Contents lists available at GrowingScience

International Journal of Data and Network Science

homepage: www.GrowingScience.com/ijds

Cybersecurity risk assessment for identifying threats, attacks and countermeasures in Internet of Things (IoT)

Mohammed Amin Almaiah[a*], Tabarak Albayari[a], Noor Taha[a], Leen Abd alghani[a], Rami Shehab[b*], Tayseer Alkhdour[b], Romel Al-Ali[c] and Theyazn H.H. Aldhyani[d]

[a]*King Abdullah the II IT School, University of Jordan, Amman 11942, Jordan*
[b]*College of Computer Science and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia*
[c]*Associate Professor, The National Research Center for Giftedness and Creativity, King Faisal University, Saudi Arabia*
[d]*Applied college in Abqaiq, King Faisal University, P.O. Box 400, Al-Ahsa 31982, Saudi Arabia*

C H R O N I C L E

Article history:
Received: July 6, 2024
Received in revised format: August 28, 2024
Accepted: September 18, 2024
Available online: September 18, 2024

Keywords:
Cyber threats
IoT networks
Risk assessment
Vulnerabilities and countermeasures

A B S T R A C T

These days, due to the increase in the number of connected devices in IoT networks, several types of new cyber threats and attacks are also coming up in IoT. Any cyber-attack can cause significant damage to the 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. Cyber threats assessment in IoT networks is a prime process due to the evolving nature of cyber-attacks. Therefore, this research focuses on addressing the current gap by performing a comprehensive analysis on identifying 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, Phishing threats were the most common technical threats in the IoT application layer with a percentage of 72% and 66% respectively. In addition, the results found that SQL Injection threat, Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF) attack also were classified as the second level of technical threats in IoT with percentage of 55%, 53% and 52% respectively. In the third level of technical threats in IoT was Password cracking attacks with a percentage of 48%. The results showed that TCP/UDP port scanning, TCP/UDP flooding attack and MQTT attack were the most common technical threats in the IoT transport layer with percentage of 34%, 33% and 31% respectively. In addition, the results found that DNS poisoning threat, SYN-flooding and De-synchronization attack also were classified as the second level of technical threats in IoT with percentage of 27%, 26% and 24% respectively. The third level of technical threats in IoT were lateral movement attacks and DoS attacks with a percentage of 18% and 15% respectively. The framework in this study is considered as a vital tool for practitioners, policymakers, and researchers to identify, classify, and mitigate cyber threats within the IoT systems. The findings from this work can help organizations to understand the types of cyber threats and develop robust strategies against cyber-attacks.

1. Introduction

IoT is one of the promising IT domains in the future and now it has become in our world. The technological advances in IoT have resulted in many benefits for many sectors such as education, medical, industry and others Ntafloukas et al., (2022). Today, all of these sectors are moving towards using IoT to meet the biggest technological advances. It is a collection of devices connected

* Corresponding author.
E-mail address m.almaiah@ju.edu.ju (M. A. Almaiah) Rtshehab@kfu.edu.sa (R. Shaheb)

ISSN 2561-8156 (Online) - ISSN 2561-8148 (Print)

doi: 10.5267/j.ijdns.2024.9.009

with each other and transfer of data between them without human intervention Sánchez-Zas et al., (2024). These IoT devices can be sensors, smart devices, mobile devices, control systems, software, etc. The heterogeneous devices in IoT networks creates a big security challenge and this will make IoT networks vulnerable to cyber-attacks (Hussain, 2024).

Today, cyber-threats are the most critical challenges facing the IoT networks as well as increasing the number of cyber-attacks on IoT networks and becoming more sophisticated. Actually, cyber-risks in the IoT networks can cause a huge impact, including data loss, reputation damage, and failure of the networks. Thus, it is necessary to understand the behavior of cyber threats on IoT networks and identify the suitable countermeasures to mitigate their impacts (Abdulhamid et al., 2024). IoT networks today play a crucial role in the new digital world. It serves as the backbone of modern IT society by supporting many applications like business operations, scientific research, and driving technological innovation etc. IoT devices have several benefits such as easy to store, retrieve, modify, and delete data and several data processing operations. IoT networks are growing day by day and this creates a big challenge due to new attacks threatening the IoT networks security AlSalem et al., (2023).

The Internet of Things (IoT) has transformed various aspects of our daily lives, but it also brings significant cybersecurity challenges. One of these challenges is IoT devices, often lacking robust security features, which are vulnerable to a range of threats and attacks in different layers, including the physical, data Link, network, transport, and application layers Kerimkhulle et al., (2023). 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 Lemos et al., (2024).

In recent years, there have been numerous examples of how even innocuous IoT devices can be abused and repurposed to cause harm. For instance, the Mirai botnet is one of the more infamous IoT security breaches that happened in 2016. In Mirai's case, the botnet consisted of 145,607 video recorders and IP cameras Czekster et al., (2023). 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. And that time, Mirai brought down huge sections of the Internet, including Netflix, Twitter, Reddit, The Guardian, and CNN. The second well known attack in IoT is called Target's credit card breach Alzahrani and Asghar (2023). In 2013, hackers successfully breached Target's network and stole 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 Yi and Guo (2023). Another cyber incident happened in 2017, 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 brand new Jeep Grand Cherokee using its multimedia system Parsons, Panaousis, Loukas and Sakellari (2023). They were successful. And 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, and more. They effectively turned the Jeep Grand Cherokee into a life size remote control car Shokry et al., (2023).

Cyber threats in IoT networks could be happening by exploiting the vulnerabilities in the various interconnected networks, devices and sensors that create the IoT ecosystem. Cyber-attacks can exploit the security weaknesses causing losses such as stealing sensitive information, manipulating data, unauthorized 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, lack of data encryption and lack of network segmentation Cheimonidis and Rantos (2023).

Despite the several benefits of IoT networks, it is more vulnerable to cybersecurity attacks Baho and Abawajy (2023). Furthermore, the increasing use of IoT networks in organizations has created new types of cybersecurity threats that can be exploited. Cybersecurity attacks have become more prevalent in IoT networks such as SQL injection attack, DDoS attack and ransomware which are the biggest risks in the IoT networks field. Cybersecurity attackers are always developing new techniques of attacks, and this cause huge challenge should be addressed by Park et al., (2023). Thus, IoT networks security analysts must follow the security threat assessment continuously to detect any new evolving threats in order to protect the IoT networks 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 the companies. Also, they should take into consideration 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 Park et al., (2023).

IoT devices can be vulnerable for attackers due to some reasons are outdated software, legacy OS, or no OS, basic micro controllers, no security-by-design, lack of device management, shadow devices and operational limitations Sheik et al., (2023). Challenges such as software piracy, malware attacks, and weak authentication exacerbate these vulnerabilities Pritika et al., (2024).

This research aims to review previous studies related to cybersecurity threats to IoT. In addition, this study aims to identify and analyze the major threats in the IoT environment and propose solutions to address these vulnerabilities. Based on that, 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 been performed to explore and classify the cybersecurity risks and threats in IoT environments. For instance, Altulaihan et al. (2024) conducted a study to identify the common threats in the IoT environment. They classified the threats based on the layers in the IoT architecture. They found 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 (2020) reviewed the different types of cybersecurity threats in IoT devices. They classified the cyber threats into three categories: application security, communications security and authentication security. In the same way, Tariq et al., (2023) examined the existing threats, attacks and countermeasures in IoT. They classified the cyber threats in IoT based on layered architecture including connectivity, communication, and management protocols. Pourrahmani et al., (2023) provided a comprehensive analysis on the current threats and vulnerabilities in IoT as well as offered the main security controls for each protocol layer in IoT architecture. The study classified the vulnerabilities based on 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. 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. Regarding 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 the perception, network, and application layers as shown in Fig. 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 almost like the eyes and ears of 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 (Waqar et al., 2023).

B. Network layer

The network layer is the brain of IoT. Its main function is the processing and transmission of the information detected in the perception layer. All communication networks (WSN, mobile networks, internet, Adhoc networks, etc.) and telecommunication are used in this layer. It provides secure data transmission as well as connection by applying data encoding and mining algorithms (Tariq et al., 2023).

C. Application layer

The application layer is the provision of 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 (Amro & Gkioulos, 2023).

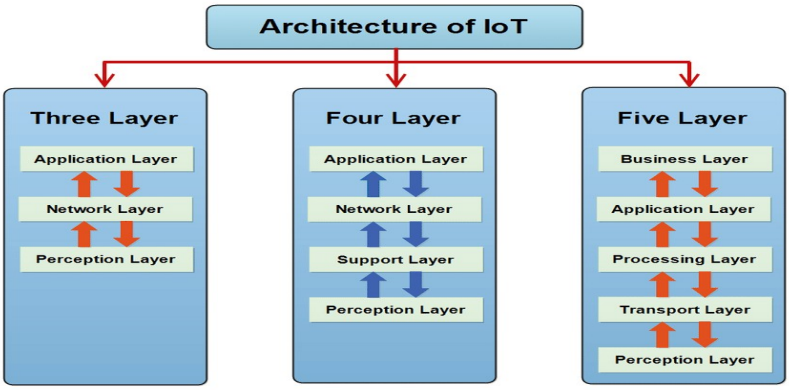

Fig. 1. 3-layers of IoT architecture

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 program. It also helps organizations communicate their risks to stakeholders and make informed decisions about how to allocate resources to reduce those risks. In the literature, there are many cybersecurity risk assessment frameworks and methodologies available, 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 their own 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, they can take steps to mitigate or reduce them. A risk assessment can also help researchers to develop a plan to respond to and recover from a cyber-attack in 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 based on proposing a risk assessment framework for IoT. The design framework incorporates four main stages including: (1) Identifying key components, (2) Threats identification, (3) Vulnerabilities identification and (4) Countermeasures identification. 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. Fig. 2 represents the main stages of the risk assessment framework.

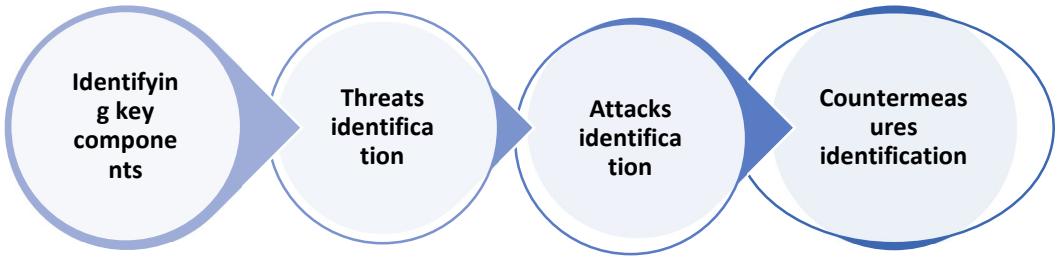

Fig. 2. The Main Stages of Risk Assessment Framework

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 performed 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 collected data in this stage will be analyzed in the next stages.

3.2 Stage Two: Threats identification

Once the data is collected in stage one, then we analyze these data 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 systems vulnerabilities and result in compromised IoT systems.

3.3 Stage Three: attacks identification

In the third stage, after the data is collected, we analyze these data to explore the existing technical security vulnerabilities that could be exploited to compromise the 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 the IoT systems.

3.4 Stage Four: Countermeasures identification

The last stage of the risk assessment framework is to identify and classify the effective countermeasures in order to address the potential cybersecurity threats and vulnerabilities in the 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 the IoT systems.

4. Cyber threats, Attacks and Countermeasures Framework

Fig. 3 represents the main steps of the framework for this research. The framework is divided into three main parts are (1) threats identification, (2) attacks identification and (3) countermeasures identification. The details of each step of the framework will be presented in the subsections below.

4.1 Threats and attacks 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 a potential to exploit IoT layers vulnerabilities and the result compromised IoT systems. The classification of threats is divided based on five IoT layers: (1) threats identification in physical layer, (2) threats identification in data link layer, (3) threats identification in network layer, (4) threats identification in transport layer and (5) threats identification in application layer. The most common cyber threats in 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 the IoT networks. In addition, threats in IoT occur at the data transmission layer, which is a part of the network layer. Thereby it is very crucial to understand and classify these types of threats and propose a suitable countermeasure at the IoT layers in order to ensure the security of IoT devices and networks. The classification analysis was based on multiple dimensions such as threats characteristics, threats 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 layers threats.

A. Threats classification in physical layer

As software-based defenses have gotten better, some attackers have turned their attention to physical security to gain access. IoT devices can sometimes be relatively easy to access, especially if they're 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, settings 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. According to Table 1, which represents the most common threats in the physical layer.

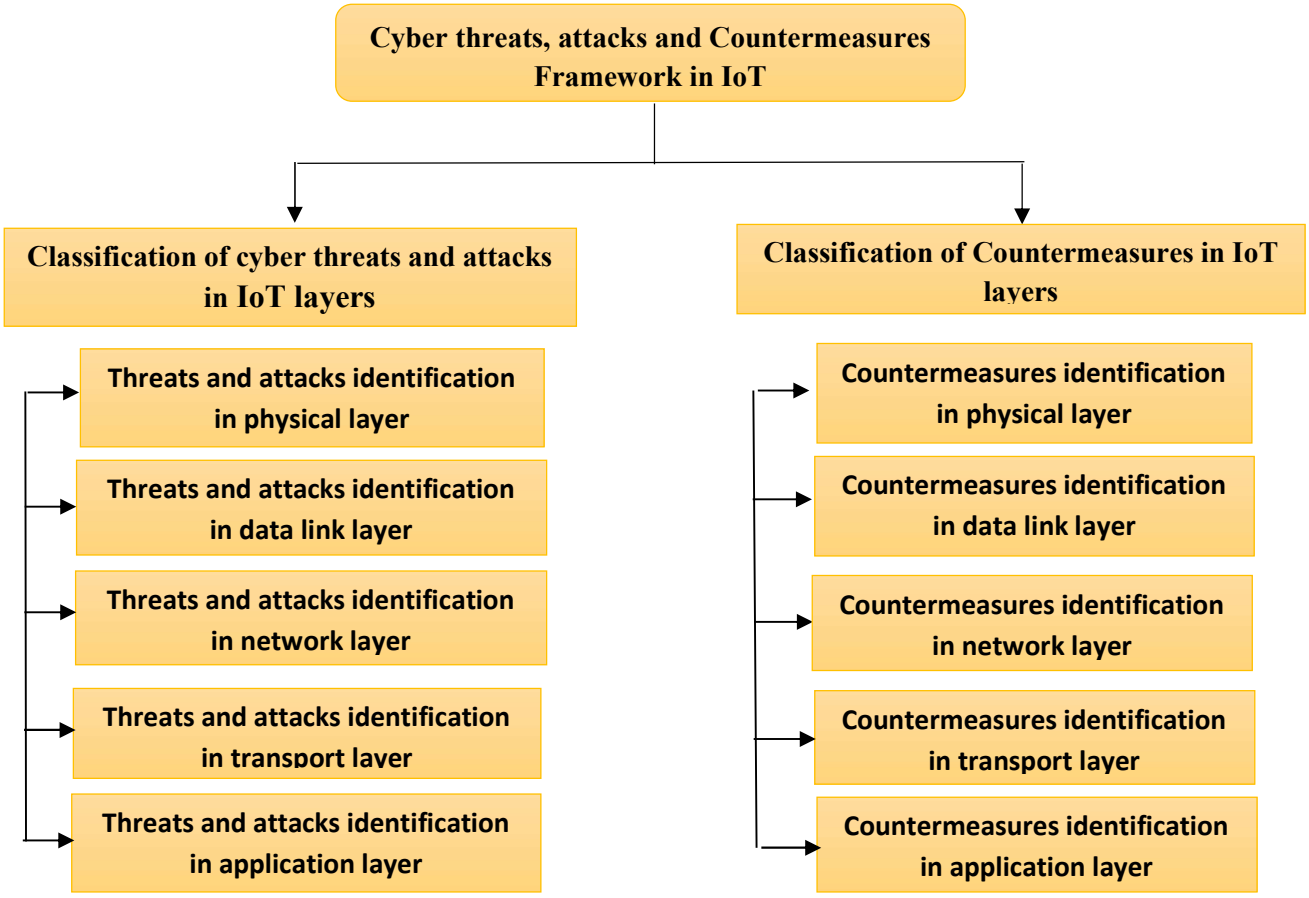

Fig. 3. Cyber threats, Attacks and Countermeasures Framework.

Table 1
Classification of cyber threats in physical layer.

	Threat	Description	Example
Physical layer	Identity faking attack	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	Using impersonation for unauthorized access; involves spoofing and cloning.	• Spoofing • Cloning
	Man in the middle attacks	If adversaries gain unauthorized access to the broker and assume a man-in-the-middle position, they could potentially take control of the entire IoT application.	• Unauthorized Access to the Broker • Control of the Entire IoT Application
	Denial of Service (DoS)	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	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	Denial of Service (DoS), jamming, and malware attacks; these can disrupt network operations	• Jamming • Malware Attacks • Denial of Service (DoS) Attacks
	Increasing power consumption	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	Gathering data from multiple sources; the data might be modified.	• Data Modification

For example, identity faking is a type of cyber-attack that involves pretending someone aims to access their personal information or conduct fraudulent activities. Another type of threat is imitation attacks such as spoofing and cloning that use impersonation for unauthorized access into IoT devices. Man in the middle is another type of threat in the physical layer, which happens when the attackers gain unauthorized access to the broker and assume a man-in-the-middle position, they could potentially take control of the entire IoT application. 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 impact of this type of threat includes service interruption, overwhelming target servers and disruption of services for legitimate users. Tampering threat through gathering data from multiple sources; the data could be modified.

B. Threats classification in data link layer

The data link layer in IoT systems is vulnerable to cyber-attacks. 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 instance, 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 interfering. 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. Threats classification in network layer

Most common cyber threats in IoT systems focused on the network layer. 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. 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, and denial of service attacks, routing attack, Sybil attack, black hole, 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. According to Table 3, which represents the most common threats in the network layer.

Table 2
Classification of cyber threats in data link layer

	Threat	Description	Example
Data link layer	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	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 analyzed by various consumer products and digital technologies.	• Unauthorized data analysis • Potential identity theft • Privacy breaches
	Privacy attack	Revealing confidential data could potentially be linked to subsequent attacks.	• Confidential Data Exposure • Increased Vulnerability • Potential for Subsequent Attacks
	Context privacy leakage	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	A lack of security awareness can result in the inadvertent exposure of sensitive company or personal data.	• Potential Damage • Inadvertent Exposure • Increased Risk
	Gathering	Gathering data from multiple sources; the data might be modified.	• Data Modification
	Fabrication	Introduces false data; compromises data integrity.	• Introduction of False Data • Compromise of Data Integrity

Table 3
Classification of cyber threats in network layer

	Threat	Description	Example
Network Layer	Sybil threat	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 influences 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	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	Revealing confidential data could potentially be linked to subsequent attacks.	• confidential data exposure • increased vulnerability • potential for subsequent attacks
	Privacy leakage	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	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	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	Gathering data from multiple sources; the data might be modified.	• data modification

Table 4
Classification of cyber threats in transport 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 analyzing 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 de-synchronize 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

For example, a 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 the peripherals to execute the attacks. Examples of these attacks include Mirai, Hydra, Bashlite, luabot and Aidra. Sybil threat is one of the most common in network layers, in which an attacker sends a lot of fake requests to the network from a single user. Where this attacker pretends many fake identities through creating several accounts from different IP addresses. In this case

an attacker can control the overall network. This type of threat can have an effect on the performance, resource utilization and data integrity. Another type of threat in the network layer is called sinkhole attack. This threat focuses on managing traffic networks through sending counterfeit data to entrance 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. Threats classification in application layer

The most common cyber threats faced by application layers in IoT include various types of attacks such as ransomware assaults, jamming, spoofing, data tampering, and fake nodes and others. IoT's widespread use in smart applications like agriculture, economies, residences, and health and fitness makes it vulnerable to these threats due to the lack of robust protection mechanisms. Researchers are particularly concerned about 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. IoT application layer suffers from various vulnerabilities that make them at risk of being compromised, including: outdated or unsecured IoT app components, weak or hardcoded passwords, unsecured network services and ecosystem interfaces, 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 IoT with their description.

Table 5
Classification of cyber vulnerabilities in 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 aren't 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. Also, IoT devices may not even have an update mechanism incorporated into them due to age or purpose, meaning admins can't 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 can't be changed. Some IT staff don't 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 6
Classification of cyber threats in 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 occurs 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

According to Table 6, which represents the most common threats in the application layer. For example, 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. 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 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. 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. Also, Cross-Site Scripting (XSS) threat occurs when malicious code is introduced into web pages being 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 like changing account settings or making transactions without the user's knowledge. 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. 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.

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 a potential to defend against IoT layers attacks and the result protect IoT systems. The classification of countermeasures is divided based on five IoT layers: (1) countermeasures identification in physical layer, (2) countermeasures identification in data link layer, (3) countermeasures identification in network layer, (4) countermeasures identification in transport layer and (5) countermeasures identification in application layer. The most important countermeasures and security controls in IoT including Web Application Firewalls (WAF), Intrusion Prevention Systems (IPS), Endpoint Protection Platforms (EPP), Network Access Control (NAC), eXtended Detection & Response (xDR), Virtual Private Network (VPN), SASE/SSE, encrypted data transfer, and network-based firewall. These countermeasures can protect sensitive information and prevent compromise of the confidentiality of the IoT networks. Thereby it is very crucial to understand and classify these types of security controls and propose a suitable countermeasure at the IoT layers in order to ensure the security of IoT devices and networks. The classification analysis was based on multiple dimensions such as type of threats and attacks, type of IoT layer and their protection roles in each layer. All countermeasures were discussed by a description that clarifies its potential role for protecting the IoT layers. In the subsections below, we provide the detailed countermeasures classification for IoT layers.

A. Countermeasures classification in physical layer

Table 7
Classification of the most critical security countermeasure for 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.

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 the cyber-attacks and take countermeasures at the physical layer to ensure the security of IoT objects. 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 cyber-attacks in the physical layer. In our study, in Table 7 we identified a range of countermeasures that represents a security control to enhance the IoT physical layer security against cyber-attacks. For instance, auditing is a security control in the physical layer that aims to ensure all important systems events are securely logged into an authorized log collection system. Another security control is 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 is a security control aimed 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 that aims to grant only the minimum required access for people to accomplish their tasks—and no more. Administrative access (root) must only be granted on a just-in-time. Device hardening also another countermeasure for the physical layer is used to ensure firmware integrity, devices should be updated, encrypted, and have intrusion detection and antimalware configured. IoT devices management is a solution that should be used to centrally manage IoT devices. Frequency Hopping Spread Spectrum technique, EPC (Electronic Product Code) technique, Anonymous Forward Secure Mutual Authentication on Protocols (AFMAP) and Access control list (ACLs).

B. Countermeasures classification in data link layer

Data link Layer is highly prone to several cyber-attacks. Therefore, it is crucial to address these attacks and take countermeasures at the data link layer to ensure the security of IoT networks. 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 cyber-attacks in the data link layer in Table 9. In our study, in Table 8 we identified a range of countermeasures that represents a security control to enhance the IoT data link layer security against cyber-attacks. Several security countermeasures methods have been developed to mitigate these types of attacks. One of the important methods is 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 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. 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. 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 like 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.

Table 8
Classification of the most critical security countermeasure for 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.

C. Countermeasures classification in 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 cyber-attacks, 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 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 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. Implementing multi-factor authentication and auditing network configurations also contribute significantly to enhancing security in the network layer. Further, employing firewalls, intrusion detection/prevention systems, and secure communication channels like Virtual Private Networks (VPNs) can help protect IoT network infrastructures from malicious attacks.

Table 9
Classification of the most critical security countermeasure for network layer

	Countermeasures	Description
Network layer	Zero trust policies	zero trust policies, which demand continuous verification of all devices and users connecting to the network, thereby reducing the attack surface and preventing unauthorized access by eliminating implicit trust.
	Regularly updating firmware and software	Regularly updating firmware and software, conducting penetration testing, and monitoring network traffic for suspicious activity.
	Encryption protocols	Encryption protocols, such as 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.
	Authentication	Implementing multi-factor authentication and auditing network configurations also contribute significantly to enhancing security in the network layer.
	Auditing network configurations	Regularly auditing network configurations also play a crucial role in strengthening the overall security in the network layer.
	Firewalls	employing firewalls,
	Intrusion detection/prevention systems	intrusion detection/prevention systems
	Secure communication channels	Virtual Private Networks (VPNs) can help protect IoT network infrastructures from malicious attacks.

D. Countermeasures classification in application layer

Application layer provides the services for users through IoT applications. Also, the layer stores information or data in his 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.

Table 9
Classification of the most critical security countermeasure for network layer.

	Countermeasures	Description
Application Layer	Web Application Firewalls (WAF)	Web Application Firewalls (WAF) is one of the critical security controls that protect web applications from various attacks, including injection attacks, cross-site scripting (XSS), cross-site request forgery (CSRF), and others, several security measures can be employed.
	Intrusion Prevention Systems (IPS)	Intrusion Prevention Systems (IPS) are designed to detect and block attacks at multiple levels.
	Endpoint Protection Platforms (EPP)	Endpoint Protection Platforms (EPP) provide multilayered security for endpoints, typically including anti-malware, endpoint firewalls, ad blockers, and intrusion prevention features.
	Network Access Control (NAC)	Network Access Control (NAC) limits unauthorized network access and can assess the security status of devices, users, and applications to enforce security policies.
	eXtended Detection & Response (xDR)	eXtended Detection & Response (xDR) consolidates data from endpoints, networks, cloud services, and applications, providing a holistic view of threats and potential intrusions.
	Virtual Private Network (VPN)	Virtual Private Networks (VPN) establish encrypted connections from remote locations to the enterprise network, ensuring secure communication within protected boundaries.
	Anti-Phishing Authentication (APA)	Anti-Phishing Authentication (APA) technique that uses 2-way authentication and zero knowledge password proof.
	Address Space Location Randomization (ASLR)	Address Space Location Randomization (ASLR) that 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.
	Authentication	Multi-factor authentication
	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.

Actually, the proliferation of IoT applications has opened up a multitude of entry points for cyber-attacks, making it imperative for researchers to identify the necessary security countermeasures. There are several security countermeasures for securing IoT applications and mitigate cybersecurity threats as presented in Table 10. For instance, Web Application Firewalls (WAF) is one

of the critical security controls that protect web applications from various attacks, including injection attacks, cross-site scripting (XSS), cross-site request forgery (CSRF), and others, several security measures can be employed. Intrusion Prevention Systems (IPS) are designed to detect and block attacks at multiple levels. Endpoint Protection Platforms (EPP) provide multilayered security for endpoints, typically including anti-malware, 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 (VPN) create encrypted tunnels from remote locations into the enterprise network, ensuring secure communication within the perimeter defenses. Black box testing, where Web crawlers are used that identify the point at where SQL can perform, then monitor the application's response. Anti-Phishing Authentication (APA) technique that uses 2-way authentication and zero knowledge password proof. Address Space Location Randomization (ASLR) that 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.

Table 10
Mapping the suitable countermeasures with against threats in physical layer

	Threat		Control measures
Physical layer	Identity faking attack	•	A proposed security verification framework for distributed industrial control systems involves modeling industrial IoT infrastructures to identify attack patterns and mitigation techniques. The effectiveness of these mitigation strategies is validated using an Alloy analyzer
	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 increasing power consumption	•	Use firewalls, packet filtering, anti-jamming measures, and up-to-date antivirus software.
	Gathering	•	Utilize encryption, identity-based approaches, and message authentication codes.

5. Analyzing 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 physical layer, data link layer, network layer, transport layer and application layer. Fig. 4 showed the analysis results of classifications of the most common cyber threats and attacks in the physical layer. The results indicated that Denial of Service attack (DoS) and man in the middle attack were the most common technical threats in IoT with percentage of 26% and 20% respectively. Man in middle attack and imitation attacks also were classified as the second level of technical threats in IoT with percentage of 20% and 14% respectively. The third level of technical threats in IoT were increasing power consumption, tampering and identity faking attacks with a percentage of 7%, 6% and 4%, respectively. The remaining types of technical threats such as physical attacks were in the lowest level of technical threats in IoT with a percentage of 2%.

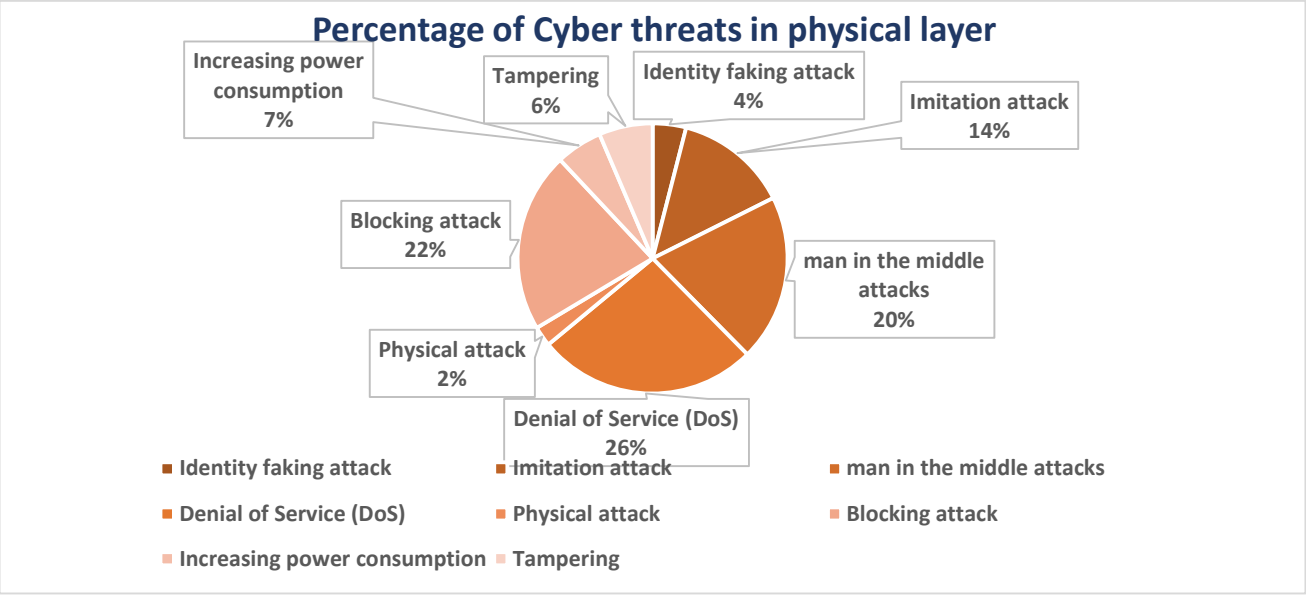

Fig. 4. Analysis of cyber threats in physical layer.

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

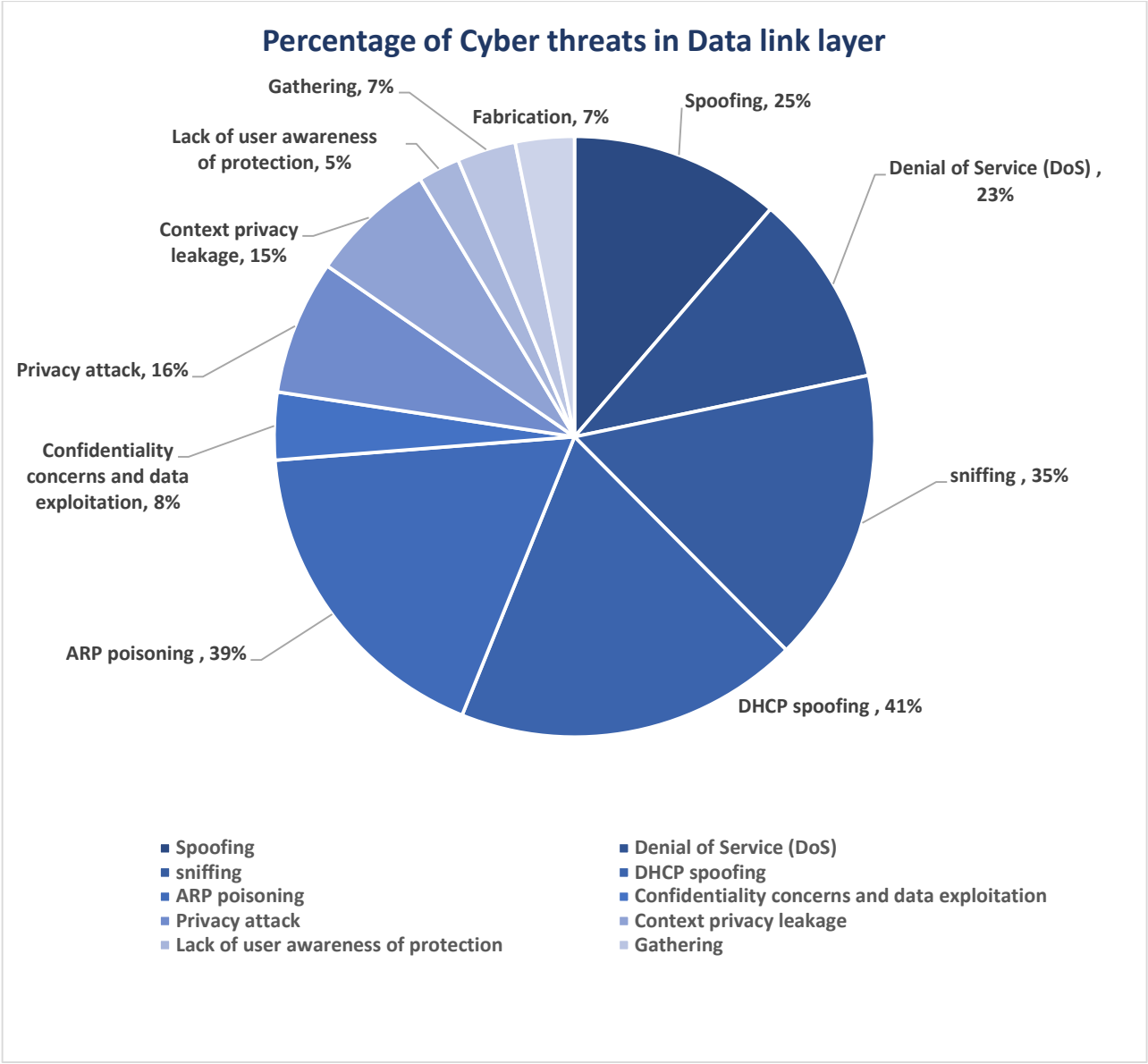

Fig. 5. Analysis of cyber threats in data link layer

Fig. 6 represents the analysis results of classifications of the most common cyber threats and attacks in the network layer. The results showed that the Sybil threat, Botnet attack and Sinkhole attack were the most common technical threats in the IoT network layer with percentage of 52%, 49% and 45% respectively. In addition, the results found that Denial of Service (DoS) attacks and reprogram attacks also were classified as the second level of technical threats in IoT with a percentage of 39% and 37% respectively. In the third level of technical threats in IoT were privacy attacks and context privacy leakage with percentage of 29% and 25% respectively. The remaining types of technical threats such as sending false code and tampering were in the lowest level of technical threats in IoT with a percentage of 12% and 10%. The results in Fig. 7 depicted the analysis results of classifications of the most common cyber threats and attacks in the transport layer. The results showed that TCP/UDP port scanning, TCP/UDP flooding attack and MQTT attack were the most common technical threats in the IoT transport layer with percentage of 34%, 33%

and 31% respectively. In addition, the results found that DNS poisoning threat, SYN-flooding and De-synchronization attack also were classified as the second level of technical threats in IoT with percentage of 27%, 26% and 24% respectively. The third level of technical threats in IoT were lateral movement attacks and DoS attacks with a percentage of 18% and 15% respectively.

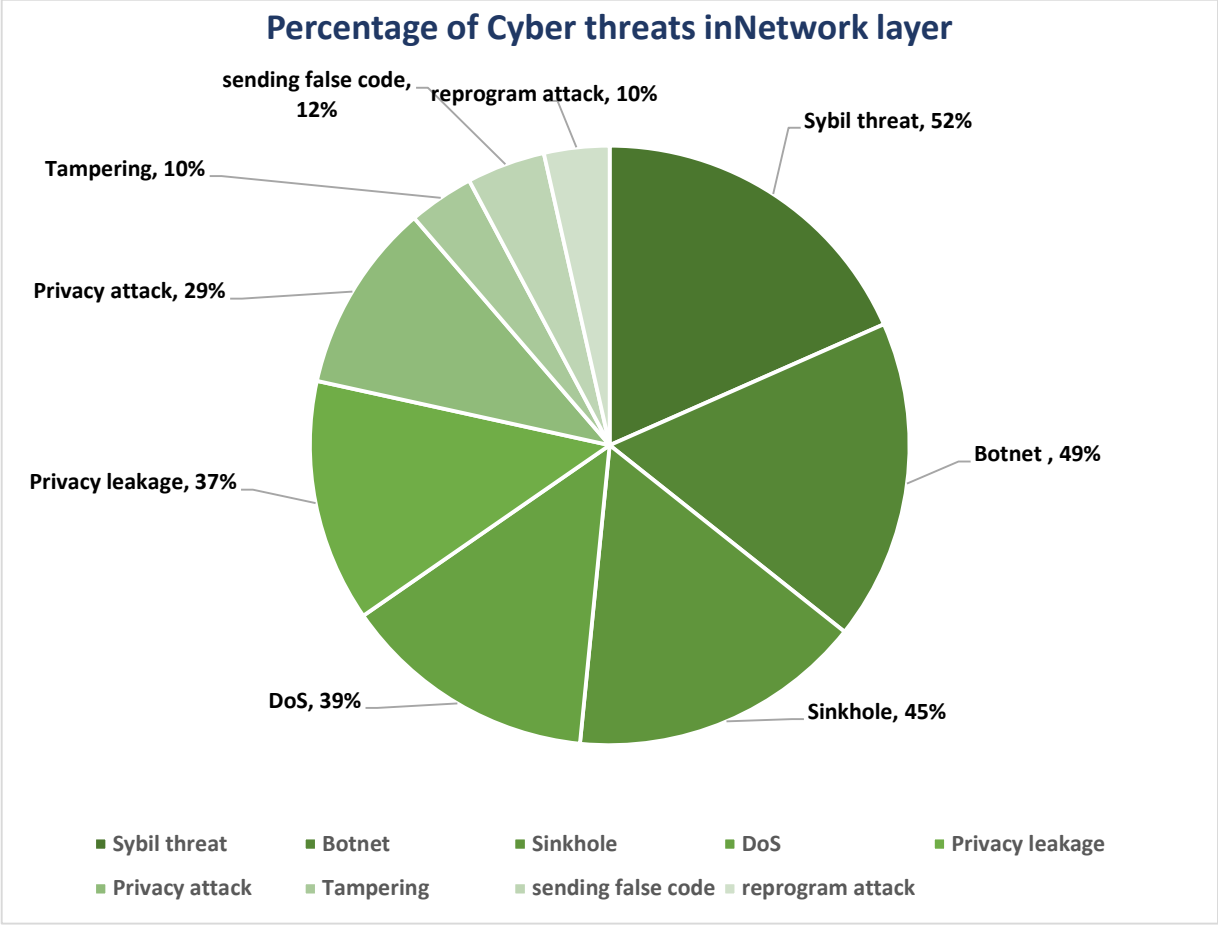

Fig. 6. Analysis of cyber threats in network layer.

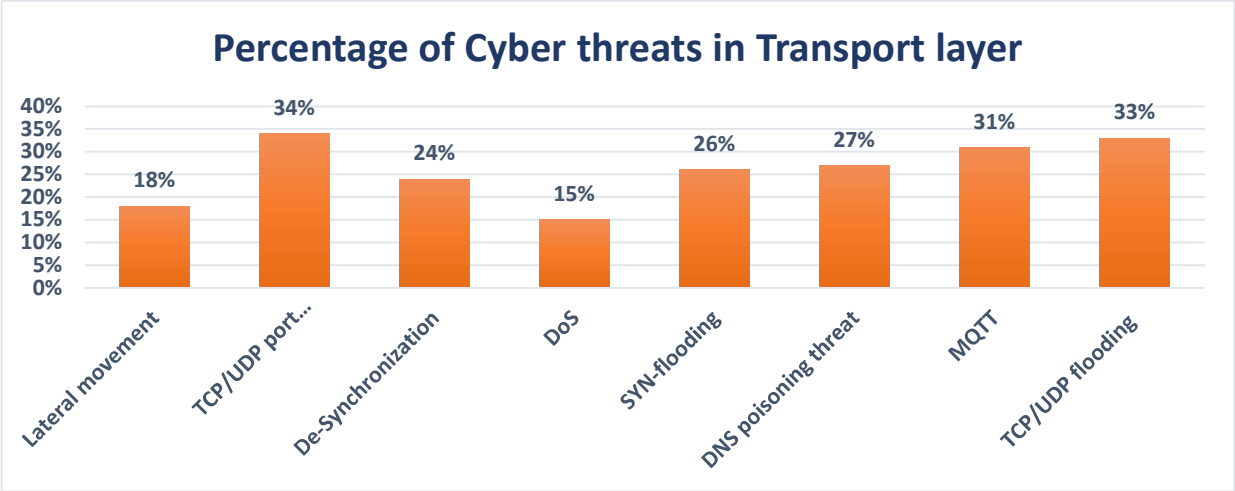

Fig. 7. Analysis of cyber threats in transport layer.

The results in Fig. 8 represented the analysis results of classifications of the most common cyber threats and attacks in the application layer. The results showed that DDoS attacks, Phishing threats were the most common technical threats in the IoT application

layer with a percentage of 72% and 66% respectively. In addition, the results found that SQL Injection threat, Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF) attack also were classified as the second level of technical threats in IoT with percentage of 55%, 53% and 52% respectively. The third level of technical threats in 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 in the lowest level of technical threats in IoT with percentage of 42% and 39%.

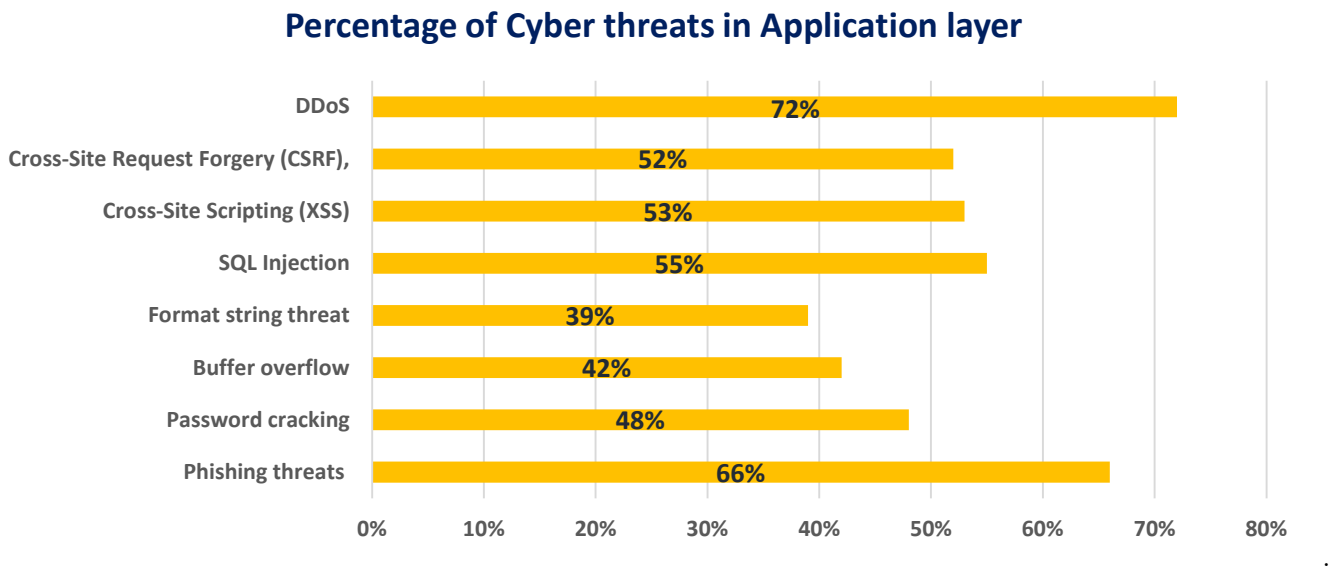

Fig. 8. Analysis of cyber threats in application layer**.**

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 physical layer, data link layer, network layer, transport layer and application layer as shown in Fig. 9. Security controls and countermeasures are mechanisms and tools developed in order to protect IoT systems from any cyber threats and attacks. These countermeasures are very important for protecting the integrity of data from any manipulation and safeguarding the database systems from unauthorized access. They can be classified into several types based on their functions, usage, effectiveness and importance. As shown in Figure 9, for example, encryption methods are considered one of the most powerful technical security controls for IoT systems for protecting sensitive data and rejecting unauthorized access. Multi-factor authentication is also a robust technique for preventing any unauthorized access to sensitive data and IoT systems. Firewalls also monitor packets in the IoT networks and defend them against attacks. Using the logs they keep they can audit and monitor every IoT access. Firewalls can offer a level of control over network traffic and prevent unauthorized access to sensitive data. Network segmentation also helps in restricting the spread of cyberattacks throughout the network and isolating vital resources and assets. Intrusion detection and Prevention systems (IDPS) also designed to detect and respond to new and advanced attacks. Intrusion Detection Systems (IDS) evaluate data using network traffic, IoT operations, SQL queries, system logs, etc. When an attack is identified, Intrusion Prevention Systems (IPS) stops them by either disabling connections, or blacklisting IP addresses, or changing firewall settings. IDPS combine signature-based and behavioral detection approaches. These two approaches help to identify zero-day attacks. Web Application Firewalls (WAF) is one of the critical security controls that protect web applications from various attacks, including injection attacks, cross-site scripting (XSS), cross-site request forgery (CSRF), and others, several security measures can be employed. Intrusion Prevention Systems (IPS) are designed to detect and block attacks at multiple levels. Endpoint Protection Platforms (EPP) provide multilayered security for endpoints, typically including anti-malware, endpoint firewalls, ad blockers, and intrusion prevention features. Ensuring secure communication within the perimeter defenses. Black box testing, where Web crawlers are used that identify the point at where SQL can perform, then monitor the application's response. Anti-Phishing Authentication (APA) technique that uses 2-way authentication and zero knowledge password proof. Address Space Location Randomization (ASLR) that 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, which demand continuous verification of all devices and users connecting to the network, thereby reducing the attack surface 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 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. Implementing multi-factor authentication and auditing network configurations

also contribute significantly to enhancing security in the network layer. Further, employing firewalls, intrusion detection/prevention systems, and secure communication channels like Virtual Private Networks (VPNs) can help protect IoT network infrastructures from malicious attacks.

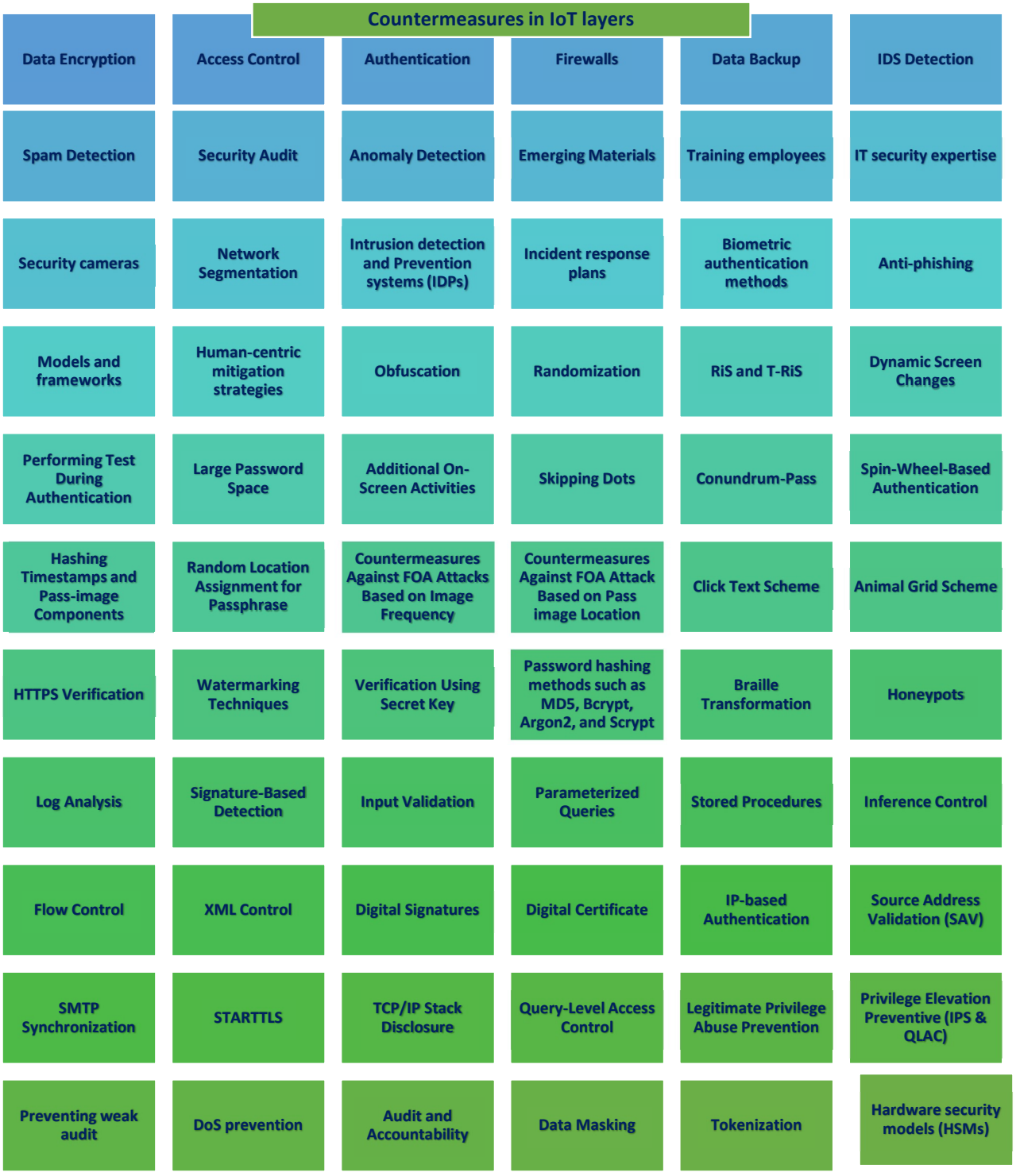

Fig. 9. The most common countermeasures in the database systems.

Table 11
Mapping the suitable countermeasures with against threats in data 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 12
Mapping the suitable countermeasures with against threats in network 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 13
Mapping the suitable countermeasures with against threats in transport 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.

Table 14
Mapping the suitable countermeasures with against threats in application 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	• A proposed framework for the security verification of distributed industrial control systems. The framework is based on modeling industrial IoT infrastructures. Patterns made by the attacks and mitigation techniques to stop the attacks. Using an alloy analyzer to prove mitigation techniques.

7. Conclusion

Now, cybersecurity-threats are the most critical challenges facing the IoT systems as well as increasing the number of cyber-attacks on IoT systems and becoming more sophisticated. Cyber-attacks in the IoT systems can cause a huge impact, including data loss, reputation damage, and failure of the system. Thus, it is necessary to understand the behavior of cyber threats on IoT systems and identify the suitable countermeasures to mitigate their impacts. Therefore, cyber-risk classifications and assessment play a prime role in risk management and establish a significant framework for determining and responding to cyber-threats. Risk assessment helps for understanding the impact of cyber-threats and develops appropriate security controls to mitigate the risk. This study provided a comprehensive analysis of cyber risks in the IoT systems, including classifying threats, attacks, impact and countermeasures. This classification assists to understand the suitable security controls to mitigate the cyber risks for each kind of threat.

The findings of this study indicated that DDoS attacks, Phishing threats were the most common technical threats in the IoT application layer with a percentage of 72% and 66% respectively. In addition, the results found that SQL Injection threat, Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF) attack also were classified as the second level of technical threats in IoT with percentage of 55%, 53% and 52% respectively. The third level of technical threats in IoT was Password cracking attacks with a percentage of 48%. The results showed that TCP/UDP port scanning, TCP/UDP flooding attack and MQTT attack were the most common technical threats in the IoT transport layer with percentage of 34%, 33% and 31% respectively. In addition, the results found that DNS poisoning threat, SYN-flooding and De-synchronization attack also were classified as the second level of technical threats in IoT with percentage of 27%, 26% and 24% respectively. The third level of technical threats in IoT were lateral movement attacks and DoS attacks with a percentage of 18% and 15% respectively. The framework in this study is considered as a vital tool for practitioners, policymakers, and researchers to identify, classify, and mitigate cyber threats within the IoT systems. Overall, our study provided a comprehensive analysis of the classification of cyber threats, vulnerabilities, impact and countermeasures in the IoT systems. The findings from this work can help organizations to understand the types of cyber threats and develop robust strategies against cyber-attacks.

Despite this research providing a comprehensive analysis of cyber risks in the IoT systems, including classifying threats, attacks, impact and countermeasures, there are still limitations that should be considered. First, cybersecurity threats and vulnerabilities are continuously evolving, and new threats can be created at all times. As a result, identification and classification of these threats may become outdated. Therefore, organizations, scholars and researchers must continuously be quick on updating their new threats investigations to stay ahead of hackers and attackers. Second, cyber threats are frequently interconnected and may occur simultaneously or in rapid succession. For instance, a cybercriminal might initiate a phishing attack to breach a database system, followed by deploying ransomware once access is obtained. In such scenarios, the traditional method of addressing threats in isolation may prove inadequate. Therefore, organizations, scholars and researchers must embrace a more comprehensive approach to threat management.

Acknowledgement

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. KFU241880).

References

Abdulhamid, A., Rahman, M. M., Kabir, S., & Ghafir, I. (2024). Enhancing safety in IoT systems: A model-based assessment of a smart irrigation system using fault tree analysis. *Electronics, 13*(6), 1156. https://doi.org/10.3390/electronics13061156

AlSalem, T. S., Almaiah, M. A., & Lutfi, A. (2023). Cybersecurity risk analysis in the IoT: A systematic review. *Electronics, 12*(18), 3958. https://doi.org/10.3390/electronics12183958

Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2024). Anomaly detection IDS for detecting DoS attacks in IoT networks based on machine learning algorithms. *Sensors, 24*(2), 713. https://doi.org/10.3390/s24020713

Alzahrani, A., & Asghar, M. Z. (2023). Intelligent risk prediction system in IoT-based supply chain management in the logistics sector. *Electronics, 12*(13), 2760. https://doi.org/10.3390/electronics12132760

Amro, A., & Gkioulos, V. (2023). Evaluation of a cyber risk assessment approach for cyber–physical systems: Maritime-and energy-use cases. *Journal of Marine Science and Engineering, 11*(4), 744. https://doi.org/10.3390/jmse11040744

Baho, S. A., & Abawajy, J. (2023). Analysis of consumer IoT device vulnerability quantification frameworks. *Electronics, 12*(5), 1176. https://doi.org/10.3390/electronics12051176

Cheimonidis, P., & Rantos, K. (2023). Dynamic risk assessment in cybersecurity: A systematic literature review. *Future Internet, 15*(10), 324. https://doi.org/10.3390/fi15100324

Czekster, R. M., Grace, P., Marcon, C., Hessel, F., & Cazella, S. C. (2023). Challenges and opportunities for conducting dynamic risk assessments in medical IoT. *Applied Sciences, 13*(13), 7406. https://doi.org/10.3390/app13137406

Hussain, I. (2024). Secure, sustainable smart cities and the Internet of Things: Perspectives, challenges, and future directions. *Sustainability, 16*(4), 1390. https://doi.org/10.3390/su16041390

Islam, M. R., & Aktheruzzaman, K. M. (2020). An analysis of cybersecurity attacks against the Internet of Things and security solutions. *Journal of Computer and Communications, 8*(4), 11. https://doi.org/10.4236/jcc.2020.84002

Kerimkhulle, S., Dildebayeva, Z., Tokhmetov, A., Amirova, A., Tussupov, J., Makhazhanova, U., Adalbek, A., Taberkhan, R., Zakirova, A., & Salykbayeva, A. (2023). Fuzzy logic and its application in the assessment of information security risk of industrial Internet of Things. *Symmetry, 15*(10), 1958. https://doi.org/10.3390/sym15101958

Lemos, J., de Souza, V. B., Falcetta, F. S., de Almeida, F. K., Lima, T. M., & Gaspar, P. D. (2024). A system for individual environmental risk assessment and management with IoT based on the worker's health history. *Applied Sciences, 14*(3), 1021. https://doi.org/10.3390/app14031021

Ntafloukas, K., McCrum, D. P., & Pasquale, L. (2022). A cyber-physical risk assessment approach for Internet of Things enabled transportation infrastructure. *Applied Sciences, 12*(18), 9241. https://doi.org/10.3390/app12189241

Park, J. S., Ham, H. M., & Ahn, Y. H. (2023). Expansion joints risk prediction system based on IoT displacement device. *Electronics, 12*(12), 2713. https://doi.org/10.3390/electronics12122713

Parsons, E. K., Panaousis, E., Loukas, G., & Sakellari, G. (2023). A survey on cyber risk management for the Internet of Things. *Applied Sciences, 13*(15), 9032. https://doi.org/10.3390/app13159032

Pourrahmani, H., Yavarinasab, A., & Monazzah, A. M. (2023). A review of the security vulnerabilities and countermeasures in the Internet of Things solutions: A bright future for the blockchain. *Internet of Things, 23*(21), 100888. https://doi.org/10.1016/j.iot.2023.100888

Pritika, Shanmugam, B., & Azam, S. (2024). Risk evaluation and attack detection in heterogeneous IoMT devices using hybrid fuzzy logic analytical approach. *Sensors, 24*(10), 3223. https://doi.org/10.3390/s24103223

Sánchez-Zas, C., Larriva-Novo, X., Villagrá, V. A., Rivera, D., & Marín-Lopez, A. (2024). A methodology for ontology-based interoperability of dynamic risk assessment frameworks in IoT environments. *Internet of Things, 27*(20), 101267. https://doi.org/10.1016/j.iot.2024.101267

Sheik, A. T., Maple, C., Epiphaniou, G., & Dianati, M. (2023). Securing cloud-assisted connected and autonomous vehicles: An in-depth threat analysis and risk assessment. *Sensors, 24*(1), 241. https://doi.org/10.3390/s24010241

Shokry, M., Awad, A. I., Abd-Ellah, M. K., & Khalaf, A. A. (2023). When security risk assessment meets advanced metering infrastructure: Identifying the appropriate method. *Sustainability, 15*(12), 9812. https://doi.org/10.3390/su15129812

Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the Internet of Things: A comprehensive review. *Sensors, 23*(8), 4117. https://doi.org/10.3390/s23084117

Waqar, A., Khan, M. B., Shafiq, N., Skrzypkowski, K., Zagórski, K., & Zagórska, A. (2023). Assessment of challenges to the adoption of IoT for the safety management of small construction projects in Malaysia: Structural equation modeling approach. *Applied Sciences, 13*(5), 3340. https://doi.org/10.3390/app13053340

Yi, J., & Guo, L. (2023). AHP-based network security situation assessment for industrial Internet of Things. *Electronics, 12*(16), 3458. https://doi.org/10.3390/electronics12163458