International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869 (O) 2454-4698 (P) Volume-8, Issue-9, September 2018

IOT – Attacks and Challenges

K.Somasundaram, Dr.K.Selvam

***Abstract*— Internet of Things (IoT) is becoming a big boom in the wireless networking. This is connectivity among different entities or things. As the devices are directly connected to each other to share the information there occurs a challenging issues in security.This is a study paper which focuses on the vulnerabilities and various attacks in each layer of the IoT.**

***Index Terms*— Authentication, Confidentiality, Integrity, Internet of Things, security**

I. INTRODUCTION

The Internet of Things, or IoT, is a network of smart devices that connect to each other in order to exchange data via the internet without human intervention. .Large number of things is interconnected through the Internet, So that the objects have sensing, communication and actuation capabilities. IoT applications include smart home, health care monitoring, smart city, utilities, smart agriculture, industrial control, environment monitoring etc., These IoT application deals with sensitive information which should not be disclosed to attackers and unauthorized persons. Applications of IoT can bring convenience to people, but it cannot ensure the security of personal information. So the security of IoT cannot be ignored. Attacks against IoT include stealing sensitive data, injecting false information or may disrupt the functions of even networks. Some attacks may lead to high risk, for example, hacking medical devices may lead to loss of human lives. Since the devices are directly connected to the user's day to day life. So security takes the highest priority. The main challenge in IoT security is to prevent attackers from the IoT systems.

This study presents a study and survey of all the security issues in IoT. Thus it gives a brief idea of IoT including the architecture of IoT and security issues of each layer

II. ARCHITECTURE OF IOT

IoT architecture is a network formed by interconnection of devices in any environment. For example, home, business or retail to facilitate communication.

It consists of 3 major layers.

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

Perception Layer: This is the upper and physical layer of IoT architecture. This has sensors for sensing and gathering information about the environment. This consists of sensors like RFID (Radio Frequency Identification) barcodes or any other sensor network. The sensor technology, nano and embedded technology belong to this layer. With the help of sensors in the objects, this layer identifies the distinct object and collects information from the physical world.

Network Layer: This layer is responsible for broadcasting the gathered information from the previous layer to network devices like WIFI, Bluetooth, 4G, Zigbee etc.,and servers. It is used for transmitting and processing sensor data. Thus it serves the function of data routing and transmission to different IoT hubs and devices over the Internet.

Application Layer: This layer has various practical application of IoT based on the needs of users. This provides the authenticity, integrity and confidentiality of the data. The purpose of IoT which is the creation of smart environments is achieved here.

IoT systems include the following components:

- Smart devices with embedded processors
- Gateways with edge processors (smartphones, hubs, or servers)
- Cloud or data centers with remote servers that exchange data through wireless connections

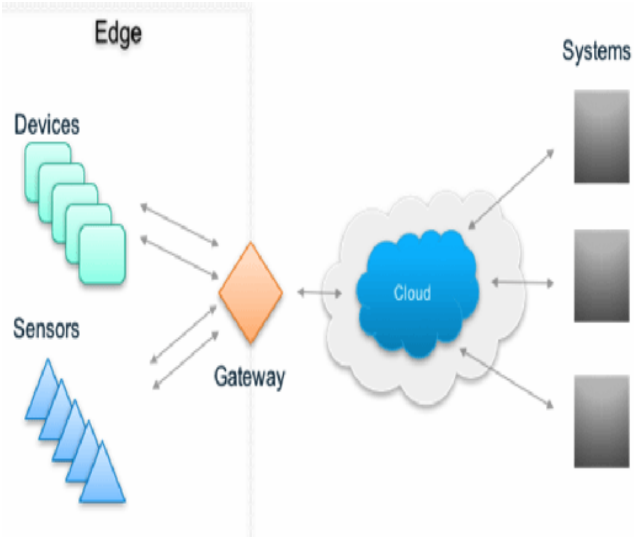


Fig 1: Components of IoT

III. ATTACKS ON THE COMPONENTS OF IOT

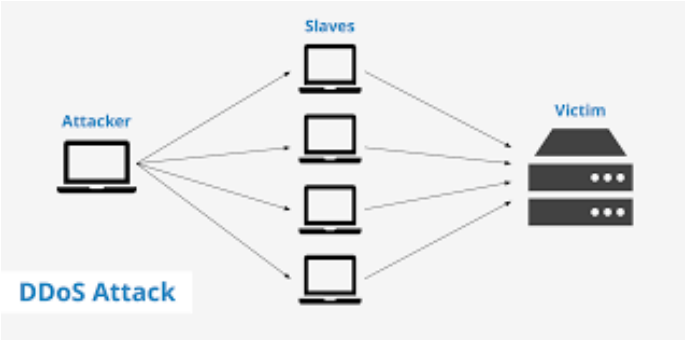
Man-in-the-middle: Unencrypted communications or poorly protected IoT networks can be exploited by attackers who insert traffic between devices and cloud-based applications. An attacker breaches, interrupts or spoofs communications between two systems. For example, fake temperature data 'generated' by an environmental monitoring device can be spoofed and forwarded to the cloud. Similarly, an attacker can disable vulnerable HVAC systems during a heat wave, creating a disastrous scenario for service providers with affected models.

K.Somasundaram, Research Scholar, Department of Computer Applications , Dr.M.G.R.Educational and Research Institute, Chennai
Dr.K.Selvam, Professor,Additional HOD, Department of Computer Applications , Dr.M.G.R.Educational and Research Institute, Chennai

Data & identity theft: Data generated by unprotected wearables and smart appliances provide cyber attackers with an ample amount of targeted personal information that can potentially be exploited for fraudulent transactions and identify theft.

Device hijacking: The attacker hijacks and effectively assumes control of a device. These attacks are difficult to detect because the attacker does not change the basic functionality of the device. It only takes one device to potentially re-infect all smart devices in the home. For example, an attacker who initially compromises a thermostat can theoretically gain access to an entire network and remotely unlock a door or change the keypad PIN code to restrict entry.

Distributed Denial of Service (DDoS): A denial-of-service attack (DoS attack) attempts to render a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. In distributed denial-of-service attack (DDoS), incoming traffic flooding a target originates from multiple sources, making it difficult to stop the cyber offensive by simply blocking a single source. For example, Mirai is a malware that turns networked devices running Linux into remotely controlled "bots" that can be used as part of a botnet in large-scale network attacks. It primarily targets online consumer devices such as IP cameras and home routers.



Permanent Denial of Service (PDoS): Permanent denial-of-service attacks (PDoS), also known as phlashing, are an attack that damages the device so badly that it requires replacement or reinstallation of hardware.

Vulnerable points to an IoT gateway

Physical Attack: The devices are attacked by unauthorized access to gateway hardware, and unauthorized geographical movement.

Software Attack: Attacks like Virus, Trojan, Worms, Denial of Services and Jamming are done in IoT gateways. Safety and critical informations such as warnings of a broken gas line, can go unnoticed through DDoS of IoT sensor information.

Network Attack: The networks are attacked by Node Capture, Node Subversion, Node Malfunctioning, Message Corruption, and by Routing Attacks.

Cryptanalysis Attack: Cryptanalysis is the science of cracking codes and decoding secrets. It is used to violate authentication schemes, to break cryptographic protocols, and, more benignly, to find and correct weaknesses in encryption algorithms. The attacks like Cipher text only, Known-plaintext, chosen plaintext, Man in the middle attack and Birthday attack.

*Side Channel Attack: side-channel attack is a form of reverse engineering. Electronic circuits are inherently leaky – they produce emissions as byproducts that make it possible for an attacker without access to the circuitry itself to deduce how the circuit works and what data it is processing. Heat and electromagnetic emissions are both viable sources of information for an attacker. Because these emissions do not play a part in the operation of the circuit itself – they are simply side effects of it working – the use of them to perform reverse engineering has earned the term 'side-channel analysis' or 'side-channel attack'. Eg***:** Micro Probing, Reverse Engineering.

IV. SECURITY CHALLENGES OF IOT

A security challenge of IoT is divided into 2 classes.

1. Technological Challenges
2. Security Challenges

Technology challenges related to wireless technology, scalability, energy and distributed nature of IoT. This arises due to the heterogeneous nature of IoT devices.

Security Challenges related to the principles and functionalities that should be enforced to achieve a secure network. This ensures security by authentication, confidentiality, end to end security, integrity etc.,

Security issues existing in the IoT layers are explained as follows.

Perceptual layer Security Issues:

This layer mainly includes nodes like Smart card, Reader, RFID tag and WSN (wireless sensor network). Each of these devices has following exposure which leads to be a security issue of IoT.

RFID implementations provide unique identification to the objects that are attached. The RFID tags are open to various attacks. The most common types of attacks are

1. Unauthorized tag disabling - authenticity attack
2. Unauthorized tag cloning – integrity attack
3. Unauthorized tag tracking – confidentiality attack
4. Replay attacks – availability attack

RFID implementations are exposed to physical and traffic analysis attacks.

Physical Attack: Many nodes are statically deployed in the area and can easily be captured by attackers

- *Brute force attack*: The ability of resource storage as well as the computation of the sensor node are restricted and are most likely to suffer from brute force attack.

- *Clone node*: The hardware structure of several perceptual nodes is simple, and hence, can be easily copied by the attacker.
- *Impersonation*: certification in the distributed environment is very difficult for the perceptual node, allowing for malicious nodes to use a fake identity for wicked or collusion attacks.
- *Routing attack*: Data forwarding and relay exist in the process of perceptual data collection. Thus, intermediate nodes might attack the data during forwarding.
- *Denial of service (DoS) attack***:** Nodes can easily be trapped under DoS attack, given their finite processing ability.
- *Node privacy leak***:** The attacker can passively or actively steal sensitive information in the node.
- *Eavesdropping*: Because of the wireless characteristics of the RFID it becomes very easy for the attacker to break the confidential information like passwords or any other data.
- *Spoofing*: Spoofing is when an attacker broadcasts fake information to the RFID systems and makes it to assume its originality falsely which makes it appearing from the original source. This way attacker gets full access to the system making it vulnerable.
- *RF Jamming*: RFID tags can also be compromised by kind of a DoS attack in which communication through RF signals is disrupted with an excess of noise signals.

WSN includes a collection of nodes like sensor nodes, actuator nodes and so on. Hence there is a possibility of vulnerability. The operations performed in a wireless sensor network can be categorized under three categories:

- Attacks on secrecy and authentication
- Silent attacks on service integrity
- Attacks on network availability.

Network layer security issues

The function of the network layer is routing. Network layer consists of the Wireless Sensor Network (WSN) which transmits the data from the sensor to its destination. In wireless networks, nodes can move freely, they can join or leave the network at any time without any prior certification. This will make wireless networks to be more

- Malicious or vulnerable for the security distress. The following are attacks taking place in the network layer.
- *Hello flood attack*: Hello flood attack causes high traffic in channels by congesting the channel with a high number of useless messages unusually. Here a single malicious node sends a useless message then that message is replayed by the attacker to create a high traffic.
- *Homing*: In this attack, a search is made in the traffic for cluster heads and key managers which having the capability to shut down the entire network.
- *Selective forwarding*: In this, a compromised node sends few selective nodes instead of all the nodes. The selection of the nodes is based on the requirement of the attacker to achieve his malicious objective and thus such node does not forward packets of data.
- *Sybil*: In this attack, the attacker replicates a single node and then presents it with multiple identities to the other nodes.
- *Wormhole*: Wormhole attack causes relocation of bits of data from its original position. The relocation of data packet is carried out while passing bits of data over a link of low latency.
- *Acknowledgement flooding*: In this type of DoS attack, a malicious node sends false information to destined neighboring nodes by the help of these acknowledgements.
- *Sinkhole Attack*: It is a kind of attack in which the adversary makes the compromised node look attractive to the nearby nodes due to which all the data flow from any particular node is diverted towards the compromised node resulting in packets drop i.e. all the traffic is silenced while the system is fooled to believe that the data has been received on the other side.
- *Sleep Deprivation Attack*: Sleep Deprivation is the kind of attack which keeps the nodes awake, resulting in more battery consumption and as a result battery lifetime is minimized which causes the nodes to shut down.
- *Denial of Service (DOS) Attack*: The kind of attack in which the network is flooded with a useless lot of traffic by an attacker, resulting in a resource exhaustion of the targeted system due to which the network becomes unavailable to the users.
- *Malicious Code Injection*: This is a serious kind of attack in which an attacker compromises a node to inject malicious code into the system which could even result in a complete shutdown of the network or in the worst case; the attacker can get a full control of the network.
- *Man in the Middle Attack*: The target of the attack is the communication channel due to which the unauthorized party can monitor or control all the private communications between the two parties.

Application layer security issues

Application layer mainly includes the devices for effective decision making. Each of these has some vulnerability which leads to be an issue of the security of IoT. The attacker is likely to destroy privacy in the application layer by a known vulnerability (e.g., buffer overflow, cross site scripting, and SQL injection), error configuration (e.g., simple password), or improperly obtained higher permission access.

- *Privacy leak*: Given that the application of IoT is executed on common operating systems and hosting services, the attacker can easily steal user data by known vulnerabilities.
- *Social engineering*: A certain relationship exists among IoT users. However, attackers can easily analyze or obtain additional information that can be used for attacks by social engineering.
- *Malicious Code Injection*: An attacker can leverage the attack on the system from end-user with some

hacking techniques that allows the attacker to inject any kind of malicious code into the system to steal some kind of data from the user.

- *Denial of Service Attack*: DoS offers a smoke screen to carry out attacks to breach the defensive system and hence data privacy of the user, while deceiving the victim into believing that the actual attack is happening somewhere else.
- *Spear Phishing Attack*: It is an email spoofing attack in which victim, a high ranking person, is lured into opening the email through which the adversary gains access to the credentials of that victim and then by retrieves more sensitive information.
- *Sniffing Attack*: An attacker can force an attack on the system by introducing a sniffer application into the system, which could gain network information resulting in corruption of the system.

V. CONCLUSION

IoT is a big achievement in communication network. It should be considered as a part of future internet as everything is going to be connected in a network so that objects can interact with each other, but still there are lots of issues which are to be solved to make this a reality. In this study, we summarized an overview of IoT including its definition, architecture, attacks and challenges.

REFERENCES

[1] Kevin Ashton, That Internet of things thing, it can be accessed at: http://www.rfidjournal.com/articles/view?4986.
[2] Knud Lasse Lueth, " IOT basics: Getting Started with Internet of Things".
[3] Luigi Atzori, Antonio Iera, Giacomo Morabito, "The Internet of Things: A Survey", in Computer Networks, pp. 2787-2805.
[4] Gartner, Inc. It can be accessed at: http://www.gartner.com/newsroom/id/2905717.
[5] Mr. Ravi Uttarkar and Prof. Raj Kulkarni, "Internet of Things: Architecture and Security," in International Journal of Computer Application, Volume 3, Issue 4, 2014.
[6] W. Zhang, B. Qu, "Security Architecture of the Internet of Things Oriented to Perceptual Layer", in International Journal on Computer, Consumer and Control (IJ3C), Volume 2, No.2 (2013).
[7] Shashank Agrawal and Dario Vieira, A survey on Internet ofThings.
[8] Aaditya Jain, Bhuwnesh Sharma, Pawan Gupta, "INTERNET OF THINGS: ARCHITECTURE, SECURITY GOALS, AND CHALLENGES- A SURVEY" in International Journal of Innovative Research in Science and Engineering, Vol. No. 2, Issue 04, April 2016.
[9] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu,"Security of the Internet of Things: perspectives and challenges", Wireless Networks, 2014, vol. 20, no. 8, pp. 2481–2501.