Counterfeiting Threats in IoT

Kayiram Kavitha, R.V.S Lalitha, T.V.Suneetha, D.Usha Sree

Abstract: ***With the advent of digitalization the entire world is greatly connected to the digital world. The modern gadgets are equipped with Internet-connectivity encouraging web browsing. Due to rapid mobility of devices numerous applications are launched while these come with lot of advantages and wide spread of information they are prone to attacks too. These attacks on IoT devices compromise the security & privacy of the user. The attackers get entry and invade through the data, inject malware, or schedule attacks on neighborhood. In this paper, we present the attacks and the vulnerabilities in IoT, along with the preventive and counter measures to be adapted to safeguard from attacks. We compiled a brief outline of the security breaches and the latest block chain application to implement security in IoT devices as work for future direction.***

Keywords : security, IoT devices, Block chain, threats, preventive measures.

I. INTRODUCTION

We are spectating a drastic change in life style. The technology is developing rapidly we witness a global exposure to our activities. Internet of Things (IoT) is interconnection of devices ranging from desktop to streetlights where every electronic device operated with some power source can be connected to form a network instantly thus each such device will have a unique IP address. As IoT has emerged in every walk of life ranging from Internet of Medical Things (IoMT), Internet of Battle Things (IoBT), and Internet of Vehicles (IoV) and so on.

With the evolution of Internet, wireless devices, Radio Frequency Identification (RFID), Wireless Sensor Network Technologies, Internet-of-Things (IoT) [1] has emerged as a concept to enable communication between heterogeneous devices (things or objects like sensors, actuators, RFID tags etc.). These IoT devices operate without a screen or user interface in a resource constrained environment usually dedicated to a single task. There are many constraints in IoT like battery power, memory space, and security as these devices are connected instantly with anything, anyplace and anytime. In contrast to traditional internet the IoT device is intelligently gathering, analyzing the human behavior [2]. The high connectivity of these intelligent objects leads to serious security issues.

Many IoT applications can be found in smart home, smart city, smart campus, smart grids, medical equipment, connected vehicles etc. According to Gartner report [3] the number of smart phones and tablets will reach up to 7.3 billion units by 2020. As a tremendous growth is observed in IoT, the communication network has challenges in terms of huge amount of data, processing power with energy consumption, security threats, and efficiency of cryptographic algorithms.

With the growing needs of the market and the technological evolution the manufacturers are in a competition for business and scooping up the new technology overlooking the security threats. As the IoT Manufacturers have not implemented a robust security system, the security experts have warned of the potential risks [4] of unsecured devices.

Now, we brief the security attacks on IoT devices reported in the past. There are many incidents of data breaches and attacks in the past and still happening. Many websites including Twitter, Netflix, Spotify, Airbnb, Reddit, Etsy, Sound Cloud and the New York Times, were reported inaccessible by users due to Distributed Denial of Service (DDoS) attack [5] through IoT devices on 21st October 2016. A botnet [6] consisting 100K compromised IoT devices launched a series of DDoS attacks that set records in attack bitrates in the year 2016. With rapid growth in IoT, the vulnerability and security threats for these devices have become a major concern. Some well-known remedies include firewalls and Intrusion Prevention System (IPS) [7]. The IPS monitors the geography using many machine learning techniques [8]. But, IoT require network connectivity to work and is too expensive and complex to maintain. Hence, light weight protocols are developed to maintain the internet connectivity. This makes it more vulnerable and easy for hacker.

It has been studied that the IoT market grows from 27 billion devices to 125 billion devices by 2030. This rapid growth calls for the device manufacturers to rush up and capture their sales. The device vendors are hence emphasizing on making profits ignoring the vulnerability and associated threats.

This gave a huge opportunity for attackers to intrude into the network. Many users are falling prey to such attackers and are losing trust in technology. Hence we intend to outline the attacks a detailed counterfeiting solutions using Block chain technology.

Smart city, smart home, smart TVs are rapidly flourishing their presence in the community, so is the increasing concern for their security as shown in Figure 1. Many of these devices come with a built in firewall, antivirus etc. But the user behaviour and cookies pose a privacy threat which is often over looked by the consumer.

Revised Manuscript Received on October 15, 2019.

Dr. Kayiram Kavitha, Associate Professor, Dept. of CSE, Gokaraju Rangaraju Institute of Engineering and Technology, Bachupally, Hyderabad, Telangana, India

Dr. R.V.S.Lalitha, Professor, Dept. of CSE, Aditya College of Engineering, Surampalem, Kakinada, A P, India

T.V.Suneetha, Assistant .Professor, Dept. of CSE ,Gokaraju Rangaraju Institute of Engineering and Technology, Bachupally, Hyderabad, Telangana, India

D.Usha Sree, Assistant Professor , Dept. of CSE ,Gokaraju Rangaraju Institute of Engineering and Technology, Bachupally, Hyderabad, Telangana, India.

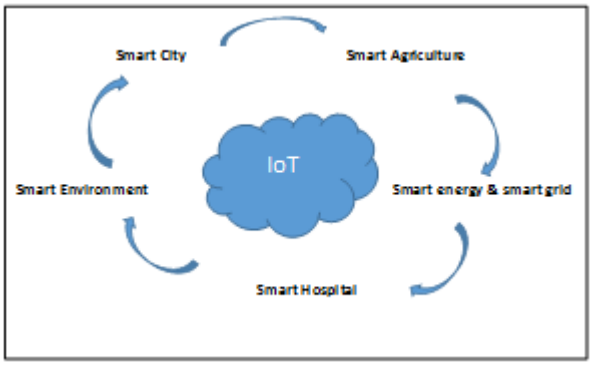

Figure 1. IoT for smart life

Rest of the paper is organized as follows. The Section 2 deals with the related work, Section 3 gives the proposed methodology, Section 4 presents the challenges, the block-chain technology is given in Section 5 and conclusion is presented in Section 6.

II. RELATED WORK

As the IoT devices are operated in a resource constrained environment, conventional security mechanisms fail due to their complicated algorithms requiring more computational power and battery power too. The authors in [9] have focused on software attacks as the most vulnerable to the IoT devices. This exploits the vulnerabilities in the system which include injecting worms, virus, and malicious code like trojan horse programs. The attacks such as monitoring the device traffic, eavesdropping are passive attacks. While active attacks include denial-of-service attacks and node malfunction.

According to research in [10], the following areas have high business value in IoT security: IoT network security, IoT encryption, IoT authentication, IoT security analytics, and IoT API security. As the focus is on IoT network security, the related research work is presented. One of the existing solutions is a smart firewall, CUJO [11] that connects to home routers. This can safeguard all IoT devices connected to its network. It is suitable only for home networks where Local area networks protocols are sufficient.

The authors in [12] worked for IoT security which uses some security policies that can be enforced. But, this cannot be used to prevent the vulnerabilities in IoT devices.

The authors in [13] have presented threat analysis of IoT and uses Artificial Neural Networks (ANN) to combat these threats. A type of ANN is trained using internet packet traces under supervised learning to perform threat analysis and compose threat patterns. This will be useful to safeguard the device from attacks in future.

III. PROPOSED METHODOLOGY

The main objectives are to:

- Design and deploy a vulnerability detection framework for remotely deployed IoT devices.
- Develop attack preventing strategy as part of mitigation policy.
- Implement cloud service for cost effective device monitoring.

It is proposed to explore attack detection frameworks to understand their suitability for remote IoT devices. While there have been several similar efforts made earlier, they have mostly been in static environments and thus may not be too challenging. The aim of the project is to design suitable mitigation policy over the cloud to maintain the IoT device security. It is proposed to set up a remote deployment of the IoT device with minimal configuration and maintain remotely with security policy hosted as a cloud service.

Here is the reason and explanation about why the traditional security mechanisms fail in IoT framework. Traditionally security methods fail in IoT era for the following reasons:

- IoT devices are tiny and have small processor for simple operations.
- IoT devices do not react to the previously unknown attacks
- Due to heterogeneous devices in IoT networks
- As these devices are operated in remote environment and they have limited power resource. Hence the security mechanisms and cryptographic algorithms are difficult to implement.

The challenges faced for security in IoT domain is highlighted in Section 4.

IV. CHALLENGES & RESULTS

As the IoT devices are increasing rapidly in number the devices are unable to establish security association in the user's trust domain.

- The device identification has also become a major concern.
- Lack of unified security protocols.
- Each of these devices have a varied vendor specific solutions.
- There is no standardization of protocols and framework due to heterogeneous devices on IoT network.
- A Unique management framework is absent to identify devices in the user domain.
- Malware and attackers are also becoming sophisticated and are way for ahead of the traditional intrusion detection systems.
- Many IoT scanners do exists in real time but the attackers are able to bypass these by compromising the internal devices in the network and launching attacks through them.

With these challenges, the block-chain technology emerged as a boon to the security community. We brief about this in the next Section.

V. BLOCK-CHAIN TECHNOLOGY

Initially block-chain technology was developed for tamper proof record keeping. But, as the technology advances, it emerged to be a better security solution for IoT. In fact block chain uses the fundamental concepts of security like hashing, cryptographic algorithms to maintain integrity and confidentiality of records at block level. Each block contain the individual information and is hashed to ensure security. Two or more blocks are connected together to form a chain. Thus the name is block chain.

Here the security need to be enforced in IoT devices and the various issues pertaining to the cryptographic algorithms, key size, etc. need to be elevated using the block chain technology to achieve high reliability, integrity, non-repudiation. This is on-going research topic to use block chain technology in place of traditional security mechanisms for IoT.

VI. CONCLUSION

As a future work, there is a lot of research opportunity to develop mitigation framework for other devices like ATM machines, driverless-vehicles etc which are prone to a lot of vulnerabilities at present. Although design standards exist in this area, IoT device vendors don't adhere to the design standards. Hence, there is opportunity for patentability too. This issue is overlooked in the current scenario of rapid technology upgrade. Some future vision is to develop light weight framework to give the user choice to plug and use it for any device.

REFERENCES

1. O'Neill M. Insecurity by design: Today's IoT device security problem. Engineering. 2016 Apr 5;2(1):48-9.
2. Saif I, Peasley S, Perinkolam A. Safeguarding the Internet of Things: Being secure, vigilant, and resilient in the connected age. Deloitte Review. 2015;17.
3. Stamford C. Gartner says the internet of things installed base will grow to 26 billion units by 2020. Retrieved April. 2013 Dec;15:2018.
4. Margaret Rouse, "Iot security (internet of things security)," http://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security, 2013.
5. Lam B, Larose C. How did the internet of things allow the latest attack on the internet.
6. Kolias C, Kambourakis G, Stavrou A, Voas J. DDoS in the IoT: Mirai and other botnets. Computer. 2017 Jul 7;50(7):80-4.
7. Kasinathan P, Pastrone C, Spirito MA, Vinkovits M. Denial-of-Service detection in 6LoWPAN based Internet of Things. In2013 IEEE 9th international conference on wireless and mobile computing, networking and communications (WiMob) 2013 Oct 7 (pp. 600-607). IEEE.
8. Shabtai A, Moskovitch R, Elovici Y, Glezer C. Detection of malicious code by applying machine learning classifiers on static features: A state-of-the-art survey. information security technical report. 2009 Feb 1;14(1):16-29.
9. Hadar N, Siboni S, Elovici Y. A Lightweight Vulnerability Mitigation Framework for IoT Devices. InProceedings of the 2017 Workshop on Internet of Things Security and Privacy 2017 Nov 3 (pp. 71-75). ACM.
10. Kayiram Kavitha, Polsani Rajashree Rao, Sreeja Tummala, Gajarla Vasavi, and Dr.R.Gururaj, Dual Tree Data Routing Scheme for Wireless Sensor Networks, Third International Conference on Advances in Information Technology and Mobile Communication, AIM -2013, 26-27, April 2013, Bangalore, India.
11. Kayiram Kavitha, Vinod Pachipulusu, Sreeja Thummala, R.Gururaj. Article: Energy Efficient Query Processing for WSN based on Data Caching and Query Containment, in International Journal of Computer Applications, Vol. 89, no. 19, Page no. 4-8, March 2014, Published by Foundation of Computer Science, New York, USA.
12. Hodo E, Bellekens X, Hamilton A, Dubouilh PL, Iorkyase E, Tachtatzis C, Atkinson R. Threat analysis of IoT networks using artificial neural network intrusion detection system. In2016 International Symposium on Networks, Computers and Communications (ISNCC) 2016 May 11 (pp. 1-6). IEEE.
13. Sharma D**,** Kavitha K, Gururaj R. Article: Estimating Node Density for Redundant Sensors in Wireless Sensor Network, in International Journal of Sensor Networks and Data Communications, Vol.4, Issue 2 no.127, November 2015, Published by OMICS International.
14. R.V.S.Lalitha, K.Kavitha, N.V.Krishna Rao, G.Rama Mounika, V.Sandhya, Smart surveillance using Smart doorbell, International Journal of Innovative Technology and Exploring Engineering, Volume-8, Issue-8 June, 2019.