International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 10 | Oct 2019 www.irjet.net p-ISSN: 2395-0072

Cyber-crimes and Privacy Concerns in IoT Security

Siddhi Desai

Mukesh Patel School of Technology Management and Engineering
Narsee Monjee Institute of Management Studies
Vile Parle (West), Mumbai, India.

Abstract-*Internet of things (IoT), also referred to as the internet of objects, is a dynamic global information network consisting of internet – connected objects. Internet of Things (IoT) is a network or interconnected system of physical objects that can be connected to internet. It is used to interact and communicate within each other and the external world. IoT helps to exchange data over the Internet. There are already 6 billion devices on the internet and within a few years these number is anticipated to scale to 20 billion devices. As the Internet of Things is transforming the entire world of business in every industry and home, we obviously need tremendous amount of Security policies.*

Key Words: **IoT, IoT security, Privacy, Cyber-crimes, Security Frameworks**

1. INTRODUCTION

IoT is a network system in both wired and wireless connection that consists of many software and hardware entities such as manufacturing management, energy management, agriculture irrigation, electronic commerce, logistic management, medical and healthcare system, aerospace survey, building and home automation, infrastructure management, large scale deployments and transportation [1]

IoT has changed the aspects of the interconnected world, it not only connects physical things with technology but it also does tasks like humans with the means of Artificial Intelligence and Machine Learning.

A new technology coming up every day is making the world much more connected and a smaller place for us. Things are getting more and more digitalized. Every device that we see, we hold, we use is connected to the internet and there is a huge amount of data all over the cloud.

With these huge amount of data over the internet, it increases the risk factor as well. The data is vulnerable and easily accessible to the cyber attackers. Cyber-attacks are increasing day by day and they pose as a hindrance in the success of the IoT.

Security is process and not product. The number of potential threats and possible effects against security or privacy of things or an individual has grown rigorously. For providing a large number of reliable services, designers stumble upon several challenges in particular, in security – related research areas. It is unfortunate that these security needs are not yet well – recognized. Hence it is necessary to study about the security threats and general privacy issues. [2]

The structure of the paper is as follows: In the types of cyber-crimes (Section II) section it list the types of different cybercrimes; Section III describes the IoT privacy and it's challenges. Section IV is about security frameworks. Section V concludes the paper.

1.1 Types of cyber- crimes

1) **Physical cyber- attacks**: Cyber-physical attacks are not the only attacks that exploit interactions between cyberspace and physical space. The reverse, where an attack in physical space aims to affect the availability, integrity, or confidentiality of information in cyberspace, is by no means new or uncommon. It's estimated that approximately 70% of all cyber-attacks are initiated from the inside, whether purposeful or the result of human error.
These types of attacks tamper with the hardware components and are relatively harder to perform because they require an expensive material. Some examples are de-packaging of chip, layout reconstruction, micro-probing, particle beam techniques, etc. [3]

2) **Software attacks:** These are programs written deliberately to vandalize someone's computer or to use that computer in an unauthorized way. There are many forms of malicious software; sometimes the media refers to all malicious software as viruses. Software attacks occurs when a file with malwares are installed on one's computer. The attackers create programs specially with malwares to attack and steal the private data. Jamming attack is the one of the ruinous invasion which blocks the channel by introducing larger amount of noise packets in a network. Jamming is the

biggest threat to IoT. Where a network consists of small nodes with limited energy and computing resources. So it is very difficult to adopt the conventional anti jamming methods to implement over IoT technologies. [4]

3) **Network cyber-attacks:** The network cyber-attacks don't need a physical environment to attack, the wireless network are most vulnerable to attacks. Basically attacks are classified as active and passive attacks.

4) **Social Engineering:** It is an act or mechanism to extract information from the people in a skillful manner. The information can be like personal details of debit/ credit cards. The victims are manipulated by the attackers to share their personal details or give access to the victim's computer, eventually extracting all the details. The purpose of the attacker may vary, but the path followed might be the same. Mostly, in social engineering, the attacks are done in the form of phishing emails.

1.2 IoT privacy challenges

Privacy in IoT defined by the Internet security glossary [5]as "the right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others".

Internet of Things privacy is a motive taken into consideration to protect the information of individuals from the exposure of IoT environment, in which almost any physical or logical entity or object can be given a unique identifier and the ability to communicate autonomously over the Internet or similar network. Since everything will be connected intruding inside the network would be easy. By entering into just a part of network would expose an individual or organization or both.

1)Device Privacy: Sensitive information in IoT could be targeted when unauthorized access happens in hardware or software. For example, an invader able to re-program a camera to make it sends information not to the authorized server only, but to invaders too.
Mobile device security means the security measures designed to protect the sensitive information stored on and transmitted by smartphones, tablets, laptops and other mobile devices. Mobile device security spans the gamut from user authentication measures and mobile security best practices for protecting against compromised data in the event of unauthorized access or accidental loss of the mobile device to combat malware, spyware and other mobile security threats that can expose a mobile device's data to hackers.

2)During Communication Privacy: Data confidentiality when data being transmitted through network channels commonly achieved using encryption techniques. Encryption in some cases adds data to packets to provide tracing property. Communication Protocol for security can provide some solutions for privacy. [6]

3)Storage Privacy and its processing: Protection of private information is essential least amount of data should be stored to prevent any risk and loss of data. Personal and sensitive data must be processed in a suitable manner and for the processing aim only.

2. Security Frameworks

The three security frameworks need to be balanced in order to ensure wise implementation and use of the mechanism. The framework is as follows:

1) **Confidentiality:** The need to keep secrecy of the information and the data.
2) **Integrity:** The assurance that the data that is transported is trustworthy and not malignant.
3) **Availability:** The availability of the resources in form of machines and information anytime that is at a particular instance along with the proper access rights.

3. CONCLUSION

The security in Internet of Things is a sensitive issue and its need to be handled and the security in IoT should be the top most priority. Measures should be taken to ensure that person's information on the IoT should be secured and not accessible to anyone. Using the IoT reference model, each layer will have its own security challenges and issues. Different threats may cause different consequences at each layer. The security challenges that constitute max security breaches in IoT landscape have now solutions identified to prevent attacks.

Henceforth, as IOT blooms as the need of the hour, stringent security measures along with the basic ones(looking at its spontaneous and rapid rate) need to be implemented and legislature should also include rules to adapt to the development and accommodate further evolution of IoT.

ACKNOWLEDGEMENT (Optional)

The author would like to say thanks to all authors of referenced papers and anonymous reviewers for their contribution to this review paper. The author would also like to say thanks to professor Dr. Seema Shah for motivating the author to write this paper, and providing the guidance for completing the paper.

REFERENCES

[1] Long Chen and Shervin Erfani, A Note on Security Management of the Internet of Things,2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE).

[2] Santhosh Krishna B V and Shervin Erfani, A Systematic Study of Security Issues in Internet-of-Things (IoT), International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC 2017).

[3]&[4] C. Ramakrishna, G. Kiran Kumar, A. Mallikarjuna Reddy and Pallam Ravi, "A Survey on various IoT Attacks and its Countermeasures," International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 5, Issue 4, April 2018

[5]&[6] Abeer Assiri, IoT Security and Privacy Issues, IEEE 2018