Security Challenges and Issues in IoT (Internet of Things)

Tushar R. Mahore[1], Asst. Prof. Pushpanjali M. Chouragade[2]

Government College of Engineering, Amravati, India

[1]mahoretushar@ooutlook.com, [2]tpushpanjalic3@gmail.com

***Abstract*— IoT (Internet of Thing) is the concept in which various objects are connected to each other and have the ability to exchange data over network. In near future more than 40 million various devices are going to get connected via internet, all these devices are going to interact among themselves. They share information, if this information contains sensitive data then Security is one of the aspect which cannot be ignored. This paper aims at the security challenges and issues related to IoT.**

Keywords—IoT (Internet of Things),

I. Introduction

Internet is system of interconnected computer networks, which has evolved over decades. At the starting of internet it is mostly defined as the World Wide Web which was a collection of linked HTML documents and was mostly static. Today the web we are using provides us the facility which enabled user participation and collaboration leading to a massive generation of a user generated content. Tiny embedded sensors are evolved and become more intelligent, such devices are uniquely identifiable when they are collaborate to mainstream internet. These devices are widely used in various applications such as Smart Home, e-commerce, e-health etc.

Internet of Things is the collection of interconnected devices, these devices communicate smartly. Connected devices equipped with sensors and/or actuators perceive their surroundings, understands what is going on and performs accordingly [1] [2]. IoT devices leads to various applications which in future provides more and more benefits in verity of areas. The basic thing to do for IoT devices is to interchange data over network, but doing this thing in secure way is the most important thing. As various devices are there in market having different architectures communicating over network is not an easy task, these devices must some provisions which ensures the security of sensitive data. Different IoT services are in market which works over cloud and ensures the secure transmission of data over network, but there is no specific architecture defined on which the concept of IoT is implemented.

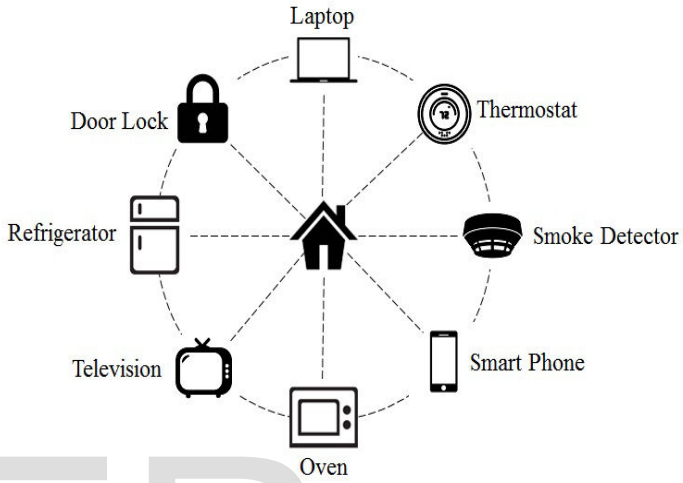

Fig. 1: Smart Home IoT application

Figure 1 shows the basic example in which connectivity among various devices is shown in Smart Home application of IoT. Here (see Figure 1) any one device can be compromised and used to get authentication of other devices over network. In IoT varity of devices are used and most of them do not come with security provisions, therefore new security problems get arises. We must focus on the security of IoT and implement accordingly into the devices, systems and protocols.

II. Work and Motivation

The concept of IoT is in existence from around 30 years, although the term was only coined 15 years ago [3]. To understand the security in IoT, we have to look at few aspects of IoT, understand various basic components included in it. Attacks on IoT devices are very simple and easy to conduct, there are several cases where researchers showed the successful takeover of smart things [4], [5], [6]. The basic attack technique is to compromise a single device in the network and get access to other devices.

Basically IoT includes the following components:

1. IoT Device
2. Coordinator

3. Sensor Bridge
4. IoT Services
5. Controllers

All of these components creates an environment which is basically referred as Internet of Things. Each of the component has a specific task to do, such as IoT Device is may be a combination of communication interface, software, sensor, actuator etc. Like that another is coordinator is actually a device which acts as a device manager, one or more smart things operate under single coordinator. Sensor Bridge also known as multi-protocol device /IoT gateway, it acts as a hub between local IoT network and the IoT services. IoT Services are the services over cloud which includes various functionalities according to the specific application. Controller is a device which operates other devices (e.g. smartphone, tablet).

III. Security in IoT

Security of data has been an important issue since the beginning of the communication networks. With the modernization and commercialization of the Internet, security worries expanded to cover personal privacy, financial transactions, and the risk of cyber-theft. In loT, security is inseparable from safety. Whether accidental or mischievous, interference with the controls of a car, pacemaker, or a nuclear reactor poses a risk to human life. Security must be addressed throughout the lifecycle of the device, from the initial design to the operational environment at all levels as discussed below, the three main levels are as follows

1. Hardware/Physical Level
2. Software/Communication/Protocol Level
3. Storage of the Data Level/Application Layer

At Hardware/Physical Level the devices must be secure, one of the main security issues includes physical security of sensing devices. This is because the low capacity, weak protection limited energy, the IoT cannot provide unified security protection system and is vulnerable to the invasion and attack.

Considering the other level i.e. Software/ Communication/ Protocol Level the risks is in existing loT communication network include illegal access, data eavesdropping, confidentiality, integrity, destruction, denial of service attacks, man-in-the middle attacks, virus attack [7].

At another level i.e. Storage of the Data Level/Application Layer stored data must be encrypted. Varity of data is get collected in IoT due to the different devices. Therefore it brings various network security aspects in front such as large data transfer requirements due to large number of nodes in IoT leading to network congestion and thus resulting in denial of service attack [8].

IV. Limitations and Requiremeents

A. Limitations

Employing conventional security mechanisms directly in the smart things is not straightforward because IoT devices are inherently resource constrained. The major security limitations are based on various aspects such as Hardware, Software and Network.

Hardware limitations are of different kinds such as computational and energy limitation, in which it is observed that due to the low computational power and energy of IoT devices it is not possible to implement large cryptographic algorithms into the device. Another hardware limitation which has to be considered is according to the memory point of view. IoT devices has limited RAM and flash memory according to traditional systems and use Real Time Operating System (RTOS) or uses lightweight version of General Purpose Operating Systems (GPOD), that's why traditional security algorithms are difficult to implement. Again tamper resisting packaging is also one of the hardware limitation.

Software limitations first of all includes the embedded software limitations in which IoT operating systems, which are embedded with the IoT devices, have thin network protocol stacks and might lack enough security modules. Therefore, the security module designed for the protocol stack should be thin, but robust and fault tolerant. Another software limitation is the dynamic security patch, installing a dynamic security patch on the IoT devices and mitigating the potential vulnerabilities is not a straightforward task. Remote reprogramming might not be possible for the IoT devices, as the operating system or protocol stack might not have the ability receiving and integrating new code or library.

Network based limitations includes lots of things such as mobility, scalability, multiplicity of communication medium, multiprotocol networking etc. all these defines various limitations based on network.

B. Requirements

For implementing IoT various are schemes are present in the market, the requirements for these schemes differs dependent on their levels, requirements such as Information security requirement, Functional security requirement, Access level security requirement and much more. Requirements states the thing we must take in consideration while implementing any IoT network.

Information security includes the integrity of information, which means the transferred data is not changed by the third party. The data transferred must be fresh, i.e. the data is recent not old data is replied. Anonymous data must not be present, each and every data must have an identity. Every node must have some technique for information protection which is necessary in data transferring.

Taking in consideration the functional requirements we have various concepts to take a look at, such as Reliability, Consistency, and Transfer Rate etc. Functional requirements shows how the components of network provides the functionality. The system must work in every case, such thing

we can call it as exception handling. Consistency is the way of working of the nodes in the IoT consistently, i.e. whenever there is a need or a request is made the node must be available.

Access level security is also one part which states there is a need to provide protection at various access levels, such as authentication, authorization etc. All these requirements plays very important role while implementing the security in IoT.

V. Security Complexity and Vulnerability

The complexity of security in IoT is way beyond of thinking, because of the devices used in IoT, which are different in every aspect from each other. One device may work on different protocol and other may on different, for example one device may use home network protocol and other may use industrial protocol, and they are connected to each other so the complexity of the security is much more. Parameters which makes the security task complex can be considered as they are proportional to each other. The parameters can be plotted as the 3D framework as shown in Figure 2 referred as the security landscape. As we go to the highest level in any direction the complexity get increased.

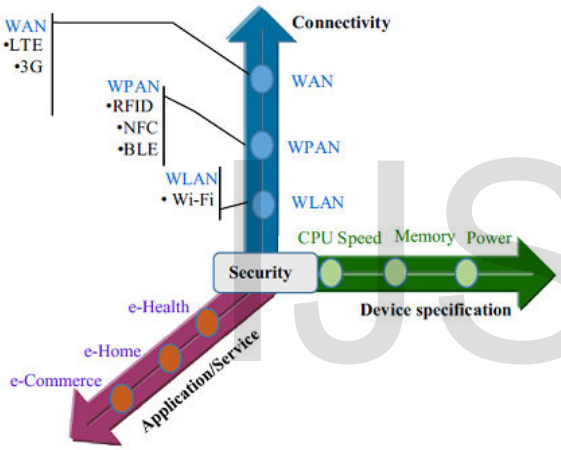

Fig. 2: Security Landscape [9]

Vulnerabilities are the open spaces where the injuries can be done by the attackers, there are various vulnerable areas in IoT. The major areas are where the attacks may occur are Local networks and Public Networks, here the attackers focus mainly and finds out the weak links for attack. The Open web application security project for IoT identifies ten critical security vulnerabilities in the Internet of Things [10]. Later, HP [4] found 50% of the commercialized IoT suffers from critical security weakness. The security points to be taken in consideration are end device security, communication security, and service security. These points are the important part of the security in which maintaining device security at every level is important, such as at sensor device level, storage device level etc. Then again in communication security lots of openings are there for attackers for example as low computational algorithms are used for security, the attackers can easily get information for communication networks. All of these are the open spaces for injuries to be made in the IoT.

VI. Attacks on IoT

Attackers basically focuses on the assets of IoT which includes energy, crypto-keys, trust, computation, protocol stack, stored data, software, OS, etc. all these assets are important for gaining access to the critical data. Attackers may be internal or external i.e. they might be inside the IoT network or outside the network. Attackers performs various attacks to gain unauthorized access to the devices residing in IoT assets and make the IoT services dysfunctional. Attacks can be performed on LLN based standard stack is listed in Table 1 and other than that various attacks which are based on IoT assets are listed in Table 2.

TABLE I: LLN stack attack

Attack Levels	Attack Types
Physical Layer	Jamming
	Tampering
Data Link Layer	Killer Bee
	Guaranteed Time Slot (GTS)
	Back off Manipulation
	ACK Attack
Network Layer	Black Hole attack on RPL
Transport Layer	Flooding
	DE synchronization
Application Layer	Using Command line exploit Tool

TABLE II: Attacks on IoT Assets

Attacks based on	Attack Types
Device Property	Low end device attack
	High end device attack
Adversary Location	Internal attack
	External attack
Access Level	Active attack
	Passive attack
Attack Strategy	Physical attack
	Logical attack
Information Damage Level	Interruption
	Man in middle
	Eavesdropping
	Alteration
	Fabrication
	Message reply
Host Attacks	User compromise
	Software compromise
	Hardware compromise
Protocol Attacks	Deviation from protocol
	Protocol Disruption

Above tables indicates the different attacks in various areas. These attacks indicates the things in which the attackers are interested.

VII. Directions for Improving Security

This section refers to the research directions to be taken in consideration while it comes to the security in IoT. Here some of the issues are mentioned which may not or poorly

addressed by the researchers. Some of the issues are, trust management in which the device have to allow the trusted party to be the part of the IoT network. Another one is end to end security, there are two types of communication in IoT network i.e. H2T (human to thing) and T2T (thing to thing), providing security to these connections are important.

Other issues are as, fault tolerance, identity management, energy efficient security, key management, group membership, and security of handling big data. All these issues are to be taken in consideration for implementing secure IoT network.

VIII. CONCLUSION

In this article we have gone through the overall study of IoT architectures and the issues related to them. We have related the IoT with real life situations and observes the issues and challenges we are facing in implementing the IoT. We believe that this survey may help research committees in their work. This work helps researchers to build more secure techniques in the way of implementing IoT.

REFERENCES

[1] 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.

[2] 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.

[3] J. Chambers, "What does the internet of everything mean for security?" World Economic Forum, Davos, Switzerland, January 21, 2015.

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

[5] C. Cerrudo, "Hacking us traffic control system." 2014, accessed on 12-April-2015. [Online]. Available: http://blog.ioactive.com/2014/04/hacking-us-and-uk-australia-france-etc.html

[6] Y. Oren and A. D. Keromytis, "From the aether to the ethernet–attacking the Internet using broadcast digital television," in Proceedings of the 23rd USENIX Security Symposium, San Diego, CA, USA, 2014, pp. 353–368.

[7] Lianshan Yan et el., "Construction and Strategies in loT Security System", Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing , vol., no., pp.1129, 1132, 20-23 Aug. 2013 doi: 1O.1109/GreenCom-iThingsCPSCom. 20 13.195

[8] Chen Qiang et el., "Research on Security Issues of the Internet of Things", International Journal of Future Generation Communication and Networking Vo1.6, No.6 (2013), pp.l-1O doi: dx.doi.orgll 0.14257/ijfgcn.20 13.6.6.0 1

[9] Md. Mahmud Hossain, Maziar Fotouhi, Ragib Hasan "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things" 2015 IEEE World Congress on Services 978-1-4673-7275-6/15 2015 IEEE DOI 10.1109/SERVICES.2015.12

[10] "Open web application security project for internet of things," accessed on 12-April-2015. [Online]. Available: https://www.owasp.org/index.php/ OWASP Internet of Things Top Ten Project guage citation [6].