International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8, Issue-1, May 2019

IoT: Security Challenges and Mitigations

Bhavana Vattikuntla, Santhya R

Abstract*: Nowadays, Internet of things (IoT) is one of the emerging domains which is growing exponentially. IoT is an idea that bridges the smart devices and let the devices to communicate with each other over the internet. IoT is an enormous system of associated gadgets – all of devices accumulate and share the information about how they are utilized and the situations in which they are working. IoT-based innovation will offer propelled dimensions of administrations and for all intents and purposes and it will change the manner in which individuals lead their day by day lives. IoT enhances machine-to-machine(M2M) communication that eliminates the need for human intervention. Smart homes, Smart Grids, Smart Cities, Earthquake detection, Healthcare, Smartphone detection, Radiation detection/hazardous gas detection, Water flow monitoring are some of the modern implementations in IoT. The future of IoT can only be assured if the security issues corresponding to IoT vulnerabilities and the mitigation techniques has been addressed. Since the IoT devices is been accessed remotely, there are many possibilities to flood the device and also results in many security issues. Hence it gives a path for the analysis of vulnerabilities in the IoT devices and evaluating the impact when the vulnerability is exploited. Based on the severity of the exploit, the mitigation techniques will be formulated. Many researchers have attempted to mention the security concerns specific to IoT layers and devices by implementing corresponding countermeasures. This paper presents a study of IoT security, IoT architecture, Security challenges, mitigation strategies for each layer of IoT, and the future work for IoT device security.

***Keywords*: CIA TRIAD, DDOS, DOS, IOT, SECURITY**

I. INTRODUCTION

IoT (Internet of Things) is an idea that bridges each and every smart devices and let the devices to communicate with each other over the internet. IoT is an enormous system of associated gadgets – all of which accumulate and share information about how they are utilized and the situations in which they are working. IoT-based innovation will offer propelled dimensions of administrations and for all intents and purposes will change the manner in which individuals lead their day by day lives. IoT enhances machine-to-machine(M2M) communication [1], [15] which eliminates the need for human intervention. Smart homes, Smart Grids, Smart Cities, Earthquake detection, Healthcare, Smartphone detection, Radiation detection/hazardous gas detection, Water flow monitoring are some of the modern implementations in IoT. Also the studies predict that more than 50 billion IoT devices will hit the market by 2050[1]. Utilization of the associated smart devices and the use of sensors are detonating and are changing to modify every aspect of our lives. Traditional enterprises are being changed just before our eyes in manners we never imaged. As there is great potential for connectivity, there is also great exposure for certain risks and vulnerabilities of the devices if not secured properly. Malicious users can easily exploit the loopholes and vulnerabilities if devices are not configured and secured properly. Since the devices directly affect the users personally, security demand will be a high requirement and there must be some legitimate scope to be defined in case of security framework with new guidelines and conventions that can constrain the conceivable dangers identified with scalability, accessibility, and security of IoT [2].

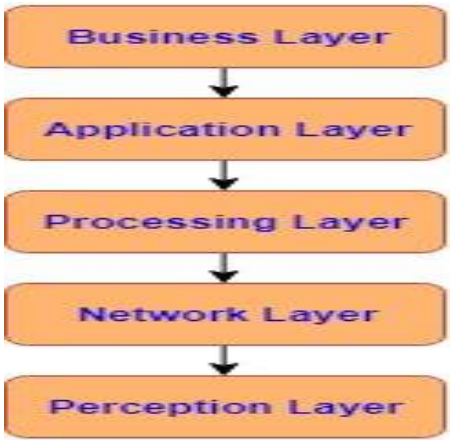
A. DoS and DDoS

A Denial-of-Service(DoS) attack is a unauthorized attempt to bombard a machine or network resource with traffic in order to intercept its normal operations. DoS attacks will generally function by flooding a targeted machine either temporarily or indefinitely by disrupting services with massive amount of requests until the usual traffic is unable to process, resulting in a denial of service to the legitimate users [9]. It is characterized by using a single source to launch the attack. A Distributed Denial of Service (DDoS) is a type of DoS attack that originates from various distributed sources. The attacker compromises some of the devices that belongs to a particular network also called Botnets. DDoS botnet refers to a group of devices that has been infected by malware or compromised by the malicious script and have come under the control of an attacker. It accomplishes tasks including sending spam, stealing data, Ransomware, etc., Devices can be captured either through unprotected system ports or by means of trojans or other malware, more often spread through spam, that would open secondary passages like open backdoors by which attackers could get in. When the devices are compromised, the controller — known as a bot herder — issues directions by means of IRC or different apparatuses. Also sometimes directions originate from a central server, however more frequently now botnets have an appropriated design i.e a distributed architecture that makes their controllers harder to find.

II. IoT ARCHITECTURE

IoT Architecture has been extended from three layer to five-layer architecture [1] [2] [3] [9]

Revised Manuscript Received on 30 May 2019.
***** Correspondence Author
Bhavana Vattikuntla*,CSE, Amrita Vishwa Vidyapeetham, Coimbatore, India.
Santhya R, TIFAC-CORE in Cyber Security, Amrita Vishwa Vidyapeetham, Coimbatore, India.



A. Perception Layer

Perception layer also known as "object" or "sensor" layer[2] is used to acquire data from sensors and actuators from the physical world. The purpose of this layer is to detect, collect and process information obtained and then transmits it to the Transport layer. It is capable of sensing other smart objects within the environment. This layer deals with different kinds of data sensors like RFID, barcodes, other sensor networks[5], etc.,

B. Network Layer

Network layer exchanges the sensor information from the perception layer to the processing layer and the other way around through systems, such as wireless, 3G, LAN, Bluetooth, RFID, and NFC[3],[9]. This layer aims to transmit data to a longer distance or to larger areas.

C. Processing Layer

Processing layer also known as the "middleware" layer, stores, analyzes and processes enormous amounts of data that come from the transport layer. It utilizes numerous advanced technologies such as databases, cloud computing, and big data processing modules. Upon processing the collected data, it takes automated decisions or actions and links it with the database for the storage of processed data. This layer is service-oriented that ensures the same levels of service across the connected devices in the entire environment.

D. Application Layer

The application layer aims at providing application level services to the customer. It provides a wide variety of practical applications such as smart home, smart cities, smartphone detection, etc.,

E. Business Layer

The main goal of this layer is to ensure users privacy i.e the CIA (Confidentiality, Integrity, Availability) Triad[1],[2].It takes care of the entire IoT system and also deals with business and profit models.

III. IoT SECURITY ISSUES

IoT needs to safeguard user's privacy and its ultimate goal is to preserve CIA (Confidentiality, Integrity, Availability) Triad as shown in the below Fig. 1.

A. Basic Security Feature Checks

1) The software image or version running on each IoT device needs to be authorized.

2) Every IoT device needs to be updated to the newer release version when a patch is released without consuming much of additional bandwidth.

3) Before sending or collecting any data, the IoT device needs to authorize itself.

4) Since IoT devices have limited memory computation and processing capabilities, firewalls are necessary to filter ingress and egress traffic, so that malicious packets cannot enter immediately and disrupt the whole network.

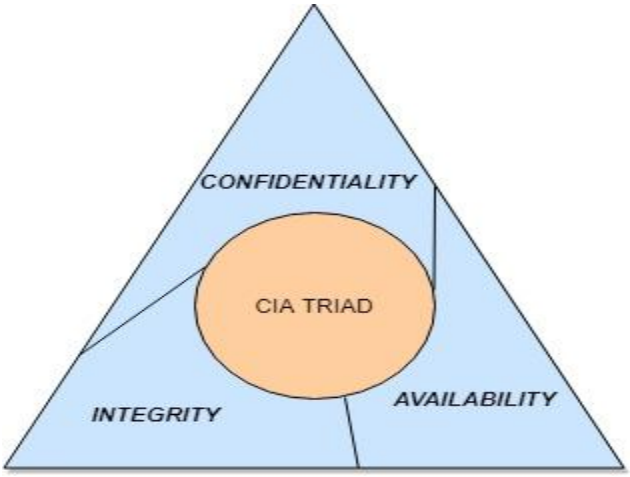


Fig. 1. CIA Traids

B. Confidentiality

It is one of the essential concept to guarantee that the information is secure and it can only accessible to authorized users. Confidentiality must ensure that the information is only accessible to the legitimate or authorized users. An IoT user can be a human, bot or honeypot which might belong to either an internal or external network. For instance, it is crucial to ensure that sensors don't uncover the gathered information to neighboring nodes. Additional confidentiality issue that also covers by which the information will be overseen and how it is managed. Data encryption is a typical method to guarantee confidentiality. User IDs and passwords establish a standard methodology; two-factor authentication is becoming the norm. Different alternatives incorporate biometric verification and security tokens, key fobs or soft tokens or session tokens.

C. Integrity

Integrity includes maintaining up the consistency, precision, and reliability of information over its whole life cycle. Amid the communication, data could be modified by the cybercriminals or could be disrupted by various other factors that are beyond human control including the crash of server or electromagnetic interference. Data Integrity aims to safeguard authorized information from the cybercriminals by means of some tracking methods, so that the data cannot be tampered or modified by unauthorized users without the threat is being filtered by the system. End-to-End security needs to be maintained in IoT communication. Other data checks might include CRC (Cyclic Redundancy Check) or even cryptographic checksums [12] to make sure that data is consistent throughout the communication.

Data Encryption is also a key factor that converts plain text to cipher text which provides an additional layer of security. Even after the placement of firewalls and other security protocols, security cannot be ensured at endpoints because of the poor computational capabilities of IoT nodes.

D. Availability

One of the primary goals of IoT Security is to provide data, devices, and services to authorized users uninterruptedly. All the services needs to be available in a timely fashion whenever the legitimate user's requests for information not only in normal conditions but also in a disastrous condition which prevents software conflicts. Positioning of firewalls and proxy servers is necessary in order to countermeasure DDoS attacks which deny the data availability to the end user which results in downtime and unreachability of network services. All timely system upgrades need to be taken care of periodically. Providing additional bandwidth and preventing bottleneck occurrence are also equally important for uninterrupted transmission. Serious consequences can be mitigated by providing Back-up devices and paths which correspond to redundancy, failover backup methods during disaster recovery plan [1].

IV. SECURITY CHALLENGES AT DIFFERENT LAYERS IN IOT

Each layer in the IoT device is susceptible to DDoS attacks, which makes the service, network or resource unavailable to the legitimate user. An attack can be either active or passive and it could have originated from external resources or from an internal network. An active attack interepts the service directly and it is capable of altering the information whereas a passive attack monitors and analyze the pattern with a hidden motive without disrupting the network and without altering the data. The frequency of the different types of DDoS as shown in Fig. 2.

A. Perception Layer

Since perception layer deals with signals mainly, various components and technologies like RFID, Sensors, Actuators, GPS comes into picture which needs to be handled carefully as they are more vulnerable to DDoS attacks because of their poor storage and computational powers. IoT sensor nodes are not only operated internally to the network but also in the outside environment. This way an attacker can gain access to the node and analyze confidential information which is known as Node Capture Attack[2]. Also an attacker is capable of adding a node with malicious content which can lead to denial of service by consuming the bandwidth and energy of the node ultimately leading to a DDoS attack. RF Jamming is a method to capture RFID tags and can be compromised wvith a kind of DoS attack. Radio Frequency jamming[3] is a technique to disrupt authorized wireless communications by a distorted electromagnetic interference or by increasing the signal to noise ratio. The attacker can capture the signal from an RFID tag and changes the data without any authorized access where a legitimate user cannot distinguish between the original tag and compromised tag, leading to Tag Cloning. The information flowing from tag to reader can be eavesdropped by the attacker to sniff confidential information such as passwords, keys, etc., Bandwidth and pulse denial leads to the jamming of the complete RF spectrum.

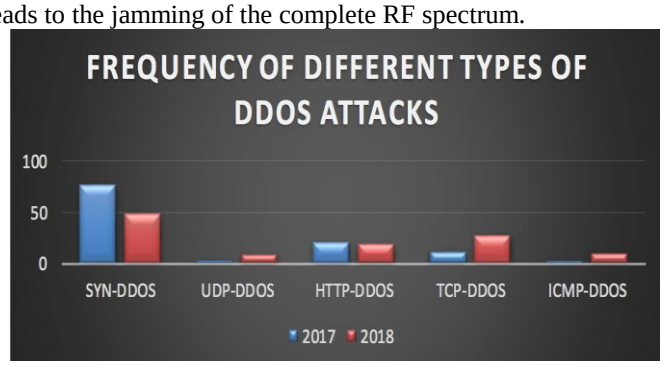


Fig. 2. Frequency of different types of DDoS Attacks

B. Network Layer

Network layer consists of WSN(Wireless sensor networks)[4],[14] which is vulnerable to Man-in-the-Middle(MITM) attack by eavesdropping the communication and acting like a proxy, DDoS attacks. Types of DDoS Attacks in the Network layer

1) Sinkhole Attack

Attacker compromises a node by injecting malicious code such that all the other nodes will send the traffic to this compromised node that results in DDoS attack by consuming bandwidth and energy[1].

2) Sleep Deprivation Attack

Nodes in WSN follow sleep routine formats to save its battery life, since they don't have good power storage capacity. This attack keeps all the nodes awake by consuming more battery which results in reduced battery lifetime, which ultimately leading to the shutdown of all the nodes.

3) Flooding Attacks

Ping by Death is a kind of DDoS attack which continuously floods malformed ICMP packets or by continuously sending ICMP Echo Request Messages consuming all the available bandwidth. DNS Flood, UDP Flood are other Flooding attacks[3].

4) Protocol Exploitation Flooding Attacks

Attacker compromises certain precise features of a protocol to make a system unresponsive for the legitimate traffic. SYN Flood is a form of DDOS attack in which a system sends continuous SYN requests by consuming all the available bandwidth and server resources. TCP SYN-ACK flood, ACK PUSH flood are other examples of protocol Exploitation Flooding attacks.

5) Amplification-based Flooding Attacks

Volumetric attacks use a form of amplification to create an enormous amount of traffic from botnets, a group of compromised devices in the network controlled by the malicious attacker or bot herder.

6) DNS Amplification

This is a formatted attack in which a request is sent to a DNS server with a spoofed IP address. The attacker frames the request from the DNS server in such a way that the original IP address receives a large amount of data which is difficult to process resulting in the reduced process and memory computational capabilities.

C. Middle-ware and Application Layer

Application layer attacks goal is to exhaust the resources of the victim. It's very difficult to mitigate and defend application layer attacks. Attacker target is on the web server where web pages are generated post response to HTTP requests. Multi-vector DDoS attacks are most common where the application layer and other layers are targeted at the same time. Types of DDoS in Application Layer are as follows

1) HTTP Flood

It's a type of volumetric attack where the attacker sends HTTP requests with the help of botnets, also known as the Zombie army. The botnets are controlled by bot herder by creating backdoors like Trojan horses. This attack doesn't need a sophisticated bandwidth as HTTP GET or HTTP POST requests are simple to create whereas generating HTTP response includes complex processing on the server side.

2) Protocol Attacks

Protocol attacks, commonly known as state-exhaustion attacks[3] consume the bandwidth available for web application servers like firewalls and load balancers by exhausting state table capacity.

3) Malicious Code Injection

In this attack, the attacker injects a malformed code or script into the system by creating backdoors and by exploiting loopholes in the system. This makes the web application more vulnerable to this kind of attack. In cross-site scripting attacks, the hacker makes use of a web application that is injected by malicious code and sends it to the user in the form of browserside script.

V. MITIGATION OF DDOS ATTACK IN EACH LAYER

A. Basic checks to secure IoT infrastructure

1) Upgrade software versions regularly and change default passwords

If patches[10] are not released properly for previous software versions or images then there is a chance of vulnerability for Smurf attack[3], a method which attacks previously exploit DoS attack by using broadcast address by sending spoofed IP packets. The system needs to be upgraded to the latest versions. Default Passwords need to be changed as they are vulnerable to a brute force attack. Also if default passwords cannot be changed then the devices should not be implemented in IoT infrastructure as Mirai Botnet attacks, the latest malware DDoS attack happens because the factory default usernames and passwords are not changed which affects thousands of devices belonging to a particular network.

2) Implementation of Firewalls and ACLs

Just the authorization and authentication mechanisms alone cannot prevent the IoT environment from being attacked. Firewalls and Router Access Control Lists(ACLS) needs to be implemented properly for an additional layer of security. Firewalls filter unnecessary traffic from entering into the network thereby preventing unauthorized access. It can be implemented in both software and hardware. ACLs filter ingress and egress traffic based on predefined set of rules or on control plane policies.

3) Vendor Reliability and reinforcement of web application security

Before implementing third-party devices in IoT infrastructure, there is a need for service level agreements between vendors and the customers so that the levels of service and quality of service defined by the vendor cannot be compromised later. A VPN implementation can tunnel or mask traffic in a secured channel that provides end to end authentication. CMS Plugins and other software components can be included to reduce vulnerabilities and loopholes in the network.

B. Perception Layer

Cryptographic Hash algorithms and Encryption techniques[12] can greatly enhance end-to-end security in the perception layer. Authorization and Authentication can be preserved by techniques like digital signatures and digital certificates. Data Privacy can be guaranteed by symmetric and asymmetric algorithms such as DSA, RSA, AES, DES, etc., To safeguard the identification and location of the device K-Anonymity approach can be used. MD5, SHA Hash algorithms eliminates the risk of collision attack, side-channel attack[8], brute force attack, etc.. An RFID tag can be compromised by sniffing EPC(Electronic Product Key)[7] and it can be added to another tag, a technique called Tag cloning. Kill Command Abuse or an automated kill command[11] from RFID reader can be sent to the RFID tag for restricting unauthorized access to the tag. Implementing fingerprinting RFID tags, a latest methodology which involves enrolling and verifying process can enhance security mechanism for RFID tags.

C. Network Layer

The communication channel can be of both wired and wireless in Network Layer. This makes the layer more susceptible to eavesdropping and passive monitoring. The most common attacks are MITM and DDoS attacks by using malformed botnets. The implementation of firewalls and Access Control Lists can prevent this layer from being attacked. ACLs can define data plane and control plane policy routing mechanisms and filters unnecessary traffic out of the network layer.

If DDoS attack is severe and persistent, then Blackhole Routing is a method that helps in routing traffic into a null route unless a packet is not filtered without any restriction. Rate Limiting limits the number of packets arriving the server depending on the proposed window size and server capabilities in order to mitigate DDoS attacks. Peer-to-Peer encryption should be assured as traffic is routed through multiple paths to long destinations. Intrusion Detection System(IDS) is a monitoring system that monitors network traffic and alerts the system if any threat is identified whereas Intrusion Prevention System(IPS)[13], a control system prevents or blocks unauthorized traffic entering the network. Data Integrity is preserved by IPS.

D. Middle-ware and Application Layer

Application layer attacks are the most prevalent and common phase of attack. Cloud computing and virtualization[1] are two main technologies used in this layer.

Insider threats are most common in these fields. Cloud computing offers services such as SAAS, PAAS, IAAS which mainly provide platform-based and infrastructure-based services. The attack in these areas can have the worst impact of damaging infrastructure as a whole incurring heavy loses to business organizations. As cloud demands on service providence to its users, there should be enough resources and bandwidth to address requests from clients. Availability in the CIA triad always needs to be attained for cloud users. Virtualization is an absolute necessity for cloud computing for rapid self-provisioning. The hypervisor is a control mechanism in virtualization that has control and access to all hardware resources. An insider or an attacker can run the malicious script on this hypervisor to gain confidential information from the host device on top of which this hypervisor is running. By modifying core functionalities and by utilizing the side-channel resistant algorithms, sidechannel attacks can be mitigated. DNS redirection or DNS routing is a diversion technique where attack traffic is redirected in order to reduce the impact of the DDoS attack. Web Application Firewall(WAF), a tool placed in between the internet and the original server acts as a reverse proxy protecting the original server from malformed traffic. Anycast network diffusion scatters and directs traffic to multiple distributed servers within the network where traffic can be captured and managed effectively reducing the effect of DDoS attacks.

VI. CONCLUSION AND FUTURE WORK

The IoT framework are vulnerable to attacks at every layer and there are number security challenges and requirements need to be addressed. The IoT has a greater possibility to change the way we live today. But, the foremost concern in realization of completely smart frameworks is security. If security concerns like privacy, confidentiality, authentication, access control, end-to-end security, trust management, global policies and standards are addressed completely, we can witness the transformation of everything to IoT in the near future. Since the IoT devices is been accessed remotely, there are many possibilities to flood the device and also results in many security issues. Hence it gives a path for the analysis of vulnerabilities in the IoT devices and evaluating the impact when the vulnerability is exploited. Based on the consequences of the exploit, the mitigation techniques will be defined. The future of IoT can only be assured if the security issues corresponding to IoT vulnerabilities and the mitigation strategies for the smart devices are defined. Many researchers have attempted to address the security concerns specific to IoT layers and devices by implementing corresponding mitigation strategies.

REFERENCES

1. Farooq, Muhammad Umar, et al. "A critical analysis on the security concerns of internet of things (IoT)." International Journal of Computer Applications 111.7 (2015).
2. Mahmoud, Rwan, et al. "Internet of things (IoT) security: Current status, challenges and prospective measures." 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE, 2015.
3. Gandhi, Anju Bhandari. "SECURITY AND DDOS MECHANISMS IN INTERNET OF THINGS." International Journal of Advanced Research in Computer Science 8.9 (2017).
4. Abomhara, Mohamed, and Geir M. Køien. "Security and privacy in the Internet of Things: Current status and open issues." 2014 international conference on privacy and security in mobile systems (PRISMS). IEEE, 2014.
5. Singh, Dhananjay, Gaurav Tripathi, and Antonio J. Jara. "A survey of Internet-ofThings: Future vision, architecture, challenges and services." 2014 IEEE World Forum on Internet of Things (WF-IoT). IEEE, 2014.
6. Weber, Rolf H. "Internet of Things–New security and privacy challenges." Computer law & security review 26.1 (2010): 23-30.
7. Roman, Rodrigo, Pablo Najera, and Javier Lopez. "Securing the internet of things." Computer 9 (2011): 51-58.
8. Zhao, Kai, and Lina Ge. "A survey on the internet of things security." 2013 Ninth international conference on computational intelligence and security. IEEE, 2013.
9. Sonar, Krushang, and Hardik Upadhyay. "A survey: DDOS attack on Internet of Things." International Journal of Engineering Research and Development 10.11 (2014): 58-63.
10. Leo, Marco, et al. "A federated architecture approach for Internet of Things security." 2014 Euro Med Telco Conference (EMTC). IEEE, 2014.
11. Tagra, Deepak, Musfiq Rahman, and Srinivas Sampalli. "Technique for preventing DoS attacks on RFID systems." SoftCOM 2010, 18th International Conference on Software, Telecommunications and Computer Networks. IEEE, 2010.
12. Suo, Hui, et al. "Security in the internet of things: a review." 2012 international conference on computer science and electronics engineering. Vol. 3. IEEE, 2012.
13. Park, PyungKoo, et al. "An effective defense mechanism against DoS/DDoS attacks in flow-based routers." Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia. ACM, 2010.
14. Doddapaneni, Krishna, and Arindam Ghosh. "Analysis of Denial-of-Service attacks on Wireless Sensor Networks using simulation." IT Security for the Next Generation-European Cup 2011 (2011).
15. Khan, Rafiullah, et al. "Future internet: the internet of things architecture, possible applications and key challenges." 2012 10th international conference on frontiers of information technology. IEEE, 2012.