Different Dimensions of IOT Security

Narendra Sharma, Reitwick Prakash, E. Rajesh

Abstract: ***IOT is wirelessly connecting things to the internet using sensors, RFID's and remotely accessing and managing them over our phone or through our voice. IOT uses various communication protocols such as Zigbee, 6LowPan, Bluetooth and has bi directional communication for exchange of information. The database for IOT is cloud which is also vulnerable to security threats. The increasing amount of popularity of IoT and its pervasive usage has made it more recurrent to prominent cyber-attacks such as botnet attack, IoT ransom ware, DOS attack, RFID hack. The challenges faced by IoT are to stop hackers from stealing data, having unattended access to the device and performing malicious activities. There are many techniques which can be used to secure IoT devices such as using a secure encrypted Wi-Fi network, using digital signature for authenticity, updating to latest patches, installing Intrusion Detection System. We'll also be assessing various IoT devices and threats associated with them in real time environment and the level of harm these threats can cause to the device if they are not properly mitigated or eradicated.***

In this paper we'll also be addressing different types of risks associated with different IOT devices and approaches to solve the security and privacy issues.

Keywords: Internet of Things, Cyber security, IoT Threats.

I. INTRODUCTION

1.1 Need of IoT Security

Several techniques like smart electricity grids, e-Heath, smart home, smart driving, auto medicine suggestions, smart city and machine to machine communication concept of IoT security are dependent on four important facts, i.e. sensors, applications and services, way of information processing and heterogeneous access along with the security [1].

Unique identifier is used in the concept of Internet of Things (IoT) for object availability for some other objects. These objects are one and only devices, which have ability to communicate over a network, also enable direct communication.

It is a latest feature of NGN (Next Generation Network). which allows traffic by network infrastructure, which is used to provide safety over a critical network. It is predicted by CISCO, that 15 billion devices are currently in 2019 and by the end of 2020, it will be approximately 50 billion. A lot of problems are faced by industry here, after applying Internet of Things (IoT) security, can provide many services in secure manner [2].

In security system of Internet of Things (IoT), there are many complications due to their undefined parameters, high dynamic and constant changes due to mobility. Internet of Things (IoT) system can also include some "Objects" or "Things", which are not designed for connecting to Internet. Internet of Things (IoT) system and part of it also may be physically vulnerable and controlled by other parties. Attacks are too much onerous to protect in favor of Internet of Things (IoT) [3].

In addition, scalability of "Human Interaction" is also not defined, makes too much difficulty for security analyst for Internet of Things (IoT) security. Addressing such kind of issues and as well as representing security solution for Internet of Things (IoT) security [3].

Internet of Things (IoT) is one of the biggest growing industry, a lot of devices and technologies are too much popular and critical. That is why, IoT devices are aim of attackers. As we take an example of smart meter, production of this IoT device is growing day by day. Nowadays production of smart IOT device is approximately 12 billion. Some techniques are developing of security analysis of IoT devices, can say remotely accessibility and installing software remotely. These points are easily accessible by any potential attacker, and also attracts to the attackers so we can say that Internet of Things (IoT) devices should be secured and full of privacy, it may increase cybercrime [4].

1.2 Issues with the challenges in the Internet of Things

In the European market, size of Internet of Things (IoT) devices is about to be approximately € 2,42,222 million by the end of 2020. Rise in the size of Internet of Things (IoT) devices is leading in Internet of Things (IoT) application development, comes with the security challenges. in this era of Internet of Things (IoT) devices, Manufacturers think about only and only production of Internet of Things (IoT) devices. Manufacturing companies thinks that who will be able to get latest device first, according to demand of the user.

Revised Manuscript Received on January 15, 2020

Correspondence Author

Narendra Sharma, M.Tech(CSE), School of Computer Science and Engineering, Galgotias University, Greater Noida, India.

Reitwick Prakash, School of Computer Science and Engineering, Galgotias University, Greater Noida, India.

Dr. E. Rajesh, Associate Professor, School of Computer Science and Engineering, Galgotias University, Greater Noida, India.

Table 1.

Issues	Description
Inadequate testing	Now days, there are approximately 23 billion devices, currently working in the world. Manufacturing companies do not focus on the testing of Internet of Things (IoT) devices and devices never get updates of security for the privacy.
Brute force and old passwords	Government says to the manufacturers, not to sell devices with default username and password, it attracts attackers to attacks. This type of weak credentials makes Internet of Things (IoT) devices in danger.
Internet of Things (IoT) malware and ransomware	Malware and ransomware, aim to combination of many types of attacks. Ransomware attacks potentially focus on stealing data of any user.
Data (Mobile, Cloud and Web) security and privacy concern	Data security issues indicate towards interconnected world, connected with Internet of Things (IoT) devices and harnessed by Internet of Things (IoT) devices.
Artificial intelligence and Automation	Billions of Internet of Things (IoT) devices, is a very difficult task to manage data collection. It increases security issue.
Remote vehicle access	Hijack of a car or any other vehicle is a threat that is possessed by the Internet of Things (IoT), it is a big challenge in Internet of Things (IoT).
Untrustworthy communication	Internet of Things (IoT) devices send messages without of any encryption, biggest Internet of Things (IoT) security risk.

II. IOT 3- LAYER ARCHITECTURE

According to many researchers IOT follows a three-layered architecture as given below [5]-

- Perception Layer- It acts as the base layer of IOT which consists of RFID sensors, ZigBee protocol, mobiles and other devices which obtain initial information from the environment and process them to the Network Layer [5].
- Network Layer- The network layer consists of the communication protocols such as 6LowPan, Bluetooth, Wi-Fi which are used to transfer information further to the Application Layer [6].
- Application Layer- This is the final layer of the IOT architecture in which the information finally reaches the IOT device [6].

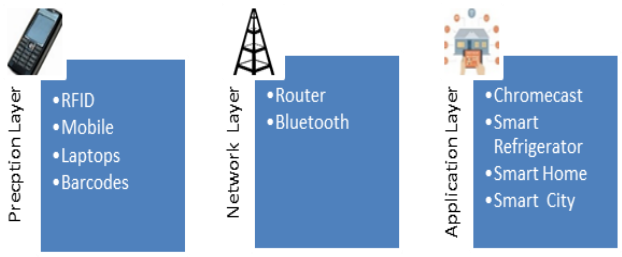

Fig. 1.

1.3 Threats and Solutions

Table 2.

. Layers	Threats	Threats explained	Solution
Perception Layer	Eavesdropping [7]	It is a real time attack in which any ongoing event such as video call, text message is obstructed by a hacker.	By installing intrusion detection system [6].
	Replay Attack/Playback attack [5]	The information sent over network is intercepted and stored by the attacker which he can transmit later.	Using timestamps and one time passwords [7] and session keys.
	Node Capture [7]	Attacker gets full control over main node such as gateway. It may make malicious node or leak all information in the node [5].	Encryption, authentication And access control
Network Layer	Denial of Service [8]	This attack overloads the network with requests thus causing it to shut down and cannot be accessed even by authorized users.	Using AES encryption or configuring a firewall which rejects ping requests [9].
	Man-in the Middle Attack [7]	The attacker acts as a middle man who obstructs the communication and acts as original sender thus making the receiver think the communication is from original sender.	Using high level encryption and digital signatures.
	Unauthorized access [6]	Anyone makes over the network accessing the IOT device.	The IOT device should also have proper authentication so that it cannot be misused
	Storage access attack [7]	Accessing the cloud storage where all information of the device is being stored. This can lead to manipulated results by the device.	2-way authentication for logging in and alert for unauthorized access.
Application Layer	Malicious Code Attacks [7] [6]	Attacks through running malicious codes.	Checking firewall at runtime.
	CSS [7]	Attacker runs malicious codes on the web browser of the victim by adding malicious code on legitimate websites thus allowing him to tamper the application.	Sanitizing user input and validating the input by the web page.
	Botnet	The hacker highjacks network of devices by Botnet and can control them from a single access point.	Using Proper Router encryption such as WPA2.
	SQL injection	Logging into the IOT device using an SQL script.	Using parameterized statements in the logging page code

2 Smart City

. Internet of Things has already become ubiquitous and now with changing times smart cities are making ways to ease of people's life. Smart cities would consist of IoT devices such as Smart homes, Smart Grids and many other legacy systems which have now been integrated with IoT. Smart city is made up of 3 Layers as stated in Deloitte white paper [10]-

- Edge Layer- Contains front end devices such as Mobiles, Sensors etc.
- Communication Layer- Uses Bluetooth, NFC etc. For bi directional communication.
- Core Layer- This layer process data and identifies the logic from the data.

While setting up a smart city there may be old systems which need to be integrated with IoT and this may contain hidden risks which need to dealt with by making security policies and procedures [10].

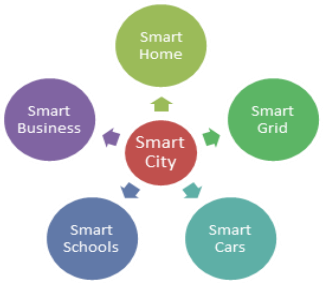

Fig. 2.

2.1 Threats in Smart Cities

As stated in [11] over 50 billion IoT devices are going to be connected by 2020.To be able to fully utilize IoT in smart cities it should also be properly secured.

1) Botnet Attacks.-

. With huge number of devices connected with each other it becomes easy target for hackers to install botnet and do malicious activities such as DOS attacks [11].

2) WSN Issues.-

. Wireless Sensor Networks are tiny sensor nodes which consume low power and are also cost effective [12] [14]. WSN's are widely used in IoT. Network such as in smart surveillance and also have privacy, authentication risks associated with it and solution to this was proposed in [12] with an algorithm named EAMSuS.

3) Cloud Data Confidentiality. -

. Huge amount of data will be processed in smart cities every second and huge amount of real time data will also be fetched by devices thus causing too much of inflow and outflow of data [11]. This may cause attacks such as MITM. Cloud computing security solutions can be utilized but as stated in [11] these solutions are not sufficient alone to meet the future requirements of IoT.

4) Heterogeneity Issues.-

. Smart city will have various IoT devices thus huge number of data will be collected in numerous ways and in various formats [11]. Therefore, there should be a standard format which can be used for data integration thus making it easier. This issue was solved in [13] by introducing Unified Registry.

III. SOLUTIONS

2.2 EAMSuS Algorithm

Efficient Algorithm for Media based Surveillance System is a WSN security algorithm proposed by authors in [12]. It is a coalesce of 2 algorithms i.e. Identity, Route and Location (IRL) and Practical algorithm for data security. It is used with HEVC which is a video compression standard.

EAMSuS operates in two rounds i.e. Neighbor node state initialization round and routing round. When a packet is to be transferred from the wireless node it is called routing round. The source node before sending the packet to the next node checks for trustworthy nodes in all the sides i.e. forward, left, right, backward and the middle. On finding a trustworthy node in any of the side it identifies a random node and forwards the packet towards it. If there is no trustworthy node present on any of the side then the packet is dropped. When the packet reaches the intermediate node, it checks whether the packet is new or old. If its new it forwards it.

Table 3.

Class	Resolution	HEVC bitrate reduction as compared to H.264
A	UHD – 2560 x 1600	64%
B – B1 and B2	HD- 1920 x 1080	62%
C	WVGA- 800 x 400	56%
D	VGA – 400 x 240	52%

The experimental results as in Table 3 have proved EAMSuS algorithm to be having less memory consumption at the WSNs as compared to the IRL/r-IRL scheme.

By using this algorithm, a faster, secure media transmission can be achieved which can be effectively used in Smart Cities.

2.3 4 Block Secure IoT structure.

In [13] the authors have proposed a 4 blocks secure architecture which aims to alleviate cyber-attacks at the beginning only.

The 4 blocks are as follows-

- Black Network-They provide secure communication at Link Layer and the Network Layer by encrypting the payload and the meta-data using Grain128a or AES for encryption.
- Trusted SDN Controller-It resolves the routing challenges faced in the black network.
- Unified Registry – It is a standard attribute which facilitates the conversion of the heterogeneous data from networks, protocols to a format which is easily understood by a smart IoT device.
- Key Management System- It is a secure key management system for each layer.

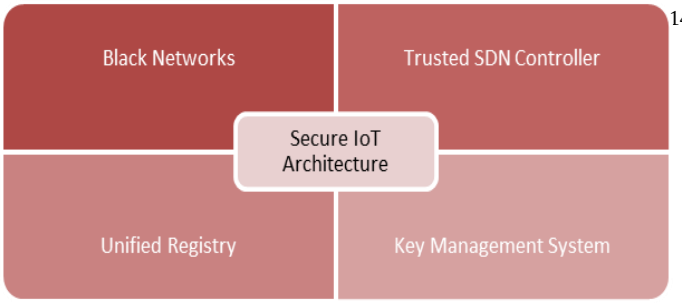

Fig. 2.

IV. RESULT

There are lots of threats and attacks that can affect the IoT devices such as Botnet attacks, DOS attacks and threats such as privacy, authentication threat and many more. Though a lot of work has been done in the field of IoT Security but there's a scope for a lot more that can be achieved in this field as this holds the future of modernization. IoT has become ubiquitous and one vulnerability, can cause a threat to a lot of important data being accessible to the hackers. A lot of successful algorithms are present like EAMSuS, 4 block secure IoT structure but no one gives 100% accuracy for threat detection and mitigation which still needs to be achieved.

V. CONCLUSION AND FUTURE WORK

We plan to study more about IoT Security and then help in the development of IoT Security by improving those algorithms or introducing our algorithms.

REFERENCES

1. Hanan Aldowah, Shafiq Ul Rehman, Irfan Umar, P.: Security in Internet of Things: Issues, Challenges, and Solutions. ResearchGate 2(5), July 2018.
2. NEETESH SAXENA, SANTIAGO GRIJALVA, NARENDRA S. CHAUDHARI, P.: Authentication Protocol for an IoT-Enabled LTE Network, ACM Transactions on Internet Technology, December 2016.
3. ELISA BERTINO, KIM-KWANG RAYMOND CHOO, DIMITRIOS GEORGAKOPOLOUS, SURYA NEPAL, P.: Internet of Things (IoT): Smart and Secure Service Delivery, ACM Transactions on Internet Technology, December 2016.
4. FARID MOLAZEM TABRIZI, KARTHIK PATTABIRAMAN, P.: Design-Level and Code-Level Security Analysis of IoT Devices, ACM Transactions on Embedded Computing Systems, May 2019.
5. R.VIGNESH, F., A.SAMYDURAI ,S.:T.: Security on Internet of Things (IOT) with Challenges and Countermeasures In:IJEDR 2017,Volume 5 ,Issue 1
6. Faheem Masoodi ,F., Shadab Alam ,S., Shams Tabrez Siddiqui, T.: SECURITY& PRIVACY THREATS, ATTACKS AND COUNTERMEASURES IN INTERNET OF THINGS, IJNSA Vol. 11, No.2, March 2019,
7. Muhammad Burhan, F., Rana Asif Rehman, S.,T.: IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey, Sensors 2018, 24 August 2018.
8. Elike Hodo, F.,Xavier Bellekens, S., T.:Threat analysis of IoT networks using Artificial Neural Network Intrusion Detection System, IEEE 2016.
9. Yasir Javed, F., Abdul Qahar, S., T.: Preventing DoS Attacks in IoT Using AES, Researchgate, January 2018.
10. Deloitte Insights paper, T.:Making smart cities Cybersecure.
11. Badis Hammi and Rida Khatoun, F., Sherali Zeadally and Achraf Fayad, S., T:IoT Technologies for smart cities, IET Network 2018,Vol 7 Issue ,pp.1-13.
12. Vasileios A. Memosa, and Kostas E. Psannis ,F., Yutaka Ishibashi ,S.,T.: An Efficient Algorithm for Media-based Surveillance System (EAMSuS) in IoT Smart City Framework, Elsevier B.V. 2017.
13. Shaibal Chakrabarty, F., Daniel W. Engels, S., T.: A Secure IoT Architecture for Smart Cities, 13th IEEE Annual Consumer Communications & Networking Conference (CCNC) 2016.
14. Mr.K.Muruganandam, F., Dr.B.Balamurugan, S., T.: Design Of Wireless Sensor Networks For IOT Application : A Challenges and survey, International Journal Of Engineering And Computer Science, Volume 7 Issue 3 March 2018, Page No. 23790-23795.

AUTHORS PROFILE

Narendra Sharma currently pursuing M.Tech in Computer Science and Engineering at Galgotias University, Greater Noida. His area of interest includes Internet of Things, Cloud Computing.. He has completed his B.Tech from same university in computer Science. He added two more credentials

Reitwick Prakash has completed his B.Tech in Computer science and Engineering, at Galgotias University, Greater Noida. His area of interest includes Internet of Things, Cyber Security.

Dr. E. Rajesh currently working as an Associate Professor in the School of computing science and engineering at Galgotias University, Greater Noida. He completed his Doctrate in Anna University, Chennai and Master in Pondicherry University, Puducherry. His area of research includes Data Mining, Computational Intelligence and Networking.