INTERNET OF THINGS: LAYERED CLASSIFICATION OF SECURITY ATTACKS

K.Kowsalyadevi, N.V.Balaji*

Abstract

The Internet of Things (IoT) is sole like today's better prominent and current research topics. It's a novel system in which physical objects are seamlessly integrated in the networks in order to deliver progressive and intelligent services to humans. People's use of the internet and smart phones has increased dramatically as a result of these developments. IoT applications are eventually introduced. Equipment in the Internet of Things (IoT) are resource-constrained. As a decision, it is susceptible to a variety of intrusion and malfunctions, obliterating all the benefits of IoT applications. As a result, it's critical to think about IoT protection. The current research examines multiple IoT attacks and identifies the most significant ones.

Keywords: Internet of Things (IoT), Intrusion, Malfunctions, Wireless networks, IoT Attacks.

I. INTRODUCTION

Internet of Things (IoT) as a term was firstly coined in 1999 by Kevin Ashton [1]. It represents a network of devices that has the ability to connect and provide communication for billions of things simultaneously. This kind of network does not require expensive components but can be made out of cheap sensors [2] and interconnected objects, which collect information from the environment and enable the improvements in the people's life. The Internet of Things is the next step in the path for the fourth industrial revolution, where the Internet is extended to include more of the physical world, introducing both more intelligence to everyday objects and hence there will be more control over the physical world. The I in IoT[3] refer to the universal interconnectivity between all perceivable objects, including the traditional computing objects such as computers and smart phones, and the new generation of smart objects. The T in IoT enabled by sensors, actuators, and all embedded computers into everyday objects, from toys and wearable to home appliances, manufacturing equipment, vehicles and up to buildings, power grids and the entire urban city.

Nowadays, IoT is implemented in many domains (Fig.1) like transport [4], farming, primary-care and power manufacturing and dispensation due to the fact that it makes the life easier aside by the use of smart devices everywhere in the day-to-day works [2]. Given the above facts, it is natural to assume that IoT plays the important part in the daily lives which is why it is predicted [3] that IoT devices will reach the usage of 28.1 billion by 2020 thus making the increase for about 30 times of that in 2009 [3].

Fig. 1. Internet of Things Applications

II. TYPES OF ATTACKS

2.1. Passive Attacks

A Passive attack attempts to learn or make use of information from the system but does not affect system resources. All methods can be used to detect it. The reason for

Department of Computer Science,
Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
*Corresponding Author

this is that the attackers [5] do not emit any radio signals. Since the invention of wireless, Wireless networks are further vulnerable to these attacks, such as shown in Fig.2 Eavesdropping, Node Destruction, Node outage, etc…because connections are easier to tap, a simple task of listening to wireless communication sensor nodes.

2.1.1 Eavesdropping

Communication lines may be tapped to listen the classified info. As a result of the ease with these wireless connections can be tapped, wireless networks [6] are also vulnerable to previous intrusions. Since, Wireless Sensor Networks use precise-space communications, an intruder may do close enough to eavesdrop on useful information. Since signals are transmitted over shorter distances, wireless technologies are used. Interception [14] of messages sent over WSNs could disclose the group of useful info: cluster heads, gateways, key delivery centers, and other nodes' physical locations; message diagnose, time space, and other areas; and around everything that isn't converted.

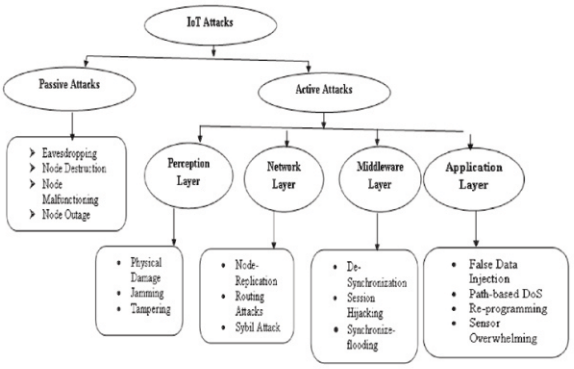

Fig.2. IoT Attacks in Each layer

2.1.2 Node Elimination

Physical Elimination [7] of nodes by any means (electronic surge and physical power).

2.1.3 Node Malfunctioning

This can be caused by including defective sensors [11], energy depletion as a result of sensor overloading.

2.1.4 Node Interruption

If a node's normal functionality fails, this attack occurs**.** In a heterogeneous network, for example, if a cluster head fails during normal operation, the WSN protocols must be able to mitigate the bad consequences of the node's failure by electing new cluster heads and offering alternate network path way.

2.1.5 Traffic Analysis

For attackers, a network's traffic pattern must be a commodity in the group of information packet [8]. The networking topology is used to derive by considering congestion arrangements. In Wireless Sensor Network, a sink node, which is closer to the base station, allows more transmission.

2.2 Active Attacks

IoT Layers are shown in Fig.3; Perception or sensor layer, Network or transmission Layer, Middleware or support Layer and Application Layer. Malicious actions are accomplished not only for data privacy [9] but also against in alive attacks. It's also used to gain intruder for accessing and use the resources, as well as disrupt an opponent's communications. A Denial-of-Service intrusion mainly focuses the availability of web benefits. A denial of service [10] is defined as any situation that absorbs resources and reduces a network's capability, preventing the network from executing its intended functionality correctly or in a timely manner.

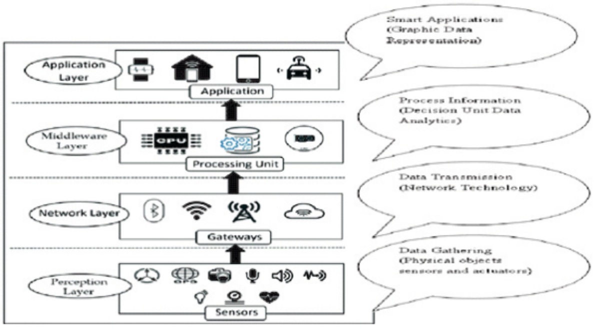
Smart Applications (Graphic Data Representation)
Application Layer
Application
Process Information (Decision Unit Data Analytics)
Middleware Layer
CPU
Processing Unit
Data Transmission (Network Technology)
Network Layer
Gateways
Data Gathering (Physical objects sensors and actuators)
Perception Layer
GPS
Sensors

Fig. 3. IoT Layered Architecture

2.2.1 Attacks towards Perception Layer

A sensor layer is another name for it. Its functions same to a person's eyes, ears and nose, in charge of analyzing objects and gathering data from them. Radio Frequency Identification, 2-Dimension barcodes, and sensors are just some of the types of sensors. Common Security attack of this layer;

2.2.1.1 Physical Damage

The attacker damages [11] components of the IoT device physically, resulting in a denial service attack.

2.2.1.2 Jamming

By transmitting at the same density as the signal, a malignant device can jam it. This signal [12] commits to the carrier's exploiting, and its merit is sufficient, lower the SNR below the threshold needed for the network using that route and to receive data properly.

2.2.1.3 Tampering

A physical attack [13] on the sensor node, as well as continuing transmission in the Wireless Sensor Network, such as connecting points to its circuit panel and gathering stored data, allow an attacker to take control of the sensor node.

2.2.2 Attacks towards Network Layer

An attacker sends large number of packets into the hub, causing traffic bottleneck [14] and depletion of power resources across the network. Network layer attacks are classified as node replication, routing attack, Sybil attack and sinkhole types.

2.2.2.1 Node-Replication

To cause inconsistency [7], an attacker positions clones of a negotiated system in several locations in the web. One of the most terrible attacks is the node replication (clone) attack, which allows an attacker to deflect the action of a network.

2.2.2.2 Routing Attack

In distraction attack, an intruder sends data to the incorrect destinations on purpose. These are accomplished by fabricating false routing broadcast and induce neighboring nodes routing suggestions to update with false information.

2.2.2.3 Sybil Attack

Sybil system [15] gets the identification of multiple nodes for a single node and behaves like them in the Sybil attack. This form of attack causes the surrounding wireless sensor network devices to agree on incorrect messages. For instance, the WSNs polling method, in which a single malicious device votes multiple times being chosen as the main portion of the routing.

2.2.2.4 Sinkhole Attack

This is a routing attack [16], and it is one of the most damaging of all routing attacks in wireless networks. The attacker tells its neighbors that it is very familiar with the shortest path to a targeted destination in this type of attack. The goal of this attack is to draw attention to a specific area so that packets can be discarded and network communication can be disrupted.

2.2.3 Attacks towards Middleware Layer

The middle level, intrusion accomplish the protocols that use contact data at each of two ends. All middle layer attacks are summarized as follows:

2.2.3.1 De-Synchronization

Through this attack [17] the data flow between two nodes, an intruder disrupts the real connections between them. Sending forged data, such as sequences of defective flags.

2.2.3.2 Session Hijacking

The "exploitation of" and "mitigate with" an appropriate communication [5] discussion in order to gain pirated access to a system's information session hijacking of TCP messages as an extension of IP networks is defined as this assault.

2.2.3.3 Synchronize-flooding

An attacker sends out a large number of emails to a large number of aims to deplete one's resources and memory by flooding a node with bogus messages, and can take control of it.

2.2.4 Attacks towards Application Layer

DOS [6] attacks can also target application layer protocols. Node localization, data aggregation, association, and fusion are all protocols that can be hampered. The following Application layer attacks are,

2.2.4.1 False Data Injection

Captured nodes [18] insert false data into the WSN in order to manipulate the overall outcome of a calculation. As a result, this attack occurs on a symbolic basis, and has little impact on anything other than rationale.

2.2.4.2 Path-based Denial of Service

This attack that occurs in the application layer, an attacker overcomes the nodes by flooding [11] point to point communications path with either concoct package, but this time from a great distance.

2.2.4.3 Re-programming

Every network unit must be patched every now and then Version restraint, code procurement [12], and encoding decoding to a freshly written program.

2.2.4.4 Sensor Overwhelming

Attacking the sensor measurements sensitivity sensors are targeted with spurious intervention, they are totally overwhelmed with fake signals and false stimuli.

III. SECURITY ATTACKS IN AGRICULTURE FIELD

3.1.1 Perception Layer

Perception layer contains the majority of hardware components. E.g. Sensors, RFID tags and play an important role. An information is gathered inside the node and master mounted in the built Information and Communication Technology like smart farming system, as well as contact between the involved devices. Malicious code is present. Non repudiation [9] is a well familiar service that delivered verification of data integrity as source in an enforceable relates that can be justified at any time by any other party with high trust and genius during the authentication process. Information repudiation causes an attacker to reject all of agriculture ICT systems Energy consumption, generated data and manufacturing process, potentially leading to a situation where facilities, authentication [18] data, or data flows are rejected through the network's node.

3.1.2 Network Layer

The most critical layer for connecting two ends, such as machine to machine, machine to fog, and back edge data sharing. In the case of a fault, connection is corrupted, and the device is essentially turned off. Inadequate email systems and a need of automated restores can force to data security concerns. Phishing Attacks [9], Data transit Attacks and Routing attacks are the most common attacks of this layer.

3.1.3 Middle Layer

This layer works in a two-way fashion, between application layer and Hardware layer. Data system management issues such as Knowledge discovery may all be affected by intrusions. Man in the Middle intruder [15], Structure Query Language Needle intruder, and Flow intruder in Fog.

3.1.4 Application Layer

The lack of service is delivery between the two parties.

Users from a variety of domains, including Farmers, Manufactures may be involved. The common attacks [9] are Data embezzlement, Entry restraint Attacks, Service rupture Attacks, and Reprogram Attack.

IV. Security and Privacy Requirements in IoT

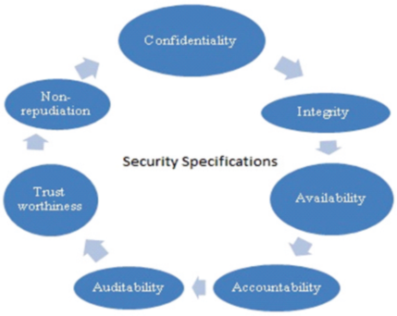

Fig. 4. IoT Security Specifications

The Security Requirements shown in Fig. 4 concern with, Confidentiality [17]: Assuring that the data is only accessible to those who are authorized.

Integrity: Assuring the precision, completeness, and absence of unauthorized data manipulation.

Availability: Assuring that all device resources are accessible when an approved user requests them.

Accountability: A system's ability to keep users accountable for their behaviour.

Auditability: The capacity of a device to continuously track all activities.

Trust worthiness: A system's ability to create confidence in a third party by verifying identity.

Non-repudiation: A system's ability to validate the occurrence or nonoccurrence of an action.

Privacy [19] in the scope of IoT can be classified into the following categories;

- Consciousness of the privacy threats presented by smart stuff and services in the data subject's environment.

- Individual control over the collection and processing of personal data by smart things in their environment[20].

- Due to the network's complexity, a single flaw will bring the entire system down, impacting everyone.

V. CONCLUSION AND FUTURE WORK

This paper discussed attacks on IoT layers as well as attacks in Agriculture Applications. Sensors are used to collect information from the domain, so IoT device are important, before being sent to the end user, this data is further aggregated, analyzed and visualized. These devices are vulnerable to a variety of attacks. Any application's success is determined by its security. Because of the limited resources in sensors and other characteristics of the IoT environment, traditional protection measures are ineffective for this application. For agriculture applications, trust-based protection is a major concern. As a result, ensuring protection in IoT agriculture needs a trust-based approach.

REFERENCES

[1] Xuanxia Yao, Fadi Farha et. al.," Security and privacy issues of physical objects in the IoT: Challenges and opportunities", Digital Communications and Networks, https://doi.org/10.1016/j.dcan.2020.09.001, 2020.

[2] H. Liu, H. Ning, Y. Yue, Y. Wan, L.T. Yang, "Selective disclosure and yoking-proof based privacy-preserving authentication scheme for cloud assisted wearable devices, Future Generation Computer Systems 78 (976–986), https://doi.org/10.1016/ j.future. 2017.04.014, 2018.

[3] H. Liu, X. Yao, T. Yang, H. Ning, Cooperative privacy preservation for wearable devices in hybrid computing-based smart health, IEEE Internet of Things Journal 6 (2) 1352–1362, https://doi.org/10.1109/JIOT.2018.2843561, 2019.

[4] X. Wang, X. Zha, W. Ni, R.P. Liu, Y.J. Guo, X. Niu, K. Zheng, Survey on block chain for internet of things, Computing Communication, 136(2) (2019) 10–29, https://doi.org/10.1016/j.com, 2019.

[5] Tariq, N., Asim, M., Maamar, Z., Farooqi, M.Z., Faci, N., Baker, T., 2019. A mobile code- driven trust mechanism for detecting internal attacks in sensor node-powered iot. J. Parallel Distributed Computing 134, 198–206, https://doi.org/10.1016/j.jpdc, 2019.

[6] Zhang, Z., Cho, M.C.Y., Wang, C., Hsu, C., Chen, C.K., Shieh, S., 2014. IoT Security: ongoing challenges and research opportunities. In: 7th IEEE International Conference on Service- oriented Computing and Applications, pp. 230–234, Japan, 2014. https://doi.org/10.1109/SOCA.2014.

[7] Tariq, N., Asim, M., Maamar, Z., Farooqi, M.Z., Faci, N., Baker, T., “A mobile code-driven trust mechanism for detecting internal attacks in sensor node-powered IoT. Parallel Distributed Computing, 198–206, https://doi.org/10.1016/j.jpdc, 2018.

[8] Narges Yousefnezhad A, Avleen Malhi A, Kary Framling, “Security in product lifecycle of IoT devices: A survey”, Journal of Network and Computer Applications 171, 2020.

[9] Roopaei, M.; Rad, P, Choo, K.R. Cloud of Things in smart agriculture: Intelligent irrigation monitoring by Thermal imaging. IEEE Cloud Computing. 2017, 4, 10–15.

[10] Barreto L, Amaral A, “Smart farming: Cyber security challenges”, In Proceedings of the 2018 International Conference on Intelligent Systems (IS), pp. 870–876, Portugal, 25–27 September 2018.

[11] Yousefnezhad, N., Madhikermi, M., Frmling, K., 2018. Medi: Measurement-based device Identification framework for internet of things. In: 16th IEEE International Conference on Industrial Informatics, Portugal, 2018, pp. 95–100, https://doi.org/10.1109/INDIN, 2018.

[12] Dan D. Koo, John J. Lee, Aleksei Sebastiani, and Jonghoon Kim,” An Internet-of-Things (IoT) system development and implementation for bathroom safety enhancement”International Conference on Sustainable Design, Engineering and Construction, Sciencedirect Procedia Engineering 145 (2016) 396 – 403.

[13] Vinay M, Shivashankar s k,” Monitoring And Controlling Of Smart Equipments In Manufacturing Industry Using Iot Applications”,International Journal of Technical Research and Applications e-ISSN: 2320-8163, www.ijtra.com Volume 4, Issue 3 (May-June, 2016), PP. 96-100.

[14] Lo’ai Tawalbeh, Fadi Muheidat, Mais Tawalbeh and Muhannad Quwaider, “IoT Privacy and Security: Challenges and Solutions”, Applied Science, doi:10.3390/app10124102, 2020.

[15] Dey, N., Hassanien, A.E., Bhatt, C., Ashour, A. and Satapathy, S.C., “Internet of Things and Big Data Analytics toward Next-Generation Intelligence”, 2018, https://doi.org/10.1007/978-3-319-60435-0.

[16] Narges Yousefnezhad, Avleen Malhi, Kary Främling, “Security in product lifecycle of IoT devices: A

survey", Journal of Network and Computer Applications, 2020. https://doi.org/10.1016/ j.jnca.2020.102779.

[17] Xuanxia Yao, Fadi Farha, Rongyang Li et. al., "Security and privacy issues of physical objects in the IoT: Challenges and opportunities", 2020, Digital Communications and Network, https://doi.org/10.1016/ j.dcan.2020.09.001.

[18] Mirza Abdur Razzaq, Muhammad Ali Qureshi et. al., "Security Issues in the Internet of Things (IoT): A Comprehensive Study", International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017.

[19] Eman Shaikh, Iman Mohiuddin, Ayisha Manzoor, "Internet of Things (IoT): Security and Privacy Threats", IEEE, 2019.

[20] Muhamaad Bhuhan, Rana Ashif Rahman, " IoT Elements, Layered Architecture and security issues: A comprehensive Survey", Sensors, 2018, doi:10.3390/s18092796.