ISSN Number: 2454-2024(Online)

International Journal of Technical Research & Science

CYBER SECURITY AND THE INTERNET OF THINGS: VULNERABILITY, THREATS AND ATTACKS

Akram Ali, Dr. Arti Vaish
E-Mail Id: akramali.mhs20@sushantuniversity.edu.in, artivaish@sushantuniversity.edu.in
Sushant University Gurugram Haryana, India

Abstract-Cyber Security is a protecting cyber space which includes our critical information or data from getting hacked or attached, damaged by some unwanted person or user [1]. It is very much important for all of us to know about cyber security because everyone of using smart phone, laptop and other digital devices in which more or less our personal data or some of the personal information is saved. So, how we can manage our private data or make it secure by the same unwanted bugs so that they can't misuse of that cyber security comprises of different software program that deals with the protection of our privacy and to protection of our privacy and to protect our personal data getting misused by some of the others programmers or the undefined theft of data. Cyber security comprises of different types of attacks such as malware, phishing and other types of cyber-attacks [1].

Keywords: - Cyber security, Cyber space, Cyber-attacks, Programmers.

1. INTRODUCTION

The vast development of the internet and its ability to offer different types of services has made the technology growing faster and widened all around the world, with huge impact on social life and business world[2]. The COVID pandemic has also made everyone all of us to connect through virtual world no matter how the concern is either it is business purpose, education, communication or the other purpose. Somehow, everyone is using smartphone and laptops for their own service purpose. There data is stored their[2]. laptops These needs to be very much secure because it may contain their private chat, data, information any record. The vast connection of devices all around and the things getting online has created the demand of cyber security of keeping the ones personal data safe and secure. There are very much increased in the cases of cyber threats rising daily and the attacks has been increased as much as the user[2]. As large as the network is growing the cyber threatening is also getting challenged to protect the data. Cyber Security has been authorized to personal to protect damaged, unauthorized access, theft or loss by keeping the confidential information about the object and making the information available whenever they needed without any harm and interruptions. We need the better understanding of the cyber threats and their impact on the program [1]. How it can damage the one's personal data, what is the disadvantage?

2. Background

Internet is the extension of virtual world for intervention with the physical entities for the different purposes as education, business, communication etc. by the different modes through the devices. So there are different modes through the devices. So there are different data involved in different entities of internet[3]. So, we share our personal thought, data, words to each other by different modalities need to conserved and should not be used unethical purpose. To look after this cyber security very much important role in this to keep our data [3].

2.1 Understanding to the Devices and Services

It is very much important to understand about the service us using from what devices because from here it is the main reason for the misplacing of data [4]. Because the some of the service which we are using are not authorized there it may have the chances of losing our privacy of data. There is no any cyber barrier to cop up with your personal devices or the service which you are using., as well there is privacy in data collecting as the data sharing and the management and their security plays and important role in creating secure communications when a number of things communicate in a uncertain inert facilities [3]. There should be the dynamic collaboration impact of both services and device to maintain our data secure and safe.

2.2 Security threats, attacks and Vulnerability

Vulnerability plays a important in a system or its design that allows encroacher to deliver commands and access the unauthorized data or to conduct service attacks [5]. The two main components of the internet service is the hardware and the software. Hardware Vulnerability are very difficult to identify and also if it is identified it is different to fix also whereas the software Vulnerability can be found in operating system, application software or like communication protocols and devices or drives [4].

2.3 Threat

A threat is an action that takes the advantages of security weakness in a system and has negative impact [4]. These threats are caused by the programmers such as malicious threats consisting of internal or external threats (means individual or organization or working outside the network) who is looking into harm and disrupt a system [2].

2.4 Attacks

Attacks are the actions taken to harm a system or disrupt the normal operation by exploiting the vulnerability using various techniques and tools. These attacks are referred as cyber-attacks which harms the ones personal data or acquire the personal information from organization, people or other hacking substitute purpose [4]. Cyber-attacks are the attacks that are related to the of people digital world. An attack may be inform of active network attacks which may be in search of unencrypted search of sensitive information, passive attacks such as hacking of any organization encrypted traffic or gathering information in any private person like back to back account or other sensitive things[5]. Some common cyber-attacks are

- Physical attacks on the tampers of the hardware components.
- Reconnaissance attacks
- Denial of Service
- Access attacks
- Attacks on Privacy
- Cybercrime it exploits user data for materialistic gains, fraud, brand theft.
- Data acquisition.

DISCUSSION

The rapid growth of internet has led to the greater security and privacy risks. The cyber security is designed in a such a way to ensure easy and safe for users [1]. Consumers need confidence to fully accept the interest or the data privacy to enjoy its benefits and avoid security and privacy risks. Cyber architect must be designed in a proper way to cope with the comprised device and be competent in detecting such incidents [4].

CONCLUSIONS

Via Internet we faces a lots of threats that must be identified for to protect and proper action need to be taken for the same. The overall goal is to identify the assets and documents the threats attacks faced by the user. The overview of the research is the internet security problems and to focus on the particular challenges surroundings to device and services. At last we may conclude that lots of security management should be taken from the vendors and the user's side both. It is important to set the standard of upcoming security management.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey,"Computer networks, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] S. Andreev and Y. Koucheryavy, "Internet of things, smart spaces, and Next generation networking," Springer, LNCS, vol. 7469, p. 464, 2012.

[3] J. S. Kumar and D. R. Patel, "A survey on internet of things: Security and Privacy issues," International Journal of Computer Applications, vol. 90, No. 11, pp. 20–26, March 2014, published by Foundation of Computer Science, New York, USA.

[4] A. Stango, N. R. Prasad, and D. M. Kyriazanos, "A threat analysis methodology for security evaluation and enhancement planning," In Emerging Security Information, Systems and Technologies, 2009. SECURWARE'09. Third International Conference on. IEEE, 2009, pp. 262–267.

[5] D. Jiang and C. ShiWei, "A study of information security for m2m of," in Advanced Computer Theory and Engineering (ICACTE), 2010.