STAP
Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions

Almaha Adel Almuqren [1]

[1] *Department of Computer Networks and Communications, King Faisal University, Al-Ahsa 31982, Saudi Arabia*

ARTICLE INFO

Article History

Received 03 Jan 2025
Accepted 20 Jan 2025
Published 22 Jan 2025

Academic Editor:

Mohammed Almaiah

Vol.2025, No.1

DOI:
https://doi.org/10.63180/jcsra.thestap.2025.1.1

ABSTRACT

The Internet of Things (IoT) has gotten a lot of interest from the information and communication technology community. The availability of tools afforded by this paradigm, such as environmental monitoring using user data and everyday items, is one of the key reasons. In addition, the IoT infrastructure's capabilities enable the creation of a wide range of new business models and applications such as smart homes, smart cities and e-health. However, there are still concerns over the security issues that need addressing to ensure an appropriate deployment. With the increasing threat of cyber-attacks, cybersecurity has emerged as one of the most critical aspects on the IoT. IoT cybersecurity aims to secure IoT assets and privacy while lowering cybersecurity risks for enterprises and consumers. In addition, new cybersecurity tools and technology have the potential to improve IoT security management. This paper aims to provide a comprehensive analysis of the classification of cyber threats, attacks in IoT layers. The study's findings show that viruses, spyware and malware attacks were the most prevalent technical threats in IoT application layer, each accounting for 30% of incidents. Malicious code attacks were identified as the second rank of main threats and attacks that representing 20% of incidents. While, phishing attacks was identified as the third level of main threats and attacks that representing 15% of incidents. In fourth classification was cross-site scripting and Botnet attacks, with 10% of incidents in IoT application layer. The results from this research could help organizations in understanding the main types of cyber-attacks in IoT applications in order to develop robust methods against these types of these attacks.

Keywords: Internet of Things (IoT); Cybersecurity; Cyber-attacks; IoT Assets and Threats.

How to cite the article

Almuqren, A. A. (2025). Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions. Journal of Cyber Security and Risk Auditing, 1(1), 1–11. https://doi.org/10.63180/jcsra.thestap.2025.1.1

1. Introduction

IoT is a concept that arises in the vast ecosystem of the infrastructure of interconnected networks of physical and virtual objects that process and exchange collect data in different contexts. IoT infrastructure is linked and interconnected using either wired or wireless networks to share information between various IoT devices, creating novel applications and services in the infrastructure to enhance service delivery in different environments. IoT allows various gadgets and appliances such as televisions, air conditioners, and washing machines to connect to the Internet. Several applications in IoT such as

*Corresponding author. Email: 222402223@student.kfu.edu.sa

healthcare, agriculture, traffic monitoring, energy conservation, water supply and etc. There are several advantages of IoT infrastructure as service efficiency and cost savings on a large scale. IoT is one of the prominent emerging technologies for delivering Value-added services to end-users. While, the disadvantage of these data-driven environments is a network connectivity, which targets cyber threats and risks. According to a study [1] the basic IoT structure is a 3-layer architecture. This structure involves the application, network, and perception layers. A study [2] each layer experiences threats depending on its functional characteristics and connectivity to the end-user.

IoT has several security issues that rely on many different factors, including heterogeneity of IoT devices because they have different hardware and software limitations [3], heterogeneity of communication protocols [4], vulnerabilities in deployment environments range from intelligent homes [5] to critical infrastructures that rely on a large scale and remote services in the cloud [6]. Analysis of security issues affecting IoT systems is the objective of many surveys [7], [8], [9] which highlighted that the most important factors are: (i) the need to constantly adapt to the environment and (ii) design and manage systems by taking into account the security and capacity of each device, which may affect the overall security level of the structure. Cyber risk assessment in IoT is performing by several methods such as quantitative, qualitative and delphi methods. Existing critical IoT infrastructures and systems are much more complex, which causes new risks [10]. Moreover, cyber risks and threats in IoT may extend to many critical IT infrastructure entities. The interruption of services provided by a smart network or a smart city may also affect the IoT system's threat, modeling, and risk analysis processes. Therefore, risk analysis and assessment methodology aims to identify the critical assets to be protected, their current vulnerabilities and related threats and suitable countermeasures to mitigate these risks. In this study, we conduct a review analysis to achieve the following objective:

(1) To determine the common types of threats and attacks in three layers of IoT.

2. Literature Review

2.1 IoT Architecture

In this study, we focused on three layers of IoT architecture including application layer, network layer and perception layer as shown in Figure 1. IoT has several security issues, which can divided based on the type of layer in IoT. In the sections below, we provided a review on the common types of security issues on three types of IoT architecture including application layer, network layer and perception layer.

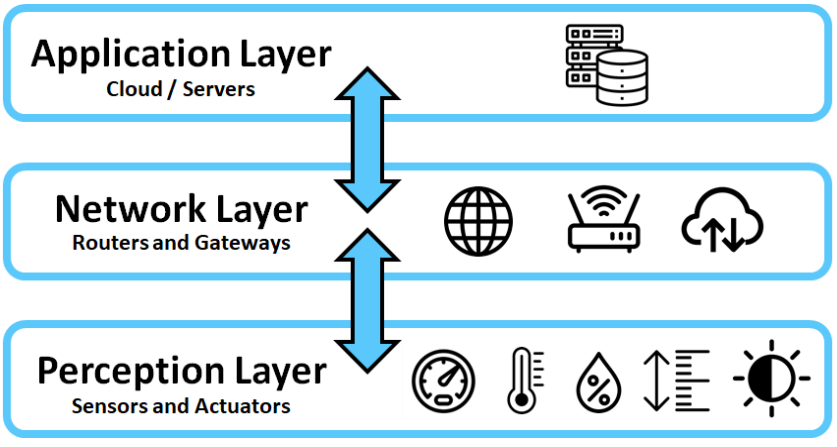


Figure 1. IoT architecture with 3-layers.

(A) Application layer

According to [11], application layer is responsible for delivering different services depending on the information stored on different servers for different applications such as smart health, smart cities, and smart homes. There are common problems

and security threats in application layer including cross-site scripting, SQL injections, HTTP floods, Slowloris attacks, and parameter tampering. Organizations use secure web gateway services and web application firewalls to enhance their application layer security systems [12]. One of the most common attack on application layer is a define cross-site scripting as an injection attack where attackers insert client-side scripts that completely alter the content of the applications made depending on their motives [13]. A malicious code attack is another form of attack where codes are used in different parts of the software to cause damage to certain systems. This attack is particularly troublesome because it cannot be controlled or blocked through anti-virus tools [14]. Moreover, it is often designed as a program that needs users' trigger to perform particular actions or programs that activity themselves [15].

(B) Network layer

Network layer encounters numerous attacks because it transmits information from physical objects through wire-based or wireless networks. One of these attacks is Denial of Service (DoS) attack is an active attack that hamper authentic users from accessing network resources or other devices. It is often accomplished through the flooding of network resources or targeted devices with redundant requests that make it impossible or difficult for authentic users to use their devices [16]. IP spoofing is another common attack in the network layer, which is used to obtain unauthorized access to servers. Attackers use trusted IP addresses to prevent the server from identifying the attacker's presence on its network. IP spoofing can also carry out other attacks such as non-blind spoofing, Man-in-the-middle attacks, and blind spoofing. The attacker's use of trusted IP addresses is one of the techniques that makes it difficult to address these cybercrime activities because servers cannot identify that it is not the authorized user but an attacker who is using the trusted IP address to access information [17]. [18] Identify the man-in-The-Middle (MiTM) attack as a passive attack technique. This is one where attackers alter communications between senders and receivers who presume that they are communicating with each other directly. These secret interceptions enable attackers to alter messages according to their needs or perceptions. In passive attacks, attackers only spy on the information sent without interruptions in the communications between the senders and the receivers of information [19].

Other attacks that can occur on the network layer are exploit and storage attacks. Storage attacks are passive attacks that involve hacking information stored in the cloud or many different devices. This information can then be altered to serve the attacker's intentions. Attackers also replicate the information they acquire, increasing the chances of attacks occurring in the future [20]. Exploit attacks are illegal attacks in command sequences, data chunks, or software. [21] Define this attack as one that involves stealing stored information and obtaining control of these systems. These attacks exploit existing security vulnerabilities in hardware, systems, or different applications. Therefore, extensive research on suitable security approaches is needed for securing the information utilized in IoT network layer [22].

(C) Perception Layer

A study by [23] confirmed common attacks in the perception layer includes replay attacks, fake node and malicious, node capture, eavesdropping, and timing attacks. Timing attacks enable attackers to identify vulnerabilities and obtain the secrets stored in a security system by observing the period it takes for systems to respond to cryptographic or input algorithms [24]. [25] Define replay attacks are those where intruders eavesdrop on information between senders and receivers. The intruder then uses the sender's information to convince the receiver to take certain actions under the pretenses of being the authentic sender [26]. In a study by [27] define fake nodes and malicious attacks as those that involve actions where attackers add nodes into systems and make fake data inputs. The major purpose of this form of attack is usually to stop the transmission of real information. In addition, the nodes added by malicious attackers destroy networks because they consume the energy that the real nodes use to function. Node capture attacks involve techniques such as using gateway nodes where attackers fully capture control over key nodes [28]. These nodes contribute to information leaks between senders and receivers of secure information. [29] Define eavesdropping as an attack in the perception layer where attackers intercept video conferences, fax transmissions, text messages, and phone calls. Attackers go after private communications to steal private information. The information collected through these techniques leads to major losses primarily because of the ability of attackers to access sensitive information [30]. Therefore, it is vital for IoT structure developers in different organizations to conduct extensive research on the most suitable security systems they should utilize for protecting perception layer.

2.2 Cyber Attacks on IoT

(A) Malicious Code Injection Attack

The attacker attacks a node by physically infiltrating it with malicious code, which allows the attacker to seize control of the IoT network. For example, consider an attacker dropping malicious code (a virus) on specific nodes; this would allow the attacker to take control of the entire system [31]. The malicious code causes problems to particular nodes, but it may also provide the attacker access to the whole IoT network.

(B) Phishing attack

Sensitive information can be obtained by an attacker using an infected email or website to impersonate the user's confirming identity. It refers to the theft of user data such as usernames and passwords, credit card information, and other bank details to steal money from bank accounts and commit other crimes [32]. In addition, phishers can deceive legitimate people by sending spam emails or launching fake websites.

(C) Spyware and Worms

Computer viruses, spyware, ransomware, Trojan horses, worms, adware, rootkits, and other harmful programs are classified as malicious software. The functioning of the IoT device might be harmed by malicious malware. Malware on an IoT (Medical) device can compromise the system's confidentiality, integrity, availability, and performance [33].

(D) Denial-of-Service (DoS) attack

The most prevalent networking attack; disables network resources and services for users by flooding the networking protocol or IoT system with traffic [34]. Land Attack, Ping of Death instructions, TearDrop, UDP flood packets, SYN flood, and other attacking techniques can all be used to produce DoS attacks.

(E) Sinkhole attack

The attacker sent all signals from wireless sensor network nodes to an unaltered point. In this attack, the attacker attempts to collect network traffic in a specific region and damage data at that location. As a result, the integrity and trustworthiness of data transit by nodes are violated [35].

(F) Man-in-Middle attack

The attacker in this assault does not need to physically arrive at a network's location; instead, he utilizes the IoT communication protocol to interfere with two sensor nodes to get classified information. In most Man-In-The-Middle (MITM) assaults, a third party or unauthorized individual sits in the middle of two authorized parties. The attacker establishes separate connections with each party and leads them to believe they are communicating [36]. Man-in-the-middle attacks aim to disrupt a network by breaching security principles such as confidentiality, integrity, and availability of sensitive data. Figure 2 summarizes the common attacks in IoT.

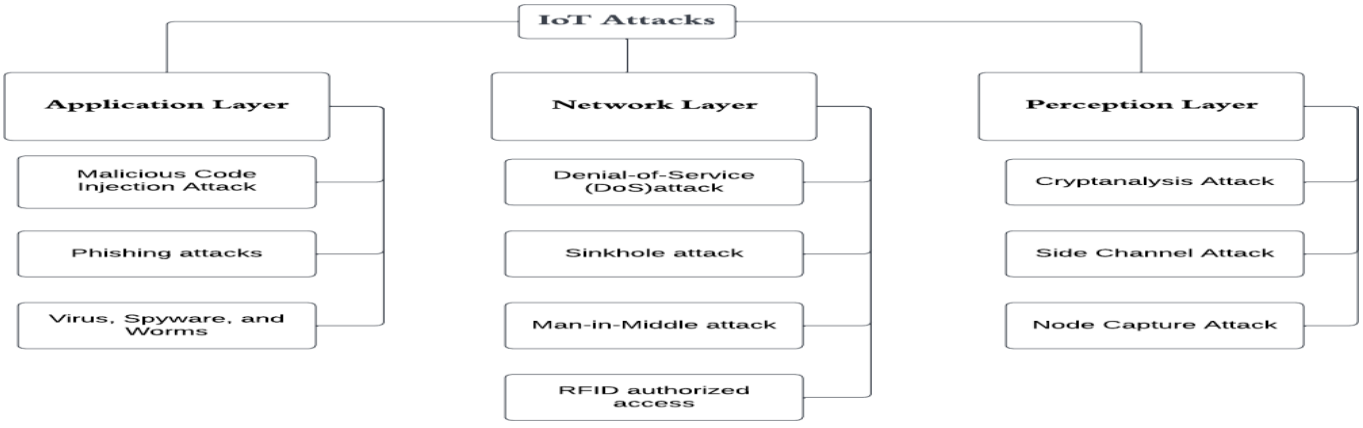


Figure 2. The common attacks in IoT.

3. Research Methodology

In this study, to achieve the research objectives, we used a Systematic Literature Review (SLR) as shown in Figure 3. A systematic literature review is one of the research methodologies used. It helps write research by identifying, selecting, and critically assessing all results from all studies that answer the research questions. This study used the PRMISA flow diagram to create our systematic review.

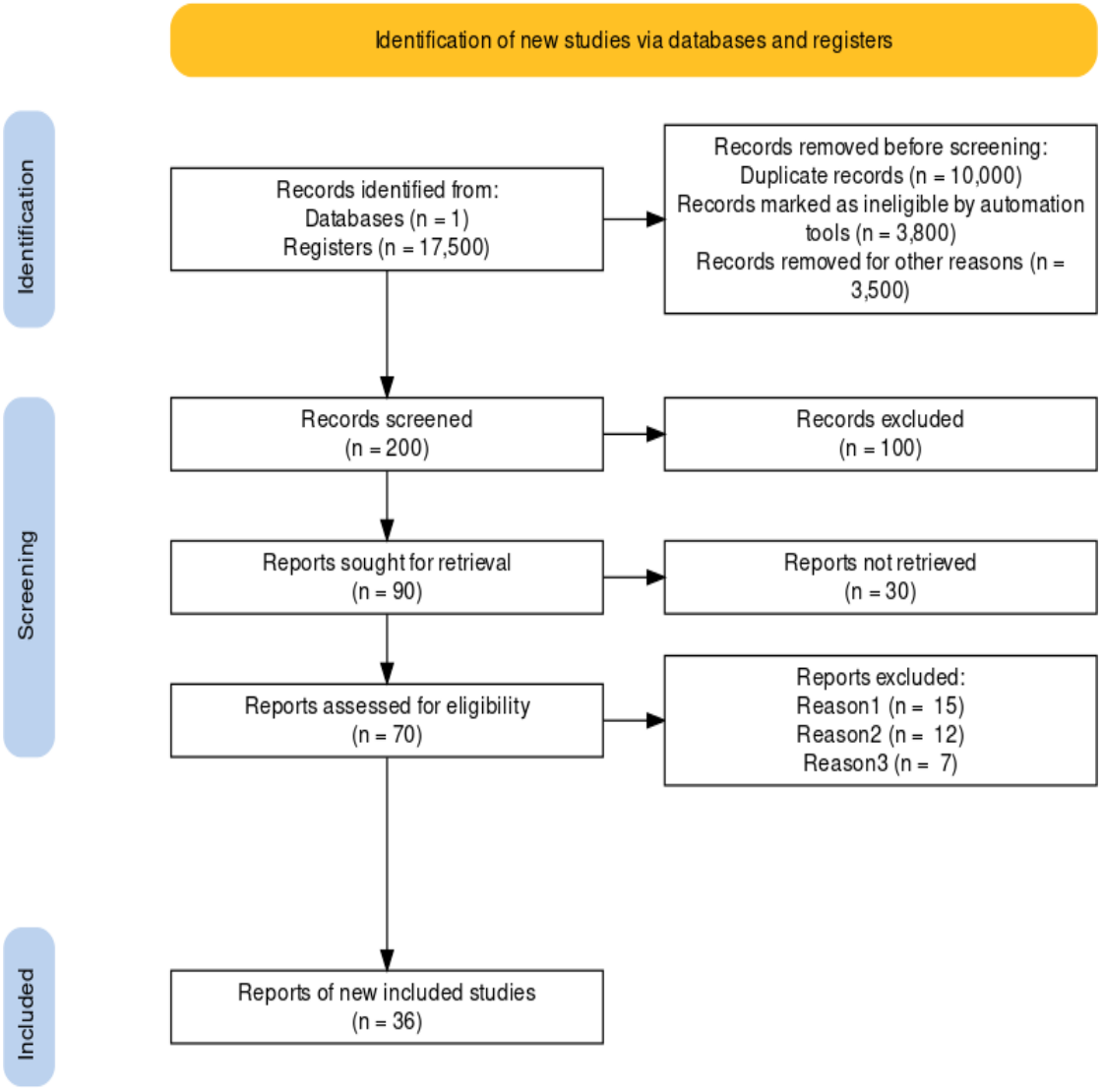


Figure 3. PRMISA methodology.

4. Analysis and Findings

As we mentioned in the preceding section, we analyzed the main threats in IoT based on three layers of IoT architecture including application layer, network layer and perception layer.

4.1 Findings of Classification of Threats and Attacks in Application Layer

Based on the analysis of the literature review, we categorized cyber threats and attacks in application layer of IoT into technical threats, as presented in Table 1. The main technical attacks and threats include several malware types that exploit vulnerabilities in the application layer protocols, services and functions including Malicious Code Attacks, Cross-Site Scripting Attack, Botnet, SQL injection, Mirai malware, Buffer Overflow, Viruses and Malware Attack.

Table 1. Classification of Threats and Attacks in Application Layer

Layer	Type of threats and attacks	Description
Application layer	Malicious Code Attacks [7], [6]	Attacks through running malicious codes.
	Cross-Site Scripting Attack [8]	Attacker runs malicious codes on the web browser of the victim by adding malicious code on legitimate websites thus allowing him to tamper the application.
	Botnet [9]	The hacker hijacks network of devices by Botnet and can control them from a single access point.
	SQL injection [3]	Logging into the IOT device using an SQL script.
	Mirai malware[30]	Using a default Telnet or SSH account, get access to an IoT device.
	Buffer Overflow[23]	That additional data spills into nearby memory regions, corrupting or overwriting the data there.
	Viruses, Malware Attack[25]	Malware is a type of cyberattack in which the malware performs illegal operations on the victim's computer.
	They are infecting the LINUX operating system of an IoT device by forcing the Telnet port.	They are infecting the LINUX operating system of an IoT device by forcing the Telnet port.
	Ransomware is an extortion method in which attackers take control of a victim's computer files and encrypt them, then demand a ransom to restore the data to their original state.	Ransomware is an extortion method in which attackers take control of a victim's computer files and encrypt them, then demand a ransom to restore the data to their original state.
	Interruption assaults render our assets useless or inaccessible to us, either temporarily or permanently.	Interruption assaults render our assets useless or inaccessible to us, either temporarily or permanently.
	Untrusted data transmit an interpreter as part of a command or query.	Untrusted data transmit an interpreter as part of a command or query.
	Malicious Code Injection Attack [15]	Malicious code is frequently written to manipulate data flow, resulting in data loss and diminished application availability.

Figure 4 shows the analysis results of cyber threats and attacks classifications for IoT application layer. The findings reveal that viruses, spyware and malware attacks were the most prevalent technical threats in IoT application layer, each accounting for 30% of incidents. Malicious code attacks were identified as the second rank of main threats and attacks that representing 20% of incidents. While, phishing attacks was identified as the third level of main threats and attacks that representing 15% of incidents. In fourth classification was cross-site scripting and Botnet attacks, with 10% of incidents in IoT application layer.

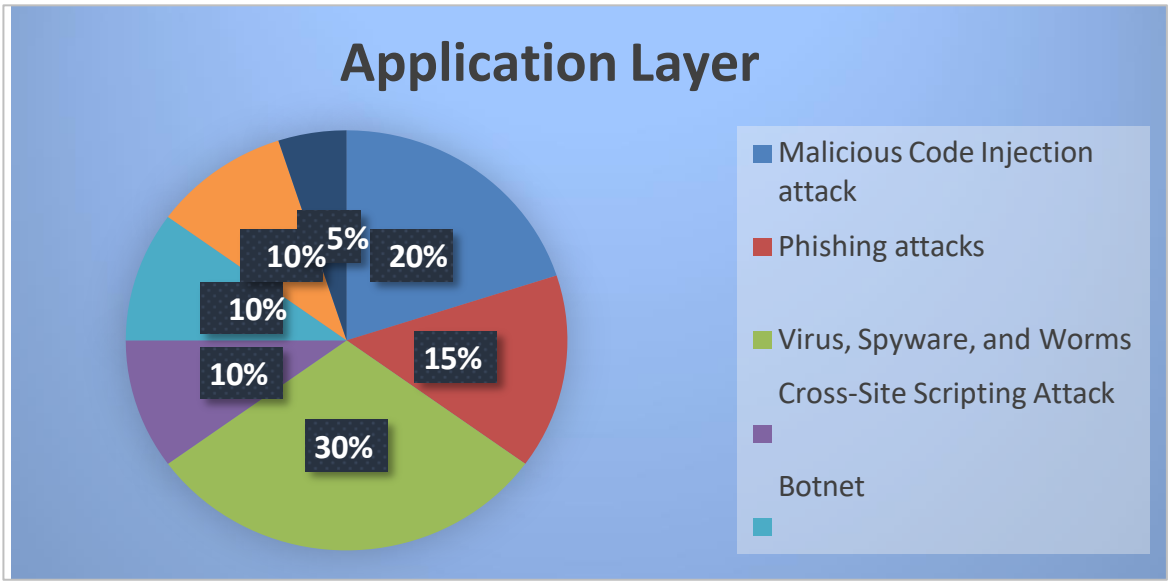


Figure 4. Findings of Classification of Threats and Attacks in Application Layer

4.2 Findings of Classification of Threats and Attacks in Network Layer

Based on the analysis of the literature review, we categorized cyber threats and attacks in network layer of IoT into technical threats, as presented in Table 2. The main technical attacks and threats include several malware types that exploit vulnerabilities in the network layer protocols, services and functions including Denial of Service, Replay, Spoofing attacks, Man-in the Middle attack, Selective forwarding and Sybil attacks.

Table 2. Classification of Threats and Attacks in Network Layer

Layer	Type of threats and attacks	Description
Network layer	Denial of Service [14]	Preventing a network resource from being used for its intended purpose. This attack floods the network with requests, causing it to crash and become unusable even for authorized users.
	Replay [20]	Reorder the data packets and manipulate the message stream.
	Spoofing attacks [21]	When an attacker impersonates an authorized device or user in order to steal data, spread malware, or get around access control systems, this is known as spoofing.
	Man-in the Middle Attack [10]	The attacker obstructs communication while impersonating the sender, leading the receiver to believe the contact came from the genuine sender.
	Selective forwarding [27]	An attacker, acting as a regular node in the routing process, discards packets from surrounding nodes selectively.
	Sybil Attack [30]	The attacker subverts the reputation system by generating many pseudonymous identities and using them to wield disproportionately enormous power.

Figure 5 presents the analysis results of cyber threats and attacks classifications for IoT network layer. The findings reveal that Denial of Service and Replay attacks were the most prevalent technical threats in IoT network layer, each accounting for 36% of incidents. Man-in the Middle attack attacks was identified as the second rank of main threats and attacks that

representing 27% of incidents. While, Selective forwarding and Sybil attacks were identified as the third level of main threats and attacks that representing 9% of incidents. In fourth classification was sinkhole attacks, with 7% of incidents in IoT network layer.

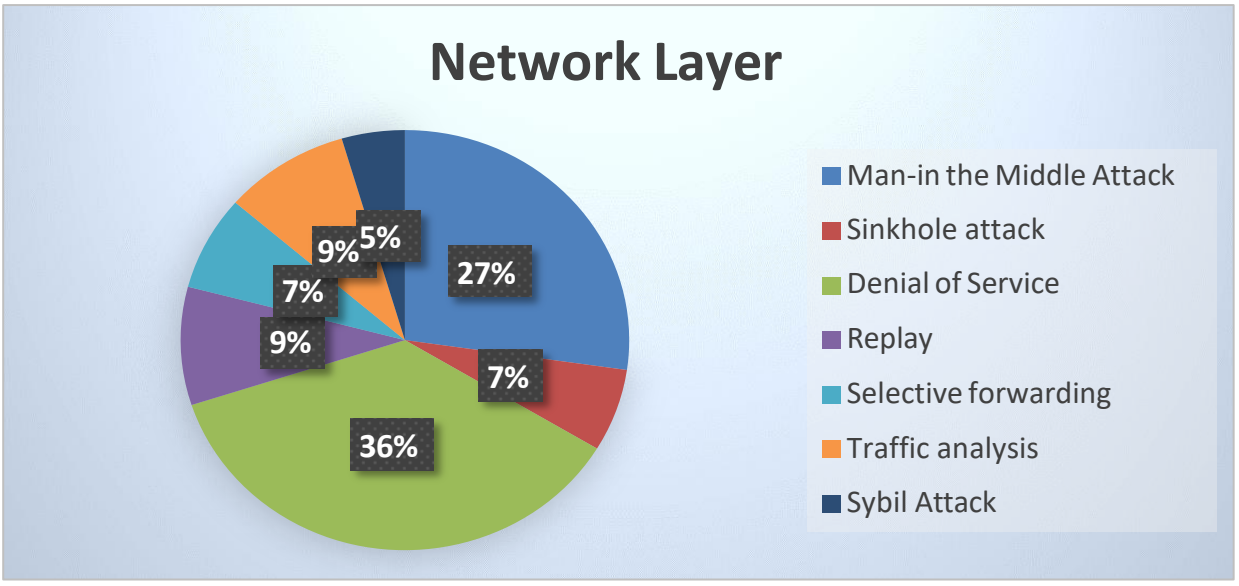


Figure 5. Findings of Classification of Threats and Attacks in Network Layer

4.2 Findings of Classification of Threats and Attacks in Perception Layer

Based on the analysis of the literature review, we categorized cyber threats and attacks in perception layer of IoT into technical threats, as presented in Table 3. The main technical attacks and threats include several malware types that exploit vulnerabilities in the perception layer protocols, services and functions including eavesdropping attack, node tempering, cyber-physical attack, sensor tracking, unauthorized access, and Storage access attack, Jamming attacks, replay Attack and node capture attack.

Table 3. Classification of Threats and Attacks in Perception Layer

Layer	Type of threats and attacks	Description
Perception layer	Eavesdropping [28]	Infer data transmitted across the network by IoT devices
	Node Tempering [16]	Node manipulation is a standard attack scenario when sensor nodes are geographically dispersed and unsupervised.
	Cyber-physical [18]	Attacking a device physically
	sensor tracking [37]	Laser light is exceptionally adequate for tracking and detecting an object far away.
	Unauthorized access [11]	Anyone may connect to the IoT gadget through the internet.
	Storage access attack [13]	Accessing the cloud storage where all information of the device is being stored. This can lead to manipulated results by the device.
	Jamming Attacks[3]	The transmission of radio signals that cause communications to be disrupted by lowering the Signal-to-Interference-plus-Noise ratio (SNR)
	Replay Attack	The attacker intercepts and stores information transferred over the network, which he may then send later.

Node Capture [15]	The attacker gains complete control of the primary node, such as the gateway. It has the potential to create a malicious node or leak all of the information in the node [5].

Figure 6 presents the analysis results of cyber threats and attacks classifications for IoT perception layer. The findings reveal that node capture attack attacks was the most prevalent technical threats in IoT perception layer, each accounting for 40% of incidents. Node tempering attacks was identified as the second rank of main threats and attacks that representing 27% of incidents. While, eavesdropping attack attacks was identified as the third level of main threats and attacks that representing 11% of incidents. In fourth classification was cyber-physical attacks, with 7% of incidents in IoT perception layer.

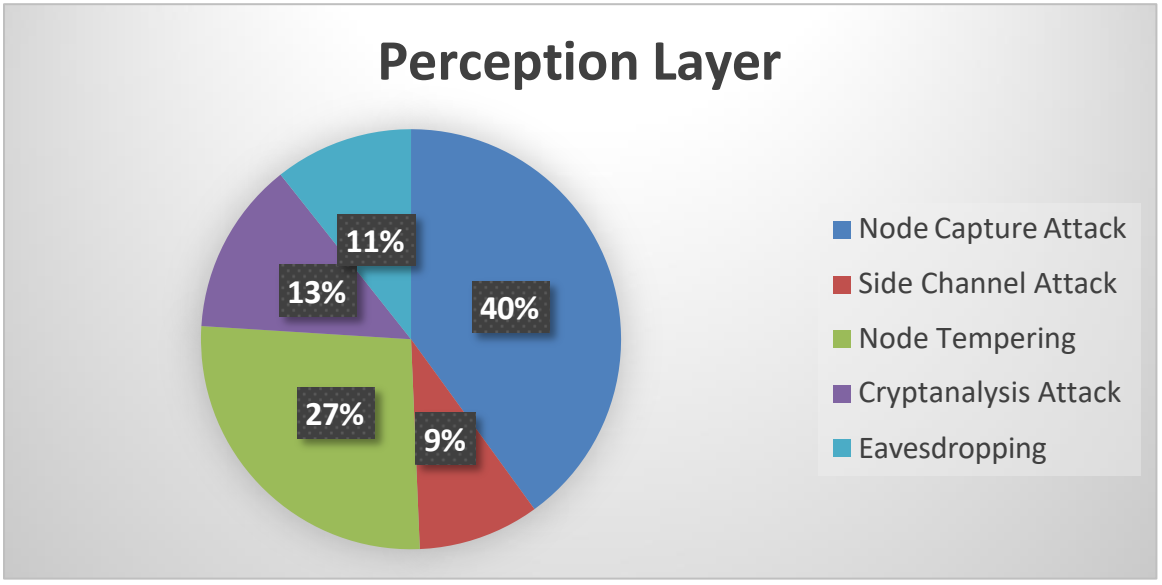


Figure 6. Findings of Classification of Threats and Attacks in Perception Layer

5. Conclusion

This paper aimed to provide a comprehensive analysis of the classification of cyber threats, attacks in IoT layers. The results from this research could help organizations in understanding the main types of cyber-attacks in IoT applications in order to develop robust methods against these types of these attacks. The study's findings showed that viruses, spyware and malware attacks were the most prevalent technical threats in IoT application layer, each accounting for 30% of incidents. Malicious code attacks were identified as the second rank of main threats and attacks that representing 20% of incidents. While, phishing attacks was identified as the third level of main threats and attacks that representing 15% of incidents. In fourth classification was cross-site scripting and Botnet attacks, with 10% of incidents in IoT application layer. The study's findings also presented that Denial of Service and Replay attacks were the most prevalent technical threats in IoT network layer, each accounting for 36% of incidents. Man-in the Middle attack attacks was identified as the second rank of main threats and attacks that representing 27% of incidents. While, Selective forwarding and Sybil attacks were identified as the third level of main threats and attacks that representing 9% of incidents. In fourth classification was sinkhole attacks, with 7% of incidents in IoT network layer. In perception layer, the study's findings showed that node capture attack attacks was the most prevalent technical threats in IoT perception layer, each accounting for 40% of incidents. Node tempering attacks was identified as the second rank of main threats and attacks that representing 27% of incidents. While, eavesdropping attack attacks was identified as the third level of main threats and attacks that representing 11% of incidents. In fourth classification was cyber-physical attacks, with 7% of incidents in IoT perception layer.

Conflicts Of Interest

The author declares no conflicts of interest.

Funding

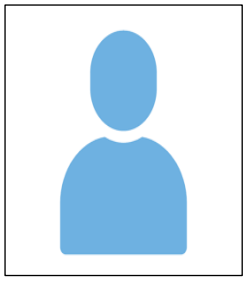
No funding.

Acknowledgment

References

[1] Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of things Journal*, *4*(5), 1250-1258.
[2] Rejeb, A., Rejeb, K., Treiblmaier, H., Appolloni, A., Alghamdi, S., Alhasawi, Y., & Iranmanesh, M. (2023). The Internet of Things (IoT) in healthcare: Taking stock and moving forward. *Internet of Things*, *22*, 100721.
[3] Sengupta, J., Ruj, S., & Bit, S. D. (2020). A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *Journal of network and computer applications*, *149*, 102481.
[4] 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.
[5] Dai, H. N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. *IEEE internet of things journal*, *6*(5), 8076-8094.
[6] Farooq, M. S., Riaz, S., Abid, A., Abid, K., & Naeem, M. A. (2019). A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming. *Ieee Access*, *7*, 156237-156271.
[7] Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer networks*, *148*, 283-294.
[8] Khraisat, A., & Alazab, A. (2021). A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity*, *4*, 1-27.
[9] Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, *38*, 8-27.
[10] Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., & Arshad, H. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. *Computers & Security*, *112*, 102494.
[11] Mohanta, B. K., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet of Things*, *11*, 100227.
[12] Rana, M., Mamun, Q., & Islam, R. (2022). Lightweight cryptography in IoT networks: A survey. *Future Generation Computer Systems*, *129*, 77-89.
[13] Ravi, N., & Shalinie, S. M. (2020). Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture. *IEEE Internet of Things Journal*, *7*(4), 3559-3570.
[14] Lee, E., Seo, Y. D., Oh, S. R., & Kim, Y. G. (2021). A Survey on Standards for Interoperability and Security in the Internet of Things. *IEEE Communications Surveys & Tutorials*, *23*(2), 1020-1047.
[15] Mohanta, B. K., Jena, D., Ramasubbareddy, S., Daneshmand, M., & Gandomi, A. H. (2020). Addressing security and privacy issues of IoT using blockchain technology. *IEEE Internet of Things Journal*, *8*(2), 881-888.
[16] 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.
[17] Kumar, R. L., Khan, F., Kadry, S., & Rho, S. (2022). A survey on blockchain for industrial internet of things. *Alexandria Engineering Journal*, *61*(8), 6001-6022.
[18] Rao, P. M., & Deebak, B. D. (2023). Security and privacy issues in smart cities/industries: technologies, applications, and challenges. *Journal of Ambient Intelligence and Humanized Computing*, *14*(8), 10517-10553.
[19] Sharma, P., Jain, S., Gupta, S., & Chamola, V. (2021). Role of machine learning and deep learning in securing 5G-driven industrial IoT applications. *Ad Hoc Networks*, *123*, 102685.
[20] Santhosh Kumar, S. V. N., Selvi, M., & Kannan, A. (2023). A Comprehensive Survey on Machine Learning-Based Intrusion Detection Systems for Secure Communication in Internet of Things. *Computational Intelligence and Neuroscience*, *2023*(1), 8981988.
[21] Younan, M., Houssein, E. H., Elhoseny, M., & Ali, A. A. (2020). Challenges and recommended technologies for the industrial internet of things: A comprehensive review. *Measurement*, *151*, 107198.
[22] Yugha, R., & Chithra, S. (2020). A survey on technologies and security protocols: Reference for future generation IoT. *Journal of Network and Computer Applications*, *169*, 102763.
[23] Nikou, S. (2019). Factors driving the adoption of smart home technology: An empirical assessment. *Telematics and Informatics*, *45*, 101283.
[24] Ande, R., Adebisi, B., Hammoudeh, M., & Saleem, J. (2020). Internet of Things: Evolution and technologies from a security perspective. *Sustainable Cities and Society*, *54*, 101728.

[25] Hajiheidari, S., Wakil, K., Badri, M., & Navimipour, N. J. (2019). Intrusion detection systems in the Internet of things: A comprehensive investigation. *Computer Networks*, *160*, 165-191.
[26] Manzoor, A., Braeken, A., Kanhere, S. S., Ylianttila, M., & Liyanage, M. (2021). Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain. *Journal of Network and Computer Applications*, *176*, 102917.
[27] Zhu, Q., Loke, S. W., Trujillo-Rasua, R., Jiang, F., & Xiang, Y. (2019). Applications of distributed ledger technologies to the internet of things: A survey. *ACM computing surveys (CSUR)*, *52*(6), 1-34.
[28] Haghi, M., Neubert, S., Geissler, A., Fleischer, H., Stoll, N., Stoll, R., & Thurow, K. (2020). A flexible and pervasive IoT-based healthcare platform for physiological and environmental parameters monitoring. *IEEE Internet of Things Journal*, *7*(6), 5628-5647.
[29] NV, R. K., & E, B. (2022). Detection and monitoring of the asymptotic COVID-19 patients using IoT devices and sensors. *International Journal of Pervasive Computing and Communications*, *18*(4), 407-418.
[30] Shahin, M., Maghanaki, M., Hosseinzadeh, A., & Chen, F. F. (2024). Advancing network security in industrial IoT: a deep dive into AI-enabled intrusion detection systems. *Advanced Engineering Informatics*, *62*, 102685.
[31] Zhang, J., Li, L., Lin, G., Fang, D., Tai, Y., & Huang, J. (2020). Cyber resilience in healthcare digital twin on lung cancer. *IEEE access*, *8*, 201900-201913.
[32] Shirvanimoghaddam, M., Shirvanimoghaddam, K., Abolhasani, M. M., Farhangi, M., Barsari, V. Z., Liu, H., ... & Naebe, M. (2019). Towards a green and self-powered Internet of Things using piezoelectric energy harvesting. *Ieee Access*, *7*, 94533-94556.
[33] Rao, P. M., & Deebak, B. D. (2023). A comprehensive survey on authentication and secure key management in internet of things: Challenges, countermeasures, and future directions. *Ad Hoc Networks*, *146*, 103159.



Almaha Adel Almuqren received his M.Sc. degree in Cybersecurity from the King Faisal University (KFU), Saudi Arabia. She has published several papers in well reputed journals and conferences. Her research interests include cybersecurity, cybersecurity risk assessment and cryptographic .