Information Sciences Letters

Volume 9
Issue 1 *Jan. 2020*

Article 3

2020

A Review on Emerging Threats and Vulnerabilities in Internet of Things and its Applications

Z. Faizal Khan
College of Computing and Information Technology, Shaqra University, KSA, Faizalkhan@su.edu.sa

Information Sciences Letters
An International Journal

http://dx.doi.org/10.18576/isl/090103

A Review on Emerging Threats and Vulnerabilities in Internet of Things and its Applications

Z. Faizal Khan

College of Computing and Information Technology, Shaqra University, KSA

Received: 2 Sep. 2019, Revised: 22 Nov. 2019, Accepted: 23 Dec. 2019
Published online: 1 Jan. 2020

Abstract: Nowadays, Internet of Things (IoT) plays a crucial part in the area of Information Technology (IT). At present, providing security to information has become one of the difficult tasks. Recently, the IoT and the devices connected on it have accepted a sizeable attention towards the research. The IoT is contemplated as the future of the Internet. IoT and its connected devices will have a considerable role and will change the style of living, standard of living, as well as the models of business in future. The applications of IoT in various fields are anticipated to increase gradually in the up-coming years. Various types of threats such as malicious based attack, network based attack and network abuse have been emerged and identified in the IoT based on virus, Phishing, Spam and the user abuse. It has been noted that these mechanisms are causing various level of complication and preferment as there is advances in IoT based devices and its technology. This paper focuses on various challenges, threats and vulnerabilities faced by cyber security especially in the field of IoT and its latest technologies. It also focuses on the techniques of security, methods and the recent trends which are changing the face of IoT based security. This paper also focuses on an attempt to classify various types of threats, besides analyzing and characterizing the intruders and attacks facing towards the IoT devices and its services.

Keywords: Internet of Things, Security, Information Technology, Networks, Performance, Vulnerabilities.

1 Introduction

Security of a system can be defined as the practice of providing a secure ingress. This is done in an application by applying various methods and technologies, practices and actions especially proposed to protect the networks, computers connected in it, programs and its associated applications, data etc. It also protects the entire system from causing damage or any other modifications [3]. Experts of security categorized the recent emerging threats as malicious based attacks, network based attacks, and abuse of the network. Malicious based attack is a process of make use of the computer of another user and contaminate the resources present in the system through viruses, Trojans and other types of spyware etc. Attacks on network are conscious on generating activities especially for destroying or muddle the flow of data in the system connected on a network, which leads to the service denial, hijacking the session, spoofing of email etc. [1,2]. Abusing the network is basically to make use of the communication in the network. It can be used by various malwares such as Spam, viruses, pharming etc. [4].

In general, the threats in the IoT based devices can observed as criminal based action which using the applications of the world wide web (WWW). These actions of attacks includes stealing then intelligent property of an organization, monitoring and acquiring bank accounts the through online, plotting and socializing viruses and other malwares towards various computers, uploading secret information on the web to disturb the basic infrastructure of an organization [5]. Threats in the IoT based devices caused huge failure to many organizations in terms of the loss in revenue as well as in their business [6,9,10]. Cyber based attacks can be defined as the process of venture to erode or destroy the process takes place in a computer or a network based system. It can also be defined as the action of identifying the transactions of users through online without their attention. These types of attacks may be imperceptible to the user who is using the system at the end. It can also pave a way for the disturbance of the entire network so that all the users can be affected [7].

The IoT has successfully integrated the fictional space and the real world on the same platform. The main aim of

[*] Corresponding author e-mail: faizalkhan@su.edu.sa

IoT is the setup of a self-conscious environment and smart based independent devices such as smart based living, smart based items, smart based health, and smart based cities etc [8]. The rate of adoption of the IoT devices is very high nowadays since more devices are connected through the Internet. This paper finds to serve to a better identification of various threats and the vulnerabilities of cyber security in the IoT and its applications which are originating from various sources. The process of finding vulnerabilities and threats in the systems connected in IoT is needed for identifying and noting a fast and full set of requirements for the security. It also identifies whether the solution for security is necessary against various malicious attacks in devices of IoT based its applications.

Rest of the paper is organized as: Section 2 discusses motivation of the proposed work. Section 3 depicts the discussion about Internet of Things, its devices, the security threats, attacks, and vulnerabilities in IoT. Section 4 depicts the conclusion of this comprehensive study.

2 Motivation of The Proposed Work

Challenges faced by the IoT based systems are as follows:

1. Various methods were proposed earlier for improving performance of IoT based security. Majority of the IoT systems are still in process for the enhancement of security and its threats and vulnerabilities, but with poor accuracy.
2. Various methods were used earlier for improving the accuracy of security in the IoT based systems. Though, it was highly scalable, but the performance was poor in terms of accuracy.
3. Therefore, the process of finding vulnerabilities and threats in the systems connected in IoT is needed for identifying and noting a fast and full set of requirements for the security. It also identifies whether the solution for security is necessary against various malicious attacks in devices of IoT based its applications.

3 Internet of Things (IoT)

The IoT [13,15] is an application of the Internet services and its connection into the world for effective communication with in the surrounding entities. Devices and its services [14] are the main paradigms connected in the IoT based area, which is shown in Figure 1. These devices have different stages and advantages in different applications.

3.1 Devices for IoT

These IoT based hardware's allows the connected devices to be the entities of this digital based world [16,17]. It is also called as a smart-aided-thing, which can be a applied in home based appliances, healthcare based devices, vehicular networks, infrastructure, production and all the entities which are connected in networks which are fixed with various sensors for obtaining or giving information about the surrounding environment such as the temperature, level of heat and air, pollution etc. actuators which are inserted in computers.

IoT devices can easily communicate with other devices which are connected in this platform. These types of devices shown in Figure 2 can transfer or receive data through various methods which comprises of the mobile based technology, wireless based technologies etc. [10]. Classification of these devices depends on size, i.e., small or normal; mobility, i.e., movable or fixed; source of power as external or internal; connection is temporary or permanent; automatic or manual etc.

3.2 Threats, Attacks, and Vulnerabilities in IoT based Security

The entire components should be computed before addressing the threats in security. In order to make it, all the IoT devices should be identified initially. It is significant to identify and analyze the total components which include all the components in IoT, its services and the devices which are connected to it. This analysis can be an economic form which is valuable and sensitive in nature. The main properties of any system connected in IoT are its hardware, software installed in it, services offered by it and the data offered by it [13].

3.2.1 Vulnerability

Vulnerabilities can be defined as the weaknesses in a system or its overall design which paves the way for an intruder to run his own commands, get the unofficial data, and also can perform the conduct attacks on denial-of service. This weakness can be found in various areas in the IoT based systems. In specific, these weaknesses can be found in hardware of the system or its software, in its policies, in its overall procedures and in its users who are accessing the system [9]. IoT based systems depends on two major components such as the overall hardware of the system and its software [12,14]. More often, the probability of possibility of flaws in these components can be more. Vulnerabilities present in the hardware are very hard to detect and it is also hard to fix it.

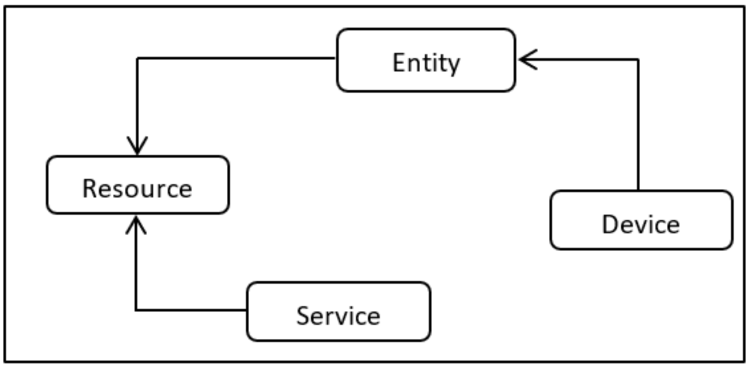

Fig. 1: Key concepts present in the IoT domain

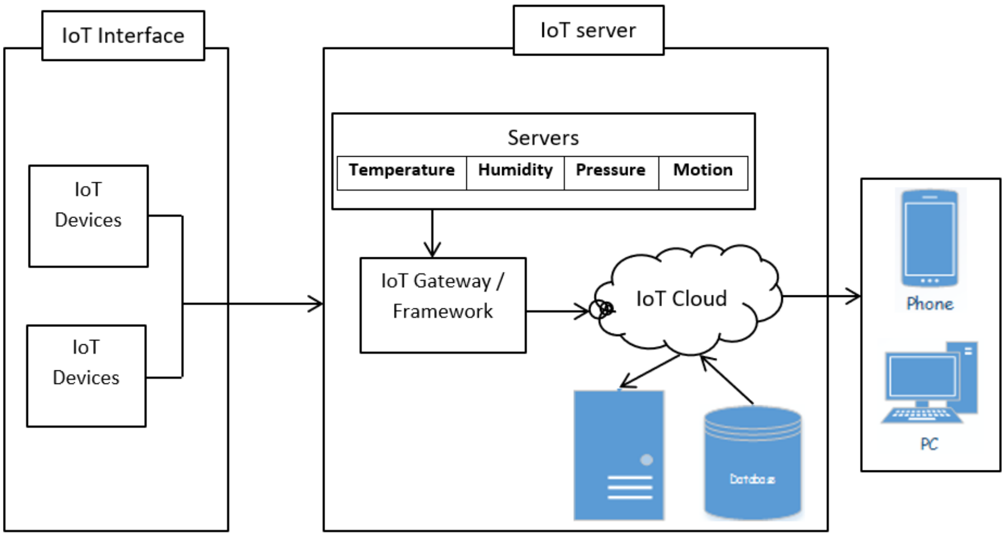

Fig. 2: Interface of IoT and its devices

3.2.2 Threats

Threat can be defined as an action which uses the advantage of the weaknesses in security in a system. It also has various negative impacts in the performance of the overall system. Threats can be arise from two main founts such as: humans and machine. Threats from the machine are data loss, data mi-management, data replication, duplication of data, etc. Data recovery options could be employed to recover the data which were lost due to the threats from machine. Threats from the human can be caused by various people from the internal user; external threats such as the users who are given access from outside can harm and change the overall system. These threats from the human are classified into the following categories:

1.Unorganized threats

2.Organized threats

3.2.3 Attacks

Attacks are measures which are done in order to disturb or destroy a system. It can also disturb the normal operation of a system by making the system potentially vulnerable using various numerous methods and devices which are available nowadays. These devices and techniques can perform various attacks in order to attain the goal. It may be a satisfaction in personal or it can be recompense. Attack cost can be defined as the measurement of the overall efforts which was expended by an attacker and which is also indicated with respect to their area of competence, assets utilized for that particular purpose. These actors of attack are the potential threat to the present era [8]. Various forms of these attackers may be hackers [11]. These attacks can be in different ways which includes network attacks which is active to unencrypted monitor traffic while searching the information which were sensitive; passive based attacks for example network communications which are unprotected and its monitoring in order to decode the encrypted traffic which are weak and obtaining the information which are authenticated etc. Most common types of IoT based attacks are as follows:

(a) Physical attacks in the IoT
The physical attacks in IoT based devices meddle the components present in the hardware. Due to the ignored and dispense nature of the IoT based devices, most of them operate usually in rugged environments. Hence, these IoT based devices are highly vulnerable to physical based attacks.

(b) Reconnaissance based attacks in the IoT
It can be defined as an unauthenticated finding and portray of systems, its various services, and various possibilities for being attacked. Examples of these reconnaissance based attacks are scanning of the ports in the network, sniffers in packet, analysis of traffic, and transmitting queries about the information of its Internet Protocol (IP) address.

(c) Service Denial in IoT
These types of attack are a venture to make the resources of a system or its connected network not able to be used to its particular users. Because of the lower in memory capacities and restricted access to the resources present in it. Large number of devices connected in the IoT is susceptible to these types of attacks.

(d) Access attacks in IoT
It can be defined as acquiring a person’s unauthorized ingress towards the networks or the other devices connected in it where the ingress is prohibited. These attach in ingress can be classified into two categories namely physical ingress and the remote ingress. Physical ingress is defined as an intruder tries to get ingress to a device physically and the remote ingress can be defined as the ingress takes place in the devices connected in an IP.

(e) IoT based attacks and its privacy
Preservation of privacy devices based on IoT has come to be progressively exigent because of the huge contents of information which are available easily through the remote access mechanisms.

(f) Cyber-crimes in IoT devices
The IoT based devices and smart objects which are connected in the Internet are used to make use of its users and the data present in it for capitalistic gain, such as the intellectual property theft, identity theft, brand theft, and various other fraudulent activities etc. [8,9].

(g) Destructive attacks in IoT
In these types of attacks, the pre-defined space is used to form a large-scale disturbance and destruction of the IoT based applications. Examples such as the attacks based on revenge, control and acquisition of data etc. These types of attacks make the TCP/IP systems more vulnerable to attacks.

The IoT based system can be attacked by any one of the following methods:
i. Using denial-of-service to permanently shut down the entire system.
ii. Using Trojans or viruses to acquire the entire control of the system.

4 Conclusion and Future Enhancements

In this paper, a review of the security issues in IoT based systems and its various infrastructure and applications. At present, securing the information in IoT based applications has become one of the biggest challenges. It has been identified that attacks, Trojans and viruses are displaying a particular complication level and advancement as the technology advances in IoT devices. This paper involves a comprehensive survey on identification of various categories of threats and vulnerabilities within the IoT based applications and its services. The process of finding vulnerabilities and threats in the systems connected in IoT is needed for identifying and noting a fast and full set of requirements for the security. Hence, various type of scenarios in attack, types of attackers, type of attacks done in IoT based devices are also mentioned. This paper also focuses on an attempt to classify various types of threats, besides analyzing and characterizing the attackers and their attacks interfacing towards the IoT based devices and its services.

References

[1] J. Lopez, R. Roman, and C. Alcaraz, Analysis of security threats, requirements, technologies and standards in wireless sensor networks, in Foundations of Security Analysis and Design V. Springer 289–338 (2009).
[2] O. Reyad, H. S. Khalifa and R. Kharabsheh, Image Pixel Permutation Operation Based on Elliptic Curve Cryptography, J. Appl. Math. Inf. Sci. 13, 183–189 (2019).
[3] R. Roman, J. Zhou, and J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Computer Networks 57, 2266–2279, (2013).
[4] M. Rudner, Cyber-threats to critical national infrastructure: An intelligence challenge, International Journal of Intelligence and Counter Intelligence 26, 453–481 (2013).
[5] O. Reyad, Text message encoding based on elliptic curve cryptography and a mapping methodology, Inf. Sci. Lett. 7(1), 7–11 (2018).
[6] R. Kozik and M. Choras, Current cyber security threats and challenges in critical infrastructures protection, In Second International Conference on Informatics and Applications (ICIA), IEEE, 93–97 (2013).

[7] M. M. Hossain, M. Fotouhi, and R. Hasan, Towards an analysis of security issues, challenges and open problems in the internet of things, In 2015 IEEE World Congress on Services (SERVICES), IEEE, 21–28 (2015).

[8] M. Abomhara and G. M. Koien, Security and privacy in the internet of things: Current status and open issues, In International Conference on Privacy and Security in Mobile Systems (PRISMS), IEEE, 1–8 (2014).

[9] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, A vision of IoT: Applications, challenges, and opportunities with china perspective, IEEE Internet of Things journal 1, 349–359 (2014).

[10] L. Atzori, A. Iera, and G. Morabito, The Internet of things: A survey, Computer networks 54, 2787–2805 (2010).

[11] Y. Benazzouz, C. Munilla, O. Gunalp, M. Gallissot, and L. Gurgen, Sharing user IoT devices in the cloud, In 2014 IEEE World Forum on Internet of Things (WF-IoT), IEEE, 373–374 (2014).

[12] G. M. Koien and V. A. Oleshchuk, Aspects of Personal Privacy in Communications-Problems, Technology and Solutions (2013).

[13] W. M. Abd-Elhafiez, O. Reyad, M. A. Mofaddel and M. Fathy, Image Encryption Algorithm Methodology Based on Multi-mapping Image Pixel, In: A. Hassanien, et al. (eds.): AMLTA 2019. AISC, vol. 921, Springer Cham, 645–655 (2020).

[14] S. Andreev and Y. Koucheryavy, Internet of things, smart spaces, and next generation networking, Springer, LNCS, 7469–464 (2012).

[15] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I. S. Jubert, M. Mazura, M. Harrison, M. Eisenhauer et al., Internet of things strategic research roadmap, Internet of Things-Global Technological and Societal Trends, 9–52 (2011).

[16] S. De, P. Barnaghi, M. Bauer, and S. Meissner, Service modelling for the internet of things, In 2011 Federated Conference on Computer Science and Information Systems (FedCSIS), IEEE, 949–955 (2011).

[17] G. Xiao, J. Guo, L. Xu, and Z. Gong, User interoperability with heterogeneous IOT devices through transformation, (2014).

Z. Faizal Khan is currently working as an assistant professor at the Department of Computer Science in the College of Computing and Information Technology (CCIT), Shaqra University, the Kingdom of Saudi Arabia. He has published more than 50 articles in referred journals and acted as an editorial member and reviewer in many reputed journals and conferences. His research interests include Image Processing, Pattern Recognition, Intelligent based Systems and Medical Image Analysis.