Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

Survey Of Iot Threats And Countermeasures: Identifying Solutions And Addressing Future Challenges

Pushpa Latha Thumma[1], Dr Prasadu Peddi[2]

[1]Research Scholar, Dept of Computer Science, Shri Jagdishprasad Jhabarmal Tibrewala University, Rajasthan.

[2]Assistant Professor, dept of computer science and Engineering, Shri Jagdishprasad Jhabarmal Tibrewala University.

ABSTRACT

The Internet of Things (IOT) may be described in a variety of ways. It encompasses many parts of your life, from linked homes and communities to connected automobiles and streets, roadways, and gadgets that monitor your activities. It is expected that one trillion Internet-connected devices will be accessible by 2020 as the eyes and ears of all apps linking these linked objects. The Internet of Things enables billions of people to communicate internationally over a public and private internet protocol network. Around 12.5 billion gadgets and ordinary things were linked to the Internet in 2010. The core concept of the Internet of Things (IoT) has been around for about two decades. Many companies and scholars are fascinated by its enormous effect on society and everyday life. IoT vulnerabilities are becoming increasingly common as the number of IoT devices on the market grows. According to analyses and findings, the enormous adoption of IoT has exposed it to new security dangers. This paper discusses IoT security concerns as well as other unresolved topics. The article also provides a foundation for future research. It also includes a list of security protocols that may be used to support a broad range of IoT applications.

Keywords: IoT,IoT applications, IoT Security, Edge Computing, Distributed Systems, Machine Learning.

1. INTRODUCTION

IoT-connected devices will reach 75 billion in 2025, according to 1 These devices can improve people's lives as well as the efficiency of businesses. However, they increase vulnerability to cybercriminals and hackers. IoT-enabled components and devices are increasingly interdependently integrating into every sector of work. The operations of interdependent components will be severely affected if one of these components is damaged. Experts and policy-

makers are becoming more concerned about protecting IT infrastructure and information from such attacks. Cyber-sabotage attacks are most likely to target people, technology and enterprise constituents. All industries have made industrial security a top priority. Many industrial control systems (ICSs) are legacy systems that have connectivity issues and are vulnerable to attacks. These systems were not intended for such connectivity and security design upgrades are required. The Internet of Things is gaining popularity, connecting every piece of equipment to it to make it easier to manage and communicate with them. This has led to an increase in the number and severity of cyberattack vectors as more industrial control systems become interconnected. The key to successful IoT application to industry is the ability to monitor the network infrastructure in real time and the associated service operations. This will allow for the automation of data delivery, which can lead to secure and high-quality services.

The Internet of Things' future is anticipated to be endless [4]. You can speed up the growth in the field of Industrial Internet through speeding up the development and that of integrating artificial intelligence mass use, automation, regulation of their usage and increasing the speed of its use. Massive amounts of actionable information will be available to you, which can also lead to automation of business processes. The IT market will see a significant shift. The Internet of things trend isn't just for the commercial and industrial sectors. It also surrounds us at our home as it controls various appliances and hospitals. We must ensure that these technologies are safe. There are many benefits, but also dangers. Insecurity can make us vulnerable to security threats and vulnerabilities. There is a possibility for cybercriminals to take advantage of security weaknesses to gain access to data and other information. They may misuse and alter it in order to use it for their own benefit. You could be at risk to various types of attacks, such as flooding, interference, denial-of-service (DOS) black holes, wormholes and black holes as well as Sybil and sinkhole types. Each layer is able to fulfill the security requirements of another layer the security requirements vary from one layer to the next [5].

2. **What is IoT?**

Kevin Ashton created the term "Internet of Things" (IoT). It was used primarily for basic things. "A basic creation" by "adding radio frequency ID and restart operation to everyday items." We chose the term "things" over the word "devices" simply because this technology encompasses everything that can be connected to the Internet. Although the term may seem somewhat new to us, it actually existed in real life since the seventies, in particular 1974. This was the year that automated teller machines were introduced, and they are now considered to be one of the IoT devices. However, 87% of IoT users did not understand the meaning of the term in 2015. These paradoxes are quite bizarre, as in 2008 Cisco reported that there were more devices connected to the Internet then people. All over the globe. In 2018, this number was almost five billion.

Fig 1: . Internet of things.

3. Security threats and attacks in IoT

Although using the Internet of Things has many advantages, such as its application across a variety of domains However, there's one thing that we must not overlook. It poses security risks and dangers that could impact users. Recent studies show that 90 percent of Internet users don't have confidence in their device's security. Security is therefore an essential element to be able to provide security and privacy to the system that runs the device [16,17]. IoT security is what you must be focusing on to safeguard devices that are connected and to preserve the networks, data and businesses within IoT [9]. The safety issues are increasing in number due to the doubling and continuous growth of Internet device usage. Because of its design system, the traditional security technology for IoT cannot be implemented directly. This limited number of devices presents problems with heterogeneity as well as scalability. It is important to remember that the system can be adapted to meet unexpected and expected risks. In order to use the appropriate algorithms and protocols as well, we need to integrate safety measures into the Internet of Things. Wireless communication is a key technique for numerous attacks and privacy breach, since it is utilized to exchange information across Internet of things devices. It is essential to ensure that the information exchanged is secure. Security issues with data [18-21] are designed to ensure the security, reliability and confidentiality of data. Security issues can then be addressed using security measures. You can improve security by making sure that only authorized users are able to access the network and removing any unauthorised users to the network. Data integrity can be maintained by ensuring that users keep data integrity. Access to networks resources, applications and services is feasible when there aren't any barriers to accessing authorized information [12]. In today's context, security and privacy are the real issues.

4. Countermeasures

Examine this section to highlight the importance of securing the infrastructure needed for the Internet of Things. Manufacturers should consider seriously the importance of searching out the

most secure and practical solutions. The manufacturer should make sure the devices are only authorized to contact services. It is imperative that you verify the authenticity of all communications before sending and receiving data. Fig. 2 shows the attack on the various layers of the Internet of Things.

Fig 2: IOT Attack and Countermeasures.

5. **Security analytics**

The analysis process includes gathering data, running analyses on it, assessing its effectiveness, and finally submitting reports. If any errors or illegal activity is found here, we will take care of it. Additionally, it offered fresh models that can anticipate and detect suspicious activity using artificial intelligence, big data, and other tools. The demand for a wider range of security analysis techniques is being driven by the urgent need to detect security lapses and assaults.

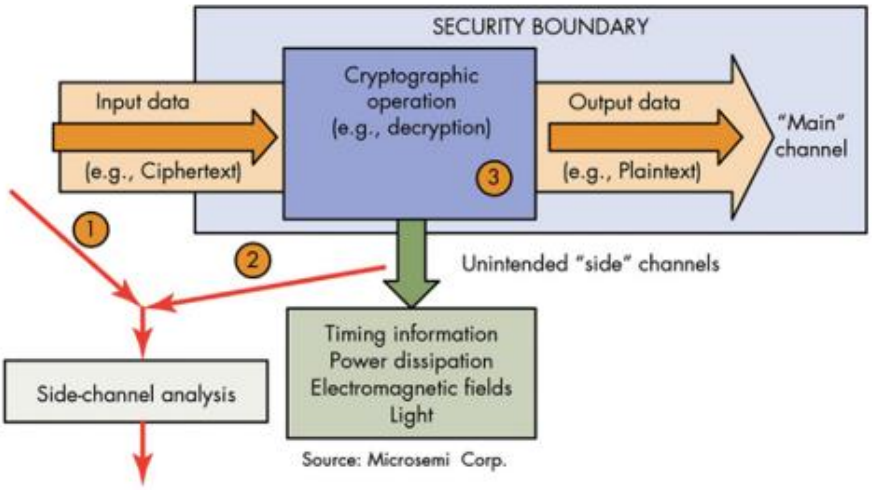

Fig. 3. Security-side-channel attacks .

6. CONCLUSION

This article examines the difficulties brought by privacy and security concerns in IoT devices. In addition, it examines the most major applications, such as "smart city," "smart housing," and "smart house," along with the associated dangers and hazards. In addition, we walked over each method and reviewed its implementation. In addition, we reviewed the potential dangers presented by each Internet of Things layer as well as the necessary steps to take against them. In addition, we discussed the most important techniques and tools for developing such a system, which will contribute to enhancing the security of the Internet of Things.

References

[1] H.A. Salam, A. Ahmed, A. Muhammad, The Internet of smart things in the field of health care, J. Acad. Res. (2019).
[2] M. Humayun, M. Niazi, N.Z. Jhanjhi, M. Alshayeb, S. Mahmood, Cybersecurity threats and vulnerabilities: A systematic mapping study, Arab. J. Sci. Eng. 45 (4) (2020) 3171–3189.
[3] M.A. AlZain, B. Soh, E. Pardede, A survey on data security issues in cloud computing: From single to multi-clouds, J. Softw. 8 (5) (2013) 1068–1078.
[4] H. Alshambri et al., Cybersecurity attacks on wireless sensor networks in smart cities: an exposition, Int. J. Sci. Technol. Res. 8 (1) (2020).
[5] M. Aazam, et al. PRE-Fog: IoT trace based probabilistic resource estimation at Fog. 2016 13th IEEE Annual Consumer Communications and Networking Conference. CCNC. 2016.
[6] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, Security, privacy and trust in internet of things: The road ahead, Computer Netw. 76 (2015) 146–164.
[7] D.K. Alferidah, N.Z. Jhanjhi, A Review on Security and Privacy Issues and Challenges in Internet of Things, Int. J. Computer Sci. Netw. Sec. IJCSNS 20 (4) (2020) 263–286.
[8] B. Atoum. History of Internet of things. 2020; Available from: https://e3arabi.com/.

[9] B. Chu, W. Burnett, J.W. Chung, Z. Bao, Bring on the bodyNET, Nat. News 549 (7672) (2017) 328–330.
[10] P. Sethi, S.R. Sarangi. Internet of Things: Architectures, Protocols, and Applications. 2017.
[11] D.K. Alferidah, N. Jhanjhi. Cybersecurity Impact over Bigdata and IoT Growth. 2020 International Conference on Computational Intelligence (ICCI). Bandar Seri Iskandar, Malaysia. 2020. 103–108. doi: 10.1109/ICCI51257.2020.9247722..
[12] P. Sethi, S.R. Sarangi, Internet of Things: Architectures, Protocols, and Applications, J. Electric. Computer Eng. 2017 (2017) 1–25.
[13] J. Vasseur, et al. The ip routing protocol designed for low power and lossy networks. Internet Protocol for Smart Objects (IPSO) Alliance. 2011.
[14] Prasadu Peddi (2018), "A Study For Big Data Using Disseminated Fuzzy Decision Trees", ISSN: 2366- 1313, Vol 3, issue 2, pp:46-57.
[15] K. Uppalapati, How IoT protocols and standards support secure data exchange in the IoT, Ecosystem? (2019).
[16] M.A. Alzain, E. Pardede. Using multi shares for ensuring privacy in databaseas-a-service. In: 2011 44th Hawaii International Conference on System Sciences. 2011. IEEE.
[17] B.O. Al-Amri, M.A. AlZain, J. Al-Amri, M. Baz, M. Masud, A comprehensive study of privacy preserving techniques in cloud computing environment, Advanc. Sci. Technol. Eng. Sys. J. 5 (2) (2020) 419–424.
[18] O.S. Faragallah, A. Afifi, W. El-Shafai, H.S. El-Sayed, E.A. Naeem, M.A. Alzain, J.F. Al-Amri, B. Soh, F.E.A. El-Samie, Investigation of chaotic image encryption in spatial and frft domains for cybersecurity applications, IEEE Access 8 (2020) 42491–42503.
[19] O.S. Faragallah, A. Afifi, W. El-Shafai, H.S. El-Sayed, M.A. Alzain, J.F. Al-Amri, F.E. A. El-Samie, Efficiently encrypting color images with few details based on rc6 and different operation modes for cybersecurity applications, IEEE Access 8 (2020) 103200–103218.
[20] M.A. AlZain, et al. Managing Multi-Cloud Data Dependability Faults, in Knowledge-Intensive Economies and Opportunities for Social, Organizational, and Technological Growth. 2019. IGI Global. 207–221.
[21] Yogesh Hole et al 2019 J. Phys.: Conf. Ser. 1362 012121

Author Bibliography:

Pushpa Latha Thumma is working as an assistant professor at St. Ann's College for Women in Hyderabad, Telangana, India. Presently, she is a research scholar at Shri JJT University, Rajasthan. She obtained her MCA from St. Ann's College for Women, Hyderabad, Telangana. She has written books on cyber security and information technology fundamentals. Her research interests are the Internet of Things, artificial intelligence, and cyber security.
pushpareddy28@gmail.com