Science Heritage Journal (GWS)

DOI : http://doi.org/10.26480/gws.02.2019.18.21

ISSN: 2521-0858 (Print)
ISSN: 2521-0866 (Online)
CODEN : SHJCAS

REVIEW ARTCLE

INTERNET OF THINGS (IOT), SECURITY ISSUES AND ITS SOLUTIONS

Fahad Azam[1], Rashid Munir[1], Mehboob Ahmed[1], M. Ayub[1], Ahthasham Sajid[2*], Zaheer Abbasi[3]

[1]Department of Information Technology, Faculty of ICT Baluchistan University of Information Technology Engineering and Management Sciences Quetta, Baluchistan, Pakistan.
[2]Department of Computer Science, Faculty of ICT Baluchistan University of Information Technology Engineering and Management Sciences Quetta, Baluchistan, Pakistan.
[3]Department of Environmental Science, FICT, BUITEMS, Quetta, Baluchistan, PAKISTAN
**Corresponding Author Email: ahthasham.sajid@buitms.edu.pk, gullje2008@hotmail.com*

ARTICLE DETAILS

Article History:

Received 25 August 2019
Accepted 27 September 2019
Available online 14 October 2019

ABSTRACT

Internet of things (IoT) plays a great role in the 21st century than a couple of years ago. Internet of things (IoT) provides us a technologically and optimistic image of the future where several computing objects are linked to the internet and they can recognize themselves with additional computing strategies. In this paper detail review of security issues over different layers of IoT has been covered. This paper also discusses the solutions possible to overcome those security issues. In this paper the brief discussion on security threats and how to measure it respectively to protect information or confidential information of the users IoT accentuations on controlling different assignments and attempt to approve the physical things to act denied of any obstruction of the human. The up and coming and existing IoT introductions are much guaranteed to expand the solace level, effectiveness, and robotization of the clients. The objects can represent digitally because IoT is very significant.

KEYWORDS

Internet of Things, Malicious, Phishing.

1. INTRODUCTION

In 1999, MIT sought to develop Electronic Product Code EPC, and the use of Radio Frequency Identification (RFID) to identify kits on the network. In 2003-04 the missions that are helping IoT ideas such as Cool town, Internet and Disappearing Computer initiative and IoT also start to appear for the first time in book titles. In 2005 IoT successfully entered to a new level when the first report is published by International Telecommunication Union ITU. In 2008-09 IoT was "Born" by the Cisco Internet Business Solutions Group (IBSG) [1]. Internet of Things is defined as the network of physical items or "Things" that are implanted with software, sensors, electronics, and network connectivity which permits these objects to gather and interchange data. The "Thing" in the Internet of Things, is an object or a physical thing that has a sole identifier, it is a fixed system and the capability to handover information or data over some network.

- Automobiles with built-in-sensors.
- Heart monitoring imp

Mark Weiser has addressed us about the visualization of the future of the Internet under the name of "Ubiquitous Computing" In 1991. Through this vision of the future of the Internet, he was very focused on exactly how to try on the smart suitable atmosphere in the presence of smartphone technology this provides us a powerful multimedia structure [2]. Kevin Ashton is one of the innovators of the Internet of Things (IoT) [3]. In 1999 Neil Gerstenfeld was speaking about the related things from the MIT (Massachusetts Institute of Technology), MIT Lab in his book of "When Things Start to Think" [1]. These devices bring together useful information or information with the help of different technologies and then they freely flow the data among other computing devices. Some researches describe the IoT as a new model that comprises all of the wireless communication technologies such as actuators, mobile networks, and wireless sensor networks. Each element of the internet of things is called the "Thing" and it has a sole address [4]. The existence of the internet is since the beginning of the 1970s but it became a famous and globally known ICT infrastructure around 1995.

It is a connecting of physical gadgets to the web to perhaps get to remote detecting information and control the whole physical world from a long separation. A structure square of the Internet of Things is the keen article [5]. The rapid expansion of the Internet of Things and its abilities to offer various kinds of services has made it the fastest-growing technology of the present time [6]. The number of security issues is rising on a huge amount day by day and the number of attacks has been increased in both number and complexity. The process to protect any object from physical damage, loss or theft, unauthorized access by maintaining the high integrity of information and high confidentiality about the object [6].

Figure 1: Internet of Things

2. LAYERS IN IOT

IoT can be separated into following layers:

- Sensing layer
- Network layer
- Middleware layer
- Application layer

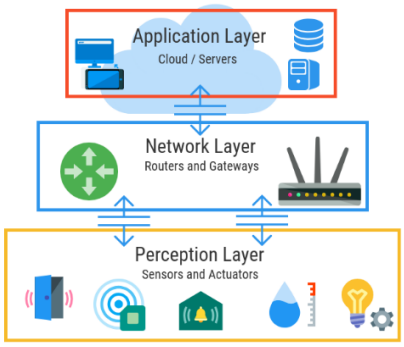

Figure 2: IoT layers [7]

Each layer in IoT utilizes different innovations that offer a few issues/dangers. The various conceivable security dangers in IoT for these layers [7].

3. THREATS OVER IOT LAYERS

This section will present a different security threat which exists over different layer of IoT as discussed in section 2 and illustrated via figure 3 bellow.

3.1 Sensing Layer Threats

The security detecting layer agreements with IoT sensors and actuators. Sensors detects the physical sensation around them, actuators, execute a convinced action on the physical surroundings, founded on the sensor data [7]. Different sensing layer is being used in IoT application like GPS, WSNs, RSNs, etc.

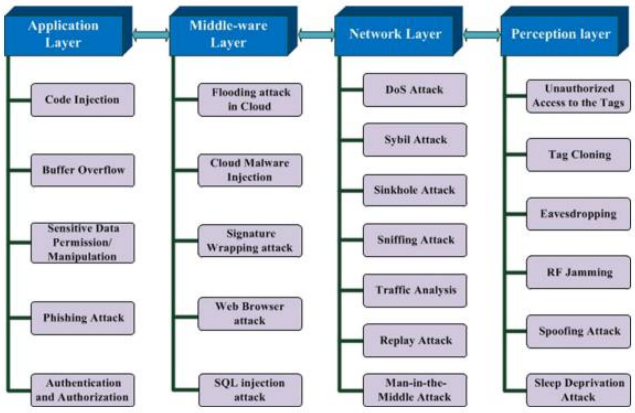

Figure 3: Security Threats in each layer

Major dangers at the sensing layer are as follows:

3.1.1 Node Catching

IoT consists of numerous low power knots such as sensers and actuators. These knots are generally susceptible to different attacks by hackers. The attacker may attempt to replace or capture the knot in the IoT with malicious code. The new knot may be the part of the system but that is measured by the hacker [8].

3.1.2 Malicious Attack

The programmer injects some malignant codes in the hubs. It is a perilous assault that endeavors a bug started by taking care of false information. The vindictive code is injected into an exposed program and changes the advancement of the execution [7].

3.1.3 False Data Attack

When a node is caught, the hacker uses it to insert erroneous data into an IoT device. The hacker uses these methods to affect a DDoS attack.

3.1.4 Side-Channel Attacks

The different attack**s** on side-channel leads to leakage of sensitive and private data [9].

3.1.5 Eavesdropping and Interface

The various nodes are deployed in an open environment. The attacker may capture or eavesdrop through altered stages like communication of data or authentication [7].

3.1.6 Sleep Deficiency Attack

The attacker tries to dugout the battery power of IoT devices. Low nodes are affected by the attacker which results in the drainage of the energy level sensors that lead to the decease of the nodes [7].

3.1.7 Booting attacks

The devices are much susceptible to attack through the booting procedure. The attacker may take benefit of this weakness and try every possible way to harm the nodes when they are being start again [9].

3.1.8 RF Jamming

Radio Frequency Identification can be compromised by any type of a DDoS attack in which communication that is being through Radio Frequency signals that are disrupted with an excess of noise signals [10].

3.2 Network Layer Threats

The network layer's job is to get the packets from sources to the destination at a minimal cost.
The major attacks on the network layer are as follows:

3.2.1 Phishing

Phishing attacks refer to those attacks where numerous devices are targeted by a slight power put by the aggressor. It is a form of identity theft. The possibility of phishing sites is that the users visiting on web pages. If after the user's username and passwords are hacked by the attacker and the entire IoT atmosphere being used by the user becomes compromised and susceptible to cyber-attack [7].

3.2.2 Access attack

Access assault happens when, an enemy or programmer gets contact to the IoT organize. The main aim of this assault to take esteemed information or data, as opposed to give any mischief to the system [5,7].

3.2.3 DDoS Attack

It such type of attack, the adversary or attacker targets the servers with a huge amount of requests. Thus, targeted servers are disrupted to provide services to genuine users [11].

3.2.4 Data transit Attack

In general, most of the data of the users are stored on devices, on local servers or clouds. Data is valuable and therefore the attacker always targets the valuable information of the user.

3.2.5 Routing Attacks

In this attack, the malicious node in IoT applications may try to readdress the routing routes when the data is in transit. The sinkhole is another attack in which rival advertises fake routing route and invites node to traffic over. A wormhole is also an attack of routing attack can become a serious attack if joined [8].

3.3 Middleware Layer Hreats

The job of this layer to make a reflection layer among the system and

application layer. The middleware layer is helpful to give a predictable and solid IoT and it is likewise suspect able to various ambushes. Numbers of attacks in the layer are as follows:

3.3.1 Man, in the Middle Attack

It is such types of attack in which an enemy alters the message among the two parties who rely on they are straight communicating with each other. One example of a MITM attack is an active attack [12].

3.3.2 SQL Injection Attack

In such sorts of assaults, the foe/aggressor can embed malignant SQL proclamations in a program [12,13]. The aggressor gets to the private information of the client and even changes or changes the records in the database [14].

3.3.3 Signature Wrapping Attack

The services of XML signatures are used in the middleware [9]. the attacker breakdowns the signature algorithm and can execute processes or modify it.

3.3.4 Flooding Attack

In such sorts of assaults, the foe/aggressor can embed malignant SQL proclamations in a program [12, 13]. The aggressors get to the private information of the client and even change or change the records in the database.

3.4 Application Layer Hreats

These layer agreements with and give administrations to the end-clients. IoT applications like a keen meter, shrewd urban communities, and savvy frameworks, and so forth. The application layer has a distinct security risk that isn't found on different layers. Such issues resemble security issues and information burglary.
Major security issues are discussed below:

3.4.1 Data Theft

It manages genuine and private information. At the point when the secret information or data is during transmission the information might be entirely suspectable to assaults than the information is very still and in IoT applications, there is a huge information development [9].

3.4.2 Access Control Attacks

An entrance control assault, in which an enemy or programmer gains admittance to the whole IoT arrange. The main reason for this assault to take explicit secret information or data, instead of to make hurt the system [5].

3.4.3 Service Interruption Attacks

The ill-conceived intrusion assaults or DDoS in the present writing. There are various instances of this kind of assaults on IoT. Its bona fide clients from utilizing the administrations of IoT by making falsely servers or systems too occupied to even think about responding.

3.4.4 Malicious Code Attacks

The aggressor infuses some malevolent code in the memory of the bunch. It is a hazardous assault that adventures a bug brought about by preparing unsuitable information. The noxious code is infused into a helpless PC program and changes the course of the execution [7].

3.4.5 Sniffing Attacks

The attacker uses the sniffer application to observe the traffic of the network in IoT. This allows the gain access to confidential data if security protocols are implemented [9].

3.4.6 Reprogram Attacks

In such kinds of attack if the programming process is not protected. Then the adversaries try to reprogram the objects of IoT remotely [15].

4. CRITICAL ANALYSIS

There are various kinds of threats or issues in the sensing layer like node capturing, malicious code injection, false data injection, eavesdropping. These issues can be prevented by applying encryption techniques on all devices IoT application that's performing communication. To avoid access control or spoofing, apply identity-based authentication protocols. The attacks and issues of network layer such as Sinkhole, Man in Middle Attack, DDoS Attack and Malicious code Injection Attack these attacks can be prevented by analyzing the data consistency and network flow information [16]. Use of some Artificial intelligence (AI) to recognize fake accounts. Workloads should be equally distributed among components according to their capacity to completely avoid exhaustion of the power of the battery. Encryption can be applied so no one can steal valuable information or modify the information or encode certain information before the transmission of valuable or private data. In both layers, the Network Layer and Application Layer cryptographic techniques can be applied to secure the network and prevent it from any damage occur. Now last but not the least, to secure the application layer, try to connect only the trusted networks in which you can trust that is not going to provide any damage [17]. Try to encrypt all the traffic flows that leave your system and scan all emails to spot the indicators in the message header, message content and domain information that can indicate a message is suspicious. These were all the solution related to certain layers of IoT and these solution techniques must be applied to ensure the security.

5. CONCLUSION

In this paper different wellsprings of security dangers at various layers of IoT. In this study quickly talked about the dangers connected to the detecting layer, arrange middleware, and application layer. This paper additionally quickly talked about the arrangements that are identified with all these four layers and how to conquer these issues/dangers and how to counteract such assaults happen in IoT. The security of the web of things has additionally been examined with a portion of the examination of future bearings to expand the security of the IoT.

6. FUTURE WORK

In the future, these attacks can be encounter or countermeasures by applying some techniques to prevent these attacks that hit any organization's secrecy or user's privacy. Some of the countermeasures are as follows: Apply encryption techniques on all IoT devices that are being used for communication. Use artificial intelligence to identify fake accounts. Encryption must be applied to secure your information stealing by some adversary or attacker. To ensure the security of the application layer, trusted networks should be connected in which you can blindly trust that they would not result in harm or damage. Such kinds of protection techniques can be used to prevent such attacks in the future.

ACNOWLEDGEMENT

This research was conducted in the Internet of Things, Security Issues and its Solution. We are especially thankful to Dr. Ahthasham Sajid, Assistant Professor of the Department of Computer Science, who has been supportive and worked actively to provide us any kind of assistance whenever we require.

REFERENCES

[1] Wilton, R. 2019. Internet of Things Devices as a DDoS Vector.

[2] Ashton, K. 2019. That 'Internet of Things' Thing.

[3] Suresh, P. 2019. A state-of-the-art review on the Internet of Things (IoT) history, technology and fields of deployment.

[4] Gulzar, M., Abbas, G. 2019. Internet of Things Security. A Survey and Taxonomy, Pp. 7.

[5] Ali, Y. 2019. Security and privacy threats in IoT architectures.

[6] Abomhara, M. 2019. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks.

[7] Hassija, V. 2019. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures.

[8] Raza, S. 2019. Routing Attacks and Countermeasures in the RPL-Based Internet of Things.

[9] Swamy, S.N., Jadhav, D., Kulkarni, N. 2019. Security threats in the application layer in IoT applications.

[10] Li, D., Chen, Y. 2010. Computer and Computing Technologies Jul.

[11] Chaithanya, R.T. 2019. Node capture attack in Wireless Sensor Network: A survey.

[12] Dorai, R., Kannan, V. 2019. SQL injection-database attack revolution and prevention. J. Int. Commercial Law Technol. Jul.

[13] Zhang, Q., Wang, X. 2019. SQL injections through back end of RFID system. in Proc.

[14] Razzaque, M.A., Milojevic-Jevric, M., Palade, A., Clarke, S. 2019. ‘‘Middleware for Internet of Things: A survey,’’ IEEE Internet Things.

[15] Abdul-Ghani, H.A., Konstantas, D., Mahyoub, M. 2019. A comprehensive IoT attacks survey based on a building-blocked reference model,

[16] Schulz, P. 2019. Latency Critical IoT Applications in 5G Perspective on the Design of Radio Interface and Network Architecture.

[17] Mitrokotsa, A., Rieback, M.R., Tanenbaum, A.S. 2019. Classification of RFID Attacks.