Analysis of Challenges and Attacks of Internet of Things

Gudapati Ramyasri, Shaik. Jakeer Hussain

Abstract: ***Internet of things plays the major innovative role in the enhancement and optimisation of habitual behaviour by the collaborative usage of smart objects and smart sensors. The main aim of IoT is to provide security for the effective and efficient interconnection of different entities. This paper mainly determines what are the different security and privacy and trust challenges and attacks faced by the IoT. These challenges are mainly determined at different layers based on the enhancing technologies, updated architectures and future scope.***

Keywords: Internet of Things, Attacks, Challenges, Security, Privacy

I. INTRODUCTION

The presence of internet of things plays its major concern in the present-day society in which everything is getting connected to the internet. Present days we are in a such a state that we cant capture difference between the actions done by the humans and devices.[1] Devices become part of humans life In this each device is connected to different other devices and takes over the actions without any human interference. The devices not only transmits and retrieves the data, it stores the data and takes the actions based on the data.[2] In future everything is going to get connected through internet. The transmission of data takes place at the rate of 40zettabytes per sec. For these security, privacy and trust plays the major role in the storage and transmission of data to different devices.[1][3] IoT not only has the same security issues as sensor networks, mobile communications networks and the Internet, but also has its specialties such as privacy issues, different authentication and access control network configuration issues, information storage and management and so on. Data and privacy protection is one of the application challenges of IoT This paper mainly presents what are different types of attacks based on the architecture, phase, component and applications[5]. In this sectorisation of attacks were done at different layers.

II. STRUCTURE OF IOT SYSTEMS

IoT ought to make certain the safety of all layers. Similarly, IoT safety need to also encompass the security of entire gadget crossing the link layer, transportation layer, network layer and alertness layer. The maximum fundamental stage is the hyperlink layer (also referred to as recognition layer), which collects all kinds of facts through physical system. The important thing thing in this layer is sensors for taking pictures and representing the physical global in the digital international. The next level is community & shipping layer which is accountable for the dependable transmission of statistics from perceptual layer, preliminary processing of information, class and polymerization. [5] The application layer is the topmost and terminal stage. Utility layer gives the customised offerings according to the needs of the customers. Security in IoT is provided in four dimensions

A. Applications
B. Phase
C. Architecture
D. components

III. SECURITY ATTACKS

A. Attacks Based on Applications

i. **Denial-of-Service:** IoT is mainly susceptible to different attacks such as channel jamming, extraction of the bandwidth width and resources. The adversary privileged insider may disorder the network.
ii. **Controlling**: The control of the entities can be gained by the active attackers based on the provision of services and data management provided by that particular entity.
iii. **Eavesdropping**: A passive attack in which the malicious attacker can gather information and also may gain authority on that particular entity and infrastructure [5]
iv. **Physical Damage:** The attackers may exploit the easy access of IoT applications and entities. Attackers with less knowledge may cause physical damage to the entity and utilize it.
v. **Node Capture:** Easy access may also be dangerous for extraction of stored data and extraction of information from capturing entities.

B. Attacks Based on Phase

IoT attacks are done at different phases of authentication, sovereignty, Data leakage or breach.

a) **Data leakage:** Data leakage can be done intentionally or unintentionally by authorised or malicious involving internal or external, hardware or software. The most dissatisfied employees send the data which is unauthorised to the unintended destination. Data leakage is mostly found in the cloud computing as most of the transactions between different tenants will take place in the cloud itself [7][5].
b) **Sovereignty:**Data sovereignty refers to the storage of data after conversion in to digital form under the laws of country as everyone's concern is to enforce privacy.

Revised Manuscript Received on July 05, 2019.
Gudapati Ramyasri, Department of ECE, VFSTR, VADLAMUDI, GUNTUR, India
Shaik.Jakeer Hussain, Department of ECE, VFSTR, VADLAMUDI, GUNTUR, India

c) **Loss of data:** The loss of data due to natural disasters or failure of software or hardware differs from the data leakage which is an intended attack.

d) **Authentication:**The reception of the data should be from the intended users. As the data can be forged from the attackers, authorisation of the perceived data from the intended receiver must be verified.

e) **Availability:** Distributed denial of service(DDOS) is nothing but an overload condition caused by multiple amount attackers which makes DCs unavailable to the intended users. This is mainly given in four ways.

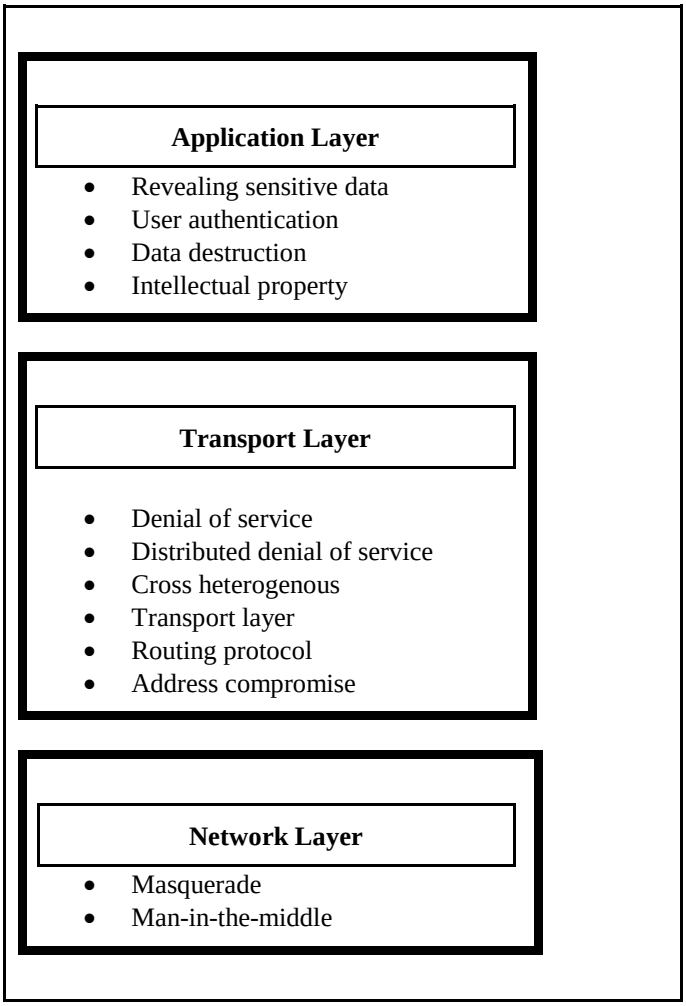
i. Flooding by attackers malicious packets
ii. Flooding by more number of legitimate users
iii. Flooding by spoofing attackers personal data like IP address
iv. Flooding by aggressive number of requests from the legitimates

f) **Sensitive data modification:** The legitimate users modify the sensitive data and sends malicious data during transmission. These modifications are mainly done in Three ways.

i. Time modification.
ii. Packet sequence modification.
iii. Data content modification

C.*Attacks* Based on Architecture

The attacks on IoT based on the applications are mainly given at different layers of Application layer, Network layer, Transport Layer, Link Layer. Fig shows the diagram representing all possible threads at different layers.[4]



Attacks based on architecture can be given by

1) Sinkhole Attack

Sinkhole attack mainly occurs on the nodes that are not connected to the network for long period of time and gains the information of surrounding nodes. These leads to some attacks like forwarding, modification and fabrication[3].

2) External Attack

Data from the user is stored in the cloud with faith irrespective of the sensitive and unsensitive data. So, that particular organisational provider may use that data for malicious purposes or can share that data with others.

3) Wormhole Attack

Warmhole attack mainly occurs in the adhoc network formed either by wired or wireless connection using static or dynamic formation of nodes. In this malicious node captures the data to another node and retransmits again which results in failure of authentication.

4) Selective forwarding Attack

Malicious node will filter some of the future used selective packets and throughs them out. It allows all the remaining packets and interrupt only selective packets.

5) Sewage pool Attack

In this attack, one malicious node attracts all the data in a particular region and modifies the base station. This results in the reduction in the effective operation of selective forwarding attack.

6) Witch Attack

Witch attack mainly takes place with the node failure which results in the loss of data by the use of factual link for future communication.

7) Overflow Attacks

a. HELLO flood attackswill effect every device as everything will transmit HELLO messages. As malicious node frequency level is greater, it effects all the nearby nodes.

b. Distributed denial of service (DDoS) sends multiple amounts of malicious requests and results in the huge traffic. As the legitimate responds based on the authorisation, the legitimate doesn't respond to any request.

c. Flash crowd mainly occurs with sudden change and increase in the traffic of page due to less bandwidth. By flash crowds pages get disappeared with huge amount of traffic.

d. Botnet attacks mainly occurs when multiple amount of computers are interconnected and control authority given to malicious party. In this overloading and prevention of services

were done based on the continuous fake calls

8) Addressing all things in IoT&IP spoof attack

IP Spoof attack for virtual machine acts as one of major challenging task for security. Malicious user will trace the IP address of machines and attack the users data based on the IP address of machine.In IP spoof attack, the attacker continuously sends the requests and doesn't care about the responses that we are getting. It is very difficult to trace the source of the attack, as each request is sent with the different addresses. Ip spoof attacks are mainly of three types.

a. Hiding attack
b. Reflection attack
c. Impersonation attack

9) Goodput

Goodput mainly represents the ratio of amount of transmission of packets and total amount of delivery time. Goodput. Delivery time includes interpacket timegaps, overhead in transmission delay, packet queuing &retransmissiontime, delayed acknowledge, and processing delay

10) Data centres (DCs)

Data centres mainly acts as a centralised authority for the physical or virtual storage of data, management and organisation of business. Each Dc will create and handle business or organisational data. Each DC may have multiple amount of hosts, in which each host will handle each component.

11) Confidentiality

It refers to the representation of the proof during the transmission of data to the intended clients.

12) Security Attacks

a. Physical securityfailure causes multiple threads. As the hardware must be in active state all the time
b. Software securityattacks will effect legitimate users based on Application programme interface and the software interfaces failure.
c. Network security gets effected by Dos and DDOS attacks, which results in the failure of communication.

13) Eavesdropping

Man-in-the-middle is a type of eavesdropping attack in which two parties believe that they both are getting communicated with each otherbut interprets communication between them.

14) Replay attack

Replay attack mainly occurs with the retransmission of previous transmitted messages to gain access to the unauthorised resources.

15) Back door

Back door attacks are mainly done by the usage of external resources like modems.

16) Sybil attack

In Sybit attack, the malicious user tries to gain the identity as privileged user from the honest user by the creation of multipe amount fake identities. After it satisfies the honest user it gets unauthorised privilege for the attack.

17) Cloud Attacks

a. Byzantine failure mainly degrades the active performance of the cloud
b. Data protection is a difficult task to check the data transmission through the cloud
c. Data deletion is incomplete. Even though data is deleted in main stored location, the duplicate copies stored in the nearby replica areas remains undeleted.

D.ATTACKS BASED ON COMPONENTS

In Internet of things everything is getting connected to the internet. These things will transfer not only the heterogeneous data but also results in the attacks in early state itself. It is even mandatory to distinguish between things and humans.

Attacks based on components cane be given by three sectors.

i. Storage

In data storage attacks, fabrication or modification of data came done at local storage space and data center.

ii. Terminals

Worms, Virus, UIM or SIM duplication, reveal of sensitive data is done at different terminals of communication devices, PD, sensors, gateways etc.

iii. End users

Attacks like intrusion compromise and impersonation be done at different end users of man and machine.

IV. CONCLUSION

In this analysis, major focus is on security, privacy and trust of IoT. The analysis was mainly done based on the sectorisation of IoT four different layers of application layer, Network layer, transport layer and link layer and listed out different types of attacks at different phases, different applications, architecture and components.

REFERENCES

1. R. Hussain and I. Abdullah, "Review of Different Encryption and Decryption Techniques Used for Security and Privacy of IoT in Different Applications," *2018 IEEE International Conference on Smart Energy Grid Engineering (SEGE)*, Oshawa, ON, 2018, pp. 293-297.
2. C. Liu, Y. Zhang and H. Zhang, "A Novel Approach to IoT Security Based on Immunology," *2013 Ninth International Conference on Computational Intelligence and Security*, Leshan, 2013, pp. 771-775.
3. Safi, Amirhossein. "Improving the Security of Internet of Things Using Encryption Algorithms." *World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering* 11.5 (2017): 546-549.
4. Schmitt, Corinna, et al. "Two-way authentication for the internet-of-things." *Internet of Things: Novel Advances and Envisioned Applications*. Springer, Cham, 2017. 27-56.
5. S. L. Keoh, S. S. Kumar and H. Tschofenig, "Securing the Internet of Things: A Standardization Perspective," in *IEEE Internet of Things Journal*, vol. 1, no. 3, pp. 265-275, June 2014.
6. S. Raza, H. Shafagh, K. Hewage, R. Hummen and T. Voigt, "Lithe: Lightweight Secure CoAP for the Internet of Things," in *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3711-3720, Oct. 2013.
7. R. Fantacci, T. Pecorella, R. Viti and C. Carlini, "A network architecture solution for efficient IOT WSN backhauling: challenges and opportunities," in *IEEE Wireless Communications*, vol. 21, no. 4, pp. 113-119, August 2014.