International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

Cyber Security Threats And Measures In Context with IOT

Shradha V. Pore[1], *Guided by* Aishwarya Gore[2], Mihir Paygude[3]

[1] Student, Third Year Electrical Engineering , AISSMS College of Engineering, Pune, Maharashtra, India
[2] Penetration Tester, Newton's Apple , Pune, Maharashtra, India
[3]Technical Analyst, Newton's Apple ,Pune, Maharashtra, India

---

Abstract - *The Internet Of Things (IOT) has grown by bounds and leaps in just a ample amount of time. With the creation of everything from smart watches to inter connected washing machines, more and more appliances and electrical devices is interconnected with the backbone network that enables its control from remote location. However IOT devices might provide a backdoor into a corporate network for cyber attacks as not only more data being shared through IOT but more sensitive data is being shared. According to recent research about 6.6 billion IOT devices are connected to internet and this count can double in next few years. Hence concern over security has been an alarming issue in most of Big Data Application as IOT services becoming pervasive. This paper present framework for calibrated security measures for IOT expedients.*

Keywords- *Cyber Attacks , Internet of Things, Privacy, Security*

1. INTRODUCTION

In the era of the advance internet communication, IoT devices are the target of increasing sophisticated cyber attacks and innovators must protect their assets and their consumers from emerging treats. Every device is interconnected with a backbone network that enables its control from a remote location. Of course, IoT security is really a collective responsibility between consumers who seek all type of connections and companies that want to use connectivity to create higher rate of customer. This is the trend in most of industrial applications as the there is a backbone network that controls physical and cyber systems. To build end-to-end protection system in smart industrial application, it is required to have calibration of the security requirement for different sub-systems. This calibration provides unique integration of the security with existing protocols of IoT thus making robust security for the entire system. Security must provide integrity, confidentiality, non-repudiation and authentication of the information flows. This is achieved through vulnerability identification of the protocol interfaces at IoT layer and at the traditional network. The messaging system used in IoT applications uses the traditional TCP/IP network at the back end for sending control commands to various control systems. The focus is on developing calibrated security measures for smart IoT device which will be the base for other IoT applications such as Industrial Control Systems(ICS).

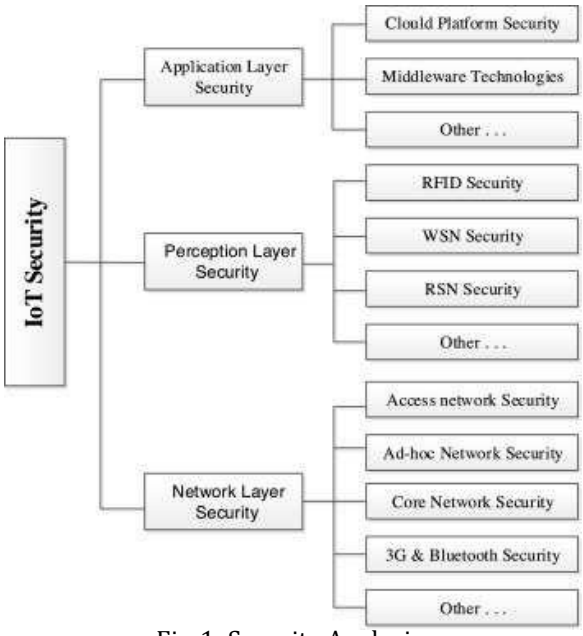

Fig-1: Security Analysis

2. IOT THREAT EXPLORATION

Cyber criminals can easily attack IoT devices due to the default software configuration, irregular updates of software installed, a long gap between patch release and it installation. The cyber criminals can have an access each device due to the default login credentials, vulnerability [11-13]. The BOT NET, mirai hacked many devices in this way. The risk can be decreased by changing the factory default name and password. Another security issue is BOT NET is ransom ware infection. It locks a device through encryption and can be accessed only with an agreement to pay a ransom. Intrusion detection systems also play a remarkable role by protecting IoT devices from DDOS. Most of the IoT devices are connected via internet which is the main perpetrator. An unprotected internet protocol using internet scanning tools such as Z-map, N-map information can easily be obtained. Intrusion detection system can used to decrease the cyber attacks. [12-14].

Numbers	Types of Incident	No. of cases
1.	Phishing	11
2.	Abuse/ Privacy	16
3.	Scams	12
4.	Malware	09
5.	Defacements	21
6.	Unauthorized Access	08
7.	DOS Attacks	01
8.	Fake Accounts	756

Table 1: Types of Cyber Crime In India

3. SECURITY ISSUES IN IOT NETWORK

Internet is key infrastructure of IoT hence there is a possibility for some prominent security issues [5]. IoT is a collection of physical objects connected to internet; hence many security issues may occur. Some of the security issues are:

1) Security issues in the wireless sensor networks (WSNs): WSN is a network of nodes that sense and control the environment. It also enables the interaction between persons or computers and the surrounding environment. WSN includes sensor nodes, actuator nodes and so on. WSN is a collection node hence there is a possibility of security issues.

i. Attacks on secrecy and authentication
ii. Silent attacks on service integrity
iii. Attacks on network availability

2) Security issues in RFID technology: In IoT, RFID technology is mainly used as RFID tags for automated exchange of information without any manual involvement. The RFID tags are vulnerable to various attacks from outside due to the incorrect security status of the RFID technology [5]. The four most common types of attacks and security issues of RFID tags are as follows:

i. Unauthorized tag disabling: In this DoS attacks the RFID tags will become incapable temporarily or permanently. Such attacks make RFID tag available to malfunction and misbehave under the scan of a tag reader. These attacks can be done remotely, allowing the attacker to manipulate the tag behavior from a distance.

ii. Unauthorized tag cloning: Capturing the identification information through the manipulation of the tags by dishonest readers falls under this category. Once the identification information of a tag is compromised, replication of the tag is made possible which can be used to bypass fake security measures as well as introducing new vulnerabilities using
RFID tags automatic verification steps [5].

iii. Unauthorized tag tracking: The dishonest readers can trace the tag, which results in giving the sensitive information, for example person's address. Thus from the viewpoint of customer, buying a product which is having an RFID tag guarantees them no confidentiality regarding the purchase of their chase and in fact endangers their privacy.

iv. Replay attacks: In Replay attacks the attacker uses a tag's response to a dishonest reader's challenge to impersonate the tag. In this attacks, the communicating signal between the reader and the tag is intercepted, recorded and replayed upon the receipt of any query from the reader at a later time, thus faking the availability of the tag.

3)Security issues in Application layer: Application of IoT is the result of closely integration between communication technology, computer technology and industry professional which can be able to find applications in many aspects. The security issues in application layer include eavesdropping and tampering [8]. This layer carries out the responsibility of traffic management. It also provides software for different applications which carries out the translation of data into a comprehensible form or helps in collection of information by sending queries [5]. A path-based DOS attack is initiated in application layer by stimulating the sensor nodes to create a huge traffic in the route towards the base station.

4. CASE STUDY OF CHANCES OF FRAUD

Step 1: Let A be a person who wants to access social networking site or social media. For example, facebook. Before getting access to any online website A has to sign up using his credentials. Query Box will take information about:

- AADHAR NUMBER
- AGE
- PAN
- FATHER'S NAME
- ADDRESS

Here, sign up will include the basic details like name, phone number, birth date, country and city while intrinsic details will include aadhar card number, age, permanent account number, father's name, address. All the details mentioned above are sufficient to identify the person. Facebook (website) sends these details to the legal portal (which will be governed by the government) and will check these details of the person from the database [10].

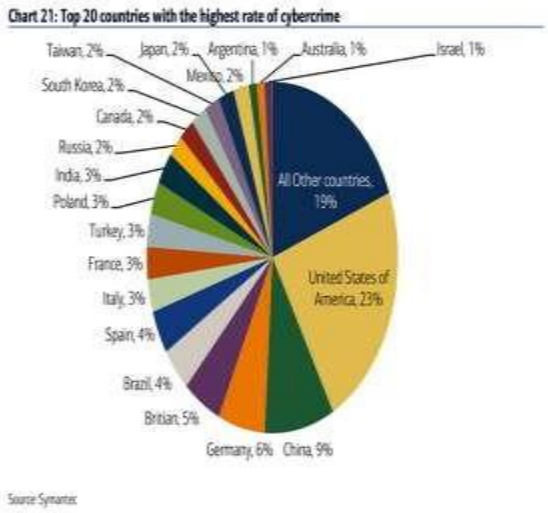

Fig-2: Cyber crime in top 20 country

Case-1: If legal portal finds False/incorrect information or crime record against that person then, it will send disapproval message to face book and face book will no allow him/her to go ahead.

Step 2: If A person gets involved in wrong activities such as spamming. Then website will report this to the legal portal and account will be deactivated / banned for some period of time(30 days) and the culprit have to pay compensation amount and this information is send to website and to the culprit.

Step 3: If A person wants to start using that website again or the other websites, then, he/she has to form an id once again after some period of time (Step 1 repeat). But now legal portal finds fraud record against A Now, the notification will be generated for culprit as well as for the websites (accessed before or any other accessed website), this notification will alert the website with crime details of the user (compensation details, date, charges levy, type of crime etc). Then it rests upon the security protocols of the accessed website, if it has any issues with the crime record and the website considers him/her as a potential threat then it will not allow him/her to go ahead otherwise allow him /her. Also, on the other end if the criminal fails to pay the required compensation amount and also does not complete the ban duration and tries another heist, then, his/her database will be blacklisted and his account will be frozen for further use [11]. The Complete execution of step 3 is given in Fig.11. After the compensation has been paid and charges are taken off by that person, his past history will not be available for detail investigation. As a home automation system, the higher Smart Care offers a motion sensor, a magnetic sensor which can be used to determine if a door has been opened and a remote switch to turn devices on and off. A compromised higher Smart Care can be used by an attacker to build a profile of its user, being able to determine whether the user is at home and possibly some of the user's habits. The leakage of this information causes privacy concerns for users.

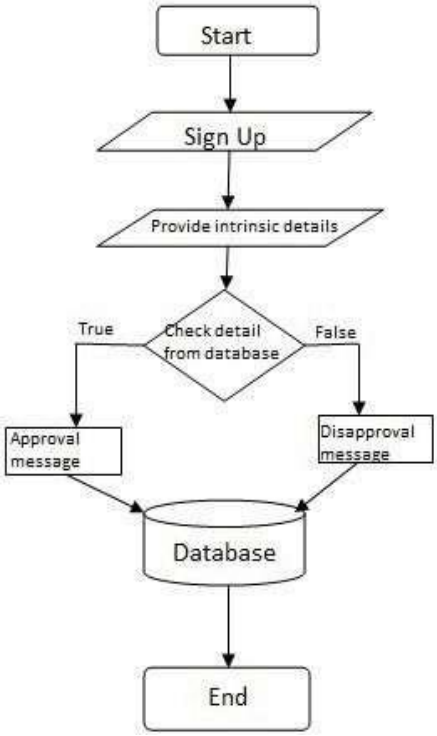

Fig-3: Flow Chart of Security Solution

5. POSSIBLE SOLUTION FOR CYBER CRIME

1) STORAGE: Cloud Computing provides three services through which massive data can be analyzed and store The three services are:
a) Infrastructure
b) Platform services
c) Software services

2) TRANSFER: New protocols and algorithms are required for big data challenges. FTP and the SECURE COPY (SCP) is not sufficient. Current Innovations are aimed at tackling massive flow challenges including:
a) GRID FTP
b) GLOBUS

3) PRIVACY AND SECURITY: It is one of the important issues of today's era. Privacy refers to a in which one is not observed or disturbed by other whereas, security refers to a state of being free from danger or threat. But in today's world one does not feel secure while sharing their personal information on internet due to increase in number of frauds, spam, malicious URLs and many more. India is at 11th position in cyber crime among top 19 countries.

CONCLUSION:

Government websites, financial systems, news and media websites, military networks, as well as public infrastructure systems are the main targets for cyber-attacks. The security development process requires through understanding of a systems assets, followed by identifying different vulnerabilities and threats that can exist. The overall goal was to identify assets and document potential threats, attacks and vulnerabilities faced by the IoT. It was concluded that much work remains to be done in the area of IoT security, by both vendors and end-users. We hope this survey will be useful to researchers in the security field by helping identify the major issues in IoT security and providing better understanding of the threats and their attributes originating from various intruders like organizations and intelligence agencies. We hope this survey will be useful to researchers in the security field by helping identify the major issues in IoT security and providing better understanding of the threats and their attributes originating from various intruders like organizations and intelligence agencies.

ACKNOWLEDGEMENT

The author acknowledges Assistant *Prof.* ***M.S Dhend****, AISSMS COE, Pune* **; *Dr. Mrs. M. P. Atre***, *Electronics and Telecommunication Department, PVG's COET, Pune and Mr.* ***Mandar Waghmare****, Mr.* ***Hrishikesh Sahane****, Newtons Apple* for the support extended during this work.

REFERENCES

1. R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems (Wiley Computer Publishing, 2001).

2. P. Bresciani, A. Perini, P. Giorgini, G. Giunchiglia, and J. Mylopoulos, Modelling early requirements in Tropos: A transformation based approach, in Agent Oriented Software Engineering II, eds. M.Wooldridge and G.Weiss, Lecture Notes in Computer Science, Vol. 2222, Springer-Verlag, 2002.

3. P. Giorgini, F. Massacci, J. Mylopoulous, and N. Zannone, Requirements engineering meets trust management: Model, methodology, and reasoning, in Proc. 2nd Int. Conf. on Trust Management (iTrust
2004), Lecture Notes in Computer Science, Vol. 2995, Springer-Verlag, Heidelberg, 2004, pp. 176–
190.

4. Y. Cheng, M. Naslund, G. Selander, and E. Fogelstrom, "Privacy in machine-to-machine communications a state-of-the art survey," in Communication Systems (ICCS), 2012 IEEE International Conference on. IEEE, 2012, pp. 75–79.

5. M. Abomhara and G. Koien, "Security and privacy in the internet of things: Current status and open issues," in PRISMS 2014 The 2nd International Conference on Privacy and Security in Mobile Systems (PRISMS 2014), Aalborg, Denmark, May 2014.

6. E. Bertino, L. D. Martino, F. Paci, and A. C. Squicciarini, "Web services threats, vulnerabilities, and countermeasures," in Security for Web Services and Service-Oriented Architectures. Springer, 2010, pp. 25–44.

7. W. Jansen, Countermeasures for mobile agent security, Computer Communications, Special Issue on Advanced Security Techniques for Network Protection, Elsevier Science, 2000.

8. A. Perini, P. Bresciani, P. Giorgini, F. Giunchiglia, and J. Mylopoulos, Towards an agent oriented approach to software engineering, in *Proc. Workshop Dagli Oggetti Agli Agenti: Tendenze Evolutive dei Sistemi Software*, Modena, Italy, 4–5 September 2001.

9. B. Schneier , secrets and lies*:* Digital Security in a Networked World (JohnWiley, 2000).

10. K. Dahbur, B. Mohammad, and A. B. Tarakji, "A survey of risks, threats and vulnerabilities in cloud computing," in Proceedings of the 2011 International conference on intelligent semantic Web-services and applications. ACM, 2011, p. 12. 11. F. Li, A. Lai, and D. Ddl, "Evidence of advanced persistent threat:Acase study of malware for political espionage," in Malicious and Unwanted Software (MALWARE), 2011 6th International Conference on. IEEE, 2011, pp. 102–109.

12. Cybersecurity analysis for USA", the National Initiative for Cybersecurity Education. [online]. available: https://www.cyberseek.org/heatmap.html

13. Imane Khaouja, Ibrahim Rahhal, Mehdi El Ouali, Ghita Mezzour, Kathleen M. Carley, and Ismail Kassou.Analyzing the Needs of the Offshore Sector in Morocco. IEEE Global Engineering Education Conference (EDUCON), April 2018.

14. S. Cass, The 2017 Top Programming Languages, July2017Available:https://spectrum.ieee.org/computi ng/software/the-2017- top-programming-languages

15. Potter, L. E., & Vickers, G. 2015. What Skills do you Need to Work in Cyber Security ? A Look at the Australian Market,
[1] .