Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Cyber Threats in Internet of Thing systems and Impact reduction

Amol Purohit[1]

amolpurohit.sdes@gmail.com

A. Mounika[2]

gangimounika@gmail.com

V.S. Madhumala[2]

vmadhumalacse@sreedattha.ac.in

K. Umarani[2]

Umarani.biet@gmail.com

A. Sai Teja Reddy[3]

saiteja.adapala@gmail.com

Shruti Thapar4

shruti.thapar@poornima.org

1. Department of Electronics & Communication Engineering
Sree Dattha Institute of Engineering & Science, Hyderabad
2. Department of Computer Science & Engineering
Sree Dattha Group of Institutions, Hyderabad
3. Department of Computer Science Engineering
Sree Dattha Institute of Engineering and Science, Hyderabad
4. Department of Electronics & Communication Engineering
Poornima Institute of Engineering & Technology, Jaipur

Article Info
Page Number: 1519-1528
Publication Issue:
Vol. 71 No. 4 (2022)

Article History
Article Received: 25 March 2022
Revised: 30 April 2022
Accepted: 15 June 2022
Publication: 19 August 2022

Abstract

As IoT is appearing as essential technology used for daily routine work associated with the home appliance and mobile. IoT is a combined structure of Internet, Network users, smart electronics devices, data and its digital form. With the development of IoT many issues are needed to be solved specially related to internet or network security. It is a prime goal to protect IoT system from various security vulnerabilities and cyber attacks. To keep system or mobile device protected from the malware is the basic foundation for the IoT. This paper reviews the theoretical perspective of the cyber attacks and security protection for the information communication technologies and smart devices being utilized for the IoT applications.

Keywords: IoT, Cyber Security, Cyber-attacks, Security Threats.

Introduction:

IoT is a system, which interconnects some smart digital devices to each other through internet. Now these days uses of IoT devices in our daily routine are increasing and have become a routine part of life. IoT is making automated control not only home devices but also system at Industries and businesses are being automated and controlled through the internet.

Implementation of IoT provides support to bring more business to various companies in their supply chains to logistic operations and help to achieve economic benefits. Benefits aside, connecting systems with the internet also bring potential cyber threats.

When a home appliance becomes internet enabled it becomes a device which may be exploited by the cyber criminal just like your phone or laptop. With the increase of the IoT with more devices, vulnerabilities will increase which will invite more cyber attacks due to weak or no cyber security. More use of IoT will lead to more cyber risks that will invite threats to security as well as integrity of the data. As per the study by 2020 the number of installed IoT devices is supposed to grow to approximately 31 billion worldwide **[1].** So it is becoming necessary to protect IoT system and entire data associated with it. So for the organizations it is required to establish cyber security measures to protect their core IoT investment and infrastructure.

Features of Internet of Things:

- IoT provides a network between two or more electronics devices for communication over the Internet at smaller and cost reliable scale.
- IoT use artificial intelligence and big data to establish the network.
- IoT devices enable passive devices in to active devices with the help of various sensors [2].

Figure 1 features of IoT

Characteristics of Internet of Things:

- All devices used for Information and communication can be connected each other through IoT.
- IoT brings diverseness among all the devices that are connected to each other through a network and hardware platform.
- IoT provide awareness of sensor technologies to the internet world by using analog means. IoT is becoming a large platform as everyday more devices are being connected through the internet. So challenges are also introduced with their data security, device security and privacy of an individual and device security [2].

Attacks:

Attacks are considered as a kind of invasion to harm a digital system and to disrupt its normal operations to steal the data or to damage the system completely. For this attackers launch various malwares to exploit the vulnerabilities of the system or network.

An attack may be active or passive attacks. Active attacks monitor the traffic of the network to search the valuable information.

While passive attacks such as monitoring a network, poor encrypted communication traffic, more vulnerable and likely to be exploited by insiders and etc.

Common cyber-attack types are as follows:

(a) Physical attacks: these types of attacks intervene with hardware involved in the IoT systems. Maximum devices in IoT operate in outdoor environment; also their mode of operation is in distributed system so chances of being compromised are high.

(b) Reconnaissance attacks: These types of attacks include unauthorized accessing of systems, services, and make use of vulnerabilities of the system. For example scanning of network ports, packets sniffing, traffic analysis and asking for the IP address.

(c)Access attacks: In this an unauthorized persons try to gain access to networks or devices to which they have no right to access. They may try to get physical access or they may try to get the remote access by accessing the IP address.

(d) Attacks on privacy: privacy of a user's or organization information in IoT is a big challenge due to huge amount of information may easily available through remote access process [3].

Protecting the IoT System:

The intellectual data which are generated by IoT system are required to be protected. The intellectual property of organization or an individual also need to be protected from competitors. If IoT system is not protected then important information or data will be on high risks to malicious activities. IoT is interconnected with other networks through internet so

security is vital act to provide safe guard due to vulnerabilities of some other part of the internet. So it is crucial to provide safe guard to one's own intellectual properties. In the fast growing IoT, risk in security and privacy is also increasing. Many of them are attributable to system vulnerabilities that comes from cyber crime and misuse of the system resources. The IoT needs to be built in such a way as to ensure easy and safe usage control. Users required to include IoT to avail full facility of IoT and avoid security breaches. To remove vulnerabilities and protecting IoT devices from common attacks using some simple steps will not be sufficient. It is mandatory to make a specific policy and guidelines supported by the stealth protection procedure are needed.

Why IoT devices are more vulnerable to Cyber attack

With compare to desktop, laptop and mobile system most of the IoT devices have their original firmware. Frequent updates are rare so IoT devices are likely to be more vulnerable also these devices are connected with the customer's local network for internet access. This result IoT devices may be compromised by attackers very easily. With IoT technology, there will be more offline objects connect to online and will become vulnerable to cyber attacks.

- Because IoT is connected with the Internet so the risk of malware attack is high and causes a catastrophic failure of the system.
- IoT systems are used by some companies, media to communicate with their technology partners or customer which has become vulnerable to Cyber attacks for hacking. Many organizations do not continuously update IoT devices after installation they are having their original firmware.
- Some IoT devices do not have the ability to update themselves and receive patches to update security settings automatically from the internet [4].

Major Cyber Threat Landscape:

There are multiple applications of IoT which are vulnerable to cyber threats. Figure 1 shows some examples of IoT applications in different Industries which are most vulnerable to cyber attacks.

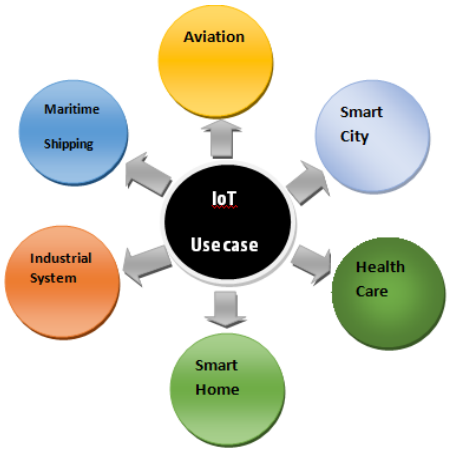

Figure 2 IoT applications in various Industries

- **Aviation**: Number of applications is there for IoT in Commercial as well as in military aviation. All the functions and commands are driven by the IoT devices like Engine performance improvement, accurate weather forecast, pilot monitoring and control p anels.

If there is any vulnerability available, this vulnerability may be exposed by the attackers and entire aviation system may come on high risk. Attackers may gain access of some sensitive information, commands such as location of troops, mission information associated with that IoT system; hacker may hijack the control of any aircraft or drones and their weapons to use it against their target enemy.

- **Smart City:** A Smart City can be equipped with IoT enabled platforms like smart grid, smart parking, public safety, traffic control, etc. for example if a smart grid of any country is not secured properly from the cyber attacks then hackers may hack the grid system and may shut down the entire city power. This may affect medical, traffic, transport and other military related entities..
- **Critical infrastructure**: Like a Smart gird the other important infrastructures having electronics systems and useful for domestic and strategic point of you may be vulnerable to the cyber threats. A huge damage or failure may be brought by a malfunctioning of these electronic systems.
- **Health care**: IOT enabled health care system is also in big threat of cyber attacks if any vulnerability found by the attackers. The information related the health care can be stolen and utilized for the financial gain for example insurance claim.
- **Smart Home**: Maximum utilization of IoT in home based appliances is growing day by day. Home door lock system, car lock system etc are some example of it. Possibilities of occurring vulnerabilities in these devices are at maximum because timely update in the software of IoT system is rare so these devices may be utilized maliciously by the attackers. Attackers may get access of IoT devices and unlock the doors or may get full control over the others home appliances by which personal data of individual or any organization may be at high risk**.[5]**

Cyber malware:

IoT may be exploited by Malware attacks. Malware is a code to steal data, controlling the access and cause harm to the IoT infrastructure.

Following are some malware which are major challenge to cyber security for the IoT and related systems. These are: Spyware, Adware, Botnets, Ransomeware, Scareware, RootKit, Virus, Trojan horse, Worms, Man in the Middle (MitM)and Man in the Mobile (MitMO). All these malware are having their separate and own properties and execution procedure.

Spyware: spyware is a program that observes operations at user side secretly. So that cyber attackers can compromise user's system while using the observed information. For example spying the credentials of master card of user attacker may use this card information for his interest.

Trojans: This is a malware which appears as a legitimate software. Cyber attackers trap users into uploading these Trojans onto their system or device where they damage or steal the data.

Ransomware: this is a kind of malware in which attackers hijack the user's information and ask to pay ransom amount by giving the threat of erasing the user's information.
Adware: Advertising software which can be used to spread malware.
Man in the Mobile (MitMO): It is a malware which allows the attacker to take control over a mobile system. It can access the information and data from the mobile. Zeus is an example to exploit the two step verification and allows attackers quietly to capture to steps verification SMS messages sent to users. By which attackers can control the mobile operated IoT systems and get personal or financial gain.

As the figure shows 33% cyber threats are due to various malware intrusion and 41% threats are due to exploitation of the vulnerabilities occurred in the system software and hardware. Whereas 26% cases of cyber threats are associated with user security practices, social Engineering and etc. users should not use their own security algorithms. It is strongly advised to use verified and tested algorithms from selected and valid security libraries only [6].

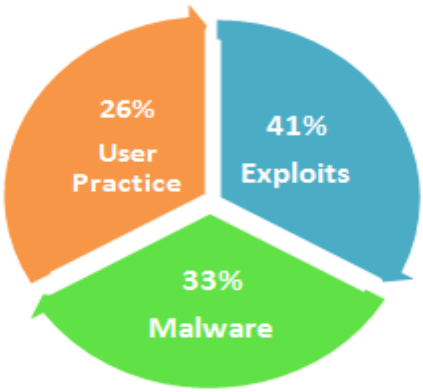

Figure 3 IoT vulnerabilities ratio

How to recognize presence of malware?

If IoT and other associated computing devices get infected from any type of malware then user can identify the symptoms of presence of malware in the system.

User can observe an increase in processor like Raspberry pi, arduino and etc. Speed of the IoT devices and network may decrease. System and devices may freeze or crash often. Web browsing speed decreases. Sometimes unexplainable network problem occur. Files and data in the system connected to each other through IoT are modified or deleted. User observes the presence of unwanted file or icon or running of unwanted processes in the system. Commands or instruction are being sent without the user's consent.

Infiltration in IoT

There are many ways by which infiltration may occur in the IoT and associated network to access the system and manipulate the information. Attackers may use any kind of the method depends upon the category and level of the attacks. Some infiltration methods are as follows

Social Engineering

It relies on people's weakness of being helpful and target their weakness as well. Pre-texting, tailgating and something for something methods considered in social Engineering to get access of the network or system. Pre-texting In which attackers calls to user and lies to them to get access of the system and in tailgating attacker quietly follows an authorized person into a secure location and find the details to access the system where as in Something for something attackers request personal information from the user in exchange for something precious .

Password Cracking

Network sniffing and brute force attacks are the possible ways to crack the password of the system or any Wi-Fi network. In brute force attacks attackers tries several possible passwords by guessing the password and in network sniffing attackers continually listen and capture the packets sent on the network. If password is unencrypted or weakly encrypted password may be cracked easily.

Phishing

In this attacker sends a fraudulent mail or message disguised from a valid or trusted source to trap the user to introduce the malware in his or her device to access the personal information.

Vulnerability exploitation

Attackers gather the information about targeted system. This information may be about the operating system and other services running on the targeted system. After knowing this information any vulnerability is searched by attackers and then attacker exploits these vulnerabilities with various malwares.

Advanced Persistent threats

Due to its complexity and high level skill requirement attackers must be skilled enough to launch a long, multiple, and advanced attacks on the system that is to be targeted. Its main targets are big organizations, state and nations.

DOS (Denial of Service)

DOS attacks are kind of network attacks which can destroy complete IoT network. In this a network or host device is sent either large quantity data or maliciously formatted packets at a rate which the host cannot handle these high rate packets and cause a slowdown or complete crash of the IoT network.

DDOS (Distributed Denial of Service)

Like a Denial of Service, infected packets are sent and make the target system infected. In this these infected packets originates from multiple and coordinated sources. The infected hosts are called zombies and the network of these infected hosts is called BOTNET of zombies which in turn the complete failure or slow down of the network.

SEO Poisoning

A malicious user can utilize Search Engine Optimization to make malicious websites appear higher in the search results. This is called SEO poisoning. By this traffic on malicious websites is increased and possibilities of attack increased.

Aftermath of security breaches on IoT

Security breach leads to loss of very private and important data like bank details and passwords that may lead to economic damage.

Cyber attacks may ruin the reputation of the organization and trust between company and client. As after maliciously accessing the network data of client connected with the network may also be manipulated. The data and information may be theft which are further become a legal issue for the company or individual. Ruined reputation of the organization may bring the revenue loss and losses in future economic deals. Some information of the individual or organization is so important which can lead towards the loss of their intellectual property damage.

Impact Reduction

100% security by any set of security practice is not possible from security breaches. Because a breach is likely to happen if any type of information on the network is available and useful for the attackers to get personal or financial gain. data breach is a very dynamic process [7]. So, important measures should be taken by the individual or company to protect their IoT network. Like inform to all internal staff and take the action against breach as early as possible. External clients must also be informed immediately through official means.

It will develop the transparency which is helpful in this type of situation. Every employee and management of the organization should be sincere and accountable during losses due to security breaches. Company should take care of the costs of identity theft protection services for affected IoT customers and users. Forensic experts should be hired to find the losses and cause of the breaches and learn the details and apply measures so that similar attacks in future may be prevented.

All the system software and hardware should be updated and upgraded regularly. Ensure that after any attack no backdoor should be create which may facilitates more future attacks in the network. Proper education regarding safe access of the system should be given to all users including employees and customers. Proper encryption of the information should be done while transmission. Software up gradation and regular backup of data will also protect IoT system from various cyber attacks. Implementation of two step authentication while using the network and timely changing of password will also provide a secure environment for the IoT system. An isolated network must be provided to the IoT infrastructure to reduce the cyber threats at significant level [8].

Conclusion:

IoT may be exposed to various security threats which must be recognized and same time security action must be taken. In this paper we studied about various applications of IoT and cyber attacks and measure to protect IoT. Our interest is to identify various malware and consequences due to any vulnerability in the IoT system. We provided an overview of the some general challenges to the IoT security while focusing on various security breaches. We also discussed the Impact reduction of cyber attacks which make a vital role just after any attacks. If provide a safe and secure environment to IoT system and network then IoT and its applications will bring immense value into our daily routine with newer wireless networks, advanced sensors and fast growing and upgraded computing capabilities.

Future Scope:

By 2025, it is estimated that there will be more than to 21 billion IoT devices. Malicious activities will also increase accordingly Cybercriminals will utilize IoT devices to facilitate DoS attacks. Also number of cities will move towards becoming smart cities so IoT based DOS attacks will increase which may cause a dangerous and fatal loss. India has turned into a breeding ground for Cyber Security experts. The scope of Cyber Security will increase in the country as well as in other parts of the world

References:

1. Shruti Thapar, M Venu Gopala Rao, Babita Jain, Rohan Sharma , "A Review on Routing Protocol of MANET with its Characteristics, Applications and Issues", International Journal of Early Childhood Special Education (INT-JECSE) DOI:10.9756/INTJECSE/V14I5.305 ISSN: 1308-5581 Vol 14, Issue 05 2022, pp. 2950-2956.
2. S. Andreev and Y. Koucheryavy, "Internet of things, smart spaces, and next generation networking," Springer, LNCS, vol. 7469, p. 464, 2012.
3. Shruti Thapar, "A Review: Study about Routing Protocol of MANET", International Conference on "Smart Innovations for Society" (ICISC-2022) on 6-7 May 2022, in Scopus Proceedings.
4. L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer networks, vol. 54, no. 15, pp. 2787–2805, 2010.
5. Shruti Thapar and Sudhir Kumar Sharma, "Detection and Prevention Policies of Attack in MANET" Proceedings of International Conference on Innovative Advancement in Science and Technology (IAET 2020), India, https://dx.doi.org/10.2139/ssrn.3548382.
6. R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Compute Networks, vol. 57, no. 10, pp. 2266–2279, 2013.
7. Shruti Thapar, M Venu Gopala Rao, Babita Jain, Rajkumar Kaushik, "A Secure Routing for MANET using Internet of Things", International Journal of Early Childhood Special Education (INT-JECSE)DOI:10.9756/INTJECSE/V14I5.305 ISSN: 1308-5581 Vol 14, Issue 05 2022, pp. 2957-2965.

8. H. Ning, H. Liu, Cyber-Physical-Social Based Security Architecture for Future Internet of Things, Advances in Internet of Things 2 (1) (2012)
9. S.Thapar and S.K.Sharma, "Direct Trust-based Detection Algorithm for Preventing Jellyfish Attack in MANET", 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), IEEE, DOI: 10.1109/ICECA49313.2020.9297601, ISBN: 978-1-7281-6387-1, pp. 749-753, 2020.
10. R. Roman, P. Najera, J. Lopez, Securing the Internet of Things, IEEE Computer 44 (9) (2011)
11. Shruti Thapar, M Venu Gopala Rao, Babita Jain, Rohan Sharma , "Research Article on Routing Protocols for MANET: A Review", International Journal of Early Childhood Special Education (INT-JECSE)DOI:10.9756/INTJECSE/V14I5.305 ISSN: 1308-5581 Vol 14, Issue 05 2022, pp 2939-2949.
12. D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, 2012.
13. Shruti Thapar and Sudhir Kumar Sharma, "Study of Direct Trust Based Detection Algorithm for Prohibiting Jellyfish Attack in MANET", ILKOGRETIM Online, doi: 10.17051/ ilkoline.2021.04.234, volume 20 issue 4, 2021, page no. -2052-2057.
14. J. Sheldon, "State of the art: Attackers and targets in cyberspace," Journal of Military and Strategic Studies, vol. 14, no. 2, 2012.
15. Shruti Thapar and Sudhir Kumar Sharma, "Analysis of Isolation access of Wormhole Attack in Mobile Ad hoc Network using Delay Prediction Technique", International journal of Advanced Science and Technology (IJAST), ISSN: 2005-4238 IJAST, volume-29 issue-6, 2020, page no.- 9401-9411.
16. A. Sarma, J. a. Gir~ao, Identities in the Future Internet of Things, Wireless Personal Communications 49 (3), 2009.
17. Shruti Thapar and Sudhir Kumar Sharma, "An Integrated Approach for Detecting Wormhole and Jellyfish Attack in MANET", International Conference on Engineering & Design (ICED) 25-26 June-2021 ISBN: 978-81-954037-0-7, pp.51- 63.
18. Shruti Thapar and Sudhir Kumar Sharm, "Attack and Security Issues of Mobile Ad Hoc Networks", Proceeding of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM 2019), India, https://dx.doi.org/10.2139/ssrn.3356214.