International Journal of Multidisciplinary Research and Publications
ISSN (Online): 2581-6187

Critique on Security Attacks in Internet of Things

S. Shunmuga Priya[1], M. Sujaritha[2]
[1]Computer Science and Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, Tamilnadu, India - 641008
[2]Computer Science and Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, Tamilnadu, India - 641008
Email address: shunmugapriyas @ skcet.ac.in, sujaritham @ skcet.ac.in

Abstract**—** *Internet of Things has changed todays contemporary world into a classy one. IoT has enormous features that attract many fields like Industry, healthcare, robotics, business and then on. IoT has stepped its foot into many disciplines and it is creating boons day by day. Though it has many pros, it is facing its own issue. Security of IoT is one among the foremost challenging issues faced today. Many researchers try to repair this issue. Creating IDS, Honeypots, Using blockchain technology, etc. are some significant approaches to unravel security problems with IoT. To overcome this issue completely it's essential to possess a transparent knowledge about the safety issues faced by the IoT. Therefore, an entire critique about security attack on IoT system may be a basic need for the security researchers. Only clearness with the problem gives clear solution. Our contribution is to perform this task. This paper explains about the security attacks faced by the IoT system. Each layer of the IoT faces and suffers from many security attacks by intruders and attackers. The list of security attacks on IoT and how they affect and impact the IoT system is deeply discussed here. This helps to create a secure solution in future.*

Keywords**—** *IoT Security, Attack, malicious, intruder, attacker, Internet of Things, IoT.*

I. INTRODUCTION

Due to the eminent growth and affordable availability of powerful devices like sensors, RFID (Radio Frequency Identification) tags, NFC (Near Field Communication) cards, etc., there is a giant growth in the field of Internet of Things (IoT). IoT is Connection of interconnected objects possessing unique address with standard protocol for anytime anywhere communication via internet infrastructure [1].

IoT has created many boons in many fields such as Smart Agriculture, Smart City, Smart Infrastructure, Supply Chain and logistics using IoT, Healthcare systems and so forth. IoT has paved way to do many tasks like Monitor shelf life, Improve customer experience, Track inventory, Have on-the-fly promotions, Evaluate customer behaviour. IoT enables devices to be mutually connected with each other to facilitate data exchange. Enormous number of devices can be connected with each other.

It is estimated that the number of devices connected to IoT will cross 18billion by 2022 [2]. These devices focus on human to machine interaction along with device to device interaction. Due to large number of device connectivity and devastating features of IoT, it is prone to many security attacks. [3]

The functionalities of IoT can be grouped into four layers, viz., Perception Layer, Network Layer, Processing Layer and Application Layer. Perception Layer consist of devices/nodes which are capable of sensing the environment and has communication capability. It includes various sensors, RFID tags, NFC cards, GPS system, web camera, etc. The Network Layer is responsible for communication and data exchange. It makes connection between the remote servers and the nodes or any clients in the lower layer. All these layers can be prone to security attack. Processing Layer has the Gateway which acts as the protocol convertor and helps the network connectivity. The Application layer gives sophisticated usability to the clients by GUI and API [4]. Intruders try to attack the IoT system by attempting attack on all these four layers. Each attack affects the IoT system in different way and creates remarkable impact. The list of all these attacks is elaborated in this paper.

This paper is organised as follows. In this paper, section I gives the introduction about the Internet of Things and the emphasis of it that kindles the intruders to attack the IoT system. The security attacks are categorised in many different ways. This is discussed in section II. The next part (section III), discusses the types of each attack on IoT system. Finally, section IV concludes the paper.

II. CATEGORISATION OF SECURITY ATTACKS

Categorisation of Security attacks differ based on scenario and experts. In this section few of the flavours of category is discussed here.

A. Category1:

Active attacks Vs Passive attacks

Attacks which compromises the devices or nodes and create harmless to the device or data or any other resources, then it is called Active attack. Attacks which listens and analyses to the data or resources without disturbing the system, it is called passive attack. Both active attack and passive attack can be triggered on any IoT system.

B. Category2:

Based on the attacks triggered on the resources of IoT systems, the attacks are classified as Physical Attacks, Network Attacks, Software attacks and Data Attacks. This categorisation deals with how each attack affects the functionalities and layers of IoT. Physical Attack attempt to make attack physically on the hardwares which are readily accessible by the intruders. Network attacks affects the communication link and data exchange and network connectivity of the legitimate nodes. Software attacks are

S. Shunmuga Priya and M. Sujaritha, "Critique on Security Attacks in Internet of Things", *International Journal of Multidisciplinary Research and Publications*, Volume 3, Issue 7, pp. 9-12, 2020.

purely performed by software and logically affects the IoT system. Data attacks deals with the encryption of data that is exchanged.

C. Category3:

Categorisation can be done by grouping the attack targeted on the layers of IoT System. These attack targets the unique functionality of the IoT system. Most of the physical attack

III. Security Attacks

There are many security attacks prevailing that affects the IoT system. Each attack has a peculiar target and performs harms to the IoT system in a unique way. Here is the list of Security attacks targeted on IoT system.

A. Physical Damage

The Perception Layer of the IoT has many powerful sensing and communicating devices. These are also referred as nodes. Due to the tradeoff between availability and security, these nodes are implanted in open environment for easy access. This makes a great issue to the security. Any intruder can easily damage these devices or any components of IoT system either intentionally or intentionally. On such scenario, the malfunctioning of these nodes causes great security issue.

B. Node Tampering

The attacker alters the contents of the compromised node physically or modifies the device or communication link. He can get access to sensitive information like encryption key, log file, etc. and corrupt it and collapse the data exchange.

C. Man in the Middle attack

The attacker plays between the sender and recipient. The attacker sits between the sender and recipient, the attacker reads and modifies the information before sending it to the recipient. Both sender and receiver will be unaware about the attacker playing in the middle. The man in the middle attack paves way for many other attacks like ARP cache poisoning, DNS spoofing, session hijacking like side-jacking, evil twin, sniffing, SSL Hijacking [9]

D. Node Jamming

With the help of devices like jammer the attacker controls the signals of wireless communication of the node and disturbs the communication of the nodes. This is called node jamming attack.

Both RF Interference and Node jamming attacks are used to trigger Denial of Service attack.

E. Malicious node Injection

Unauthorised and unintended node can be injected physically in the IoT system. Injecting these nodes in perception layer is a quiet easy task. These malicious node settles between two nodes and modifies the data and passes wrong information to the other nodes. The attacker takes replica of the victim node and along with that it uses more number of malicious nodes to perform this attack. The verifier node or the monitoring node also gets collapsed due to this attack. There is a chance that legitimate nodes are reported as malicious by the verifier nodes.

F. Malicious Code Injection:

The attacker introduces suspicious codes physically into the node of the IoT system. Thus, the attacker can gain complete control of the IoT system and perform required malicious actives.

G. Barrage Attack:

For extending the power and network longevity, the sensor nodes enter low power sleep mode. To avoid the sensors to enter the sleep mode, the attacker sends legitimate requests to the sensor nodes and avoid the sensor entering low power sleep mode. [6]

H. Sleep Deprivation Attack:

The aim of this dangerous attack is to interrupt the sensors entering the low power sleep mode. The attacker makes request to the victim node at periodic intervals. The request to the sensor is made such that the sensor never enter the low power sleep mode. Thus, the power of sensor gets depleted and node dead condition occurs. [6]

I. Traffic Analysis Attacks:

It is a passive attack. The attacker gets the information by analysing the network traffic without harming the victim nodes. Based on the gained information from the network traffic indirect harms can be caused to the IoT system.

J. RFID Attacks:

RFID is used for sensing by the perception layer and many attacks are performed by capturing or malfunctioning the RFID tag and RFID technology. [7] The following are some of the RFID attacks.

a. RFID spoofing

A malicious node imitates the RFID signals. The attacker captures the information about the security protocol used in the RFID system. Using this information, the attacker writes the received data with the same format to his own blank RFID tags and thus performs tag duplication. On doing this the reader things the information is from original tag but actually it is from the spoofed tag. Sensitive information like price, expiry date, etc. can be modified by the attacker with his duplicate tag.[8]

b. RFID cloning

Cloning and Spoofing looks to be similar, but they are entirely different. The attacker replicates the information of a original tag in to a new black chip. The attacker owns this tag.

c. RF interference

This attack is targeted on RFID tags. Noise signals are created and sent over the RF signals or signals from the sensors. Thus, the RFID communication gets interrupted due to the heavy noise signal. The RFID ’s communication is disrupted or collapsed by the attacker

d. RFID eavesdropping

With the help of a fake RFID reader the communication information is lured by the attacker. When fake reader communicates at the same frequency as that of the original reader, the fake reader can gain the information transferred

S. Shunmuga Priya and M. Sujaritha, “Critique on Security Attacks in Internet of Things”, *International Journal of Multidisciplinary Research and Publications*, Volume 3, Issue 7, pp. 9-12, 2020.

between the original read and the tag. Due to the storage limitations the RFID system transfers non-encrypted text which can easily be eavesdropped with the fake reader. This paves way to Replay Attack.

e. RFID jamming

In RFID Communication there are two main components RFID tag which is attached with the objects to be tracked and the RFID Reader which tracks the tag and give information. There will always be a wireless communication between the tag and the reader. Jamming attack heckles the air interface between the reader and the tag and prevents their communication. Disruption in air medium is done easily. Producing Radio noise at the same frequency of the RFID system collapses the communication between the tag and the reader very easily.

f. RFID deactivation

The motto of this attack is to deactivate the RFID tag without the knowledge of the RFID reader. The attacker sends deactivating commands like delete or kill to the tag. On receiving this, the tag stops its functionalities. After this process, the genuine reader will be unable to identify or detect the presence of the tag even though the tag is in the detection range.

g. Detaching the tag

RFID tags are physically attached to the objects or things. The attacker simply detaches the tag physically from the original thing and switch it to another thing/object. The reader will not have the knowledge regarding this and thinks the tag is attached with the original object.

h. RFID replay attack

To listen the communication for long time and to make the victims believe that no passive attack is happening, the fake reader performs replay attack. It performs eavesdropping attack and gains all the information. Then the fake reader replicates the message to the original reader or the tag by acting as the original source.

K. Denial of Service Attack (DoS):

The target of DoS attack to make the IoT resources unavailable to the legitimate intended users. The victim node can be the IoT server at application layer or even the RFID reader or any device which respond to the request in the IoT system. The attacker floods the network with flooding messages. It can be SYN Flood with Spoofed IP, TCP Connect Flood or using ping with random source IP. [12] Thus the genuine server will be busy in responding these fake flooded requests resulting in exhausting of resource and thus legitimate intended users are starved without getting required responses.

L. Distributed Denial of Service attack (DDoS):

DDoS attack affects the frequently utilised things with the IoT system. The attacker sends control packets to the genuine nodes and compromise them. These compromised nodes are subsequently manipulated to send the rouge data packets to the victim node and thus the attack is triggered resulting in resource depletion or starving of legitimate nodes from getting serviced. The system affected by malware like worm, trojan horses etc are preferably chosen to cause this DDoS attack. The strength of this attack is that more than one type of attack to one particular target system can be generated in a little time duration. [11]

M. Sinkhole Attack

This attack is one of the destructive attacks comparing other routing attacks. The attacker advertises that it has good route knowledge so that it knows the shortest path to reach the desired receiver. Thus, all the traffic is attracted towards the attacker. Then it discards the packets and demolishes the network communication.

N. Sybil Attack

The attacker creates fake identities. These identities are either stolen or fabricated. With tis fake identities multiple distinct nodes acquire disproportionate level of control and reduces the effectiveness of the network. This attack is capable of affecting data integrity, resource utilisation and overall network performance. [13]

O. BOTNet Attacks

The attacker compromises a greater number of devices (these are sometimes called as zombies or bots) and forms an interconnected network called botnet. The bots are so much powerful that it can compromise more devices and strengthen the botnetwork. With this botnet the attacker can do malicious activities like sending large volumes of spam messages targeting a victim, steal credentials at scale, or even spy on other device, people or even organisations.

P. Bad Mouthing Attack:

This attack is popularly seen in trust-based system and recommendation system. The attacker sends false recommendations targeting the legitimate nodes to get lower trust values there by increasing the trust value of the intruder systems. This attack performs collusion. In this process, malicious nodes collude with each other to send bad recommendation on a particular target node.

Q. Phishing Attack:

The theft of identity is the root cause to perform Phishing attack. Phishing attack targets to steal sensitive information like username, password, important credentials and online banking details from the victim. Social Engineering is the backbone of the phishing attack. [14]

R. Malwares

These are purely software attacks. The attacker writes a piece of code to compromise the victim. The malware includes Virus, Worms, Trojan horse, Spyware, Aware and so on. Virus is a self-replicating code targeting to devas all the data resources in the IoT device. Worms affect the devices in the network connectivity. Trojan horse works with the help of backdoor in the IoT system.

IV. Conclusion and Future Work

In this paper, List of security attack on IoT system is discussed in detail. The emphasis and impact of each attack is stated clearly. Security of IoT is very much essential to have

smooth real time projects. So, the list of attacks affecting the security of IoT is identified and presented in this paper. The future work is to identify countermeasures to overcome these security issues in IoT.

REFERENCES

[1] G. M. Luigi Atzori, Antino Iera, "The internet of things: A survey," Elsevier journal on Computer Netwroks, vol. 54, pp. 2787–2805, 2010.
[2] Ericsson, The connected future, https://www.ericsson.com/en/mobility-report/internet-of-things-forecast.
[3] A. Mosenia, N. K. Jha, A comprehensive study of security of internet-of-things, IEEE Transactions on Emerging Topics in Computing 5 (4) (2017) 586–602.
[4] A Comprehensive survey on attacks, security issues and Blockchain Solutions for IoT and IIoT.
[5] S.N Uke, A.R Mahajan, R.C Thool "UML Modeling of Physical and Data Link Layer Security Attacks in WSN", International Journal of Computer Applications, Volume 70– No.11, May 2013.
[6] Matthew Pirretti, Sencun Zhu, N. Vijaykrishnan, Patrick Mcdaniel, and Mahmut Kandemir "The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense" ISSN 1550-1329 1550-1477 International Journal of Distributed Sensor Networks, Vol. 02, No. 03, May 2006: pp. 267 - 287
[7] Denver Braganza* and B. Tulasi, "RFID Security Issues in IoT: A Comparative Study", Oriental Journal Of Computer Science & Technology, ISSN: 0974-6471 March 2017, Vol. 10, No. (1): Pgs. 127-134
[8] Tri Van le, Mike Burmester and Breno de Medeiros, 2007, Forward-secure RFID Authentication and Key Exchange, IACR ePrint.
[9] Zoran Cekerevac, Zdenek Dvorak, Ludmila Prigoda, Petar Cekerevac, " Internet Of Things And The Man-In- The-Middle Attacks Security And Economic Risks ", Security and economic risks MEST Journal Vol. 5 No. 2 pp. 15-25.
[10] Lulu Liang, Kai Zheng, Qiankun Sheng, Xin Huang, A Denial of Service Attack Method for an IoT System, 2016 8th International Conference on Information Technology in Medicine and Education
[11] Isolation of DDoS Attack in IoT: A New Perspective Upendra Kumar Shreyshi Navaneet Neeraj Kumar Subhash Chandra Pandey, Wireless Personal Communications Wireless Personal Communications. ISSN 0929-6212 October 2020
[12] L. Wallgren, S. Raza, and T. Voigt, "Routing attacks and countermeasures in the rpl-based internet of things," International Journal of Distributed Sensor Networks, vol. 2013, 2013.
[13] K. Zhang, X. Liang, R. Lu and X. Shen, "Sybil attacks and their defenses in the Internet of Things", IEEE Internet Things J., vol. 1, no. 5, pp. 372-383, Oct. 2014.
[14] B. B. Gupta, Nalin A. G. Arachchilage, Kostas E. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions", Telecommun Syst Springer Science , May 2017.