International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET229423

Security Threats to Internet of Things : A Survey

Faiza Soomro[1*], Zeeshan Jamil[2], Hafiza Rafia Tahira[2]
[*1,3]Software College, Northeastern University, Shenyang, China
[2]Department of ICS/IT, The University of Agriculture Peshawar, Pakistan

Article Info
Volume 9, Issue 4

Page Number : 130-135

Publication Issue :
July-August-2022

Article History
Accepted : 05 July 2022
Published: 20 July 2022

ABSTRACT

Internet of things (IoT) is an emerging technology in the present era. The term IoT refers to as an interconnection of several smart nodes through some heterogeneous link for the purpose of data communication. Some particular protocols control the entire communication in IoT. Due to plenitude of devices, it becomes a huge task to check the loyalty status of each node which is going to be a part of IoT environment. These nodes sometimes get involved in some malicious activities which may cause critical threats to this environment. These anonymous activities may include some attack on the working or security of IoT. In this uncongenial circumstance we need a strong security measurement to countermeasure these attacks. Innumerable efforts have been made to improve the security of IoT. This paper is an effort to make a glance of some of these security schemes

Keywords : IoT, Cyber Threats, Network Security, Communication

I. INTRODUCTION

The growing speed of technology led several innovations for the sake of convenience to human beings. IoT is one of these technologies. It comprises almost all the fields of our life. The human interaction to machines is reduced to some extent in this technology. Many nodes or even many smart buildings are in connection with each other to perform communication in a fast and responsive manner. Following figure 1 explains the connectivity architecture of IoT.

The size of this IoT networks grows along with new incoming devices in this environment. To check the security of all these new devices is almost impossible. Therefore, a few times these devices may create some challenges to this entire environment. Due to its wide range of applications, these critical challenges are need to be troubleshoot. In this way we are in need of strong security check some to secure of IoT system from all internal and external security threats. There may exist some attacks or some other anonymous activities to harm the working or security of IoT. There may also be another desire to shake the privacy of IoT users. We have categorized some of these attacks as follows in figure 2.

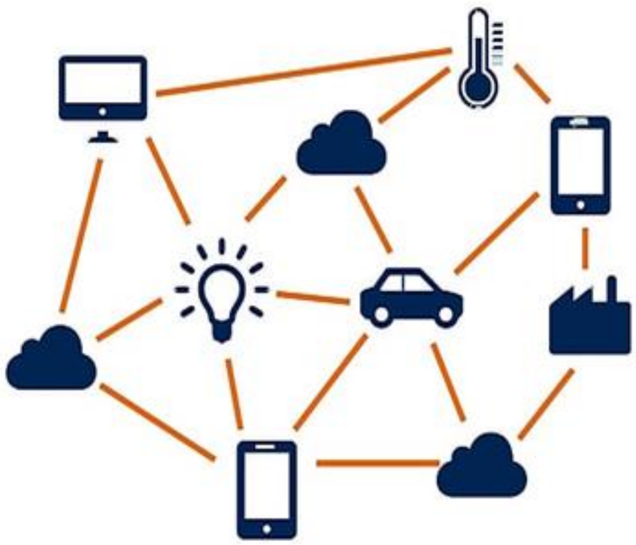

Figure 1. IoT Architecture

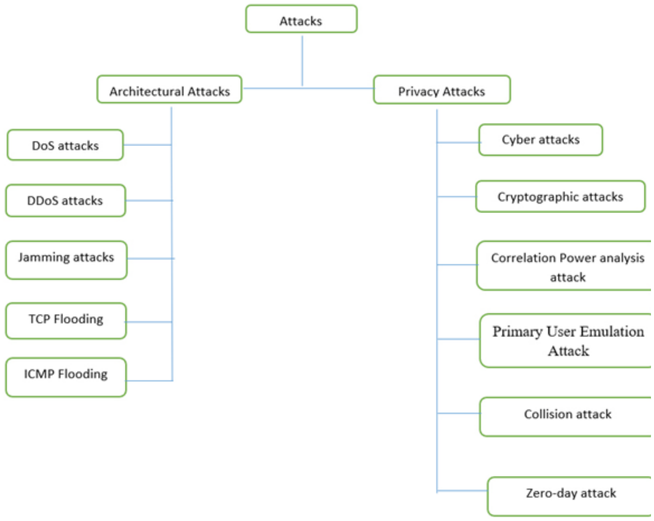

Figure 2: Attacks Category

These attacks categorized into two main categories. Architectural attacks and privacy attacks [1]. The architectural attacks concerns with the working and routing behavior of IoT environment. These may include denial of services attack (DoS), jamming attacks and transmission control flooding (TCP) etc. [2]. The main purpose behind these attacks is to create disturbance in the working of IoT mechanisms. The other type of attacks is attacks is privacy attacks. These attacks are launched to shake the privacy of users. Some of these attacks are directly triggered on the data collection and some of them are concerned with the ways to get illegal access to user's data. The attacks are sometimes physical or sometimes in cyber form [3].

With the advent of cloud computing, the IoT technology gain faster momentum. All of the data is being stored on the cloud to make it available for everyone. Cloud computing makes over lifer easier however there is a major drawback of this technology. An attacker can gain illegal access to cloud and can manipulates the bulk of user's data which has been stored on the cloud. Here comes the concept of cryptography in which the data is stored in an encrypted form. This thing hinder the attacker to manipulate the data facts [4]. The spreading quantity of smart nodes enhances the chances of architectural attacks. Ere sometimes occurs a process in which nodes send a bundle of simultaneous requests to the main server. If the quantity of compromised nodes is limited, then this attack is simple called DoS. However if the requests are being sent from more than one node then this attack is known as distributed DoS [5]. Following section contains scientific work related to this domain.

II. LITERATURE REVIEW

IoT covers almost all the aspects of communicational sciences. This is because of its proper architecture and involvement of several devices in connected with each other through heterogeneous communication links. The communication links between these devices may cause some security threats to entire IoT. In other words, it arises a strong need of a proper security model in order to achieve secure and efficient communication. Innumerable efforts has been made to deal with security aspects of IoT. Here we discussed some of scientific contribution related to this space.

Authors in [6] presented a honeypots security model to prevent an IoT server against DOS attacks. In IoT. Several devices are integrated with the help of high quality sensors. The main purpose behind this integration is exchange of data and rapid response among these devices. However if some devices continuously send an innumerable amount of data to the server, the functionality of server becomes slow and sometimes server is crashed. To overcome this problem, honeypots comes with its unique characteristics of seducement and acts as a decoy in the main server in order to mitigate attack on the main server.

Presence of large volume of IoT devices enhances the probability of security threats in IoT. Furthermore the high level of heterogeneity in these devices also plays a vital role to invite attacks on such type of networks. A software defined networks based framework is presented in [7] called softthings. This framework consists on the main master controller which is integrated with IoT devices to reduce the burden on them. This master controller makes the under contention framework capable to detect and diminish the influences of common security threats like TCP flooding, internet control messaging protocol (ICMP) flooding and DDoS attacks.

Cloud computing is an emerging technology in the present era. It makes everything available for everyone at any time. Different servers are integrated with cloud to outsource valuable data on cloud. In some circumstance cloud computing technology works with IoT to magnify the effectiveness of IoT. However, besides the benefits of this combination, this phenomena led a little bit security challenges for IoT. An illegitimate user can gain unauthorized access to these servers and hence privacy of user's can be shacked. In [8], authors presented some cryptographic approaches to encrypt user's data in order to keep it secure in case of any attack.

Another security model based on advanced encryption standard is presented in [9] to secure IoT against correlation power analysis attacks (CPA). In CPA, the attacker intended to get the secret encryption key by analyzing the relation between input and power consumption. For the sake of eliminate the possibilities of this attack, a false key and wave dynamic differential logic (WDDL) assisted advance encryption standard (AES) technique is used.

In [10], authors presented a methodology to detect the presence of any intruder in the mesh of IoT devices. Due to plenitude of IoT devices, it becomes difficult to indicate the compromised node. However, the proposed idea of authors is capable to identify suspicious events within the network.

Another type of threat on IoT security is discussed in [11]. Suppose an IoT environment, where some secondary user or a third party manipulates the facts by announcing itself as a primary user. The motive behind this scenario would be either desire to get unauthorized access or it may be another desire to perform some malicious activity within the network. Such type of attack is referred as primary user emulation attack (PUEA), Authors proposed two-tier device-based authentication protocol (T2DAP), to provide a solid defense against this attack. Simulations are performed to test the effectiveness of this protocol. The results shows that proposed protocol is minimize the chances of under contention attack to a notable extent however, here it arises the problems of high energy consumption.

In [12], collision attacks and their countermeasure is discussed. The basic architecture of IoT environment is an ideal place for such types of attack to occur. A fog computing based model is used as an antidote for this attack. This model has also some characteristics of software defined networks (SDN) system layer to provide the facility of easily integration of fog nodes. . Both these features get combined to make the system capable to identify the presence of collision attack and malicious user who intending to perform this attack.

In IoT environment, the existence of various heterogeneous links maximize the possibilities of some malware or some other malicious program to get in. These programs give birth to many cyber-attacks in IoT space. Here we need a secure framework which resists the incoming of malicious programs from different nodes. Same type of security scheme is presented in [13], which reduces the malware spreading to a fixed limit like device to device connection. And hence the target bandwidth of malware is lessened within the IoT environment.

In [14], authors proposed an intrusion detection system (IDS) to expose wormhole attack. Wormhole attack concerns with the routing behavior of network during communication. The occurrence of this attack creates a tunnel in between of two negotiated routers. All the traffic flow diverts toward that particular tunnel because this tunnel exhibits itself as a shortest path of data flow. In this way routing mechanism is badly disturbed and may causes many of serious issues regarding data transmission. The under contention IDS has contains efficient algorithm which can easily monitor routing activities and detect wormhole attack. Another security treat known as zero-day attack has considered in [15]. This attacks refers to the security lope holes in during the software designing for IoT. A distributed diagnosis system based security approach has been used to legitimate this attack. In this approach, there exist an integration between central service provider and local user cite. If the attack occurs, then after its identification a special data sharing protocol is used which ensures sending of alert messages and also build a trust between network entities and IoT nodes. The presented approach also prove its efficiency in terms of network cost and communication overhead. Deep Learning has also proven its ability in different fields, i.e., allocation problem [16], selection and evaluation [17], threat detection [18-19], and disease detection [20]. Here we explained all of above-mentioned literature review in the following table:

Table 1: Existing Literature

Ref:	Published Year	Attack Name	Attack Description	Countermeasure	Achievements
[6]	2017	DoS attack	A node send a lot of requests to server which disturbs the functionality of server	Honeypots	mitigation of attack
[7]	2022	TCP flooding	An extreme flow of data to distrait the working of server	SDN based framework, Softthings	Detection of attack, efficient communication
[8]	2017	Cyber attack	Attacker can gain remotely access to network to perform malicious activities	Cryptographic approaches	Attacks are stooped to a notable extent
[9]	2017	CPA	In correlation power analysis attacks, the attacker tries to obtain the secret encryption key	WDDL based AES	Encryption of data
[10]	2017	Physical Attack	Attacker gain physical access to attack the system	IDS based algorithm	Identification of malicious activities
[11]	2017	PUEA	In Primary User Emulation Attack, the secondary user acts as a primary user	Two-Tier Device-Based Authentication Protocol	Effective authentication process
[12]	2017	CA	Collision attack consists on illegal tries to get system compromised by get combined all the available information.	A fog computing based model	Prevention against collision attack
[13]	2017	Malware attacks	Viruses or malicious activities are injected in the main network through some compromised node.	Malware defensive mechanism	Malware and malicious programs are banned
[14]	2020	Wormhole attack	This attack disturbs the routing behavior of network	Intrusion detection system	Security of IoT
[15]	2018	Zero-Day attack	Attacker tries to attack the system by finding weakness in the software design of system.	A distributed diagnosis system based security approach	Effective security accomplishment

III. CONCLUSION

There exist a vast range of IoT applications in almost every field our daily life. All this making our life easier day by day. However there also exists some threats to this IoT environment. There may be some internal or external factors which may cause problems to the working or security of IoT. Internal threat are due to wide range of devices which are connected in surrounding of each other. Compromised behavior of any one of them may cause serious risks to IoT. All these challenges comes with a strong need of some security frameworks. In order to secure entire structure and data protection in IoT, plenitude of scientific schemes have been proposed. All of these schemes proves their efficiency in terms of security. However there is still a tradeoff between security and efficiency of IoT.

IV. REFERENCES

[1]. Javeed, D., Gao, T., & Khan, M. T. (2021). SDN-enabled hybrid DL-driven framework for the detection of emerging cyber threats in IoT. Electronics, 10(8), 918

[2]. Al Razib, M., Javeed, D., Khan, M. T., Alkanhel, R., & Muthanna, M. S. A. (2022). Cyber Threats Detection in Smart Environments Using SDN-Enabled DNN-LSTM Hybrid Framework. IEEE Access, 10, 53015-53026.

[3]. Javeed, D., Gao, T., Khan, M. T., & Ahmad, I. (2021). A hybrid deep learning-driven SDN enabled mechanism for secure communication in Internet of Things (IoT). Sensors, 21(14), 4884.

[4]. Ali, S., Javaid, N., Javeed, D., Ahmad, I., Ali, A., & Badamasi, U. M. (2020, April). A blockchain-based secure data storage and trading model for wireless sensor networks. In International Conference on Advanced Information Networking and Applications (pp. 499-511). Springer, Cham.

[5]. Tamotsu KAWAMURA, Masaru FUKUSHI, Yasushi HIRANO, Yusuke FUJITA and Yoshihiko HAMAMOTO "An NTP-based Detection Module for DDoS Attacks on IoT" 2017 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW)

[6]. Anirudh M, Arul Thileeban S. Daniel Jeswin Nallathambi "Use of Honeypots for Mitigating DOS Attacks targeted on IoT Networks" IEEE International Conference on Computer, Communication, and Signal Processing (ICCCSP-2017)

[7]. Javeed, D., Gao, T., Khan, M. T., & Shoukat, D. (2022). A hybrid intelligent framework to combat sophisticated threats in secure industries. Sensors, 22(4), 1582.

[8]. Tanupriya Choudhury, Ayushi Gupta, Saurabh Pradhan, Praveen Kumar, Yokes Singh Rathore, "Privacy and Security of Cloud-Based Internet of Things (IoT)", 2017 International Conference on Computational Intelligence and Networks

[9]. Weize Yu and Selçuk Köse, "A Lightweight Masked AES Implementation for Securing IoT against CPA Attacks", IEEE Transactions on circuits and systems

[10]. Jesus Pacheco Salim Hariri, "Anomaly behavior analysis for IoT sensors", special issue article, WILEY

[11]. Shih-Chang Lin, Chih-Yu Wen, and William A. Sethares, "Two-Tier Device-Based Authentication Protocol against PUEA Attacks for IoT Applications"

[12]. Qussai Yaseen, Monther Aldwairi, Yaser Jararweh, Mahmoud Al-Ayyoub, Brij Gupta, "Collusion attacks mitigation in internet of things: a fog based model"

[13]. Shin-Ming Cheng, Pin-Yu Chen, Ching-Chao Lin, and Hsu-Chun Hsiao, "Traffc-Aware Patching for Cyber Security in Mobile IoT".

[14]. Javeed, D., Khan, M. T., Ahmad, I., Iqbal, T., Badamasi, U. M., Ndubuisi, C. O., & Umar, A. (2020). An efficient approach of threat hunting using memory forensics. International Journal of Computer Networks and Communications Security, 8(5), 37-45

[15]. Vishal Sharma, Jiyoon Kim, Soonhyun Kwon, Ilsun You, Kyungroul Lee, Kangbin Yim "A framework for mitigating zero-day attacks in IoT"

[16]. Ahmad, I., Liu, Y., Javeed, D., & Ahmad, S. (2020, May). A decision-making technique for solving order allocation problem using a genetic algorithm. In IOP Conference Series: Materials Science and Engineering (Vol. 853, No. 1, p. 012054). IOP Publishing.

[17]. Ahmad, I., Liu, Y., Javeed, D., Shamshad, N., Sarwr, D., & Ahmad, S. (2020, May). A review of artificial intelligence techniques for selection & evaluation. In IOP Conference Series: Materials Science and Engineering (Vol. 853, No. 1, p. 012055). IOP Publishing.

[18]. Khan, T. U. (2019). Internet of Things (IOT) systems and its security challenges. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 8(12).

[19]. Javeed, D., Badamasi, U. M., Iqbal, T., Umar, A., & Ndubuisi, C. O. (2020). Threat detection using machine/deep learning in IOT environments. International Journal of Computer Networks and Communications Security, 8(8), 59-65.

[20]. Raza, A., Ayub, H., Khan, J. A., Ahmad, I., S Salama, A., Daradkeh, Y. I., ... & Hamam, H. (2022). A Hybrid Deep Learning-Based Approach for Brain Tumor Classification. Electronics, 11(7), 1146.

Cite this article as :

Faiza Soomro, Zeeshan Jamil, Hafiza Rafia Tahira, "Security Threats to Internet of Things : A Survey ", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 9 Issue 4, pp. 130-135, July-August 2022. Available at doi : https://doi.org/10.32628/IJSRSET229423
Journal URL : https://ijsrset.com/IJSRSET229423