

An Analysis of Security Attacks on IoT Applications

Khalid Hamad Alkhamisi^{*1}

¹Department of Computer Science and Artificial Intelligence, University of Jeddah, Saudi Arabia

Corresponding Author: Khalid Hamad Alkhamisi* (kalkhamisi.stu@uj.edu.sa)

ABSTRACT

The Internet of Things (IoT) has emerged as an innovation equipped for interfacing heterogeneous objects, like individuals, gadgets, and foundation, and simplifying our day-to-day routines, more secure, and productive. Therefore, IOT directly impacts the security and privacy of its all-interconnected nodes as reported in the state-of-the-art literature. Consequently, privacy and security are becoming substantial challenges of the IoT. This study aims to identify and analyze numerous security and privacy challenges faced by the IoT-based environment. Jamming, spoofing, data tempering, and fake nodes are among the crucial challenges encountered by IoT environments.

Keywords: Security, Privacy, Internet of things, vulnerabilities

1. INTRODUCTION

The idea of the Internet of Things (IoT) is new as it is still in its infancy. The term IoT was coined between 2008-2009 but still no single definition on which research agreed [1]. The IoT can be defined as a system of interconnected digital devices, objects, mechanical machines, people, and even animals, this interconnection of devices is also illustrated in Figure 1. These interrelated devices are assigned a distinct identifier and are capable to transfer data through a network without the need for human or computer contact [1]. IoT systems are becoming mainstream because wireless networks are expanding quickly and there are more sensing devices available. IoT technology deals with enormous sensing devices, machines virtual entities, and objects that interact with each other [2]. This technology is attracting practitioners at a rapid pace and more than 100 billion devices are expected to be interlinked in coming years. The acceptance of IoT has amplified at a rapid pace, as Internet technologies are utilized for diverse purposes like education, health, business, transportation, and communication [3].



Figure 1. Components of IoT

IoT has arisen as an innovation equipped for interfacing heterogeneous objects, like individuals, devices, and foundations, and simplifies our day-to-day routines, more secure, and productive. This IOT environment is highly risky facing attacks like jamming, phishing, sleep denial, fake nodes, and data tempering. These threats can be encountered by the Gaussian SVM, Bayesian risk-based, Rep-tree (used for detecting the jamming signal), and K-nearest neighbor. The PHY Authentication is deployed amongst the collecting nodes and sending nodes for authentication to remove spoofing between the nodes. To protect from sleep denial, SVM-based authentication is used for medical devices. Fake nodes, ANN-based model is trained on the real-time data traffic, uses to detect the fake nodes. IoT is taken on in a broader assortment to utilize smart homes [4], savvy offices [5, 6], computerized industry [7], shrewd cities [8], canny cultivating and farming [9], astute transportation frameworks [10], production network [11] and smart medical care [12].

Various sensors are utilized in IoT objects to gather information from the climate and ship off the implanted gadgets. These objects are compelled for processing abilities and move information to haze or potentially cloud hub through wire or remote organization for creating experiences. IoT utilizes multi-facet engineering like detecting, accessing, handling, and application layers. Each IoT layer is dependent on a unique security plan and assurance defects, which are truly tested to address and give a suitable countermeasure [13].

A contextual investigation has been conducted by [14] about the awkwardness of IoT devices in the moderation of an attack by introducing Edina SP-2101W in an iPad and ready to send off normal assaults, for example, gadget examining assault, savage power assault, satirizing assault, and firmware attack. Creators likewise demonstrated that IOT hub assets were inadequate to fuse complex encryption advances. Along these lines, security and security taking care of in IoT networks are quite possibly the main tests.

1.1 Problem Statement

There is a frequent danger to the security of the information which is being shared among the devices which share data in IoT devices. So some security measures are required to be taken to protect the data integrity and to implement the C.I.A triad for the secure transmission of data. In this paper, an investigation of a total answer for IoT networks that can guarantee information security is done. The layer-wise study of the security dangers to the IoT environment is conducted, and the security attacks at the network, application, transport, and perception layer are elaborated in detail which will enable to block the dangers to the security.

2. SECURITY THREATS, VULNERABILITIES & CHALLENGES IN IoT

Numerous types of research studies have been conducted considering recent trends in IoT security and services [3, 15]. However, the state of the literature related to the IoT security challenges is lacking with the proper investigation regarding the security and privacy requirements to establish users' trust. Most of the studies focused on highlighting the difficulties faced by the scientific community, but no meaningful solution was developed.

Web-associated devices offer an assortment of safety chances. Normal security challenges on IoT are man-in-the-center assault, falsification assault, heterogeneous organization assault, application hazard of IPv6, remote neighborhood (WLAN) application struggle, and forswearing of administration (DoS) or disperse refusal of administration (DDoS). Although the Internet of Things has given new gadgets more power to the interface, general network protection concerns are not new. Here are absolutely the most real dangers to a company organization that desires correct IoT network safety.

Over the most recent few years, numerous scientists have led audits on current IoT security countermeasures to give a guide for potential work. Because of the assortment of IoT networks, an intruder might make malicious attempts to bypass the normal authentication process. This segment addresses IoT security-related audit papers. Layer-wise investigations regarding security attacks have been conducted by [16] emphasizing their level of effect on IoT networks alongside the asymmetric and symmetric encryption calculations for client authentication and access control. Moreover, the study focused on different difficulties with regular security arrangements. An effort has been made by [17] to conduct a review of IoT security vulnerabilities and challenges. The authors have delineated those attacks comprising Physical Attacks, Network Attacks, and Software and Encryption attacks. Encryption-based security countermeasures are featured to coordinate the future work of security in heterogeneous IoT conditions. For example, cryptography hash is tended to for secure booting, gadget confirmation, information respectability, steering security, and information security. It has been claimed by [18] that the establishment of safe and secure communication is one of the major security challenges of the IoT environment. There are security concerns

associated IoT technology, as this technology consists of various networks where a user does not have control over the network hence data becomes vulnerable exposing various security and confidentiality threats. Furthermore, the involvement of numerous devices makes it challenging to assure data security [19].

2.1 Layers in IoT

The IoT architecture comprises four layers that are named the Network layer, perception layer, application layer, and transport layer [20]. The layered architecture is depicted in Figure 2.

2.1.1 Perception Layer

This can also be termed the physical layer and in this layer, the sensors aggregate senses the environment and collects information about the surrounding. It comprises the wireless sensor network (WSNs) which monitor the environment and the physical conditions the data is then communicated across the network and determines radio frequency identification (RFID) through data that can be sent and received by radio waves, IMD, GPS, and others.

2.1.2 Network layer

This layer connects network devices, smart devices, and servers and also enables the transfer and processing of data. It includes different networks like 4G, 3G, Infrared, Wi-Fi, and WiMAX. It has the responsibility to carry the incoming data from the transport center on the network layer. A routing protocol RPL has already been developed for lost and low-power networks

2.1.3 Transport layer

Enormous amount of data is generated because of the heterogeneous nature of the devices in the IoT architecture. The middle layer works to fulfill the main tasks which involve the managing of the service and the other task is the storage of the flow of information from the various layers of the database.

The services of the IoT could be disrupted due to attacks that impact the processing layer, burnout could occur as a result of hostile attacks like DOS (Denial of Service) which overwhelms the victim with a large number of requests thus minimizing the important requests and makes the network unavailable for the main users [21]. The purpose of this attack could be the exertion of the resources like batteries and the memory of devices.

2.1.4 Application layer

This layer is an interface that provides the services for the applications and the user. The responsibility of this layer is the formatting of the data, it depends upon the hypertext transfer protocol (HTTP) although this protocol is not enough when it enters the environment having limited availability of resources because it casts the massive burden of analysis because of length. In the IoT environment, MQTT, and CoAP could be used as alternatives to this protocol.

2.2 Security issues in IoT

The security issues of IoT applications are delineated in this section. The perception and the network can be combined and could be named the physical layer. In the physical layer, the hardware device is implied and the sensor devices are connected through various gateways. The hardware devices have limited capabilities and are vulnerable to attacks. The components could be hacked by the hacker. The security issues are delineated below.

2.2.1 Node Capture Attack

The smart devices are used in the architecture of the IoT, the attacker can attack the network and can replace the devices with the wrong ones to get network access. It becomes very difficult to find the actual nodes.

2.2.2 Replay Attacks

In such attacks, the attacker intercepts the message from the communication media and sends the message later to the same network. The hacker can hack the smart devices and can send the data as an authorized node. Authentication of the users can help to tackle this attack [22].

2.2.3 Malicious code attack

It is a coded attack that specifically targets the code part of the software and causes unwanted damage to the network, the intruder then sends the malicious code into the software which infects the software [23, 24].

2.2.4 Side Channel Attack

In this attack, the attacker tries to extract the plain text from the cipher text and tries to get the key for decrypting the data. The prevention of this attack is to use a time-constant system for encryption and decryption.

2.2.5 Cross-site Scripting

It is also termed an injection attack and allows the attacker to insert a client-side script in different

websites that are used by different users. The intruder may forge the data and the original contents of the website and can illegally use the user's data [25].

2.2.6 Eavesdropping

This attack occurs when smart devices are compromised. The insecure communication channel leads the attacker to read the communication between the devices [26]. It is a passive attack in which the attacker gets the data from the insecure transmission media.

2.2.7 Denial of Service (DoS)

In this attack, the attacker shuts down the network by sending fake requests and prevents the authenticated user from accessing the data or the other resources of the network. Crashing services and Flooding services are the two attack types. When enormous traffic hits the server then flooding attack occurs and the service-to-crash attacks exploit the vulnerability of the network [22].

2.2.8 Storage Attack

The personal and useful information of the users is stored on the cloud or storage devices. The precious information can be modified by the attacker from the cloud and from the storage devices as well. The attacker can also manipulate the information of the user with incorrect details

2.2.9 Spoofing Attack

A fake node is an attack where the attacker adds an extra node into the system and then enters false data in the system for disrupting the security of the system. In Table 1 the summary of the security and privacy issues along with the countermeasures is presented.

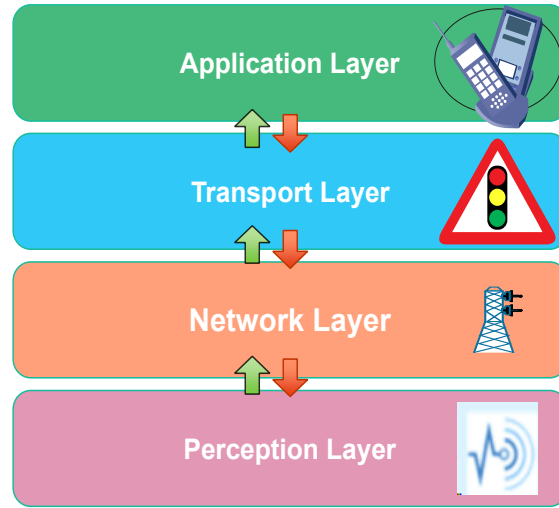


Figure 2. Layers of IoT Architecture

Table 1. Attacks on different layers and their countermeasures

Serial number	Layer	Attack	Countermeasure
1.	Application Layer	Phishing attack, malicious virus	Trustworthy firewall, worm detector software
2.	Transport Layer	Collision, Data transit attacks	Spread spectrum
3.	Network Layer	DoS attack, Spoofing attack	Authorization, access control
4.	Perception Layer	Malicious code injection attacks,	Secure encryption algorithm

	Eavesdropping attacks, replay attacks	
--	---------------------------------------	--

3. CONCLUSION

Due to the advent of emerging technologies, IoT systems are becoming an essential part of modern society. Various IoT devices can easily observe from homes to schools and from markets to workplaces nowadays. Therefore, establishing smart environments like smart transportation systems, smart traffic mechanisms, smart homes, and even smart educational institutions. The concept of IoT is enhancing at a fast pace while encountering various challenges like security and privacy issues for secure communication among the interconnected devices, the secrecy of data over the network, availability and reliability and etc. Security in IoT systems has emerged as one of the crucial challenges which need to be addressed on priority if the network is accepted and is being used in various activities. These human activities may include entertainment, business, education, learning, and training. PUFs based security protocols can be utilized to identify and authenticate IoT objects using time stamps and unique keys to verify the nodes in the accepted network. Hence, to establish a safe and secure IoT-based smart environment, there is a need to deploy more secure encryption algorithms. So that only authorized entities can acquire desired services.

In the future, more efforts can be made considering cryptographic security methods that are capable of operating in an IOT base smart environment having limited resources. Moreover, there is a need to formulate models or procedures for the data collected by IoT devices connected to the internet. These procedures can assist to reduce the number of unforeseen vulnerabilities and associated attacks on heterogeneous platforms.

REFERENCES

- [1] N. Miloslavskaya and A. Tolstoy, "Internet of things: information security challenges and solutions," *Cluster Computing*, vol. 22, no. 1, pp. 103-119, 2019.
- [2] Z. Safdar, S. Farid, M. Pasha, and K. Safdar, "A security model for iot based systems," *Technical Journal*, vol. 22, no. IV, 2017.
- [3] L. a. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT Privacy and security: Challenges and solutions," *Applied Sciences*, vol. 10, no. 12, p. 4102, 2020.
- [4] F. K. Santoso and N. C. Vun, "Securing IoT for smart home system," in *2015 international symposium on consumer electronics (ISCE)*, 2015, pp. 1-2: IEEE.
- [5] H. N. Rafsanjani and A. Ghahramani, "Towards utilizing internet of things (IoT) devices for understanding individual occupants' energy usage of personal and shared appliances in office buildings," *Journal of Building Engineering*, vol. 27, p. 100948, 2020.
- [6] F. Loukil, C. Ghedira-Guegan, A. N. Benharkat, K. Boukadi, and Z. Maamar, "Privacy-aware in the IoT applications: a systematic literature review," in *OTM Confederated International Conferences "On the Move to Meaningful Internet Systems"*, 2017, pp. 552-569: Springer.
- [7] S. Aheleroff *et al.*, "IoT-enabled smart appliances under industry 4.0: A case study," *Advanced engineering informatics*, vol. 43, p. 101043, 2020.
- [8] P. J. Basford, F. M. Bulot, M. Apetroaie-Cristea, S. J. Cox, and S. J. Ossont, "LoRaWAN for smart city IoT deployments: A long term evaluation," *Sensors*, vol. 20, no. 3, p. 648, 2020.
- [9] E. Symeonaki, K. Arvanitis, and D. Piromalis, "A context-aware middleware cloud approach for integrating precision farming facilities into the IoT toward agriculture 4.0," *Applied Sciences*, vol. 10, no. 3, p. 813, 2020.
- [10] M. S. Kaiser *et al.*, "Advances in crowd analysis for urban applications through urban event detection," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 10, pp. 3092-3112, 2017.
- [11] T. De Vass, H. Shee, and S. J. Miah, "Iot in supply chain management: a narrative on retail sector sustainability," *International Journal of Logistics Research and Applications*, vol. 24, no. 6, pp. 605-624, 2021.
- [12] S. Selvaraj and S. Sundaravaradhan, "Challenges and opportunities in IoT healthcare systems: a systematic review," *SN Applied Sciences*, vol. 2, no. 1, pp. 1-8, 2020.
- [13] M. Burhanuddin, A. A.-J. Mohammed, R. Ismail, M. E. Hameed, A. N. Kareem, and H. Basiron, "A review on security challenges and features in wireless sensor networks: IoT perspective," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. 10, no. 1-7, pp. 17-21, 2018.
- [14] Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu, and X. Fu, "Security vulnerabilities of internet of things: A case study of the smart plug system," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1899-1909, 2017.

- [15] W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Computer networks*, vol. 148, pp. 283-294, 2019.
- [16] I. Ali, S. Sabir, and Z. Ullah, "Internet of things security, device authentication and access control: a review," *arXiv preprint arXiv:1901.07309*, 2019.
- [17] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in *2015 IEEE symposium on computers and communication (ISCC)*, 2015, pp. 180-187: IEEE.
- [18] N. Alhalafi and P. Veeraraghavan, "Privacy and Security Challenges and Solutions in IOT: A review," in *IOP conference series: Earth and environmental science*, 2019, vol. 322, no. 1, p. 012013: IOP Publishing.
- [19] K. Rose, S. Eldridge, and L. Chapin, "The internet of things: An overview," *The internet society (ISOC)*, vol. 80, pp. 1-50, 2015.
- [20] H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman, and M. J. T. J. o. S. Bilal, "Smart home security: challenges, issues and solutions at different IoT layers," vol. 77, no. 12, pp. 14053-14089, 2021.
- [21] Y. Lu and L. J. I. I. o. T. J. Da Xu, "Internet of Things (IoT) cybersecurity research: A review of current research topics," vol. 6, no. 2, pp. 2103-2115, 2018.
- [22] K. Doshi, Y. Yilmaz, S. J. I. T. o. D. Uludag, and S. Computing, "Timely detection and mitigation of stealthy DDoS attacks via IoT networks," vol. 18, no. 5, pp. 2164-2176, 2021.
- [23] N. Kashyap, A. Rana, V. Kansal, and H. Walia, "Improve Cloud Based IoT Architecture Layer Security-A Literature Review," in *2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, 2021, pp. 772-777: IEEE.
- [24] A. Mosenia and N. K. J. I. T. o. e. t. i. c. Jha, "A comprehensive study of security of internet-of-things," vol. 5, no. 4, pp. 586-602, 2016.
- [25] N. Mishra and S. J. I. A. Pandya, "Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review," 2021.
- [26] G. Liu *et al.*, "Softwarized iot network immunity against eavesdropping with programmable data planes," vol. 8, no. 8, pp. 6578-6590, 2021.