International Interdisciplinary Virtual Conference on
'Recent Advancements in Computer Science, Management and Information Technology'
International Journal of Scientific Research in Computer Science,
Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Review of Attacks on Physical Objects and Their Counter measures in WSN of IoT Framework

C. R. Mankar[1], Dr. Prof. V. M. Patil[2], G. P. Gawali[3]

[1]Research Scholar, [2]Research Guide, [3]Assistant Professor & Head

[1,2]Department of Computer Science, Shri Shivaji College, Akola, Maharashtra, India

[3]Department of Computer Science, R.A. College, Maharashtra, India

ABSTRACT

As the number of IoT applications is increasing day by day, the Security of the physical objects at different layers of IoT framework is a crucial issue. Physical objects like Smart Wearable devices, Smart Home Applications, etc. are sharing information like personal data, across the network, attacks on security to the physical objects is a main aspect of this research paper.

This paper represents the different attacks on the physical objects throughout the framework that are being observed, and the countermeasures needed for them to have secure physical objects.

Keywords: IoT: Internet of Things, WSN: Wireless Sensor Network, Wi-Fi, RFID, NFC

I. INTRODUCTION

Internet of Things is a heterogeneous network of Physical objects which are connecting various devices via different media to internet and connected together for communication and sharing information across the network.

In Internet of Things, the physical objects are connected and embedded in systems to act smart and share data across a network. The embedded systems are connected through different techniques like Wi-Fi, Bluetooth, etc. with a limited number of resources like bandwidth, power source, and ability to process the gathered data and share across the network to achieve a particular goal.

The term Internet of Things (IoT) refers to be:

IoT= Sensors + Networks + Data + Services.

The IOT technology works apart in aspect of time and place. IoT is capable of being implemented across the world and embedded systems are designed such that they can work with limited amounts of resources like power, storage, etc. in real-time.

II. IOT FRAMEWORK

There is no uniform framework for IoT, it depends upon the requirement for the project how many layers to be in the framework, general IoT framework has three layers, as shown in fig.1 [1]:

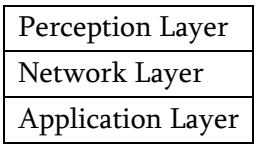

fig.1 three tier Architecture of IoT

Many researchers have analyzed these layers to have many layers in between them. The perception layer is the layer where sensor work which is most exposed to the physical world and is of importance and prone to attacks from intruders. The basic functionality of this layer is to collecting data from connected sensors and share it securely. From various studies done on this layer, the communication and sharing of data is done by using the technologies like Bluetooth, RFID, NFC, etc. [1-4]

The network layer is the layer at the core and is responsible for transmission of data, ensuring delivering the data to the right destination and flowing the data through various routers. Various technologies like IPV4/IPV6 are used for addressing devices with high effort.[1-4]

The application layer is the topmost layer in the framework, developed to provide service and present the data to the user according to the need. It provides the facility like a dashboard, representation of the data, and handling of the data.[1-4]

This framework is enhanced into five layers as in shown following diagram:

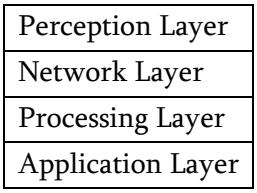

Fig.2 Enhanced IoT Architecture

By some researchers, the Processing layer is added in between the network layer and application layer to provide the functionality of computing and processing the received data. This layer is also responsible for the storage of data, varying to the devices being used.

III. ATTACKS ON PHYSICAL OBJECTS IN WSN OF IOT FRAMEWORK

The attacks are categorized into active attacks and passive attacks. [14]

Active attacks: These types of attacks are done to affect the performance of the system/network as well as to manipulate the data received/transported through the network.

Passive attacks: In these types of attacks the data is observed and monitored, and analysis of data traffic is done, here data is not damaged. [14]

Some of the Active attacks which are mainly seen are as follows:

- Distributed Denial of Service(DDoS): here the attacker introduces malicious nodes in the system to affect the services, either to change the data and then transmit the altered data on the network.[8][14]
- Jamming: in this type of attack the attacker gets control over the data transmission and prevents the data from transmission either from the system or to the system. Here the data packets are stopped from being transmitted.[14]
- Physical node attack: here the attacker physically damages the physical objects to stop the system from working. Here the physical objects can suffer permanent damage. [14]
- Node Tampering: here the attacker captures the physical object and gets control over it and modifies the services. [14]
- Spoofed Routing Information: the working of the network is affected here by spoofing.[14]

Some of the Passive attacks are as follows:

- Eavesdropping: here the attacker observes the data generated and transmitted over the network, where the data is not damaged physically but the protocols for privacy are violated. [12][14]
- Analyzing Data Traffic: here the attacker observes the data patterns that are being transmitted.[12][14]
- Homing Attack: here the attacker aims to find the resources of the network, and get access to the system for the active attacks.[12][14]
- Traffic Analysis: Monitoring the network this attack can be prevented from the pattern disclosure.[14]

IV. COUNTERMEASURES FOR ATTACKS IN WSN OF IOT

- DDoS: these types of attacks can have countermeasures by providing encryption algorithms, to stop the availability of resources to the attacker.[15]
- Jamming: these attacks can be overcome by splitting the network spectrum, to have a smooth data transmission.[15]
- Physical nodes attack: Tamper proofing is the solution to these attacks which prevents the system from having damaged physical objects.[15]
- Node Tampering: Having an efficient key distribution mechanism that keeps on changing the distributed key frequently, to prevent tampering with the node. [15]
- Homing Attack: Having a novel encryption technique, to prevent the network's resources. [15]
- Spoofed Routing Information: The MAC authentication can prevent the system from this type of attack.
- Authentication: A good authentication mechanism to strengthen the system from infringements.[16]

V. CONCLUSION

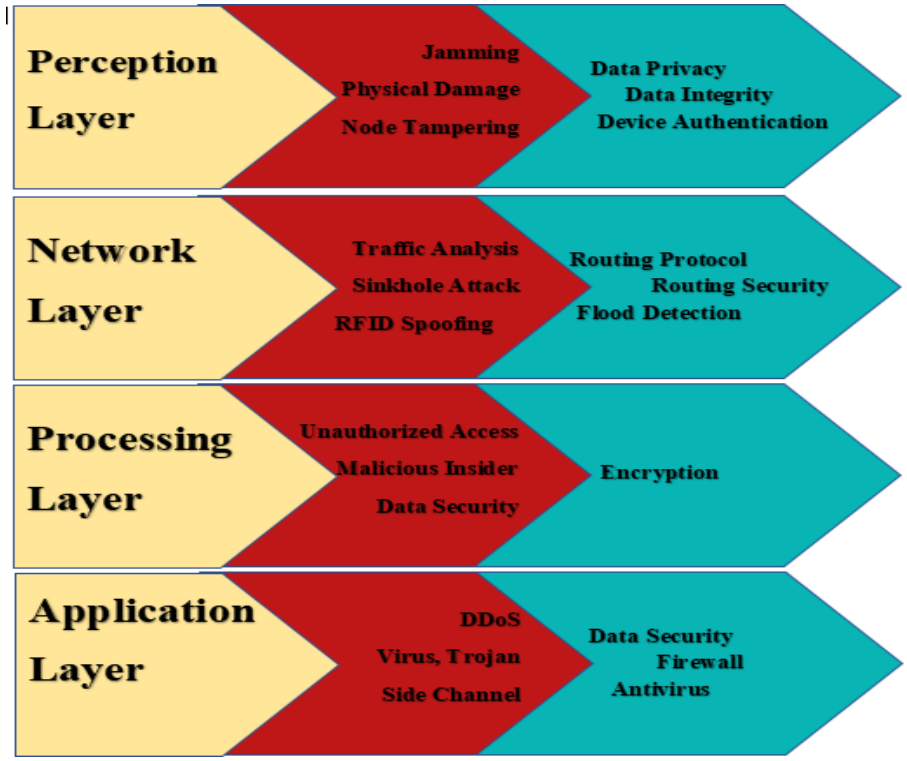

Fig. 3 Attacks in IOT and Countermeasures [2]

Paper discusses different attacks in IoT at various Layers, with effective Countermeasures to give clear view to the researchers to identify different attacks and provide countermeasures in their security mechanisms. The active attacks like DDOS, Jamming, Physical Nodes, Node Tampering, Spoofed routing and passive attacks like Eaves-Dropping, Analyzing Data Traffic can be effectively countered by given countermeasures. Using Encryption techniques at various layers of framework, can be an effective countermeasure for the attacks which affect Security, Privacy, and Integrity of the data.

VI. REFERENCES

[1]. Q. Jing, et al. Security of the Internet of Things: perspectives and challenges. Wireless Network 20, 2481–2501, 2014.

[2]. K. Y. Najmi, et al. A survey on threats and countermeasures in IoT to achieve users confidentiality and reliability, Materials Today: Proceedings, 2021

[3]. Lan Li, Study on Security Architecture in the Internet of Things, 1ntemational Conference on Measurement, Information and Control (MIC) 2012

[4]. D. Singh, et. al., Security Issues In different Layers of IoT And Their Possible Mitigation, IJSTR, VOLUME 9, ISSUE 04, APRIL 2020

[5]. A. Munshi, et al. DDOS Attack on IoT Devices, ICCAIS, 2020

[6]. L. Liang, et al. A Denial of Service Attack Method for an IoT System. ITNE 360-364, 2016

[7]. R. Ibrahim, et al. DDoS Attack Prevention for Internet of Thing Devices Using Ethereum Blockchain Technology, Sensor, 2022

[8]. S.B. Gopal, et al. Mitigating DoS attacks in IoT using Supervised and Unsupervised Algorithms-A Survey, IOP Conf. Ser.: Mater. Sci. Eng. 1055, 2021

[9]. Jeyakumar, et al. Fake Sensor Detection, and Secure Data Transmission Based on Predictive Parser in WSNs. Wireless Personal Communications,110, 2020

[10]. Md. Uddin, et al. A survey on the adoption of blockchain in IoT: challenges and solutions, Blockchain: Research and Applications, 2021

[11]. J. Deogirikar, el at. Security attacks in IoT: A survey. I-SMAC 32-37, 2017

[12]. A. Mohan, Survey Paper on IoT attacks and its prevention mechanisms, Information Management and Computer Science. 3. 38-41. 2020

[13]. R. Navas, et al. Physical resilience to insider attacks in IoT networks: Independent cryptographically secure sequences for DSSS anti-jamming, Computer Networks, Volume 1887, 2021

[14]. M. Keerthika, et al. Wireless Sensor Networks: Active and Passive attacks – Vulnerabilities and Countermeasures, Global Transitions Proceedings, Volume 2, 2021

[15]. X. Yao, et al. Security and privacy issues of physical objects in the IoT: Challenges and opportunities, Digital Communications and Networks, 2020

[16]. A. Mohammad, et al. User Authentication and Authorization Framework in IoT Protocols, MDPI Computers, 2022