

Review Article

IoT Security Issues and Challenges: A Systematic Literature Review

Hassan Saad Al-Qahtani

Department of Information Technology, College of Computing and Informatics, Saudi Electronic University, Riyadh,
Kingdom of Saudi Arabia.

Corresponding Author : hh.alqahtani@seu.edu.sa

Received: 03 November 2025

Revised: 17 August 2026

Accepted: 21 August 2026

Published: 30 September 2026

Abstract - The rapid and continuous growth, popularity, and diversity of IoT applications are aligned with the increment in cyber-attacks that are targeting IoT applications. In order to establish the process of approach development that aims to solve, prevent, or avoid those kinds of issues, we have to have an overview of the identified security issues and challenges. For that, this study presents a systematic literature review of the IoT security issues and challenges, which will help categorize these issues and illustrate the implications as well. The investigated studies have been evaluated across nine criteria, and have been limited to five years only, which guarantees the quality of the studied works. The majority of the highlighted issues are associated with the nodes (Things), and this is caused by several reasons: for instance, the geographical distribution, lack of physical barriers, and resource limitations.

Keywords - Internet of Things, Cybersecurity, Security issues, Security challenges.

1. Introduction

The Internet of Things (IoT) has been presented as a huge infrastructure that combines connected nodes (Things), software, hardware, and edge computing capabilities, which aim to process the collected data from the environment [1]. The huge growth in IoT consumption, which is expected to reach more than 75 billion nodes (Things) by the end of 2025, and the IoT market is expected to increase from \$546 billion in 2022 to reach \$991 billion by 2028 [2]. According to [3], that rapid growth will be derived by two core factors: i) the edge computing, and ii) the 5G. However, that growth varies based on the regions and the market needs as well. Practically, the utilization of IoT might be categorized according to the use into: Transportation, healthcare, government, agriculture, sustainable energy, and retail. However, there are some obstacles and concerns that have been identified as issues that might impact the adopting / utilizing the IoT solutions; security and privacy are two of them.

This study aims to identify the IoT security issues and challenges, and categorize these issues. In addition, that categorization will help to prioritize these issues and understand the impact and the influence as well. A clear understanding of these IoT security and privacy concerns is crucial for developing strategies to mitigate, prevent, and avoid their negative consequences. The implications of these threats extend beyond individual adoption choices; a market of this scale presents significant industrial, economic, and

national opportunities that could be squandered if these obstacles are not addressed.

1.1. Paper Origination

The remainder of the study is organized as follows: Section 2 illustrates the applied research methodologies, the SLR phases, and the selection procedures. A brief explanation of the IoT will be provided in Section 3; that section shows the hierarchy, applications, and the involved technologies as well. Subsequently, the identified IoT security issues and challenges are presented in Section 4. The findings of the conducted Systematic Literature Review are explained in Section 5. Finally, the study will be concluded in Section 6.

2. Research Methodology

As we mentioned earlier, the systematic literature review is an important and crucial step that will help to provide a comprehensive understanding of the IoT security and privacy issues and their implications. For that, the Kitchenham systematic review guideline has been adopted as a literature review methodology [4, 5], which will help to provide a clear approach for the conducted steps. Generally, the implemented systematic literature review tasks might be grouped into three phases Figure 1.

The review protocol consists of three phases as follows: planning, conducting, and reporting. The planning phase focuses on developing the plan that will be followed during



the review process. Practically, that phase will start with identifying the research question, as it is essential to know the knowledge that we are looking for, and help to keep the search focusing on the scope of the study; the developed research questions will be discussed next. The second phase maintains the quality of the selected studies and guarantees that each study meets the developed criteria. Finally, the third phase will be about writing the findings of the conducted study and providing a clear answer to the developed research questions.

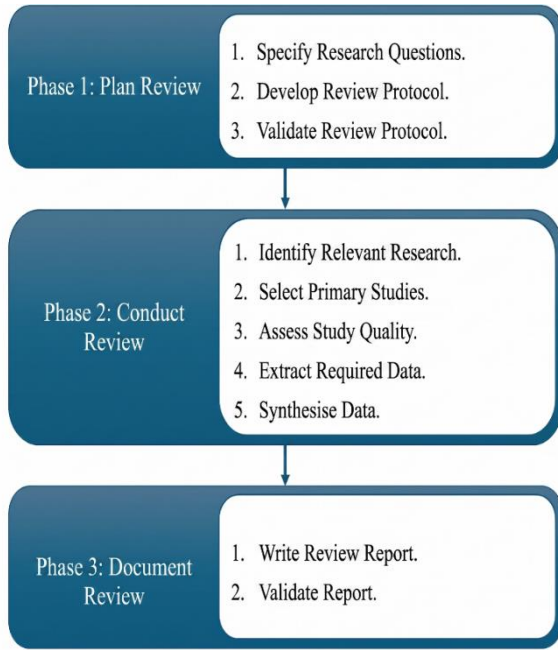


Fig. 1 Systematic literature review workflow

2.1. Aims and Research Questions

In order to facilitate achieving the developed aims for the conducted study, a set of research questions has been asked. This study aims to identify the IoT security issues and challenges, and categorize these issues; and there are three questions have been developed to guarantee that the study aims will be achieved, and avoid any vagueness that might lead to fail to achieve the study goals.

2.1.1. What is the Available Information about IoT Security?

The purpose of this question is to establish a broad understanding of the target research domain. Specifically, it facilitates the definition of the investigation's boundaries. Practically, it helps to highlight the area that we need to investigate, identify the relevant technologies, and provide different prospective for the conducted study. For example, the issue X has been noticed, but are there other parties who are involved or not? Is that issue related with IoT application, or is a result of adopting other technologies? That question helps to expand the scope of conducted research, and guarantee that the conducted study will not ignore/discard any other perspective.

2.1.2. What are the most Critical Security Issues of IoT?

The purpose of this question is to investigate deeply and identified the IoT security issues. Practically, the answer to that question will help to under the issue itself, the implications, the purpose, and help to provide an overview about how the identified issues can be mitigated, prevented, or avoided. Also, the answer will help to point out the involved parties and clarify the sources of those issues.

2.1.3. How can we Categories the Identified IoT Security Challenges?

This question seeks to provide a categorization of the identified security issues, that categorization provides a comprehensive understanding of the issues' sources and implication as well. That understanding helps to develop the solutions that aim to overcome these issues, and know in advance the components that might be affected, and must be considered during the solution development. Moreover, that categorization provides a broad overview about the security issues, and its impact, and how these issues must be prioritized according to the level of impact, severity, and importance.

2.2. Search and Selection Process

In order to maintain the quality of the selected studies, the searching process was limited to the most reliable and respected resources, for example, Elsevier, IEEE, and MDPI, and the publication years are limited to 2020 to 2025.

Table 1. Assessing the study criteria

Dimension	Criteria	Associated Questions
Aim and contribution	Research aim	Does the publication state the aim of the conducted study in a clear way?
	Research contribution	Does the publication state the contribution and the added value to the knowledge?
Research methodology	Research design	Does the publication illustrate the applied research methodologies?
	Sampling	Does the publication explain how the applied research methodologies are?
	Data collections	Does the publication explain how the data was collected?
Findings	Data analyzing	Is the data analysis process clearly described?
	Research findings	Does the research findings presented clearly and discussed?
Related Field	IoT	Is the publication related to IoT?
	IoT security	Is the publication related to IoT security?

Applying that criteria will be to guarantee that the selected studies went through a clear procedure, before getting published; that procedure aims to maintain the reliability and validity of the published results/ findings. However, a quality assessment has been developed in order to maintain the quality of the included studies.

Table 1 illustrates the developed criteria. If the answer to the asked question is “YES”, then the study will gain a point,

and only the paper that has 5 points will be included in our study.

The conducted study investigates about 90 studies; the distribution of the included studies over the years is illustrated in Figure 2. As we mentioned earlier, all the included studies meet the developed criteria in order to guarantee the quality of the investigated studies. Figure 3 shows the distribution of studies over the publishers.

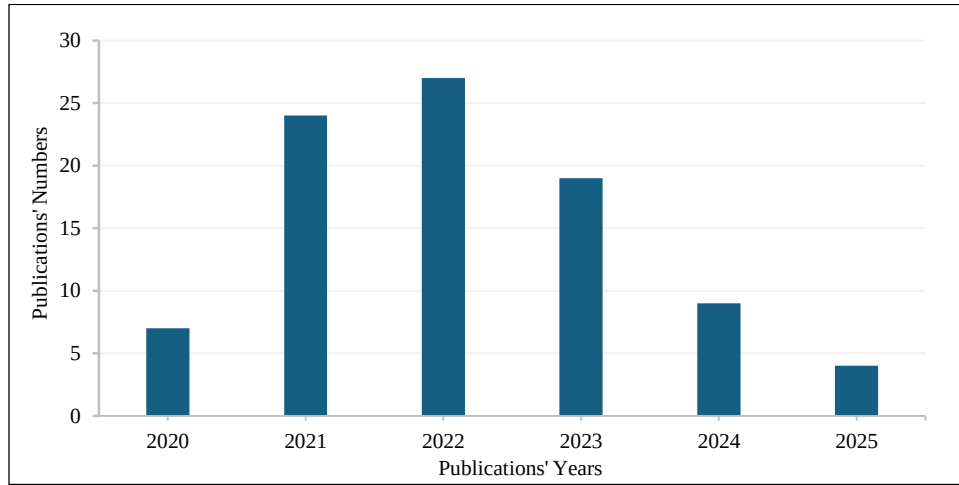


Fig. 2 Studies distribution (year)

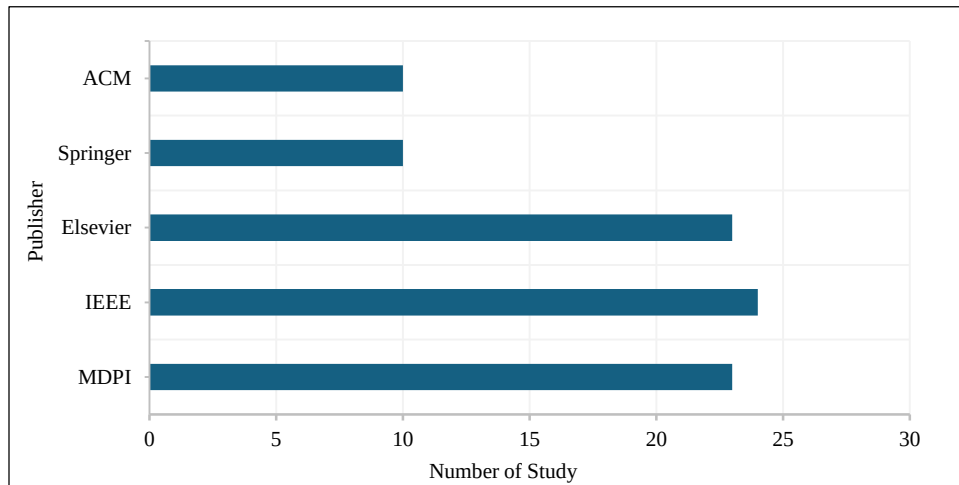


Fig. 3 Studies distribution (publisher)

3. Internet of Things

According to [6], the beginning of IoT era was established 2009; and the application was limited to the capabilities were limited to connecting “Devices” to the internet. On the other hand, the term “Internet of Things” itself was introduced by Kevin Ashton in 1999. The IoT might be defined as a collective of interconnected nodes (devices) and supported technologies that help to connect the distributed things (nodes) and the cloud computing services [7], and aims to “connect the connected” [6].

By moving to Publications' Years the IoT architecture, there is a lack of standard; similar to any other technology that is still in the development phase, the architecture varies between three and five layers. For instance, [8] introduces three layers as follows: application, network, and perception layer; while [9] introduces five layers: business, application, middleware, network, and perception layer. Technically, the IoT architecture might varies based on the application itself, scale of application, involved technologies, and the business model [10].

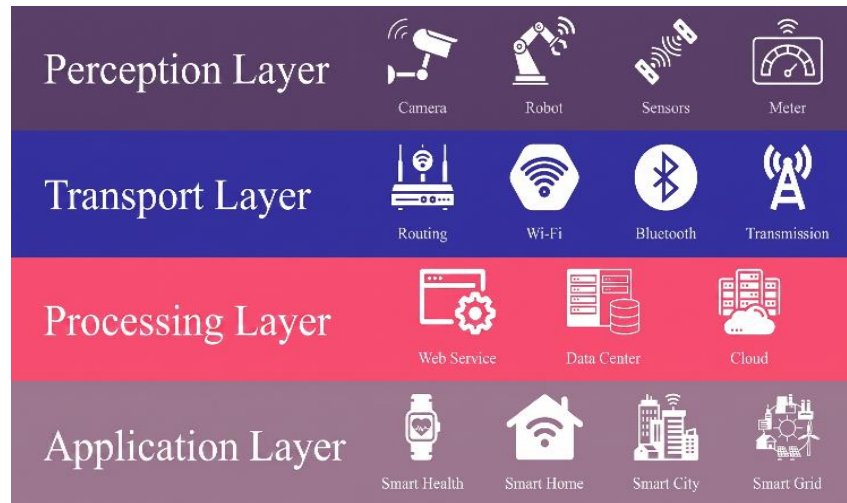


Fig. 4 IoT architecture

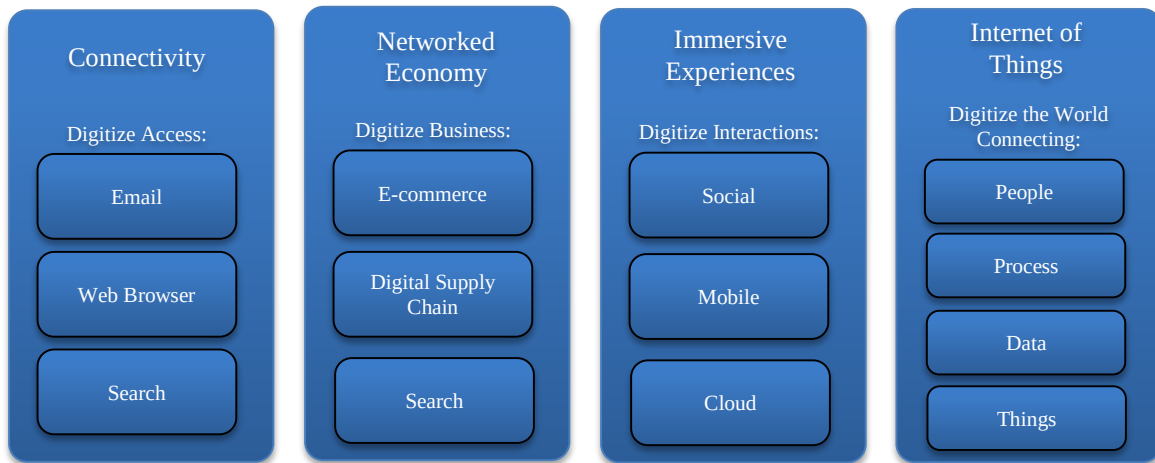


Fig. 5 Evolutionary phases of the internet [6]

Technically, the IoT is a result of the continuous evolution of the internet. Figure 5 illustrates the internet phases from connectivity to IoT. By moving to IoT applications, there are a wide spectrum of developed applications. Those applications vary in terms of purpose, scale, data type, and backhaul connectivity. For example, Healthcare applications might be considered as massive IoT, and might be organizational and individual level. According to [11], the IoT might help to enhance efficiency and safety in the workplace. Besides that, IoT helps to provide more information about the working environment and the process characteristics, which might be utilized in order to support the decision-making process. Also, the IoT applications help to improve the automation, accuracy, and control of the physical devices (Things) in the field. Moreover, the IoT will bring the capabilities of monitoring and tracking the implemented action in the field.

On the other hand, the IoT will come with a set of obstacles, challenges, and open issues that might influence shifting the

newly emerged technology. Those obstacles vary between organizational, technical, strategics, and business. Here, the provided overview will be limited to technical issues only. The scalability and the heterogeneity have been addressed as a critical challenge for IoT. Also, handling the collected data and maintaining the ownership dilemma have been highlighted as core challenges; the importance of this point will increase when IoT deal with sensitive/private data. In addition, the cybersecurity, privacy, and access control management might be considered as open issues [11]; the complexity of these issues will increase according to the geographical distribution of the things, environment, hardware, and the other metrics that will be discussed next; Figure 6 summarizes IoT challenges.

Practically, Figure 6 focuses on the technical aspects, but there is a set of issues that might be considered as challenges; these issues are related to management, policies, law, and governance as well. However, these issues have a direct impact on the level of the provided and requested security.

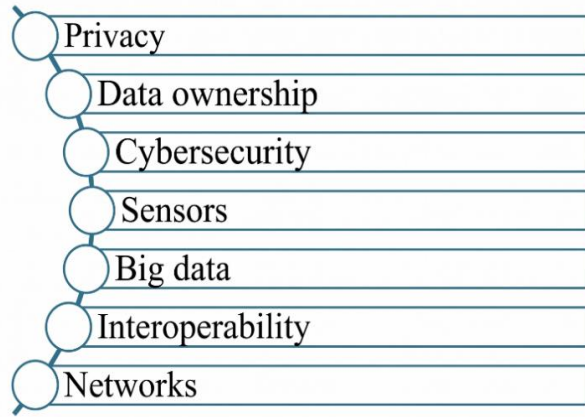


Fig. 6 Summary of IoT main challenges

4. IoT Security Issues and Challenges

Similar to any ICT solution, the security issues and challenges might be distributed over the layers of the system. Besides that, the relationship between layers will lead to make it extremely difficult to deal with the addressed issues as an isolated challenge. Practically, the dependency between the hierarchy of IoT and the utilized technologies requires that any proposed solution that aims to solve/mitigate the targeted security issues consider any implications that might affect the system components and prevent any sequences that might lead to expose the IoT systems, in terms of data protection, safety, privacy, integrity, and authenticity.

It is worth to mention that the security requirements will vary according to the IoT application itself. For example, the security requirements for IoT are different from the Smart city's requirements; the conducted study did not consider that variation, and we attempt to coinvestigate the IoT security issues and challenges from a general perspective, and avoid to be dedicated in a specific application. Also, the issues that might be caused by the human factor (end-user) were not addressed. The following section illustrates the identified security issues and challenges, and categorizes these issues according to the IoT layers.

4.1. Physical Device Layer

One of the core issues that IoT suffer from is the inadequate physical security, which might allow the attacker to cause physical damage to the things, and might lead to gain access to the system [4]; besides that, the tampering attack might occur when the attacker modifies the distributed node (Things) [12-16]. An insecure neighbor discovery issue, which is caused by applying insufficient access control, might be used as a method to consume the provided resource. Practically, that kind of attack keeps sending discovery packets over the system, which will lead to DoS. Besides that, an attacker might gain access to the IoT system if there is a lack of effective verification for transmitting establishment [12]. One of the security issues that is associated with the

physical access is the malicious node attack [12, 14, 15, 17], where the attacker exploits the lack of physical barriers, and the heterogeneity to add a malicious node to the system, that kind of attack might lead to expose the privacy of the data, validity of the collected data, or losing the availability as well, worth to mention that some resources define this kind of attack as Fake Node Injection [12, 14, 15, 18, 19].

Maintaining data privacy, integrity, and security starts from the physical layer, before collecting the data. The IoT system must be capable of delivering an efficient and effective encryption algorithm; the core obstacle here is the power consumption. Practically, the traditional encryption algorithms might not be suitable to be applied over IoT systems, as these kinds of algorithms need specific requirements in terms of resources, computation capabilities, and power as well; which is an issue in IoT systems. Although there are several low-power consumption algorithms that have been proposed as a promising solution, such as [20-24], but these algorithms suffer from several drawbacks.

The limitations of resources and capabilities in IoT raise a set of security issues and challenges. One of the attacks that try to take advantage of the resource's limitation is the sleep deprivation attack [25-27]. The attacker aims to consume the power by keeping the targeted node awake [12, 28]. It is stated that a power consumption attack might be implemented by executing an infinite loop, which will lead to lose the availability of the targeted node (Things). According to [25, 26, 29-32], the buffer reservation attack might be considered as one of the attacks that exploit the limitation of the resources, as the attacker aims to occupy the provided network buffer, which will lead to the received packets, and cause DoS [33]. According to [12, 34-36], the Side Channel Attack DoS might be considered as one of the most common attacks, which led to loss the availability of the provided services, which will be the result of targeting the physical node (Things) with an enormous number of packets. The Sybil attack [14, 16, 29] will be implemented in this layer. The mechanism of this attack is implanting a malicious node into the IoT system, and that single node will introduce itself through the system for an enormous time, which gives the attacker the ability to manipulate the collected data and the IoT behavior as well [16].

The software issues in this layer concern the code that will be installed on the physical devices, and aim to collect the data and control the environment. According to [14, 37, 38], the vulnerable code might be an optimal environment for conducting an injection attack. Also, unsecured and unverified code will increase the probability of introducing other attacks, such as password and unauthorized access [37, 39]. One of the issues that will be caused by malware that led to wipeout/sabotage the firmware is the Permanent Denial of Service (PDoS) [14]; Table 2 summarizes the security issues in the physical device layer.

Table 2. Physical device layer

Physical Device Layer	Physical Damage
	Un-authorized In-person Access
	Tampering Attack
	Insecure Neighbor Discovery
	DoS
	DDoS
	PDoS
	Sybil Attack
	Sleep Deprivation Attack
	Buffer Reservation Attack
	Injection Attack
	Unauthorized Access
	Malicious Node
	Privacy
	Availability
	Data Integrity

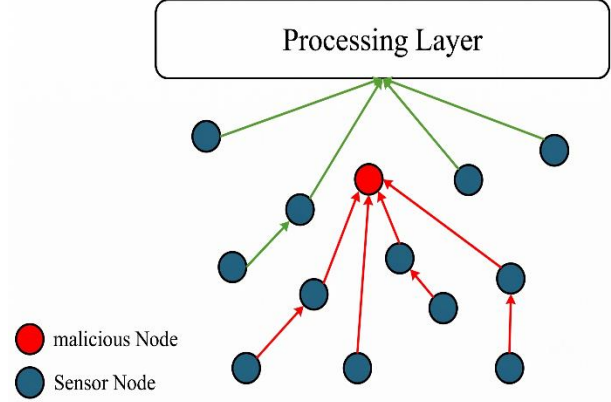
4.2. Connectivity Layer

Practically, the security issues and challenges for the connectivity will be inherited from the utilized network; one of the attacks that proves this concept is the jamming attacks. As the data will be exchanged through the IoT system wirelessly, the attacker will cause the jam by sending a radio frequency signal which will led to a loss of availability [40]. According to [16, 35], the jamming attack can be considered as a subset of a DoS attack. This kind of attack is not limited to or caused by IoT systems, but it is inherited from the adopted/adapted technologies. Practically, the Connectivity attacks might be considered as one of the easiest and most efficient attacks, which is caused by the lack of physical barriers, and the vulnerabilities of the used protocol as well.

Relying on unsecure protocols for data exchange between the distributed devices (Things) and the edge layer is one of the critical issues. Technically, the nature of the IoT paradigm and the limitations of resources and capabilities are the cause of these issues. In order to transmit data via such a system, the protocols used will not be able to maintain data security and privacy, such as Bluetooth or ZigBee. Relying on that kind of protocol will expose the communication channel and make the system vulnerable to attacks such as MITM, which will allow to gain access to the exchange data, unauthorized access, losing the availability, controlling and manipulating the physical device [37, 39, 41-44].

Violation of privacy and the DoS are two critical security issues in IoT; the level of seriousness depends on the IoT application itself. In addition, the Distributed Denial of Service (DDoS) attack has been highlighted as one of the security issues that might target IoT systems [14, 16], as the attacker will use more than one node (Things) to implement that kind of attack. The sinkhole and wormhole attacks might be considered as one of the effective attacks that cause these issues, at sinkhole the attacker node will allocate itself through

the routing process, and utilized the received packet to cause the targeted attack. In order to enhance the effectiveness of that attack, the sinkhole attack can be combined with a wormhole attack [17, 37, 45-54]. Figure 7 illustrates the layout of the sinkhole attack.

**Fig. 7 Sinkhole/wormhole attack**

According to [55, 56], relying on a robust protocol is important; however, the utilized protocols have to have self-healing capabilities, which will help to enhance the maintenance of the provided security level. The Traffic Analysis Attack aims to scan the port, or sniff the exchange data, which will violate the data confidentiality and do not need to access the communication channel [14, 16, 29]. The collected data might be used to trigger other attacks or cause a data leakage. The sniffing attack will violate the confidentiality of the exchange data; besides the data itself, the attacker might extract other information, such as the followed route [29].

Furthermore, [12, 37] stated that the Routing Information and the Selective Forwarding attacks are effective attacks that might violate the data confidentiality and integrity as well. In a Selective Forwarding attack, the malicious node (Things) will be used in order to gain access to the IoT system, then that node will be capable to intercept the exchange data, and modify, delete, or sabotage that data; also, that malicious node has the capability to forward unreliable data to other nodes, the identified security challenges of connectivity layer are represented in Table 3.

Table 3. Connectivity layer

Connectivity Layer	Jamming Attack
	Connectivity Attack
	Unsecure Protocol
	MITM
	DDOS
	Wormhole Attack
	Sinkhole Attack
	Sniffing Attack
	Selective Forwarding Attack

4.3. Fog Computing Layer

By moving to the Cloud Computing and Fog Computing layers, these layers will be adopted/adapted in the IoT system in order to overcome the resource limitation issues and the need for computation capabilities over the IoT system. The Fog computing layer will help to bridge the distributed nodes (Things), which the Cloud Computing Layer, as it enhances the efficiency of the IoT system by making the computation and the storage close to the nodes. Technically, Fog Computing will help to reduce the latency, distribute the data processing, and help to improve the reliability [12].

Practically, Fog Computing will bring its security issues and challenges to IoT systems, which are similar to the status of the network. One of the addressed issues in the Fog Computing layer is the integrity of the exchanged data, as the MITM attack might target the data while it is transmitting to the Fog Computing layer from the physical node, and from the Fog Computing layer to the Cloud Computing layer [37]. Table 4 shows the addressed security issues of the Fog computing layer.

Table 4. Fog computing layer

Fog Computing Layer	MITM Attack
	Data Integrity
	Insecure Interface
	Firmware Updates Attack

4.4. Cloud Computing Layer

By moving to the Fog Computing and Cloud Computing layers, the characteristics of the identified security issues and challenges will be changed from issues that concentrate on physical devices and their limitations to challenges and issues focusing on software and databases. Practically, the resource limitations and lack of computational capabilities will not be a challenge here, and the attackers cannot exploit these weaknesses to trigger their attacks. According to [16, 57, 58], integrating Cloud computing with IoT will help to enhance the security, but that integration will introduce new security challenges.

One of the shared issues between the Fog Computing and Cloud Computing layers is the insecure interfaces [15]. Practically, that might occur when the developed interfaces and the utilized APIs have been developed in an inappropriate way, which means a lack of good practices, a lack of testing, and a lack of sufficient security. Relying on an insecure interface might led to threat the data integrity, facilitate malicious attacks, unauthorized access, and expose the functionality of the IoT system [15, 59-61].

In addition, the Cloud and Fog Computing might be a target for DoS attacks, and the various types of attacks that are targeting the data, for instance, SQL injection, and End-to-End

encryption [12, 16]. Moreover, both Cloud and Fog Computing might be targeted via firmware updates, which might led expose the whole IoT system by taking control or provide unauthorized access to the attacker. According to [12, 18, 62, 63], relying on insecure interfaces, poor encryption algorithms, and bad practice access control might led to storage attacks. Table 5 represents the security issues in the cloud computing layer.

Table 5. Cloud computing layer

Cloud Computing Layer	API
	Insecure Interface
	Malicious Attack
	Unauthorized Access
	Dos Attack
	SQL Injection
	Firmware Updates Attack
	Storage Attack

4.5. Application Layer

As we mentioned before, the security issues and challenges cannot be isolated in one layer. Practically, all the layers are connected and will be Influenced, affected, and interacted among each other. One of the issues that has been addressed is the Voice Squatting Attack (VSA), which is associated with IoT natural language processing applications, such as voice assistance [37, 54]. In VSA, the attacker might synthesize the user voice, or via installing malicious applications [37, 64-66]; these kinds of attacks might be used to initiate a process, grant access, or activate a command. Moving to the software, insecure/outdated software is one of the security challenges. The geographically distributed things, the resource limitations, and the enormous quantity of the distributed devices will make it difficult to guarantee being updated; and that might be considered as a real threat, as the attacker might choose the rural / far things as a start point for the conducted attack [67].

The attacks that are associated with software and malware might be allocated in the application layer. For example, virus, malware, spyware, and worms. Each single attack has its own aim and mechanism to be implemented [14, 16]. However, the expected impact focus on two areas: i) access to the data, and ii) consume and occupy the provided resources. Moreover, the data attacks might take place through all layers; but these kinds of attacks are allocated to the application layer, because the IoT application plays a core role in determining the most appropriate layer to launch these types of attacks. For example, the unauthorized access to the data might happen in the physical layer in an agriculture IoT application, in the Cloud Computing Layer in an Industrial IoT application, and in end-user software in a smart home. Practically, each single IoT application defines its requirements in terms of security and protection, and these requirements must be aligned with

cost, IoT purpose, and IoT hierarchy. The data privacy issue cannot be limited to a specific layer. Practically, the violation of data privacy might be a result of various things; for instance, a lack of encryption algorithm, a lack of physical barriers, or unauthorized access, each one of them is allocated in a different layer as we stated before that it is extremely difficult to isolate the IoT layer and try to solve the identified issues and challenges in an independent way [15]. The hierarchy of IoT and the requirements of the IoT application itself play a core role in highlighting the most appropriate solution to solve/overcome the identified challenges. Table 6 shows the security issues in the application layer.

Table 6. Application layer

Application Layer	Voice Squatting Attack
	Insecure / Outdated Software
	Malware Attack
	Data Attack
	Encryption Algorithm

4.6. Utilized Technologies

There are several technologies that might be unloosed in order to enhance the quality of the provided services of the IoT system. These technologies will act as a supportive technology that aims to solve/overcome specific issues/ obstacles-for example, Artificial Intelligence, Machine Learning, and Blockchain. For instance, machine learning might be utilized in order to handle several issues, for example, the Intrusion Detection system, Impersonation, and Malware detections. On the other hand, the Blockchain might help to maintain the Identity verification, Trust management, and data integrity [68]. Here, we are not examining the effectiveness of these technologies, but we have to highlight the issues that might arise if this approach were adopted/adapted.

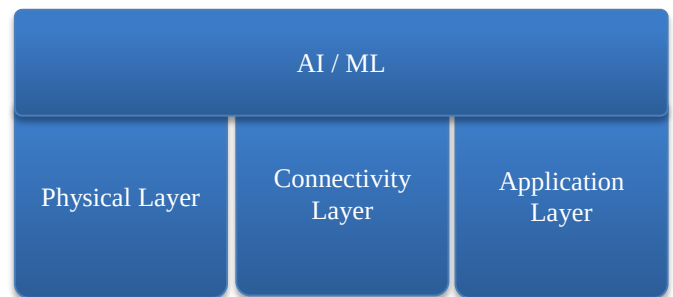
The core issue with similar approach's is the need to include more stakeholders, and rely on third parties, which will rise issues related to data ownership, vendor-lock in, data integrity, losing the availability, and outsourcing the data [68, 69]. The previous issues might led to influence the shifting to IoT solutions, which has already been identified as a core reason that prevents organizations from migration from tradition computing to Cloud computing. However, the sensitivity of the collected data in IoT systems (Smart Hospital, Smart Transportation, Health, and Smart Grid) might influence the incorporation of these approaches; because of that, all the implications and side effects must be addressed before integrating these technologies with IoT [26, 70-74]. For example, the Blockchain can be utilized in order to maintain storing the data in a decentralized, trustworthy way. The blockchain will enhance the IoT system in terms of auditability, trust, and data provenance, but it will produce new drawbacks, such as huge power consumption, as it requires implementing a large number of computations. Table 7 illustrates the associated security issues with the utilized technologies.

Table 7. Utilized technologies

Utilized Technologies	Data Ownership
	Data Integrity
	Availability
	Vendor-lock In
	Compatibility

One of the most critical concerns raised regarding the utilized technologies is the associated with Artificial Intelligence (AI). We thought that investigating AI security must be studied as a layer for several factors; for instance, the rapid and huge adoption of that computing paradigm, and the impact and consequences of attacks, threats, and issues that are linked with AI. However, the reason for allocating those issues within the utilized technologies section is due to the absence of adopt/adapt the AI in some of the IoT systems; and the limitation of utilization duo to higher cost and requirements as well; which is against the IoT system concept that depends on low-cost infrastructure [75]. One of the most critical security challenges is prioritizing functionality over the security factors, and that prioritizing is not limited to the operational phase, but it starts from the design and development of the utilized AI solution. On the other hand, adopting AI within an IoT system will lead to a series of issues, and this is caused by a lack of consideration for the security requirements in the IoT environment, which is completely different from other computing paradigms, not to mention the further complexity. By moving to the technical part, the AI solutions suffer from several security issues; for example, the poisoning attacks, evasion attacks, and adversarial attacks [75, 76].

Moreover, the Large Language Model (LLM) and Generative Artificial Intelligence (GenAI) introduce additional security issues, such as prompt injection and jailbreak attacks [77, 78]. Also, the lack of global security standards and the absence of transparency when we are studying the used defensive techniques and mechanisms make this area very ambiguous and vague [78]. Also, the interference of AI within IoT layers might lead to magnitude the implications of the associated security threats and issues. Figure 8 illustrates the allocation of AI within IoT architecture, similar to other technologies that hierarchy varies depends on the application itself and its requirements as well.

**Fig. 8 AI & IoT**

5. Findings

The characteristics of the IoT system bring a lot of capabilities, and allow to utilize this technology via a wide spectrum of applications. Although there is a variety of applications, the lack of standardization and developing affordable Things might be the sources of the identified security challenges and issues. The lack of physical barriers that manage and control the physical access to the distributed

nodes (Things) facilitates the majority of attacks that target the physical layer. Moreover, the limitation of the computation capabilities, resources, and power makes the physical layer extremely vulnerable. Practically, the complicated calculations and processes must be shifted to Fog and Cloud Computing. In addition, rely on specific communication protocols that show obvious failure plays a critical role in attacks.

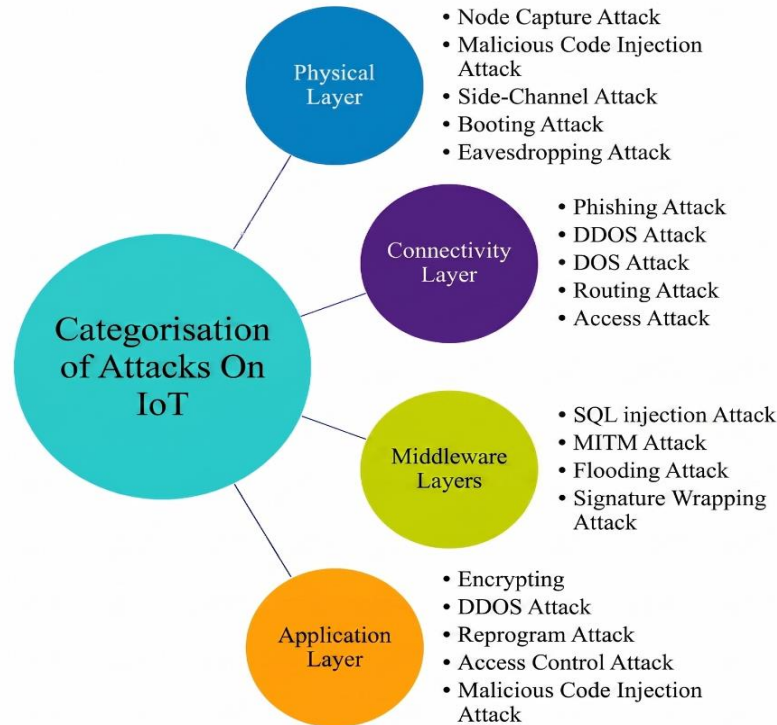


Fig. 9 Categorization of attacks on IoT

By moving to Fog and Cloud Computing, these two technologies bring their security issues and challenges to the IoT system. Moreover, the lack of standardization and the variation in security requirements for IoT applications lead must be considered, as we need to balance between the IoT applications' requirements and Cloud and Fog Computing capabilities. Also, the other technologies that might be utilized must be integrated in a way that maintains the safety and security of the IoT system; Figure 9 provides a classification of the identified attacks.

Finally, the rapid utilization of the emerged technologies such as AI / ML will raised a very critical issues associated with security and governance perspectives. It is important to highlight that the governance perspective must be studies and investigated as this study is concerned with the technical perspectives only. In order to remove any obstacles that might influence the decision of using the AI / ML [79], according to [79, 80], the majority of unpartially addressed security issues are caused by the lack/limitation of international standards and references; for instance, ISO. In addition, the huge number of

involved stakeholders will be a challenge, as we need to select or develop a new governance framework that focuses on AI [81].

Moreover, the dilemma of the data ownership will be more complicated; as in IoT its infinity debit how owns the data (vendor, system owner, cloud computing service provider, edge computing service provider, communication channel, etc.) besides that, dealing with the data through the AI / ML solutions; which will raise several questions must be answer clearly in order to provide a clear vision about data handling. For instance: how the data will be treated over the AI / ML, the data format, data storing and other questions. Practically, the training and the accuracy of the decision, as the source of the training data must be reliable and valid, and the decision must be as accurate as we can. Also, the geographical location of the used infrastructure will play a critical role in the governance and ethics of the used AI/ML, as the regulations and legislations vary according to the region and countries.

6. Conclusion

This paper illustrates the IoT security issues and challenges and explains how the addressed attacks might be conducted. The conducted SLR follow Kitchenham [4, 5]. An important point that must be highlighted is that the characteristics of IoT systems might be considered as the cause for some issues and challenges that have been identified. For example, one of the advantages of an IoT system is the capabilities to distribute a large number of nodes (Things) across the environment; the lack of control over the connected node and the characteristics of the node itself might be an issue. The utilized node, which is a low-cost node that usually lacks a continuous source of power and computation

capabilities, was the main vulnerability that the attackers relied on when they implemented their attacks. The paper categorizes the security issues and challenges into groups according to the layer in which the identified issues fall. Besides that, the utilized technologies utilized in order to enhance the quality of the provided services were investigated. To sum up, the area needs more investigation in terms of the integration of IoT systems and new emerging technologies, such as Machine Learning, Artificial Intelligence, and Blockchain, that might be adopted/adapted in IoT systems. The integration process must be balanced and try to prevent and avoid any consequences that might occur because of that integration, and maintain the characteristics of the IoT system.

References

- [1] Apostolos Gerodimos et al., "IoT: Communication Protocols and Security Threats," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 1-13, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [2] Gartner, Forecast: IoT Market Opportunity by Technology Segment, 2022-2028, Gartner, 2024. [Online]. Available: <https://www.gartner.com/en/documents/5499495>
- [3] Market Research, Markets and Markets, 2026. [Online]. Available: <https://www.marketresearch.com/MarketsandMarkets-v3719/>
- [4] Barbara Kitchenham, "Procedures for Performing Systematic Reviews," *Keele University, Keele*, vol. 33, pp. 1-26, 2004. [[Google Scholar](#)]
- [5] Barbara Kitchenham, and Pearl Brereton, "A Systematic Review of Systematic Review Process Research in Software Engineering," *Information and Software Technology*, vol. 55, no. 12, pp. 2049-2075, 2013. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [6] David Hanes et al., *IoT Fundamentals: Networking Technologies, Protocols, and use Cases for the Internet of Things*, Cisco Press, 2017. [[Google Scholar](#)] [[Publisher Link](#)]
- [7] Neera Batra, and Sonali Goyal, *IoT Fundamentals with a Practical Approach*, 1st ed., CRC Press, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [8] Miao Wu et al., "Research on the Architecture of Internet of Things," *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, Chengdu, pp. V5-484-V5-487, 2010. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [9] Rafiullah Khan et al., "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," *2012 10th International Conference on Frontiers of Information Technology*, Islamabad, Pakistan, pp. 257-260, 2012. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [10] Madhusanka Liyanage et al., *IoT Security: Advances in Authentication*, John Wiley and Sons, 2019. [[Google Scholar](#)] [[Publisher Link](#)]
- [11] Farshad Firouzi, Krishnendu Chakrabarty, and Sani Nassif, *Intelligent Internet of Things: From Device to Fog and Cloud*, 1st ed., Springer Cham, 2020. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [12] Swastik Kumar Sahu, and Kaushik Mazumdar, "Exploring Security Threats and Solutions Techniques for Internet of Things (IoT): From Vulnerabilities to Vigilance," *Frontiers in Artificial Intelligence*, vol. 7, pp. 1-16, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [13] Aditya Kumar Pathak et al., "Anomaly Detection using Machine Learning to Discover Sensor Tampering in IoT Systems," *ICC 2021-IEEE International Conference on Communications*, Montreal, QC, Canada, pp. 1-6, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [14] Jayasree Sengupta, Sushmita Ruj, and Sipra Das Bit, "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, pp. 1-20, 2020. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [15] Tinashe Magara, and Yousheng Zhou, "Internet of Things (IoT) of Smart Homes: Privacy and Security," *Journal of Electrical and Computer Engineering*, vol. 2024, no. 1, pp. 1-17, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [16] Stefan Balogh et al., "IoT Security Challenges: Cloud and Blockchain, Postquantum Cryptography, and Evolutionary Techniques," *Electronics*, vol. 10, no. 21, pp. 1-22, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [17] Hamed HaddadPajouh et al., "A Survey on Internet of Things Security: Requirements, Challenges, and Solutions," *Internet of Things*, vol. 14, pp. 1-19, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [18] Nivedita Mishra, and Sharnil Pandya, "Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review," *IEEE Access*, vol. 9, pp. 59353-59377, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [19] Ashwin Karale, "The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws," *Internet of Things*, vol. 15, pp. 1-20, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [20] Saurabh Singh et al., "Advanced Lightweight Encryption Algorithms for IoT Devices: Survey, Challenges and Solutions," *Journal of Ambient Intelligence and Humanized Computing*, vol. 15, no. 2, pp. 1625-1642, 2017. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]

- [21] Umeshwer Singh, Manu Sood, and Robin Singh Bhadoria, "Underpinning of Resource-Constrained IoT Networks: Analysis and Countermeasures for Attacks and Vulnerabilities," 2025 *IEEE 14th International Conference on Communication Systems and Network Technologies (CSNT)*, Bhopal, India, pp. 467-473, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [22] Phillip Williams et al., "A Survey on Security in Internet of Things with a Focus on the Impact of Emerging Technologies," *Internet of Things*, vol. 19, pp. 1-24, 2020. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [23] Barjinder Kaur et al., "Internet of Things (IoT) Security Dataset Evolution: Challenges and Future Directions," *Internet of Things*, vol. 22, pp. 1-23, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [24] Payal Sharma, and B.R. Purushothama, "Securing Polynomial based Group Key Management Scheme against Strong Active Adversary Model," *International Journal of Information Technology*, vol. 14, no. 5, pp. 2329-2334, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [25] Iqbal H. Sarker et al., "Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions," *Mobile Networks and Applications*, vol. 28, no. 1, pp. 296-312, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [26] Muhammad Nasir Mumtaz Bhutta et al., "A Survey on Blockchain Technology: Evolution, Architecture and Security," *IEEE Access*, vol. 9, pp. 61048-61073, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [27] Dorsaf Swessi, and Hanen Idoudi, "A Survey on Internet-of-Things Security: Threats and Emerging Countermeasures," *Wireless Personal Communications*, vol. 124, no. 2, pp. 1557-1592, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [28] Shidrokh Goudarzi et al., "An IoT-based Prediction Technique for Efficient Energy Consumption in Buildings," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 4, pp. 2076-2088, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [29] Nathalie Tan Yhe Huan, and Zuriati Ahmad Zukarnain, "A Survey on Addressing IoT Security Issues by Embedding Blockchain Technology Solutions: Review, Attacks, Current Trends, and Applications," *IEEE Access*, vol. 12, pp. 69765-69782, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [30] Yasmine Harbi et al., "Recent Security Trends in Internet of Things: A Comprehensive Survey," *IEEE Access*, vol. 9, pp. 113292-113314, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [31] Yahya Al-Hadhrani, and Farookh Khadeer Hussain, "DDoS Attacks in IoT Networks: A Comprehensive Systematic Literature Review," *World Wide Web*, vol. 24, no. 3, pp. 971-1001, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [32] Sonam Lata, Shabana Mehruz, and Shabana Urooj, "Secure and Reliable WSN for Internet of Things: Challenges and Enabling Technologies," *IEEE Access*, vol. 9, pp. 161103-161128, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [33] Abbas Shah Syed et al., "IoT in Smart Cities: A Survey of Technologies, Practices and Challenges," *Smart Cities*, vol. 4, no. 2, pp. 429-475, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [34] Wei Hu et al., "An Overview of Hardware Security and Trust: Threats, Countermeasures, and Design Tools," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 40, no. 6, pp. 1010-1038, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [35] Bhabendu Kumar Mohanta et al., "Survey on IoT Security: Challenges and Solution using Machine Learning, Artificial Intelligence and Blockchain Technology," *Internet of Things*, vol. 11, pp. 1-17, 2020. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [36] Sri Harsha Mekala et al., "Cybersecurity for Industrial IoT (IIoT): Threats, Countermeasures, Challenges and Future Directions," *Computer Communications*, vol. 208, pp. 294-320, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [37] Nivedita Singh, Rajkumar Buyya, and Hyoungshick Kim, "Securing Cloud-based Internet of Things: Challenges and Mitigations," *Sensors*, vol. 25, no. 1, pp. 1-45, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [38] Hannelore Sebestyen, Daniela Elena Popescu, and Rodica Doina Zmaranda, "A Literature Review on Security in the Internet of Things: Identifying and Analysing Critical Categories," *Computers*, vol. 14, no. 2, pp. 1-45, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [39] Ahmed Fawzi Ootom, Wafa' Eleisah, and Emad E. Abdallah, "Deep Learning for Accurate Detection of Brute Force Attacks on IoT Networks," *Procedia Computer Science*, vol. 220, pp. 291-298, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [40] H.M.K.K.M.B. Herath, and Mamta Mittal, "Adoption of Artificial Intelligence in Smart Cities: A Comprehensive Review," *International Journal of Information Management Data Insights*, vol. 2, no. 1, pp. 1-21, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [41] Leonardo Babun et al., "A Survey on IoT Platforms: Communication, Security, and Privacy Perspectives," *Computer Networks*, vol. 192, pp. 1-26, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [42] N. Sivasankari, and S. Kamalakannan, "Detection and Prevention of Man-in-the-Middle Attack in IoT Network using Regression Modeling," *Advances in Engineering Software*, vol. 169, pp. 1-7, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [43] Badis Hammi et al., "Survey on Smart Homes: Vulnerabilities, Risks, and Countermeasures," *Computers and Security*, vol. 117, pp. 1-25, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [44] Naba M. Allifiah, and Imran A. Zuolkernan, "Ranking Security of IoT-based Smart Home Consumer Devices," *IEEE Access*, vol. 10, pp. 18352-18369, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [45] Muhammad Aqeel et al., "A Review of Security and Privacy Concerns in the Internet of Things (IoT)," *Journal of Sensors*, vol. 2022, no. 1, pp. 1-20, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]

- [46] Ankur O. Bang et al., "Assessment of Routing Attacks and Mitigation Techniques with RPL Control Messages: A Survey," *ACM Computing Surveys*, vol. 55, no. 2, pp. 1-36, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [47] S.V.N. Santhosh Kumar, M. Selvi, and A. Kannan, "A Comprehensive Survey on Machine Learning-based Intrusion Detection Systems for Secure Communication in Internet of Things," *Computational Intelligence and Neuroscience*, vol. 2023, no. 1, pp. 1-24, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [48] Safwan Mawlood Hussein, Juan Antonio López Ramos, and Abubakar Muhammad Ashir, "A Secure and Efficient Method to Protect Communications and Energy Consumption in IoT Wireless Sensor Networks," *Electronics*, vol. 11, no. 17, pp. 1-21, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [49] Hafiz Abid Mahmood Malik et al., "Resolving Security Issues in the IoT using Blockchain," *Electronics*, vol. 11, no. 23, pp. 1-14, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [50] Muhammad Zulkifl Hasan, and Zurina Mohd Hanapi, "Efficient and Secured Mechanisms for Data Link in IoT WSNs: A Literature Review," *Electronics*, vol. 12, no. 2, pp. 1-23, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [51] Zhibo Wang et al., "A Survey on IoT-Enabled Home Automation Systems: Attacks and Defenses," *IEEE Communications Surveys and Tutorials*, vol. 24, no. 4, pp. 2292-2328, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [52] Wenbing Liang, and Nan Ji, "Privacy Challenges of IoT-based Blockchain: A Systematic Review," *Cluster Computing*, vol. 25, no. 3, pp. 2203-2221, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [53] Peng Cheng, and Utz Roedig, "Personal Voice Assistant Security and Privacy - A Survey," *Proceedings of the IEEE*, vol. 110, no. 4, pp. 476-507, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [54] Chen Yan et al., "A Survey on Voice Assistant Security: Attacks and Countermeasures," *ACM Computing Surveys*, vol. 55, no. 4, pp. 1-36, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [55] Abid Khan et al., "Authorization Schemes for Internet of Things: Requirements, Weaknesses, Future Challenges and Trends," *Complex and Intelligent Systems*, vol. 8, no. 5, pp. 3919-3941, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [56] Mays Alshaikhli et al., "Evolution of Internet of Things from Blockchain to IOTA: A Survey," *IEEE Access*, vol. 10, pp. 844-866, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [57] Aleksandr Ometov et al., "A Survey of Security in Cloud, Edge, and Fog Computing," *Sensors*, vol. 22, no. 3, pp. 1-27, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [58] Yunusa Simpa Abdulsalam, and Mustapha Hedabou, "Security and Privacy in Cloud Computing: Technical Review," *Future Internet*, vol. 14, no. 1, pp. 1-27, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [59] Yuba Raj Siwakoti et al., "Advances in IoT Security: Vulnerabilities, Enabled Criminal Services, Attacks, and Countermeasures," *IEEE Internet of Things Journal*, vol. 10, no. 13, pp. 11224-11239, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [60] Abiodun Esther Omolara et al., "The Internet of Things Security: A Survey Encompassing Unexplored Areas and New Insights," *Computers and Security*, vol. 112, pp. 1-31, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [61] Fursan Thabit et al., "Cryptography Algorithms for Enhancing IoT Security," *Internet of Things*, vol. 22, pp. 1-29, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [62] Yousef-Awwad Daraghmi et al., "Edge-Fog-Cloud Computing Hierarchy for Improving Performance and Security of NB-IoT-based Health Monitoring Systems," *Sensors*, vol. 22, no. 22, pp. 1-17, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [63] Waqas Ahmad et al., "Cyber Security in IoT-based Cloud Computing: A Comprehensive Survey," *Electronics*, vol. 11, no. 1, pp. 1-34, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [64] Nadeen Ahmed et al., "Detecting Replay Attack on Voice-Controlled Systems using Small Neural Networks," *2022 IEEE 7th Forum on Research and Technologies for Society and Industry Innovation*, Paris, France, pp. 50-54, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [65] George Vardakis et al., "Review of Smart-Home Security using the Internet of Things," *Electronics*, vol. 13, no. 16, pp. 1-35, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [66] Yanyan Li, Sara Kim, and Eric Sy, "A Survey on Amazon Alexa Attack Surfaces," *2021 IEEE 18th Annual Consumer Communications and Networking Conference*, Las Vegas, NV, USA, pp. 1-7, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [67] Omer Ali et al., "A Comprehensive Review of Internet of Things: Technology Stack, Middlewares, and Fog/Edge Computing Interface," *Sensors*, vol. 22, no. 3, pp. 1-43, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [68] Razan Alajlan, Norah Alhumam, and Mounir Frikha, "Cybersecurity for Blockchain-based IoT Systems: A Review," *Applied Sciences*, vol. 13, no. 13, pp. 1-26, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [69] Xiaoqi Li et al., "A Survey on the Security of Blockchain Systems," *Future Generation Computer Systems*, vol. 107, pp. 841-853, 2020. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [70] Nazish Khalid et al., "Privacy-Preserving Artificial Intelligence in Healthcare: Techniques and Applications," *Computers in Biology and Medicine*, vol. 158, pp. 1-21, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]

- [71] Taher M. Ghazal et al., "IoT for Smart Cities: Machine Learning Approaches in Smart Healthcare-A Review," *Future Internet*, vol. 13, no. 8, pp. 1-18, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [72] Abdul Rehman Javed et al., "A Survey of Explainable Artificial Intelligence for Smart Cities," *Electronics*, vol. 12, no. 4, pp. 1-40, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [73] Moez Krichen et al., "Blockchain for Modern Applications: A Survey," *Sensors*, vol. 22, no. 14, pp. 1-27, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [74] Md Rafiqul Islam et al., "A Review on Blockchain Security Issues and Challenges," *2021 IEEE 12th Control and System Graduate Research Colloquium*, Shah Alam, Malaysia, pp. 227-232, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [75] Sidhant Narula et al., "Exploring Research and Tools in AI Security: A Systematic Mapping Study," *IEEE Access*, vol. 13, pp. 84057-84080, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [76] Erik Derner et al., "A Security Risk Taxonomy for Prompt-based Interaction with Large Language Models," *IEEE Access*, vol. 12, pp. 126176-126187, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [77] Umar Iqbal, Tadayoshi Kohno, and Franziska Roesner, "LLM Platform Security: Applying a Systematic Evaluation Framework to OpenAI's ChatGPT Plugins," *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, vol. 7, no. 1, pp. 611-623, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [78] Haoran Li et al., "Privacy in Large Language Models: Attacks, Defenses and Future Directions," *arXiv preprint*, pp. 1-42, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [79] Mohammad Tahaei et al., "A Systematic Literature Review of Human-Centered, Ethical, and Responsible AI," *arXiv preprint*, pp. 1-39, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [80] Heiko Kreutz, and Hamid Jahankhani, *Impact of Artificial Intelligence on Enterprise Information Security Management in the Context of ISO 27001 and 27002: A Tertiary Systematic Review and Comparative Analysis*, Cybersecurity and Artificial Intelligence, Springer, pp. 1-34, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [81] Anna Sidorova, and Kashif Saeed, "Incorporating Stakeholder enfranchisement, Risks, Gains, and AI decisions in AI Governance Framework," *Proceedings of the 55th Hawaii International Conference on System Sciences*, pp. 5943-5952, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]