



Internet-of-Things Security and Vulnerabilities: Case Study

Ghaida Alqarawi, Bashayer Alkhalifah, Najla Alharbi & Salim El Khediri

To cite this article: Ghaida Alqarawi, Bashayer Alkhalifah, Najla Alharbi & Salim El Khediri (2022): Internet-of-Things Security and Vulnerabilities: Case Study, Journal of Applied Security Research, DOI: [10.1080/19361610.2022.2031841](https://doi.org/10.1080/19361610.2022.2031841)

To link to this article: <https://doi.org/10.1080/19361610.2022.2031841>



Published online: 03 Feb 2022.



Submit your article to this journal [↗](#)



Article views: 156




View related articles [↗](#)



View Crossmark data [↗](#)



Internet-of-Things Security and Vulnerabilities: Case Study

Ghaida Alqarawi, Bashayer Alkhalifah, Najla Alharbi, and Salim El Khediri 

Department of Information Technology, College of Computer, Qassim University, Buraidah, Saudi Arabia

ABSTRACT

The incorporation of IoT in the world has had tremendous popularity in the field of Technology. This great innovation has enabled seamless transformation in business and operation transformation. However, significant usage of this innovation also poses a security threat which has become a more critical point of concern to many businesses across the globe. Many companies that depend on IoT have faced security breaches and threats. The IoT countermeasures have not been well-factored upon, which poses a more significant challenge to many organizations that heavily rely on this technology. In this survey, we propose a security survey that will help tackle the problems associated with IoT and offer security solutions on all the IoT layers. The results show that authentication is the most critical security measure to implement in IoT.

KEYWORDS

Internet of things; IoT security; cyber security vulnerabilities; attacks

Introduction

The internet of things (IoT) connects (heterogenous) physical devices to the internet, allowing information to be sent and received via the internet. In 1999, the concept of IoT was first used by Kevin Ashton (Ogonji et al., 2020). The IoT term has evolved into various technologies like sensors, real-time analysis, machine learning, and embedded systems. It's all about the smart hospital idea and other devices controlled via wireless or fixed internet. Smart devices can acquire data and share data in everyday life to do the required task (Javaid & Khan, 2021). IoT applications apply to smart cities, devices, cars, connected healthcare, homes, and entertainment systems. According to cisco research, roughly 500 billion gadgets will use sensors and be connected to the internet by 2030. it is said that the IoT is the network that associates these devices for data communication (Aman et al., 2020; Alqallaf, 2021).

There are still security concerns due to many devices being connected to the internet and the large amount of data associated with it. Notably, in sectors with systems critical to the safety of individuals and the community at large, for example, smart transportation systems and connected cars must be secure to avoid accidents and injuries and safeguard the privacy of drivers who may be tracked on the road roads (Obaidat et al., 2020). Security on IoT refers to the degree of protection of, or resilience to, IoT applications and infrastructure. These devices have become an easy target for intruders since they heavily rely on external resources and thus are often left unattended. Once the network layer has been compromised, it becomes very easy for cyber attackers and hackers to easily gain access and control of a device and use the device to attack other close devices through the compromised network node. A recent study conducted by HP showed that 70% of all the devices on the internet are easily vulnerable to attack (Kumar et al., 2016).

With the increasing developments in IoT, security continues to be an important issue, and concerns will continue to arise. However, in 2021, there will be even more opportunities for new techniques to make IoT devices more secure. Most existing techniques for securing the IoT do not focus on the new types of security risks IoT infrastructure may face. Therefore, they cannot detect vulnerabilities or attacks that might originate from the IoT service. Moreover, very few existing works have investigated the different layers of the IoT infrastructure as a whole.

Motivation

The primary goal of this survey is to evaluate the security issues that are found in the IoT devices and also evaluate the privacy issues that exist in IoT applications. The survey discussed the IoT technologies and architecture model, identified security and privacy issues in the IoT system, and provided a taxonomy of attacks based on the IoT layer models.

- We discussed the basic IoT architecture.
- We highlighted the classification of the various IoT layers.
- We discussed the security threats associated with IoT.
- We discussed the countermeasures that should be implemented in the IoT system.

The structure of this paper is organized as follow: section Background of IoT of the report describes the background of IoT. Section Attacks threats and vulnerabilities provide the current security issues that IOT infrastructure faces at different layers are investigated. Section Countermeasures

presents the solutions proposed to solve the related security issues. The paper is concluded in section Conclusion.

Background of IoT

With the growth of technology and advancement in the Internet across the globe, many innovative solutions and names for the Internet have come into existence. Various phases have led to the tremendous growth of the Internet across the globe. The first phase which was given the name Pre-internet phase entailed the communication of people over a fixed telephone booth that used a telephone line channel and Short Message Service form. In the later stages, the medium of communication was then upgraded to incorporate a mobile telephony device. The second phase of internet communication was called the Internet of Content Phases, which entailed sending large-sized messages through an email channel medium. This phase allowed the capability of incorporating attachments, entertainment, and information data.

The Third phase of internet communication was called the Internet of Services phase, which mainly focused on electronic media applications. This included the uses of e-commerce and e-productivity. The fourth phase, which was referred to as the Internet of people, is the state upon which people associated with each other directly through social media platforms and other mediums of communications platforms like YouTube, Skype, and Facebook.

The current phase is the IoT. The future will have a functional model aspect that will enable the connection of devices over the Internet. This will enable the devices to communicate amongst each other and connect and perform various programmed activities based on the design and functional capabilities of various data objects. However, the current era is not the end of the road for this concept. Artificial Intelligence is the future of communication. Incorporating this technology in devices will have a new dimension in the era of communication. However, it may not be incorrect to term the incoming phase as the IoT phases powered by Figure 1 shown, but how the use of the IoT has evolved from the Internet. By starting from scientists, engineers, and researchers from various technical areas, it has



Figure 1. The evolution of the internet from pre-internet to IoT.

passed from various phases and is moving to a new dimension of IoT (Khanna & Kaur, 2019).

Incorporating IoT requires a very specific standard of architecture to provide a collaborative environment for various competitors in the business world to enhance quality and efficiency for the organization. A very detailed evaluation and analysis of the traditional Internet architecture needs to be performed very well to measure the capability and capacity to meet the challenges that have been associated with the IoT. This technology has enabled the connection of various large numbers of heterogeneous objects through the Internet (Alansari et al., 2018). Recently, various IoT architecture models have been proposed since no single model has been agreed upon (Masoodi et al., 2019). The basic IoT architecture model consists of Four key layers shown in Figure 2. They include:

1. Perception layer:

This is the lowest layer of the IoT model architecture. It is mainly referred to as the brain of four-layered architecture and is also called the physical layer. The sensing devices, i.e., sensors, are mainly found in this layer. Also referred to as the sensor layer (Kumar et al., 2016).

2. Network layer:

This layer holds the network communications software and the physical

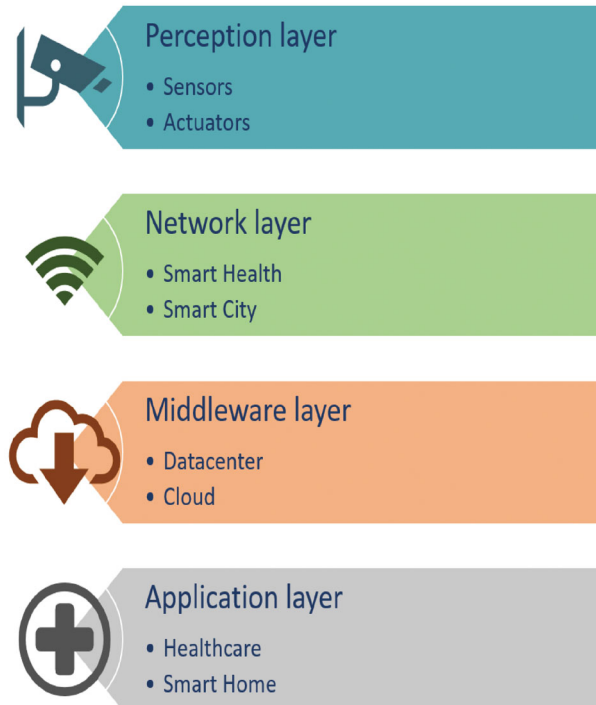


Figure 2. IoT layers.

components, i.e., the topologies, servers, network components, and nodes. It allows the devices to communicate, and its primary purpose is to allow for the transmission of data between one device to another and the receivers (Aziz & Haq, 2018).

3. **Middleware layer:**

This layer deals with the analysis, storage, and processing of information. It is also referred to as the processing layer. It deals with the provision of services to the lower layers and can compute and process information automatically. Many AI technologies, i.e., Cloud Computing and Big Data analysis, are done in this layer (Aziz & Haq, 2018).

4. **Application layer:**

This layer is based upon a client's request and is entirely dependent on the functional values of the entities used, i.e., temperature and humidity measurements gauge. This layer provides a high level of intelligent services to meet the client requirements specification (Alansari et al., 2018).

Attacks threats and vulnerabilities

This section examines IoT attacks and security/privacy issues based on the four-layer architecture outlined above. The attack classification was shown in [Figure 3](#).

Perception layer

The first layer, also referred to as the Physical IoT sensor, helps to support the collection of data and processing. It incorporates the use of various technologies like RFID (radio-frequency identification) and GPS systems. This layer is mainly made up of sensors and actuators that help to provide various measurements (Frustaci et al., 2018). The attacks at the perception layer mainly aim to destroy and inhibit communication and collection of data.

Unauthorized access to the tags

RFID tags are an important component of an IoT network. The integrity of the system is ensured by authorized access to these tags. If an unauthorized individual obtains to access the system, he can edit or delete the tag, compromising the system's confidentiality and integrity. In the IoT context, a smart verification algorithm (SVA) is used (Imdad et al., 2020).

Tag cloning

Tag cloning technique involves attaching tags to various objects and their data components to read and modify them using hacking techniques.

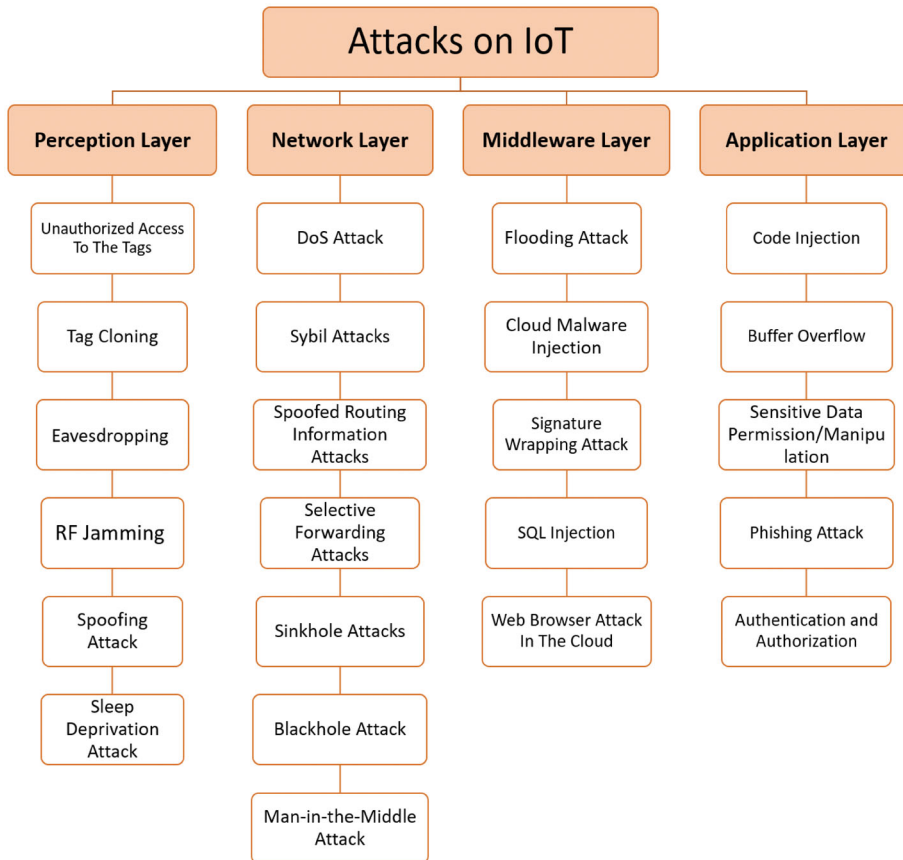


Figure 3. IoT attack classification.

Attackers make a replica of tags and compromise the system reader in that it cannot differentiate between a compromised and the original tag (Robles & Endencio-Robles, 2019).

Eavesdropping

The IoT applications mainly consist of a group of nodes deployed in open settings, which makes them vulnerable to eavesdropping. During the transmission and authentication steps, the attacker may be able to collect data (Hassija et al., 2019).

RF jamming

The RF waves are delivered to the network in this attack to disrupt communication between the tags and readers. By interfering with all the signals within its range, attackers might use RF jamming to prevent readers from communicating with all tags (Rahimi et al., 2018).

Spoofing attack

This form of attack enables an attacker to gain and have full access to the IoT systems. After gaining full access to the system, the attacker will then send malicious data into the systems. This form of attack includes the RFID spoofing form of attack where an attacker fakes and records the facts of an aerial RFID tag and then later transfer malicious data into the IoT device using the tag identification technique (Kamble & Bhutad, 2018).

Sleep deprivation attack

This is a form of attack that attacks the sensor node of a Wi-Fi sensor due to its inactivity. The batteries in the sensor nodes have a given duration of life span. This is a form of attack that occurs at the node and result in the use of extra charge and battery thus inhibiting the battery life, which thus results in the node closing down (Kamble & Bhutad, 2018).

Network layer

The network layer is the next tier, following the perception layer in the IoT layer's architecture. The network layer is in charge of providing information security as well as enabling network transmission. Mobile devices, the internet, and cloud computing are all part of it. Wireless sensor networks make up the network layer (WSN) (Shruthi & Vinay, 2016).

DoS Attack

The devices or servers are overburdened to the point that they cannot provide service to those who require it. DoS attacks prevent data from being transferred between devices and their source. The gadget receives an overflow of data, which causes it to shut down its processes. A good example is the seizure of health information systems and services implemented in a low bandwidth capacity environment. There exist risks of life-threatening scenarios, and commercial losses are associated with IoT networks (Kumar et al., 2016).

Sybil attacks

To confuse nodes, a malicious node offers several identities to the network, making an adversary appear to be present in multiple positions/locations simultaneously. The "sybil attacks" are a type of attack. In a spectrum where all nodes participate collaboratively in decision making, an attacker can provide incorrect sensing information, resulting in incorrect sensing decisions, allowing unneeded false information to travel down the entire node chain via the pub channels. The node employs its identity validation

mechanism to counteract this attack, which employs both direct and indirect validation methods. Indirect validation, each node verifies the validity of the identities of the others. Indirect validation, on the other hand, allows other confirmed nodes to validate other nodes. By owning a unique key shared only with the base station, all participating nodes must confirm their identities (Shruthi & Vinay, 2016).

Spoofed routing information attacks

The most direct attack on the system that would happen on a directing convention is concentrating it on the system's routing data. An attacker could fake, modify, or replay routing data to disrupt the system's seamless communication. Making a routing loop, modifying the routing length, producing phony blunder messages, dividing the network, and increasing end-to-end delay are examples of these disruptions. An authentication system is required to prevent the attack, and only valid routing information should be received (Khattak et al., 2019).

Selective forwarding attacks

All nodes in a multi-hop network system must forward messages precisely. This is commonly used in dense WSNs. An attacker may set up a node to only transmit a few messages while dropping the rest. The support vector machines employed in the assault and the packet sequence numbers must be reviewed regularly to prevent the attack (Khattak et al., 2019).

Sinkhole attacks

Because CRNs primarily use multi-hop routing, malicious nodes find it simple to attack legal nodes in hops. According to the sinkhole attack scenario, the attacker will portray himself as the best route provider to a given target, which is usually a low latency route. When other legal nodes use this bogus route to deliver data packets, the attacker either misuses or discards the packet from the network. The attacker can exploit the packet to carry out a variety of assaults, including eavesdropping, modifying information in the packet and resending it, and selectively forwarding packets from specific nodes (Tuan et al., 2020).

Blackhole attack

In this form of attack, the network traffic is routed to a specific node that does not exist in the network in this attack. Packets are thus dropped as a result of this, resulting in significant data loss. A Security Aware Routing (SAR) protocol is then used for WSNs to prevent the blackhole attack (Prabu et al., 2015).

Man-in-the-middle attack

This form of attack is similar to eavesdropping attacks. The communication channel where unauthorized users are present is the target of an attack. The communication between the user and the device can be monitored and controlled by the user. Two other people, Unauthorized users, can also take advantage of this feature. Assume the victim's identity and then obtains information via communication across the channel (Shruthi & Vinay, 2016).

Middleware layer

Attackers can affect the application layer by attacking the middleware layer, which provides services to the application layer. This form of attack on the server and database affects both the information and operation functionality of the system. The Attacks on the cloud servers mainly focus on virtualization and big data, which pose a significant threat to user privacy.

Flooding attack

This attack sends much useless traffic through the network, making the target system unreachable (Khader & Eleyan, 2021). The damage done by an attack went beyond server outages and flooded websites; it also caused consumers to lose confidence in the service industry (Vishwakarma & Jain, 2020).

Cloud malware injection

The attacker can control the system by injecting malicious malware or launching a virtual computer into the cloud. The attacker acts as a legitimate service by having a virtual machine or as a form of malicious service (Gavra et al., 2020).

Signature wrapping attack

This form of attack exploits a vulnerability in the XML signatures, thus invalidating the digital signature features, such as non-repudiation (Zhao et al., 2020). XML signatures are utilized in the middleware's web services. In a signature wrapping attack, the attacker exploits soap flaws to break the signature algorithm and conduct operations or change eavesdropped messages (Alqallaf, 2021).

SQL injection

This foam of attacks occurs at the SQL queries and updates. This attack occurs due to additional instructions injected into the database's queries,

thus stealing information or altering a change in the database entries (Zhao et al., 2020).

Web browser attack in the cloud

Authentication and authorization requests and other commands can be executed over http/https. Without two-factor authentication, an attacker can access the server via a web browser vulnerability (Roohi et al., 2019).

Application layer

The application layer helps in the delivery of on-demand tasks and services to the user. This layer also processes the network layer's data. Software assaults and lifetime permissions are the principal threats to this layer. These attacks aim to access IoT users' sensitive information, resulting in data confidentiality and privacy violations (Obaidat et al., 2020).

Code injection

This attack involves injecting malicious code into the system by taking advantage of program faults (Chen et al., 2018). The main goal of code injection is to obtain passwords, reveal confidential information, gain system access, steal data, or spread worms to the IoT devices and thus infect others nodes in the system. The most prevalent types of code injection are html and script injections (Obaidat et al., 2020).

Buffer overflow

A buffer overflow also referred to as a buffer overrun, is a type of attack that allows an attacker to write more data into a buffer than the buffer's capacity allows. The real aim is to overwrite the existing data in the buffer with malicious code that will allow them to take control of the entire machine. Stack overflow and global data area overflow are some instances of these assaults. Typically, assembly code is used by the attacker to carry out such an attack. These assaults are designed to compromise a system's integrity and validity. Their influence is "significant," and the likelihood of occurrence is "possible." Secure programming is an effective countermeasure against this attack (Grammatikis et al., 2019).

Sensitive data permission/manipulation

This assault results in the illegal manipulation of sensitive data and the invasion of users' privacy. This type of attack frequently takes advantage of flaws in the recognition model's design (Rahimi et al., 2018).

Phishing attack

The attacker acquires confidential information, such as usernames and passwords (Deogirikar & Vidhate, 2017). The fake website will be spread by online advertising, email, and pop-ups. Suppose customers trust this website and enter their credentials to access their accounts. In that case, they have handed phishers their personal information, and they are led to the main website via a ploy not to doubt the scenario. The fake websites' addresses are similarly identical to the actual site (Ghasemi et al., 2019).

Authentication and authorization

In IoT devices, there is no standardized authentication technique. As a result, no authentication mechanism exists to meet the needs of all types of IoT devices. For example, an attacker may utilize an application update to inject a destructive payload into an IOT device or system to gain access to or control the IoT device or system (Obaidat et al., 2020).

Countermeasures

IoT threats are being explored by researchers all over the world. New methods and solutions are suggested. This section examines the many methodological and inventive approaches used by various researchers to improve IoT security. Tables 1, 2 show how we categorized the solutions depending on layers.

Tables 1, 2 show different types of attacks on each layer and the countermeasures. In addition, as can be seen in the table, security authentication is one of the main ways to prevent most attacks in a multilayer IoT. However, attacks can be initiated on the IoT system based on the layer categories.

In an IoT system, the perception layer is the most vulnerable layer. Attacks are very prevalent in this layer. However, at the network layer, attacks can still occur. At the middle layer, an attacker can easily initiate an attack on the IoT system. The application layer can easily be exploited in the entire IoT system.

With the growth of technology, attackers have devised new sophisticated methods that can be used to attack IoT systems. There is a need for an organization to implement new strategies for protecting the IoT systems due to the ever-evolving nature of technology. IoT security is becoming a significant challenge to any organization due to proper standardization authentication measures. The implemented security strategies are not feasible to one another, which poses a new channel for attackers to target this system. Thus, there is a need for proper standardization for IoT systems. The IoT network nodes don't have the security measures to handle

Table 1. IoT issue attacks and countermeasures at perception and network layer.

Layer	Attack name	Effect	Countermeasures	Threat level	References
Perception layer	Unauthorized access to the tags	Affect system integrity and confidentiality.	RF signal-based reader authentication	Medium to high	Ding et al., 2018; Imdad et al., 2020
	Tag cloning	Affect authenticity.	Blockchain-based mutual authentication security protocol.	Medium to high	Robles & Endencio-Robles, 2019; Wang et al., 2018
	Eavesdropping	Affect user's confidentiality and privacy.	Link-layer encryption, secrecy enhancing technique.	Medium	Burhan et al., 2018; Butun et al., 2020; Hassija et al., 2019
	RF jamming	Prevent readers from communicating with all tags	Spread-spectrum, priority, message, code, spreading, and mode change	Medium	Rahimi et al., 2018
Network layer	Spoofing attack	Gain and have full access to the IoT systems	Authentication	High	Duangphasuk et al., 2020; Kamble & Bhutad, 2018
	Sleep deprivation attack	A power failure and stop functioning	ProEnergy scheme, random vote scheme, round robin scheme, secured duty cycle mechanism, and the hash-based scheme	Medium	Kamble & Bhutad, 2018; Sarma & Barbhuiya, 2019
	DoS attack	The system's network becomes unavailable to users.	RSSI, hop count monitoring scheme, data consistency & network flow information approach with a based scheme.	High	Karlof & Wagner, 2003; Kumar et al., 2016
	Sybil attacks	Attack system by manipulating the node	Monitoring and authentication Using strategies, such as SybilGuard, SybilShield, SybilLimit, SybilDefender, and SyMon Using anonymous Ids.	Medium	Shruthi & Vinay, 2016
	Spoofed routing information attacks	Disrupt the system's seamless communication	Authentication, packet leases, Needham-Schroeder verification protocol, verifying the bidirectionality of a connection.	Medium	Biswas & Ali, 2017; Khattak et al., 2019
	Selective forwarding attacks	Transmits a few messages while dropping	Multi-path routing probe, multi-path routing in combination, braided paths without common node and sequential nodes are used.	Medium	Biswas & Ali, 2017; Khattak et al., 2019; Su et al., 2009
	Sinkhole attacks	Data leakage (data of the nodes)	Procedures for geo-routing, checks for redundancy, fusion center authentication, restriction on routing access, mint route detection, next-hop probabilistic selection.	Medium	Nadeem & Howarth, 2018; Tuan et al., 2020
	Blackhole attack	Significant data loss	TOGBAD based on topology graph for OLSR protocol, sequence check number, adaptive algorithm, AODVSEC.	High	(Park et al., 2018; Prabu et al., 2015)
	Man-in-the-middle attack	Data privacy violation	Point-to-point encryption	High	Ahemd et al., 2017; Shruthi & Vinay, 2016

Table 2. IoT issue attacks and countermeasures at middleware and application layer.

Layer	Attack name	Effect	Countermeasures	Threat level	References
Middleware layer	Flooding attack	Affect reliability, and availability	Client puzzles	Medium to high	Butun et al., 2020; Khader & Eleyan, 2021; Vishwakarma & Jain, 2020
	Cloud malware injection	Can cause illegitimate access to the data	Cloud antivirus	Medium to high	Bedi et al., 2019; Gavra et al., 2020
	Signature wrapping attack	Affect signature algorithm resulting in eavesdropping attack	Encrypted query processing	Low to medium	Alqalaf, 2021; Roohi et al., 2019; Zhao et al., 2020
Application layer	SQL injection	Affect SQL database	Multi-source data analysis	Medium to high	Ross et al., 2018; Zhao et al., 2020
	Web browser attack in the cloud	Data accessed by unauthorized parties	Authentication	Medium	Roohi et al., 2019
	Code injection	Obtain passwords, reveal confidential information, gain system access, steal data, or spread worms	Authentication, regular check for similarity, Testing the system prior installing	High	Duangphasuk et al., 2020; Jha et al., 2021; Obaidat et al., 2020
	Buffer overflow	Compromising a system's integrity and validity.	Secure programming	Medium	Grammatikis et al., 2019
	Sensitive data permission/manipulation	Illegal manipulation of sensitive data and the invasion of users' privacy	Securing the communication channel and encrypting the communication	Medium	Panchal et al., 2018; Rahimi et al., 2018
	Phishing attack	Acquires confidential information, such as usernames and passwords	Authorization, Authentication, and Educating people	High	Deogirikar & Vidhate, 2017; Duangphasuk et al., 2020; Rahimi et al., 2018
	Authentication and authorization	Gain access to or control the IoT device or system	Account locking, Delayed response and multi-factor authentication schemes	Medium	Obaidat et al., 2020; Panchal et al., 2018

complex security algorithms like cryptography. Thus, there is a need to implement algorithms on the low processing devices to counter security threats that might exist in IoT systems.

Conclusion

IoT innovation has had tremendous growth and revolution in the technology world. As with any network technology, it has had its security challenge. Security threats are still very prevalent in IoT systems. These threats have hindered its development from incorporating full-proof security systems. In this report, we have described and outlined the four layers of the IoT system and then highlighted the security threats associated with various layers.

Furthermore, we evaluated the security countermeasures that can be implemented and adopted to prevent and secure the IoT architecture system of any security threats. We also recommended some security measures to enhance and improve the IoT network architecture and make it more secure. There is a need to implement security measures that should play a key role in safeguarding the IoT system to improve its performance, efficiency, and effectiveness.

ORCID

Salim El Khediri  <http://orcid.org/0000-0002-9765-1605>

References

- Ahemd, M. M., Shah, M. A., & Wahid, A. (2017, April). IoT security: A layered approach for attacks & defenses. In *2017 International Conference on Communication Technologies (ComTech)* (pp. 104–110). IEEE. <https://doi.org/10.1109/COMTECH.2017.8065757>
- Alansari, Z., Anuar, N. B., Kamsin, A., Belgaum, M. R., Alshaer, J., Soomro, S., & Miraz, M. H. (2018, August). Internet of things: Infrastructure, architecture, security and privacy. In *2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE)* (pp. 150–155). IEEE. <https://doi.org/10.1109/iCCECOME.2018.8658516>
- Alqallaf, M. (2021). Towards a safe and secure internet of things critical infrastructure. *International Journal of Computer Science and Information Security*, *19*(2).
- Aman, A. H. M., Yadegaridehkordi, E., Attarbashi, Z. S., Hassan, R., & Park, Y. J. (2020). A survey on trend and classification of internet of things reviews. *IEEE Access*, *8*, 111763–111782.
- Aziz, T., & Haq, E.-U. (2018). Security challenges facing IoT layers and its protective measures. *International Journal of Computer Applications*, *179*(27), 31–35. <https://doi.org/10.5120/ijca2018916607>
- Bedi, A., Pandey, N., & Khatri, S. K. (2019, February). Analysis of detection and prevention of malware in cloud computing environment. In *2019 Amity International Conference on*

- Artificial Intelligence (AICAI)* (pp. 918–921). IEEE. <https://doi.org/10.1109/AICAI.2019.8701418>
- Biswas, K., & Ali, M. L. (2017). *Security threats in mobile ad hoc network* [Master thesis]. Department of Interaction and System Design School of Engineering Blekinge Institute of Technology, Sweden.
- Burhan, M., Rehman, R. A., Khan, B., & Kim, B. S. (2018). IoT elements, layered architectures and security issues: A comprehensive survey. *Sensors*, 18(9), 2796. <https://doi.org/10.3390/s18092796>
- Butun, I., Österberg, P., & Song, H. (2020). Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. *IEEE Communications Surveys & Tutorials*, 22(1), 616–644. <https://doi.org/10.1109/COMST.2019.2953364>
- Chen, K., Zhang, S., Li, Z., Zhang, Y., Deng, Q., Ray, S., & Jin, Y. (2018). Internet-of-things security and vulnerabilities: Taxonomy, challenges, and practice. *Journal of Hardware and Systems Security*, 2(2), 97–110. <https://doi.org/10.1007/s41635-017-0029-7>
- Deogirikar, J., & Vidhate, A. (2017, February). Security attacks in IOT: A survey. In *2017 International Conference on IOT in Social, Mobile, Analytics and Cloud (I-SMAC)* (pp. 32–37). IEEE.
- Ding, H., Han, J., Zhang, Y., Xiao, F., Xi, W., Wang, G., & Jiang, Z. (2018, April). Preventing unauthorized access on passive tags. In *IEEE INFOCOM 2018-IEEE Conference on Computer Communications* (pp. 1115–1123). IEEE.
- Duangphasuk, S., Duangphasuk, P., & Thammarat, C. (2020, June 20). Review of internet of things (IoT): security issue and solution. In *2020 17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)* (pp. 559–562). IEEE. <https://doi.org/10.1109/ECTI-CON49241.2020.9157904>
- Frustaci, M., Pace, P., Aloï, G., & Fortino, G. (2018). Evaluating critical security issues of the IOT world: present and future challenges. *IEEE Internet of Things Journal*, 5(4), 2483–2495. <https://doi.org/10.1109/JIOT.2017.2767291>
- Gavra, V. D., Dobra, I. M., & Pop, O. A. (2020, May). A survey on threats and security solutions for IOT. In *2020 43rd International Spring Seminar on Electronics Technology (ISSE)* (pp. 1–5). IEEE. <https://doi.org/10.1109/ISSE49702.2020.9120977>
- Ghasemi, M., Saadaat, M., & Ghollasi, O. (2019). Threats of social engineering attacks against security of internet of things (IOT). In *Fundamental research in electrical engineering* (pp. 957–968). Springer.
- Grammatikis, P. I. R., Sarigiannidis, P. G., & Moscholios, I. D. (2019). Securing the internet of things: challenges, threats and solutions. *Internet of Things*, 5, 41–70. <https://doi.org/10.1016/j.iot.2018.11.003>
- Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IOT security: Application areas, security threats, and solution architectures. *IEEE Access*, 7, 82721–82743. <https://doi.org/10.1109/ACCESS.2019.2924045>
- Imdad, M., Jacob, D. W., Mahdin, H., Baharum, Z., Shaharudin, S. M., & Azmi, M. S. (2020). Internet of things (IOT); Security requirements, attacks and counter measures. *Indonesian Journal of Electrical Engineering and Computer Science*, 18(3), 1520–1530. <https://doi.org/10.11591/ijeecs.v18.i3.pp1520-1530>
- Javaid, M., & Khan, I. H. (2021). Internet of things (IOT) enabled healthcare helps to take the challenges of covid-19 pandemic. *Journal of Oral Biology and Craniofacial Research*, 11(2), 209–214.

- Jha, R., Kour, K., Kumar, H., & Jain, M. (2021). Layer based security in narrow band Internet of Things (NB-IoT). *Computer Networks*, 185, 107592. <https://doi.org/10.1016/j.comnet.2020.107592>
- Kamble, A., & Bhutad, S. (2018, January). Survey on internet of things (IOT) security issues & solutions. In *2018 2nd International Conference on Inventive Systems and Control (ICISC)* (pp. 307–312). IEEE. <https://doi.org/10.1109/ICISC.2018.8399084>
- Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks*, 1(2–3), 293–315. [https://doi.org/10.1016/S1570-8705\(03\)00008-8](https://doi.org/10.1016/S1570-8705(03)00008-8)
- Khader, R., & Eleyan, D. (2021). Survey of DoS/DDoS attacks in IOT. *Sustainable Engineering and Innovation*, 3(1), 23–28. <https://doi.org/10.37868/sei.v3i1.124>
- Khanna, A., & Kaur, S. (2019). Evolution of Internet of Things (IoT) and its significant impact in the field of precision agriculture. *Computers and Electronics in Agriculture*, 157, 218–231. <https://doi.org/10.1016/j.compag.2018.12.039>
- Khattak, H. A., Shah, M. A., Khan, S., Ali, I., & Imran, M. (2019). Perception layer security in internet of things. *Future Generation Computer Systems*, 100, 144–164. <https://doi.org/10.1016/j.future.2019.04.038>
- Kumar, S. A., Vealey, T., & Srivastava, H. (2016, January). Security in internet of things: Challenges, solutions and future directions. In *49th Hawaii International Conference on System Sciences (HICSS)* (pp. 5772–5781). IEEE. <https://doi.org/10.1109/HICSS.2016.714>
- Masoodi, F., Alam, S., & Siddiqui, S. T. (2019). Security & privacy threats, attacks and countermeasures in Internet of Things. *International Journal of Network Security & Its Applications*, 11(02), 67–77. <https://doi.org/10.5121/ijnsa.2019.11205>
- Nadeem, A., & Howarth, M. P. (2018). A survey of MANET intrusion detection & prevention approaches for network layer attacks. *IEEE Communications Surveys & Tutorials*, 15(4), 2027–2045.
- Obaidat, M. A., Obeidat, S., Holst, J., Al Hayajneh, A., & Brown, J. (2020). A comprehensive and systematic survey on the internet of things: security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. *Computers*, 9(2), 44. <https://doi.org/10.3390/computers9020044>
- Ogonji, M. M., Okeyo, G., & Wafula, J. M. (2020). A survey on privacy and security of internet of things. *Computer Science Review*, 38, 100312. <https://doi.org/10.1016/j.cosrev.2020.100312>
- Panchal, A. C., Khadse, V. M., & Mahalle, P. N. (2018). Security issues in IIoT: A comprehensive survey of attacks on IoT and its countermeasures. In *2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)* (pp. 124–130). IEEE.
- Park, S., Al-Shurman, M., & Yoo, S.-M. (2018, April). Black hole attack in mobile *ad hoc* network. In *ACMSE'04*, Huntsville, AL, USA.
- Prabu, M., Rani, S., Kumar, R., & Venkatesh, P. (2015). dos attacks and defenses at the Network layer in *ad-hoc* and sensor wireless networks, wireless *ad-hoc* sensor networks: a short survey. *European Journal of Applied Science*, 7(2), 80–85.
- Rahimi, H., Zibaenejad, A., Rajabzadeh, P., & Safavi, A. A. (2018, September). On the security of the 5g-IOT architecture. In *Proceedings of the International Conference on Smart Cities and Internet of Things* (pp. 1–8). <https://doi.org/10.1145/3269961.3269968>
- Robles, R. J., & Endencio-Robles, D. (2019). State of internet of things (IOT) security attacks, vulnerabilities and solutions. *Computer Reviews Journal*, 3, 255–263.
- Roohi, A., Adeel, M., & Shah, M. A. (2019, September). DDoS in IOT: A roadmap towards security & countermeasures. In *2019 25th International Conference on Automation and Computing (ICAC)* (pp. 1–6). IEEE. <https://doi.org/10.23919/ICAC.2019.8895034>

- Ross, K., Moh, M., Moh, T. S., & Yao, J. (2018, March). Multi-source data analysis and evaluation of machine learning techniques for SQL injection detection. In *Proceedings of the ACMSE 2018 Conference* (pp. 1–8). <https://doi.org/10.1145/3190645.3190670>
- Sarma, R., & Barbhuiya, F. A. (2019, June). Internet of Things: Attacks and defences. In *2019 7th International Conference on Smart Computing & Communications (ICSCC)* (pp. 1–5). IEEE. <https://doi.org/10.1109/ICSCC.2019.8843649>
- Shruthi, N., & Vinay, C. K. (2016). Network layer attack: Analysis & solutions a survey. *IOSR Journal of Computer Engineering*, 18(2), 67–80.
- Su, K., Wang, W., & Chang, W. (2009). Detecting Sybil attacks in wireless sensor networks using neighboring information. *Computer Networks*, 53(18), 3042–3056. <https://doi.org/10.1016/j.comnet.2009.07.013>
- Tuan, T. A., Long, H. V., Son, L. H., Kumar, R., Priyadarshini, I., & Son, N. T. K. (2020). Performance evaluation of Botnet DDoS attack detection using machine learning. *Evolutionary Intelligence*, 13(2), 283–294. <https://doi.org/10.1007/s12065-019-00310-w>
- Vishwakarma, R., & Jain, A. K. (2020). A survey of DDoS attacking techniques and defence mechanisms in the IOT network. *Telecommunication Systems*, 73(1), 3–25. <https://doi.org/10.1007/s11235-019-00599-z>
- Wang, S., Zhu, S., & Zhang, Y. (2018, June). Blockchain-based mutual authentication security protocol for distributed RFID systems. In *2018 IEEE Symposium on Computers and Communications (ISCC)* (pp. 00074–00077). IEEE. <https://doi.org/10.1109/ISCC.2018.8538567>
- Zhao, W., Yang, S., & Luo, X. (2020, August). On threat analysis of IOT-based systems: A survey. In *2020 IEEE International Conference on Smart Internet of Things (smartIOT)* (pp. 205–212). IEEE. <https://doi.org/10.1109/SmartIoT49966.2020.00038>