ZIBELINE INTERNATIONAL PUBLISHING

ISSN: 2616-5961 (Online)
CODEN: IMCSBZ

Information Management and Computer Science (IMCS)

DOI: http://doi.org/10.26480/imcs.02.2020.38.41

CrossMark

REVIEW ARTICLE

SURVEY PAPER ON IOT ATTACKS AND ITS PREVENTION MECHANISMS

Sher Ali[a], Syed Babar Ali Rizvi[a], Yousaf Ali[a], Ahthasham Sajid[a*], Afia Zafar[b]

[a] Department of Computer Science, Faculty of ICT, BUITEMS Quetta, Pakistan
[b] Department of Computer Science, NUTECH University Islamabad, Pakistan
**Corresponding Author Email: ahthasham.sajid@buitms.edu.pk, gullje2008@hotmail.com*

ARTICLE DETAILS

Article History:

Received 07 November 2020
Accepted 10 December 2020
Available online 28 December 2020

ABSTRACT

IoT has turned into an amazing system of worldwide and worldwide changes, including numerous internet advisors, interchanges, and information trade. This paper presents state-of-the-art background, introduction, characteristics, challenges, threats, attacks, related work, and security architecture and research limitation of IoT technology. This paper discusses key security issues and attacks over different layers of IOT along with its existing prevention techniques. This paper deals with the security of services used in IoT. In detail, IoT devices are mentioned in this paper, which are the premise of IoT and their significance. In addition, IoT Security Architecture highlights some recent studies. This paper is far from comprehensive and mainly focuses on attacks and IoT devices prevention mechanism and covers related discussion and arguments.

KEYWORDS

Internet of Things, IOT attacks, IOT challenges, Security mechanism.

1. BACKGROUND

The term Internet of things, is 19 years of age, but the real concept of related gadgets had been around longer, since the 70s. Back in the years concept was often called "embedded internet" or "pervasive computing". The genuine term "Internet of Things" was first specified by Kevin Ashton during 1999. The main web associated gadget was definitely not a self-driving vehicle or a robot however - it was a Coke machine, which was introduced at Carnegie Mellon University, returning back to the 1980s that could report its stock levels through the ARPANET, as it was known in those days.

The possibility of smart machines that could remove the problem from regular day to day existence kept on being a significant subject. Ten years back, one model that appeared to manifest everywhere was the 'Smart Refrigerator' that could monitor your food supplies and naturally request more when you were coming up short. Utilizing IP network without human difficulty IoT is known as system of gadgets. Therefore, Internet of Things (IoT) environment comprises of intelligent items, gadgets, smartphones and tablets and so on.

2. INTRODUCTION

The internet has been around for some time now, however it's been broadly speaking the product of people, so every one of the information, pictures, games, books, e-commerce and all of that was made by individuals for individuals and about individuals (Singh and Singh, 2015). We're already familiar with the fact that how significant and changeover invention the internet is, it's like a computerized texture that's woven into our lives that has brought a tremendous shift to the world (Singh and Singh, 2015).

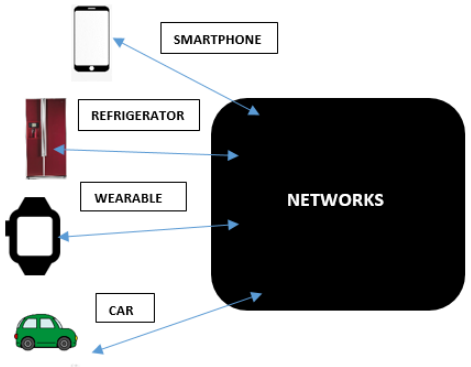

Figure 1: IoT Over Networks

Lately, a new internet is getting an immense amount of recognition, and it is going to take us to new realms of innovations because new internet isn't exactly about bridging people with people, but 'things' with 'things', therefore the name "Internet of Things (IoT)". For instance, your smart watch can track the hours of sleep you took last night, the number of steps taken in a day and each of your daily activity as it communicates through

Quick Response Code	Access this article online	
	Website: www.theimcs.org	**DOI:** 10.26480/imcs.02.2020.38.41

network (Singh and Singh, 2015). Regrettably, this Internet of Things (IoT) is not dependable and safe until it is secure because IoT and security aren't regularly found in a similar spot, they are extremely at risk and people face enormous issues with the privacy of their personal data, and chances are that their data might get locked up or encrypted, since the security mechanism of IoT's often get neglected by the IoT makers (Lee and Fumagali, 2019). It is projected that IoT devices will exceed to 20 billion devices by the year 2020 (Ziegler et al., 2015). As the number of Internet of things devices increases, the security concerns increase as well.

3. Related Work

3.1 IOT Security Architecture

As a result of many researches, IOT devices are more thought to be modelled for more associations for the items in their association forms. This thought has not reached any executable form so far, as it is too imprecise and it requires a number of additional gadgets for its working. The security idea for IOT needs to be understood for any implications. IOT design has a number of procedures including highlights, for example, sensors, conventions, actuators, cloud administrations, and layers. It is thought to be as the third rush of the World Wide Web (WWW). The IOT is a comprehensive system that has a distinguishing sort of articles combined together by means of a prominent web convention entitled Internet Protocol (IP).

As stated to researchers the conventional IOT architecture be made up of three layers:

1. Perception Layer
2. Network Layer
3. Application Layer

Another layer, named the help or support layer, has also been distinguished by few scientists which is incorporated into IOT's most recent design and it lie down betwixt the application layer and system layer. The help layer comprises of mist figuring and distributed computing. Distributed computing is said to be the most popular subject today in research.

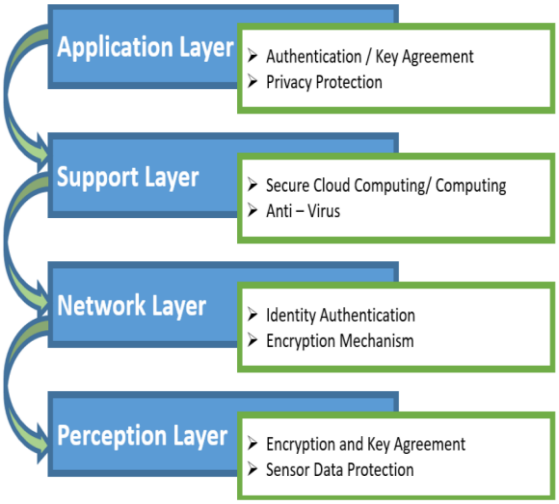

Figure 2: Security over IOT Layers

3.1.1 Perception Layer

Perception layer is likewise called the observation layer or the affirmation layer. It is the most negligible layer of the normal plan of IoT. The essential target of this layer is to accumulate supportive information/data from things or the earth, (for instance, WSN, heterogeneous devices, sensors type certified articles, clamminess, and temperature, etc.) and transform them in an electronic/computerized arrangement. These things are stand-out area unmistakable verification and correspondence between short-run propels, for instance, RFID, Bluetooth, Near-Field Communication (NFC), 6LoWPAN (Low Power Personal Area Network). The perception layer is alluded to as the cerebrum of an overall IOT plan.

3.1.2 Object Layer

The observation layer speaks to another layer called article layer or object layer. This layer's main goal is to gather data and information from various heterogeneous class gadgets, then this information afterward processed and digitized. In addition, it also moves the handled information into upper layers of IOT design.

3.2 Object Abstraction Layer

The object layer then speaks to an object reflection layer. The work of object reflection layer is of a mediating layer that sits between the administration of executives and the article layer. In object reflection (also called article reflection), RFID, WIFI and Third Generation (3G) correspondence advances are utilized.

3.3 Application Layer

This is the uppermost layer of general IOT design. The application layer is additionally partitioned into three sub-layers on the basis of different functionalities. The layer's primary objectives include encouraging data handling, basic leadership, and control of matching requestor data preparing for pertinent errands. As per the pre-requests of the clients, the application layer allocates prominent great offices. The Business layer speaks to the plan of action and information that it has been gotten all from the application layer. The IOT mindfulness relies upon the obligatory segments.

4. IOT Research Limitation

The structure pursued to perform the directed study is outlined here to assess the exploration works that done in writing and to make decision whether these points has been totally examined. As IoT vision and its security is commonly new, our obsession was on the disseminations that were proposed from 2000 to 2017. These creations consolidate books, journals, meetings, sites, white-papers, and reports. While implementing and looking into latest IoT-related applications, we have to deal with the usual specialized prerequisites, for example, adaptability, dependability, Quality of Service, security, interoperability, portability, and so on. Such necessities can be tried and approved in customary research labs.

In any case, a methodology concentrated on specialized necessities may prompt a missed objective if the end-client viewpoint isn't appropriately considered. In the IoT area, end-client prerequisites are presumably as much significant as specialized ones. Henceforth, understanding the end-client acknowledgment and fulfillment is basic. IoT Lab is building up a stage for analysts who need to address the two measurements. It empowers them to test and send IoT cooperation's out in the open spaces, while gathering publicly supporting and group detecting contributions from end-clients.

5. Characteristics of IoT

a. Interconnectivity: IoT provides the ability to interconnect devices through internet.
b. Smart Sensing: IoT devices have smart sensing capabilities for example, the use of thermostat to turn on/off the heat in homes.
c. Safety: IoT devices also ensures safety of individual's life. For example: smart watches/phones, gives information about heart pulse rate.
d. Intelligence: IoT devices changes their states dynamically, depending on the environment, time, location or speed.
e. Expressing: IoT devices can give information to other connected devices about their current state within its surrounding. Furthermore, provides better communication flow between humans as well as machines.

6. Attacks on IoT

6.1 Physical Based Attacks

As an attacker attack on the product of IoT gadgets. Correspondingly, they can likewise attack on the equipment segment of IoT gadgets. For instance,

RFID readers, sensor, and diverse RFID TAG types. This all are powerless against the physical assaults. In this area we will portray various kinds of physical assault that are exposed to an equipment part of IoT gadgets.

6.2 Object replication attacks

An attack in which the attacker basically adds some objects to the network. Giving an example, a malicious line of code as to be added to the network. In order to decrease the performance of the network. The primary task of this malicious object is to corrupting or misdirecting the received packet.

6.3 RF Interference on RFID

Type of attack in which the attacker will send a huge amount of noise signal over frequency.

6.4 Hardware Trojan

The main concern to all the security issues. The hardware Trojan i.e. malicious modification made by third party for integrating circuit and system use in critical application.

6.5 Outage Attacks

By putting the group of IoT devices into an unattached environment this attack can be done by the attackers. The attackers will stop operating the devices by powering off or by using much power.

6.5.1 Object Jamming

As we know, about the benefits of wireless in IoT devices but it cannot be a safe communication as attackers may jam the signal by jammers.

6.5.2 Physical Damage

As we deployed our IoT devices in unattached environment. So, it can be harmful to the hardware component of IoT.

6.5.3 Camouflage

In this type of attacks the attackers will physically insert his object to the network in hidden way among the other objects. The main functionality of the object is to redirect the packet.

6.5.4 Malicious Node Injection

Attackers will insert the malicious object in the network. As result an unapproved can get to the IoT network. It might likewise embed bogus information to hamper the conveyance of message.

6.5.5 Social Engineering

Authors has described social engineering as a physical attack. In this sort of assault, the assailant controls the client of IoT framework and may likewise get their significant information.

6.5.6 Side-Channel Attack

Side-channel attack can be used to break the encryption mechanism by getting information about what devices do while operating encryption process.

6.6 Network Attacks

The growing reality of the IoT also means recognizing its possible consequences. IOT systems are likely to be affected by various network attacks.

6.6.1 RFID Spoofing

This is a type of attack in which the attacker spoofs the RFID signals. The attacker will give false information which will be accepted by system.

6.6.2 Traffic Analysis Attack

In Traffic Analysis Attack, attacker expropriate and inspect the messages in order to get facts and figures from communication.

6.6.3 RFID Cloning

The attackers copy data from pre-existing RFID from another RFID, the attacker cannot get the original id of RFID. The main function is inserting wrong data and control the data processing.

6.6.4 RFID Unauthorized Access

The RFID will check if the authentication is correct or wrong. In case, the adversary is observing, then it will change or remove the data on nodes.

6.6.5 Man in the Middle Attack

This attack can be done over the internet between two nodes to intercept their communication and to get their important data through eavesdropping.

6.6.6 Denial of Service (DOS)

The attackers ping flood over the server so that services are unavailable to the requested node.

6.6.7 Routing Information Attack

This is the attack in which the attacker makes the network complex by spoofing. Attacker modify the routing information. The main function of this attack is providing inappropriate information and to break the network.

6.7 Software Attacks

Attacks that can be done by viruses, worm etc. In order to loot data and deny the services of the targeted IOT device.

6.7.1 Phishing

It's a common formation of bluffing in which a fake internet site is fabricate that looks just like the legalized internet site. The fake internet site is on a server under the control of the attacks.

6.7.2 Viruses of Different types

Virus is nothing but a part of program which harms our data badly. Viruses decrease the performance of the device. For example:

- Worm
  Program that fills the computer with self-replicating files
- Macro-Virus
  This virus is used to infect application software while opening the infected file, macro virus is charged into main memory and then knocks down the stored data.

6.7.3 Malicious Scripts

Is an illegitimate program that lives inside a legitimate program. It creates secret ways for attackers to get through into your system. The attacker inserts the malicious script in order to get access of the devices.

7. IOT CHALLENGES

The biggest and the most imperative aspect of the IoT is the security of the devices connected to the network. The application on which an IoT device operates, can gather information which could be personal, industrial, or even enterprise and this data should be save from attacks like theft, tempering, traffic analysis. For example, an IoT device can store historical data about an individual's movement patterns. Health, shopping behavior, business orders and even location. The main concern is the transmitted data which is sent over the internet via a secured private networks or virtual private network. The Internet of Things (IoT) tasks should make sure to provide application-level security protection i.e., DDoS. Denial of Service attack. Furthermore, it should also take certain measures to recognize entities that are requesting access including any form of data that includes multi-factor authentication.

7.1 Data Privacy

Smart devices like smart watches or smart TVs can collect information about the movement patterns or viewer's preferences and they can send the data to the manufacturer.

7.2 Data Security

As IoT devices transfer load of data from surveillance devices over the internet for live analytics, the security of data still exists.

7.3 Technical Concerns

The network on which an IoT device sends or receive data should be of high capacity so that It can handle high capacity and density of the devices. Furthermore, it should be able to distinguish between the devices that are permitted and those which are not.

8. IOT SECURITY MECHANISM

IoT's cycles the capacity which includes gathering information from other IoT gadgets, information preparing and furthermore connection with different facilities for dynamic about additional exercises, for example, initiating actuators. The developed platforms in terms of security requires more time as well as a larger number of people to maintain the security. The reliable infrastrcutures like IaaS and PaaS are being frequently used by the develoed platforms as a result of which the responsibilities invloving physical exxecution of the operating system software is transfered to others, therefore, resulting in reduced responsibility of the team developing its own platform. The objective is to provide a platform through which data privacy and security is emphasized. Application developers have to play key role for the development and functionalities related to security. A built-in security mechanism would be the main objective. Some of the IoT prevention mechanism are as follows:

8.1 Cryptographic Algorithm

Cryptography is utilized to change plain content into figure text with the goal that the programmer can't recover the data. Different keys are generated through different algorithms that can convert the plain text into cipher text. An encryption plan of action has five fixings. (Plain content, Encryption Algorithm, Secret Key, Cipher Text, and Decryption Algorithm). To make sure about correspondence between IoT gadgets and organizations there are hardly any cryptographic calculations.

- Symmetric Encryption/Private Key: In this encryption addressee and beneficiary (recipient) shares a familiar key. All traditional encryption algorithms are private key.
- Asymmetric Encryption: In this encryption method key is different between sender and recipient.
- Hashing: Hashing is a method of cryptography that change any type of information into any line of text. Any piece of information can be hashed, regardless of its size or type.
- Hash Function: Hashing contains different hash functions. Hash functions are used in security based programs to make sure data integrity and digital signature. Hash esteem is a (single direction) hash (numerical) work that takes an information string and changes it into a fixed length twofold arrangement. Whenever the converted hash value of sender and receiver matches, this means the message is appropriate.
- No Direct Device –to-Device Communication: Mainly, the term used in IoT is Machine-to-Machine (M2M). It is the misunderstanding that IoT devices communicate among them at first hand.

Furthermore, highlighting that IoT devices communication are routed to application layer within backend host. If IoT devices require communication among IoT device A and IoT device B this should be done through application layer at backend host. It is possible to configure direct communication between multiple IoT devices through carrier's data center. Suppose, IoT devices communicate directly without approaching application layer, then no record and foot prints are recorded in customer's router or backend host system (Ziegler et al., 2015).

8.2 PIN Locking of SIM

PIN locking in IoT is used as a device security strategy. The device manufacture makes a protected hashing algorithm inside the gadget's processor's firmware that is stored from hardware serial number for example, IMEI consist of 4-digit number. Furthermore, manufacturer configured SIM to locked state with 4-digit number. At power up or restart SIM demands open code by means of radio interface to the device 's processor. Moreover, firmware executes the hashing algorithm to produce the 4-digit open code. If the code matches with SIM, the SIM will be enabled. If the PIN doesn't coordinate after three tries the SIM is rendered, unusable or blocked. There is an unblocking arrangement utilizing 8-digit code known to the device's manufacturer and if that code is inaccurately controlled ten times SIM turns inoperable for all time (Ziegler et al., 2015).

9. CONCLUSION

The presence of IoT worldview over the most recent couple of years has released such a large number of dangers and achievable assaults against security and protection of IoT items and people. These dangers lead to hamper the acknowledgment of this worldview on the off chance that they have been left without legitimate countermeasures. This paper, in this way, tries to give a far-reaching classification of IoT assaults alongside proposed countermeasures to reduce them. Given IoT designers and specialists, willing to build up a protected IoT framework, a chance to explore which assaults have been fired, how they have been alleviated, which assaults still stick around was the primary target of this paper.

REFERENCES

Singh, S., Singh, N., 2015. Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce. Proc. Int. Conf. Green Comput. Internet Things (ICGCIoT), Noida, India, Pp. 1577–1581.

Lee, C., Fumagalli, A., 2019. Internet of Things security–multilayered method for end-to-end data communications over cellular networks. Proc. IEEE 5th World Forum Internet Things (WF-IoT), Limerick, Ireland, Pp. 24–28.

Ziegler, S., Nikoletsea, S., Krco, S., Rolim, J., Fernandes, J., 2015. Internet of Things and crowd sourcing—A paradigm change for the research on the Internet of Things. in Proc. IEEE 2nd World Forum Internet Things (WF-IoT), Milan, Italy, Pp. 395–399.