Cyber Security Threats and Vulnerabilities in IoT

Ankit Dhatrak[1], Anshuman Sarkar[2], Guided by Aishwarya Gore[3], Mihir Paygude[4], Mandar Waghmare[5], Hrishikesh Sahane[6]

[1,2]Student, Third Year EXTC, MIT School Of Engineering, Pune, India
[3]Penetration Tester, Newton's Apple , Pune, India
[4]Technical Analyst, Newton's Apple ,Pune, India
[5,6]Software Developer Security Analyst, Newton's Apple ,Pune , India

---***---

Abstract - *Nowadays portable devices like smartphones tablets and laptops are getting more and more adaptive informative and interactive. Peripherals can be interfaced and remotely accessed using Wi-Fi. Numerous of application can be controlled by using some kind of controller or processor. These all application and peripherals controlled come under one concept known as IOT.*

IOT combines all the peripherals like wireless sensors, networks, data acquisition, data analytics, cloud computing to provide solutions such that the peripheral objects are embedded in a network to provide object to object communication and user control over a same network. IOT innovation is leading us to smart cities to e-industries. It provides smart solutions to the problems faced by the industries as well as problems faced by common people in day to day life. Due to the environment of IOT the risk of cyber threats is of rising concern. Cyber-attacks basically focus on system infrastructure also digs into system vulnerabilities which may be of some concern not only to the vendors but also to the consumers. Cyber-attacks are not new to IOT but the rising involvement of IOT in our day to day lives it has become necessary to address this concern and take some measures to secure this threat.

This paper aims to demonstrates cyber security in the field of Internet of Things (IoT) the issues it encounters.

Keywords—*Cyber security, Internet Of Things (IoT), sensors, internet protocol IP, interconnection, information, etc.*

1. INTRODUCTION

The era of computing aims to reach the apex of automation through the growth in technology via Internet of Things (IoT). Internet of Things (IoT) is the wireless network of large number of devices which are interconnected and can have a communication link between each other without any external interference caused by humans. Basically, in IoT the peripheral devices are connected to a server which may be a cloud server, and through this server the peripherals can be programmed and can also be accessed according to the requirement of the consumer. The basic idea behind IoT is to make our everyday used devices smarter and easy to access. The term Internet of Things (IoT) first introduced and coined by Kevin Ashton in the year 1999. The number of devices connected to the Internet, including the machines, sensors, and cameras that make up the Internet of Things (IoT), continues to grow at a steady pace. A new forecast from International Data Corporation (IDC) estimates that there will be 41.6 billion connected IoT devices, or "things," generating 79.4 zettabytes (ZB) of data in 2025.

We know that in Internet of Things all the peripheral devices which include sensors like temperature sensor, IR sensor, RFID, etc. are connected to a cloud server, therefore all the threats that are present in cloud computing will also be inherent threats in Internet of Things. As Internet of Things applications are already present in our surrounding the main concern which has limited the outreach of the Internet of Things is its protection against cyber security threats. The different threats that are present in Internet of things (IoT) are device attack, application service attack, web interface attack, etc.

Security has been defined as the process in which an object physical or abstract is protected from any potential damages, the damages may be physical damages or not, access which is unauthorized, burglary, by maintaining high level of privacy and integrity of the object and making the details of the object available whenever needed. An object is said to be secure only if the said object maintains its asset value under different conditions. Therefore, the requirement of different attributes for security purpose in Internet of Things (IoT) is similar to any Information Communication Technology (ICT) system. Furthermore, to maintain the security conditions in Internet of Things (IoT) can therefore be maintained by maintaining its asset value.

This paper is a review paper which deals with cyber security threats in the field of Internet of Things (IoT). In this paper the concept of Internet of Things (IoT) is explained and also the structure of Internet of Things (IoT) and how this structural limitation lead to vulnerabilities to cyber-attacks and other such threats. The different such threats are discussed in this paper.

2. CONCEPT AND APPLICATIONS OF INTERNET OF THINGS (IOT)

2.1. Definitions

As said by Atzori et. al. [7], Internet of Things can be realized in three paradigms – internet-oriented (middleware), things oriented (sensors) and semantic oriented (knowledge). Although this type of description is required due to the interdisciplinary nature of the subject, the full potential of Internet of Things (IoT) can be unleashed only in an application domain where the three paradigms converge.

Taking in consideration the different definitions given by different journals we have derived our definition so that it is more reader friendly and easy to understand so as to have a greater outreach. Our definition for Internet of Things (IoT) is:

Internet of Things (IoT) is a network of interconnected peripherals containing sensors and actuators which has the inherent ability to perform its programmed tasks and share the said information obtained by the above tasks through a platform which is capable to communicate between different devices be it small or large and logical and physical such that these actions make our day to day tasks easier.

2.2. Applications

There are a lot of application of Internet of Things (IoT). The applications can be classified based on the type of network availability, coverage, scale, heterogeneity, repeatability, user involvement and impact. Whenever we think of IoT systems, the most important and efficient application that stands out is the smart home. Control of home equipment such as air conditioners, refrigerators, washing machines etc., will allow better home and energy management. Environmental monitoring is the first common application which is implemented to keep a track of the number of occupants and manage the utilities within the building. Sensors have always been an integral part of IoT. Different IoT devices consist of RFID, WSN. This will eventually be replaced by wireless system giving the flexibility to make changes to the setup whenever required. Smart grid and smart metering is another potential IoT application which is being implemented around the world. Efficient energy consumption can be achieved by continuously monitoring every electricity point within a house and using this information to modify the way electricity is consumed. This information at the city scale is used for maintaining the load balance within the grid ensuring high quality of service.

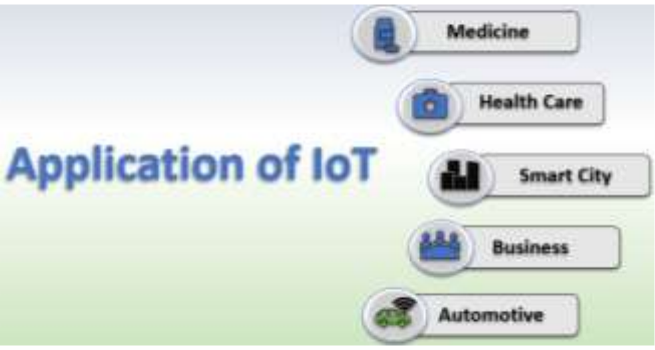

Fig-1: Applications of IoT

IoT can be used in a home appliance, healthcare device, vehicle, building, factory and almost anything networked and fitted with sensors providing information about the physical environment.

Surveillance, the most widely used camera network applications, helps track targets, identify suspicious activities, detect left luggage and monitor unauthorized access. Water network monitoring and quality assurance of drinking water is another critical application that is being addressed using IoT.

As IoT become a reality, a growing number of universal devices has raised the number of the security threats with significance for the general public. Unfortunately, IoTs comes with new set of security threat. There is a growing awareness that the new generation of smart-phone, computers and other devices could be targeted with malware and vulnerable to attack.

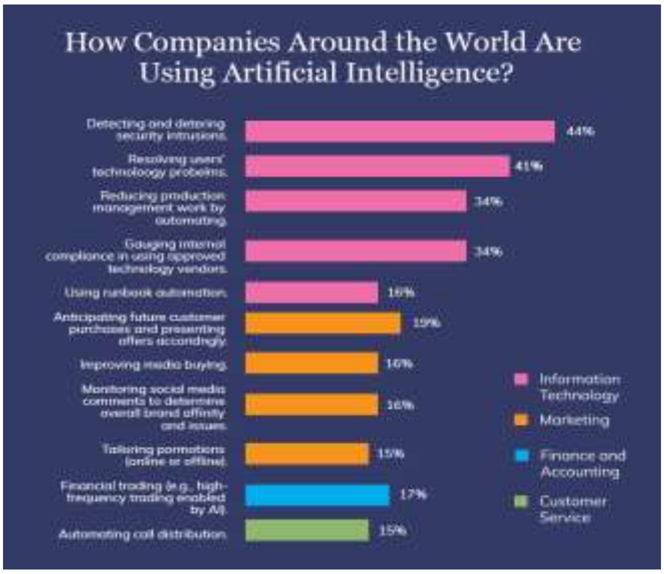

Fig 2: Trends in IoT

3. SECURITY THREATS IN IOT

In the paper published by Roman et. al., there are many challenges to make Internet of Things (IoT) functional in the real world but security tops it all. As we know Internet of Things (IoT) all the devices "things" are interconnected to each other to perform specific tasks sensing, communicating, information processing, but each of this interconnected can be a potential doorway into the Internet of Things (IoT) infrastructure and it is a threat. There are some security threats which are introduced in Internet of Things (IoT) due to its merging with cloud computing. The liabilities which are inherent in cloud computing applications are most likely to have an impact on the Internet of Things (IoT) services. Internet of Things (IoT)in itself many security challenges because the sources expose the infrastructure setup to various attacks. These sources include device, firmware, applications based on system and network interfaces or ports. These bi-directional ports are links between object to object communication which leaves the system vulnerable to network related attack. The major example is Internet Protocol (IP) misconfiguration which decreases system performance and reliability. As Internet of Things (IoT) is becoming more user friendly and interactive using webpages or mobile application which are mostly designed by Application Programming Interface (API) using PHP, JAVA, XML, HTML. Basically, Internet of Things (IoT) structure and system are designed keeping in mind cyber-attacks and vulnerabilities but any misconfiguration or error at any level of Internet of Things (IoT) may lead to failure in the working. For ex., in any battery-operated Internet of Things (IoT) system, power fluctuation may lead to data loss which in turn leads to potential malfunction.

3.1 Security Threats

The security attacks include application service attack, network attack, data integrity attack. These attacks are caused due to IP misconfiguration, injection, DoS, etc. One of the types of attack is device attack which is capable of compromising Internet of Things (IoT) devices which can compromise critical architectural functions of a system. As we know that many devices are connected using Internet of Things (IoT), the network attack mainly focuses on the intercommunication link between these devices which makes monitoring or connected devices futile.

Account listing, lack of account lookout or weak access credential may lead to a Web Interface Attack caused by IP misconfiguration, sql injection, Cross Site Reference Forgery (CSRF) and Cross Site Scripting (XSS). For instance, in CVE-2016- 7571, a cross-site scripting (XSS) vulnerability in Drupal 8.x before 8.1.10 allows remote attackers to inject arbitrary web script or HTML via vectors involving an HTTP exception. Similarly, in CVE-2016-8581, a persistent XSS vulnerability exists in the User-Agent header of the login process of AlienVault OSSIM and USM before 5.3.2 allows an attacker to steal session IDs of logged in users when the current sessions were viewed by an administrator. Another type of attack is Data Integrity Attack where a threat agent tries to manipulate data i.e. inserting, altering or completely deleting a data so as to delude the smart devise to make in accurate decision. As we already know the Internet of Things (IoT) runs on user interface by web servers and mobile application, Application Service Attack compromises the above-mentioned things. Raspberry Pie is one of the major contributors to make IoT enabled applications based on Linux kernel. Vulnerabilities present in kernel are also exposed to the IoT devices. In CVE-2016-5344, ''multiple integer overflows in the MDSS driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allow attackers to cause a denial of service via a large size value, related to mdss_compat_utils.c, mdss_fb.c, and mdss_rotator.c". Man-in-the-middle: An attacker breaches, interrupts or spoofs communications between two systems. In an IoT scenario, an attacker could assume control of a smart actuator and knock an industrial robot out of its designated lane and speed limit – potentially damaging an assembly line or injuring operators. Distributed Denial of Service (DDoS): A denial-of-service attack (DoS attack) attempts to render a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. In the case of a distributed denial-of-service attack (DDoS), incoming traffic flooding a target originates from multiple sources, making it difficult to stop the cyber offensive by simply blocking a single source.

DoS and DDoS attacks can negatively affect a wide range IoT applications, causing serious disruptions for utility services and manufacturing facilities. Permanent Denial of Service (PDoS): Permanent denial-of-service attacks (PDoS), also known as plashing, is an attack that damages the device so badly that it requires replacement or reinstallation of hardware. BrickerBot, coded to exploit hard-coded passwords in IoT devices and cause permanent denial of service, is one such example of malware that could be used to disable critical equipment on a factory floor, in a wastewater treatment plant, or in an electrical substation. Some attempts made to hack IoT devices are:

- Back in October of 2016, the largest DDoS attack ever was launched on service provider Dyn using an IoT botnet. This leads to huge portions of the internet going down, including Twitter, the Guardian, Netflix, Reddit, and CNN. This IoT botnet was made possible by malware called Mirai. Once infected with Mirai, computers continually search the internet for vulnerable IoT devices and then use known default usernames and passwords to log in, infecting them with malware. These devices were things like digital cameras and DVR players.

- TechNewsWorld reports, "TRENDnet marketed its SecurView cameras for various uses ranging from home security to baby monitoring and claimed they were secure, the FTC said. However, they had faulty software that let anyone who obtained a camera's IP address look through it and sometimes listen as well. Further, from at least April 2010 [until about January 2012], TRENDnet transmitted user login credentials in clear, readable text over the Internet, and its mobile apps for the cameras stored consumers' login information in clear, readable text on their mobile devices, the FTC said.

4. COUNTER MEASURES

Firmware integrity and secure boot: Secure boot uses cryptographic code signing techniques, assures that a device only executes code generated by the device OEM or another trusted party. Use of protected boot technology restricts hackers from changing firmware with malicious instruction sets, thereby avoiding attacks. Unfortunately, not all Internet of Things (IoT) chipsets are equipped with secure boot capabilities. In such a scenario, it is important to ensure that Internet of Things (IoT) devices can only communicate with authorized services to avoid the risk of replacing firmware with malicious instruction sets.

Mutual authentication icon: During every transmission or reception of data from any sensor or actuator through a network, prior authentication must be done which ensures that device is legitimate. Secure and mutual authentication helps protect against malicious attacks. Cryptographic algorithms involving symmetric keys or asymmetric keys can be utilized for two-way authentication. For example, the Secure Hash Algorithm (SHA-x) along with hash-based message authenticated code (HMAC) can be used for symmetric keys and Elliptic Curve Digital Signature Algorithm (ECDSA) for asymmetric keys.

Secure communication (end-to-end encryption): Secure communication capabilities protect data in transit between a device and the cloud. Encryption ensures that only legitimate user can access transmitted data. For example, a smart actuator that sends usage data to the SCADA must be able to protect information from digital eavesdropping.

Security monitoring and analysis: Security monitoring captures data on the overall state of an industrial system, including endpoint devices and connectivity traffic. Data is analyzed to detect possible threats present in the system. Once detected, large no. of actions mentioned in the context of system security policy are executed, such as cancelling device credentials or isolating an Internet of Things (IoT) device based on anomalous behavior. It is critical to ensure that endpoints devices like RFID which includes sensors and actuators are secured from data manipulation, which could result in the incorrect reporting of events.

5. CONCLUSION

In this paper we have discussed the basic concept of Internet of Things (IoT) its application and the security threat it faces. As there is increase in the number of Internet of Things (IoT) devices, the emerging concern regarding the security is also increasing exponentially. As Internet of Things (IoT) is gaining more and more popularity within masses its security against cyber-attacks is getting more and more difficult. Internet of Things (IoT) is nowadays integrating with cloud computing and other various platforms their inherent vulnerabilities are also a concern. Hence in this paper we have enlisted number of cyber security threats faced by Internet of Things (IoT) applications and also tried to provide countermeasures to make Internet of Things (IoT) a more stable and secure system. We enumerated a number of countermeasures against such cyber security attacks which are viable and can be easily applied. Hopefully this will help more work on the security concerns and provide more detailed countermeasures to such concerns.

REFERENCES

1) Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Paliniswami, “Internet of Things: A vision, architectural elements and future directions” in Future Generation Computer Systems 29 (2013) 1645–1660, Elseiver.

2) Aishwarya Pandey, “Paper on Internet of Things (IoT)” in National Conference on Technological Advancement and Automatization in Engineering (2016) 194, IJSRD.

3) Jyoti Deogirikar, Amarsinh Vidhate “Security Attacks in IoT: A Survey” in International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), (I-SMAC 2017).

4) Mohamed Abomhara and Geir M. Køien “Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks” Publication 22 May 2015.

5) Samuel Tweneboah-Koduah, Knud Erik Skouby1, Reza Tadayon “Cyber Security Threats to IoT Applications and Service Domains” Wireless Pers Commun DOI 10.1007/s11277-017-4434-6.

6) Saloni Khurana “A Review Paper on Cyber Security” in International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Volume 5, Issue 23.

7) Ashton, K. (2009). That ‘Internet of Things’ thing. RFID Journal, 22, 97–114.

8) Statista, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.

9) IDC, https://www.idc.com/getdoc.jsp?containerId=prUS45213219

10) https://irdeto.com/news/new-2019-global-survey-iot-focused-cyberattacks-are-the-new-normal/

11) J. M. Kizza, Guide to Computer Network Security. Springer, 2013.

12) L. Atzori, A. Iera, G. Morabito, The Internet of Things: A survey, Comput Netw. 54 (2010) 2787–2805.

13) https://clipartart.com/categories/iot-logo-clipart.html

14) A.P. Castellani, N. Bui, P. Casari, M. Rossi, Z. Shelby, M. Zorzi, Architecture and protocols for the Internet of Things: A case study, in: 2010: pp. 678–683.

a. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, T. Razafindralambo, A Survey on Facilities for Experimental Internet of Things Research, IEEE Commun Mag. 49 (2011) 58–67.

15) M. Yun, B. Yuxin, Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid, Advances in Energy Engineering (ICAEE). (2010) 69–72.

16) https://www.educba.com/applications-of-iot/

17) https://towardsdatascience.com/top-14-iot-trends-to-expect-in-2020

18) Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266–2279.

19) Jari Porras*, Jayden Khakurel, Antti Knutas and Jouni P?k??nen, Security Challenges and Solutions in the Internet of Things, Lapeenranta University of Technology, Finland.

20) NVD—Detail. https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-8581.

21) CVE-2016-7571: Cross-site scripting (XSS) vulnerability in Drupal 8.x before 8.1.10 allows remote attackers to inject arbitrary web scr. http://www.cvedetails.com/cve/CVE-2016-7571/.

22) CVE-2016-5344. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5344.

23) G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

24) J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

25) S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

26) K. Elissa, “Title of paper if known,” unpublished.

27) R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

28) Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

29) M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.