electronics

MDPI

Review

Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions

Esra Altulaihan [1], Mohammed Amin Almaiah [1,2,*] and Ahmed Aljughaiman [1]

[1] Department of Computer Networks and Communications, King Faisal University, Al-Ahsa 31982, Saudi Arabia
[2] Faculty of Information Technology, Applied Science Private University, Amman 11931, Jordan
* Correspondence: malmaiah@kfu.edu.sa

Abstract: The Internet of Things (IoT) interconnects physical and virtual objects embedded with sensors, software, and other technologies, which exchange data using the Internet. This technology allows billions of devices and people to communicate, share data, and personalize services to make our lives easier. Despite the multiple benefits offered by IoT, it may also represent a critical issue due its lack of information security. Since the number of IoT devices has been rapidly increasing all over the world, they have become a target for many attackers, who try to steal sensitive information and compromise people's privacy. As part of the IoT environment, data and services should be protected with features such as confidentiality, accuracy, comprehensiveness, authentication, access control, availability, and privacy. Cybersecurity threats are unique to the Internet of Things, which has unique characteristics and limitations. In consideration of this, a variety of threats and attacks are being launched daily against IoT. Therefore, it is important to identify these types of threats and find solutions to mitigate their risks. Therefore, in this paper, we reviewed and identified the most common threats in the IoT environment, and we classified these threats based on three layers of IoT architecture. In addition, we discussed the most common countermeasures to control the IoT threats and mitigation techniques that can be used to mitigate these threats by reviewing the related publications, as well as analyzing the popular application-layer protocols employed in IoT environments and their security risks and challenges.

Keywords: Internet of Things (IoT); cybersecurity; attack; vulnerabilities; threat; countermeasures; mitigation

Citation: Altulaihan, E.; Almaiah, M.A.; Aljughaiman, A. Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions. *Electronics* **2022**, *11*, 3330. https://doi.org/10.3390/electronics11203330

Academic Editors: Cristina Stolojescu-Crisan and Alexandru Isar

Received: 26 September 2022
Accepted: 14 October 2022
Published: 16 October 2022

1. Introduction

Today, the Internet of Things (IoT) is regarded as one of the most advanced technologies in the world [1]. The IoT is a term used to refer to the network of all physical devices connected to the Internet. It refers to computer devices that are web-enabled and capable of detecting, collecting, and transmitting data. There are a variety of applications for IoT, including the ability to remotely control appliances [2]. Through IoT, everything is connected to the Internet. The IoT is set to revolutionize the way we live. It is now a booming industry. According to analysts, the growth of IoT products and services is expected to accelerate in the next few years. IoT entails networked objects that can communicate their data across systems and servers, and their data can be controlled.

In IoT, objects, networks, and humans communicate using conscious and/or unconscious actions. By automating and reducing human input, IoT differs from the Internet, which relies on human input to run. In a wide range of areas, such as supply chain management, social media, medicine, and energy consumption (for example, smart health devices), the IoT has created opportunities for social and economic interaction.

The IoT has become an integral part of society; therefore, it is essential that these devices provide adequate security. With the increase in digitization, much of a user's data

is available on these devices, making the development of a secure device more important than ever. As internet-enabled devices are easier to hack, securing data is the paramount concern in any system [2].

IoT systems are unique when it comes to security vulnerabilities because of their complexity and heterogeneity of technology and data [3]. Addressing IoT security concerns is therefore critical. Data and services provided in the IoT environment need to be protected with features such as confidentiality, accuracy, comprehensiveness, authentication, access control, availability, and privacy. In terms of cyber security threats, the IoT has unique characteristics and limitations. Due to this, a variety of attacks and threats are emerging every day in relation to IoT [4]. Therefore, we must learn about the threats posed by this technology and find solutions to mitigate its risks. Knowing the types of attacks that can be made, as well as the techniques used to defend against them, is important [3].

People and organizations are experiencing a wide range of problems due to widespread and ever-increasing cybersecurity attacks against IoT systems. Cyberattacks have grown rapidly, in part due to the proliferation of IoT technologies in areas such as smart grids, environmental monitoring, patient monitoring systems, smart manufacturing, and logistics. The IoT presents security challenges due to the dynamic and transient nature of the connections between devices, the variety of actors capable of interacting within IoT systems, and the limited resources available [5]. As a result, we require special cyber security techniques to protect our systems and devices to ensure that our information is secure. Therefore, this study aimed:

- To review the recent threats and risks that have been associated with IoT.
- To classify threats on each layer of IoT architecture.
- To review the most recent mitigation techniques on IoT risks and identify the common methods that individuals and organizations can use to protect themselves from cyber-attacks that occur via IoT.
- To identify the suitable countermeasures for the IoT risks.

Several literature reviews have been conducted in the context of cybersecurity in IoT networks to identify the security vulnerabilities in IoT technologies and suggest solutions to mitigate them. For instance, Obaidat et al. [6] provided an overview of IoT application areas, security architecture frameworks, and security concerns, as well as reviewing recent security and privacy studies. Additionally, Elbekali [7] conducted a systematic literature review, which presents an in-depth analysis of the security of IoT, considering the generic architecture with layers and their security issues and solutions. In a recent study conducted by Albalawi and Almaiah [8], they assessed and identified the major cybersecurity attacks in IoT environments, as well as presenting the most important mitigation techniques that could be useful in IoT networks. In addition, Ghazal et al. [9] highlighted the core IoT security systems by identifying the main issues and countermeasures that need to be considered in IoT systems. The study focused on analyzing the different countermeasures for the cybersecurity for the different type's threats to protect the data loss in IoT-based systems to ensure information security. In a different literature review study, Abdullahi et al. [10] classified the types of cybersecurity attacks in IoT based on Artificial Intelligence techniques. The researchers found that two types of AI algorithms, namely support vector machines (SVM) and random forest (RF), are among the most used methods, due to high-accuracy detection. Nevertheless, our review paper differs from other papers in this area because it covers a wide range of topics related to IoT security. This study will define the overall architecture of IoT system. Additionally, this paper will explore the threats associated with the IoT environment as well as classify the threats on each of the three layers of the IoT architecture. As well as analyzing the popular application layer protocols employed in IoT environments and their security risks and challenges. Moreover, this study discusses the countermeasures methods that can be applied to such environments. Additionally, it outlines and discusses some techniques for mitigating risks in the IoT. This study aims to increase awareness about IoT security and to improve it. Additionally, this paper will help to raise awareness among individuals and organizations who have been

or may become victims on cybercrime due to their usage of IoT technologies. Table 1 presents a comparison of details of other related studies with our study in the context of IoT. Our systematic review will provide an in-depth analysis with future recommendations regarding cybersecurity risks and challenges and countermeasures in IoT networks and different security concerns in IoT application-layer protocols.

Table 1. Comparison of other related studies with our study in the context of IoT: (√: yes; x: no).

Literature	Year	IoT Architecture	IoT Security	IoT Protocols Security	Classification of IoT Threats	Classification of Mitigation techniques	Countermeasures
Obaidat et al. [6]	2020	x	√	x	√	x	√
Elbekali [7]	2022	x	√	x	√	x	x
Albalawi and Almaiah [8]	2022	√	√	x	√	√	√
Ghazal et al., [9]	2020	x	√	x	x	x	√
Abdullahi et al., [10]	2022	x	√	x	√	√	x
Our Study		√	√	√	√	√	√

The paper is organized as follows: Section 2 presents IoT's three-layer architecture. Section 3 analyzes security issues in IoT application-layer protocols. Section 4 describes the research methodology. In Section 5, related works are discussed. Section 6 summarizes the results. Section 7 concludes and discusses future research.

2. IoT Architecture

There is no universally accepted IoT architecture. Researchers have proposed different architectures. Several authors have proposed that the IoT architecture can be divided into three layers [8], as shown in Figure 1, which is the most basic architecture.

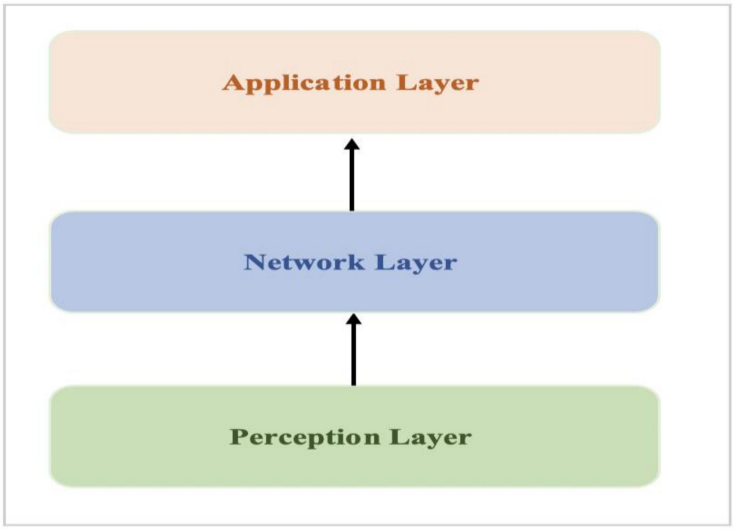

Figure 1. Three layers IoT architecture.

2.1. Perception Layer

Also known as the physical layer, this layer includes sensors that gather and provide information about the environment [9]. As a part of this layer, information is detected, gathered, and processed, and then transmitted to the network layer. Additionally, this layer enables IoT nodes to collaborate within a local or short-range network.

In security terms, the IoT perception layer has three security issues. Firstly, the signal strength of wireless signals. The majority of signals transmitted between IoT sensors are

transmitted via wireless technologies, whose efficiency can be compromised by disturbances. Secondly, the sensor node in IoT devices can be intercepted not only by the owner, but by the attackers as well, because IoT nodes usually operate in external and outdoor environments. This can lead to physical attacks on IoT sensors and devices aimed at tampering with their hardware components. The third aspect is that IoT nodes are often moved around due to the dynamic nature of network topology. As sensors and RFIDs make up most of the IoT perception layer, their storage capacity, power consumption, and computation capability are very limited, making them vulnerable to attacks and threats [9].

A replay attack, timing attack, node capture attack or a DoS attack can easily compromise the confidentiality of this layer. To address these security issues at the perception layer, encryption can be used (from point-to-point or end-to-end), authentication can be used (to verify the identity of the sender) and access control can be implemented.

2.2. Network Layer

This is for the transmission of data. Connections to other smart things, network devices, and servers are handled by it. This layer includes cloud computing platforms, Internet gateways, switches, and routing devices that employ very recent technologies, such as WIFI, LTE, Bluetooth, 3G, Zigbee, etc. [8].

There is a risk of DoS attacks at the network layer of the IoT. As well as DoS attacks, the adversary can also attack the confidentiality and privacy of network traffic by eavesdropping, passive monitoring, and traffic analysis. Since remote access and data exchange are common features of electronic devices, these attacks have a high likelihood of occurring. Man-in-the-middle attacks are also highly susceptible to eavesdropping on the network layer. The secure communication channel will be compromised if the keying material is intercepted. IoT key exchange mechanisms must be secure enough to prevent intruders from eavesdropping and committing identity theft. It is important to protect the network as well as the objects in the IoT [9]. A network object should be able to monitor the network's state and protect itself from attacks. It is possible to achieve this by having good protocols and software that enable objects to respond to situations and behaviors that may be considered abnormal or potentially dangerous.

2.3. Application Layer

Provides application-specific services to the user. The application layer ensures the data's integrity, authenticity, and confidentiality. This layer is where the smart environment or purpose of IoT is realized. It describes a range of applications into which the IoT can be deployed, such as smart homes, smart cities, and smart health. Each layer has a set of threats and vulnerabilities associated with it.

In terms of application layer security, there are many issues. Data privacy and identity authentication can be very difficult to ensure due to the different authentication mechanisms used by different applications. Applications that analyze the data will have a lot of overhead due to the large amount of connected devices sharing data, which can have a big impact on availability. Additionally, when designing IoT applications, it is important to consider how different users will interact with them, how much data will be revealed, and who will manage them. Data should be controlled by the users, and they should be aware of how the data will be used, who will use them, and when.

An architecture can also consist of five layers, adding the processing and business layers. Figure 2 shows the five layers: perception, transport, processing, application, and business. The role of the perception and application layers is the same as in the architecture with three layers. We outline the functions and security issues of the remaining three layers.

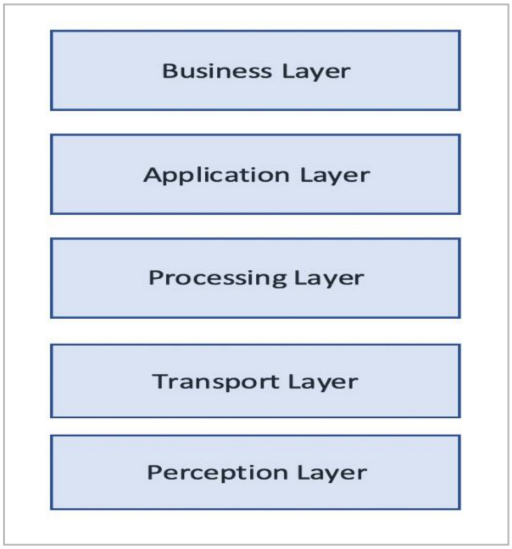

Figure 2. Five-layers IoT architecture.

2.4. The Transport Layer

Transmits sensor data from the perception layer to the processing layer, and vice versa, through wireless, 3G, LAN, Bluetooth, RFID, and NFC networks.

Among the threats at this layer are: De-Synchronization, where control flags are sent to synchronize endpoints. Another threat is SYN-flooding, where a system flood occurs during the SYN handshaking phase. For the MQTT protocol, data Transit Attacks and Scalable Key Management are also possible. Message authentication, optimizations in the transport layer, network filtering, Secure MQTT, and the ABE algorithm can be used to mitigate these threats [10].

2.5. The Processing Layer

This is also called the middleware layer. The transport layer stores, analyzes, and processes huge amounts of data. As well as managing and providing a wide range of services, it can also integrate with the lower layers. Various technologies are used, including databases, cloud computing, and big data processing.

2.6. The Business Layer

Manages the entire IoT system, including applications, business models, and user privacy.

3. Security Services in IoT Application-Layer protocols

In this section, we present the IoT application-layer protocols, which are considered the main component of the IoT environment as shown in Figure 3. In addition, these protocols are the backbone for all communications between IoT devices and between IoT devices and network infrastructure [10]. The two key functions of these protocols included (1) exchanging the messages and sharing data between IoT devices and (2) offering the service discovery by detecting IoT devices. Based on this, these protocols were divided into two categories as follows:

- Messaging protocols, including five protocols, namely: MQTT, CoAP, AMQP, DDS and XMPP.
- Service discovery protocols, including two protocols, namely: mDNS and SSDP.

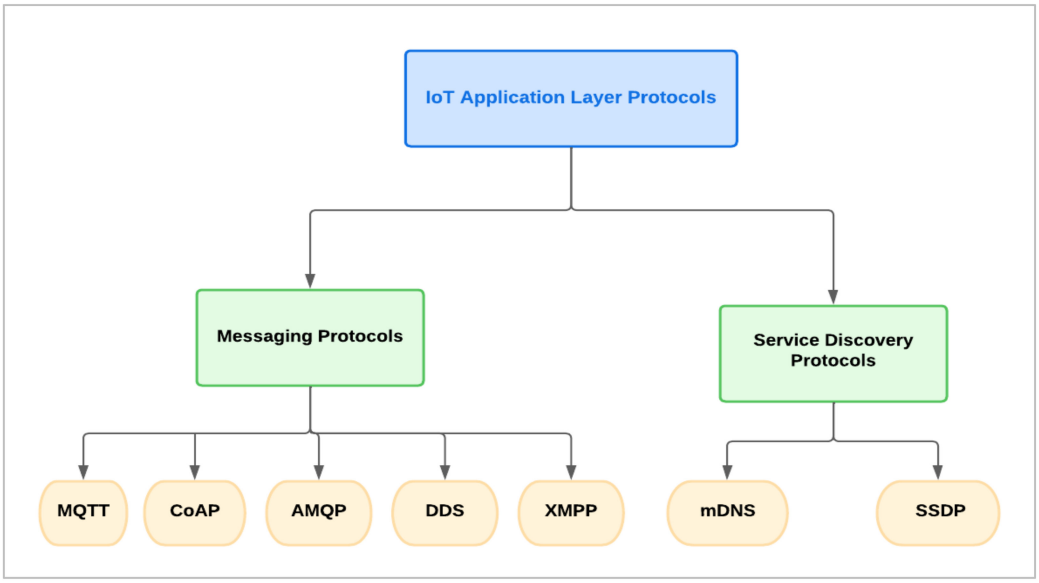

Figure 3. IoT application-layer protocols.

Regarding security services provided by IoT application protocols, there are several mechanisms and functions that help in mitigating attacks, such as encryption, authentication, authorization and confidentiality. However, some of protocols, like MQTT, CoAP, AMQP, DDS and XMPP, support encryption, authentication, authorization and confidentiality. Meanwhile, mDNS and SSDP do not offer any kind of security mechanism. Table 2 presents security services provided by IoT protocols for mitigating attacks.

Table 2. Classification of security services provided by IoT protocols for mitigating attacks.

Protocol/Service	Encryption Service	Authorization Service	Authentication Service	Confidentiality Service
MQTT	√	×	√	√
CoAP	√	×	×	√
AMQP	√	×	√	√
DDS	√	√	√	√
XMPP	√	√	√	√
mDNS	×	×	×	×
SSDP	×	×	×	×

3.1. Messaging Protocols

A discussion of messaging protocols in IoT environments is presented in this section. IoT environments prefer MQTT and CoAP, which are widely accepted, while AMQP, DDS, and XMPP can find uses in IoT despite not being considered typical IoT solutions.

3.1.1. Message Queuing Telemetry Transport Protocol (MQTT)

MQTT is a lightweight (M2M) connectivity protocol from OASIS/ISO, a publish/subscribe protocol that manages messages between nodes, which is an alternative to traditional client/server protocols, which connect the client directly to the endpoint. Publishers, subscribers, and brokers are the fundamentals of MQTT. Brokers act as servers, while publishers and subscribers act as clients. Brokers are intermediary nodes that relay messages based on their topics. Hierarchical organization is used to organize the topics. Messages sent to all subscribers of a given topic can be deleted by the broker, as well as messages that do not have subscribers. A publisher, subscriber, or both can be embedded

in an IoT device or network service or process [11]. The MQTT protocol supports a variety of authentication mechanisms as well as encryption based on TLS. These services, however, are not enough to protect MQTT-enabled devices, particularly brokers.

MQTT can be used by any IoT platform for unconstrained devices. The upper layer is responsible for ensuring network availability and minimizing data transfer costs. Due to the infrequent transfer of short data, some constrained devices can support TCP and non-compressed messages. MQTT, however, is generally not a good choice for constrained devices. Data acquisition and notification/alarm analysis are possible with an IoT device that is only a publisher. IoT devices that are only subscribers can execute dispatched commands. IoT devices that act as both publishers and subscribers can be used for device discovery and configuration, data querying, and remote control. In the case of peer-to-peer communication between neighboring devices, MQTT may not be suitable. Many IoT applications use MQTT.

Based on the identification of potentially vulnerable processes of MQTT-enabled devices, the following classifications are possible: Authentication, in which the MQTT broker does not properly verify publisher/subscriber identities. An attacker could exploit these vulnerabilities to take control of MQTT devices or overload the broker and eventually cause it to crash. Authorization, in which publisher and subscriber permissions are not properly set by the MQTT broker. Data or functions of MQTT devices can be controlled by an attacker through this vulnerability. The delivery of messages that cannot be delivered because there aren't any subscribers [12]. A significant degradation of broker performance could result from this vulnerability. Message validation occurs when a publisher sends messages containing disallowed characters that broker and subscriber cannot correctly interpret. Many malicious attacks can be performed using this vulnerability. Message encryption, in which clients and servers exchange messages in plaintext, allowing attackers to eavesdrop and spoof them. Man-in-the-Middle (MiTM) attacks could be conducted using this vulnerability. There are also authentication and authorization security issues, such as clients who set their username to "#" and subscribe to all MQTT topics by bypassing access control mechanisms. An attacker can access sensitive data from all publishers with serious consequences for confidentiality as a result of this vulnerability [12].

There have been some proposals in the past for securing MQTT. Model-based Security Toolkit can be integrated with MQTT to meet security and privacy requirements, for example. In addition, Secure MQTT (SMQTT) was defined for MQTT and MQTT-SN. Based on lightweight Elliptic Curve Cryptography, this extension allows encrypted messages to be broadcast to multiple nodes at the same time. It is noteworthy, however, that the solutions mentioned above were not included in the most recent version of MQTT from 2019, which includes enhanced authentication methods, among others. In most cases, this method is used to carry SASL mechanisms, but it can also handle other mechanisms like Kerberos. Several mechanisms should be included in MQTT implementations in order to combat security threats, including authentication of users and devices, authorization of server resources, integrity of MQTT control packets and application data, and privacy of MQTT control packets and application data.

Finally, we can conclude that, although MQTT supports a huge number of security services, the services in general do not fully mitigate all security risks. Thus, we classified the potential security vulnerabilities in MQTT protocol as follows:

1. Security vulnerabilities in the encryption service: the threat arises from Man-in-The-Middle (MiTM) attacks performed by eavesdropping on messages exchanged between client and server, and then spoofing the messages.
2. Security vulnerabilities in authentication service: the attacker can exploit vulnerabilities in the MQTT protocol because the MQTT broker does not support important functions such as properly checking subscriber identity, and does not block repeated authentication attempts.

3. Security vulnerabilities in authorization service: the attacker can control data or functions of MQTT devices because the MQTT protocol has weaknesses with respect to properly setting permissions.

3.1.2. Constrained-Application Protocol (CoAp)

An application-layer protocol developed for constrained devices, it enables wireless sensor network nodes to communicate with the Internet. Data are transferred between clients/servers over the Internet using this protocol. The protocol is intended to be used between constrained nodes (low-power, loss networks, etc.), constrained nodes of different constrained networks, and constrained nodes and general Internet devices. Due to its simple design, it is ideal for (M2M) applications. It is possible to use CoAP with most devices that support UDP (user datagram protocol). A CoAP server will be added to end nodes (like sensors) from an architectural perspective. The CoAP client should be installed on the controller, where several end nodes will be managed by it. Sensors and actuators can communicate on the Internet of Things using CoAP, which is similar to HTTP for restricted devices [11].

CoAP, the Datagram Transport Layer Security (DTLS) protocol, which provides equivalent security assurances to TLS, is used. There are four security modes in the DTLS binding for the CoAP protocol, ranging from no security to certificate-based security. It is up to developers to find the best balance between performance/energy constraints and security requirements. Obviously, attackers could easily compromise CoAP environments if they lacked appropriate security services [13].

The following classifications are possible based on the identification of potentially vulnerable processes in CoAP-enabled devices: message parsing, where the logic behind the client and server parsers does not correctly handle incoming messages. Due to overload conditions, this vulnerability could affect CoAP node availability and even allow the attacker to remotely execute arbitrary code on the target node. A proxy or cache that does not properly implement access control mechanisms. By exploiting this vulnerability, CoAP messages could be compromised, resulting in a loss of confidentiality and integrity. Bootstrapping involves improperly setting up new CoAP nodes. A vulnerability such as this could allow unauthorized nodes to access a CoAP environment. Moreover, key generation, the generation of cryptographic keys, is not sufficiently robust. CoAP nodes could be compromised if these keys were used. In addition to spoofed response messages and acknowledgments, an attacker could perform reflection/amplification attacks by forging the IP addresses of CoAP nodes. A cross-protocol exchange occurs when an attacker sends a message to a node with a false IP address and a fake source port number; this node responds by forcing the target node to interpret the received message according to its rules.

The CoAP protocol can be used by any IoT platform with constrained devices or unconstrained devices. For constrained devices, special consideration should be given to how the payload is coded in order to minimize the payload's size and volume. An IoT device acting as a client can be used to collect data, monitor notifications and alarms, and discover and configure devices. Using an IoT device as a server, one can execute commands, query data, and control the device remotely. Using IoT devices both as clients and servers in any communication schema, including peer-to-peer networks, is possible. The CoAP protocol can be used in any application that is Web-of-Things based. The protocol is just as flexible as HTTP, but is best suited for device-to-device communication. When designed and programmed thoughtfully, it is effective for communicating with constrained devices. To ensure complete stability, the Constrained Application Protocol (CoAP) uses DTLS connectors with different protection modes. A particular RFC-7252 format is used for CoAP messages in order to protect correspondence. For CoAP multicast support, authentication and key management (AKM) are required [12]. DTLS is strongly recommended as a means of securing CoAP nodes. The literature has also discussed several mitigation measures for different scenarios, including access control mechanisms and secure communication mechanisms.

3.1.3. Advanced Message Queuing Protocol (AMQP)

AMQP is an OASIS open standard binary middleware application-layer protocol for message-oriented middleware applications. It replaces existing proprietary messaging middleware. It offers queuing, routing, orientation, security, and reliability (SASL/TLS). Messages and communication patterns can be efficiently exchanged using AMQP. Because AMQP depends heavily on the messaging provider and client, different implementations of the protocol are interoperable. The data format description is sent across the network as a stream of bytes because AMQP is a wire level protocol. The ability of tools to manage messages confirms that data formats can be interoperable with other tools regardless of the programming language used [11].

AMQP can be used by any IoT platform for devices that are not constrained. Application programming is needed for pay-per-use devices connected to the Internet via AMQP to minimize communication costs. AMRQP does not define roles for communicating devices, but it specifies messages that simplify the design of a wide variety of complex application networks. It is possible to use AMQP to support all IoT communication schemas. It might not be very efficient, however, if peer-to-peer data exchange is opportunistic. Applications that can make use of AMQP's rich functionality would be a good choice. The origins of this protocol are related to applications in distributed financial applications. Business applications mostly use this protocol.

A key aspect of AMQP's security is its support for Simple Authentication and Security Layer (SASL) and Transport Layer Security (TLS) to ensure the integrity and confidentiality of communications. Security services such as MQTT and CoAP, on the other hand, are generally enabled by default, thereby reducing security risks. However, the NVD database shows that a wide variety of vulnerabilities have been found in AMQP-based products and services over the past six years. As a result of these vulnerabilities, several processes are affected, such as access control, message and identity validation, as well as message queue management. Vulnerabilities such as these can be exploited to escalate privileges, reveal sensitive information, cause denial of service attacks, bypass authentication and authorization, execute remote code, or hijack traffic. As a result of several vulnerabilities involving hostname and certificate validation, attackers can spoof identities and intercept traffic for MiTM attacks. Likewise, attackers can execute privileged commands in message queues due to the lack of access control. In addition, broker configurations pose security risks in AMQP environments. Although AMQP brokers have a web user interface, they can be challenging to set up. It is possible for serious vulnerabilities to develop as a result of incorrect choices in the configuration of message queues, exchanges, producers, and consumers. Furthermore, the user interfaces may be vulnerable to vulnerabilities common to the web domain [12].

3.1.4. Data Distribution Service (DDS)

DDS is maintained by the Object Management Group (OMG). Despite being an open standard, some solutions in the standard are protected by US patents. The DDS communication service operates on a publish–subscribe paradigm, without a broker. By using terminal nodes, it performs its functions in a distributed manner. DDS works by publishing data to local caches associated with subscribers, and automatically propagating that data between caches. The node can only be a publisher or subscriber, or both. A defined QoS attribute governs the data transfer process. Furthermore, DDS automates the switch between the primary and backup nodes in case of a failure of the primary node.

DDS can be used on any IoT platform. Additionally, DDS supports every communication schema used in IoT systems. When it comes to data queries, however, it is not very efficient. Direct peer-to-peer communication is possible with DDS, but discovery and authentication are carried out by a known server, making this difficult to implement. A machine-to-machine communication solution needs to be reliable, perform well, provide real-time operations support, and be scalable. Among the applications that DDS is intended to support are the industrial internet, cyber-physical systems, and mission-critical systems.

In terms of security, the DDS protocol offers a wide range of mechanisms. Both TLS and DTLS are supported by DDS, as are other messaging protocols. A set of built-in plugins is used in the newest OMG DDS security specification to ensure confidentiality, integrity, and authenticity of the exchanges. DataWriters and DataReaders can be authenticated and authorized via plugins, thus preventing unauthorized publication and subscription. Despite this, both the specification and the plugins are vulnerable. Attackers can discover potentially sensitive reachability information by intercepting the handshake protocol used for permission attestation. Attackers are able to collect information that could be used for malicious purposes by exploiting this vulnerability. Furthermore, plugins per se do not guarantee the security of DDS environments. There were two vulnerabilities found in the Access Control plugin that could allow participants to connect unintentionally or unauthorizedly. Additionally, not every DDS product or service is compliant with the security specifications, and even compliant implementations can be vulnerable. It has been shown that node misconfiguration can be exploited in DDS to perform malicious activities.

3.1.5. Extensible Messaging Protocol (XMPP)

This is an XML communication protocol designed for message-oriented middleware that supports a broad range of applications, such as presence and instant messaging collaboration. Data is exchanged between network nodes in close to real-time using extensible and structured formats. It allows instant messaging between applications and is extensible. In this protocol, XML elements are streamed over a network in near-real-time to exchange messages and presence data. Aside from that, it supports publish–subscribe systems over TCP, including VoIP signaling, video, file transfers, and IoT applications such as social services and smart grids.

A key advantage of XMPP is that it is decentralized; it does not require a central server; anyone can run their own server. It is free to implement standards, and you do not have to pay royalties or permissions to do so. In terms of security, authentication, encryption, etc. Furthermore, it supports interoperability and it is easy to understand and implement the protocol. Using the XMPP protocol, Google-Talk can be accessed by any instant messaging provider. However, the disadvantages of XMPP include the fact that it does not support Quality of Service (QoS), text-based communications induce higher network overheads, and binary data must first be encoded in base64. Additionally, clients and servers for XMPP are not officially supported [13].

In terms of security, the XMPP protocol provides robust security services through SASL authentication and TLS data encryption. Due to the fact that these services are built into the core specifications of the protocol, they are enabled by default. Despite this, the protocol is vulnerable to various types of threat due to its lack of end-to-end encryption support. An attacker could, for example, modify, delete, or replay stanzas or gain unauthorized access to a server. In addition to its security issues, XMPP-based products and services have numerous vulnerabilities. It is possible to exploit these vulnerabilities in different ways, such as making the services unavailable, obtaining sensitive information, or gaining access to XMPP servers. There are also vulnerabilities associated with custom functionalities that can be built over XMPP [14].

The XEP series of XMPP incorporates several practices designed to mitigate security threats. For instance, measures aimed at discouraging DoS attacks focus on the proper use of certificates for SASL authentication. Despite this, several XEPs contain vulnerabilities as a result of incorrect implementations of the XEPs themselves. It is possible for attackers to exploit these vulnerabilities in order to gain access to private data or to impersonate users and carry out social engineering attacks.

3.2. Service Discovery Protocols

There are several Service Discovery Protocols (SDPs) for IoT environments that help clients find services available on the network. In this section, we will introduce the most commonly used SD protocols, including mDNS and SSDP.

3.2.1. Multicast Domain Name System (mDNS)

This open protocol based on the Internet Protocol (IP) and the User Datagram Protocol (UDP) is defined by the Internet Engineering Task Force (IETF). An mDNS client can discover an endpoint's IP address by resolving the hostname. mDNS clients send IP multicast query messages over the network. This message calls the host with that name for a reply and identification. It replies with a multi-cast message that contains its IP address once it receives the message. That multicast message updates the mDNS caches of all nodes in the network receiving it. A combination of this protocol with DNS-based Service Discovery (DNS-SD) enables environments to seamlessly integrate new devices and perform DNS-like functions without the need for conventional DNS servers.

A major advantage of mDNS is the fact that it is designed for small networks and is intended to make them more user-friendly. The idea is to make it possible for users to connect devices to secret LANs without any problems. IP addresses allow all devices to communicate with one another, so there is no need to establish a server or directory. By doing so, additional devices can be imported quickly and dynamically. The disadvantages are as follows: the multicast process itself, although the protocol tries to keep network traffic low, requires constant monitoring of the network by the computers involved, and the allocation of host names is also problematic.

Security-wise, mDNS does not include any built-in security features, unlike messaging protocols. Therefore, mDNS environments are vulnerable to security attacks, similar to DNS. DNSSEC and DNS over TLS are recent attempts to enhance DNS security, but they are generally too complex for self-configuring networked environments. The potential security threats of mDNS include: Denial of Service attacks, where attackers flood nodes with messages exploiting specific characteristics of the protocol. If these messages invalidate cache entries or block probing, nodes could become unresponsive or unavailable. Another threat involves spoofing mDNS response messages and advertising fake services, which are frequently exploited for further attacks against unaware targets. Using mDNS-enabled nodes, attackers can abuse services for various purposes, such as DDOS attacks and sensitive data collection. Additionally, the multicast nature of the communications and the lack of encryption mechanisms might result in security and privacy issues that are often undetected. Personal information, as well as sensitive information about the nodes of the network and the services provided, is frequently disclosed in messages.

As already mentioned, mDNS does not include any security features. Due to the fact that the protocol is susceptible to a variety of threats, it is of paramount importance to develop effective mitigation measures. Solutions may be provided by simple measures offered by operating systems or by sophisticated solutions based on the mDNS protocol. Specific measures, mainly aimed at mitigating DDoS attacks, could include the following: Reducing the attack surface by disabling mDNS services whenever not needed, and blocking traffic from/to outside the local link by disabling mDNS UDP port 5353.

3.2.2. Simple Service Discovery Protocol (SSDP)

The SSDP protocol is based on IP, UDP, and SOAP. When an SSDP client detects SSDP services, it multicasts a discovery request to the SSDP multicast channel and port. An SSDP service listens on that channel until a discovery request matches the service they provide, and then responds by unicasting. Plug-and-play devices can be transparently configured using this protocol as part of the Universal Plug-and-Play architecture (UPnP).

Security-wise, SSDP is very weak, similar to mDNS, because no built-in mechanism is provided. SSDP-enabled devices are therefore subject to a variety of security risks. In general, these risks exploit the multicast nature of service discovery. Amplification/Reflection Distributed Denial of Service attacks are a major threat to SSDP nodes, which render devices unresponsive and services unavailable. In addition to exploiting the characteristics of UDP and SSDP, these attacks also take advantage of device misconfigurations. With a spoofed IP address, an attacker could send an M-SEARCH message to the target node. As a result of such attacks, a set of vulnerable SSDP devices will flood the node target of the

attack with high-amplification response messages. Passive attacks by eavesdropping on multicast messages exchanged as plaintext over the network represent another security threat affecting SSDP-enabled nodes. Consequently, this threat could allow access to sensitive information without any warning, resulting in serious privacy and confidentiality concerns. The following security issues can also be exploited with SSDP-enabled nodes: Poisoning attacks, which use NOTIFY request messages to advertise fake services. It is common for these services to be exploited for further attacks against unaware systems. Additionally, attackers exploit vulnerabilities in misconfigured devices to gain access to internal network resources or use them to conduct further malicious activities through device reconfiguration.

To mitigate these threats, SSDP-enabled nodes are exposed to threats and attacks due to the lack of built-in security services. It is, therefore, necessary to seek appropriate countermeasures. It is particularly important to consider SSDP's peculiarities. This type of incoming traffic might need to be blocked as a mitigation measure against conventional DDoS attacks. Open SSDP is already known to be vulnerable. These measures, however, are not effective for mitigating DDoS attacks targeting SSDP nodes that use random ports. It is important to disable SSDP services on individual nodes whenever they are not needed, since they are often enabled by default. Due to the abnormal use of this type of message, unicast M-SEARCH request messages should also be handled carefully. Additionally, it is important to note that encryption mechanisms that ensure the authenticity and confidentiality of the exchanges and prevent possible abuse of the content must be implemented at the level of the SSDP services, not at the protocol level itself.

4. Research Methodology

To conduct this study, we followed PRISMA as it progressed through four stages. For the identification stage, we searched the Saudi digital library database and the Google scholar database for papers describing cybersecurity threats and IoT, and for papers published between January 2016 and April 2022. Among the exclusion criteria were papers not written in English, papers not directly related to cybersecurity threats on IoT, and papers not available online. The source types were academic journals or conference papers. At the identification stage, 8695 papers were identified; after removing duplication, 6560 papers remained. Out of 250 papers screened for title and abstract, 150 were excluded for not fitting the criteria closely at the screening stage. At the eligibility stage, 100 studies were eligible to move on to the final stage. A total of 100 articles were included in the inclusion stage; of these, 65 were eliminated, leaving 35 for further review. Figure 4 illustrates the selection of previous studies.

Table 3 lists the publication years of the selected papers from 2016 to 2022, and as shown in Figure 5, most of the selected papers were published in 2021.

Table 3. Distribution of selected papers publication year.

Year	Number of Papers
2016	2
2018	1
2019	2
2020	7
2021	18
2022	5

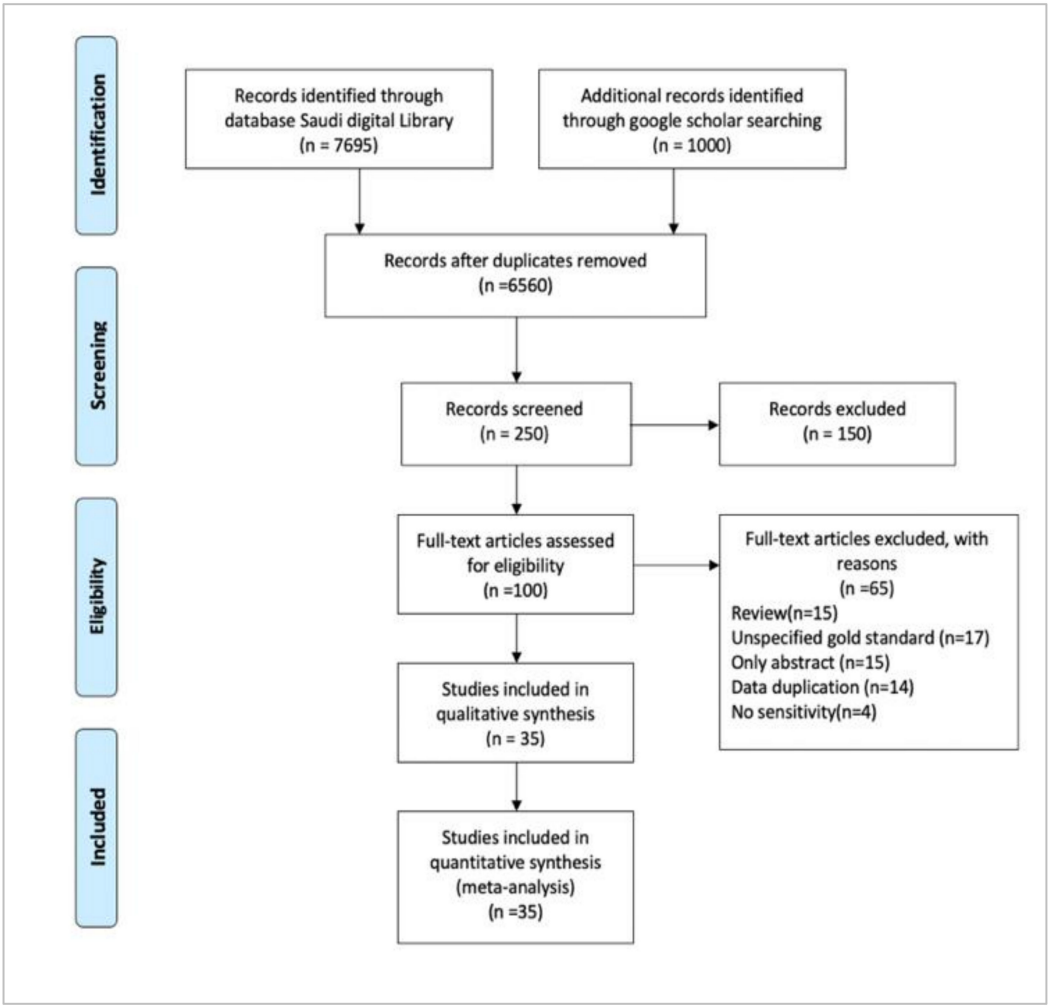

Figure 4. Schematic diagram PRISMA literature review.

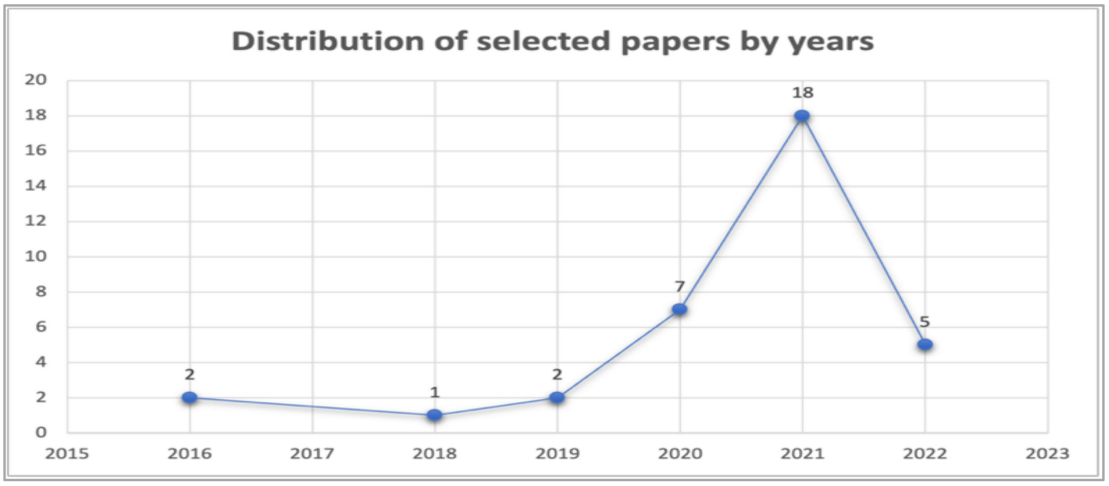

Figure 5. Distribution of the selected papers' publication year.

5. Existing Work

In this section, several research studies are reviewed that are related to cybersecurity threats associated with IoT technology.

5.1. Threats in IoT

Choudhary et al. [2] explored threats, vulnerabilities and challenges posed by IoT technology. Then, the paper suggested several security controls that would protect against each vulnerability.

Patel [15] discussed IoT architecture, threats in IoT devices, and solutions for each layer in the IoT architecture. The purpose of this paper was to define the architecture of the IoT devices, to categorize threats in the four-layer architecture, and to implement security techniques at each layer.

Dange et al. [16] analyzed the recent major attacks targeting IoT systems, as well as a list of possible attacks targeting IoT systems at the physical and network layers. The evolution of IoT botnet is discussed, along with its architecture, lifecycle, and comparison with traditional botnets. A case study of the Mirai botnet is presented. Additionally, tools and techniques that can be used to detect botnets are discussed. In addition, they considered the importance of preventing IoT botnet proliferation. The paper aimed to enhance the security of this devices by studying recent attacks on IoT systems. There was more attention paid to the IoT botnet, which has become a major threat.

Hasan Ali et al. [17] examined evolution sparse convolution network (ESCNN) intrusion and threat activities on the Internet of things (IoT). The study's primary aim was to reliably detect threats and intrusions from data traffic presented on the network and on the host. Study limitations included fast computation, high reliability, and a reduced complexity of computation. Future work using big data approaches and deep learning CNN architecture models will improve the effectiveness of the system using a metaheuristic optimizer to estimate the global solution to attack prediction. The paper's major contributions are that: In the IoT paradigm, threats and attacks have posed significant security and privacy concerns. Security and privacy concerns were raised by this IoT paradigm due to threats and attacks. Furthermore, training patterns are used in the network to classify the standard and the threat.

Aamer [18] analyzed security threats related to IoT, and a three-dimensional security model for IoTs was proposed. Additionally, each layer's safety-critical technologies were presented in the full model. The Internet has many security issues, as a large-scale integrated system with multiple layers. The purpose of this paper is to analyze the security situation of IoT based on real-life attack cases, analyze the security threats from the perspective of physical security, computing security, and data security, and lay out the technologies that should be prioritized in the security of IoT.

A generic IoT architecture was discussed and presented in Gerodimos et al. [19], as well as communication protocols. They also discussed current security threats in IoT. Moreover, they examined current challenges and offers effective solutions. The purpose of this study was to review IoT fundamentals from a general standpoint by addressing issues such as standardization, security and use cases.

Pahlevanzadeh et al. [5] presented a four-layered IoT security framework. Additionally, threats and vulnerabilities identified and analyzed for each IoT layer were discussed, along with security solutions and considerations that could improve security services. Having a secure system requires enhancing the basic security principles in network implementation, including making the network as safe and secure as possible, creating scalable protection, and ensuring data privacy. This study aimed to gain a deeper understanding of the emerging IoT security threats and appropriate approaches to protecting against them by studying the challenges and solutions associated with IoT security. Researchers pointed out that in future research, we need to pay attention to intelligence, active defense systems, and resource conservation capabilities, comprehensive prevention, improved information security, ongoing technological research, and ensuring IoT control capabilities.

Tsiknas et al. [20] provided a review of literature on surveys on the threats associated with the industrial IoT systems. It also provided a comprehensive analysis of the most popular methods of attacking industrial applications. It outlined the major security risks and suggested possible countermeasures. The study began with an examination of related

studies. A description of the key risks affecting industrial IoT, how they operate, and the effective solutions being offered in the most recent literature was then provided. Lastly, they summarized their findings. As part of the study, a detailed description of industrial IoT attacks and their associated vulnerabilities is provided, as well as a detailed analysis of indicative solutions against these vulnerabilities, which have been proposed in recently published literature. This study provides researchers, and organizations working with industrial IoT technologies in general, with a comprehensive study of threats related to cyber-attacks on industrial equipment.

Ahmad et al. [21] elaborated on the different types of security attacks in relation to the different layers of IoT, including physical attacks, software attacks, network attacks, and encryption attacks. There was also a presentation of some IoT applications such as Smart Homes, Smart Cities, Smart Grids, Health Sector, and Security & Emergencies. Researchers and manufacturers will be able to use the results of this study to evaluate and decrease the attack range on IoT devices. The paper's main contribution is examining a few different security issues associated with various IoT layer infrastructures. The study is designed to provide information to IoT researchers and manufacturers to help them improve the security of future devices.

Ahlawat et al. [22] presented the architecture or model of IoT, as well as the challenges encountered by researchers like data mining problems and privacy issues. The study aimed to describe the architecture or model of the Internet of Things and the challenges faced by researchers, such as data mining challenges and privacy concerns. Furthermore, various security attacks have been described at various levels, including the perception, transportation, and application layers. A comparison of various security models and the techniques used was also presented. Several security issues were presented at the application layer, including data theft, service interruption, sniffing, access control, reprogramming, and malicious code injection attacks. Additionally, the paper presented four major IoT challenges, namely data management, privacy, security, and chaos.

Wheelus et al. [23] considered the security risks related to IoT systems, and they proposed a machine-learning-based approach to categorize and detect IoT attacks. Two essential goals of the study were to provide practical insights into IoT network threats and risks, so researchers and practitioners could understand the commonalities and differences between IoT network security and general network security. Secondly, to create a data-driven reference framework as a mechanism for detecting attacks and security breaches in real-world IoT systems. As a platform, they used a real-world IoT system with secured gate access, and introduced the IoT system in detail, including features for capturing cybersecurity threats/attacks. They analyzed data collected over a nine-month period to evaluate the effectiveness of predictive models trained through machine learning and proposed design principles and a loose framework for implementing secure IoT systems. They analyzed IoT system and network characteristics as well as IoT threats and risks.

Ben-Eid [24] introduced two basic IoT architectures, namely the three-layer architecture and the five-layer architecture, since these are the most recommended. The three-layer architecture includes the perception layer, the network layer, and the application layer. The five-layer IoT architecture includes the sensing (perception) layer, the network (communication) layer, the middleware layer, the application layer, and the business layer. The paper then outlined some of the features of the IoT, including intelligence, connectivity, its dynamic nature, sensing, heterogeneity, and security. Afterward, they listed reasons that IoT technology is vulnerable to specific kinds of security threats (attacks) and categorized them according to severity. Additionally, in this study, various possible threats were discussed for each of the layers of the IoT system.

Kabulov et al. [25] discussed the security issues as well as operational requirements for the IoT automation system, including interoperable devices and systems, real-time operations, and engineering simplicity. Additionally, the study provided a layer-by-layer overview of potential security threats in industrial IoT and possible mitigations. The paper was written with the following sections: sensors, actuators, gateways and networking,

data processing, and application layers. An important contribution of the study was a layered analysis of the security issues surrounding IoT automation, as well as a detailed development solution for mitigation measures.

Haque et al. [26] discussed IoT architecture layer interpretations, the interplay of IoT elements, and IoT applications. The paper also critically analyzed recent literature on IoT security and privacy issues. IoT cybersecurity situations are presented in this paper in a state-of-the-art overview. Furthermore, a recent literature review revealed future research areas to address for this technology to reach its peak. As mentioned throughout the paper, an IoT system with limited resources presents many technological challenges. Additionally, as new technological innovations emerge, there will be challenges that need to be addressed. In the paper, some of the recommendations are mentioned, while others will be implemented in the future.

Dhirani et al. [27] highlighted the cybersecurity challenges for IIoT/I4.0 and the risks to which the technology is vulnerable regardless of the cybersecurity standards and security protocols implemented. It also explained how to align different security and communication standards. Additionally, a review was provided of the author's previous research published in journals, conferences, and white papers relevant to the topic. Additionally, the report examined IT/OT convergence issues in detail.

Svotwa [28] examined IoT security and privacy concerns. It also discussed how insecure software impacts the IoT. In this study, the researchers assessed the security implications of IoT from both consumer and organizational perspectives and discussed possible solutions to these security issues. Data leaks that affect consumer privacy, unchanged default passwords by the consumer, and slow patches released by software developers are some of these security concerns. They mentioned that these security concerns can be addressed by establishing standards that describe which level of security and the conditions that must be met can be considered acceptable, by defining a framework for identifying defects, and by training developers on how to consider security during development.

Kozlov et al. [29] discussed IoT architectures, particularly from the perspective of security, privacy, and trust. The purpose of the paper was to examine the security, privacy, and trust implications of IoT infrastructure built from the bottom up and the top down. An additional consideration is the relationship between energy consumption and SPT and IoT architecture. They started by proposing a layered architecture. Following that, they analyzed the threat at different levels of security and privacy. They also examined the latest EU legislation pertaining to privacy and security. Among the findings of this analysis is the fact that managing IoT architectures requires an understanding of the domains of management. Who controls which aspects at what level? Regulations imposed by the EU would require, for example, an individual to have control over data about them at all levels of the architecture, particularly if they receive the data. A special focus was given to IoT architecture issues, as well as security, privacy, and trust, which people would attach to IoT architectures. The SWT program was discussed, as well. The paper reflects the overall architecture and threat analysis, including the EU's efforts to curb IoT threats.

Cvitić et al. [30] examined IoT security as it relates to cloud computing, computer networks and AIDC technologies as part of the IoT architecture. During this research, the collected data were analyzed, and new findings and risk classifications were presented. These findings provided a research direction for further studies on the safety critical layers of IoT architecture. The risk classification of layers is based on a qualitative assessment due to the lack of precise data. Due to the lack of exact data, each layer's risk classification is limited to a qualitative assessment. While the risk assessment can be affected by a variety of factors, classification of risk is primarily based on the growth of IoT applications in various environments during the period of 2013 and 2014. The study examined the problem from the perspective of a fundamental protection component of all information and communication environments: security risk. According to the results of the research, classification of security risks of architecture layers is proposed, as well as classification by type of usage of IoT.

Cunningham et al. [31] examined the history and evolution of IoT devices through the review of related papers, then analyzed IoT devices and how they work. The paper also identified pros and cons of IoT devices. Then, it reviewed security and privacy concerns related to IoT. It also looked at threats and attacks against IoT devices. The article examines how smart homes can be used, and the evolution of the IoT, as well as the challenges they face and their prospects. The paper contributes to gaining insight on how dangerous and vulnerable IoT devices in the home can be, but also provides many positive aspects to a Smart home such as better security.

Ikrissi et al. [32] investigated IoT security challenges and threats from multiple perspectives by reviewing related studies. In the study, different security issues were evaluated in the physical, network, platform, and application layers of the IoT architectural framework. The physical layer is the lowest level of the architecture. This layer contains a variety of devices, including actuators and sensors, that gather data and transmit it to the architecture's upper layer. Examples of threats here include malicious code injection attacks and eavesdropping attacks. A network layer is composed of basic networks such as communications networks, the Internet, and wireless sensor networks. This layer is vulnerable to outing, sniffing, and traffic analysis attacks. Between the application layer and the network layer, the platform layer serves as an intermediary layer. The platform layer is vulnerable to cloud malware injections, SQL injections, storage attacks, and dodechannel attacks. The application layer, on the other hand, provides users with intelligent, smart applications and services that meet their individual needs. In this layer, security issues are specific to a variety of applications: they may relate to privacy violations, data theft, etc.

Abdalla et al. [33] discussed the most critical IoT security threats and proposed a new method of classifying them using the AHP approach. Researchers found that DOS/DDOS attacks can be very severe for IoT services, especially if they target smart hospitals, smart vehicles, and security alarm systems. The IoT network can also be vulnerable to malware spreading very rapidly and compromising confidentiality and integrity. As a result of the experiment, different security countermeasures and resources should be available to IoT environments depending on the IoT context and users.

Krishna et al. [34] discussed the comprehensive taxonomy of security and threats in the context of IoT. As well as detailed findings, presumptions, and outcomes of the challenges presented, they provide information on how IoT developers can better address risks and security flaws. In addition to the existing three-layer IoT architecture, five-layer and seven-layer models are presented. The threat and attack scenarios related to these three architectures, as well as the standards and protocols, are discussed. Additionally, a comprehensive discussion is presented of the impact of threats and attacks, and how to identify them, mitigate them, and prevent them.

A recent case study presented by Shaikh et al. [35] demonstrated that Generational Adversarial Networks (GANs) can be effectively used to identify malicious IoT devices inside and outside networks to detect anomalous behavior.

Loukas et al. [36] presented a Smart Home Behavior and Attitude Risk Model (SHBARM), which is, to their knowledge, the first risk assessment model that focuses on the habits and attitudes of homeowners. In addition to their novel methodology for assessing smart home risks, they provide results that can be used to reduce and build awareness of smart home risks through an interconnected approach. In addition to their model, they presented a model for assessing risks within which their model can be applied, along with a small-scale case study on the findings. To evaluate risky WFH-RO networks in the home, this model identifies the human elements that can increase or decrease maximum expected loss. In an organization with remote workers, this model can be used to discover how to decrease risk while in a decentralized state, with the potential to be incorporated into risk management plans. In a time where many workers work from home, this model can help them determine how much risk they are exposed to based on their decisions. To close this gap, they attempt to standardize the way in which risk is accessed within the home, focusing on human factors that can affect this risk.

Yoshioka et al. [37] examined the increasing threats to IoT devices. The authors show that Telnet-based attacks on IoT devices have risen dramatically since 2014. Moreover, at least five DDoS malware families attack IoT devices according to the paper. They also identified at least eight types of botnet architectures, including worm-type botnets, when analyzing the architectures of IoT botnets.

Harbers et al. [38] addressed SPS threats by presenting a framework for addressing technological and non-technological challenges and obstacles. To minimize SPS threats, the framework advocates adopting SPS by design, and identifies four things that prevent this from happening: (1) IoT complexity, (2) lack of awareness, (3) lack of incentives, and (4) lack of monitoring and enforcement. In this contribution, non-technological challenges and measures are addressed at levels of policymaking, governance, and strategy. The proposed framework was designed to help policymakers make decisions that will positively influence others (such as service providers, manufacturers, and consumers) to develop, deploy, and use IoT systems in a secure, privacy-friendly, and safe manner. This study concludes that there is no one-size-fits-all solution to address SPS threats. Instead, multiple measures are needed to achieve an IoT that is SPS-friendly.

Anjum et al. [39] provided a thorough overview of IoT security threats and attacks. The paper includes existing security measures and analysis. This paper analyzed threats to security in the IoT. IoT applications and challenges are discussed, including botnets, denial-of-service attacks, man-in-the-middle attacks, identity theft, ransomware, and remote recording. In addition, the report provided gaps and opportunities as well as future predictions.

Haque et al. [40] provided a detailed discussion of the integration of blockchain technology with IoT. This paper presented a comprehensive analysis of how IoT can be integrated with blockchain after highlighting the foundations of IoT. The purpose of this paper was to examine the possible privacy and protection threats associated with IoT component activity and how this relates to distributed ledger-based blockchains (DL-BCs). The study examined blockchain implementations in several different sectors and categories. IoT-specific challenges and blockchain technology are also discussed in this paper.

Alevizopoulou et al. [41] reviewed existing classification models used to classify vulnerabilities, as well as existing monitoring systems for Twitter. They then describe the data preprocessing phase and present the creation of training, evaluation, and testing datasets for evaluating different classification methods. With thousands of CVEs extracted from the NVD database, they created a large dataset (covering the period 2002–2019). They filtered the CVEs, since they wanted to develop a classifier for detecting IoT vulnerabilities. For the filtering mechanism, they took into account the fact that when a CVE has at least one hardware CPE descriptor, these records will be defined as IoT vulnerabilities, because the CVE is a component of the perception or network layer of an IoT device. In addition to those CVEs related to IoT device vulnerabilities, the remaining CVEs with application-related or software-related CPE descriptors were disregarded. Only 9,941 of the 140,380 CVE records are related to hardware. The ML algorithms were also evaluated to determine which classification model was best suited to their set-up, and a classification model was then used as the basis of the monitoring system.

Schiller et al. [42] explored the characteristics of IoT devices, clearly indicating that traditional security measures cannot be directly applied one-to-one to these devices because of features like usability, limited resources, ubiquity, and short time to market. Security in the IoT domain requires special models and products. To reduce the number of attack vectors adversaries are likely to use to target IoT devices, manufacturers can use the list of IoT security objectives compiled and the threat taxonomy developed to specify, design, and implement secure devices. On the market, there exist several promising technologies and products that can secure the use of IoT technology. To complement these products, institutions and working groups pool their knowledge and efforts to develop guidelines that will allow manufacturers to design secure IoT devices in the first place. Nonetheless, there is room for more security products and services as the markets' growth trajectory

demands. Consequently, the security landscape of IoT is currently on the rise and moving in the right direction.

Borcherding et al. [43] discussed various types of IoT threats, as well as shallow and deep (deep neural networks, deep belief networks, long short-term memory, and bidirectional LSTM)-based intrusion detection systems (IDS) for the IoT environment, including decision trees, random forests, and support vector machines [44].

Abbas et al. [45] proposed a threat-modeling approach to mitigate IoT device threats during the initial design phase. Two significant IoT use-cases, namely smart AVS and smart home, were considered as proofs of concept for the proposed threat-modeling approach. They described the applications of smart connected devices in daily life using different zones. To identify the threats in the system, they adopted STRIDE, a threat-modeling approach that uses all the system's component details. So first, they performed a use-case reconnaissance to collect detailed information on each stakeholder in both use-cases. In a threat-modeling tool, they designed a DFD based on the information they collected. In addition, the DFDs of both use cases were subjected to the STRIDE threat-modeling approach to identify the potential threats in the underlying IoT devices. As a result of their investigation, they determined which of the identified threats could be leveraged to perform phishing attacks. Furthermore, this study provided threat-mitigation techniques that can be used to protect the IoT against phishing attacks in both systems.

Prakash et al. [46] identified some issues related to internet of things security such as data integrity, encryption, and decryption capabilities, privacy issues, common frameworks, automation, and updating. Following that, the study outlined some IoT networks that have been proposed by many researchers. An IoT security model was proposed by the author, which includes six main layers: coding, perception, network, middleware, application, and business. There are a variety of communication protocols, standards, and components that make up an IoT security architecture.

Podder et al. [47] analyzed the current state of security in IoT, and security threats relating to IoT were discussed in their study. They describe the applications of IoT in industrial and medical service scenarios and discuss the security threats associated with IoT healthcare architectures at various layers. In addition, different types of malware are discussed in relation to IoT, including spyware, viruses, worms, keyloggers, and trojan horses. Furthermore, some of the recent malware attacks, such as Mirai, echobot and reaper, are discussed. The paper analyzes existing security issues and open challenges.

Based on the reviewed studies, Table 4 presents the key findings in terms of threats addressed in IoT environments, advantages, and limitations of each study.

Table 4. Summary of the addressed threats.

Author	Publication Year	Addressed Threats	Advantages	Limitations
Choudhary et al. [2]	2021	Discussed threats, vulnerabilities and challenges posed by IoT technology including DDoS attack, Sybil attack, selective forwarding attack, wormhole attack, hello flood attack, sinkhole attack, blue borne attack, attack on HVAC systems, jamming attack, man-in-the-middle attack	Improve security and awareness of IoT devices.	No limitations found.
Patel [15]	2020	Determinized the threats in each layer of IoT architecture.	Well and in a clear way they listed the threats in each layer of IoT and solutions for each of them.	Conclusion is too short and does not include future work.

Table 4. *Cont.*

Author	Publication Year	Addressed Threats	Advantages	Limitations
Dange et al. [16]	2019	Possible attacks targeting IoT systems at the physical and network layers. The evolution of IoT botnet is discussed along with its architecture, lifecycle, and comparison with traditional botnets.	Provided recent major attacks on IoT system along with a listing of the possible attacks on the IoT system at the physical and network layer.	To handle the IoT botnet efficiently, a long-term strategic solution is required.
Hasan Ali et al. [17]	2022	Analyzing intrusions and threats in IoT networks.	Improved genetic algorithm to detect intrusions.	Fast computation, high reliability, and a reduced complexity of computation.
Aamer [18]	2021	Internet of things security from the perspectives of physical security, computer security, and data security.	Focused on the key technologies that must be focused on for Internet of Things security.	Does not provide enough information in how to secure the IoT devices.
Gerodimos et al. [19]	2022	Discussed current security threats in each layer of IoT and examined current challenges.	Analyzed some of the communication protocols designed specifically for the Internet of Things.	Does not provide clear countermeasures or suggest solutions to the threats posed.
Pahlevanzadeh et al. [5]	2021	The security concerns associated with IoT layered architecture, encryption mechanisms, threats, and vulnerabilities.	Security solutions and considerations were presented to improve security services at each IoT layer based on various threats and vulnerabilities.	In addition to intelligence, active defense, and resource conservation capabilities, comprehensive prevention and information security improvements, enhanced technology management, ongoing technology research, and ensuring IoT control capabilities must be considered.
Tsiknas et al. [20]	2021	Threats associated with industrial IoT systems include phishing attacks, ransomware attacks, protocols attacks, supply chain attacks and systems attacks.	An up-to-date, complete, and valid reference framework for identifying and assessing industrial risks that are ever-evolving.	Need to identify special protection techniques against the physical security of IoT devices, in order to prevent third parties from exploiting mechatronic subsystems that are part of this network.
Irfan Ahmad et al. [21]	2020	Examine security threats to IoT devices relating to different IoT layers (e.g., physical, software, network and encryption).	Researchers and manufacturers can use this survey to enhance the security level of future IoT appliances.	Do not provide solutions for each threat in different IT layers.

Table 4. *Cont.*

Author	Publication Year	Addressed Threats	Advantages	Limitations
Ahlawat et al. [22]	2021	Security attacks at various levels including Perception, Transportation, and Application layer. Additionally, several security issues at the application layer, including data theft, service interruption, sniffing, access control, reprogramming, and malicious code injection attacks.	The technical challenges faced by users during real-world implementation were discussed.	Does not provide clear countermeasures or suggest solutions to the threats posed.
Wheelus et al. [23]	2020	Focused on IoT reference models, and the challenges of security and risks in IoT network. Worm, DDOS, SQL injection, spoofing, eavesdropping, jamming, malware, brute force and reverse engineering.	An IoT framework to ensure secure IoT implementation is proposed.	• It is necessary to conduct penetration testing in order to identify attacks that are not discovered organically, as well as to design and evaluate attributes that are designed to identify specific characteristics of each attack type. • Implementation of an operational system.
Ben-Eid [24]	2021	The characteristics and nature of IoT networks, to identify major security threats and challenges.	Providing a good overview of IoT security threats and challenges, and illustrating fog computing and blockchain as two solutions to improve IoT security.	Limited solutions to improve IoT security, need to discuss how to enhance the security in against each layer threats.
Kabulov et al. [25]	2021	Provide a layer-by-layer overview of potential security threats in industrial IoT.	Provide clear discussion about the security threats that may arise in various layers of IoT architecture and suggested mitigation techniques for each of these threats.	Not mentioned the future work of this study.
Haque et al. [26]	2020	IoT security and privacy issues, and IoT cybersecurity situations.	• Good analysis of the recent literature contributions related to IoT security and privacy. • Offered some recommendations on how to secure IoT networks.	Did not provide details on how to implement the proposed solutions.

Table 4. *Cont.*

Author	Publication Year	Addressed Threats	Advantages	Limitations
Dhirani et al. [27]	2021	Cybersecurity challenges for IIoT/I4.0 and the risks to which the technology is vulnerable regardless of cybersecurity standards.	Provide a clear understanding of converged/hybrid cybersecurity standards, best practices, and a roadmap for aligning, mapping, converging, and implementing them.	Future work and how to improve this work was not mentioned.
Svotwa [28]	2020	Privacy and security concerns of IoT devices.	It presents the security posture of the devices and products expected to run on the Internet of Things, and potential solutions that can guarantee their protection and security.	• Limited dissection about the issues and solutions. • Need to propose framework or standard as guidelines to the threats posed.
Kozlov et al. [29]	2021	Examine the security, privacy, and trust implications of IoT infrastructure.	Examined the known and new threats to security, privacy, and trust (SPT) at different levels of architecture.	Does not provide clear countermeasures or suggest solutions to the threats posed.
Cvitić et al. [30]	2016	Risk classification of IoT architecture.	New knowledge about security risks in the IoT environment is provided by the findings presented in the study.	Need to provide the most vulnerable layers of the architecture and the implementation of appropriate measures to protect them.
Cunningham et al. [31]	2022	Threats to privacy and security via IoT devices.	The article revealed how dangerous and vulnerable IoT devices can be in the home, but also provided positive aspects of a smart home, such as improving security.	Does not provide clear countermeasures or suggest solutions to the giving threats.
Ikrissi et al. [32]	2021	Some threats related to the Internet of Things in the smart environment.	• Provide detailed expansion of the different security issues were evaluated in the layers of the IoT architectural framework. • In each layer of IoT architecture, some countermeasures are presented for dealing with security attacks.	No limitations found.

Table 4. *Cont.*

Author	Publication Year	Addressed Threats	Advantages	Limitations
Abdalla et al. [33]	2021	Critical IoT security threats include physical threats, network threats and software threats.	Proposed new classification of IoT threats based on the AHP approach.	Need to develop a more suitable framework for IoT security.
Krishna et al. [34]	2021	Taxonomy of security and threats in the context of IoT.	Provide good description of the threat and attack scenarios related to the three-layer IoT architectures, as well as the standards and protocols.	Currently, there are few generic validated architectures for IoT, since most of them are either domain-specific or application-specific. This means that the security enhancement methodology may not be appropriate for the most generic architecture used in the study.
Shaikh et al. [35]	2019	Identify external as well as internal threats to IoT devices in given network.	The proposed GAN-based models can effectively detect previously unknown IoT threats and capture the latent distributions of both benign and malicious samples.	Need to improve feature selection methodology to increase the accuracy of the used algorithm.
Loukas et al. [36]	2020	Threats associated with IoT and human vulnerability.	Provide a smart home risk model which considers the human factor towards risk. To validate their solution, they used realistic use cases and risk assessments.	Provide users with guidance on selecting the right security measures for their homes.
Yoshioka et al. [37]	2016	Analyzed the increasing threats against IoT devices and Telnet-based attacks on IoT devices.	• Uncovered five malware families with worm-like spreading behaviors, all of which are actively used for DDoS attacks against IoT devices. • Proposed IoTBOX, a multi-architecture malware sandbox that can be used as a component of ITPOT or independently for the analysis of captured binaries as part of IoTPOT.	It is necessary to extend the sandbox to support even more IoT architectures and environments.

Table 4. *Cont.*

Author	Publication Year	Addressed Threats	Advantages	Limitations
Harbers et al. [38]	2018	Threats to security, privacy, and safety (SPS) in IoT.	• Assist policymakers in adopting policies and strategies that encourage others to develop, deploy, and use IoT devices, applications, and services securely and safely. • As opposed to other works on the topic, this work lays out a conceptual framework that captures fundamental challenges to a successful deployment of literature-proposed solutions and offers some solutions to these fundamental challenges.	The conceptual framework needs to be improved and specified.
Anjum et al. [39]	2021	Examine the many security and privacy concerns associated with the IoT. Botnets, denial of device, man-in-the-middle, social engineering, advanced persistent threats, ransomware and remote recording, remote recording.	A good analysis of the threats and security issues facing IoT, as well as an understanding of the level of problems.	Does not provide enough details about the recommended solutions, which include blockchain.
Haque et al. [40]	2021	Issue of IoT data protection and privacy	IoT-specific challenges and contributions of Blockchain technology were clearly discussed.	Simulation-based performance measurements are not available to demonstrate the scalability and reliability of blockchain technologies.
Alevizopoulou et al. [41]	2020	Investigated real-time threat detection from the Twitter stream using social media monitoring.	Using the proposed system, users will be able to identify recent/trending vulnerabilities and exploits on IoT systems.	Adding a ranking component to the monitoring system to take into account the reliability, popularity, and freshness of users and tweets.
Schiller et al. [42]	2022	IoT security challenges and threat taxonomy.	An excellent overview of IoT security that emphasizes the importance of secure IoT product and application development.	No limitations found.

Table 4. *Cont.*

Author	Publication Year	Addressed Threats	Advantages	Limitations
Borcherding [43]	2022	Various types of IoT threats were discussed, as well as shallow (such as decision trees, random forests, and support vector machines) and deep (such as deep neural networks and deep belief networks, as well as long short-term memory and bidirectional LSTM)-based intrusion detection systems (IDS) in the IoT environment.	Contributes to the development of transparent machine learning-based intrusion detection approaches by developing a better understanding of how a network intrusion detection system works.	Further investigation is needed for the taxonomy for ML-based ICS NIDS, the branch differentiating the model generation process.
Abbas et al. [45]	2021	Phishing attack threats in IoT identification and mitigation.	• Proposed threat-modeling approach that helps identify and mitigate potential threats in IoT devices during the initial design phase. • Introduced threat-mitigation techniques to secure IoT against threats that can trigger phishing attacks.	• Additional use cases should be included. • Validate the proposed mitigation techniques using the proposed threat mitigation remedies.
Prakash et al. [46]	2021	Issues related to internet of things security, such as data integrity, encryption, and decryption capabilities, privacy issues, common frameworks, automation, and updating.	• Focused on significant security issues relating to IoT. • The proposed model can be used to reduce the power consumption and time consumption of IoT systems by choosing the appropriate security methods for IoT layers. • As mentioned, the proposed model is capable of handling various threads and attacks to protect sensitive data and private information.	Need to implement the proposed model and measure its performance.

Table 4. *Cont.*

Author	Publication Year	Addressed Threats	Advantages	Limitations
Podder et al. [47]	2021	Different types of malware in relation to IoT, including spyware, viruses, worms, keyloggers, and Trojan horses. Furthermore, some of the recent malware attacks such as Mirai, echobot and reaper.	• Discussed the relationship between IoT and cloud computing environments, as well as different security requirements for IoT communication environments. • Various machine learning techniques are evaluated for classification and Android malware detection. • This paper can assist in developing more secure IoT networks and providing users with a secure online experience.	No limitations found.

Every IoT architecture layer has its own set of security and infrastructure challenges that should be considered during the IoT creation and development process. As a result of analyzing the studies, Table 5 summarizes and classifies IoT threats based on three layers of its architecture, which are physical layer, network layer and application layer.

Table 5. Classify threats on each of three layers IoT.

Author	Physical Layer Threats	Network Layer Threats	Application Layer Threats
Patel et al. [15]	Data manipulation, side channel attacks, boot attacks, and node capturing.	MITM attack, Sybil attack, and DDoS attack.	Data leakage, DoS attacks, and malicious code injection
Gerodimos et al. [19]	Eavesdropping, node capture, malicious fake node, replay attack and timing attack.	Denial of service (DoS) attack, IP fragmentation attacks, man-in-the-middle attacks, storage attacks and exploit attack.	Cross-site scripting, malicious code attack, Cinderella attacks and big data handling.
Tsiknas et al. [20]	Jamming DoS attacks Collision/exhaustion/unfairness attacks data transit attacks	Routing and DoS attacks Data transit attacks threats to neighbor discovery protocol (IPv4/IPv6)	-
Pahlevanzadeh et al. [5]	Timing attack, node capture, fake node, cloning of things, malicious substitutions of things, security parameters extraction and privacy threats.	Blackhole or sinkhole attack, selective transformation, wormhole attack, and Sybil attack.	SQL injection, XSS Cross-site scripting attacks, enumeration (CWE / SANS), common weakness, phishing attack, sniffing attack and buffer overflow.

Table 5. *Cont.*

Author	Physical Layer Threats	Network Layer Threats	Application Layer Threats
Ahlawat et al. [22]	-	-	Data theft, service interruption, sniffing, access control, reprogram, and malicious code injection attack.
Wheelus et al. [23]	-	Worm, DDOS, SQL injection, spoofing, eavesdropping, jamming, malware, brute force and reverse engineering.	-
Ben-Eid [24]	Adding/replacing malicious nodes, harmful code attack, boot process attack and draining the battery.	Phishing, unauthorized access, DDoS/DoS attack, routing attack, person-in- the-middle, SQL injection attack, signature wrapping attack, and cloud malware injection, flooding the cloud.	Data theft, access control attack, denial of service (DoS) attack, code injection attack, sniffing attack, reprogramming attack.
Yarasho et al. [25]	Tampering and denial of service and sensors as security treats.	Denial of service attacks and eavesdropping.	-
Ikrissi et al. [32]	Sleep deprivation attack. Capturing and fake node injection. Malicious code injection attack. Eavesdropping attack.	DDOS attack. Routing attack. Sniffing attack. Traffic analysis attacks.	Reprogram attack. Sniffing attack. Data thefts. Service interruption attacks.
Bdalla et al. [33]	Node tempering, RF interference, node jamming, physical damage, side-channel attack, social engineering, Sleep deprivation attack and malicious code attacks injection on the node.	Traffic analysis attacks, man-in-the-middle attack, routing information attacks and sybil attack.	Malware, phishing attacks, denial of service and disrupted denial of service, and cryptanalysis attacks.
Shaikh et al. [34]	Eavesdropping, malicious data injection, sybil attack, disclosure of critical information, side-channel attacks, exhaustion attack and node cloning.	Hello flood, sinkhole, blackhole, traffic analysis, wormhole, selective forwarding and RPL exploit.	Software modification, malicious code, data tampering, cross-site scrip, identity thefts, virus attack, spyware attack, code injection, intersection, and brute force attack.

5.2. Countermeasures and Mitigation Techniques for the for IoT Threats

Choudhary et al. [2] discussed several IoT security tools in order to assist organizations in limiting the vulnerabilities associated with IoT, thus protecting devices and networks from various types of cyberattacks. The purpose of the paper was to improve the security of IoT devices by spreading awareness. They also found that, given the wide scope of IoT, there is no single solution that defines security for IoT. The authors discovered that there is no single security solution that meets the needs of IoT due to its wide scope. In addition, they suggested that designers of IoT devices determine what security requirements apply to their products, considering the design objectives, deployment environments, and regulatory requirements. Keeping such devices secure for longer periods of time also requires timely updates and security patches. IoT devices can contribute to the development of society if they are developed responsibly.

Patel [15] suggested some countermeasures in each layer of the IoT architecture. Sensing Layer: authenticity and data privacy. Network Layer: authenticity, routing security and data privacy. Middleware Layer: confidentiality and data storage. Application Layer: authenticity, intrusion detection and data security. The researcher discovered that to ensure the security and privacy of IoT devices, they should comply with the CIA triad, comprising confidentiality, integrity, and availability. Each of them is critical to the security of the devices.

Dange [16] suggested that, in order to deal with IoT botnets, a different mechanism was required. Prevention represents the best long-term solution, and the network-based approach is the most efficient method. It would be helpful to develop a new hybrid approach that uses network-based botnet detection to identify the IoT botnet specifically so as to protect the IoT network from IoT botnet attacks.

Hasan Ali et al. [17] presented an intrusion detection system based on the DDoS Evaluation Dataset. Data collected are divided into training, testing, and validation sets. As a result, attack detection accuracy is improved by training data according to multiple layers of long short-term networks. Based on the features extracted from the tested data and the training data, a sparse matrix is constructed. Thus, the overall accuracy of attack detection is improved, while the number of false alarms decreases. MATLAB's implementation of the system achieved 98.98% detection rate, 99.29% accuracy, and 90.26% performance ratio, with a minimum computation complexity of 90.26%.

Aamer [18] presented a technological solution for improving IoT security, including key security technologies for the perception layer, network-layer technological solutions, and application-layer technological solutions. Gerodimos [19] suggested that governments and engineers should collaborate to overcome the challenges of applying Internet of thing networks to traditional networks to make the phrase credible. Pahlevanzadeh et al. [5] described standardized global security mechanisms, effective and efficient lightweight encryption techniques, and consideration of the future of IoT security. Tsiknas et al. [20] provided the latest countermeasures for its protection, through a benchmarking and critical analysis framework. Among IIoT surveys, this one is unique, in that it provides a complete, up-to-date, and validated reference framework for identifying and assessing the risk associated with an ever-evolving industrial environment. Irfan Ahmad et al. [21] discussed four ways of securing IoT applications and their environment, including (1) edge computing, (2) fog computing, (3) blockchain, and (4) machine learning. Ahlawat et al. [22] provided various solutions like blockchain solutions, but mentioned that new protocols and algorithms could provide greater security and privacy. In addition, they reviewed various security models proposed by various authors, along with comparisons of the techniques used. Various techniques and algorithms can be used to mitigate IoT security attacks in order to increase its adaptability by users. Wheelus et al. [23] proposed a data-driven framework for implementing IoT systems and generalized principles for implementing, deploying, and managing IoT services. The researchers analyzed network traffic collected from IoT-based companies providing smartphone-enabled secure access solutions for commercial buildings, gated communities, parking garages, and storage facilities, as well as other related secure access solutions. Their analysis of raw packet data totaled 100 gigabytes. Ben-Eid [24] described several simple steps users can take to increase the security of the IoT system, as well as fog computing and blockchain. Kabulov et al. [25] mentioned that, in order to plan, implement, place, and process a secure and safe IoT system, the following steps must be taken: first, the right technologies, architectures, and tools must be selected. Second, the setting up, programming, and and verification of projects. The third step is to provide deployment and commissioning services. Operation and maintenance are the final steps.

Haque et al. [26] provided recommendations of solutions by analyzing the state of the art of current cybersecurity situations of the IoT, including anti-jamming mechanisms, safe physical layer communication, detection of Sybil attacks and spoofing threats, inadequate physical protection, sleep deprivation attacks, high-level privacy/security solutions, and

blockchain. Dhirani et al. [27] proposed a roadmap for implementing a unified standard framework for mitigating cyber threats and standardization challenges because of the IT/OT convergence gap. Through the study of cybersecurity standards and providing insights for designing/converging IT/OT security architectures, this research contributes to advanced knowledge in IIoT. Moreover, they emphasize the importance of implementing interoperable and hybrid standards for connecting multiple complex interfaces, as they ensure strategic alignment, and mitigate IT/OT cyber risks in IIoT/I4.0 by bridging the IT/OT divide. Svotwa [28] provided some recommendations on possible solutions or countermeasures, such as better understanding the potential effects of the IoT movement, developing policies for the handling of various types of data, and establishing policy implementation mechanisms. Developers should be trained on how to address security problems by integrating IoT security features into products that include firewalls and intrusion prevention systems and allowing users to access the IoT security features built into their devices. In addition, companies must do everything in their power to simplify connected systems, improve security and standardize apps, and ensure users' privacy and protection on any computer, at anytime, anywhere. Additionally, an appropriate framework for designing privacy is one that gives users control over their own data, as it is right now. As well as forcing users to change their passwords after a specified period, developers can select a password that meets the strongest password requirements.

Ikrissi et al. [32] presented countermeasures for IoT attacks that included lightweight cryptography, blockchains, machine learning, and biometrics. When designing and implementing new smart systems, it is important to take security and privacy threats into account. Abdalla et al. [33] proposed a new method of classifying them using the AHP approach. The new model is based on stakes pertaining to particular types of users. To gain user trust, IoT service providers should focus on both user security and user trust. For IoT systems to achieve this, precise security measures combine expert knowledge with the needs of regular users, thereby reducing cost and complexity. An AHP approach was applied in this study to propose a security classification for IoT threats. They divided 80 users into three classes (G1, G2, and G3): The first class consisted of 50 college students using IoT devices and possessing basic knowledge of security attributes including confidentiality, availability, and integrity. The second class G2 was comprised of 17 PhD holders who were working with IoT devices but did not have experience with information security. There were 13 PhD holders in class G3, who were established in the fields of cybersecurity, wireless networks, and IoT, and had published a wide range of papers on these areas. To start the survey, the participants were thoroughly explained the criteria, subcriteria, and IoT threats. There were two questionnaires completed to gather the data needed. To calculate the weight using the AHP algorithm, they collected data that represented the relationship between the sub-criteria. This was performed by G3 to ensure the weight calculations were as accurate as possible. A scale of 1–9 was used, with 1 representing "Extremely Important" and 9 representing "Extremely Important". Secondly, the questionnaire tracked the relationship between the threat and the element of security, which affects system trust. A total of 80 users filled out the questionnaire. The risk value was measured as being between 0 and 5, with 0 being no impact and 5 being high impact.

Krishna et al. [34] discussed how to enhance the security features in IoT devices using blockchain technology, fog computing, edge computing, and machine learning and state-of-the-art solutions. Shaikh et al. [35] presented two network-based solutions for detecting anomalies that make use of recently described models of generational adversarial networks (GANs) that can effectively identify malicious IoT devices inside and outside of networks. In GANs, a latent representation of the data is effectively presented, and it is possible to reconstruct a distribution from this representation. As part of their experimental setup, the first methodology trained GAN models on benign traffic generated by three widely deployed commercial IoT devices. Malware such as Mirai and Bashlite were then used to attack these devices, alongside the use of other exploitation techniques, using the Kali Linux operating system. To test the GAN model's effectiveness, both benign and

anomalous samples were used. It is important to note that these data were augmented with network traffic for 28 IoT devices that were made public. Moreover, they tested a second methodology that used GAN models to discover the distributions of anomalous samples in darknets or network telescopes. The algorithm was tested both with benign and malicious samples. Additionally, they evaluated a model trained on malicious samples using passive measurements (i.e., darknet data), as well as simulating real-world attack scenarios by including Nessus scanning and Mirai attack vectors. The results of the study showed that GAN-based models were able to effectively detect previously unknown IoT threats and capture the latent distributions of both benign and malicious samples. Furthermore, using feature matching loss in ALI GAN-based frameworks, trained on benign samples, their results demonstrated that the framework with the shortest inference time was the most effective. Models like this can be used in conjunction with IDS/IPS systems to aid in the proactive detection of unwanted activities directed towards or originating from IoT devices.

Loukas et al. [36] proposed that a risk model for the smart home must factor in a user's behavior and attitude towards IoT devices. It also considered human factors in the assessment of IoT risks. To discuss the importance of human behavior and attitudes within the home, they proposed the smart home behavior and attitude risk model (SH-BARM) to provide a solution that will assist smart home inhabitants and organizations. Yoshioka et al. [37] developed a sandbox to attract and analyze Telnet-based attacks against a variety of IoT devices running different CPU architectures such as ARM, MIPS, and PPC. This study is notable for its observations that telnet-based attacks have increased, as have IoT devices. To analyze the scope and variety of the attacks, the authors proposed a novel honeypot called IoTPOT, which simulates IoT devices and captures Telnet intrusions. The researchers then analyzed the threats further and proposed the IoTBOX, which would allow them to run the captured malware on eight different CPU architectures. Harbers et al. [38] provided a conceptual framework that models and captures the fundamental challenges that impede the deployment of solutions proposed in the literature, and it provides some suggestions for addressing these fundamental challenges. Anjum et al. [39] mentioned that it is possible to increase security and reliability by implementing blockchain technology. Haque et al. [40] discussed how blockchain could resolve the problems associated with IoT systems. In addition, the latest developments, along with the integration of blockchain with IoT, are discussed. It is then shown how blockchain can be used as a service for various IoT applications as a blockchain technology for the IoT. Alevizopoulou et al. [41] created a social media monitoring system specifically for IoT devices that identifies recent/trending vulnerabilities and exploits in IoT devices. In the proposed monitoring system, data are acquired in two phases (I) and a trained classification algorithm is used to classify the tweets collected. The researchers used binary classification in this study in order to categorize tweets into two distinct groups, namely related and unrelated to IoT vulnerabilities. To determine which traditional machine learning model would be most effective in their case, they experimented with logistic regression, multinomial naive bayes, decision tree classifiers, k-nearest neighbors classifiers, support vector machines, and random forest classifiers; the best-performing algorithm was then implemented in the monitoring system as the classification model. Furthermore, they released a new dataset consisting of security-related tweets annotated in terms of whether they contain IoT CTI; this dataset is expected to facilitate research in the area of security-oriented social media content classification as well as support reproducibility. In addition, they publicly release all annotated datasets created during this process in order to support research on the field and provide reproducibility of results.

Schiller et al. [42] mentioned that, although many IoT devices and threats have been increasing exponentially these days, they need to increase their speed of development. Products well designed to determine the security requirements in detail will soon be developed by manufacturers. Resource-constrained IoT devices require more affordable security measures. Consumers should take responsibility for their privacy and security, along with regulations, guidelines, and governments who pay enough attention to this

market. Manufacturers, consumers, and governments all have a role to play in leveraging the power and innovation that IoT offers, but they also have a role to play in making the world a safer place. Borcherding et al. [43] proposed an optimal attack detection model for IoT systems using a comprehensive workflow. This research has used three different datasets in addition to the most frequently used datasets (NSL-KDD and DS2OS), including IoTDevNet, IoTID20, and IoT Botnet. The principal target of the framework is to construct an IoT-based system that distinguishes its vulnerability, provides a secure firewall against all cyberattacks, and recovers from them. Therefore, this paper proposed a learning-based methodology that can be used to recognize anomalies and ensure the security of infrastructures. The errand was performed by deploying three shallow ML classifiers and five DL models. The paper also performs comparisons between simple models like DT and RF and complex networks like deep belief networks (DBN), long short-term memory (LSTM), bidirectional long short-term memory (Bi-LSTM) for anomaly detection. The researchers found that deep learning IDS outperformed shallow learning IDS in detecting IoT attacks. Kim-Hung Le et al. [44] introduced IMIDS, a powerful intrusion detection system that uses a CNN. The purpose of this study was to identify various cyberattacks accurately using an IDS and an artificial method for generating useful training data. A key component of IMIDS is the feature extractor, which extracts features from raw network packets and transforms them into network features, while the attack detection model identifies malicious behavior. Interestingly, IMIDS was able to distinguish between normal and abnormal activities, as well as to identify whether they were cyber-attacks. As part of enhancing IMIDS's detection performance, the researchers proposed a conditionally generated adversarial network to generate attack data. It consists of conditional generators, which can learn conditional distributions from samples in a dataset. During the experiments, IMIDS detected nine cyber-attacks, on average, with an F-measure of 97.22 percent. Additionally, IMIDS' detection performance was significantly improved after being trained with their attack data generator's training data. Detections of worms and analysis attacks, for example, improved from 35.58% to 70.94% and 49.12% to 83.64%, respectively. Based on these results, IMIDS was found to be a viable IDS for IoT systems. Abbas et al. [45] proposed that a threat-modeling approach could be useful for security analysts, developers, and IoT device vendors to identify and design for IoT devices' vulnerabilities during their initial design phase. Threat modeling is only able to identify threats during the design phase of a system. The researchers proposed threat-mitigation remedies to protect IoT systems from phishing attacks based on the identified threats.

Prakash et al. [46] suggested a security model based on the security architecture of IoT might be able to offer protection from unwanted threats and attacks and un-authentication, while protecting private information. There were three stages of development involved in the proposed model, including layers of security, security protocols, and database servers. They identified protocols suitable for different layers of the proposed security architecture, including the IEEE 802.11 protocol at the perception layer, the 6LowPAN network protocol, and the SMQTT application protocol. The proposed model uses algorithms such as the hash algorithm and end-to-end authentication in order to guarantee IoT security layers such as access control, privacy, confidentiality, integrity, availability, and authorization. As a follow-up to step one, the security protocols and security control mechanisms for the different layers of IoT security architecture are described in step two. This model also includes database servers that store data and parameters of security concern for all security layers, client profiles, security component errors, log records of the IoT framework, and access control records. The process consists of collecting the data from physical media like sensors and converting them into digital signals for further processing. Users can also give their instructions via the user interface to control the system processes. The encryption of digital signals is achieved using appropriate key-generating algorithms. Data from encrypted signals is aggregated with that from users. Through the interface of an IoT gateway, data are transferred to a database via the web server, where it is decrypted and displayed to the user using the same encryption key. Additionally, the decrypted data

are stored in the database for future use. As a result of using this model, IoT systems can be designed to perform better, saving both energy and time by selecting the appropriate security methods for the IoT layer. Podder et al. [47] used machine learning algorithms to defend against IoT threat. Researchers have found that the k-nearest neighbor (kNN) machine learning algorithm can detect malware with excellent accuracy. Various tools have also been reviewed to perform ransomware detection, classification, and analysis.

In Table 6, we summarize and present the key findings of studies regarding countermeasures for IoT threats.

Table 6. Summary of the countermeasures for IoT threats.

Author	Methodology	Countermeasures
Umamaheswari et al. [2]	Qualitative	Provide number of countermeasures corresponding to each vulnerability in IoT. They also suggested that designers of IoT devices determine what security requirements apply to their products considering the design objectives, deployment environments, and regulatory requirements.
Patel [15]	Qualitative	They suggest some countermeasure in each layer of the IoT architecture. Sensing Layer: authenticity and data privacy. Network Layer: authenticity, routing security and data privacy. Middleware Layer: confidentiality and data storage. Application Layer: authenticity, intrusion detection and data security.
Dange et al. [16]	Qualitative	It would be helpful to develop a new hybrid approach that uses network-based botnet detection to identify the IoT botnet specifically so as to protect the IoT network from IoT botnet attacks.
Hasan Ali et al. [17]	Quantitative	Employ the IGA-BP network as a countermeasure to internet security challenges in the age of big data, using an autoencoder network model, as well as an improved genetic algorithm to detect cyber intrusions.
Gerodimos et al. [19]	Qualitative	Engineers and governments should join forces and take on the challenges to make IoT networks mainstream and make the term Internet of Things a real possibility.
Pahlevanzadeh et al. [5]	Qualitative	Each IoT security approach requires a new design of security classification that to provide more accurate and easier classification of IoT security threats.
Tsiknas et al. [20]	Qualitative	Provide latest countermeasures for the protection of the infrastructure in question, through a critical and benchmarking framework. Packets' rerouting to alternative routes, FHSS techniques, data encryption algorithms, ingress filtering and IDS solutions, compressed transport protocols (for instance DTL), use of IPsec, SEND protocols, message authentication, optimizations in transport layer apply network filtering and secure MQTT, ABE algorithm.
Ben-Eid [24]	Qualitative	Described several simple steps users can take to increase the security of the IoT system, include: The default password of the device should be changed. Making sure your password is strong and changing it regularly. Multifactor authentication should be implemented. Firmware and software must be kept up to date. Disable any device functions that are unused. Carefully read security and privacy policies and do not ignore any suspicious messages.

Table 6. *Cont.*

Author	Methodology	Countermeasures
Kabulov et al. [25]	Qualitative	It is imperative to plan, implement, place, and process an IoT system that is secure and safe via the following steps:(1) The selection of technologies, architectures, and tools. (2) Project setup, programming, and verification, (3) Providing deployment and commissioning service. (4) Operating and maintaining.
Svotwa [28]	Qualitative	IoT security concerns can be addressed by establishing standards that describe which level of security and the conditions that must be met can be considered acceptable, by defining a framework for identifying defects, and by training developers on how to consider security during development.

Table 7 summarizes the mitigation techniques suggested in the reviewed studies to mitigate threats in IoT environments.

Table 7. Summary of the suggested mitigation for IoT threats.

Author	Methodology	Suggested Mitigation
Aamer [18]	Qualitative	Provided some technological solutions to improve the security of the Internet of Things
Ahmad et al. [21]	Qualitative	They discussed four methods of securing IoT applications and their environment, including: (1) Edge computing, (2) Fog computing, (3) Blockchain, and (4) Machine learning.
Ahlawat et al. [22]	Qualitative	Provided various solutions like blockchain and suggested that new protocols and algorithms can provide greater security and privacy.
Wheelus et al. [23]	Quantitative	Proposed an IoT framework for implementing secure IoT systems.
Ben-Eid [24]	Qualitative	Fog computing and Blockchain.
Haque et al. [26]	Qualitative	Proposed anti-jamming mechanisms, safe physical layer communication, detecting Sybil attacks and Spoofing threats, inadequate physical protection, sleep deprivation attacks, high-level privacy/security solutions, and blockchain.
Dhirani et al. [27]	Qualitative	Proposed a roadmap for implementing a unified standard framework for mitigating cyber threats and standardization challenges because of the IT/OT convergence gap.
Cvitić et al. [30]	Mixed	Proposed a security risk classification for IoT concepts based on their deployment types.
Ikrissi et al. [32]	Qualitative	Lightweight cryptography, blockchains, machine learning, and biometrics.
Abdalla et al. [33]	Quantitative	Proposed a new classification based on the AHP approach.
Krishna et al. [34]	Qualitative	Blockchain technology, fog computing, edge computing, and machine learning.
Shaikh et al. [35]	Qualitative	Proposed two generative adversarial network (GAN)-based models to detect threats to IoT devices from within and outside the network of interest.

Table 7. *Cont.*

Author	Methodology	Suggested Mitigation
Loukas et al. [36]	Qualitative	Proposed the Smart Home Behavior and Attitude Risk Model (SH-BARM).
Yoshioka et al. [37]	Quantitative	Proposed a novel honeypot called IoTPOT, which simulates IoT devices and captures Telnet intrusions.
Harbers et al. [38]	Qualitative	Proposed a conceptual framework for addressing IoT SPS threats
Anjum et al. [39]	Qualitative	Blockchain technology.
Haque et al. [40]	Qualitative	Proposed blockchain technology.
Alevizopoulou et al. [41]	Quantitative	Developed a novel social media monitoring system tailored specifically to the IoT domain that identifies recent/trending vulnerabilities and exploits in IoT devices.
Schiller et al. [42]	Qualitative	The threat taxonomy was developed.
Borcherding et al. [43]	Quantitative	Presented an analytical approach to detecting intrusions in the IoT environment.
Kim-Hung Le et al. [44]	Quantitative	IMIDS was presented, a system for protecting IoT devices and addressing the lack of training data shortage, as well as an attack data generator that employs a conditional generative adversarial network.
Abbas et al. [45]	Qualitative	A threat-modeling approach was proposed to identify and mitigate potential threats in IoT devices during the initial design phase.
Prakash et al. [46]	Qualitative	Proposed a security model to protect the IoT network from threats and attacks.
Podder et al. [47]	Qualitative	k-nearest neighbor (kNN) machine learning algorithm that can detect malware with excellent accuracy.

6. Results and Discussion

In the previous section, the results showed common threats at each layer of the three-layer IoT architecture. The most common threats in the physical layer, as shown in Figure 6, are node capture, eavesdropping, side-channel attack, boot attack, and timing attacks, where node capture poses the greatest threat to the physical layer. A key component of these attacks is the control of key nodes, such as gates [48–55]. In this way, all data, including matching keys for data and group communication keys, are disclosed, posing a threat to the entire network.

In the network layer, the main threats are DoS/DDOS attack, man-in-the-middle attack, traffic analysis attack, Sybil attack, and routing attack, as shown in Figure 7. In addition, the DDOS/DoS attack poses a major threat to the network layer according to the analyzed studies [56–62]. This attack aims to disrupt server availability through a flood of impersonated IoT requests on the communications channel [63–69]. Due to the complexity and heterogeneity of IoT networks, the network layer is vulnerable to them. It is common for IoT devices used in IoT applications to be poorly configured, making them easy targets for DoS and DDoS attacks in the target environment [70–74].

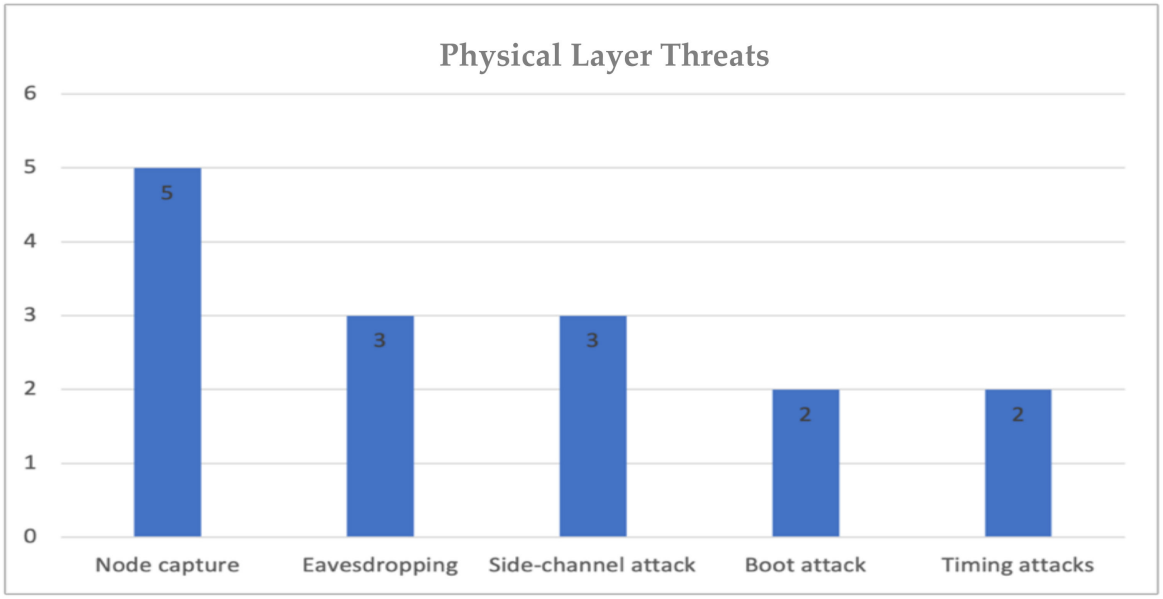

Figure 6. Common threats in the IoT physical layer.

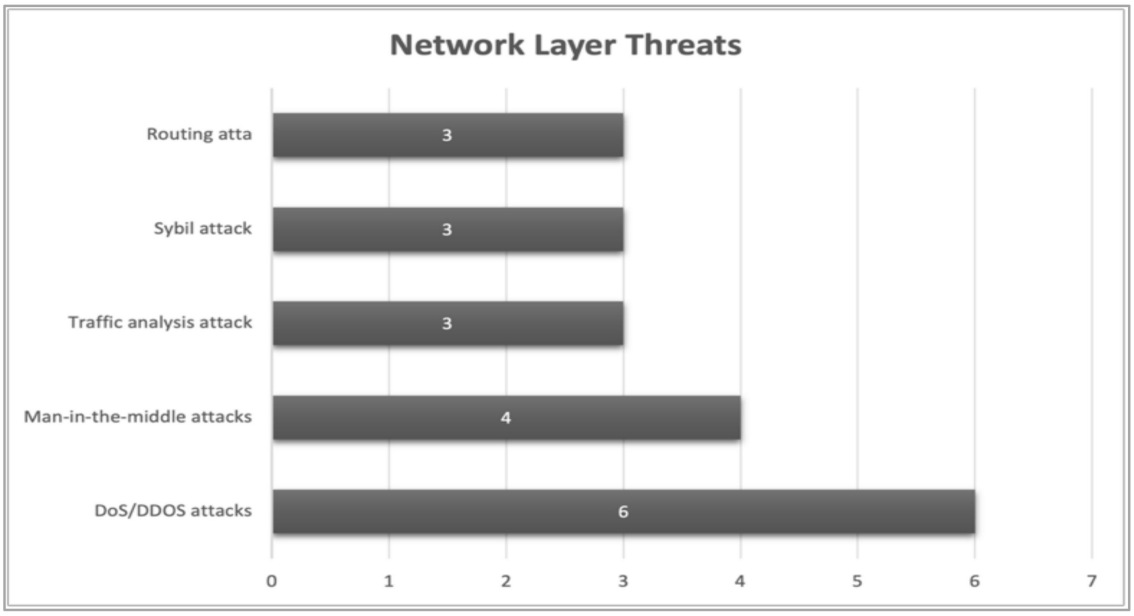

Figure 7. Common threats in the network layer.

In the application layer, the common threats are malicious code injection, cross-site scripting attack (XSS), data theft, DoS and DDOS attack, sniffing attack, and reprogramming attack, as shown in Figure 8, where the malicious code injection attacks pose a major threat to the application layer according to the analyzed studies. The easiest or simplest way for an attacker to break into a device or network is usually the easiest one. The simplest and easiest methods are often used by attackers to gain access to a network or device. The device becomes the first point of entry for an attacker if it is vulnerable to spiteful scripts and misdirection caused by inadequate code testing [75,76].

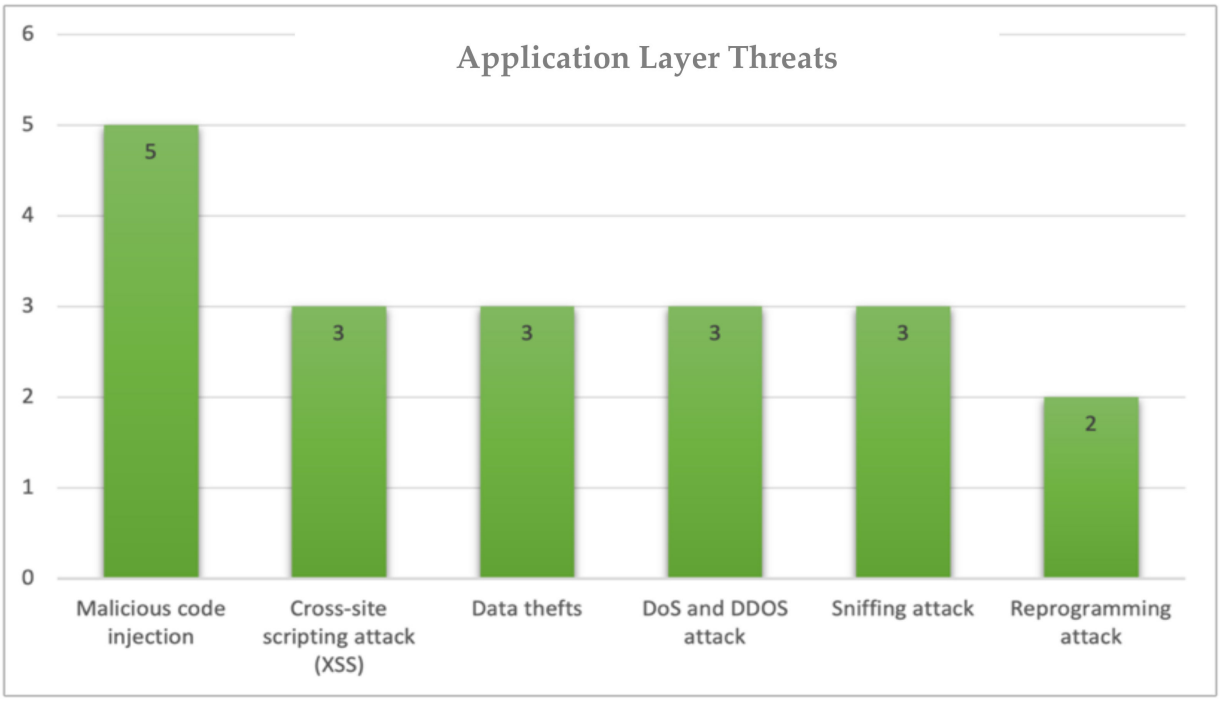

Figure 8. Common threats in the application layer.

Based on three layers of IoT architecture, Figure 9 illustrates the most common threats. The layers are the physical layer, the network layer, and the application layer.

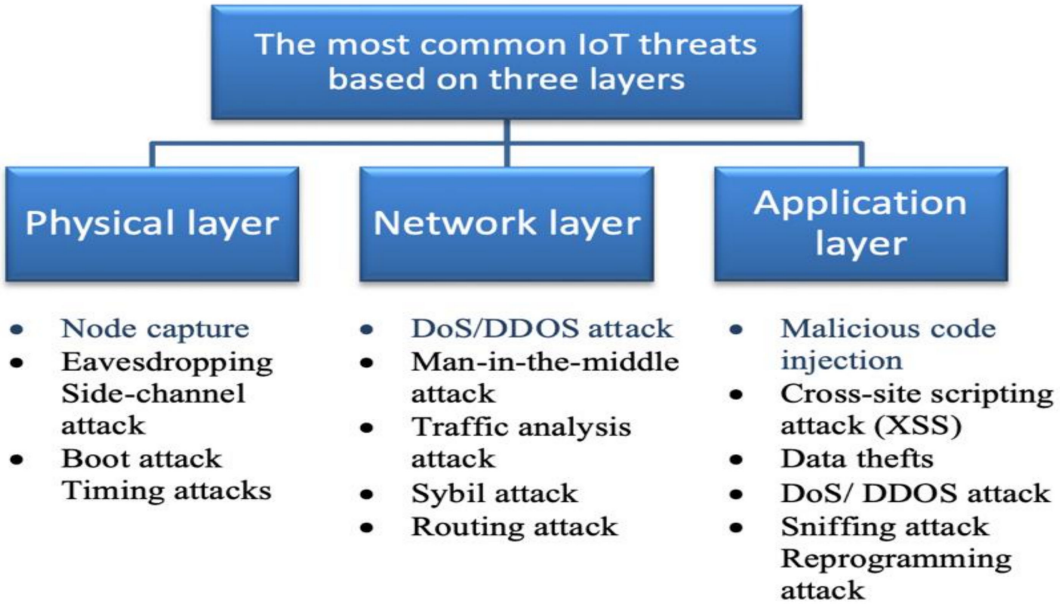

Figure 9. Summary of the most common threats on IoT based on three layers architecture.

The common technologies used to address IoT threats according to analyzed studies are: blockchain, machine learning, fog computing, and edge computing. As shown in Figure 10, the most frequently suggested technology is blockchain.

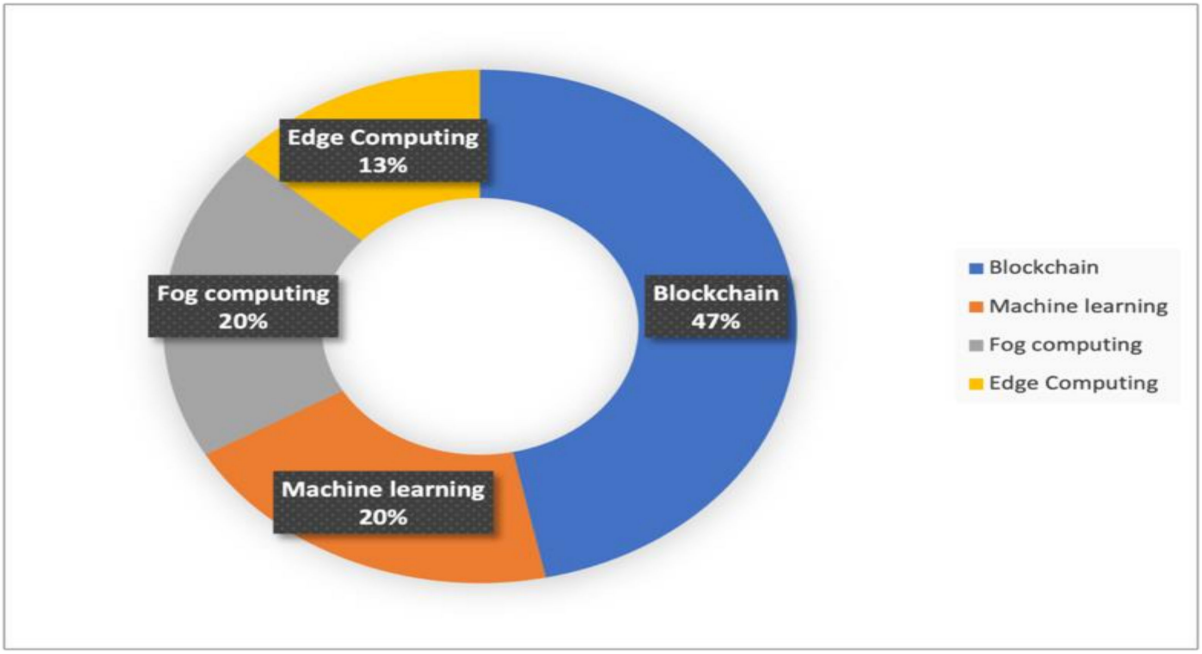

Figure 10. Common technologies used as a countermeasure for IoT threats.

7. Recommendations for Future Research Directions

In recent years, the security of IoT devices has attracted the attention of researchers in both industry and academia. In our paper, we offered a comprehensive review of the threats that target IoT networks. These threats can be classified into three categories based on IoT layers namely: node capture threat, DDoS attack and code injection.

In this study, we summarize the following future directions:

First, we recommend more future research investigation on the use of Artificial Intelligence techniques to enhance the IoT security and privacy.

Second, despite the increasing interest in cybersecurity of IoT, little research has been performed on the security of IoT application-layer protocols. There are several challenges and security issues in IoT application-layer protocols still to be addressed. We recommend more future research investigating the security issues in IoT application-layer protocols.

Third, our findings also identify the different types of cybersecurity threats in IoT, such as DDoS, man-in-the-middle attack, Sybil attack, routing attack, and others. Other researchers could explore other types of threats in IoT layers and identify the weaknesses in each layer.

Fourth, one of the main concerns in IoT is providing highly efficient detection methods that have a high probability of detection with low probabilities of false-alarm and miss-detection. The current detection techniques have many limitations. One of these issues is that most of the developed methods need modification to the IoT network infrastructure and their security protocols. Additionally, the majority of these techniques do not support high detection rates while having high false-alarm rates. Furthermore, the detection process is not in real time, which decreases the efficiency of these techniques. Therefore, we need more research investigating the provision of detection techniques in order to address these challenges.

8. Conclusions

IoT devices are becoming increasingly common throughout the world, which makes them a target for many hackers, who are trying to trespass on people's privacy by collecting sensitive information and using it in suspicious ways. Therefore, this study conducted a systematic literature review of 35 existing research publications on cybersecurity threats associated with the IoT environment. In this paper, we present a comparison of 35 publi-

cations based on the threats, countermeasures, and mitigation techniques. Additionally, we classified IoT threats based on a three-layer IoT architecture. As well as analyzing the popular application-layer protocols employed in IoT environments and their security risks and challenges. According to our findings, node capture is the most significant threat to the physical layer or perception layer, and DoS/DDOS attacks pose significant threats to the network layer. Furthermore, malicious code injection is a common threat in the application layer. In addition, it was observed that the most frequently suggested mitigation technique for IoT threats was blockchain. However, few studies have discussed machine learning as a mitigation technology for IoT threats. As a result, this paper recommends that researchers in this area focus on machine learning technologies.

Author Contributions: Conceptualization, M.A.A. and E.A.; M.A.A.; methodology; M.A.A. and E.A formal analysis, A.A. investigation, M.A.A. and E.A; resources, M.A.A. and E.A; writing original draft preparation, M.A.A. writing—review and editing, M.A.A.; supervision, M.A.A.; project administration, M.A.A.; funding acquisition, M.A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by King Faisal University.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: This work was supported through the Annual Funding track by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Project No. Grant No. 1785).

Conflicts of Interest: All authors declare no conflict of interest.

References

1. Radanliev, P.; De Roure, D.C.; Maple, C.; Nurse, J.R.; Nicolescu, R.; Ani, U. Cyber Risk in IoT Systems. *Preprints* **2019**, *43*, 2019030104. [CrossRef]
2. Choudhary, Y.; Umamaheswari, B.; Kumawat, V. A study of threats, vulnerabilities and countermeasures: An iot perspective. *Shanlax Int. J. Arts Sci. Humanit.* **2021**, *8*, 39–45. [CrossRef]
3. Lee, I. Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet* **2020**, *12*, 157. [CrossRef]
4. Kandasamy, K.; Srinivas, S.; Achuthan, K.; Rangan, V.P. IOT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP J. Inf. Secur.* **2020**, *2020*, 8. [CrossRef]
5. Pahlevanzadeh, B.; Koleini, S.; Fadilah, S.I. Security in IOT: Threats and vulnerabilities, layered architecture, encryption mechanisms, challenges and solutions. *Commun. Comp. Inf. Sci.* **2021**, 267–283. [CrossRef]
6. Obaidat, M.A.; Obeidat, S.; Holst, J.; Al Hayajneh, A.; Brown, J. A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. *Computers* **2002**, *9*, 44. [CrossRef]
7. Bekkali, A.; Essaaidi, M.; Boulmalf, M.; Majdoubi, D. Systematic Literature Review of Internet of Things (IoT) Security. *Adv. Indynamical Syst. Appl. (ADSA)* **2022**, *21*, 25–39.
8. Albalawi, A.M.; Almaiah, M.A. Assessing and reviewing of cyber-security threats, attacks, mitiga tion techniques in iot environment. *J. Theor. Appl. Inf. Technol.* **2022**, *100*, 2988–3011.
9. Ghazal, T.M.; Afifi, M.A.; Kalra, D. Security vulnerabilities, attacks, threats and the proposed countermeasures for the Internet of Things applications. *Solid State Technol.* **2020**, *63*, 31–45.
10. Abdullahi, M.; Baashar, Y.; Alhussian, H.; Alwadain, A.; Aziz, N.; Capretz, L.F.; Abdulkadir, S.J. Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. *Electronics* **2022**, *11*, 198. [CrossRef]
11. Sethi, P.; Sarangi, S.R. Internet of things: Architectures, Protocols, and applications. *J. Electr. Comput. Eng.* **2017**, *2017*, 9324035. [CrossRef]
12. Yousuf, T.; Mahmoud, R.; Aloul, F.; Zualkernan, I. Internet of things (IOT) security: Current status, challenges and countermeasures. *Int. J. Inf. Secur. Res.* **2015**, *5*, 608–616. [CrossRef]
13. Deogirikar, J.; Vidhate, A. Security attacks in IoT: A survey. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), Palladam, India, 10–11 February 2017; pp. 32–37.
14. Hamid, G.H.; Alisa, Z.T. A survey on IOT Application Layer Protocols. *Indones. J. Electr. Eng. Comput. Sci.* **2021**, *21*, 1663. [CrossRef]

15. Nebbione, G.; Calzarossa, M.C. Security of IOT Application Layer Protocols: Challenges and findings. *Future Internet* **2020**, *12*, 55. [CrossRef]
16. Bibi, N.; Iqbal, F.; Akhtar, S.; Anwar, R.; Bibi, S. A Survey of Application Layer Protocols of Internet of Things. *Int. J. Comput. Sci. Netw. Secur.* **2021**, *21*, 301–311. [CrossRef]
17. Mitra, D.; Goswami, S.; Hati, D.; Roy, S. Comparative Study Of Iot Protocols Pjaee. *Smart Appl. Data Anal. Smart Cities (SADASC'18)* **2021**, *17*, 2020.
18. Cyber Security in Domain of IOT: A Review Threats. Available online: https://www.researchgate.net/publication/346715495_Cyber_Security_in_Domain_of_IoT_A_Review_Threats_and_Security (accessed on 20 February 2021).
19. Dange, S.; Chatterjee, M. IOT botnet: The largest threat to the IOT Network. *Advances in Intelligent Systems and Computing* **2019**, *22*, 137–157. [CrossRef]
20. Ali, M.H.; Jaber, M.M.; Abd, S.K.; Rehman, A.; Awan, M.J.; Damaševičius, R.; Bahaj, S.A. Threat analysis and distributed denial of service (ddos) attack recognition in the internet of things (IOT). *Electronics* **2022**, *11*, 494. [CrossRef]
21. Fadhil, S.A. Internet of things security threats and key technologies. *J. Discret. Math. Sci. Cryptogr.* **2021**, *24*, 1951–1957. [CrossRef]
22. Gerodimos, A.; Maglaras, L.; Ayres, N. IOT: Communication protocols and security threats. *Preprints* **2021**, *25*, 2021110214. [CrossRef]
23. Tsiknas, K.; Taketzis, D.; Demertzis, K.; Skianis, C. Cyber threats to industrial IOT: A survey on attacks and countermeasures. *IoT* **2021**, *2*, 163–186. [CrossRef]
24. Ahmad, I.; Niazy, M.S.; Ziar, R.A.; Khan, S. Survey on IOT: Security threats and applications. *J. Robot. Control. (JRC)* **2021**, *2*, 38–49. [CrossRef]
25. IOT System Model, Challenges and Threats. Available online: https://www.ijstr.org/final-print/mar2020/Iot-SystemModelchallenges-And-Threats.pdf (accessed on 21 March 2019).
26. Wheelus, C.; Zhu, X. IOT network security: Threats, risks, and a data-driven defense framework. *IoT* **2020**, *1*, 259–285. [CrossRef]
27. Ben-Eid, N. Privacy and security in internet of things (IOT): Threats, challenges, and solutions. *IJARCCE* **2021**, *10*, 21–38. [CrossRef]
28. Kabulov, A.; Yarashov, I.; Vasiyeva, D. Security Threats and Challenges in Iot Technologies. *Sci. Educ.* **2021**, *2*, 170–178. [CrossRef]
29. Haque, A.K.; Tasmin, S. Security threats and research challenges of IOT—A Review. *J. Eng. Adv.* **2020**, *1*, 170–182. [CrossRef]
30. Dhirani, L.L.; Armstrong, E.; Newe, T. Industrial IOT, cyber threats, and standards landscape: Evaluation and roadmap. *Sensors* **2021**, *21*, 3901. [CrossRef]
31. Ndatabaye, S.; Svotwa, L.; Dushimimana, P. IoT Database' Technologies:Report. Available online: https://www.researchgate.net/profile/Lynet-Svotwa-2/publication/346529799_IoT_Database'_Technologies_Report/links/5fc8dad092851c00f849d8e0/IoT-Database-Technologies-Report.pdf (accessed on 1 May 2022).
32. Kozlov, D.; Veijalainen, J.; Ali, Y. Security and Privacy Threats in IoT Architectures General. In Proceedings of the 7th International Conference on Body Area Networks (BodyNsets '12), Oslo, Norway, 24–26 February 2012. [CrossRef]
33. Ivan, C.; Vujic, M.; Husnjak, S. Classification of security risks in the IOT Environment. *Ann. DAAAM Proc.* **2016**, *20*, 731–740. [CrossRef]
34. Cunningham, T.; Cunningham, T. Evolution of IoT devices: Future for Smart homes or a threat to your privacy and security? 2022. Available online: https://www.researchgate.net/publication/357805873_Evolution_of_IoT_devices_Future_for_Smart_homes_or_a_threat_to_your_privacy_and_security (accessed on 1 May 2022).
35. Ikrissi, G.; Mazri, T. IOT-based Smart Environments: State of the art, security threats and solutions. *Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci.* **2021**, *XLVI4/W5-2021*, 279–286. [CrossRef]
36. Mohamed, I.A.; Aissa, A.B.; Hussein, L.F. Classification for IoT Threats Based on the Analytic Hierarchy Process. *Int. J. Sci. Technol. Res.* **2020**, *9*, 4860–4867.
37. Krishna, R.R.; Priyadarshini, A.; Jha, A.V.; Appasani, B.; Srinivasulu, A.; Bizon, N. State-of-the-art review on IOT threats and attacks: Taxonomy, challenges and solutions. *Sustainability* **2021**, *13*, 9463. [CrossRef]
38. Shaikh, F.; Ghani, N.; Bou-Harb, E. IoT Threat Detection Leveraging Network Statistics and GAN. 2019. Available online: https://www.researchgate.net/publication/335540870_IoT_Threat_Detection_Leveraging_Network_Statistics_and_GAN (accessed on 1 May 2022).
39. Parsons, E.K.; Panaousis, E.; Loukas, G. How secure is home: Assessing human susceptibility to IOT threats. In Proceedings of the 24th Pan-Hellenic Conference on Informatics, Athens, Greece, 20–22 November 2020; Available online: https://doi.org/10.1145/3437120.3437277 (accessed on 30 May 2019). [CrossRef]
40. Pa, Y.M.; Suzuki, S.; Yoshioka, K.; Matsumoto, T.; Kasama, T.; Rossow, C. IoTPOT: A novel honeypot for revealing current IOT threats. *J. Inf. Processing* **2016**, *24*, 522–533. [CrossRef]
41. Harbers, M.; Bargh, M.; Pool, R.; Van Berkel, J.; Van den Braak, S.; Choenni, S. A conceptual framework for addressing IOT threats: 49 Challenges in meeting challenges. In Proceedings of the 51st Hawaii International Conference on System Sciences, Hilton Waikoloa Village, HI, USA, 3–6 January 2018. [CrossRef]
42. Anjum, A.; Siddiqua, A.; Sabeer, S.; Kondapalli, S.; Kaur, C.; Rafi, K. Analysis Of Security Threats, Attacks In The Internet Of Things. *Int. J. Mech. Eng.* **2021**, *6*, 2943–2946.
43. Haque, S.; Kumar, K.; Haque, M.; Faizanuddin, M.; Shakeb, E.; Singh, A. Blockchain Technology for IoT Security. *Turk. J. Comput. Math. Educ. (TURCOMAT)* **2021**, *12*, 549–554.

44. Alevizopoulou, S.; Koloveas, P.; Tryfonopoulos, C.; Raftopoulou, P. Social Media Monitoring for IOT Cyber-Threats. In Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 26–28 July 2021. [CrossRef]
45. Schiller, E.; Aidoo, A.; Fuhrer, J.; Stahl, J.; Ziörjen, M.; Stiller, B. Landscape of IoT security. *Comput. Sci. Rev.* **2022**, *44*, 100467. [CrossRef]
46. Borcherding, A.; Feldmann, L.; Karch, M.; Meshram, A.; Beyerer, J. Towards a better understanding of machine learning based network intrusion detection systems in Industrial Networks. In Proceedings of the 8th International Conference on Information Systems Security and Privacy, Online, 9–11 February 2022. [CrossRef]
47. Le, K.-H.; Nguyen, M.-H.; Tran, T.-D.; Tran, N.-D. IMIDS: An intelligent intrusion detection system against Cyber Threats in IOT. *Electronics* **2022**, *11*, 524. [CrossRef]
48. Abbas, S.G.; Vaccari, I.; Hussain, F.; Zahid, S.; Fayyaz, U.U.; Shah, G.A.; Bakhshi, T.; Cambiaso, E. Identifying and mitigating phishing attack threats in IOT use cases using a threat modelling approach. *Sensors* **2021**, *21*, 4816. [CrossRef]
49. Prakash, C.; Saini, R.K. A model on IOT security method and protocols for IOT security layers. In *Mobile Radio Communications and 5G Networks*; Springer: Singapore, 2020; pp. 771–780. [CrossRef]
50. Podder, P.; Mondal, M.R.; Bharati, S.; Paul, P.K. Review on the security threats of internet of things. *Int. J. Comput. Appl.* **2020**, *176*, 37–45. [CrossRef]
51. Almaiah, M.A.; Al-Zahrani, A.; Almomani, O.; Alhwaitat, A.K. Classification of cyber security threats on mobile devices and applications. In *Artificial Intelligence and Blockchain for Future Cybersecurity Applications*; Springer: Cham, Switzerland, 2021; pp. 107–123.
52. Almaiah, M.A. A new scheme for detecting malicious attacks in wireless sensor networks based on blockchain technology. In *Artificial Intelligence and Blockchain for Future Cybersecurity Applications*; Springer: Cham, Switzerland, 2021; pp. 217–234.
53. Adil, M.; Almaiah, M.A.; Omar Alsayed, A.; Almomani, O. An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks. *Sensors* **2020**, *20*, 2311. [CrossRef]
54. Adil, M.; Khan, R.; Almaiah, M.A.; Al-Zahrani, M.; Zakarya, M.; Amjad, M.S.; Ahmed, R. MAC-AODV based mutual authentication scheme for constraint oriented networks. *IEEE Access* **2020**, *8*, 44459–44469. [CrossRef]
55. Adil, M.; Khan, R.; Ali, J.; Roh, B.H.; Ta, Q.T.; Almaiah, M.A. An energy proficient load balancing routing scheme for wireless sensor networks to maximize their lifespan in an operational environment. *IEEE Access* **2020**, *8*, 163209–163224. [CrossRef]
56. Adil, M.; Khan, R.; Almaiah, M.A.; Binsawad, M.; Ali, J.; Al Saaidah, A.; Ta, Q.T. An efficient load balancing scheme of energy gauge nodes to maximize the lifespan of constraint oriented networks. *IEEE Access* **2020**, *8*, 148510–148527. [CrossRef]
57. Al Hwaitat, A.K.; Almaiah, M.A.; Almomani, O.; Al-Zahrani, M.; Al-Sayed, R.M.; Asaifi, R.M.; Adhim, K.K.; Althunibat, A.; Alsaaidah, A. Improved security particle swarm optimization (PSO) algorithm to detect radio jamming attacks in mobile networks. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*, 19–33. [CrossRef]
58. Almaiah, M.A.; Dawahdeh, Z.; Almomani, O.; Alsaaidah, A.; Al-Khasawneh, A.; Khawatreh, S. A new hybrid text encryption approach over mobile ad hoc network. *Int. J. Electr. Comput. Eng.* **2020**, *10*, 6461–6471. [CrossRef]
59. Khan, M.N.; Rahman, H.U.; Almaiah, M.A.; Khan, M.Z.; Khan, A.; Raza, M.; Al-Zahrani, M.; Almomani, O.; Khan, R. Improving energy efficiency with content-based adaptive and dynamic scheduling in wireless sensor networks. *IEEE Access* **2020**, *8*, 176495–176520. [CrossRef]
60. Ali, A.; Almaiah, M.A.; Hajjej, F.; Pasha, M.F.; Fang, O.H.; Khan, R.; Teo, J.; Zakarya, M. An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network. *Sensors* **2022**, *22*, 572. [CrossRef]
61. Bubukayr, M.A.; Almaiah, M.A. Cybersecurity concerns in smart-phones and applications: A survey. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; IEEE: Piscataway, NJ, USA; pp. 725–731.
62. Almaiah, M.A.; Hajjej, F.; Ali, A.; Pasha, M.F.; Almomani, O. A Novel Hybrid Trustworthy Decentralized Authentication and Data Preservation Model for Digital Healthcare IoT Based CPS. *Sensors* **2022**, *22*, 1448.
63. Al Nafea, R.; Almaiah, M.A. Cyber security threats in cloud: Literature review. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; IEEE: Piscataway, NJ, USA; pp. 779–786.
64. AlMedires, M.; AlMaiah, M. Cybersecurity in Industrial Control System (ICS). In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; IEEE: Piscataway, NJ, USA; pp. 640–647.
65. Qasem, M.H.; Obeid, N.; Hudaib, A.; Almaiah, M.A.; Al-Zahrani, A.; Al-Khasawneh, A. Multi-agent system combined with distributed data mining for mutual collaboration classification. *IEEE Access* **2021**, *9*, 70531–70547. [CrossRef]
66. Almaiah, M.A.; Al-Zahrani, M. Multilayer neural network based on MIMO and channel estimation for impulsive noise environment in mobile wireless networks. *Int. J. Adv. Trends Comput. Sci. Eng.* **2020**, *9*, 315–321. [CrossRef]
67. Siam, A.I.; Almaiah, M.A.; Al-Zahrani, A.; Elazm, A.A.; El Banby, G.M.; El-Shafai, W.; El-Samie, F.E.; El-Bahnasawy, N.A. Secure Health Monitoring Communication Systems Based on IoT and Cloud Computing for Medical Emergency Applications. *Comput. Intell. Neurosci.* **2021**, *2021*, 8016525. [CrossRef]
68. Alamer, M.; Almaiah, M.A. Cybersecurity in Smart City: A systematic mapping study. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; IEEE: Piscataway, NJ, USA; pp. 719–724.

69. Almomani, O.; Almaiah, M.A.; Alsaaidah, A.; Smadi, S.; Mohammad, A.H.; Althunibat, A. Machine learning classifiers for network intrusion detection system: Comparative study. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; IEEE: Piscataway, NJ, USA; pp. 440–445.
70. Almaiah, A.; Almomani, O. An investigation of digital forensics for shamoon attack behaviour in FOG computing and threat intelligence for incident response. *J. Theor. Appl. Inf. Technol.* **2020**, *15*, 98.
71. Qasem, M.H.; Hudaib, A.; Obeid, N.; Almaiah, M.A.; Almomani, O.; Al-Khasawneh, A. Multi-agent Systems for Distributed Data Mining Techniques: An Overview. In *Big Data Intelligence for Smart Applications*; Springer: Cham, Switzerland, 2022; pp. 57–92.
72. Almudaires, F.; Almaiah, M. Data an overview of cybersecurity threats on credit card companies and credit card risk mitigation. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; IEEE: Piscataway, NJ, USA; pp. 732–738.
73. Almaiah, M.A.; Ali, A.; Hajjej, F.; Pasha, M.F.; Alohali, M.A. A Lightweight Hybrid Deep Learning Privacy Preserving Model for FC-Based Industrial Internet of Medical Things. *Sensors* **2022**, *22*, 2112. [CrossRef] [PubMed]
74. Almaiah, A.M.; Almomani, O.M. An Investigator Digital Forensics Frequencies Particle Swarm Optimization for Dectection and Classification of Apt Attack in Fog Computing Enviroment (IDF-FPSO). *J. Theor. Appl. Inf. Technol.* **2020**, *15*, 98.
75. Ali, A.; Pasha, M.F.; Fang, O.H.; Khan, R.; Almaiah, M.A.; K Al Hwaitat, A. Big Data Based Smart Blockchain for Information Retrieval in Privacy-Preserving Healthcare System. In *Big Data Intelligence for Smart Applications*; Springer: Cham, Switzerland, 2022; pp. 279–296.
76. Khan, Z.A.; Naz, S.; Teo, J.; Ghani, A.; Almaiah, M.A. A Neighborhood and Machine Learning-Enabled Information Fusion Approach for the WSNs and Internet of Medical Things. *Comput. Intell. Neurosci.* **2022**, *2022*, 5112375. [CrossRef]