International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 9, ISSN No. 2455-2143, Pages 160-163
Published Online January 2020 in IJEAST (http://www.ijeast.com)

A SURVEY ON VARIOUS IOT ATTACK AND IT'S LIMITATIONS

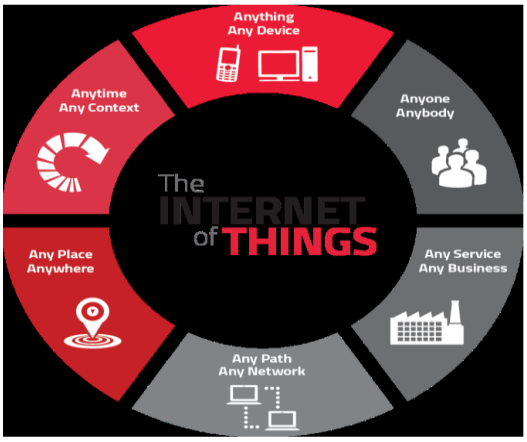
Anamika Goel
Asst. Prof., Department of Information Technology,
SGIT School of Management, Ghaziabad, India

ABSTRACT: The term Internet of Thing (IOT) can be defined as a network of connected device-all of which collect and share information about how they are used and the environments in which they are operated. In that way each devices will be learning from the experience of other devices, as human do. They are used in our homes, in hospital, prevent fires, and many more beneficial functionality. However, all those benefits can come with more risks of privacy loss and security issues. As the network grows, volumes of data increase and more information is at risk. To secure the IOT devices, many research works have been conducted to identify security issues and find a better solution to eliminate these issues, or at least minimize their effects on the user's privacy and security requirements. In this paper we briefly discussed about what IOT is, characteristics of IOT & what are the limitation of IOT. After discussing limitation of IOT, we also discuss some solution to overcome the limitation of IOT and after that we also discuss various possible attacks on IOT Network.

Key Terms: *IOT (Internet of Things) definitions, IOT characteristics, IOT Attacks, privacy and security.*

I. INTRODUCTION

The term Internet of Thing (IOT) can be defined as a network of physical devices embedded with different kinds of sensors called "things" or smart devices which allows these devices to collect and exchange data. According to "Dr.Ovidiu Vermesan (2104)"There is no hotter technical field right now than the Internet of Things (IOT). Everyone who is providing an internet connected device has an IOT story. Before I discuss about an IOT security strategy today, I just want to explain why we want to connect things. The benefits are easy access, sharing information and various resources, control application, performances and optimization. When everything is connected and communicating, devices work together, We can access all these things, information/data from everywhere and anywhere. we also collect, share and analyze information in a better way All of this connectivity leads to higher performing systems, cost savings and new revenue streams.



Internet of things

Internet of Things extended the communication with the help of internet to all the things that surround us. It is not a single technology, but it is a mixture of different hardware & software technology. As we gain benefits from the IOT, not forget about privacy and security. Dr. Ovidiu Vermesan SINTEF, Norway, Dr. Peter Friess EU, Belgium (2013) Existing data privacy and security solutions to the Internet of Things (IOT) application is not easy to implement because of IOT device heterogeneity, dynamic changes and possibly unprotected surroundings. As both the originator and recipients of the IOT, we must need to design various security measures/application for privacy and safety. It includes the safety of our personal information and the safety of our physical well-being.

Characteristics of IOT

Following are the fundamental characteristics of the IOT devices.

Interconnectivity: According to the IOT, any devices can be interconnected with the global information and communication infrastructure.

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 9, ISSN No. 2455-2143, Pages 160-163
Published Online January 2020 in IJEAST (http://www.ijeast.com)

Things-related services: Thing-related services meaning are security and semantic consistency between physical and virtual things. In order to provide thing-related services, both the technologies in the physical world and information world will change.
Heterogeneity: The devices in the IOT are heterogeneous on the bases of different hardware platforms and networks. They can interact with each other devices through different networks.
Dynamic changes: The devices state change dynamically, e.g., sleeping and waking up, connected and/or disconnect. Moreover, the number of devices can change dynamically.
Enormous scale: The devices connected to the internet is larger than the order of magnitude to the devices needs to be managed and communicated with each other.
Safety: Apart from gaining some benefits of IOT, we must not forget about safety. As both the originator and recipients of the IOT, we must need to design various security measures/application for privacy and safety. It includes the safety of our personal information and the safety of our physical well-being. for example If a situation comes like a hacker changes your medical prescription and you are supplied expired medicines then there would be a health disaster. Since the user would be dependent entirely on the technology.

Limitations of IOT Devices

The following is the some of the limitation of IOT that need to be addressed before adoption of IOT can occur. Dr. Ovidiu Vermesan SINTEF, Norway, Dr. Peter Friess EU, Belgium (2013,2014)

A. Security: IOT technology creates a system of connected devices. Since everything will be connected inside the network would be easy by the hackers. By entering into just a part of network would reveal everything. During this process, the system may offer some authentication control mechanism apart from sufficient security measures.

B. Privacy: Even without the active participation on the user, the IOT System provides substantial personal data in maximum detail. This creates lots of privacy issues.

C. Cost versus Usability IOT uses to connect physical devices to the Internet. Adoption for IOT to increase, the cost of components that are needed to support sensing, tracking and control mechanisms need to be relatively inexpensive in the coming years.

D. Interoperability

IOT systems require high degree of compatibility or interoperability. It is the most basic term; first requirement of Internet connectivity is that "connected" systems be able to "talk the same language" of protocols and encodings. Today Different industries use different standards/Methods to support their applications. With numerous sources of data and heterogeneous devices, the use of standard interfaces between these diverse objects becomes important. For example Apple devices don't accept the connectivity with any other device.

E. Data Management

Data management is a most important aspect in the Internet of Things. When considering a world of devices interconnected and regularly exchanging all types of information, so the large volume of the generated data and the processes involved in the handling of those data become critical.

F. Device Level Energy Issues

One of the most challenging question come in our mind is how to connect "things" in a way while taking into account the energy constraints, knowing that the communication is the most energy consuming task on devices.

G. Complexity:
Designing of an IOT system is quite complicated that's why it's deployment and maintenance also not very easy.

Requirement of IOT Security: following are the some basic requirement to overcome some IOT limitations.

- **Trust** – Firstly authenticate and establish trust between devices/users when it connects to the network. It. Once trust is established, devices/users and services can securely communicate encrypted data /information to each other.
- **Privacy** – When more number of things/devices connected in a single network, huge volume of information is generated/collected and shared. A strong IOT network can ensure all kind of information are secure and in encrypted forms and also ensure communication will remain private.
- **Safety** – The safety of the users is very important. This can be in an environment where a malicious

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 9, ISSN No. 2455-2143, Pages 160-163
Published Online January 2020 in IJEAST (http://www.ijeast.com)

attack on the single sensor could cause harm to devices/users. When the defect goes unnoticed before going to market, user safety can also be at risk.

- **Integrity** – Integrity applies to both the devices and the information being transmitted within the IOT system. The integrity of a device define it is what it says it is. With a unique identity of a device, we can ensure that the device software and firmware are legitimate – reducing and protecting a company's brand. Basically integrity define What good is connecting all of these devices if the information being transmitted is unreliable?

II. CLASSIFICATION OF IOT ATTACKS

According to Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad,R.(2011).

We can classify generally five categories of IoT security attacks, namely:

1. Botnet
2. Man-in-the Middle
3. Identity Theft
4. Social Engineering
5. Denial Of Service

Botnet:

It is a group of computer work together to complete some particular task and sharing computer resources. Also combined together with the purpose of remotely taking control and distributing malware. "Shancang Li & Li Da Xu & Shanshan Zhao"(26 April 2014)they are used by criminals on a grand scale for many things. for example stealing private information, exploiting online banking data DDOS attack.

Man-in-the Middle:

Man–in-the Middle attack a hacker, or unauthorized users are looking to interrupt communication between two separate systems. "I.Andrea, C. Chrysostomou, and G. Hadjichristofi"(july 2015) It can be dangerous because it is one where the attacker secretly intercepts and transmits message between two parties when there are under the belief that they are communicating directly with each other.

Identity Theft:

The main strategy of identity theft is to a mass data and with a little bit of patience, there is a lot to find. General data available on internet, combined with social media information plus data from smart watches, fitness trackers, smart fridge and much more. These all give a great all round ideas of or personal identity.

Social Engineering:

It is the act of manipulating people, so they give up confidential information. Then The type of information that the hacker is searching can vary when any single user are targeted. "Antonio J. Jara, Miguel A. Zamora and Antonio F. G. Skarmeta,"(2010)their criminal is usually trying to deceive the user in to giving them the password or bank information.

Denial of Service:

It happens when a service that would usually work is unavailable. There can be many reasons for unavailability but is usually referring to infrastructure that cannot cope due to capacity overload.

According to Andrea et al.(2010) IOT devices attacks classify in four distinct types: and each type can cover the different layer of IOT architecture 1) physical Attack;2) network attack; 3) software attack; and 4) encryption attacks. This layered structure also use some IOT protocol for encrypt information first physical attack is performed when the attacker is in a near distance of the device. It comes under physical layer of IOT Structure. Second kind of attack is network attack come under network layer of IOT structure. This attack manipulating the IOT network system to cause damage. Third kind of attack is software attack this attack happen when the IOT applications present some security vulnerabilities and harm the system. Encryption attacks come under the application layer of IOT Architecture. Following kind of attacks come under the encryption attacks like side channel, cryptanalysis, and man-in-the-middle attacks.

According to Andrea et al. [2016] The solution of following security Attacks is at the physical layer, the connecting devices uses a cryptographic hash algorithm and digital signature to verify device authentication and integrity of the software. In addition to that, to maintain confidentiality and data integrity of a device should also uses various error detection algorithms and data is in encrypted form. At the network layer, to ensure privacy and security of data /information various authentication mechanisms and point-to-point encryption techniques used. The application layer allows only the authorized users to access data/information through firewalls and use of anti-virus software. This layer

provide security by means of authentication, encryption, and integrity of data/devices.

III. CONCLUSION

IOT technology introduces several new applications and various exciting opportunities. However, it is critical that solutions be adopted to ensure safety security and privacy of IOT systems with minimal impact on performance, usability and scalability. The Internet of things technologies are exposed to various types of attacks. An attacker can attack for different objectives. In this paper, we identified, discussed, and presented various types of IOT and its countermeasures in a systematic way. Here we also explore the most significant Limitations of IOT devices and its requirements.

IV. REFERENCES

[1] Dr. Ovidiu Vermesan SINTEF, Norway, Dr. Peter Friess EU, Belgium (2014),"Internet of Things–From Research and Innovation to Market Deployment",river publishers' series in communications.

[2] Dr. Ovidiu Vermesan SINTEF, Norway, Dr. Peter Friess EU, Belgium(2013)."Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems", river publishers' series in communications.

[3] Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad,R.(2011).Proposed embedded security framework for internet of things (Iot). In Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE),2nd International Conference on IEEE (pp. 1-5)..

[4]I.Andrea, C. Chrysostomou, and G. Hadjichristofi (july 2015) "Internet of Things: Security vulnerabilities and challenges," in Proc. IEEE Symp. Comput. Commun. (ISCC), Larnaca, Cyprus, pp. 180–187.

[5] E. Ronen and A. Shamir march (2016)"Extended functionality attacks on IoT devices: The case of smart lights," in Proc.IEEE Eur. Symp. Security Privacy (EuroS P), Saarbrücken, German, pp. 3–12.

[6] Karlof, C., & Wagner, D. (2003). Secure routing inwireless sensor networks: Attacks and countermeasures. Ad hoc networks, 1(2), 293-315.

[7] Shancang Li & Li Da Xu & Shanshan Zhao 26 April 2014"The internet of things: a survey", Published online: 26,Springer Science+Business Media New York 2014

[8] Antonio J. Jara, Miguel A. Zamora and Antonio F. G. Skarmeta,2010 "An architecture based on Internet of Things to support mobility and security in medical environments", University of Murcia, Computer Science Faculty, Murcia, Spain.