Mesopotamian journal of Cybersecurity
Vol.5,No.2, **pp**. 514–537
DOI: https://doi.org/10.58496/MJCS/2025/032; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

Cybersecurity risk assessment for identifying threats, vulnerabilities and countermeasures in the IoT

Mohammed Amin Almaiah[1,*], Rami Shehab [2], Tayseer Alkhdour [2], Mansour Obeidat [3], Theyazn H.H. Aldhyani [4]

[1] *King Abdullah the II IT School, University of Jordan, Amman 11942, Jordan.*
[2] *College of Computer Science and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia*
[3] *Applied College, King Faisal University, Al-Ahsa, Saudi Arabia*
[4] *Applied College in Abqaiq, King Faisal University, P.O. Box 400, Al-Ahsa 31982, Saudi Arabia.*

ARTICLE INFO

Article history
Received 19 Jan 2025
Revised 19 Mar 2025
Accepted 04 Apr 2025
Published 18 Jun 2025

Keywords
Cybersecre threats
IoT networks
Risk assessment
Vulnerabilities
Countermeasures

ABSTRACT

To increase the number of connected devices in IoT networks, several types of new cyber threats and attacks also arise in the IoT. Any cyber-attack can cause significant damage to IoT networks and loss of service. Therefore, identifying these threats is one of the main steps in risk assessment and should be considered to create a robust security strategy to avoid IoT network breaches. Cybersecurity assessment in IoT networks is a prime process due to the evolving nature of cyberattacks. Therefore, this research focuses on addressing the current gap by performing a comprehensive analysis to identify the critical threats, vulnerabilities and countermeasures on IoT layers, including physical, data link, network, and transport and application layers. The findings of this study indicated that DDoS attacks and fishing threats were the most common technical threats in the IoT application layer, with percentages of 72% and 66%, respectively. In addition, the results revealed that the SQL injection threat, cross-site scripting (XSS) and cross-site request forgery (CSRF) attacks were also classified as second-level technical threats in the IoT, with percentages of 55%, 53% and 52%, respectively. The third level of technical threats in the IoT was password cracking attacks, with a percentage of 48%. The results revealed that TCP/UDP port scanning, TCP/UDP flooding attack and MQTT attack were the most common technical threats in the IoT transport layer, with percentages of 34%, 33% and 31%, respectively. In addition, DNS poisoning, SYN flooding and desynchronization attacks were also classified as second-level technical threats in the IoT, with percentages of 27%, 26% and 24%, respectively. The third level of technical threats in the IoT included lateral movement attacks and DoS attacks, with percentages of 18% and 15%, respectively. The framework in this study is considered a vital tool for practitioners, policymakers, and researchers to identify, classify, and mitigate cyber threats within IoT systems. The findings from this work can help organizations understand the types of cyber threats and develop robust strategies against cyberattacks.

1. INTRODUCTION

The IoT is one of the promising IT domains in the future, and it has now become a promising domain worldwide. Technological advances in the IoT have resulted in many benefits for many sectors, such as education, medical, industry and others [1]. Today, all of these sectors are moving towards the use of the IoT to meet the greatest possible technological advances. It involves a collection of devices connected with each other and the transfer of data between them without human intervention [2]. These IoT devices can be sensors, smart devices, mobile devices, control systems, software, etc. The heterogeneous devices in IoT networks create a large security challenge, increasing the vulnerability of IoT networks to cyberattacks [3].

Today, cyberthreats are the most critical challenges facing IoT networks, as are increasing the number of cyberattacks on IoT networks and becoming more sophisticated. In fact, cyber-risks in IoT networks can have a considerable impact, including data loss, reputation damage, and network failure. Thus, it is necessary to understand the behavior of cyber threats on IoT networks and identify suitable countermeasures to mitigate their impacts [5]. IoT networks today play a crucial role in the new digital world. IoT devices serve as the backbone of modern IT society by supporting many applications, such as

*Corresponding author. Email: m.almaiah@ju.edu.jo

business operations, scientific research, and driving technological innovation. IoT devices have several benefits, such as being easy to store, retrieve, modify, and delete data and performing several data processing operations. IoT networks are growing daily, creating considerable challenges because new attacks that threaten IoT network security have appeared [6]. Although the Internet of Things (IoT) has transformed various aspects of our daily lives, it also presents significant cybersecurity challenges. One of these challenges is that IoT devices, which often lack robust security features, are vulnerable to a range of threats and attacks in different layers, including the physical, data link, network, transport, and application layers. These vulnerabilities can lead to severe consequences, such as unauthorized data access, identity theft, and system disruptions. Addressing these security challenges requires a comprehensive understanding of the specific threats and attacks associated with each layer, alongside the implementation of effective countermeasures to safeguard IoT environments [7].

In recent years, there have been numerous examples of how even innocuous IoT devices can be abused and repurposed to cause harm. For example, Mirai botnet is one of the more infamous IoT security breaches that occurred in 2016. In Mirai's case, the botnet consisted of 145,607 video recorders and IP cameras [8]. The hacker (a college student) launched an unprecedented attack on OVH (a French web hosting service), using the botnet to take up nearly one terabyte of bandwidth per second. The Mirai botnet targeted another service provider: Dyn. In addition, that time, Mirai brought down enormous sections of the internet, including Netflix, Twitter, Reddit, The Guardian, and CNN. The second well-known attack in the IoT is called Target's credit card breach [9]. In 2013, hackers successfully breached Target's network and stolen credit card information from millions of transactions. They stole login credentials from an HVAC vendor, who was using IoT sensors to help Target monitor their energy consumption and make their systems more efficient [10]. Another cyber incident occurred in 2017, when the FDA announced that more than 465,000 implantable pacemaker devices were vulnerable to hacking. While there were no known hacks and St. Jude Medical quickly updated the devices to fix their security flaws, it was a disturbing revelation with deadly implications. With control of one of these devices, a hacker could literally kill someone by depleting the battery, altering someone's heart rate, or administering shocks. An IoT security flaw essentially turned a life-saving device into a potentially deadly weapon. In 2015, two cybersecurity experts set out to hack a new Jeep Grand Cherokee via its multimedia system. They were successful. They demonstrated that they could use the multimedia system to connect to another piece of software in the vehicle, reprogram it, and then control the engine, steering wheel, brakes, transmission, etc. They effectively turned Jeep Grand Cherokee into a life-size remote control car [11].

By exploiting the vulnerabilities in various interconnected networks, devices and sensors that create the IoT ecosystem, cyber threats in IoT networks can occur. Cyberattacks can exploit security weaknesses, causing losses such as stealing sensitive information, manipulating data, unauthorizing access to IoT devices and disrupting critical infrastructure. Other kinds of security weaknesses in IoT networks include botnets, insecure web or mobile interfaces, outdated software in IoT devices, a lack of data encryption and a lack of network segmentation [12].

Although IoT networks have several benefits, they are more vulnerable to cybersecurity attacks [13]. Furthermore, the increasing use of IoT networks in organizations has created new types of cybersecurity threats that can be exploited. Cybersecurity attacks, such as SQL injection attacks, DDoS attacks and ransomware, which are the greatest risks in the IoT network field, have become more prevalent in IoT networks. Cybersecurity attackers are always developing new attack techniques, and this is an enormous challenge that should be addressed [14]. Thus, an IoT network security analyst must follow the security threat assessment continuously to detect any new evolving threats to protect the IoT network and its data from any modification. Additionally, companies must keep up with the possible threats to their IoT networks, understand their impacts, take measures to prevent them, and mitigate their negative impact on companies. Additionally, they should consider the vulnerabilities of the systems and devices they use and work to address them as soon as they are discovered and try to maintain the confidentiality, integrity and availability of data. The most common threats in IoT networks include malware, SQL injections, and DDoS [15].

IoT devices can be vulnerable for attackers for several reasons, such as outdated software, legacy OS, no OS, basic micro controllers, no security-by-design, a lack of device management, shadow devices and operational limitations [16]. Challenges such as software piracy, malware attacks, and weak authentication exacerbate these vulnerabilities [17]. This research aims to review previous studies related to cybersecurity threats to the IoT. In addition, this study aims to identify and analyse the major threats in the IoT environment and propose solutions to address these vulnerabilities. Therefore, this research aims to answer the following questions:

(1) What are the main cybersecurity threats in IoT environments?
(2) What are the main cybersecurity attacks in IoT environments?
(3) What are the main cybersecurity countermeasures in IoT environments?

2. LITERATURE REVIEW AND BACKGROUND

2.1 Related works

In the literature, several works have explored and classified cybersecurity risks and threats in IoT environments. For example, Altulaihan, Almaiah and Aljughaiman [21] conducted a study to identify the common threats in the IoT environment. They classified the threats on the basis of the layers in the IoT architecture. They reported that DDoS attacks, Man-in-Middle attacks and code injection attacks are the most common types of threats in the IoT environment. The study also identified the most suitable countermeasures to mitigate the impact of cyber threats. Islam and Aktheruzzaman [22] reviewed the different types of cybersecurity threats in IoT devices. They classified cyber threats into three categories: application security, communications security and authentication security. Similarly, Tariq et al. [23] examined existing threats, attacks and countermeasures in the IoT. They classified cyber threats in the IoT on the basis of layered architecture, including connectivity, communication, and management protocols. Pourrahmani et al. [24] provided a comprehensive analysis of the current threats and vulnerabilities in the IoT and offered the main security controls for each protocol layer in the IoT architecture. The study classified the vulnerabilities on the basis of hardware, communication, application and web. They also suggested countermeasures such as secure messaging protocols, implementing encryption, enhancing physical security and separating IT and IoT network traffic.

2.2 IoT architecture layers

In recent years, the term IoT has gained popularity. The IoT is still being researched and developed, and as it grows, it will be able to power more innovative and superior user experiences. Devices, network architecture, and cloud technology form the IoT architecture, which allows IoT devices to connect with one another. An organization's connected deployment has a much better probability of success if its IoT architecture framework is well defined. With respect to IoT architecture, there is no one, broadly accepted consensus. Different researchers have presented several architectural designs. This study focuses on the 3-layer IoT architecture. The 3-layer architecture was introduced in the early stages of the IoT area and consists of perception, network, and application layers, as shown in Figure 1.

A. Perception layer

The perception is the layer where communication with the outside world is provided, objects are recognized and perceived, and necessary information is collected from objects. It is similar to the eyes and ears of the IoT. Technologies such as 2-D barcode tags and readers, GPS, sensors, wireless sensor networks, RFID tags and readers, infrared, and radar are used in this layer [18].

B. Network layer

The network layer is the brain of the IoT. Its main function is the processing and transmission of the information detected in the perception layer. All communication networks (WSNs, mobile networks, the internet, ad hoc networks, etc.) and telecommunication are used in this layer. It provides secure data transmission as well as connections by applying data encoding and mining algorithms [19].

C. Application layer

The application layer provides smart application services to users by combining demanded industrial requests with information technology. The information collected at the network layer is used in many areas, such as smart homes, smart management, smart grids in the application layer, and providing smart solutions [20].

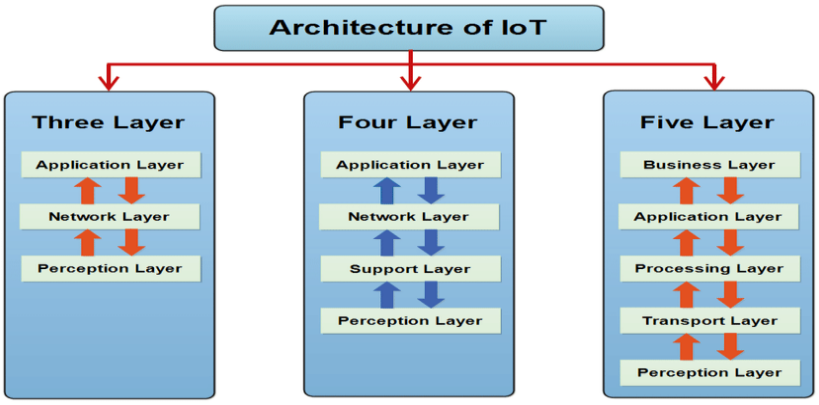

Fig. 1. Three layers of the IoT architecture

2.3 Cybersecurity risk assessment

Cybersecurity risk assessment refers to an assessment of an organization's ability to protect its information and information systems from cyber threats in the IoT field. The main purpose of a cybersecurity risk assessment is to identify, assess, and prioritize threats and attacks to IoT systems. A cybersecurity risk assessment helps organizations identify and prioritize areas for improvement in their cybersecurity programs. It also helps organizations communicate their risks to stakeholders and make informed decisions about how to allocate resources to reduce those risks.

Many cybersecurity risk assessment frameworks and methodologies are available in the literature, but they all share a common goal. For example, the National Institute of Standards and Technology (NIST) cybersecurity framework is one of the most popular risk assessment frameworks. It provides a flexible and structured approach for organizations to assess their cybersecurity risks and prioritize actions to reduce those risks. Another popular risk assessment framework is the ISO 27001:2013 standard. This standard provides a comprehensive approach to information security management, including requirements for risk assessment and risk treatment. Thus, researchers can also develop customized risk assessment frameworks and methodologies. Whatever approach a researcher chooses, the goal should be to identify, assess, and prioritize threats to information and information systems.

In our study, cybersecurity risk assessment is an important process because it can help identify threats and risks in IoT networks and systems. By identifying these risks, steps can be taken to mitigate or reduce them. A risk assessment can also help researchers develop a plan to respond to and recover from a cyberattack in the IoT. In addition, researchers should conduct cybersecurity risk assessments on a regular basis to keep risk profiles up to date in IoT environments.

3. RESEARCH DESIGN AND FRAMEWORK

This section of the study provides the research design and proposes a risk assessment framework for the IoT. The design framework incorporates four main stages: (1) identifying key components, (2) identifying threats, (3) identifying vulnerabilities and (4) identifying countermeasures. Each stage is guided by the results from the literature review. The main objective of the risk assessment framework in this research is to be robust and comprehensive for all types of threats, vulnerabilities and countermeasures for IoT systems. Figure 2 represents the main stages of the risk assessment framework.

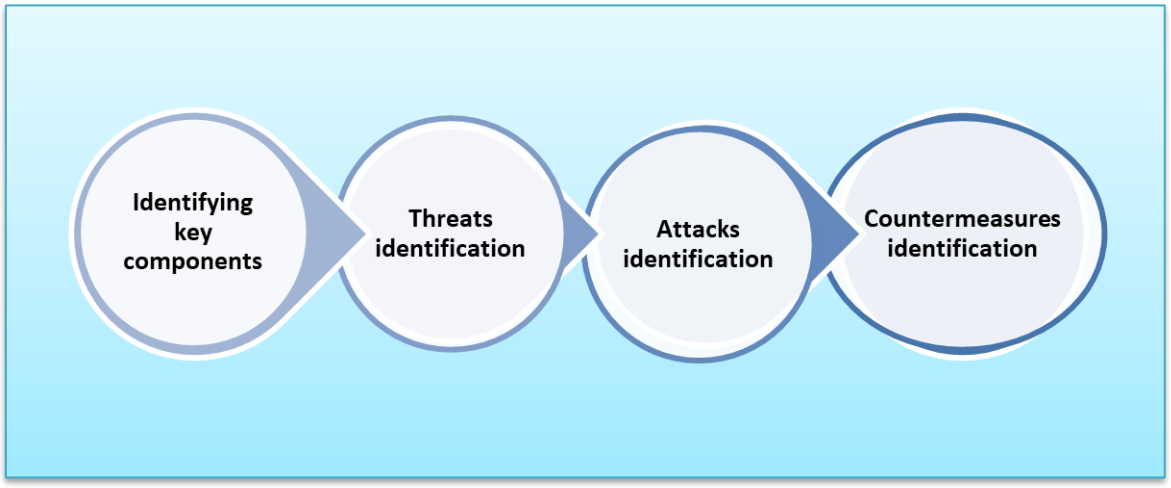

Fig. 2. The main stages of the risk assessment framework

3.1 Stage one: Identifying key components

The first stage in the risk assessment framework includes collecting the data from the literature review findings that form the dataset for this study. This is accomplished through an extensive review of existing studies, models, frameworks and literature in the IoT systems field. The collected data include threat types, vulnerability types and countermeasures methods. The data collected in this stage are analysed in the next stages.

3.2 Stage Two: Threat identification

Once the data are collected in stage one, we analyse them to identify and classify the existing cybersecurity threats in the IoT systems. This stage includes a comprehensive systematic identification of all types of threats that have the potential to exploit IoT system vulnerabilities and result in compromised IoT systems.

3.3 Stage Three: attack identification

In the third stage, after the data are collected, we analyse them to explore the existing technical security vulnerabilities that could be exploited to compromise IoT systems. As part of the risk assessment framework, this stage incorporates a comprehensive systematic review on identifying the critical types of vulnerabilities that could be exploited to compromise IoT systems.

3.4 Stage Four: Countermeasures identification

The last stage of the risk assessment framework involves identifying and classifying effective countermeasures to address potential cybersecurity threats and vulnerabilities in IoT systems. Identifying these countermeasures will be linked with all types of threats and vulnerabilities identified in the previous stages' findings. As a result, this stage is a solution for these threats that could be exploited to compromise IoT systems.

4. FRAMEWORK OF CYBER THREATS, ATTACKS AND COUNTERMEASURES

Figure 3 represents the main steps of the framework for this research. The framework is divided into three main parts: (1) threat identification, (2) attack identification and (3) countermeasures identification. The details of each step of the framework are presented in the subsections below.

4.1 Threats and attack classification in IoT layers

In the first stage of the framework, we identify and classify the existing cybersecurity threats in the IoT layers. This stage incorporates a comprehensive systematic classification of all types of threats that have the potential to exploit IoT layer vulnerabilities and the resulting compromised IoT systems. The classification of threats is divided into five IoT layers: (1) threat identification in the physical layer, (2) threat identification in the data link layer, (3) threat identification in the network layer, (4) threat identification in the transport layer and (5) threat identification in the application layer. The most common cyber threats in the IoT include botnet attacks, man-in-the-middle attacks, social engineering, data and identity defeats, and denial of service attacks. These threats can exploit sensitive information and compromise the confidentiality of IoT networks. In addition, threats in the IoT occur at the data transmission layer, which is a part of the network layer. Therefore, it is crucial to understand and classify these types of threats and propose suitable countermeasures at IoT layers to ensure the security of IoT devices and networks. The classification analysis was based on multiple dimensions, such as threat characteristics, threat behavior and their impacts in each layer. Each type of threat is discussed by a description that clarifies its potential impact on the IoT layers. In the subsections below, we provide the detailed threat classification of IoT layer threats.

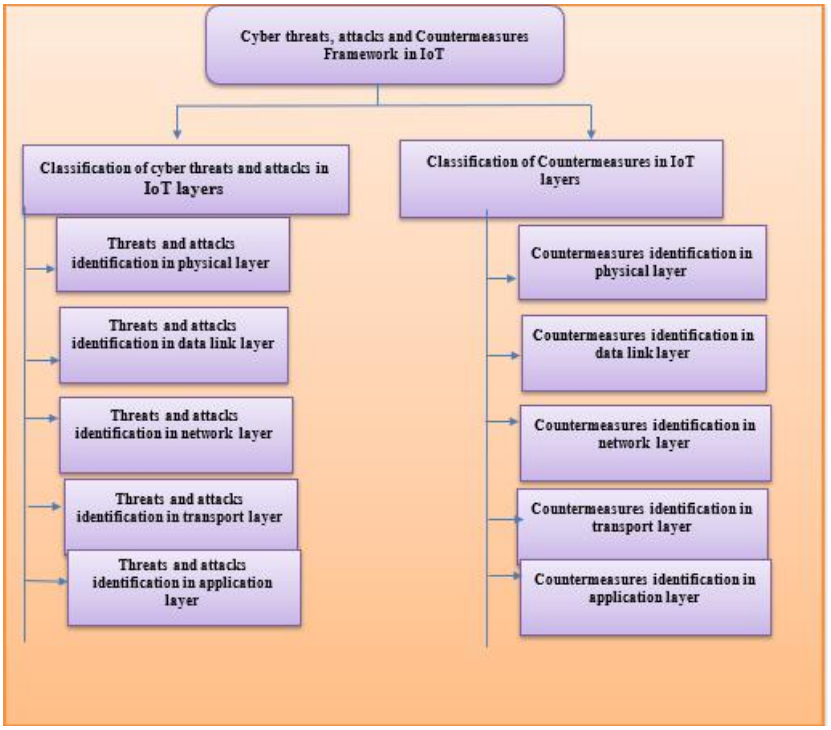

Fig. 3. Framework of cyber threats, attacks and countermeasures.

A. Threat classification in the physical layer

As software-based defenses have improved, some attackers have turned their attention to physical security to gain access. IoT devices can sometimes be relatively easy to access, especially if they are in remote or unmonitored locations. A breach of the physical IoT security layer could allow malicious attackers to gather information about an IoT device itself, copy any data about or gathered by the device, and even change its programming. Physical access to IoT devices could enable side-channel analysis, setting resets, physical tampering, optical or electromagnetic fault injection, and other attacks. Ultimately, a compromised IoT device can be used to access other parts of the network. Examples of physical layer threats include node tampering, jamming and replication. Table 1 shows the most common threats in the physical layer.

For example, identity faking threat is a type of cyber-attack that involves pretending that someone aims to access their personal information or conduct fraudulent activities. Another type of threat is imitation attacks such as spoofing and cloning, which use impersonation for unauthorized access to IoT devices. Man in the middle is another type of threat in the physical layer, which occurs when attackers gain unauthorized access to the broker and assume a man-in-the-middle position; they could take control of the entire IoT application. The denial of service (DoS) threat in the physical layer occurs when attackers disrupt services for legitimate users by overwhelming target servers with an extensive volume of requests. The impacts of this type of threat include service interruption, overwhelming target servers and disruption of services for legitimate users. Tampering threats through gathering data from multiple sources, the data can be modified.

TABLE I. CLASSIFICATION OF CYBER THREATS IN THE PHYSICAL LAYER.

	Threat	Description	Example
physical layer.	Identity faking attack [1(23)]	A type of cyber-attack that involves pretending to be someone else to access their personal information or conduct fraudulent activities.	• Access to Personal Information or Fraudulent Activities
	Imitation attack [2]	Using impersonation for unauthorized access; involves spoofing and cloning.	• Spoofing • Cloning
	man in the middle attacks [2][3]	If adversaries gain unauthorized access to the broker and assume a man-in-the-middle position, they could take control of the entire IoT application.	• Unauthorized Access to the Broker • Control of the Entire IoT Application
	Denial of Service (DoS) [2][3]	Attackers disrupt services for legitimate users by overwhelming target servers with an extensive volume of requests.	• Service Interruption • Overwhelming Target Servers • Disruption of Services for Legitimate Users
	Physical attack [1(28)]	When an individual or group physically assaults or threatens to harm an asset, with or without tools.	• Physical injury • Emotional trauma • Increased fear and insecurity
	Blocking attack[2]	Denial of Service (DoS), jamming, and malware attacks; these can disrupt network operations	• Jamming • Malware Attacks • Denial of Service (DoS) Attacks
	increasing power consumption[3]	Attackers could manipulate IoT edge devices by injecting false code or creating infinite loops, leading to excessive power usage and rapid battery depletion	• Injection of False Code or Infinite Loops • Excessive Power Usage and Rapid Battery Depletion
	Tampering [2]	Gathering data from multiple sources; the data might be modified.	• Data Modification

B. Threat classification in the data link layer

The data link layer in IoT systems is vulnerable to cyberattacks. A breach at this layer could allow attackers to exploit MAC protocols to carry out various attacks. These threats often target specific vulnerabilities in systems that are misconfigured or not updated properly, and some are particularly associated with LAN networks. Common threats at the data link layer include collision, denial of service (DoS), ARP spoofing, and unfairness. For example, spoofing is an identity theft technique where an attacker impersonates another device on the network by altering its MAC address. DoS attacks aim to disrupt or limit access to a network device by overwhelming it with excessive traffic. Sniffing occurs when an attacker passively monitors transmitted traffic without interference. DHCP spoofing involves an attacker placing a fake DHCP server on the network to distribute false network information to clients. ARP poisoning manipulates the ARP table, where IP addresses associated with MAC addresses are stored, allowing the attacker to replace a legitimate MAC address with their own to redirect traffic.

C. Threat classification in the network layer

The most common cyber threats in IoT systems focus on the network layer [30], [31]. The network layer is considered one of the vulnerabilities in IoT networks, and attacks can disrupt the packets while they are in transit between the source and the destination. The cyber threats in the network layer can exploit sensitive information and compromise the confidentiality of the network. These threats include botnet attacks, man-in-the-middle attacks, social engineering, data and identity defeats, denial of service attacks, routing attacks, Sybil attacks, black holes, spoofing and alteration. It is crucial to identify and address these threats and take precautions at the network layer to ensure the security of IoT devices and networks. Table 3 shows the most common threats in the network layer. For example, botnet is essentially a distributed network of computers. A botnet is an army of devices that can take down servers. These threats consist of infected devices such as sensors, cameras and printers, also known as "zombies," to launch coordinated large-scale distributed denial of service attacks (DDoS) and compromise other IoT devices. Command and control servers are used with peripherals to execute the attacks. Examples of these attacks include Mirai, Hydra, Bashlite, luabot and Aidra. Sybil threat is one of the most common threats in the network layer, in which the attacker sends many fake requests to the network from a single user. This attacker pretends many fake identities by creating several accounts from different IP addresses. In this case, the attacker can control the overall network. This type of threat can affect performance, resource utilization and data integrity. Another type of threat in the network layer is called a sinkhole attack. This threat focuses on managing the traffic network through sending counterfeit data to enter the entire traffic of other adjoining meeting focuses. DoS is another type of threat in this layer; this technique attempts to prevent or limit access to a network device by saturating some of its resources, for example, by flooding the target device with unwanted traffic.

E. Threat classification in the application layer

The most common cyber threats faced by the application layer in the IoT include various types of attacks, such as ransomware assaults, jamming, spoofing, data tampering, and fake nodes. The widespread use of the IoT in smart applications such as agriculture, economies, residences, and health and fitness makes it vulnerable to these threats because of the lack of robust protection mechanisms. Researchers are particularly concerned with securely transferring data among IoT objects, highlighting the critical importance of addressing security challenges at the application layer level. These security concerns impact the interconnected nodes of IoT systems, emphasizing the need for comprehensive strategies to mitigate risks and safeguard sensitive information within IoT environments. The IoT application layer suffers from various vulnerabilities that are at risk of being compromised, including outdated or unsecured IoT app components, weak or hardcoded passwords, unsecured network services and ecosystem interfaces, a lack of an update process or mechanism and unsecured data storage and transfer. Table 5 summarizes the common cyber vulnerabilities in the application layer of the IoT with their descriptions.

Table 6 shows the most common threats in the application layer. For example, fishing is a type of social engineering attack that often involves fake emails sent from seemingly legitimate sources, such as known contacts or trusted vendors, urgently requesting assistance or information. This attack is sometimes referred to as a business email compromise (BEC) attack. Another common threat at the application layer is password cracking, where cybercriminals use password-cracking tools or brute force methods to access passwords stored in databases. Weak passwords, especially those reused across multiple sites, are particularly at risk. Buffer overflow attacks occur when malicious input is fed into a vulnerable program, causing it to overflow its memory and trick the computer into executing the attacker's code. Additionally, format string attacks occur when an application fails to properly validate input, allowing a crafted input string to overwrite the application with malware or cause it to crash. SQL Injection, this threat involves injecting malicious SQL code into input fields on a website. If the program does not adequately validate or sanitize user input, an attacker can change the SQL queries executed, potentially gaining unauthorized access to a database or affecting its integrity. Additionally, cross-site scripting (XSS) threats occur when malicious code is introduced into web pages that are read by other users. Cross-site request forgery (CSRF), a CSRF threat, involves an attacker tricking a user into acting on a website without their knowledge. This can lead to actions such as changing account settings or making transactions without the user's knowledge. DDoS Thats on Specific Applications: Some threats target applications, such as web services, APIs, or online gaming servers. Attackers flood these applications with traffic to disrupt their functionality. In summary, application layer threats are malicious activities that compromise the security, integrity, and availability of computer systems and user data. These attacks can result in significant harm to individuals, organizations, and even society as a whole.

TABLE II. CLASSIFICATION OF CYBER THREATS IN THE DATA LINK LAYER

Threat	Description	Example
Spoofing	Spoofing is an identity theft technique where an attacker impersonates another device on the network by altering its MAC address.	• Spoofing
Denial of Service (DoS)	DoS attacks aim to disrupt or limit access to a network device by overwhelming it with excessive traffic.	• flooding the target device with unwanted traffic
sniffing	Sniffing occurs when an attacker passively monitors transmitted traffic without interfering.	• sniffing
DHCP spoofing	DHCP spoofing involves an attacker placing a fake DHCP server on the network to distribute false network information to clients.	• DHCP spoofing
ARP poisoning	ARP poisoning manipulates the ARP table, where IP addresses associated with MAC addresses are stored, allowing the attacker to replace a legitimate MAC address with their own to redirect traffic.	• ARP poisoning
Confidentiality concerns and data exploitation [1(2)]	Data exploitation involves the illicit use of personal information, frequently enabled by AI models. This results in privacy violations because people are often unaware of the data being generated and analysed by various consumer products and digital technologies.	• Unauthorized data analysis • Potential identity theft • Privacy breaches
Privacy attack [2].	Revealing confidential data could be linked to subsequent attacks.	• Confidential Data Exposure • Increased Vulnerability • Potential for Subsequent Attacks
Context privacy leakage [1(26)]	Privacy breaches can happen when a user unknowingly grants "dangerous" permissions to a malicious application, allowing it access to sensitive data and personal information.	• Unauthorized access to sensitive data • Increased vulnerability to cyber attacks • Malicious Exploitation
Lack of user awareness of protection [1(26)]	A lack of security awareness can result in the inadvertent exposure of sensitive company or personal data.	• Potential Damage • Inadvertent Exposure • Increased Risk
Gathering[2]	Gathering data from multiple sources; the data might be modified.	• Data Modification
Fabrication [2]	Introduces false data; compromises data integrity.	• Introduction of False Data • Compromise of Data Integrity

TABLE III. CLASSIFICATION OF CYBER THREATS IN THE NETWORK LAYER

	Threat	Description	Example
Transport layer	Lateral movement	An attacker employs network scanning, discovery, and vulnerability exploits to detect devices within the network, progressively moving from one device to another until gaining full access to the entire network.	The attacker can control the overall network and damage it.
	TCP/UDP port scanning	Discovers vulnerabilities by sending packets to specific ports and then analysing the responses from the device	TCP/UDP port scanning
	De-Synchronization	Sending control flags that synchronize endpoints	The attacker injects packets with fake sequence numbers of control flags that desynchronize endpoints.
	DoS	This threat attempts to prevent or limit access to a network device by saturating some of its resources, for example, by flooding the target device with unwanted traffic.	Flooding the target device with unwanted traffic.
	SYN-flooding	System flooding during the SYN handshaking phase.	System flooding during the SYN handshaking phase
	DNS poisoning threat	DNS poisoning is a threat where false information is injected into a DNS server, causing it to respond to queries by redirecting users to a malicious site. DNS does not verify the accuracy of the entered information, making it vulnerable to such attacks.	Corrupt information is inserted into a DNS server, which then responds to queries by directing users to a malicious destination.
	MQTT	Data Transit Attacks, Scalable Key management	Transit Attacks, Scalable Key management
	TCP/UDP flood	TCP/UDP flood (DDoS) attacks target the host's ports at Layers 3 and 4 by sending a large volume of IP packets with UDP datagrams, overwhelming the device and rendering it unable to respond.	Overwhelming the device and rendering it unable to respond

TABLE IV. CLASSIFICATION OF CYBER THREATS IN THE TRANSPORT LAYER

	Threat	Description	Example
Network layer	Sybil threat [2].	Sybil threat is one of the most common in network layer, which attacker sends a lot of fake requests to network from single user. Where this attacker pretends many fake identities through creating several accounts from different IP addresses.	The attacker can control the overall network. This type of threat can effect on the performance, resource utilization and data integrity.
	Botnet	Botnet is essentially a distributed network of computers. These threats consist of infected devices such as sensors, cameras and printers, also known as “zombies” to launch coordinated large scale distributed denial of service attacks (DDoS) and compromise other IoT devices.	A botnet is an army of devices that can take down servers.
	Sinkhole	This threat focuses on managing traffic network through sending counterfeit data to entrance entire traffic of other adjoining meeting focuses.	Sinkhole
	DoS	DoS attacks aim to disrupt or restrict access to a network device by overwhelming its resources, such as flooding the target with excessive, unwanted traffic.	Flooding the target device with unwanted traffic.
	Privacy leakage [1(26)]	Privacy leakage can happen when a user unknowingly grants "dangerous" permissions to a malicious application, allowing it access to sensitive data and personal information.	• unauthorized access to sensitive data • increased vulnerability to cyber attacks • malicious exploitation
	Privacy attack [2].	Revealing confidential data could be linked to subsequent attacks.	• confidential data exposure • increased vulnerability • potential for subsequent attacks
	privacy leakage[3]	The gathering of personal data, including health information, location details, or images, threatens client privacy.	• compromised client privacy • potential misuse of sensitive data • increased risk of identity theft and fraud
	sending false code [3]	This false code can force sensors to execute unintended actions or compromise the entire IoT system, potentially leading to a distributed denial of service (DDoS) attack.	• execution of unintended actions • compromise of the entire iot system • potential distributed denial of service (ddos) attack
	reprogram attack [3]	if the programming process is not properly secured, adversaries may try to rewrite the secret code, which can cause the entire IoT system to malfunction	• rewriting of secret code • malfunctioning of the entire iot system
	Tampering [2]	Gathering data from multiple sources; the data might be modified.	• data modification

TABLE V. CLASSIFICATION OF CYBER VULNERABILITIES IN THE APPLICATION LAYER

	Vulnerabilities	Description
Application layer	Outdated or unsecured IoT app components.	Many IoT applications use third-party frameworks and libraries when built. If they're obsolete or have known vulnerabilities and are not validated when installed in a network, they could pose security risks.
	Lack of an update process or mechanism.	IT admins unintentionally exclude many IoT apps and devices from updates because they are invisible on the network. Additionally, IoT devices may not even have an update mechanism incorporated into them due to age or purpose, meaning admins cannot update the firmware regularly.
	Unsecured network services and ecosystem interfaces.	Each IoT app connection has the potential to be compromised, either through an inherent vulnerability in the components themselves or because they're not secured from attack. That includes any gateway, router, modem, external web app, API or cloud service connected to an IoT app.
	Weak or hardcoded passwords.	Many passwords are easy to guess, publicly available or cannot be changed. Some IT staff do not bother changing the default password that shipped with the device or software.
	Unsecured data storage and transfer.	Different data types may be stored and transmitted between IoT applications and other connected devices and systems. All must be properly secured via Transport Layer Security or other protocols and encrypted as needed.

TABLE VI. CLASSIFICATION OF CYBER THREATS IN THE APPLICATION LAYER

	Threat	Description	Example
Application Layer	Phishing threats	Phishing is a type of social engineering attack, often involving fake emails sent from seemingly legitimate sources, such as known contacts or trusted vendors, urgently requesting assistance or information.	User Harm: Individual users can be harmed by application layer attacks such as phishing, which fool them into revealing sensitive information or engaging in harmful actions.
	Password cracking	Password cracking, where cybercriminals use password-cracking tools or brute force methods to access passwords stored in databases.	Weak passwords that are reused across multiple websites are particularly susceptible to compromise.
	Buffer overflow	Buffer overflow attacks occur when malicious input is fed into a vulnerable program, causing it to overflow its memory and trick the computer into executing the attacker's code.	This can deceive the computer into executing the attacker's program.
	Format string threat	Format string attacks happen when an application fails to properly validate input, allowing a crafted input string to overwrite the application with malware or cause it to crash.	When an application fails to properly validate input, a malicious input string can overwrite the application, leading to a crash or allowing malware to be injected.
	SQL Injection	SQL Injection, this threat involves injecting malicious SQL code into input fields on a website. If the program does not adequately validate or sanitize user input, an attacker can change the SQL queries executed, potentially gaining unauthorized access to a database or affecting its integrity.	Unauthorized access to a database or affecting its integrity.
	Cross-Site Scripting (XSS)	Cross-Site Scripting (XSS) threat, this threat occur when malicious code is introduced into web pages being read by other users.	Unauthorized access to a webpage or affecting its integrity.
	Cross-Site Request Forgery (CSRF),	CSRF threat involves an attacker tricking a user into acting on a website without their knowledge. This can lead to actions like changing account settings or making transactions without the user's knowledge.	Changing account settings or making transactions without the user's knowledge.
	DDoS	DDoS threats on Specific Applications: Some threats target applications, such as web services, APIs, or online gaming servers.	Attackers flood these applications with traffic to disrupt their functionality

4.2 Countermeasures classification in IoT layers

In the next stage of the framework, we identify and classify the necessary countermeasures and security controls in the IoT layers. This stage incorporates a comprehensive systematic classification of all types of countermeasures and security controls that have the potential to defend against IoT layer attacks, and the results can be used to protect IoT systems. The classification of countermeasures is divided into five IoT layers: (1) countermeasure identification in the physical layer, (2) countermeasure identification in the data link layer, (3) countermeasure identification in the network layer, (4) countermeasure identification in the transport layer and (5) countermeasure identification in the application layer. The most important countermeasures and security controls in the IoT include web application firewalls (WAFs), intrusion prevention systems (IPSs), endpoint protection platforms (EPPs), network access control (NAC), eXtended detection & response (xDR), virtual private networks (VPNs), SASE/SSE, encrypted data transfer, and network-based firewalls. These countermeasures can protect sensitive information and prevent compromising the confidentiality of IoT networks. Therefore, it is crucial to understand and classify these types of security controls and propose suitable countermeasures at IoT layers to ensure the security of IoT devices and networks. The classification analysis was based on multiple dimensions, such as the type of threats and attacks, the type of IoT layer and their protection roles in each layer. All the countermeasures were discussed via a description that clarified their potential role in protecting the IoT layers. In the subsections below, we provide the detailed countermeasure classification for IoT layers.

A. Countermeasures classification in the physical layer

Physical layer security is crucial, as IoT devices are compact and have limited computational capabilities, making traditional encryption methods insufficient. It is crucial to address cyberattacks and take countermeasures at the physical layer to ensure the security of IoT objects. Thus, in this section, we conduct an extensive analysis of the necessary countermeasures with the aim of reducing and mitigating the impact of the vulnerabilities associated with cyberattacks in the physical layer. In our study, in Table 7, we identified a range of countermeasures that represent security controls to enhance the IoT physical layer security against cyberattacks. For example, auditing is a form of security control in the physical layer that aims to ensure that all important system events are securely logged into an authorized log collection system. Another security control method is authorization, and access control is used to configure all systems to ensure that only authorized personnel can access the system. In addition, all systems are configured to ensure that only authorized personnel can access assets according to their permissions level. Least functionality is a security control that aims to reduce

the device's attack surface by reducing the number of applications, daemons, and services or ports that operate on a device to only those that are required for basic operation. Another security control method is least privilege, which aims to grant only the minimum required access for people accomplish their tasks—and no more. Administrative access (root) must only be granted just-in-time. Device hardening, another countermeasure for the physical layer, is used to ensure firmware integrity. Devices should be updated, encrypted, and intrude detection and antimalware configured. IoT device management is a solution that should be used to manage IoT devices centrally. The frequency hopping spread spectrum technique, electronic product code (EPC) technique, anonymous forward-secure mutual authentication on protocols (AFMAP) and access control list (ACLs) are used.

B. Countermeasures classification in the data link layer

The data link layer is highly prone to several cyberattacks [32]. Therefore, it is crucial to address these attacks and take countermeasures at the data link layer to ensure the security of IoT networks [33], [34]. Thus, in this section, we conducted an extensive analysis of the necessary countermeasures with the aim of reducing and mitigating the impact of the vulnerabilities associated with cyberattacks in the data link layer in Table 9. In our study, in Table 8, we identified a range of countermeasures that represent security controls to enhance the IoT data link layer security against cyberattacks. Several security countermeasures have been developed to mitigate these types of attacks. One of the important methods is the spanning tree protocol (STP), which prevents network loops by creating a single path between devices using bridge priority and protects against bandwidth flooding attacks by filtering specific Layer 2 packets, such as fraudulent broadcast requests or bridge protocol data unit (BPDU) frames. Port security measures, such as the 802.1x Protocol extension, restrict access to ports, allowing only authenticated devices to connect by enabling ports after successful authentication against a server. Another security feature is MACsec (Media Access Control Security – 802.1AE), which ensures confidentiality by encrypting transmitted information to prevent interception (sniffing) and verifying the authenticity and integrity of the data source [35], [36], [37]. DHCP Snooping, operating at Layer 2, filters unauthorized DHCP traffic, preventing DHCP spoofing attacks by blocking unauthorized DHCP servers and preventing fraudulent IP address acquisition. Additional security measures include closing unused ports, ensuring access through secure protocols such as SSH instead of Telnet, changing default passwords on network devices, monitoring devices with centralized alerts for event correlation, configuring logs for traceability, and maintaining external backups of device configurations [38], [39].

TABLE VII. CLASSIFICATION OF THE MOST CRITICAL SECURITY COUNTERMEASURES FOR THE PHYSICAL LAYER

	Countermeasures	Description
Physical Layer	Auditing	Auditing is a security control in physical layer that aims to ensure all important systems events are securely logged into an authorized log collection system.
	Authorization and access control	Authorization and access control is used to configure all systems to ensure that only authorized personnel can access the system. In addition, configure all systems to ensure that only authorized personnel can access assets according to their permissions level.
	Least functionality	Least functionality is a security control aims to reduce the device's attack surface by reducing the number of applications, daemons, and services or ports that operate on a device to only those that are required for basic operation.
	Least privilege	Least privilege that aims to grant only the minimum required access for people accomplish their tasks—and no more. Administrative access (root) must only be granted on a just-in-time.
	Device hardening	Device hardening also another countermeasure for physical layer is used to ensure firmware integrity, devices should be updated, encrypted, and have intrusion detection and antimalware configured.
	Secure Device Placement	Ensure that IoT devices are installed in physically secure locations, away from unauthorized access. This prevents tampering or theft of devices, reducing the risk of security breaches.
	Tamper-Resistant Enclosures	Utilize tamper-resistant enclosures and casings for IoT devices to deter physical attacks. These enclosures should be designed to withstand tampering attempts and provide mechanisms for detecting unauthorized access.
	Physical Access Controls	Implement robust access control measures to restrict physical access to critical infrastructure components, such as server rooms or data centers. This may include biometric authentication, keycard systems, or security personnel stationed at entry points.
	Encryption and Authentication	Employ encryption techniques to secure data transmitted over IoT networks, ensuring confidentiality and integrity. Additionally, implement strong authentication mechanisms to verify the identity of devices and users accessing the network.

C. Countermeasures classification in the network layer

In the IoT network layer, maintaining strong security is critical for safeguarding sensitive data and ensuring system integrity. The widespread adoption of IoT networks has introduced numerous potential entry points for cyberattacks, underscoring the need for effective security measures. Securing IoT networks requires implementing zero-trust policies, proactive defense strategies, and robust network security protocols to mitigate threats. One key approach is the adoption of zero-trust policies, which demand continuous verification of all devices and users connecting to the network, thereby reducing the attack surface area and preventing unauthorized access by eliminating implicit trust. Additional defenses include regularly updating firmware and software, conducting penetration testing, and monitoring network traffic for suspicious activity. Encryption protocols, such as the advanced encryption standard (AES) and secure hash algorithm (SHA), are essential for protecting IoT ecosystems by encoding data to prevent unauthorized access and ensure confidentiality. The implementation of multifactor authentication and auditing network configurations also contributes significantly to enhancing security in the network layer. Furthermore, employing firewalls, intrusion detection/prevention systems, and secure communication channels such as virtual private networks (VPNs) can help protect IoT network infrastructures from malicious attacks [43-47].

TABLE VIII. CLASSIFICATION OF THE MOST CRITICAL SECURITY COUNTERMEASURES FOR THE DATA LINK LAYER

	Countermeasures	Description
Data Link Layer	Spanning Tree Protocol (STP)	Spanning Tree Protocol (STP) prevents network loops by creating a single path between devices using bridge priority and protects against bandwidth flooding attacks by filtering specific Layer 2 packets, such as fraudulent broadcast requests or Bridge Protocol Data Unit (BPDU) frames.
	Port Security such as 802.1x Protocol extension	Port Security measures, like the 802.1x Protocol extension, restrict access to ports, allowing only authenticated devices to connect by enabling ports after successful authentication against a server.
	MACsec such as Media Access Control Security – 802.1AE	MACsec (Media Access Control Security – 802.1AE), which ensures confidentiality by encrypting transmitted information to prevent interception (sniffing) and verifying the authenticity and integrity of the data source.
	DHCP Snooping	DHCP Snooping, operating at Layer 2, filters unauthorized DHCP traffic, preventing DHCP Spoofing attacks by blocking unauthorized DHCP servers and preventing fraudulent IP address acquisition.
	Close any unused ports	closing unused ports
	SSH	ensuring access through secure protocols like SSH instead of Telnet
	change the default passwords	changing default passwords on network devices
	Monitor the devices	monitoring devices with centralized alerts for event correlation
	Configure log settings	Configuring logs for traceability, and maintaining external backups of device configurations.

TABLE IX. CLASSIFICATION OF THE MOST CRITICAL SECURITY COUNTERMEASURES FOR THE NETWORK LAYER

	Countermeasures	Description
Application Layer	Web Application AF)	Web Application Firewalls (WAF) is one of the critical security controls that protect web applications from various ding injection attacks, cross-site scripting (XSS), cross-site request forgery (CSRF), and others, several security be employed.
	Intrusion Prevention)	Intrusion Prevention Systems (IPS) are designed to detect and block attacks at multiple levels.
	Endpoint Protection PP)	Endpoint Protection Platforms (EPP) provide multilayered security for endpoints, typically including anti-malware, valls, ad blockers, and intrusion prevention features.
	Network Access C)	Network Access Control (NAC) limits unauthorized network access and can assess the security status of devices, plications to enforce security policies.
	eXtended Detection & DR)	eXtended Detection & Response (xDR) consolidates data from endpoints, networks, cloud services, and providing a holistic view of threats and potential intrusions.
	Virtual Private Network	Virtual Private Networks (VPN) establish encrypted connections from remote locations to the enterprise network, ure communication within protected boundaries.
	Anti-Phishing n (APA)	Anti-Phishing Authentication (APA) technique that uses 2-way authentication and zero knowledge password
	Address Space domization (ASLR)	Address Space Location Randomization (ASLR) that randomly moves around the address space locations of data cally, buffer overflow attacks need to know the locality of executable code, and randomizing address spaces makes impossible.
	Authentication	Multifactor authentication
	Authorization and l	Authorization and access control is used to configure all systems to ensure that only authorized personnel can stem. In addition, configure all systems to ensure that only authorized personnel can access assets according to their evel.

D. Countermeasures classification in the application layer

The application layer provides services for users through IoT applications. Additionally, the layer stores information or data in its database and retrieves information when the user needs it. Therefore, applying robust security countermeasures is paramount to protect sensitive data and maintain the integrity of applications. The proliferation of IoT applications has opened up a multitude of entry points for cyberattacks, making it imperative for researchers to identify the necessary security countermeasures. There are several security countermeasures for securing IoT applications and mitigating cybersecurity threats, as presented in Table 10. For example, Web Application Firewalls (WAFs) are critical security controls that protect web applications from various attacks, including injection attacks, cross-site scripting (XSS), cross-site request forgery (CSRF), and others, and several security measures can be employed. Intrusion prevention systems (IPSs) are designed to detect and block attacks at multiple levels. Endpoint protection platforms (EPPs) provide multilayered security for endpoints, typically including antimalware, endpoint firewalls, ad blockers, and intrusion prevention features. Network access control (NAC) restricts unauthorized access to networks and can also validate the security posture of devices, users, and applications to enforce policies. eXtended Detection & Response (xDR) integrates data from endpoints, networks, cloud services, and applications, offering a comprehensive view of threats and intrusions. Virtual private networks (VPNs) create encrypted tunnels from remote locations in the enterprise network, ensuring secure communication within perimeter defenses. In black box testing, a web crawler is used to identify the point at which the SQL can perform; then, the application's response is monitored. The antiphishing authentication (APA) technique uses 2-way authentication and zero-knowledge password proof. Address space location randomization (ASLR), which randomly moves around the address space locations of data regions. Typically, buffer overflow attacks need to know the locality of executable code, and randomizing address spaces makes this virtually impossible.

5. ANALYSING THE MOST COMMON THREATS AND ATTACKS IN IOT LAYERS

This section presents an analysis of the most common threats and attacks in IoT layers, including the physical layer, data link layer, network layer, transport layer and application layer. Figure 4 shows the analysis results of the classifications of the most common cyber threats and attacks in the physical layer. The results indicated that denial-of-service attacks (DoS) and middle-level attacks were the most common technical threats in the IoT, with percentages of 26% and 20%, respectively. Man-in-middle attacks and imitation attacks were also classified as the second level of technical threats in the IoT, with percentages of 20% and 14%, respectively. The third level of technical threats in the IoT included increasing power consumption, tampering and identity faking attacks, with percentages of 7%, 6% and 4%, respectively. The remaining types of technical threats, such as physical attacks, were at the lowest level of technical threats in the IoT, with a percentage of 2%.

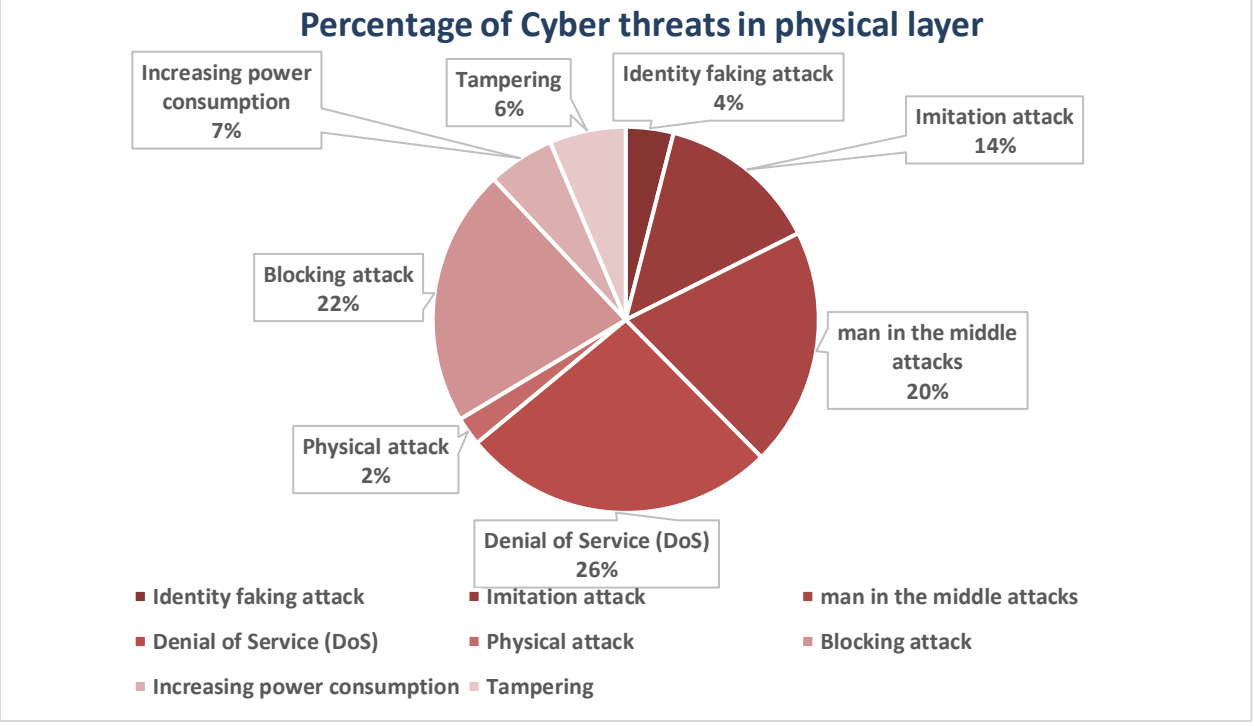

Fig. 4. Analysis of cyber threats in the physical layer.

Figure 5 shows the analysis results of the classifications of the most common cyber threats and attacks in the data link layer. The results indicated that DHCP spoofing attacks, ARP poisoning attacks and sniffing were the most common technical threats in the IoT, with percentages of 41%, 39% and 35%, respectively. Spoofing attack and Denial of Service (DoS) attacks were also classified as the second level of technical threats in the IoT, with percentages of 25% and 23%, respectively. The third level of technical threats in the IoT included privacy attacks and context privacy leakage, with percentages of 15% and 16%, respectively. The remaining types of technical threats, such as confidentiality concerns, data exploitation attacks, and gathering and fabrication, were at the lowest level of technical threats in the IoT, with percentages of 8% and 7%, respectively.

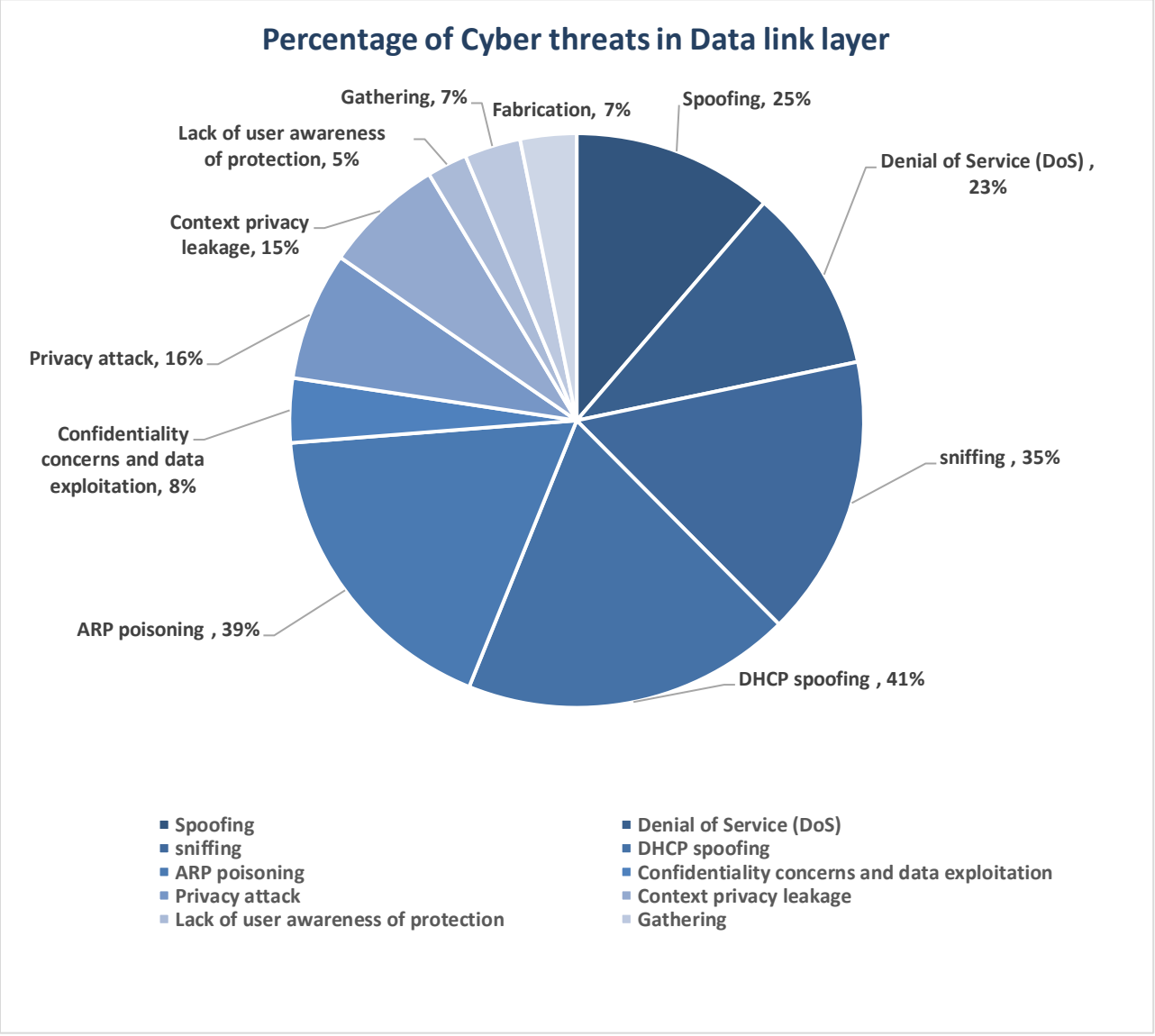

Fig. 5. Analysis of cyber threats in the data link layer.

Figure 6 presents the analysis results of the classifications of the most common cyber threats and attacks in the network layer. The results revealed that Sybil threats, Botnet attacks and sinkhole attacks were the most common technical threats in the IoT network layer, with percentages of 52%, 49% and 45%, respectively. In addition, the results revealed that denial-of-service (DoS) attacks and reprogramming attacks were also classified as the second level of technical threats in the IoT, with percentages of 39% and 37%, respectively. The third level of technical threats in the IoT includes privacy attacks and context privacy leakage, with percentages of 29% and 25%, respectively. The remaining types of technical threats, such as sending false code and tampering, were at the lowest level of technical threats in the IoT, with percentages of 12% and 10%, respectively.

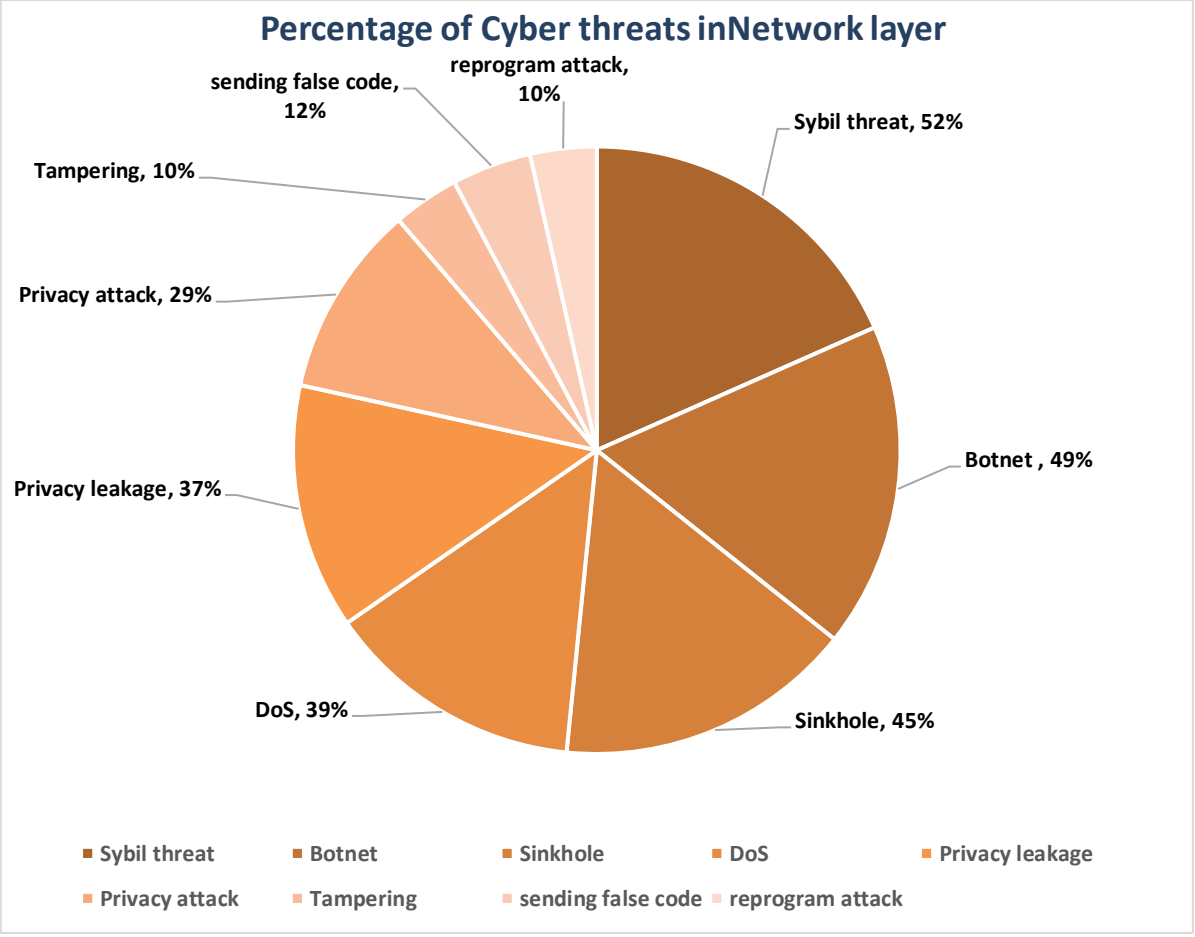

Fig. 6. Analysis of cyber threats in the network layer.

The results in Figure 7 depict the analysis results of the classifications of the most common cyber threats and attacks in the transport layer. The results revealed that TCP/UDP port scanning, TCP/UDP flooding attack and MQTT attack were the most common technical threats in the IoT transport layer, with percentages of 34%, 33% and 31%, respectively. In addition, DNS poisoning, SYN flooding and desynchronization attacks were also classified as second-level technical threats in the IoT, with percentages of 27%, 26% and 24%, respectively. The third level of technical threats in the IoT included lateral movement attacks and DoS attacks, with percentages of 18% and 15%, respectively.

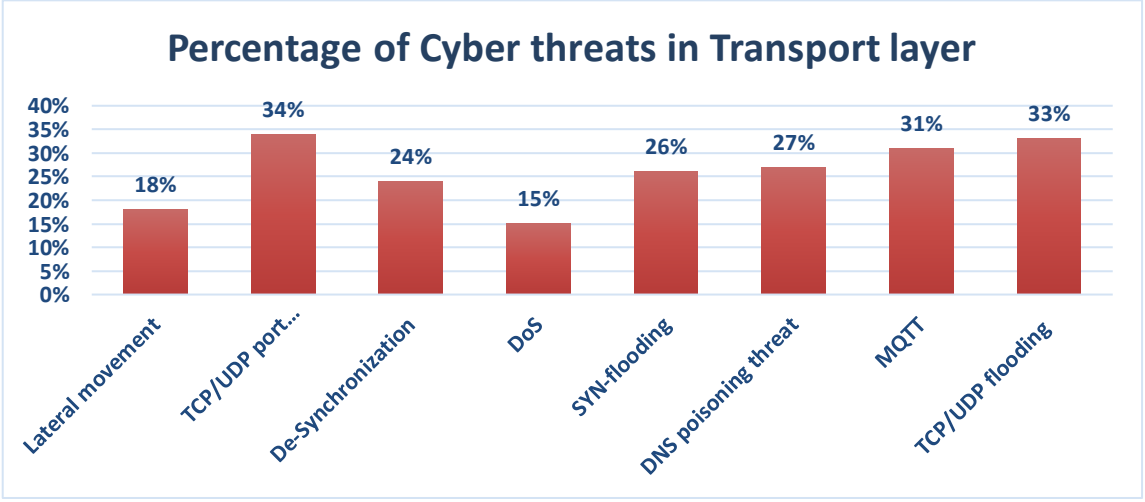

Fig. 7. Analysis of cyber threats in the transport layer.

The results in Figure 8 represent the analysis results of the classifications of the most common cyber threats and attacks in the application layer. The results revealed that DDoS attacks and phishing threats were the most common technical threats in the IoT application layer, with percentages of 72% and 66%, respectively. In addition, the results revealed that the SQL injection threat, cross-site scripting (XSS) and cross-site request forgery (CSRF) attacks were also classified as second-level technical threats in the IoT, with percentages of 55%, 53% and 52%, respectively. The third level of technical threats in the IoT was password cracking attacks, with a percentage of 48%. The remaining types of technical threats, such as buffer overflow and format string threat, were at the lowest level of technical threats in the IoT, with percentages of 42% and 39%, respectively.

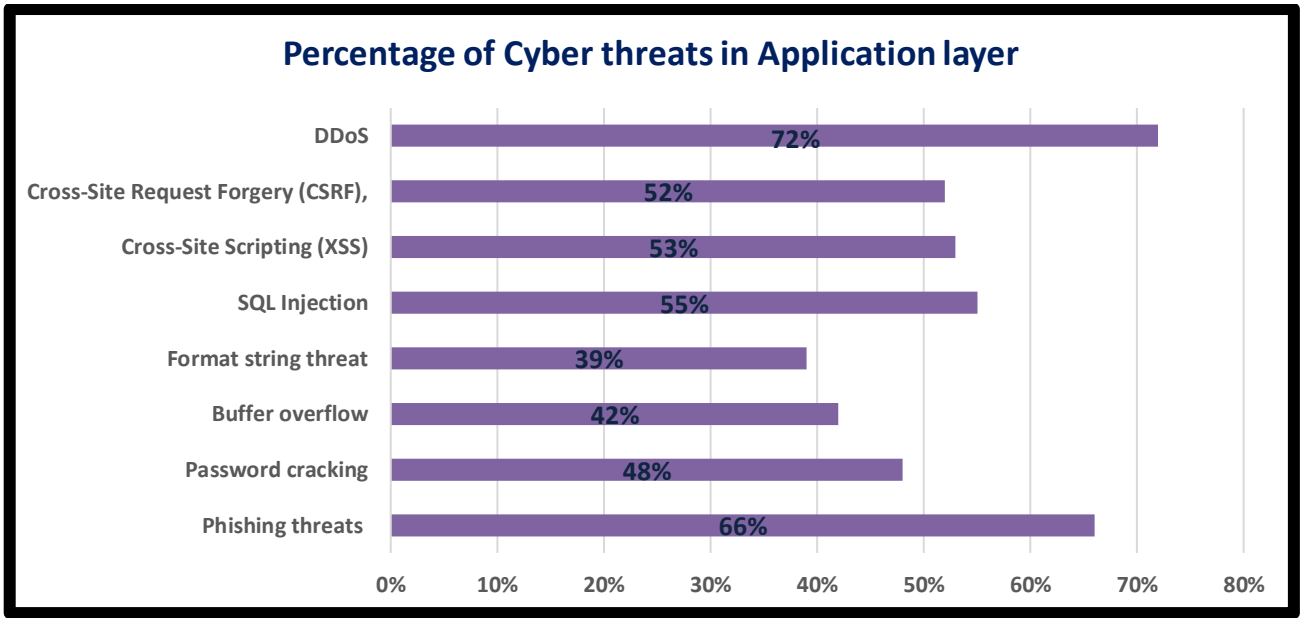

Fig. 8. Analysis of cyber threats in the application layer.

6. A COMPREHENSIVE FRAMEWORK OF THE MOST CRUCIAL COUNTERMEASURES AGAINST IOT THREATS AND ATTACKS IN IOT LAYERS

This section presents a comprehensive framework of the most crucial countermeasures against IoT threats and attacks in IoT layers, including the physical layer, data link layer, network layer, transport layer and application layer, as shown in Figure 9. Security controls and countermeasures are mechanisms and tools developed to protect IoT systems from cyber threats and attacks. These countermeasures are very important for protecting the integrity of data from manipulation and safeguarding database systems from unauthorized access. They can be classified into several types on the basis of their functions, usage, effectiveness and importance. As shown in Figure 9, for example, encryption methods are considered among the most powerful technical security controls for IoT systems for protecting sensitive data and rejecting unauthorized access. Multifactor authentication is also a robust technique for preventing any unauthorized access to sensitive data and IoT systems. Firewalls also offer monitor packets in IoT networks and defend them against attacks. Using the logs, they can audit and monitor every instance of IoT access. Firewalls can offer a level of control over network traffic and prevent unauthorized access to sensitive data. Network segmentation also helps restrict the spread of cyberattacks throughout the network and isolate vital resources and assets. Intrusion detection and prevention systems (IDPSs) are also designed to detect and respond to new and advanced attacks. Intrusion detection systems (IDSs) evaluate data via network traffic, IoT operations, SQL queries, system logs, etc. When an attack is identified, intrusion prevention systems (IPSs) stop them by disabling connections, blacklisting IP addresses, or changing firewall settings. IDPS combines signature-based and behavioral detection approaches. These two approaches help to identify zero-day attacks. Web application firewalls (WAFs) are critical security controls that protect web applications from various attacks, including injection attacks, cross-site scripting (XSS), cross-site request forgery (CSRF), etc.,etc., and several security measures can be employed. Intrusion prevention systems (IPSs) are designed to detect and block attacks at multiple levels. Endpoint protection platforms (EPPs) provide multilayered security for endpoints, typically including antimalware, endpoint firewalls, ad blockers, and intrusion prevention features. Ensuring secure communication within perimeter defenses. In black box testing, a web crawler is used to identify the point at which the SQL can perform; then, the application's response

is monitored. The antiphishing authentication (APA) technique uses 2-way authentication and zero-knowledge password proof. Address space location randomization (ASLR), which randomly moves around the address space locations of data regions. Typically, buffer overflow attacks need to know the locality of executable code, and randomizing address spaces makes this virtually impossible. Zero-trust policies demand continuous verification of all devices and users connecting to the network, thereby reducing the attack surface area and preventing unauthorized access by eliminating implicit trust. Additional defenses include regularly updating firmware and software, conducting penetration testing, and monitoring network traffic for suspicious activity. Encryption protocols, such as the advanced encryption standard (AES) and secure hash algorithm (SHA), are essential for protecting IoT ecosystems by encoding data to prevent unauthorized access and ensure confidentiality. The implementation of multifactor authentication and auditing network configurations also contributes significantly to enhancing security in the network layer. Furthermore, employing firewalls, intrusion detection/prevention systems, and secure communication channels such as virtual private networks (VPNs) can help protect IoT network infrastructures from malicious attacks.

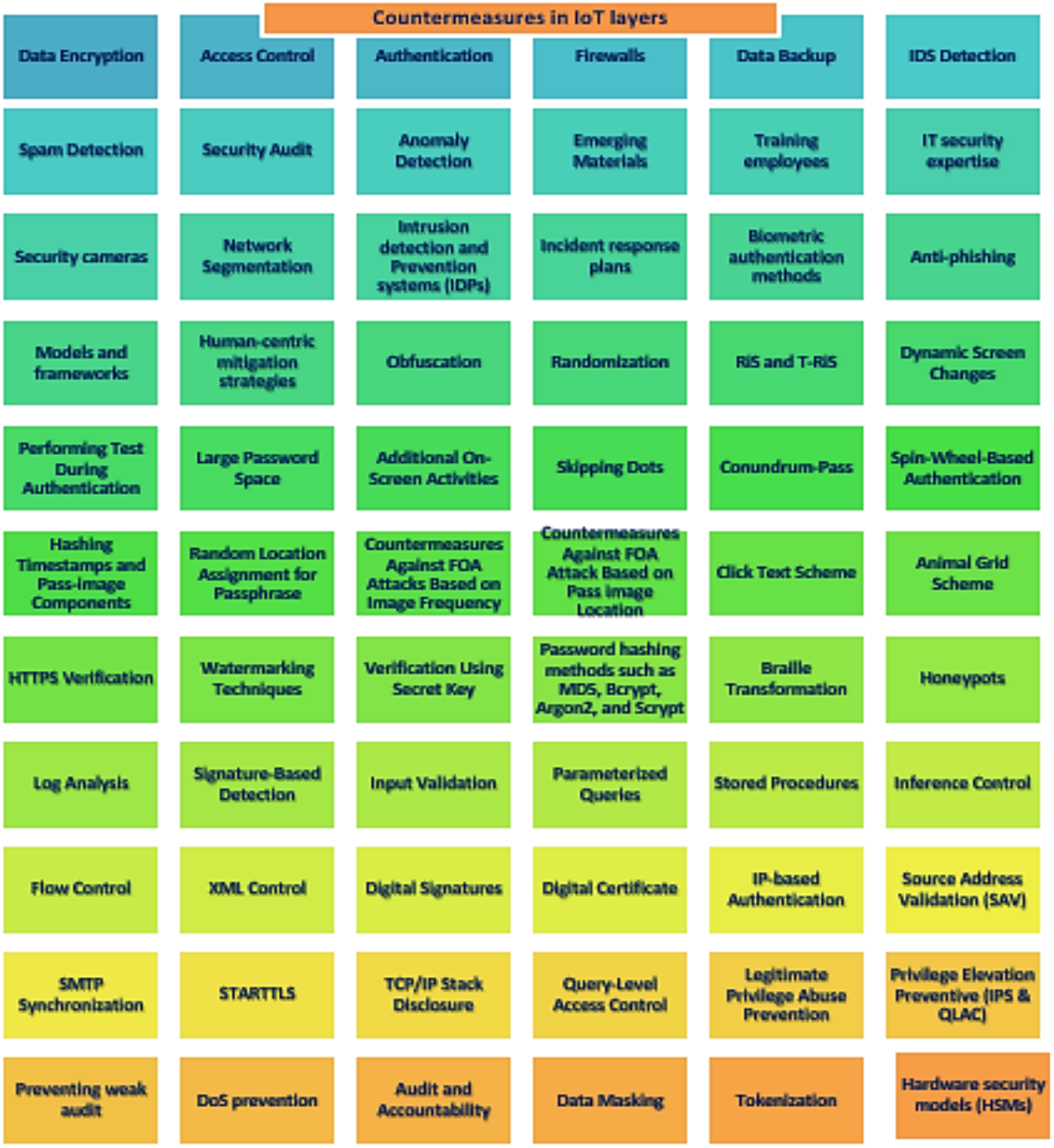

Fig. 9. The most common countermeasures in database systems.

TABLE X. MAPPING SUITABLE COUNTERMEASURES AGAINST THREATS IN THE PHYSICAL LAYER

	Threat	Control measures
Physical Layer	Identity faking attack	• A proposed security verification framework for distributed industrial control systems involves modelling industrial IoT infrastructures to identify attack patterns and mitigation techniques. The effectiveness of these mitigation strategies is validated using an Alloy analyser
	Imitation attack	• Utilize identity-based authentication protocols and implement anti-cloning measures.
	man in the middle attacks	• Ensure data confidentiality, perform thorough data integrity checks, and use encryption.
	Denial of Service (DoS)	• Utilize cryptographic methods, verify authenticity, and block malicious users.
	Physical attack	• A Security Framework for Protecting Home IoT Environments with Customized Real-Time Risk Management.
	Blocking attack	• Use firewalls, packet filtering, anti-jamming measures, and up-to-date antivirus software.
	increasing power consumption	-
	Gathering	• Utilize encryption, identity-based approaches, and message authentication codes.

TABLE XI. MAPPING SUITABLE COUNTERMEASURES AGAINST THREATS IN THE DATA LINK LAYER

	Threat	Control measures
Network Layer	Confidentiality concerns and data exploitation	• risk analysis based on the EBIOS methodology
	Context privacy leakage	• The Enhanced Cuckoo Search (ECS) algorithm for optimizing a back-propagation neural network (BPNN) to improve accuracy and stability.
	Privacy attack	• Employ anonymous data transfer methods, utilize sample datasets, and implement techniques that preserve privacy
	privacy leakage	
	Lack of user awareness of protection	• Enhanced Cuckoo Search (ECS) algorithm for optimizing a back-propagation neural network (BPNN) to improve accuracy and stability
	safety risk issues	• Techniques for preserving data privacy and 5G IoT environments, alongside computational intelligence for cyber defense.
	Gathering	• Utilize encryption, identity-based approaches, and message authentication codes.

TABLE XII. MAPPING SUITABLE COUNTERMEASURES AGAINST THREATS IN THE NETWORK LINK LAYER

	Threat	Control measures
Data Link Layer	Confidentiality concerns and data exploitation	• Risk analysis based on the EBIOS methodology.
	Privacy attack	• Employ anonymous data transfer methods, utilize sample datasets, and implement techniques that preserve privacy
	Context privacy leakage	• The Enhanced Cuckoo Search (ECS) algorithm for optimizing a back-propagation neural network (BPNN) to improve accuracy and stability.
	Lack of user awareness of protection	• Enhanced Cuckoo Search (ECS) algorithm for optimizing a back-propagation neural network (BPNN) to improve accuracy and stability.
	Gathering	• Utilize encryption, identity-based approaches, and message authentication codes.
	Fabrication	• Establish data authenticity verification to maintain information integrity.

TABLE XIII. MAPPING SUITABLE COUNTERMEASURES AGAINST THREATS IN THE TRANSPORT LINK LAYER

	Attack	Control measures
Application Layer	phishing site attack	• User awareness
	Imitation attack	• Utilize identity-based authentication protocols and implement anti-cloning measures
	spoofing	• Employ symmetric encryption methods to guarantee data confidentiality.
	man in the middle attacks	• Ensure data confidentiality, perform thorough data integrity checks, and use encryption
	Denial of Service (DoS)	• Utilize cryptographic methods, verify authenticity, and block malicious users.
	Software attack	• A Security Framework for Protecting Home IoT Environments with Customized Real-Time Risk Management
	Software piracy and malware attacks	• Utilizing a Tensor Flow deep neural network to detect pirated software. • Employing tokenization and feature weighting to eliminate noisy data. • Applying deep learning techniques to identify source code plagiarism
	Passive attack	• Employ symmetric encryption methods to guarantee data confidentiality.
	Fabrication attack	• Establish data authenticity verification to maintain information integrity
	Identity faking attack [1(23)]	• A proposed framework for the security verification of distributed industrial control systems. The framework is based on modelling industrial IoT infrastructures. Patterns made by the attacks and mitigation techniques to stop the attacks. Using an alloy analyser to prove mitigation techniques.

TABLE XIV. MAPPING SUITABLE COUNTERMEASURES AGAINST THREATS IN THE APPLICATION LINK LAYER

	Threat	Control measures
Transport layer	Confidentiality concerns and data exploitation	• risk analysis based on the EBIOS methodology
	Privacy attack	• Employ anonymous data transfer methods, utilize sample datasets, and implement techniques that preserve privacy.
	Context privacy leakage	• The Enhanced Cuckoo Search (ECS) algorithm for optimizing a back-propagation neural network (BPNN) to improve accuracy and stability
	Lack of user awareness of protection	• The Enhanced Cuckoo Search (ECS) algorithm for optimizing a back-propagation neural network (BPNN) to improve accuracy and stability
	sending false code	-
	Gathering	• Utilize encryption, identity-based approaches, and message authentication codes.

7. ASSESSING THE RISKS OF CYBERSECURITY THREATS OF THE IOT INFRASTRUCTURE

In this study, qualitative methods were employed to assess the risk level in IoT layers. The risk level can be calculated via the following equation:

$$\text{Risk level} = \text{Likelihood} \times \text{Impact}$$

The risk level can be categorized into four levels based on the likelihood and impact on a scale from 1--4, which produces the risk matrix shown in Figure 10 and Table 15. Table 16 summarizes all the results for the risk level for all the IoT layers.

TABLE XV. RISK LEVEL WITH LIKELIHOOD AND IMPACT INDICES

Index	Likelihood	Impact	RA	Risk Level	Color
1	Unlikely	Low impact	1-4	Low Risk	
2	Moderate	Moderate impact	5-8	Moderate Risk	
3	Likely	High impact	9-11	High Risk	
4	Very Likely	Very high impact	12-16	Very high Risk	

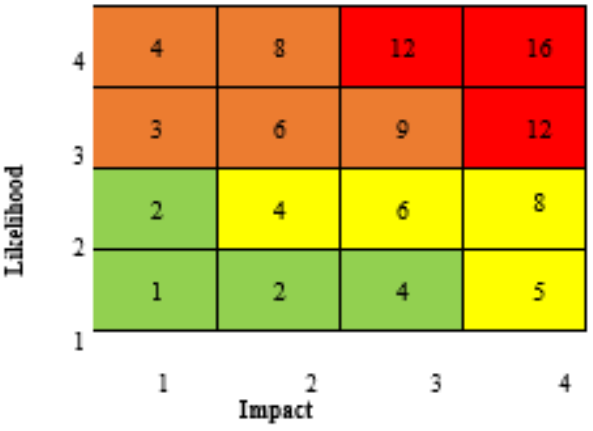

Fig. 10. Risk Matrix

On the basis of the risk matrix analysis in Figure 11, the results indicate that the risk level for the application layer in the IoT has the highest RA of 16, which means that the application layer has the highest risk with a high probability of occurrence and a high impact of losses.

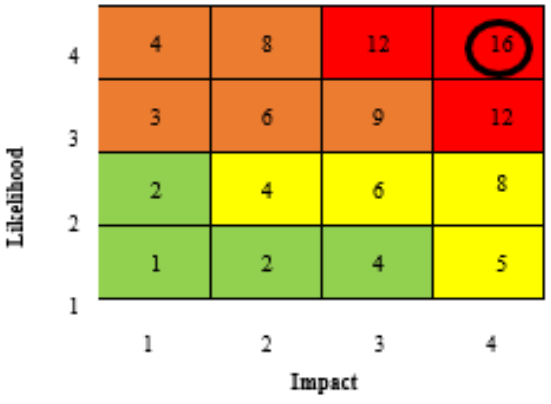

Fig. 11. Risk level for the application layer.

Figure 12 shows that the risk matrix analysis for the transport layer revealed a high RA with a value of 12, which means that the transport layer has the highest risk with a high probability of occurrence and a high impact of losses.

Fig. 12. Risk level of the transport layer.

Figure 12 shows that the risk matrix analysis for the network layer has the highest RA, with a value of 16, which means that the network layer has the highest risk, with a high probability of occurrence and a high impact of losses.

Fig. 13. Risk level of the network layer.

On the basis of the risk matrix analysis in Figure 13, the results indicate that the risk level for the data link layer in the IoT has a moderate RA value of 4, which means that the data link layer has a moderate risk with a moderate probability of occurrence and a moderate impact on losses.

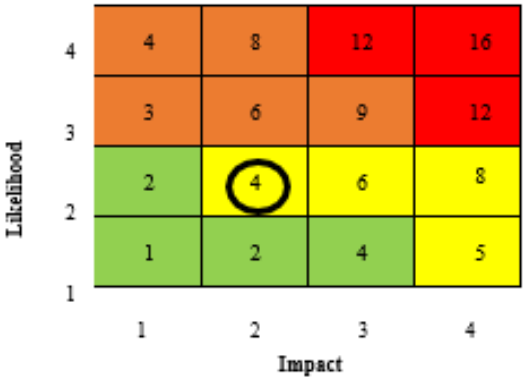

Fig. 14. Risk level for the data link layer.

Finally, on the basis of the analysis of the risk matrix in Figure 14, the results indicate that the risk level for the physical layer in the IoT has a low RA with a value of 2, which means that the physical layer has a low risk with a low probability of occurrence and a low impact of losses.

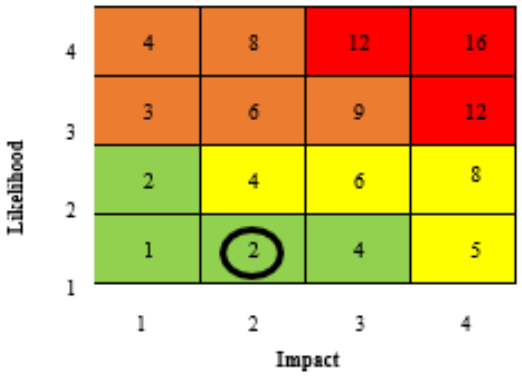

Fig. 15. Risk level for the physical layer.

TABLE XVI. RISK LEVEL WITH LIKELIHOOD AND IMPACT INDICES FOR IOT LAYERS

Layer	Likelihood	Impact	RA	Risk Level
Application Layer	Very Likely	Very high impact	16	Very high Risk
Transport Layer	Likely	High impact	12	High Risk
Network Layer	Very Likely	Very high impact	16	Very high Risk
Data link Layer	Moderate	Moderate impact	4	Moderate Risk
Physical Layer	Low	Low impact	2	Low Risk

7. CONCLUSION

Owing to the rapid growth of IoT systems, cybersecurity threats have become increasingly prevalent. These threats pose significant risks to service availability, data integrity, and user privacy. Therefore, understanding the behavior of cybersecurity threats within IoT systems and identifying suitable countermeasures to mitigate their impacts are crucial. Cyber-risk classification and assessment play pivotal roles in effective risk management, providing an essential framework for identifying, evaluating, and responding to cybersecurity threats. A thorough risk assessment facilitates the understanding of potential impacts and guides the development of robust security controls.

This research classifies and assesses cyber threats in IoT systems, highlighting vulnerabilities, impacts, and appropriate countermeasures. The results indicate that phishing attacks and SQL injection threats are among the most common technical threats in the IoT application layer, with occurrence rates of 72% and 66%, respectively. Additionally, cross-site scripting (XSS) and cross-site request forgery (CSRF) attacks were identified as second-level threats, with occurrence rates of 55%, 53%, and 52%, respectively. Password-cracking threats were classified as third-tier threats at 48%.

In the IoT transport layer, the research identified TCP/UDP port scanning, TCP/UDP flooding, and DNS poisoning as prominent threats, occurring at rates of 34%, 33%, and 31%, respectively. The SYN flooding and desynchronization attacks were identified as secondary threats, with occurrence rates of 27%, 26%, and 24%, respectively. Lateral movement and Denial-of-Service (DoS) attacks were the third-tier threats, with occurrence rates of 18% and 15%, respectively.

The developed risk classification and assessment framework serves as an essential tool for organizations, scholars, and security professionals, enabling them to proactively identify, evaluate, and mitigate cyber threats. However, owing to the rapidly evolving nature of cybersecurity threats, continuous monitoring, regular updates, and rapid responsiveness to emerging threats are crucial. Furthermore, recognizing that cyber threats often occur in interconnected or sequential forms is vital. For example, an attacker may initially use phishing to gain system access, followed by subsequent database breaches or ransomware attacks.

In conclusion, this research provides comprehensive insights into cybersecurity threats in IoT systems, highlighting vulnerabilities, potential impacts, and recommended countermeasures. The outcomes enable organizations to better understand cyber threats and develop robust strategies for effective cybersecurity management.

Conflicts of interest

The authors declare that they have no conflicts of interest.

Funding

None.

Acknowledgment

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. 252197).

References

[1] K. Ntafloukas, D. P. McCrum, and L. Pasquale, "A cyber-physical risk assessment approach for Internet of Things enabled transportation infrastructure," *Applied Sciences* , vol. 12, no. 18, p. 9241, Sep. 2022.
[2] C. Sánchez-Zas, X. Larriva-Novo, V. A. Villagrá, D. Rivera, and A. Marín-Lopez, "A methodology for ontology-based interoperability of dynamic risk assessment frameworks in IoT environments," *Internet of Things* , vol. 27, p. 101267, Oct. 2024.
[3] I. Hussain, "Secure, sustainable smart cities and the Internet of Things: Perspectives, challenges, and future directions," *Sustainability* , vol. 16, no. 4, p. 1390, Feb. 2024.
[4] A. Abdulhamid, M. M. Rahman, S. Kabir, and I. Ghafir, "Enhancing safety in IoT systems: A model-based assessment of a smart irrigation system using fault tree analysis," *Electronics* , vol. 13, no. 6, p. 1156, Mar. 2024.
[5] T. S. AlSalem, M. A. Almaiah, and A. Lutfi, "Cybersecurity risk analysis in the IoT: A systematic review," *Electronics* , vol. 12, no. 18, p. 3958, Sep. 2023.
[6] S. Kerimkhulle et al., "Fuzzy logic and its application in the assessment of information security risk of industrial Internet of Things," *Symmetry* , vol. 15, no. 10, p. 1958, Oct. 2023.
[7] J. Lemos et al., "A system for individual environmental risk assessment and management with IoT based on the worker's health history," *Applied Sciences* , vol. 14, no. 3, p. 1021, Jan. 2024.
[8] R. M. Czekster, P. Grace, C. Marcon, F. Hessel, and S. C. Cazella, "Challenges and opportunities for conducting dynamic risk assessments in medical IoT," *Applied Sciences* , vol. 13, no. 13, p. 7406, Jun. 2023.
[9] A. Alzahrani and M. Z. Asghar, "Intelligent risk prediction system in IoT-based supply chain management in logistics sector," *Electronics* , vol. 12, no. 13, p. 2760, Jun. 2023.
[10] E. K. Parsons, E. Panaousis, G. Loukas, and G. Sakellari, "A survey on cyber risk management for the Internet of Things," *Applied Sciences* , vol. 13, no. 15, p. 9032, Aug. 2023.
[11] J. Yi and L. Guo, "AHP-Based network security situation assessment for industrial internet of things," *Electronics* , vol. 12, no. 16, p. 3458, Aug. 2023.
[12] M. Shokry, A. I. Awad, M. K. Abd-Ellah, and A. A. Khalaf, "When security risk assessment meets advanced metering infrastructure: Identifying the appropriate method," *Sustainability* , vol. 15, no. 12, p. 9812, Jun. 2023.
[13] P. Cheimonidis and K. Rantos, "Dynamic risk assessment in cybersecurity: A systematic literature review," *Future Internet* , vol. 15, no. 10, p. 324, Sep. 2023.
[14] S. A. Baho and J. Abawajy, "Analysis of consumer IoT device vulnerability quantification frameworks," *Electronics* , vol. 12, no. 5, p. 1176, Feb. 2023.
[15] J. S. Park, H. M. Ham, and Y. H. Ahn, "Expansion joints risk prediction system based on IoT displacement device," *Electronics* , vol. 12, no. 12, p. 2713, Jun. 2023.
[16] A. T. Sheik, C. Maple, G. Epiphaniou, and M. Dianati, "Securing cloud-assisted connected and autonomous vehicles: An in-depth threat analysis and risk assessment," *Sensors* , vol. 24, no. 1, p. 241, Dec. 2023.
[17] Pritika, B. Shanmugam, and S. Azam, "Risk evaluation and attack detection in heterogeneous IoMT devices using hybrid fuzzy logic analytical approach," *Sensors* , vol. 24, no. 10, p. 3223, May 2024.
[18] A. Waqar, M. B. Khan, N. Shafiq, K. Skrzypkowski, K. Zagórski, and A. Zagórska, "Assessment of challenges to the adoption of IoT for the safety management of small construction projects in Malaysia: Structural equation modelling approach," *Applied Sciences* , vol. 13, no. 5, p. 3340, Mar. 2023.
[19] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, "A critical cybersecurity analysis and future research directions for the Internet of Things: A comprehensive review," *Sensors* , vol. 23, no. 8, p. 4117, Apr. 2023.
[20] A. Amro and V. Gkioulos, "Evaluation of a cyber risk assessment approach for cyber–physical systems: Maritime- and energy-use cases," *Journal of Marine Science and Engineering* , vol. 11, no. 4, p. 744, Mar. 2023.
[21] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Anomaly detection IDS for detecting DoS attacks in IoT networks based on machine learning algorithms," *Sensors* , vol. 24, no. 2, p. 713, Jan. 2024.
[22] M. R. Islam and K. M. Aktheruzzaman, "An analysis of cybersecurity attacks against Internet of Things and security solutions," *Journal of Computer and Communications* , vol. 8, no. 4, pp. 1–11, Apr. 2020.
[23] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, "A critical cybersecurity analysis and future research directions for the Internet of Things: A comprehensive review," *Sensors* , vol. 23, no. 8, p. 4117, Apr. 2023.
[24] H. Pourrahmani, A. Yavarinasab, and A. M. Monazzah, "A review of the security vulnerabilities and countermeasures in the Internet of Things solutions: A bright future for the blockchain," *Internet of Things* , vol. 23, p. 100888, Oct. 2023.
[25] A. A. Almuqren, "Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions," *Journal of Cyber Security and Risk Auditing* , vol. 1, no. 1, pp. 1–11, Jan. 2025, doi: 10.63180/jcsra.thestap.2025.1.1.
[26] S. Otoom, "Risk auditing for digital twins in cyber physical systems: A systematic review," *Journal of Cyber Security and Risk Auditing* , vol. 2025, no. 1, pp. 22–35, Jan. 2025, doi: 10.63180/jcsra.thestap.2025.1.3.

[27] A. Alshuaibi, M. Almaayah, and A. Ali, "Machine learning for cybersecurity issues: A systematic review," *Journal of Cyber Security and Risk Auditing* , vol. 2025, no. 1, pp. 36–46, Feb. 2025, doi: 10.63180/jcsra.thestap.2025.1.4.
[28] R. S. Mousa and R. Shehab, "Applying risk analysis for determining threats and countermeasures in workstation domain," *Journal of Cyber Security and Risk Auditing* , vol. 2025, no. 1, pp. 12–21, Jan. 2025, doi: 10.63180/jcsra.thestap.2025.1.2.
[29] E. Alotaibi, R. Bin Sulaiman, and M. Almaiah, "Assessment of cybersecurity threats and defense mechanisms in wireless sensor networks," *Journal of Cyber Security and Risk Auditing* , vol. 2025, no. 1, pp. 47–59, Feb. 2025, doi: 10.63180/jcsra.thestap.2025.1.5.
[30] "Improvement of Internet of Things (IoT) interference based on pre-coding techniques over 5G networks," *Mesopotamian Journal of CyberSecurity* , vol. 5, no. 1, pp. 11–22, 2025, doi: 10.58496/MJCS/2025/002.
[31] "Internet of Things for smart building security: Leveraging a blockchain for enhanced IoT security," *Mesopotamian Journal of CyberSecurity* , vol. 5, no. 1, pp. 187–201, 2025, doi: 10.58496/MJCS/2025/013.
[32] "An innovative method of malicious code injection attacks on websites," *Applied Data Science and Analysis* , vol. 2024, pp. 39–51, 2024, doi: 10.58496/ADSA/2024/005.
[33] S. Y. Mohammed and M. Aljanabi, "From text to threat detection: The power of NLP in cybersecurity," *SHIFRA* , vol. 2024, pp. 1–7, 2024, doi: 10.70470/SHIFRA/2024/001.
[34] M. M. Abdulrahman, A. D. Abbood, and B. A. Attea, "Exploring signed social networks: Algorithms for community detection and structure analysis," *KHWARIZMIA* , vol. 2023, pp. 37–45, 2023, doi: 10.70470/KHWARIZMIA/2023/004.
[35] "A real-time intrusion detection system for DoS/DDoS attack classification in IoT networks using KNN-neural network hybrid technique," *Babylonian Journal of Internet of Things* , vol. 2024, pp. 60–69, 2024, doi: 10.58496/BJIoT/2024/008.
[36] "Smart wearables powered by AI transforming human activity recognition," *Babylonian Journal of Artificial Intelligence* , vol. 2024, pp. 128–133, 2024, doi: 10.58496/BJAI/2024/014.
[37] I. I. Al Barazanchi and W. Hashim, "Enhancing IoT device security through blockchain technology: A decentralized approach," *SHIFRA* , vol. 2023, pp. 10–16, 2023, doi: 10.70470/SHIFRA/2023/002.
[38] A. K. Bhardwaj, P. Dutta, and P. Chintale, "Securing container images through automated vulnerability detection in shift-left CI/CD pipelines," *Babylonian Journal of Networking* , vol. 2024, pp. 162–170, 2024, doi: 10.58496/BJN/2024/016.
[39] Y. Yang, H. Wang, C. Ji, and Y. Niu, "Artificial intelligence-driven diagnostic systems for early detection of diabetic retinopathy: Integrating retinal imaging and clinical data," *SHIFAA* , vol. 2023, pp. 83–90, 2023, doi: 10.70470/SHIFAA/2023/010.
[40] O. Aljumaiah, W. Jiang, S. R. Addula, and M. A. Almaiah, "Analyzing cybersecurity risks and threats in IT infrastructure based on NIST framework," *Journal of Cyber Security and Risk Auditing* , vol. 2025, no. 2, pp. 12–26, 2025.
[41] M. Riyadh Alboalebrah and S. Al-augby, "Unveiling the causes of fatal road accidents in Iraq: An association rule mining approach using the Apriori algorithm," *Journal of Cyber Security and Risk Auditing* , vol. 2025, no. 2, pp. 1–11, 2025, doi: 10.63180/jcsra.thestap.2025.2.1.
[42] R. Almanasir, D. Al-solomon, S. Indrawes, M. A. Amin Almaiah, U. Islam, and M. Alshar'e, "Classification of threats and countermeasures of cloud computing," *Journal of Cyber Security and Risk Auditing* , vol. 2025, no. 2, pp. 27–42, 2025, doi: 10.63180/jcsra.thestap.2025.2.3.
[43] A. AlShuaibi, M. W. Arshad, and M. Maayah, "A hybrid genetic algorithm and hidden Markov model-based hashing technique for robust data security," *Journal of Cyber Security and Risk Auditing* , vol. 2025, no. 3, pp. 42–56, May 2025.
[44] B. Almelehy, M. Ahmad, G. Nassreddine, M. Maayah, and A. Achanta, "Analytical analysis of cyber threats and defense mechanisms for web application security," *Journal of Cyber Security and Risk Auditing* , vol. 2025, no. 3, pp. 57–76, 2025.
[45] G. Lippi, M. Aljawarneh, Q. Al-Na'amneh, R. Hazaymih, and L. D. Dhomeja, "Security and privacy challenges and solutions in autonomous driving systems: A comprehensive review," *Journal of Cyber Security and Risk Auditing* , vol. 2025, no. 3, pp. 23–41, 2025.
[46] M. A. Almedires, A. Elkhalil, and M. Amin, "Adversarial attack detection in industrial control systems using LSTM-based intrusion detection and black-box defense strategies," *Journal of Cyber Security and Risk Auditing* , vol. 2025, no. 3, pp. 4–22, 2025.
[47] S. Ang, M. Ho, S. Huy, and M. Janarthanan, "Utilizing IDS and IPS to improve cybersecurity monitoring process," *Journal of Cyber Security and Risk Auditing* , vol. 2025, no. 3, pp. 77–88, Jul. 2025.