1. **Device property-based attack.**
   a. Low End Device Attack:

The contender can attack using IoT devices with similar capabilities and configurations to native network's IoT devices. A contender with malicious wearable device which contains malicious applications – might get unauthorized access to smart TV and launch different types of attacks which threatens communication, message integrity, privacy, etc. Here, capabilities of wearable device and smart home-devices are more or less similar.

b. High End Device Attack.

Here, the attacker uses more powerful devices – personal-computer, cloud PC– to get to access to native IoT network and device from anywhere and launch severe attacks.

2. **Access Level Based attack**

a. Active attacks:

When the aggress or does activities in order to disturb the normal functionality of IoT device, then those hateful activities are referred as active attacks. For example denial of service (DoS), etc.

b. Passive attacks:

In this case, it is alike to the official IoT device and performs unlawful activities to gather information from the trusted IoT devices and networks, however communication is not disturbed. This type of attacks is against the confidentiality of IoT.

3. **Information damage level Based attacks:**

a. Interruption:

Other than interruptions that may happen ordinarily like power outages or service shut downs, DoS attacks are used to cause resource exhaustion and hence make some services not available. Disaster recovery mechanisms are important to implement here.

b. Man in the middle attack:

This attack is a cyber-attack where a harmful impersonate or injects himself into a conversation between two nodes, impersonates both nodes and gains access to information that the two nodes were trying to send to each other. A man-in-the-middle attack gives access to a malicious actor to intercept, send and receive data meant for someone other, or not meant to be sent at all.

c. Eavesdropping:

An eavesdropping attack, that are also called as a sniffing or snooping attack, is an attack where someone tries to steal information from computers, smartphones, or other devices over a network. This attack takes advantage of network communications that are not secured so that the sent and received data cannot be accessed. These attacks are not easy to detect because they don't cause network transmission to appear to be operating not casually.

d. Alteration:

Alteration attacks involve misusing or destroying with our asset. If we access a document in a manner that is not authorized and alter the data it contains, we have affected the integrity of the data contained in the document.

e. Fabrication:

In this attack a fake message is injected into the network by an user who is not authorized as if the user is valid. This results in the loss of confidentiality, authenticity and integrity of the message.

4. **Protocol Based Attack:**

a. Deviation from protocol:

An attacker goes away from standard protocols (e.g. application protocols, networking protocols) becoming an insider and acts dangerously.

b. Protocol disruption:

An attacker might be sent inside or outside the network and perform not legal actions on standard protocols: synchronization protocol, etc.

7. CONCLUSION

In this paper, we have seen the most crucial security aspects of the IOT with focus on what is being carried out and what issues require further more research. We also perform a deep analysis of the problems of the inter-connected objects by looking for their limitation, energy limitation, resource limitation etc. This work analyses previous research problems and challenges and gives opportunities for future research in this field. In conclusion, we believe this survey has given a valuable contribution to the research community, by stating the current security problems of this very vast area of research and encouraging researchers interested in developing new protocols to address security in the background of the IOT.

REFERENCES

[1] R. H. Weber, "Internet of things – new security and privacy challenges," Computer Law & Security Review, vol. 26, pp. 23-30, 2010.

[2] Q. Zhou and J. Zhang, "Research prospect of Internet of Things geography," in Proceedings of the 19th International Conference on Geoinformatics. IEEE, 2011, pp. 1–5.

[3] Y. Yu, J. Wang, and G. Zhou, "The exploration in the education of professionals in applied Internet of Things engineering," in Proceedings

of the 4th International Conference on Distance Learning and Education (ICDLE). IEEE, 2010, pp. 74–77.

[4] "Internet of Things research study," 2014, accessed on 19-April- 2014.[Online]. Available: http://www8.hp.com/h20195/V2/GetPDF.aspx/ 4AA5-4759ENW.pdf

[5] "Proofpoint uncovers Internet of Things cyberattack," 2014, accessed on 19-April-2015. [Online]. Available: http://investors.proofpoint.com/ releasedetail.cfm?releaseid=819799