applied sciences

Systematic Review

Internet of Things Botnet Detection Approaches: Analysis and Recommendations for Future Research

Majda Wazzan [1,*], Daniyal Algazzawi [2], Omaima Bamasaq [1], Aiiad Albeshri [1] and Li Cheng [3]

[1] Computer Science Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia; obamasek@kau.edu.sa (O.B.); aaalbeshri@kau.edu.sa (A.A.)
[2] Information Systems Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia; dghazzawi@kau.edu.sa
[3] Xinjiang Technical Institute of Physics & Chemistry Chinese Academy of Sciences, Urumqi 830011, China; chengli@ms.xjb.ac.cn
* Correspondence: mwazzan0002@stu.kau.edu.sa

Abstract: Internet of Things (IoT) is promising technology that brings tremendous benefits if used optimally. At the same time, it has resulted in an increase in cybersecurity risks due to the lack of security for IoT devices. IoT botnets, for instance, have become a critical threat; however, systematic and comprehensive studies analyzing the importance of botnet detection methods are limited in the IoT environment. Thus, this study aimed to identify, assess and provide a thoroughly review of experimental works on the research relevant to the detection of IoT botnets. To accomplish this goal, a systematic literature review (SLR), an effective method, was applied for gathering and critically reviewing research papers. This work employed three research questions on the detection methods used to detect IoT botnets, the botnet phases and the different malicious activity scenarios. The authors analyzed the nominated research and the key methods related to them. The detection methods have been classified based on the techniques used, and the authors investigated the botnet phases during which detection is accomplished. This research procedure was used to create a source of foundational knowledge of IoT botnet detection methods. As a result of this study, the authors analyzed the current research gaps and suggest future research directions.

Keywords: Internet of Things; IoT; botnet; detection; systematic literature review; SLR

check for updates

Citation: Wazzan, M.; Algazzawi, D.; Bamasaq, O.; Albeshri, A.; Cheng, L. Internet of Things Botnet Detection Approaches: Analysis and Recommendations for Future Research. *Appl. Sci.* **2021**, *11*, 5713. https://doi.org/10.3390/app11125713

Academic Editor: Eui-Nam Huh

Received: 14 April 2021
Accepted: 7 June 2021
Published: 20 June 2021

1. Introduction

Recently, the Internet of Things (IoT) has become an influential area in academia and industry. IoT has emerged as a significant technology to provide the basis for the infrastructure of different innovations in smart environments, such as smart homes, smart healthcare and smart everything. The exponential growth of IoT devices and the advances in technology are resulting in its adoption in a variety of applications to enhance services. IoT devices include electronics, software, sensors, actuators and connectivity between them, permitting these devices to connect, interact and exchange data. The low price of the IoT devices is increasing their popularity and growth. As predicted by Cisco [1], IoT devices could number more than 29 billion by the end of 2023. However, IoT devices are resource constrained—e.g., low processing power and small amounts of memory. They also have to be adaptable to heterogeneous environments. These restrictions are producing challenges in offering and developing security solutions for IoT devices. The lack of efficient security and standards for IoT devices has led vulnerabilities that cyber-criminals can exploit. The device restrictions further amplify emerging obstacles to the IoT ecosystem. Various types of attacks are also probable owing to the vulnerabilities of IoT devices. One of the key attack scenarios is an attacker compromising IoT devices to use them as parts of an IoT botnet. Once an IoT device is infected and compromised, the attacker controls the infected device and involves it in the execution of different attacks. The latter step comes after the completion of the process of the attacker taking control of as many IoT devices as possible. In this way, the attacker creates and expands his own IoT botnet. Creating IoT botnets is one of the main criminal activities related to IoT; they expand rapidly and can cause more harm than disparate malicious activities. The impacts of IoT botnets could be severe. To exemplify that, the famous and huge Mirai Botnet embattled the Domain Name Server (DNS) provider company (Dyn) through exploiting different kinds of vulnerable IoT devices. Mirai Botnet used closed-circuit television cameras, routers and digital video recorders (DVRs) to send requests from ten million IP addresses. The attacks generated traffic exceeding one terabyte per second (Tbps) and brought down major Internet platforms, including Twitter, the Guardian, Netflix and CNN; and consequently, the attack caused failure of the services and disrupted the Internet. Gartner [2] predicted that this attack is an example of similar attacks to come. Unsurprisingly, in light of that prediction, and in addition to the tremendous growth of the IoT devices, IoT botnets are a hot research area.

To the best of our knowledge, no prior research has carried out a detailed systematic literature review (SLR) that classifies IoT botnet detection approaches. Therefore, it is difficult to define the methods and techniques used to detect IoT botnets, and to discern gaps in research and future directions relevant to this important topic. Our study, therefore, is a systematic literature review that defines, explicates, contrasts and assesses current methods used in the IoT botnet research area. Our goal was to respond to the following questions:

- RQ1: What are the different phases of forming an IoT botnet?
- RQ2: What types of malicious activity and which scenarios involve IoT botnets?
- RQ3: What methods and techniques are utilized to detect IoT botnets?

Finally, we specify the current research gaps and suggest future research directions. The following subsections will explain our motivation and highlight the contributions of this research.

1.1. Research Motivation

The IoT botnet threat is an issue facing Internet of Things (IoT) that demands efficient defense and response methods and techniques. Different approaches and technologies could provide enhancements in the detection of IoT botnets and improve the overall security of the IoT ecosystem. By probing the recent literature on IoT botnet detection, it became clear to us that there is a lack of in-depth study on solutions to IoT botnet detection, and a lack of systematization for such solutions. Thus, the research is quite undeveloped and has much potential.

There are still some reviews and surveys related to IoT botnet detection. Singh et al. [3] thoroughly surveyed IoT botnet detection solutions that applied Domain Name Space detection. Their research offers a novel classification framework for botnet detection techniques dependent on DNS and provides a detailed overview of each technique. Koroniotis et al. [4] surveyed the current methods of deep learning and forensic mechanisms for botnets in IoT, and discussed their issues. Furthermore, the researchers explored the use of deep learning algorithms in network forensics. Prospective directions of research have also been highlighted. Al-Hajri et al. [5] investigated the use of machine learning in IoT botnet anomaly detection. The researchers considered the feasibility of using autoencoder algorithms for detection, and suggested future research directions for the use of machine learning algorithms in this area. Finally, Ali et al. [6] presented the research most closely related to this study. They provided a demographic review on IoT-based botnets and classified the approaches into avoidance and detection, and provided recommendations for investigation into avoidance approaches.

The formation of a botnet has several phases, and accordingly, the detection techniques differ based on the phases that are targeted. Each phase may express different activities; thus, a detailed analysis of the detection tactics in each phase is required. However, hitherto there was no comprehensive and thorough review of IoT botnet detection with botnet phases taken into account. Hence, we found the need for a thorough analysis focusing on the phases of IoT botnets in which detection is performed and the different types of attacks.

1.2. Contributions of This Research

To guarantee providing a comprehensive and clear vision of the current research to outline new directions for research, this study followed the guidance referred to in the studies [7–10] to conduct the SLR.

This SLR provides baseline knowledge for current IoT botnet detection techniques. It provides background for specialists to understand the present methods and techniques, and provides information for researchers who want to investigate emerging gaps or be at the forefront of mainline research. Concisely, the major contributions of our study are summarized below:

- Conducting a systematic review and investigating the present approaches for IoT botnet detection.
- Recapping the experimental attestations to the advantages and restrictions of the current IoT botnet detection approaches.
- Providing insights into the phases of the IoT botnet and the different types of attack and attack scenarios that utilize IoT botnets.
- Recognizing the challenges and issues in the detection of IoT botnets.
- Outlining the vital ways future studies could enhance the process of IoT botnet detection.

The remaining parts of this research paper continue in the following manner: Section 2 offers a concise overview of Internet of Things and IoT botnets. The methodology of the study, the research questions, the domain and the procedure of the SLR are described in Section 3. Section 4 addresses the key findings of the systematic analysis, including the limitations of the review. Section 5 ends the study and points out directions for new studies. The arrangement of this paper is shown graphically in Figure 1.

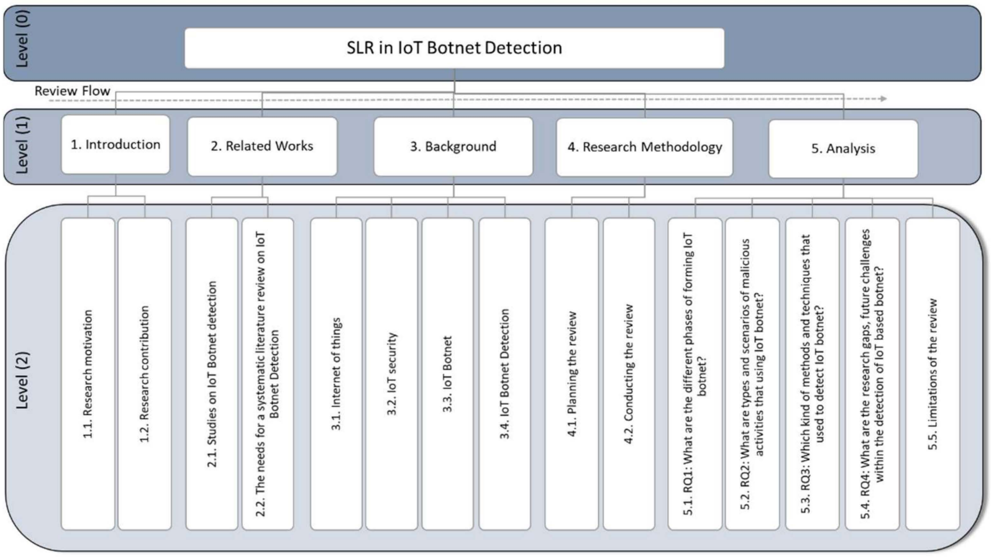

Level (0)
SLR in IoT Botnet Detection
Review Flow
Level (1)
1. Introduction
2. Related Works
3. Background
4. Research Methodology
5. Analysis
Level (2)
1.1. Research motivation
1.2. Research contribution
2.1. Studies on IoT Botnet detection
2.2. The needs for a systematic literature review on IoT Botnet Detection
3.1. Internet of things
3.2. IoT security
3.3. IoT Botnet
3.4. IoT Botnet Detection
4.1. Planning the review
4.2. Conducting the review
5.1. RQ1: What are the different phases of forming IoT botnet?
5.2. RQ2: What are types and scenarios of malicious activities that using IoT botnet?
5.3. RQ3: Which kind of methods and techniques that used to detect IoT botnet?
5.4. RQ4: What are the research gaps, future challenges within the detection of IoT based botnet?
5.5. Limitations of the review

Figure 1. The SLR structure from the main topic in level 0 to the subsections in level 2.

2. Relevant Reviews

In order to highlight the need for this SLR, Section 2 presents a literature review of IoT botnet detection methods.

2.1. The Previous Studies on IoT Botnet Detection

This section identifies the previous studies that are relevant to the topic of this SLR. So far, there have been several surveys that addressed the issue of IoT botnet detection in different ways, as explained in Table 1. Many of these studies each focused on a specific kind of detection method or technique [4,5,11,12]. For instance, S. Dange et al. [11] studied methods based on machine learning techniques; they reviewed the various types of possible IoT attacks and evaluated the significance of each type for botnet attackers. N. Koroniotis et al., in [4] reviewed the network forensics and deep learning methods that could be applied in IoT botnet detection, and investigated the problems and the current solutions for deep learning and IoT botnet forensics mechanisms. Moreover, R. Al-Hajri et al., in [5] surveyed and investigated the works that used autoencoder algorithms in IoT botnet detection, and outlined potential research directions for the use of machine learning in this area. In the same manner, J. Sengupta et al., in [12] also surveyed the attacks and security challenges in industrial IoT and blockchain. They focused on solutions based on blockchain as they considered it promising technology for IoT botnet detection methods.

Table 1. A comparison of the related reviews.

Authors	Year	Study Type	Topics	SLR	IoT Botnet	Detection Methods	Detection Phases	Malicious Activities Type	Purpose	Ref
S. Dange et al.	2020	Survey	Attack on IoT	✗	✓	Focus on machine learning detection techniques	✗	✗	Generic Review	[11]
Y. Ji et al.	2019	Study	Mirai IoT botnet	✗	✓	Not provided	✗	✗	Mirai Review	[13]
N. Koroniotis et al.	2018	Study	Forensics and deep learning mechanisms for IoT Botnet	✗	✓	Network Forensics Method for IoT Botnet	✗	✗	Network Forensics Review	[4]
R. Alhajri et al.	2019	Survey	IoT botnets detection using auto-encoders	✗	✓	Focus on using Auto-Encoder in detection techniques	✗	✗	Auto-Encoder survey	[5]
M. Salim et al.	2019	Survey	DDoS in IoT	✗	✗	Focus on DDoS detection classification	✗	✗	DDoS Survey	[14]
M. Singh et al.	2019	Survey	DNS based botnet in IoT	✗	✓	Focus on DNS based botnet detection methods	✗	✗	DNS based botnet survey	[3]
J. Sengupta et al.	2020	Survey	Attacks on IoT	✗	✗	Focus on blockchain based methods	✗	✗	IoT security issues survey	[12]
Ali et al.	2020	SLR	IoT Botnet Attack	✓	✓	Sketchy review of IoT Botnet Detection techniques	✗	✗	Demographic review	[6]
This SLR	2020	SLR	IoT Botnet Attack	✓	✓	Review all detection techniques	✓	✓	IoT Botnet detection review	—

Other studies reviewed IoT botnet detection shallowly, without explaining the details of each method. Ali et al. [6] provided a demographic survey of IoT botnet attacks. Moreover, some reviews each focused on only studying one type of IoT botnet malware without providing a review of the relevant detection methods. Y. Ji et al. [13] studied Mirai Botnet's malware comprehensively; they conducted a review evaluating and investigating the botnet and its IoT avoidance policies. They studied Mirai Botnet's architecture and elements in detail; in addition, the authors investigated the attack methods and the impact factor of the botnet propagation model.

M. Salim et al. [14] handled the detection of a certain attack type triggered by an IoT botnet; they reviewed the distributed denial of service (DoS) attack and defenses against it in the context of IoT. They identified the reasons why the attackers tended to utilize DDoS attacks on IoT devices, and they presented the main methods used against DDoS attacks for protection. Finally, M. Singh et al. [3] focused on the detection methods that are based on specific protocols (DNS) in IoT environments, with a detailed study of each technique. This work offered a novel categorization framework for DNS-based botnet detection methods. The next subsection will explain the importance of the existence of a systematic review of the literature on IoT botnet detection.

2.2. The Importance of the Existence of a Systematic Literature Review on the Detection of IoT Botnets

Before carrying out this study, we came across some papers addressing IoT botnet detection. Although these studies deal with IoT botnet detection, none of them provides a systematic literature review that handles the issue comprehensively. We did encounter one SLR that directly related to IoT botnet detection, however. The researchers in that study [6] reviewed studies that utilized network forensics for IoT botnet detection, and summarized the use of certain datasets and evaluation metrics. They focused on providing a demographic SLR for the selected studies.

As explained, to the best of our knowledge, this is the first systematic literature review that deeply analyzes and compares studies on IoT botnet detection. It emphasizes studying the different detection solutions according to the phases of forming the botnet. It also explains the types of malicious attacks that the solutions focus on detecting.

To the best of our knowledge, [6] did not present insights into research gaps and future work regarding IoT botnet detection approaches, further solidifying our motivation for creating this systematic review. Consequently, the key contribution of this SLR is a widespread review of the literature on botnet detection for IoT systems. Likewise, we desire to provide beginners with concise and beneficial content so that they might grasp this research. Again, no preceding reviews have categorized and investigated detection approaches based on the phase of the botnet. As it is an evolving field, the suggested research directions have not been explored by prior studies, to our knowledge.

None of the reviewed studies (see Table 1) refers to any of the research questions elaborated in Section 4. The major advances in detection methods and their challenges are described herein. In addition, perspectives are offered concerning the open issues and for recommendations of future study. This research also provides a systematic analysis of the literature on IoT botnet detection methods from 2016. The authors found 243 papers, which were narrowed down through an accurate and iterative selection process to 37 primary studies. Thanks to the trends in research identified, this survey will directly help academics and practitioners in developing powerful methods for the detection of botnets in the IoT context.

3. Background

This section provides background that paves the way to the review topic; it describes the Internet of Things (IoT), IoT security, IoT botnets and IoT botnet detection.

3.1. Internet of Things

3.1.1. The Internet of Things Concept

The IoT has matured in recent years in both complexity and functionality. It has evolved and become an integral part of modern society in numerous applications. Ashton et al. introduced the "Internet of Things" during a presentation in 1999 [4,15], describing the importance of providing machines that capture and use data in an automated and contextual manner. IoT has several definitions in the literature, owing to its many characteristics, such as the wide array of technologies utilized, the multiplicity of the connected protocols in one infrastructure (as explained in in the next Section 3.1.2), the ability to move and its polymorphic nature. All of these characteristics play instrumental roles in increasing the difficulty of determining a single thorough concept that best defines it the IoT as a whole. The Internet of Things Global Standard Initiative (IoT-GSI) from ITU defined the IoT as follows: "A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies." The IoT makes effective use of things to provide all forms of applications with services, while guaranteeing that security and privacy standards are met; therefore, the IoT has social and technological impacts.

3.1.2. IoT Architecture

There are different proposed IoT architectures in the literature—for example, middleware based, SOA based, six-layer and three-layer architectures [16]. In this section, for the purpose of addressing the basic communication, this SLR focuses on the basic three-layer IoT architecture. The three layers are a perception layer, a network layer and an application layer, as follows:

- The perception layer is a physical devices and communication layer that consists of sensors and actuators that aggregate, sense and process data, and then transmit the data to the network layer. This layer contains physical objects such as cameras, RFIDs and baby monitors.
- The network and transport layer is a communication layer which transmits and routes the aggregated data from the perception layer to the application layer using different devices, such as gateways, switches, and routers.
- The application layer is a messaging layer containing the application that interacts with users. E-health, smart factory and smart transport fields all utilize such applications.

As described in Figure 2, each IoT layer uses different protocols and standards [17,18]. The physical devices and communication technology use standards such as WiFi, 4G/5G and LoRaWAN. The network and transport are use different protocols, such as IPv6, 6LowPAN, RPL, TLS and DTLS. The application and messaging protocols include MQTT, CoAP, HTTP and XML. In addition, there are different protocols that are used for authentication and key management, such as Oauth2.0, OpenId and PKI.

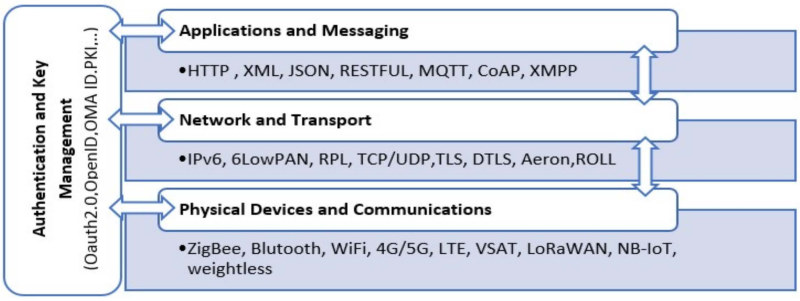

Authentication and Key Management
(Oauth2.0,OpenID,OMA ID,PKI...)
Applications and Messaging
•HTTP , XML, JSON, RESTFUL, MQTT, CoAP, XMPP
Network and Transport
•IPv6, 6LowPAN, RPL, TCP/UDP,TLS, DTLS, Aeron,ROLL
Physical Devices and Communications
•ZigBee, Bluetooth, WiFi, 4G/5G, LTE, VSAT, LoRaWAN, NB-IoT, weightless

Figure 2. The protocols and standards of IoT.

3.2. IoT Security Issue

To recap, the IoT ecosystem includes physical or virtual entities that connect to the Internet. These entities have IP addresses and the ability to interact with other objects or human users. The exponential growth of IoT devices and the advances in technology have resulted in the adoption of these devices in diverse types of applications in our lives. In today's world, the IoT is an integral part of most fields. For IoT devices with limited computational ability, memory, radio bandwidth and power resources, it is generally unaffordable or not even possible to have them perform security tasks, particularly under heavy data streams because of the requirements for intensive computing and no latency.

Most current security solutions produce heavy processing and communication loads for IoT devices indeed. This makes them inappropriate solutions for protecting IoT devices, so IoT devices are typically more susceptible to attacks than computer systems. Hence, there is a need to address the security issues related to IoT devices and the whole IoT environment.

IoT Attacks

In the heterogenous IoT environment, IoT attacks come in different forms. There are physical attacks, such as side channel attacks and sleep denial attacks. There are network attacks, such as routing attacks, sybil attacks and man in the middle attacks. There are software attacks, such as viruses, trojans and malware insertion [12]. The IoT attacks have increased with the number of vulnerable devices linearly, since 70% of IoT devices are vulnerable devices [19]. Consequently, many incidents have occurred, and they affect society and economies. Therefore, following a high number of incidents involving IoT products, IoT security became a major concern. It has been said that most attacks are botnet-based attacks in IoT environments. Again, on IoT devices, many security vulnerabilities still exist because most of them do not have adequate memory and computing resources for robust security mechanisms [19].

The impacts of IoT botnets could be great, and most IoT malware attempts to create a botnet [19,20]. For example, in October 2016, Mirai Botnet target the Domain Name Server (DNS) provider company (Dyn) through exploiting different kinds of vulnerable IoT devices, including closed circuit television cameras, routers and digital video recorders (DVRs). Using those devices, requests were sent from ten million IP addresses. This attack generated traffic exceeding 1 Tbps and brought down major Internet platforms, including Twitter, the Guardian, Netflix and CNN. Consequently, the attack caused disruptions in those services and disrupted the Internet overall.

3.3. IoT Botnet

The low price of IoT devices was the cause of increasing their popularity and growth. As predicted by Cisco [1], IoT devices may number more than 29 billion by the end of 2023. However, these devices lack efficient security and standards, which leaves them vulnerable to being attacked and controlled by attackers. One of the most important attack scenarios is IoT devices being compromised and added to a IoT botnet. Once the IoT device is infected and compromised, the attacker can control it and use it to share in the execution of different attacks.

Generally, the botnet can be defined as a collection of compromised devices known as bots running malicious code and controlled by an administrator called the botmaster [21–23].

Typically, a botnet consists of three primary components:

- The attacker;
- The malicious infrastructure;
- The bots.

These components communicate and act differently in different botnet architectures. Botnets have a wide variety of malicious uses, including the distribution of email spam, distributed denial of service (DDoS) attacks, cracking passwords, key logging and cryptocurrency mining [11,23]. However, the first botnet was designed with benign intentions. When the first bot known as "Eggdrop" appeared in 1993, it offered administrative assistance to Internet Relay Chats (IRC) with its key functionality [4]. The malicious bot started appearing after that in 1998; the first was known as the "GTbot," which was capable of executing scripts when prompted via its IRC channel's command and control (C&C).

More than a decade ago, the first IoT botnet was recognized. Then, it was followed by many IoT botnets that became the building blocks of the IoT botnets seen today. The Hydra IoT botnet, which appeared in 2008 [21,22,24,25], infected routers and had DDoS and spreading competences. Mirai, in 2016, was the largest IoT botnet, which infected millions of devices and dominated them to perform the biggest DDoS ever [22,26,27]. The year 2016 also witnessed the emergence of another type of botnet competing with Mirai, which was known as Hajime, a peer-to-peer (P2P) IoT botnet [28,29]. It did not show any acts of sabotage, so some believed that it had a protective role for Internet of Things devices. In addition, during the year 2017 an IoT botnet called Brickerbot [29] appeared that aimed to permanently destroy devices through permanent denial of service (PDoS) attacks. In 2018, and according to [30], a new IoT botnet appeared which scanned for vulnerable IoT devices and spread its malware inside the IoT environment; it offered attack as a service or botnet as a service for herders. In [31], the researchers investigated a potential attack in which a botnet uses IoT devices with high electrical power to control requests and subsequently interrupt the processes of a power grid. The researchers in [27,32] used IoT devices to reverse DDoS attacks, which are hard to track; they also discussed the possibilities of DDoS attacks. Finally, in 2020, Mukashi [33], a new variant of Mirai and one of its malware family of IoT botnets, took advantage of the CVE-2020-9054 vulnerability existing in Zyxel NAS devices utilizing firmware version 5.21, permitting malicious code to be executed on the vulnerable machines by remote attackers.

Some of the distinguished IoT botnets found over the years are noted in Table 2.

Table 2. IoT malware families.

IoT BotNet	Description	Estimated Number of Devices [34]
Bashlight (2014–2016)	Has IRC based targeting Linux based IoT devices (BusyBox) like cameras and DVRs. It executes brute force with default credentials with open TelNet port.	(120,000)
Mirai (2016)	Centralized architecture model targeting closed circuit television cameras, routers and Digital Video Recorders (DVRs). It uses TelNet port and predefined attack vectors Dictionary attack based on 62 entries.	(145,000+)
Brickerbot (2017)	Bruteforce the TelNet password then run command to corrupt storage, delete all files and make the device inoperable.	(10,000,000+)
Hajime (2016–2018)	Same as Mirai targeting Devices through TelNet but it has Peer-to-Peer architecture model. Recently Hajime evolve to use different ports and different exploits. Until now Hajime just scan and infect vulnerable devices but does not launch any DDoS attack	(300,000)
Wirex (2017)	Working on android devices and proliferate through application in Google Play	(100,000+)
Reaper (2018)	Exploit the vulnerabilities of IoT devices such as routers of LinkSys, DLink and connected cameras.	(1,000,000+)

3.3.1. Botnets in IoT Networks

Several families of malware have been released to target IoT devices and form IoT botnets. Some of the botnets discovered in IoT networks were Mirai, Bashlight, Wirex, Brickerbot Reaper and Hajime. An explanation of each of them is given in Table 2 [25,34–36].

3.3.2. IoT Botnet Life Cycle Phases

Many studies [21,22,27,37] have agreed that IoT botnets carry out their actions in at least the three main phases (see Figure 3), as described below:

Phase 1: Scanning Phase: In order to locate a vulnerable device, a bot (or malicious code) implements scanning and reconnaissance. The botmaster scans for vulnerable IoT devices. Once it finds one, it starts to infect it through brute force or by exploiting a vulnerability. Once the vulnerable device is compromised, it becomes a bot and starts communicating with the botmaster. Mirai malware families, for example, send fingerprint packets to scan for pseudorandom IPv4 addresses to locate IoT devices that are attainable through Telnet service on port 23 or port 2323 [26]. Through abusing frail credentials using brute force or exploiting the known vulnerabilities of IoT devices, the bot compromises new victims.

Phase 2: Propagation Phase: A suitable version of the bot is installed and executed based on the architecture of the vulnerable device. Oftentimes, to avoid targeting devices victimized by any other potential malware and acquire complete control, the bot kills the process bound to the related service [26] in order to delete any other previous malware and lock ports to itself. The malicious code recruit new bots and propagates to expand the IoT botnet as quickly as possible. In this phase, the bots are still awaiting commands from the botmaster.

Phase 3: Attack Phase: Execution of malicious activities such as DDoS, crypto mining and spam. The attacker initiates the attack by sending the commands through the command and control server to all the distributed bots to trigger the attack. Consequently, the bots start the attack after receiving the identical commands.

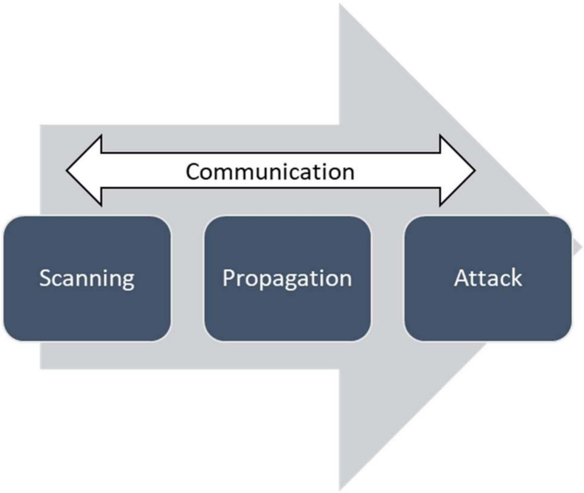


Figure 3. Phases of an IoT botnet's life cycle.

During all phases and depending on the architecture of the botnet, a communication and control process are established. In this process, the bot interacts with the controller host that manages the commands to receive instructions and exchange messages.

3.3.3. Basic Components of IoT Botnets

Understanding the way Internet botnets work is very important in order to find new and effective ways to discover these bots and deal with them to limit their damages. Understanding the workings of these bots more comprehensively will help us to resist them and keep cyberspace clean, and thus help to ensure the security of the Internet. After the source code for Mirai was published, many cybercriminals cloned and adjusted the code and issued copies of IoT malware that aimed to create Internet of Things (IoT) botnets and compete in controlling the largest possible number of IoT devices [26]. Therefore, most IoT malware has similar working steps. In the following steps, how these IoT botnets work will be explained (see Figure 4).

Figure 4 illustrates how IoT botnets work. It is clear from the figure that botnets work in several steps. They are generalized and summarized in seven steps as follows:

- The bots search the IP address space for devices running Telnet or SSH and try to log in using a hard-coded IoT credential dictionary.
- Once successful, a bot reports the IP address of the victim and related credentials to a report server.

- The report server dispatches this information to the loader server.
- The loader server simultaneously forces the device to be infected in a way dependent on the architecture of the victim.
- The attacker sends a command to the command and control server specifying the target and the requested details to start the attack.
- The command and control server informs the bots in preparation for an attack.
- The bots trigger the attack against the specified target.

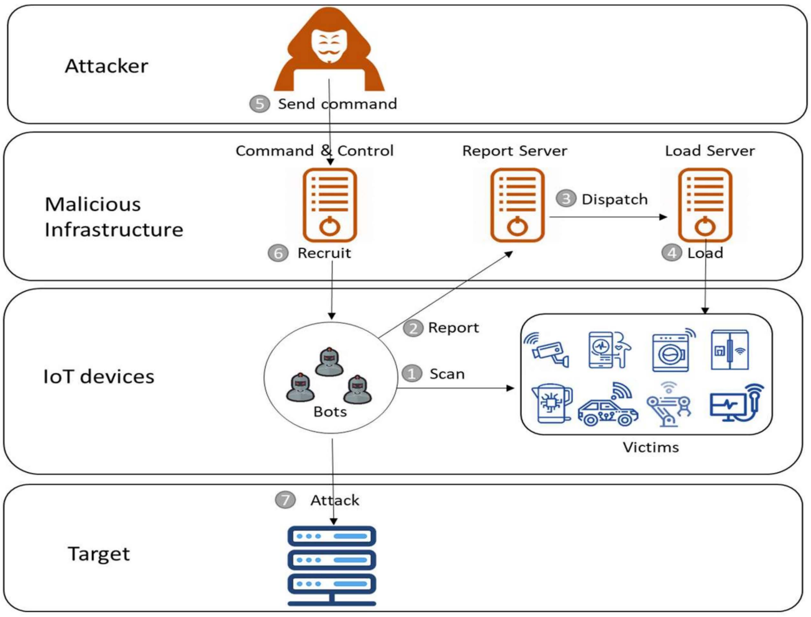


Figure 4. A flow diagram of an IoT botnet.

It is noteworthy that malware for the Internet of Things is developing and being modified for different reasons. These reasons include having different purposes for the IoT botnets, and exploiting new vulnerabilities. Therefore, maintenance [27] is performed for such malware. Reconfiguration of such a botnet or adding new devices to it increases its size and makes it more powerful. These changes may make IoT botnets more sophisticated and increase the difficulties in IoT botnet detection.

3.3.4. IoT Botnet Architecture

Conventional botnets share the same architectures as IoT botnets. They can be defined as centralized botnets, decentralized (peer-to-peer) botnets and hybrid botnets.

- Centralized botnets. The botmaster manages and tracks all bots from a unified central server, which decreases the latency; i.e., all bots receive instructions from and report to a central server (C&C server) [11,21]. The botmaster in this architecture may have one or more central servers to use [23]. The server uses protocols such as HTTP and IRC. The botmaster server may have the disadvantage of being a single point that can cause total failure [11,21]. One of the famous families of centralized IoT botnets is the Mirai family [26].
- Decentralized botnets. These are also called peer-to-peer (P2P) botnets. Each bot operates as a client and a server; each bot is linked to at least one other bot. Only if all the bots are interconnected will the commands reach each bot. In this architecture, it is difficult to coordinate between bots, but at the same time, it is more sophisticated and not easy to detect because of the different communication between peers. This type of IoT botnet uses a peer-to-peer protocol in communication [11,21]. One of the well-known decentralized (P2P) IoT botnets is Hajime [38].

- Hybrid botnets. A hybrid botnet contains two types of bots; some of them have functionality as servers and clients, and others just as clients, so it is a combination of the previous two types (centralized and decentralized) of architecture. There is high message latency [21].

3.3.5. The IoT Botnet Boom and the Marketplace

The number of botnets has increased in the Internet of Things drastically over time, and they have become a great danger due to what we referred to previously regarding their uses for illegal purposes. The occurrence of this boom is due to several factors, which we refer to in the following points:

- Usually, it is possible to exploit Internet of Things devices because these devices use default authentication data. Moreover, services are exposed and easy to access.
- IoT devices are continuously connected to the Internet of Things networks; that is, they are accessible all the time because of the functions they perform that do not accept halting.
- Their market growth is accelerating considerably [37].
- The security standards for these devices are very low. Few end users change the default manufactory nomenclature once deployed; therefore, it is easy to be speculated that often they use root:root and admin:admin. The attacker can alter default passwords effortlessly, blocking users from logging in and other attackers from taking control.
- An attacker can easily shut down or dominate large numbers of IoT devices at once when these devices are improperly monitored and mismanaged.

After the public release of IoT botnet codes, such as those of Bashlite and Mirai, more botnets have appeared, and attackers are hunting for new victims to exploit. Financial gain is a major incentive for spreading more IoT botnets. Thus, there arose the so-called Internet of Things bot market, in which IoT botnets are offered for a price. For example, many renowned cybercriminal groups have already monetized their capabilities by renting out IoT botnets with their powerful stressed services to be used by benefiters in DDoS attacks. This allows inexperienced attackers to conduct DDoS attacks at over 100 Gbps effortlessly [39]. Recently, botnets have been involved in different notable attacks, resulting in denial of service and regression, data exfiltration and theft, lost revenue and tarnished reputations for organizations. Consequently, IoT botnets have become a major issue that affects the security of the Internet of Things and the whole Internet. In the next section, we will explain the importance of IoT botnet detection.

3.3.6. IoT Botnet Detection

Our lives have been dramatically changed by the digital revolution, in which the Internet of Things (IoT) plays a significant role. However, the IoT's rapid growth contributes to various and great cybersecurity threats. Therefore, both academia and industry have recently had considerable interest in detecting and preventing possible attacks on IoT networks. As it mentioned before, creating an IoT botnet is a major attack; usually organizations use several security controls such as intrusion detection and threat intelligence in order to detect and block IoT botnets. These methods may be somewhat effective, but they cannot detect the formation of zero-day IoT botnets that have no known signatures. This is the reason for both academia and industry to focusing on IoT botnet detection mechanisms. The aim is normally to find the origins of an attack and reduce that traffic. Both industry and academia can also help to analyze how botnet structures occur in IoT systems, which should facilitate enhancing security controls for detecting recognized and the new botnets. The study of the distinct behaviors of IoT botnets is improving the means to combat them.

4. Materials and Methods

In this section, we explain the materials and methods that we used in this research, so that any researcher can follow the same steps to get the results. The remainder of the paper focuses on a systematic literature review (SLR) with a methodology proposed by [7,10]. The study in [7] proposed three major stages for SLR:—planning, conducting and reporting—as explained in Figure 5.

Stage 1. Plan the SLR in the following three steps: identify the needs of the SLR; define the research question(s); develop a protocol for the review.

Stage 2. Conduct the review in three steps: select the studies; define quality assessment criteria; extract and synthesize data.

Stage 3. Report the SLR with the following three steps: specify the strategy of distribution; format the report; evaluate the report.

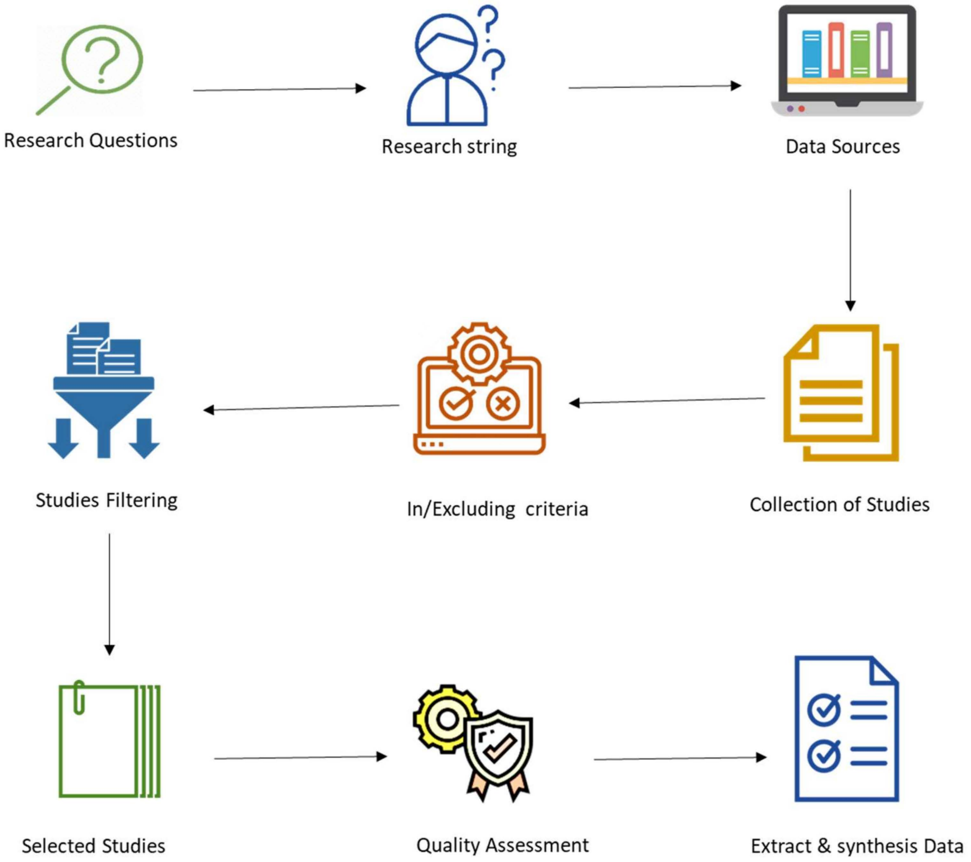


Figure 5. The steps of a systematic literature review.

4.1. Planning the SLR

In this SLR, the authors started the planning stage by identifying the need for this SLR and developing the review protocol as follows.

4.1.1. Step 1: Identification of the Need for the Review

The main objectives of this systematic literature review were to investigate how other research has addressed the issue of detection IoT botnet using different methods and techniques. Therefore, this SLR had the following objectives:

1. To identify what research about IoT botnet detection has been addressed using different methods and techniques.
2. To identify gaps in IoT botnet detection and suggest directions for future work.

4.1.2. Step 2: Specifying the Research Questions

The authors believe that identifying the research questions clearly is an important step of any systematic literature review, because the questions drive the whole methodology of the SLR. Therefore, the goal of this process is to allocate research questions that clearly identify the research problem. The questions of the research should be focused and clear—not vague, nor broad, nor too specific. Therefore, before formulating the research questions and to ensure the research questions were well-built, the authors used the question formatting practice PICOC [7,10] (population, intervention, comparison, outcome, context).

Consequently, the research questions and the motivations of this review were created as shown in Table 3.

Table 3. Research questions and the motivations of the SLR.

Research Questions	Motivations
RQ1: What are the different phases of forming an IoT botnet?	M1: To determine the phases of IoT botnet
RQ2: What types of malicious activity and which scenarios involve IoT botnets?	M2: To get insight into different types and scenarios of attacks that use IoT botnets.
RQ3: What methods and techniques are utilized to detect IoT botnets?	M3: To identify the opportunities and trends in IoT Botnet detection methods and techniques.

4.1.3. Step 3: Developing the Review Protocol

This step aims to reduce the possibility of potential bias during the SLR; that is, it avoids driving the analysis by the authors expectations. The authors defined the review protocol by the following: gathering background information; forming research questions; creating a search strategy for the primary studies; choosing databases; searching using keywords and queries; establishing selection criteria and procedures; performing quality assessments; utilizing a data extraction strategy; combining the extracted data and preparing them for presentation. The authors further refined the protocol during the SLR process.

4.1.4. Step 4: Evaluating the Protocol of the Review

The objective of this evaluation process was to have experts evaluate the protocol to ensure its objectivity and make the needed refinements. The authors asked experts to do this step since the protocol is a critical element of any SLR. Figure 5 explains the steps of this SLR.

4.2. Conducting the Review

4.2.1. Step 1: Identification of Research

The authors in this step identified the research by generating an iterative search strategy which included performing a preliminary search and assessing the number of the potentially related studies. Using pilot search queries with diverse search expressions boosted the results for the previously selected research questions. After this, the authors checked the search results. Then they went to an expert in the field for consultation. The authors managed the large number of references by using a bibliography management tool, “Mendeley” [40]. As part of the search process, the authors selected the appropriate data sources related to the research field to ensure getting relevant articles. The data sources are listed in Table 4. The authors searched digital libraries to ensure good coverage of the literature.

4.2.2. Step 2: Selection of Primary Research

In this step, the authors developed the search terms according to the approach in [41].

The authors followed the above approach by specifying three main groups of keywords related to the research questions and the PICOC. The authors added synonyms and abbreviations related to each keyword and grouped them together. Group one was “Internet of Things,” and it aimed to retrieve all the studies related to the Internet of Things. Group two was “botnet,” and it aimed to find all the studies related to botnets. Group three was “Detection,” and it aimed to retrieve all the studies related to detection. Our research focused on the intersection between the three groups.

Table 4. The data sources used.

Data Source	Website
Springer	rd.springer.com
ScienceDirect	sciencedirect.com
IEEE eXplore	ieeexplore.ieee.org
ACM DL	dl.acm.org
Willy	onlinelibrary.wiley.com
Taylor & Francis	tandfonline.com

The authors took the advantage of the Boolean operators "AND" and "OR" when constructing the search terms. They used "OR" to concatenate the keywords within the same groups and "AND" to concatenate keywords from different groups. Finally, the following search terms were used for searching the data sources (Table 4) and retrieving the relevant publications. It is worth mentioning that the last search date by the authors was on 2 February 2020.

The search phrase: (("Internet of things" OR "IoT") AND ("Botnet") AND ("Detection")).

Subsequently, the authors adjusted the search phrase and adapted it to conform to each data source. We searched by title, keywords and abstract; then we limited the search by year of publication to 2016–2020. Many studies in the field were conducted beforehand [42–44], but we chose to focus on a short period.

The articles retrieved from the search results went through a preliminary review of content by the authors. This was to ensure the relevance of each article to the purpose of this SLR. Then the authors followed the "include" and "exclude" criteria illustrated in Table 5. The authors eliminated duplicate versions of studies and discarded the unrelated articles (e.g., if they identified another subject as the main research interest), and the authors then progressed to analyzing the articles that addressed the research questions. The initial number of total articles was 243, and after enforcing the inclusion and exclusion criteria, only 37 articles where chosen. Figure 6 shows a graph explaining the search results. Finally, the selected articles are shown in Table 6.

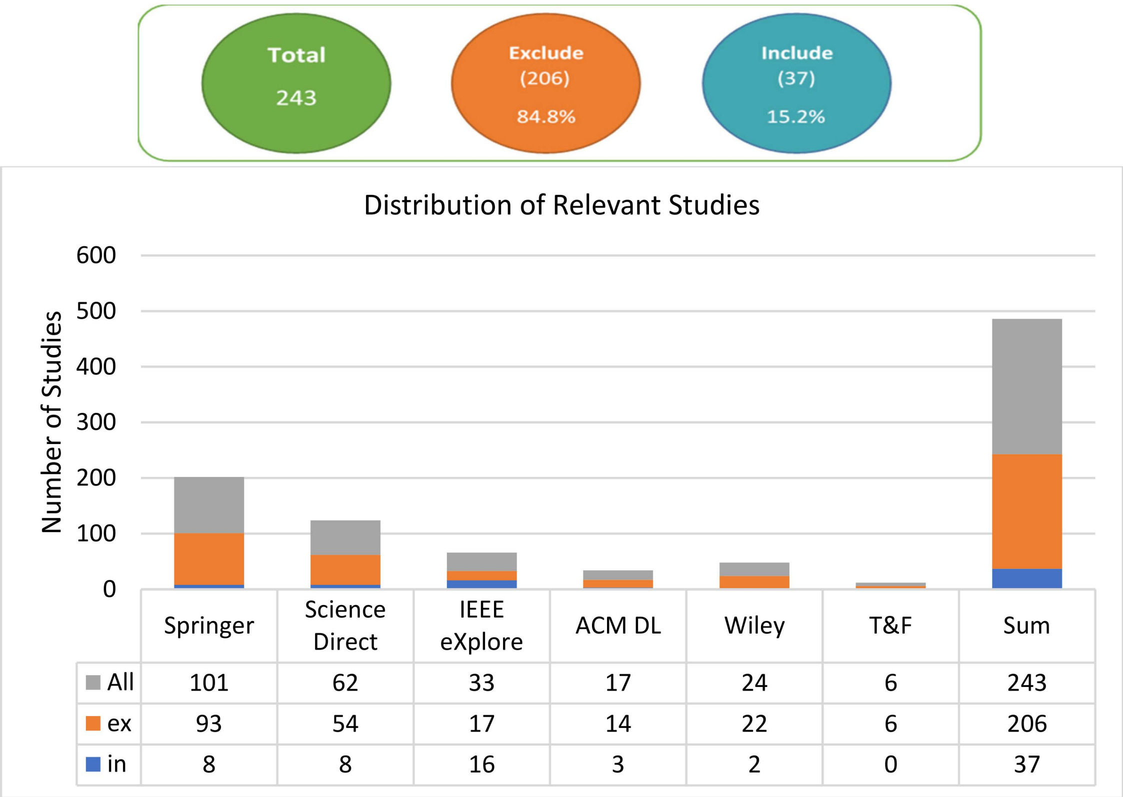
Table 5. Inclusion and exclusion criteria for studies.

Including Criteria	Excluding Criteria
• Methods, techniques and model for detecting botnet in IoT environment	• Methods, techniques and model for detecting botnet in general environment
• Include Technical studies to detect IoT botnet	• Exclude studies that related to Detection but not related to IoT botnet
• Include studies that published between (1 January 2016 to 1 January 2020)	• Exclude studies that related to IoT botnet but not related to Detection
• Include the studies published in English in electronic copy	• Exclude survey, review and chapters studies
• Include the newest version of studies if more than one available	• Exclude non-conference and non-journal studies
• "IoT Botnet" or "IoT Malware" in the paper title	• Exclude books, book chapter, posters, workshops and theses

4.2.3. Step 3: Quality Assessment

The goal of the quality assessment was to rate the selected articles depending on the quality assessment rules below. The assessment was based on relevance to research questions, research quality and the presence of recommendations for research opportunities and future work. The authors used a scale of 1–10 for each paper: The authors gave a score for each research paper for each criterion (0, 0.5, 1). The scores had the following scale: 1 means the paper fully answered the assessment rule (AR), 0.5 means the paper partially answered the assessment rule and 0 means the paper did not answer the assessment rule. If the paper earned 5 or more, then it was used. The scoring results are shown in Table 7. The following are the assessment rules:

AR1: Was the research objective set clearly?
AR2: Has the study been referenced by another paper?
AR3: Does the study explain a specific phase of an IoT botnet obviously?
AR4: Does the study explain a specific malicious activity scenario?
AR5: Was the design of the experiment reasonable?
AR6: Was the experiment conducted on a sufficient IoT dataset?
AR7: Was the design justification of the proposed technique/method identified?
AR8: Was the proposed technique/method compared to others?
AR9: Were the results of the test well evaluated?
AR10: Was there proof that the method of interest improved the results?



	Springer	Science Direct	IEEE eXplore	ACM DL	Wiley	T&F	Sum
■ All	101	62	33	17	24	6	243
■ ex	93	54	17	14	22	6	206
■ in	8	8	16	3	2	0	37

Figure 6. Number of studies distributed through search sources.

Table 6. The studies selected after filtering.

SID	Authors	Title	Year	Publisher	References
S01	Prokofiev, Anton O., Yulia S. Smirnova, and Vasiliy A. Surov	A method to detect Internet of Things botnets	2018	IEEE	[45]
S02	McDermott, Christopher D., Farzan Majdani, and Andrei V. Petrovski	Botnet detection in the internet of things using deep learning approaches	2018	IEEE	[46]
S03	Vishwakarma, Ruchi, and Ankit Kumar Jain	A Honeypot with Machine Learning based Detection Framework for defending IoT based botnet DDoS Attacks	2019	IEEE	[47]
S04	Tzagkarakis, Christos, Nikolaos Petroulakis, and Sotiris Ioannidis	Botnet Attack Detection at the IoT Edge Based on Sparse Representation	2019	IEEE	[48]
S05	Nguyen, Huy-Trung, Quoc-Dung Ngo, and Van-Hoang Le	IoT botnet detection approach based on PSI graph and DGCNN classifier	2018	IEEE	[49]

Table 6. *Cont.*

SID	Authors	Title	Year	Publisher	References
S06	Meidan, Yair, Michael Bohadana, Yael Mathov, Yisroel Mirsky, Asaf Shabtai, Dominik Breitenbacher, and Yuval Elovici	N-baiot—Network-based detection of Iot botnet attacks using deep autoencoders	2018	IEEE	[50]
S07	Nõmm, Sven, and Hayretdin Bahşi	Unsupervised anomaly based botnet detection in IoT networks	2018	IEEE	[51]
S08	Kumar, Ayush, and Teng Joon Lim	Edima: early detection of IoT malware network activity using machine learning techniques	2019	IEEE	[52]
S09	Liu, Junyi, Shiyue Liu, and Sihua Zhang	Detection of IoT botnet Based on Deep Learning	2019	IEEE	[53]
S10	Bahşi, Hayretdin, Sven Nõmm, and Fabio Benedetto La Torre	Dimensionality reduction for machine learning based IoT botnet detection	2018	IEEE	[54]
S11	Li, Wanting, Jian Jin, and Jong-Hyouk Lee	Analysis of botnet Domain Names for IoT Cybersecurity	2019	IEEE	[55]
S12	Nguyen, Huy-Trung, Doan-Hieu Nguyen, Quoc-Dung Ngo, Vu-Hai Tran, and Van-Hoang Le	Towards a rooted subgraph classifier for IoT botnet detection	2019	ACM	[56]
S13	Alazzam, Hadeel, Abdulsalam Alsmady, and Amaal Al Shorman	Supervised detection of IoT botnet attacks	2019	ACM	[57]
S14	Salim, Mikail Mohammed, and Jong Hyuk Park	Deep Learning Based IoT Re-authentication for botnet Detection and Prevention	2019	Springer	[58]
S15	Nguyen, Huy-Trung, Quoc-Dung Ngo, and Van-Hoang Le	A novel graph-based approach for IoT botnet detection	2019	Springer	[59]
S16	Al Shorman, Amaal, Hossam Faris, and Ibrahim Aljarah	Unsupervised intelligent system based on one class support vector machine and Grey Wolf optimization for IoT botnet detection	2019	Springer	[60]
S17	Javed, Yousra, and Navid Rajabi	Multi-Layer Perceptron Artificial Neural Network Based IoT botnet Traffic Classification	2019	Springer	[61]
S18	Koroniotis, Nickolaos, Nour Moustafa, Elena Sitnikova, and Jill Slay	Towards developing network forensic mechanism for botnet activities in the iot based on machine learning techniques	2017	Springer	[62]
S19	Shire, Robert, Stavros Shiaeles, Keltoum Bendiab, Bogdan Ghita, and Nicholas Kolokotronis	Malware Squid: A Novel IoT Malware Traffic Analysis Framework Using Convolutional Neural Network and Binary Visualisation	2019	Springer	[63]
S20	Habib, Maria, Ibrahim Aljarah, Hossam Faris, and Seyedali Mirjalili	Multi-objective Particle Swarm Optimization for botnet Detection in Internet of Things	2020	springer	[64]
S21	Jung, Woosub, Hongyang Zhao, Minglong Sun, and Gang Zhou	IoT botnet detection via power consumption modeling	2020	Science Direct	[65]
S22	Koroniotis, Nickolaos, Nour Moustafa, Elena Sitnikova, and Benjamin Turnbull	Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset	2019	Science Direct	[66]
S23	Nguyen, Huy-Trung, Quoc-Dung Ngo, Doan-Hieu Nguyen, and Van-Hoang Le	PSI-rooted subgraph: A novel feature for IoT botnet detection using classifier algorithms	2020	Science Direct	[37]

Table 6. *Cont.*

SID	Authors	Title	Year	Publisher	References
S24	Shafiq, Muhammad, Zhihong Tian, Yanbin Sun, Xiaojiang Du, and Mohsen Guizani	Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city	2020	Science Direct	[67]
S25	Pour, Morteza Safaei, Antonio Mangino, Kurt Friday, Matthias Rathbun, Elias Bou-Harb, Farkhund Iqbal, Sagar Samtani, Jorge Crichigno, and Nasir Ghani	On data-driven curation, learning, and analysis for inferring evolving internet-of-Things (IoT) botnets in the wild	2020	Science Direct	[68]
S26	Karanja, Evanson Mwangi, Shedden Masupe, and Mandu Gasennelwe Jeffrey	Analysis of internet of things malware using image texture features and machine learning techniques	2020	Science Direct	[69]
S27	Spaulding, Jeffrey, Jeman Park, Joongheon Kim, DaeHun Nyang, and Aziz Mohaisen	Thriving on chaos: Proactive detection of command and control domains in internet of things-scale botnets using DRIFT	2019	Willey	[70]
S28	Sagirlar, Gokhan, Barbara Carminati, and Elena Ferrari	AutoBotCatcher: blockchain-based P2P botnet detection for the Internet of Things	2018	IEEE	[71]
S29	Falco, Gregory, Caleb Li, Pavel Fedorov, Carlos Caldera, Rahul Arora, and Kelly Jackson	Neuromesh: Iot security enabled by a blockchain powered botnet vaccine	2019	ACM	[72]
S30	Ozawa, Seiichi, Tao Ban, Naoki Hashimoto, Junji Nakazato, and Jumpei Shimamura	A study of IoT malware activities using association rule learning for darknet sensor data	2020	Springer	[73]
S31	Hashimoto, Naoki, Seiichi Ozawa, Tao Ban, Junji Nakazato, and Jumpei Shimamura	A darknet traffic analysis for IoT malwares using association rule learning	2018	Science Direct	[74]
S32	Özçelik, Mert, Niaz Chalabianloo, and Gürkan Gür	Software-defined edge defense against IoT-based DDoS	2017	IEEE	[75]
S33	Yin, Lihua, Xi Luo, Chunsheng Zhu, Liming Wang, Zhen Xu, and Hui Lu	ConnSpoiler: Disrupting C&C Communication of IoT-Based botnet through Fast Detection of Anomalous Domain Queries	2019	IEEE	[76]
S34	Sajjad, Syed Muhammad, and Muhammad Yousaf	UCAM: usage, communication and access monitoring based detection system for IoT botnets	2018	IEEE	[77]
S35	Hu, Jen-Wei, Lo-Yao Yeh, Shih-Wei Liao, and Chu-Sing Yang	Autonomous and malware-proof blockchain-based firmware update platform with efficient batch verification for Internet of Things devices	2019	Science Direct	[78]
S36	Sun, Hao, Xiaofeng Wang, Rajkumar Buyya, and Jinshu Su	CloudEyes: Cloud-based malware detection with reversible sketch for resource-constrained internet of things (IoT) devices	2017	Willey	[79]
S37	Giachoudis, Nikolaos, Georgios-Paraskevas Damiris, Georgios Theodoridis, and Georgios Spathoulas	Collaborative Agent-based Detection of DDoS IoT botnets	2019	IEEE	[80]

Table 7. Assessment scores for selected studies (1 = fully answered, 0.5 = partially answered and 0 = not answered).

Study ID	Assessment Rules										Total
	AR1	AR2	AR3	AR4	AR5	AR6	AR7	AR8	AR9	AR10	
S01	1.0	0.5	1.0	0.5	0.5	0.5	1.0	0.0	1.0	0.0	6.0
S02	1.0	0.5	0.5	1.0	1.0	0.5	1.0	0.5	0.5	0.5	7.0
S03	0.5	0.5	0.5	0.5	1.0	1.0	1.0	0.0	0.0	0.0	5.0
S04	0.5	0.5	0.5	0.5	0.5	1.0	1.0	1.0	0.5	0.5	6.5
S05	1.0	0.5	1.0	0.5	1.0	1.0	1.0	0.5	1.0	1.0	8.5
S06	1.0	1.0	1.0	1.0	1.0	1.0	1.0	0.0	1.0	1.0	9.0
S07	0.5	0.5	0.5	0.5	1.0	1.0	1.0	0.5	0.0	0.0	5.5
S08	1.0	0.5	0.5	0.5	1.0	0.5	1.0	0.0	1.0	1.0	7.0
S09	1.0	0.5	0.5	0.5	1.0	1.0	1.0	1.0	1.0	1.0	8.5
S10	1.0	0.5	0.5	0.5	1.0	1.0	1.0	0.0	1.0	1.0	7.5
S11	0.5	0.5	0.5	0.5	1.0	0.5	1.0	0.5	0.0	0.0	5.0
S12	1.0	0.5	1.0	0.5	1.0	1.0	1.0	1.0	1.0	1.0	9.0
S13	0.5	0.5	0.5	0.5	1.0	1.0	1.0	0.0	1.0	1.0	7.0
S14	1.0	0.0	0.5	0.5	1.0	0.0	1.0	0.0	0.0	0.0	4.0
S15	0.5	0.5	1.0	0.5	1.0	1.0	1.0	0.5	1.0	1.0	8.0
S16	1.0	0.5	0.5	0.5	1.0	1.0	1.0	1.0	1.0	1.0	8.5
S17	1.0	0.0	0.5	0.5	1.0	0.5	1.0	0.0	1.0	1.0	6.5
S18	0.5	0.5	0.5	0.5	1.0	1.0	1.0	1.0	1.0	1.0	8.0
S19	0.5	0.5	0.5	0.5	1.0	0.5	1.0	1.0	1.0	1.0	7.5
S20	0.5	0.5	0.5	0.5	1.0	1.0	1.0	1.0	0.0	0.0	6.0
S21	1.0	0.5	0.5	0.5	1.0	0.5	1.0	1.0	1.0	1.0	8.0
S22	1.0	1.0	0.5	1.0	1.0	1.0	1.0	0.5	1.0	1.0	9.0
S23	1.0	0.5	1.0	0.5	1.0	1.0	1.0	1.0	1.0	1.0	9.0
S24	1.0	0.5	0.5	0.5	1.0	1.0	1.0	0.5	1.0	1.0	8.0
S25	1.0	0.5	0.5	0.5	1.0	1.0	1.0	0.5	1.0	1.0	8.0
S26	1.0	0.5	1.0	1.0	1.0	1.0	1.0	0.5	1.0	1.0	9.0
S27	0.5	0.5	0.5	0.5	1.0	1.0	1.0	0.5	1.0	1.0	7.5
S28	1.0	0.5	1.0	0.5	1.0	0.0	1.0	0.0	0.0	0.0	5.0
S29	0.5	0.5	0.5	0.5	1.0	0.0	1.0	0.0	0.0	0.0	4.0
S30	0.5	0.5	0.5	0.5	0.5	0.5	1.0	0.0	1.0	1.0	6.0
S31	0.5	0.5	0.5	0.5	0.5	1.0	1.0	0.0	0.5	0.5	5.5
S32	1.0	1.0	0.5	0.5	0.5	0.0	1.0	0.0	0.0	0.0	4.5
S33	1.0	0.5	0.5	0.5	0.5	1.0	1.0	1.0	1.0	1.0	8.0
S34	1.0	0.5	0.5	1.0	0.5	0.0	1.0	0.0	0.5	0.5	5.5
S35	0.5	0.5	0.5	0.5	1.0	0.0	1.0	1.0	0.0	0.0	5.0
S36	1.0	1.0	1.0	1.0	0.5	0.0	1.0	1.0	1.0	1.0	8.5
S37	1.0	0.5	0.5	1.0	0.5	0.0	1.0	0.0	1.0	1.0	6.5
Total	**30.0**	**19.5**	**23.0**	**22.0**	**32.5**	**25.0**	**37.0**	**17.0**	**26.0**	**25.0**	**AVG = 6.9**

4.2.4. Step 4: Data Extraction and Synthesis

The purpose of this phase was to gather the needed data. We collected the data provided in Table 8 from each study in order to address the research questions.

Table 8. A comparison of the methods used for the selected studies.

Ref	Publisher	Entity Detected	Detection Methods	Dataset	Evaluation Measurement	Botnet Phase	Malicious Activities
S01	IEEE	device	logistic regression model	100 botnets device	97.3%	propagation	IoT botnet
S02	IEEE	Malicious traffic	unidirectional LSTM-RNN and Bidirectional Deep BLSTM-RNN	Simulated using 3 servers and 2 cameras	99%	attack	DDoS
S03	IEEE	Malicious traffic	Machine Learning, not specified	Collected from honeypot: ThingPot + simulated data	Not mentioned, proposal	Attack	zero day DDoS
S04	IEEE	device	sparsity representation, thresholding rule	N-BaIoT	better than single hidden layer autoencoder	Attack	IoT botnet
S05	IEEE	Malware file	DG-CNN convolutional neural network	IOTPOT + collected benign ELF	Accuracy of 92% and a F-measure of 94%.	propagation	IoT malware
S06	IEEE	device	Deep Autoencoder	N-BaIoT,9 devices in lab	FPR of zero	Attack	IoT botnet
S07	IEEE	malicious traffic	Support Vector Machine (SVM), Isolated Forest	balanced N-BaIoT	More than 90%	Attack	IoT botnet
S08	IEEE	malicious traffic	Random Forest, k-Nearest Neighbors (k-NN), Gaussian Naive Bayes	Stored scanned patterns	Accuracy = 77.5%, 94, 88.5%, F1-score = 0.96	Scanning	Scan Attack
S09	IEEE	malicious traffic	convolutional neural network (CNN)	N-BaIoT	accuracy of 99.57%	Attack	IoT botnet
S10	IEEE	malicious traffic	Decision Tree, k-Nearest Neighbors (k-NN), Dimensionality Reduction	N-BaIoT	accuracy = 0.98, 0.94	Attack	IoT botnet
S11	IEEE	C&C domain name, IP queries	Adaboost, Bagging, Naive Bayes and k-Nearest Neighbors (kNN)	collect the DNS querying log data	KNN, Precision, Recall, F-Measure, ROC Area = 1	Attack	IoT botnet
S12	ACM	malware file	Random Forest (RF), Bagging, Radial Basis Function Support Vector Machine RBF SVM, Decision Tree.	VirusShare and IoTPOT, 9943 ELF samples	accuracy = 97%, F-score = 98%	propagation	IoT malware
S13	ACM	malicious traffic	Naive Bayes, K Nearest Neighbors (KNN), and Random Forest	Subset of N-BaIoT	99% TPR, 100% TNR, and near-zero false alarms	attack	IoT botnet

Table 8. *Cont.*

Ref	Publisher	Entity Detected	Detection Methods	Dataset	Evaluation Measurement	Botnet Phase	Malicious Activities
S14	Springer	device	Deep Learning + Software Defined Network (SDN)	no implementation	no implementation	Scanning	IoT botnet
S15	Springer	malware file	PSI Graph, graph2Vec using convolutional neural network (CNN)	11,200 ELF files	accuracy of 98.7%,	propagation	IoT malware
S16	Springer	malicious traffic	One Class Support vector machine (OCSVM),Grey Wolf Optimization (GWO)	N-BaIoT	96–99%	Attack	IoT botnet
S17	Springer	malicious traffic	the Multi-Layer Perceptron (MLP) Artificial Neural Network (ANN)	subset for 2 devices of N-BaIoT dataset	100%	Attack	IoT botnet
S18	Springer	malicious traffic	Decision Tree C4.5 (DT), Association Rule Mining (ARM), Artificial Neural Network (ANN) and Naïve Bayes (NB)	USNW-NB15, KDD99	93% for DT	Attack	IoT botnet
S19	Springer	malicious traffic	convolutional neural network (CNN)	collected 100 pcap from repositories.	96% for botnet and 89% for DDoS	attack	IoT malware
S20	springer	malicious traffic	k-Nearest Neighbors (K-NN)	5 datasets from N-BaIoT	100%	Attack	IoT botnet
S21	Science Direct	malicious behavior	convolutional neural network (CNN)	collected power consumption data	Accuracy = 96.5%	Attack	IoT botnet
S22	Science Direct	malicious traffic	Support Vector Machine (SVM), Short Term Memory Recurrent Neural Network (LSTM-RNN), RNN	BoT-IoT	Accuracy for SVM = 99%	Attack	DoS/DDoS
S23	Science Direct	malware file	Random Forest, Decision Tree, Bagging, k-NN, SVM	IoTPOT, VirusShare	97% true positive rate, RF	propagation	IoT malware
S24	Science Direct	malicious traffic	Naïve Bayes, Bayes Net, C4.5 decision tree, Random Forest	Bot-IoT	acc = 99.99 for random tree	Attack	IoT botnet
S25	Science Direct	device	convolutional neural network (CNN)	Collected dataset consisted of 34,974 IoT and 7193 non-IoT.	no. of compormised device = 400.000	scanning	Scan Attack
S26	Science Direct	malware file	KNN, naïve Bayes and random forest	IoTPOT	95% accuracy for Random Forest	propagation	IoT malware
S27	Willey	C2 domain name	nearest centroid neighborhood (NCN) classifier	99%	N/A	Attack	IoT botnet

Table 8. *Cont.*

Ref	Publisher	Entity Detected	Detection Methods	Dataset	Evaluation Measurement	Botnet Phase	Malicious Activities
S28	IEEE	device	blockchain	N/A	N/A	propagation	IoT botnet
S29	ACM	IP address	neural network, Blockchain	not mentioned	not mentioned	attack	IoT botnet
S30	Springer	device	Association rule	collected from darknet	N/A	scanning	Scan Attack
S31	Science Direct	TCP SYN packets	Association Rule Learning	1,840,973,403 packets	not specified	scanning	scan attack
S32	IEEE	malicious traffic	Software Defined Network (SDN)	not specified	N/A	Attack	DDoS
S33	IEEE	C2 domain name	Threshold Random Walk (TRW)	94%	DNS traffic generated by 19 different botnet	Attack	IoT botnet
S34	IEEE	malicious traffic	defined policies on SIEM	compare Usage, Contact and Access Monitoring	Not specified	attack	DDoS
S35	Science Direct	device	blockchain-based	N/A	N/A	scanning	scan
S36	Willey	malware file	signature based anti-malware	N/A	460,000 to 3,700,000 signature	propagation	IoT malware
S37	IEEE	malicious traffic	traffic profile	N/A	N/A	Attack	DDoS

5. Analysis

Having explained in depth the methodology for this research in the previous section, we can now present the analysis in this section, as per the three research questions previously identified. The research questions are addressed in Section 5.1, Section 5.2 and Section 5.3, respectively.

5.1. RQ1: What Are the Different Phases of Forming an IoT Botnet?

One of the major motivations of cybercriminals, when taking over IoT devices, is to use the devices as parts of botnets. As we mentioned in Section 3, an IoT botnet is a network comprising infected IoT devices controlled by malicious software named a bots. Cyber criminals have the ability to use special software to circumvent detection and intrusion prevention systems. They can obtain illegal access and control IoT devices to incorporate them into global networks called botnets that can be controlled remotely. The An IoT botnet is created in a series of phases, as seen in Figure 3. In the studies we selected, researchers chose different numbers of the phases for forming IoT botnets. They considered the process to have three phases, four phases, five phases or seven phases. The reasons for the different numbers of phases could have been the researchers wanting to put more emphasis on certain events and wanting to be more detailed. Phases help create models for protective methods. For example, in [81] the authors considered that IoT botnets have seven phases: (1) Searching the (inter)network for open ports on connected devices. (2) Brute force attacks on the exposed ports to obtain access to the victims. (3) Killing possible competitors on infected hosts. (4) Building a channel to the botmaster (command and control (C&C) channel). (5) Running a malicious script (and sometimes removing others) in the RAM. (6) Spreading across the network by looking for new instances. (7) Initiating attacks or executing other malicious acts.

In article [45], the authors considered that an IoT botnet goes through five phases—namely, initial infection, secondary infection, communication, malicious activity, upgrade and maintenance. Initial infection: Compromising an exposed device. Secondary infection: Downloading malware which will communicate with a botmaster. Communication: Connecting to the command and control server (C&C) to receive commands from the botmaster. Malicious activity: Performing malice acts upon the directives of the botmaster (DDoS, scams, etc.). Upgrade and maintenance: Efficiently observing contaminated hosts whenever possible, adapting their behavior through downloading malicious code updates. In the same context, article [57] considered IoT botnets to have four phases—specifically, scanning, attack, infection and violation. In the scanning phase, the botmaster orders the bots to scan for exposed IoT devices on the Internet that have available ports for Telnet services or other services. In the attack phase, the successful login credentials for the new IoT system (cracked via brute force attack with a list of established default credentials) are sent to the C&C. Infection is when the infected device is directed to transfer and run the conformable payload binary. Some malware is extremely aggressive and will try to delete other malware found on the device. When run, the binary malware will be deleted and will only run in RAM to prevent detection. In the violation phase, the IoT botnet will be used for mounting a DDoS attack, i.e., via HTTP, UDP floods, etc. Other research, such as [82], in the same manner considered the IoT botnet's lifecycle to be composed of four phases: formation, control and compromise, attack, and post attack. The first phase of the bot is the discovery of a vulnerability in the target system. The vulnerability is abused in the next step and the host is compromised. The host then provides access to targeted device to the botmaster. Then, the bot will install some binary or executable files that are malicious, and in this process, the target machine will turn into an infected device, i.e., a bot. The final phase is a protective phase, during which the bot uses a technique to counter detection or removal. In addition, the authors in [51] divided the IoT botnet into four phases—formation, command and control, attack and post attack. Likewise, in the article [83], the authors divided IoT botnets into four different phases as follows: selection of the target; device fingerprinting and infection; detection of avoidance and persistence; and activation. In a different manner, [84] considered that IoT botnets have three phases: host scanning, system acquisition and service attack denial.

In summary and from the above, it can be noted that each study divided the phases of development for a botnet in a different way. They provided acceptable phases based on the objectives of the solutions proposed, which could be the discovery of the malware file, the discovery of suspicious activities carried out by the botnet or the discovery of the devices attached to the botnet.

As seen in Figure 7, the results show that most of the selected studies, approximately 62%, concentrated on proposing solutions for detecting the IoT botnet in the attack phase, which is considered a late phase in the IoT botnet's lifecycle. Only 16% of the selected studies focused on proposing solutions for detection in the scanning phase, and 22% focused on the propagation phase for their solutions. Thus, fewer papers concentrated on detection in the early phases. Hence, it appears that there is little interest in the early stages. Table 9 displays the numbers of studies that focused on the various phases of IoT botnet development.

Table 9. Numbers of studies focusing on the different phases of IoT botnet development.

Phase of Botnet	Number of Studies
Scanning	6
Propagation	8
Attack	23
Sum	37

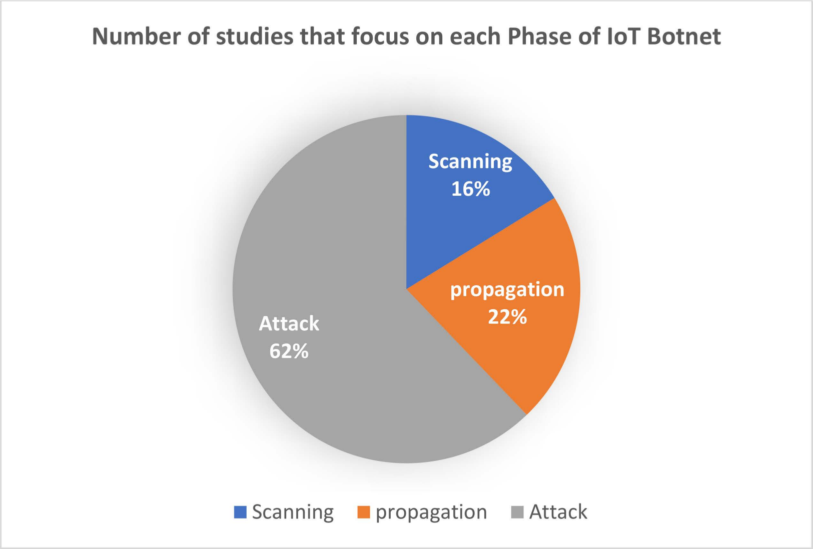


Figure 7. Percentages of studies focusing on the different phases of IoT botnet development.

Finally, we believe that the most appropriate for proposing a solution of detection the IoT botnet is detecting the IoT botnet in the early phase of the lifecycle i.e., Scanning and Propagation, since that the IoT botnet in these phases does not start their harm activities.

5.2. *RQ2: What Types of Malicious Activity and Which Scenarios Involve IoT Botnets?*

Regarding to the second research question in this study, which is to deliver the types and scenarios of attacks that using IoT botnet and have been studies by the selected studies. From this review, and after analyzing all the selected studies, it can be found out that they dealt with four types of attacks or malicious activities, which are IoT botnet, DoS/DDoS, scanning attack and analyzing IoT malwares. In this section, we will explain the types and scenario of attacks that investigated by the selected studies. Table 10 displays these types.

Table 10. Number of studies found by type of malicious activity.

Malicious Activities	Number of Studies
IoT botnet	19
IoT malware	7
DoS/DDoS	6
Scan	5
Sum	37

5.2.1. Forming an IoT Botnet

The majority of chosen studies targeted IoT botnets by their malicious activities. As explained before, cybercriminals try in the propagation phase to rally as many compromised devices as possible to expand their botnets. As has been stated in Section 3.3.3, IoT botnets are remotely managed through command and control channels to trigger different malicious activities, for example, DDoS attacks, sensitive data theft, phishing [85] or mining of cryptocurrency. An attacker that gains access to a network and gets control, spreads his malware by exploiting the IoT devices. Different vulnerabilities in IoT environments facilitate the process of forming IoT botnets. Cyber criminals are monetizing IoT botnets by actually selling them to interested customers and offering them as a service. Therefore, in the coming years, IoT botnets will continue to be a part of the threat landscape. According to the studies selected in this SLR, most research focuses on solutions for detecting IoT botnets through detecting the malicious devices. As Figure 8 explains, 51% of the studies concentrated recruitment activity—19 studies, as Table 10 displays. Some of those studies are [45,71,73].

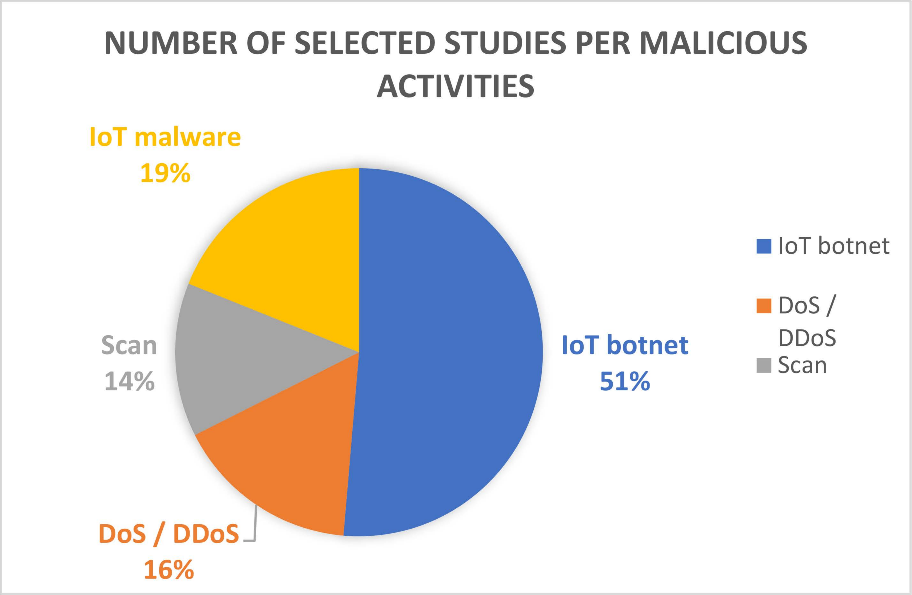


Figure 8. Number of studies selected per malicious activity.

5.2.2. Downloading IoT Malware

IoT malware is malicious software designed to access, exploit and compromise an IoT device; it is different from other malware in that it has the ability to adapt to various CPU architectures, including MIPS, ARM, Intel x86 and PowerPC [56]. IoT malware has various essential models to finish its functions, including a scanner, an attacker and a killer [86]. After scanning and receiving the information of a vulnerable IoT device, the attacker uses a downloader server to download the bot. After that, the new bot starts its functions and communication with the C&C. Some of the selected studies concentrated on proposing techniques for detecting whether an input executable file is malware or benign [49,56,69,79]. As Figure 8 explained, 19% of the studies concentrated on this type of attack—nine studies, as Table 10 displays.

5.2.3. Denial of Service (DoS/DDoS) Attacks

The aim of a DDoS attack is to harm, collapse or close down a service or to block the benign users from using said service by employing many previously infected sources. An attacker aims to make the target inaccessible by overwhelming its resources with a large volume of traffic using IoT devices [87]. A large number of DDoS attack botnets are employed to start an attack, once the compromised devices are usable. If the DDoS attack is not discovered and avoided, the DDoS will flood the target with illegitimate requests and reject the requests of the authentic users [88]. DDoS is one of the types of attack that has been a significant challenge in the IoT environment. It comes in different types: flooding attacks (e.g., UDP flood or HTTP flood), amplification and IP spoofing, selective forwarding, hello floods, overloading, sinkholes, wormhole attacks, packet fragmentation attacks, exhaustive attacks and jamming attacks [89]. Figure 9 explains the DDoS attack mechanism. Throughout DDoS attacks, the attacker utilizes a command mechanism to exploit and compromise other devices by imposing malicious code on them and creating a dispersed network of controlled IoT devices. As Figure 8 explains, 16% of the studies concentrated on this type of attack—six studies, as Table 10 displays [46,47,63,66,74,77,80].

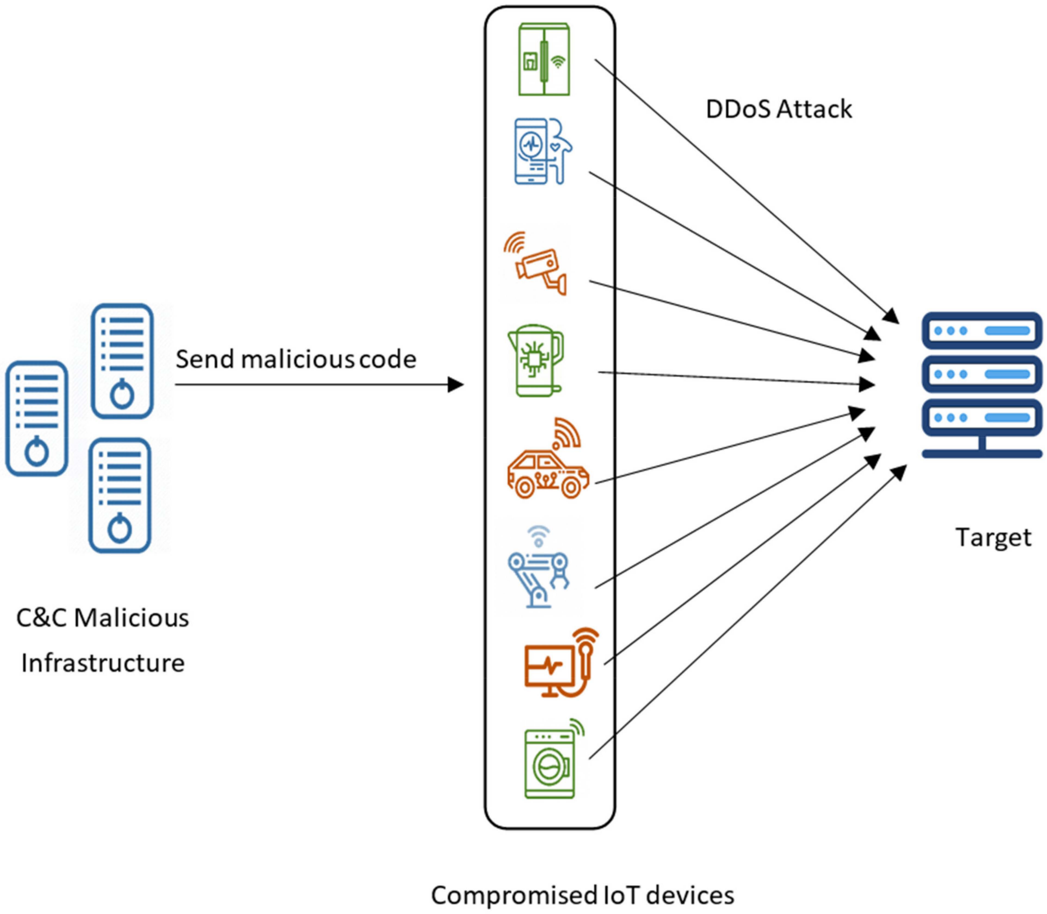


Figure 9. The mechanism of DDoS.

5.2.4. Scanning Attacks

In this type of attack, the cybercriminal illegally scans the IoT devices in a network to gather information about them prior to launching sophisticated attacks. For example, they send packets by bots to find out whether a specific port is open on the device and return the information back to the botmaster to take the advantage of this information to exploit this device. In the literature, some studies analyzed scanning techniques to identify coordinated IoT campaigns that sought open ports that could be exploited for amplification attacks [90]. Others checked for updates and applied patches for device software to be proactive, as this prevents vulnerabilities from being discovered by attackers [91]. Finally, [92] proposed a solution that detects port scanning behavior. Some of the selected studies focused on bots scanning for vulnerable devices [52], whereas the article [74] analyzed the Dark Web to detect the scanning activities of IoT botnets. As Figure 8 explained, 14% of studies concentrated on this type of attack—five studies, as Table 10 displays. Some of the selected studies that focused on this attack are [52,74,78].

5.3. RQ3: What Methods and Techniques Are Utilized to Detect IoT Botnets?

As shown in Figure 10, the revised selection of studies from 2016 to 2020 that used various methods to detect IoT botnets numbered, on average, 7.5 each year. In the following section, we discuss the methods and techniques that have been used, and we summarize the relevant studies for each method according to categories of methods.

In the overview, we concentrate on the concept behind each approach; the dataset used, if any; the outcome; the deficiencies, if found; and the standing in comparison to other studies. For the analysis, we classified the selected studies into a few main categories according to the methods proposed by the studies, as shown in Table 11. It explains these categories and the number of selected studies per category.

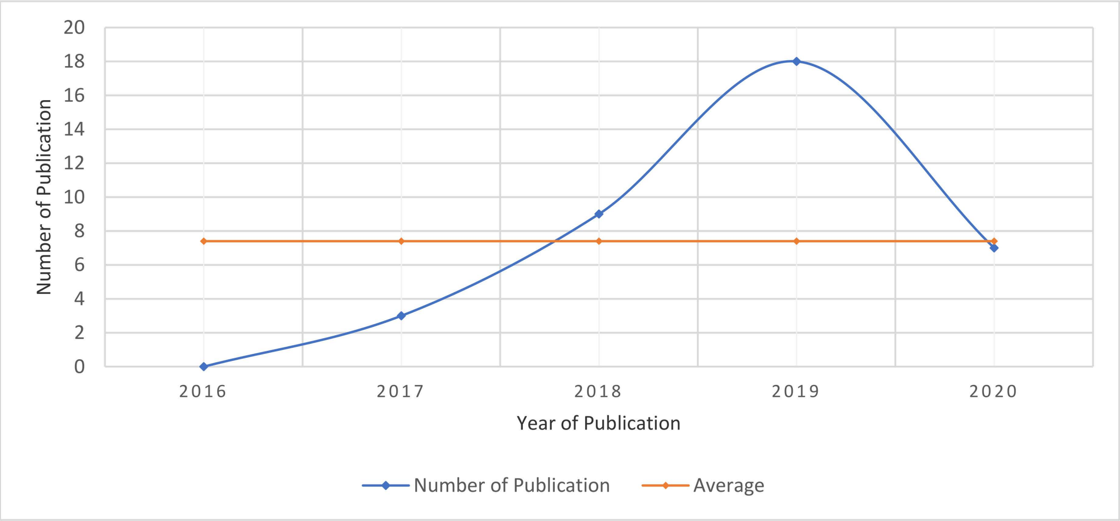


Figure 10. Number of publications per year.

Table 11. Number of studies selected per detection method.

	Type of Used Method	Number of Studies	References
1	AI Supervised Learning	15	[37,45,48,51,52,54–57,61,62,64,67,69,70]
2	AI Unsupervised Learning	3	[60,73,74]
3	AI Deep Learning	11	[46,47,49,50,53,58,59,63,65,66,68]
4	Blockchain based	3	[71,72,78]
5	SDN based	1	[75]
6	Specification based	3	[76,77,80]
7	Signature based	1	[79]
	Sum	37	-

It is worth noting that most of the studies relied on artificial intelligence to suggest solutions for the problem of detecting botnets in the Internet of Things—78% of the studies. Figure 11 shows the percentage of selected studies per category.

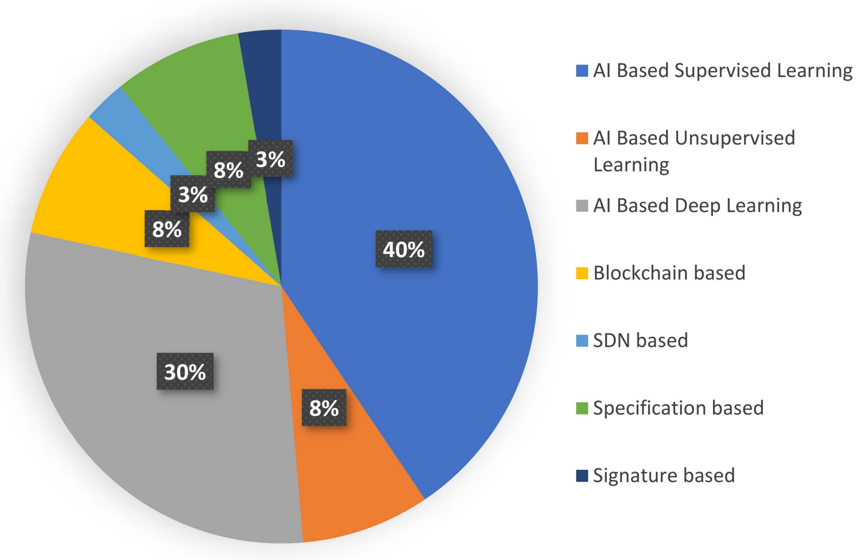


Figure 11. Number of selected studies per detection method.

In the following sections, we describe these methods and describe the relevant selected studies. Figure 12 explains these methods' categories.

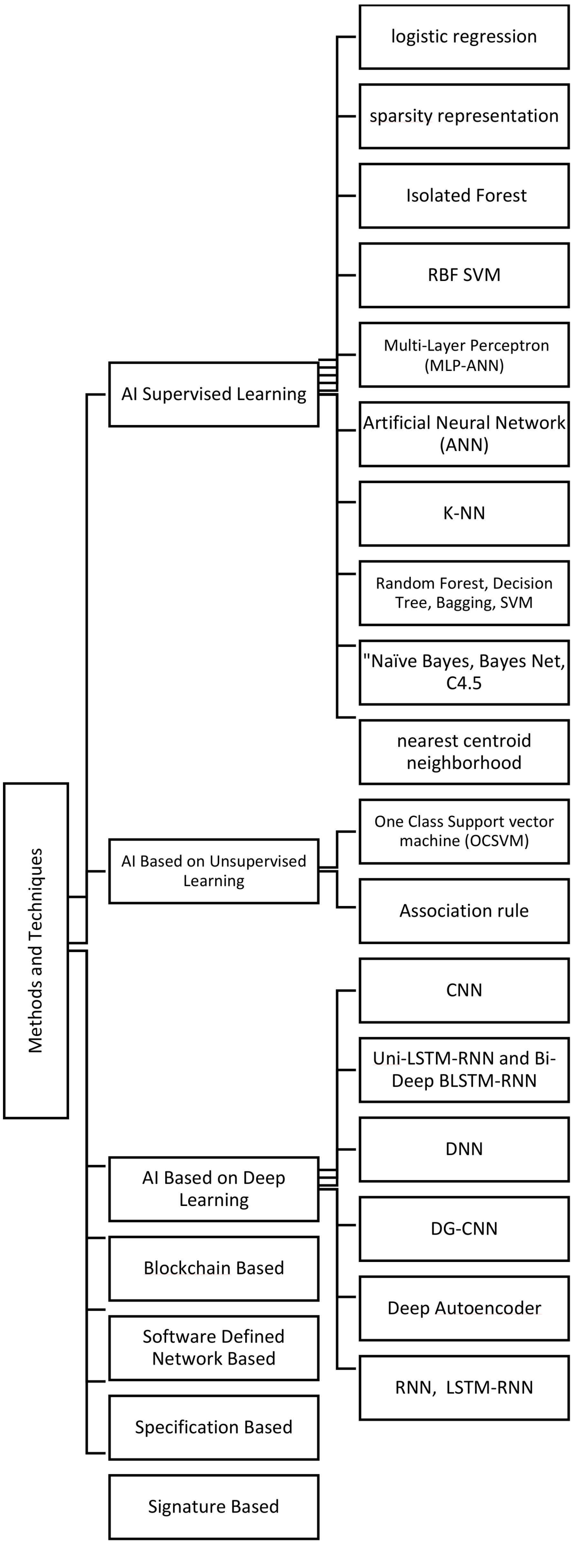

Methods and Techniques
AI Supervised Learning
logistic regression
sparsity representation
Isolated Forest
RBF SVM
Multi-Layer Perceptron (MLP-ANN)
Artificial Neural Network (ANN)
K-NN
Random Forest, Decision Tree, Bagging, SVM
"Naïve Bayes, Bayes Net, C4.5
nearest centroid neighborhood
AI Based on Unsupervised Learning
One Class Support vector machine (OCSVM)
Association rule
AI Based on Deep Learning
CNN
Uni-LSTM-RNN and Bi-Deep BLSTM-RNN
DNN
DG-CNN
Deep Autoencoder
RNN, LSTM-RNN
Blockchain Based
Software Defined Network Based
Specification Based
Signature Based

Figure 12. Methods and techniques extracted from the selected studies.

5.3.1. Methods Based on Artificial Intelligence Algorithms

This section reviews the suggested approaches that depend on artificial intelligence algorithms (AI) for detecting IoT botnets. The concept behind AI and its branches, machine learning and deep learning, is providing an algorithm that can analyze information and recognize patterns, and thereby construct a model that could be used by the machine to analyze information that it has not seen before. The algorithm learns continuously and should be able to make reliable decisions repeatedly as systems provide more data to it [93]. The selected studies used different AI algorithms and different datasets, as explained in this section.

AI-Based Supervised Learning

One article [45] suggested a method for distinguishing IoT botnets at the propagation phase, i.e., when compromised devices (bots) that are a portion of a botnet infect other devices to expand the botnet. The method is based on a logistic regression model. The paper describes an established logistic regression model that allows the likelihood of a bot being run by a system initiating a connection to be calculated. A list of network protocols that are employed to gain illegal access to devices and get commands from a command and control server is also given. The model given is appropriate for the detection of botnets propagated by brute force attacks exploiting the Telnet and SSH services.

The authors in [48] suggested a method of rapid detection of IoT botnet attacks based on a small number of benign instances for training and a single malicious instance for detection. The experimental evaluation showed that regarding to F1 ratings, detection rate and precision, the suggested method performed better than the autoencoder. They presented a diagnostic approach for instantaneous IoT botnet attack detection with the ultimate goal of minimizing the impacts of the attacks through instant quarantining of infected IoT devices placed at the IoT edge. They were highly concerned with delivering an efficient IoT botnet attack detector that uses as little training and testing data as possible, because of the restricted computational resources that regulate IoT devices on the edge. They believe that no preceding knowledge of untrustworthy traffic on an IoT network is needed in the training phase.

In systems of detecting IoT botnets with only normal traffic training the learning model, it is possible to achieve lower computational complexity through decreasing the feature collection. The researchers in [51] showed that in an unsupervised learning model that offers anomaly-based detection in IoT, a feature selection process is able to decrease the number of features needed. The reduced feature set makes it possible to use fewer computational resources, which leads to results that are more interpretable. It was shown that with less than ten features, one model using conventional learning techniques, for example, SVM or isolation forests, can accomplish acceptable detection ratios that have desirable scalability. On the other hand, while one common learning model can achieve reasonable detection rates for a whole network, better detection rates are provided by creating a separate model for each device. Nevertheless, the study showed that their trained model produced fair results regarding accuracy and precision.

In [52], the authors proposed a modular solution which is distributed and can be applied during the scanning/infection process rather than during an attack. Thus, it can expose the behavior of large infected IoT networks, such as those of large organizations or ISPs. For edge devices' traffic classification, EDIMA uses machine learning algorithms, a database of packet traffic feature vectors, a module for the policy and a module for elective packet subsampling. In order to detect potentially malicious activities based on pattern-scanning traffic, a machine learning algorithm is used at the user access gateway. Furthermore, a policy module was built to discover the actions necessary for malicious packets. In addition, a database was used to store the scanned patterns to update or obtain them if necessary. Via test bed experiments, the authors assess the classification efficiency of EDIMA and demonstrated the results attained.

In the article [54], the authors built the suggested model based on one general classifier being used to develop a classifier for each device individually; it looks appealing from deployment and online usage perspectives when considering core networks. To reduce the number of characteristics for the detection of IoT bots, it applies feature selection. They proved that alongside a multiclass classifier built on a shallow process, a decision tree, fewer features can accomplish very elevated precision rates and offer explainable findings.

From various perspectives, the behaviors of Rustock botnet domain names that only employ fast-flux as the technique of communication among C&C and the bots were analyzed intensely in [55]. The results showed that the Rustock domain name resolution used only four DNS query forms, and the sum of a type of RR predominated between them. The Rustock domain names have minimal static values for querying density. In addition, there were only two change points for Rustock domain names, and there were several change points within 24 h for benign domain names. Furthermore, the lifespan of the Rustock domain was quite short, and the regular behaviors were evidently disparate. In addition, 32 specific features of Rustock domain name query traffic were extracted. To select suspicious domain names from the DNS traffic utilizing the 32 features, multiple common classifiers were then adopted.

To create a new feature-based PSI-rooted subgraph to detect cross-architecture IoT botnet malware in a fully static way, the researchers in [56] proposed a technique that combines deep learning with machine learning. They argued that this function is sufficiently powerful, due to its accuracy of about 97% and F-score of about 98%. When compared to various common machine learning classifiers, the experiments showed that their approach is efficient and robust. Furthermore, they argued that their technique is different to established earlier research; the findings showed that their technique works superiorly.

The authors in [57], with the aim of detecting zero-day attacks, used a supervised machine learning technique to identify patterns and distinguish anomalies in an IoT environment. They employed a random forest classifier, and considered only four types of attack in the training data and 10 types of attack for testing. When detecting the new attacks, the proposed model was productive, and attained a TPR of 99%, a TNR of 100% and around zero false alerts.

The researchers in [61] suggested an artificial intelligence-grounded approach for the detection of malicious behavior. They investigated the accuracy of the artificial neural network multi-layer perceptron learning algorithm in the identification of botnet behavior in IoT devices compromised by two significant botnets, Mirai and Bashlite. The MLP-ANN algorithm succeeded in achieving 100% accuracy in the classification of IoT botnet traffic in the testing stage after refinement and optimization. To demonstrate that the proposed solution can attain a similar degree of accuracy even with restricted sources, they used a subset of the N-BaIoT dataset.

The functions of machine learning methods used for detecting and inspecting botnets were discussed in article [62]. On the USNW-NB15 dataset, four ML algorithms were tested—DT, ANN, NB and ANN—and they were evaluated in terms of the accuracy and false alarm rate. The findings showed that DT was superior to the other algorithms. As a network forensics process, they found the finest machine learning algorithm and flow identifiers of IP addresses (source and destination), and protocols capable of identify botnets and their sources effectively and efficiently.

The goal of the study in [64] was to build a multi-objective particle swarm optimization (MOPSO) detection model for the identification of malicious traffic in IoT network. MOPSO's performance was validated against the multi-objective, non-dominating genetic sorting algorithm (NSGA-II), popular conventional machine learning techniques and some traditional filter-based feature selection techniques. According to the results achieved, MOPSO beat NSGA-II, traditional machine learning techniques and filter-based techniques on most of the datasets examined.

In article [37], the authors proposed a new high-level, PSI-rooted, subgraph-based function for IoT botnet detection. They produced a reduced number of features with detailed behavioral descriptions that required littler space and less processing time. They showed results having effectiveness and robustness. In addition, the proposed approach obtained a better output compared to other work. Finally, they published all of the materials on GitHub.

In article [67], the researchers proposed a fusion algorithm-based system model. First, the BoT-IoT recognition dataset was used, and its 44 successful features were chosen from a variety of features for the machine learning algorithm. Next, five efficient machine learning algorithms were picked for malicious and anomaly behavior detection, and the most commonly used ML algorithm performance assessment metrics were selected. They utilized a bijective soft-set approach to figure out which fusion ML algorithm was most successful in detecting IoT anomalies and intrusion behavior. The experiment's findings prove that the suggested algorithm was successful at selecting ML algorithms, and it was obvious that the naïve Bayes algorithm was efficient in the detection.

In article [69], the authors offered a method for analyzing and classifying IoT malware using machine learning and by employing Haralick image texture features. They used different algorithms—specifically, k-nearest neighbors, naïve Bayes and random forest. A binary file was transferred to a grayscale image. The gray level co-occurrence distribution was calculated for each of the mined images. Then, five Haralick features were determined and used to identify malware. The experimental findings demonstrate that the proposed method achieved 95% accuracy with random trees, 89% accuracy with naïve Bayes and 80% accuracy with k-nearest neighbors. Generally, they showed that the use of texture features results in a computationally simple and platform-independent classification method.

Finally, one paper [70] presented DRIFT, a method for identifying command and control domain names on the Internet of Things botnet scale. By applying an inherent feature of malicious domain name queries preceding registration, they developed a difference-based, lightweight feature for detecting malicious C&C domain names. Using NXDomain queries and answers from common malware, they evaluated the efficiency of the method, and found 99% accuracy and above 48 h prior to registering. The technique works as a detection method for whenever other methods dependent on entropy or on domains generating reversing algorithms are unfeasible.

AI-Based Unsupervised Learning

The purpose of the algorithm proposed in article [60] was to identify IoT botnet behavior by using the Grey wolf optimization (GWO) algorithm to optimize one-class support vector machine hyperparameters and operate selection features together. The experimental results on the NN-BaIoT dataset (a subset of the N-BaIoT dataset [50]) showed the GWO's effectiveness in improving the results of the one-class support vector machine classifier. The suggested algorithm surpassed three other unsupervised algorithms widely applied for anomaly detection. It attained the shortest detection time, whilst decreasing the number of features picked.

In article [73], the authors introduced a method that uses association rule learning to find out from data collected on a large-scale from darknets, with a big stream, the uniformities of attacks. They were able to discover the behaviors of hitting hosts related to recognized malware groups by discovering symmetries in IoT-related signs, for instance, destination ports, operation type and TCP window size. As a case study, prior to and following the first source code publication of Mirai, they performed a noteworthy inspection of the attack operations. The experiments confirmed that the proposed framework is accurate and productive in the early detection and monitoring of new malware on the Internet. Thus, it is a promising means of automating and speeding up detection and avoiding the latest threats.

The authors in article [74] conducted a darknet study. The common pattern mining and association rule learning were applied on a large collection of TCP SYN packets gathered from 1 July 2016 to 15 September 2016, with a darknet sensor called NICT/16. The total number of packets received was 1,840,973,403, sent from 17,928,006 separate hosts. In this analysis, they concentrated on commonly occurring groupings of "window sizes" in TCP headers. They fruitfully obtained several frequent patterns and association rules for window sizes, and they listed source hosts that delivered SYN packets which fit either of the rules obtained. Additionally, they demonstrated that nearly all such hosts dispatched

SYN packets to meet the three circumstances recognized from Mirai source code. These hosts began the scanning activities 3 days prior to the publishing of the source code.

AI-Based Deep Learning

In combination with word embedding, the authors of [46] introduced an application of a bidirectional long short term memory recurrent neural network (BLSTM-RNN) for botnet detection. The proposed solution was contrasted with a unidirectional LSTM-RNN. This was done to decide if the improved accuracy and loss metrics achieved on the captured dataset could be matched by the latter technique. For the different attack vectors used by Mirai, the two models equally achieved high-level precision and minimal loss metrics.

In article [47], the authors presented a malware detection honeypot-based method that employs machine learning algorithms. The produced IoT honeypot data were utilized as a dataset for the successful and lively training of a machine learning algorithm. As a proactive start to countering zero-day DDoS attacks, which has now surfaced as an open challenge in protecting IoT devices against DDoS attacks, the proposed method can be used. To catch several attempts at installing malware onto the IoT device, they used a honeypot method. The collected information was used in the form of log files as inputs to the machine learning model, so it was utilized for training purposes. The training process repeats once it surpasses the permissible size of training data to render the process active and effortlessly operable on resource-limited IoT devices. The benefit of employing the honeypot method to teach the model is that rather than only utilizing restricted identified data, the unknown variants of malware families can also train the model. Using honeypots guarantees the logging of new malware features, which can then be used to train classifiers effectively using the ML-based detection system.

Researchers in [49] proposed an approach to generating a PSI-graph to reflect the connections among PSI, which was very valuable for static analysis details in order to boost the identification of IoT botnet malware. The graphic convolution neural network classifier was also applied for IoT malware detection based on a convolutional neural network (CNN) and was able to identify malware without obtaining the previously chosen features. In their study, they suggested a novel approach based on the combination of a PSI graph and a CNN classifier for Linux IoT botnet detection. For the experiment, 10033 ELF files were used, including 4002 IoT botnet samples and 6031 benign files. The outcome of the test indicated that the PSI graph CNN classifier achieved 92% precision and a 94% F-measure. It does not deal with packed .exe files.

As a full means to detect botnet attacks, researchers in [50] employed completely detached automatic autoencoder algorithms to detect anomalies in IoT traffic instead of using them partially, as in previous studies. An autoencoder was usually used as an initial method for feature training, for reducing of dimensionality or as a half-manual detector for outliers that depend significantly on human labeling for consequential classification or additional investigation by security analysts. For the technique in article [50], the authors were dependent completely on deep autoencoders to detect IoT botnet attacks and learned by statistical characteristics obtained from non-malicious traffic data of the system. Detected anomalies can show that a device is compromised when the method is employed for new potentially contaminated data from an IoT device. This technique consists of four main phases: collection of data, extraction of features, training of an anomaly detector and continual monitoring.

The authors of [53] proposed an approach focused on deep learning for IoT botnet detection. In order to extract fundamental traffic features of IoT devices, the authors used the dampened incremental statistics and applied the z-score technique to standardize the features. Subsequently, the multivariate correlation analysis (MCA) algorithm based on triangle area maps (TAM) was used to produce datasets. They built a convolutional neural network to train on the dataset, and detected the traffic using the learned CNN. The last tests indicated that the proposed method can effectively differentiate benign traffic and various forms of attacks and achieved 99.57% precision.

Since they are assigned weak passwords during manufacturing, IoT devices are recognized for having weak default verification processes. Consequently, IoT devices are vulnerable to different attacks. Intruders can seize power over them using brute force. If hijacked, vital services such as healthcare and transportation can be endangered. Using a bot, an attacker may force the surrender of power from officers and users of smart city networks. In the article [58], the authors proposed a software defined IoT protection (SDID) mechanism based on deep learning that tracks and contrasts the historical traffic flow of devices with current trends to decide whether an attack is being carried out on a system. In addition, the technique compares data with neighboring nodes to decide if the traffic stream is abnormal or not, in order to avoid false detection in flash-crowd cases.

The authors in [59] proposed a lightweight IoT botnet detection method based on extracting high-level characteristics for each executable file from function call graphs, known as PSI graph. This function deals with the issue of multi-architecture while averting the difficulty of analyzing control flow graph utilized by the majority of the current approaches. The experimental findings revealed that with the dataset of 11,200 ELF files comprising samples of 7199 pieces of IoT botnet traffic and 4001 pieces of benign traffic, the proposed approach achieved a precision of 98.7%. In addition, a comparative analysis with other current approaches indicated that the technique produced better outcomes. Finally, through GitHub the source code was made accessible.

The authors of [63] offered a new IoT malware traffic analysis technique, powered by multilevel artificial intelligence, that operates as a blend of a neural network and a binary image. The technique could be utilized to safeguard IoT devices on the gateway level, avoiding the limitations related to the IoT environment. From the preliminary experimental outcomes, the technique appears encouraging and capable of detecting unrecognized malware. Furthermore, the technique learns from misclassifications, which enhances its effectiveness. An improvement of this techniques could be added by including the usage of extra samples for learning and testing and by using a GPU for binary imagining and CNN classification. The proposed technique should be tested for encrypted traffic.

The authors of [65] offered a CNN-based deep learning model consisting of a data handling component and an 8-layer CNN. Until implementing the CNN model, they segmented and standardized the energy utilization data obtained, to help the CNN model to attain greater precision. The model categorizes handled data into four classes, including the botnet class, which is the prime objective. To show results, they conducted a self-evaluation; a cross-device assessment; and leave-one-device-out and leave-one-botnet-out examinations on three conventional kinds of IoT devices—a security camera, a router and a voice assistant. The self-assessment reached a classification accuracy of 96.5%, and cross-tests attained approximately 90% accuracy. In the same manner, leave-one-out tests attained more than 90% accuracy for botnet identification.

The paper [66] presented a brand-new dataset, named Bot-IoT, which includes legal and modeled IoT network traffic, in conjunction with different forms of attacks. The authors introduced a practical experimental environment to address the current dataset disadvantages of collecting full network details, correct labeling and having the latest and most complicated attack varieties. After all, they tested the BoT-IoT dataset's reliability by applying various statistical and machine learning approaches for forensic functions, and contrasted the results to those achieved with existing datasets. The proposed solution provides a basis for activating botnet identification through IoT-specific networks.

The original probabilistic model in [68] was designed to clean irrelevant flow by eliminating noise samples, such as misconfigured traffic. Then, multiple low and deep learning models were tested in an endeavor to create an efficient multi-window convolutional neural network. Through using active and passing weights while creating learning datasets, the goal of the neural network is to precisely classify infected IoT devices. Therefore, to understand organized and unwanted behaviors produced by well-cooperating IoT botnets, tiered conglomerative clustering is used to analyze a collection of creative and effective network features. Analyzing 3.6 TB of the freshly captured darknet flow uncovered a substantial 440,000 infected IoT devices and created proof-based objects associated with 350 IoT botnets. In addition, by performing a detailed study of such indirect projects, they exposed the scan activities, packet time intervals, rates of jobs and geo-scanning. While some campaigns displayed substantial declines in those variables, some showed the opposite via being restricted to particular geolocations or due to carrying out arbitrary port scans in addition to their core objectives. Whilst many of the implied botnets are parts of formerly reported campaigns such as Hide, Seek, Hajime and Fbot, in fact more events represent the emerging existence of such IoT risk trends. These events show increasing cryptojacking abilities or affect industrial management services.

5.3.2. Methods Based on Blockchain Technology

This section reviews the proposed methods that are based on blockchain technology. Initially, blockchain was used to register financial transactions; such transactions are encrypted and managed by all parties (e.g., Bitcoin and other cryptocurrencies). All transactions are thus transparent, and any changes can be easily tracked and identified [94]. It is possible to apply blockchain to boost IoT botnet detection. Three of the selected studies that used blockchain are discussed below.

The goal of AutoBotCatcher [71] was to analyze IoT device communities dynamically, according to their network traffic flow. The authors implemented a dynamic P2P botnet identification and prevention framework for IoT based on blockchain, referred to as AutoBotCatcher, which performs group identification on IoT application network flows. IoT gateway devices become peers of a BFT blockchain in AutoBotCatcher, where system vendors and/or security regulators take positions as block generators and engage in the process of consensus. Blockchain was used for snapshots of the IoT devices' mutual communication graph to perform dynamic, network-based botnet group identification.

The researchers of [72] created a lightweight security IoT solution that uses hacker tools against hackers, an IoT vaccine, in essence. The solution provides IoT devices with managed protection and intelligence using a "friendly" botnet powered by the Bitcoin blockchain, a validated existing communication framework for distributed systems. To date, NeuroMesh has been tested on routers, cameras with CCTV and smart meters. NeuroMesh was able to destroy the Mirai botnet in all cases and prevent the running of errant processes. In addition, access to the system was effectively blacklisted for any IP address sent through the blockchain communication channel.

The authors of [78] proposed new firmware to modernize a platform for IoT devices. The firmware improved the upgrade procedure, making it more efficient and secure. In specific, the suggested method was founded on blockchain and makes use of smart contracts to guarantee firmware integrity and attain malware-resistant properties. To ensure accessibility of the new platform, they used a peer-to-peer file distribution method that not merely stores a variety of firmware editions of devices in a dispersed way, but reduces the ability to perform DDoS attacks with protected devices. In addition, this platform greatly enhances device scalability by checking multiple signature requests at the same time. Massive assessments and operation simulations were performed to ensure that the anticipated method can achieve exceptional operating effectiveness for IoT devices on the firmware update platform. They considered the effectiveness related to computing costs and overhead connections, and compared it to the most current works.

5.3.3. Methods Based on Software Defined Network Technology

Software defined networking (SDN) is a modern technology that enables the overall behavior of a network to be managed by a central program, named the SDN controller. The controller allows fast security threat responses, granular traffic filtering, and the implementation of complex security policies [95]. SDN can support IoT botnet detection. One of the selected studies that was based on SDN is discussed below.

In [75], the authors developed a detection and mitigation method using the Mirai botnet as a particular case study for IoT-originating DDoS attacks. By performing the mitigation near the IoT devices, protection contra DDoS attacks from IoT to ICT public services came to be successful. SDN was utilized as a compliant resolution for this purpose in order to impose different flow rules and actively renew them when needed. Even though the proposed work is aimed at Mirai variations, it is possible to easily configure and extend its detection mechanism for various BotNet threats. To enable the proposed solution in this setting, they also used fog computing. The proposed scheme has shown that when forcing attacks the edge first by using fog computing, DDoS attacks can be alleviated by exploiting SDN. This solution can also be offered in the fog computing environment as a security as a service (SECaaS) plan. There are practical problems with the integration of this method into IoT networks, which are characteristically diverse, loosely administered and emergent systems. On the other hand, a huge base of IoT infrastructure previously implemented without SDN and inheritance devices. The vital role of IoT networks as portion of the upcoming Internet is to make these remedies necessary and highly valuable.

5.3.4. Specification-Based Methods

The following methods did not use AI algorithms, and instead used specification-based methods for detection. Generally, a specification detection method depends on specifications that describe the intended behavior. It can detect non-previously-encountered attacks and has a low false positive rate, but it has the disadvantages of being less effective than anomaly detection methods and more time consuming.

The authors in [76] introduced an agile detection system termed ConnSpoiler that can identify IoT botnets accurately in a resource-restricted way. ConnSpoiler operates via rapidly categorizing the flows of NXDomain queries to build openings for the C&C link to be interrupted. The results indicated that the ConnSpoiler had a 94% probability of identifying queries prior to their being sent to the C&C, and achieved great accuracy and scalability of detection using a month of labeled data. In addition, ConnSpoiler can identify the domains created by six DGAs that relate to recognizing botnet groups and six new DGAs that were not recorded any earlier DNS traces gathered from two separate huge, scaled ISP networks.

The authors of [77] proposed the IoT Based Botnet Detection System for Usage, Contact and Access Monitoring. The descriptor specifies policies for system use, communication and access. The monitor observes the current states of device use, contact and access; and the comparator detects abnormalities. In the open-source security event and information management system, they developed the detection system. The researchers selected the open-source Security Information Management (OSSIM) alien vault and set up the OSSIM detection system. Results showed that Mirai IoT malware is detected effectively by the proposed detection mechanism.

In article [80], the authors proposed a different method for IoT security focused on a scattered multi-agent framework. In every single one of several IoT systems, for example, smart homes, they employed a lightweight agent to work in cooperation to detect security incidents and avoid likely attacks. To test the efficiency of the proposed technique, a simulation was performed. In particular, the technique was used to mitigate the effects of using IoT system botnets, for instance, the Mirai Botnet, for distributed denial of service attacks. The key concept is to employ an effective number of path messages to cumulatively create a behavioral profile for possible victims of DDoS attacks that passes via agents installed on different IoT sites. Additionally, the results obtained have shown that in the cases examined, a length coefficient of 0.3 was efficient. The lowest degree of coordination needed to detect such an attack was assessed. Although there are still many open issues about the application of such a scheme or the core consensus method, studies show that large-scale DDoS attacks can be identified.

5.3.5. Signature-Based Methods

The signature-based methods retain databases of known intrusion techniques (attack signatures) and detect intrusion by comparing behaviors to the database. They accurately detect known attacks and require less resources to detect intrusions. They have the disadvantage of being ineffective at detecting unknown or emerging attacks.

The authors of [79] suggested a cloud-based system termed CloudEyes that is resistant to malware and offers effective and secure services for resource-concentrated devices. For cloud servers, CloudEyes, introduces suspect container cross-filtering, a new signature identification method founded on a mutable plan framework that offers fair and precise identification of signature malicious parts. For the host, CloudEyes implements a lightweight scanning agent that uses signature fragments to significantly decrease the variety of precise fitting. In addition, by communicating, sketch synchronizing and modular hashing, CloudEyes guarantees both data privacy and low-cost communication. They tested the efficiency of the proposed solution through using both suspicious traffic on site and regular files. The findings showed that the methods in CloudEyes are efficient and realistic, and the approach could surpass other current systems with less time and interaction.

6. Results

After analyzing the selected studies, and as a result of the above analysis, it can be realized that there are various research gaps, open issues and future directions. In this section, we explain the importance of each of them.

6.1. Research Gaps and Challenges

The following research gaps and challenges are summarized to guide the researchers who investigate in this field.

6.1.1. Early Phases IoT Botnets

As has been explained in Section 3.3.2, the IoT botnet's lifecycle has three phases, scanning, propagation and attack. Throughout these phases, there is communication amongst the bots and the C&C, and among the bots. From Figure 7, it is clear that most of the studies developed detection techniques for IoT botnets in the late phase, when they are launching and triggering attacks on the targets, whereas they could be detecting botnets in earlier phases, for instance, when the attacker starts the scanning or propagation activities. Therefore, researchers need to further investigate the detection of IoT botnets in their early phases before triggering attacks; this would reduce the illegal utilization of the devices' resources, and thereby disrupt or deny the services of the IoT network [52,96].

6.1.2. Types of Malicious Activities

It is obvious that most of the effort put toward the detection of IoT botnets goes into developing detection techniques for DoS/DDoS, scanning or IoT malware as attacks launched by IoT botnets—mainly by Mirai—instead of proposing solutions for detecting the other attacks (see Figure 8). The reviewed studies also have not encompassed the recent trends in attacks, such as attacks with intent to illegally utilize the resources of IoT devices in computational tasks, for example, cryptomining, other tasks or fraud on social media. This was caused by the lack of datasets, the difficulty of implementing experiments associated with other types of suspicious activities and the lack of simulations. More investigations are needed in these areas.

6.1.3. Methods and Techniques

Most of the studies herein proposed techniques based on employing artificial intelligence (AI). AI is considered as an interesting approach in detecting IoT botnets because it can accelerate the process of making decisions, and these approaches and techniques could be integrated with different trendy technologies to form more powerful techniques, such as SDN [97–99] or blockchain [72]. Hence, more studies are required in this area. At the same time, the proposed methods tend to be concentrated on defensive techniques, whereas a proactive approach could help to understand the techniques of IoT botnet and therefore prevent the damage that may be caused by a variety of malicious activities by IoT botnets.

6.1.4. IoT Datasets

The construction of IoT datasets from commercial products faces immense challenges due to the restrictions on obtaining attacks of diversity or privileged access. Mirai malware and its variants are believed to be known attacks, but only for particular types of IoT devices, such as IP camera surveillance devices. Therefore, some studies resorted to constructing synthetic datasets through simulation tools [99] or carrying out experiments using limited sets of smart home devices and generating datasets that way. It is worth mentioning that some IoT datasets available for the public have been used by many researchers, such as N-BaIoT [50], BoT-IoT [66] and the recently published IoT23 [100] and MedIoT [101]. On the other hand, and regarding the selected studies, the used datasets do not include sufficient different suspicious activities related to bot networks, as the datasets were either not derived from IoT devices and thus does not reflect the IoT ecosystems, or do not represent the data of Internet of Things. Furthermore, they were extracted from IoT devices and are limited to specific purposes or to specific environments, such as the home system. As a consequence, a number of proposed solutions may face difficulties if they are applied to other ecosystems or if different other devices are present. More IoT botnet datasets are needed, and researchers should investigate building more datasets and finding solutions for extracting real datasets.

6.1.5. Competent Frameworks

Given on the above points, it can be noted that there is a need for a competent and proficient IoT botnet detection and prevention framework. It should be leveraged from the trendy technologies and can be adapted to the requirements such that it covers different layers of IoT architecture and takes into consideration defense against all the phases of IoT botnet's lifecycle.

6.2. Open Issues and Future Trends

6.2.1. Explainable Artificial Intelligence (XAI)

One of the important trends and directions for study is using explainable artificial intelligence. In XAI the outcomes and the decisions of an AI solution are understandable by humans, so the administrator can understand why the AI solution considered certain traffic as malicious or benign, in contrast to the existing blackbox AI solutions. This will give useful feedback for understanding the reasons behind the AI decisions and give the administrator the ability to either reject or accept the decisions related to his system. Consequently, this will reduce the number of false positive alerts and improve the system.

6.2.2. Offensive Techniques

Offensive techniques are some of the open issues that need to be investigated. That will enable a deeper understanding of how the Internet of Things botnets work through reverse engineering or by exploitation of functions that may exploit the vulnerabilities of the botnet itself. More studies are required for this research. Understanding and knowing the methods and techniques of cybercriminals through offensive techniques will facilitate and improve the defensive techniques.

6.2.3. The Representative IoT Dataset Issue

As discussed earlier, many factors have recently contributed to the increase in the spread of the Internet of Things networks. These factors include the digital transformation, where organizations desire to automate and share their services. Another factor is the appearance of the COVID-19 pandemic; that is, the spread of this virus and the desire to track and monitor society through different types of devices. For this reason, a properly organized and descriptive dataset is important for the training and validation of the trustworthiness of a system. While there are many IoT networks, in extreme situations there is no knowledge about the IoT botnet scenarios present. More research is therefore required to propose new botnet datasets that combine legal IoT network traffic generated through simulations with various kinds of attacks [66]. An IoT network produces a noisy, heterogeneous stream of data, whereas IoT botnet detection techniques need high quality data; this issue should be investigated to improve of the quality of data. On the other hand, it is necessary to consider how the detection techniques can handle such IoT data. This is one of the open issues.

6.2.4. IoT Honeypots

A honeypot is an isolated and independent network tool that mimics a genuinely useful network that would be to use by attackers. The goal is to draw attackers into it, and thus track the communication between the attackers and the compromised computer. It is a powerful tool for IoT security researchers in botnet attack identification. Moreover, it provides the logging of communications of the attackers, as IoT attackers usually hide their fingerprints and extract other IoT attacks features. Thus, honeypots are a powerful and useful tool for IoT botnet detection, because they can detect new waves of technology hitting IoT devices, particularly those that exploit zero-day vulnerabilities [102]. Honeypot-based detection techniques can deal with new IoT malware variants [47]. On the other hand, IoT honeypots should be open source to support the research community in this field [103]. A deployment framework for IoT honeypots is required; it is important to research which honeypots should be deployed, how they can attract attackers and how they can be enhanced on the basis of the information collected [104]. It is necessary to adapt honeypots so they can deceive the attackers to expose their origins [105].

6.2.5. Big Data, IoT Threat Intelligence and Analytics

The IoT threat intelligence should be further investigated: terabytes of data are used daily in collaborations among different countries. This data should be analyzed, visualized and shared with other organizations. The analytics of this data can support the detection of IoT botnets and improve the security of the Web in general.

6.2.6. Integration of Machine Learning with other Technologies

The following technologies can be integrated with machine learning algorithms to build a better defense model that takes advantage of these technologies.

Deep Learning

Deep learning is a subdivision of machine learning with three types—supervised learning, e.g., CNNs and restricted Boltzmann machines (RBM); semi-supervised learning; and unsupervised learning, e.g., autoencoders. It comprises several layers of artificial neural networks. Each layer covers some neurons with initiation functions that can be used to generate non-linear outputs [106]. It has strong analytical capabilities which are used for various applications, including malicious activity detection and IoT botnet detection. Important improvements in efficiency over some machine learning algorithms can be seen in [107] and have lately been utilized in some IoT applications with edge and fog computing. Deep learning can be used to mine for the features in datasets that will best enhance machine learning classification algorithms. IoT applications need significant amounts of data to be transmitted across a network, and deep learning provides improved performance with more massive data than shallow learning. In addition, deep learning can operate with new features and resolve difficulties with no interference. Deep learning can ease time-consuming manual analysis and increase detection accuracy by automatically detecting Internet of Things (IoT) software vulnerabilities [108]. Various approaches using deep neural networks have been used as IoT classification engines to identify IoT connections as natural and to identify attacks using an intelligent intrusion detection engine. The results of the performance assessments indicate the efficacies of these approaches [46,50,53,106,109–111]. Deep learning can be used with software defined networks (SDN) to analyze and contrast the chronological traffic stream of a device with existing trends to decide whether the device seems to be under attack [58].

Software Defined Network (SDN) Technology

Managing and protecting a sizeable and diverse network of devices, such as an IoT networks, is challenging, and software defined networking (SDN) solves these difficulties through its simplicity and comprehensive network vision. SDN is the latest evolving technology for fundamental networks that can be used to deal with malicious activities created by many IoT devices, such as IoT botnets, as it offers network flow observing and unified control of network devices [75]. SDN has various features, including traffic engineering, complex policy enforcement tracking, on-time access control and system mobility [112]. It offers centralized control of defense for IoT networks. It facilitates detecting and preventing IoT botnets because SDN is responsible for the continuous examination of traffic data through the IoT network with the purpose of delivering an ideal mode and faster responses of attacks, such as DDoS [113,114]. On the other hand, the SDN controller could be a single point of failure.

Edge Computing

Edge computing provides processing units that increase computer power with the capability of processing and storing real time data close to the sensors instead of sending them to the cloud, which improves the response time and reduces latency. IoT botnet detection and prevention needs rapid responses that cannot be realized under a conventional data transmission model that includes a data center for central handling until restoration by a user. Edge cloudlets also serve as data extraction and grouping resources that only transmit mandated data to the conventional cloud data center and redeem critical network resources, such as bandwidth, electricity and storage [115]. Hence, edge computing lowers the cost of transmitting and processing massive amounts of data compared to using the cloud, reduces delays, enhances the efficiency of energy and increases the scalability of lightly-weight IoT devices. There is a necessity, therefore, to explore the deployment of edge-based detection of IoT botnets [48,75], which should provide a reduction in network traffic loads through its effective structure for handling the data. In addition, edge computing can integrate with SDN [75,99,115] to avoid a single point of failure.

Blockchain

A blockchain relies on the idea of a distributed directory managed by a peer-to-peer network. It is a public, decentralized and fault-tolerant ledger to which registers are appended in sequence chronologically, and registers become more permanent every time a new register is published [116]. Blockchain relies on the idea of a distributed directory managed by a peer-to-peer network. It currently offers one of the most reliable communication protocols, which relies on proof of work (PoW) to validate transactions and is a non-trusting protocol that provides pseudo-anonymity. Blockchain has an enormous amount of distributed computing capacity behind it, and to date it has been difficult to hack [72]. Therefore, blockchain can enable multiple parties to work together to detect botnets. A blockchain platform does not need a trusted centralized party to verify the correct execution of cooperative botnet detection, nor to ensure clarity of the obtained snapshots of IoT devices to address the potential lack of confidence between the parties involved in botnet detection [71]. While blockchain is primarily intended to store and verify digital currency (such as Bitcoin) transactions, it may have key roles in management, administration and securing IoT devices and detecting IoT botnets. In addition, blockchain offers privacy preservation and anonymity for IoT applications. Often, it ensures that the data are original and keeps them secure from data tampering. The combination of IoT botnet detection methods and the blockchain system would improve the reliability of the models, improve the reliability of the data and enhance the key management of the IoT devices. On the other hand, blockchain is not light-weight because the proof of work procedure has a high cost due to the intense using of resources. In addition, generating a block increases the throughput and latency [117]. Thus, each of these problems needs to be resolved in order to improve IoT protection and privacy based on blockchain.

Fog Computing

In recent times, the idea of fog computing has been implemented, wherein processing models bring the required processing power and storage closer to the computers in need. It typically involves cloud computing in a layer-based design. It allows instantaneous data analysis by analyzing data in fog with the cooperation of edge layer data, and provides an enabling method to support the generation of high-bandwidth and low-latency networks and applications. Fog computing is hierarchical and offers computing, networking, storage, power and acceleration anywhere from cloud to Internet of Things, whereas edge computing appears to be restricted to edges. Fog computing allows data analysis closer to the edge than to the cloud, which ensures that decisions can be made more easily [93]. Fog computing also helps with delivering an effective attack detection technique in conjunction with edge and SDN for IoT ecosystems by contributing to reducing the time required to detect and mitigate attacks [75,113,118], and thus helps with detecting IoT botnets using fog-based detection systems [109]. The detection mechanisms should consider the presence of fog devices in the center with the goal of increasing protection, while at the same time providing reliability and timeliness [78,119].

Network Function Virtualization (NFV)

Network function virtualization (NFV) is a technique to add virtualization to network services—for instance, routers, firewalls and load balancing systems—which have historically been operated on private hardware. The services are promoted as virtual machines (VMs) on product hardware, enabling one to operate networks on common servers instead of private ones. Various computing nodes operate security functions unloaded from IoT devices using the NFV technique that actively enables virtualized network functions for a variety of protection services. This technique with integration to SDN enhances the detection of IoT botnets [120].

7. Discussion

In this section, we go over the limitations of our SLR and how the COVID-19 Pandemic relates to IoT botnets.

7.1. The Limitations of the This SLR

This research was limited to journals and related conference papers on Internet of Things botnet identification that were published in English. We applied our research approach to a large number of articles, but found that most of these articles had no relevance. Therefore, we picked just the studies that were issued between 2016 and 2020 that completely met this study goals and the quality evaluation criteria. We faced some challenges which made it hard to sketch satisfactory conclusions for this SLR: The empirical studies claimed to have dealt with IoT botnet detection, prevention and mitigation of malicious botnet activities and botnet as a blackbox. Nevertheless, there is a shortage of experimental research dealing with IoT botnets via white-box approach. In addition, there are disparities and disagreements about the phases of the IoT botnet, and there was a lack of clarification about the assessment calculations in some experiments. Some other studies appeared to concentrate on the verification of authentication and so on, rather than the detection of the botnet.

7.2. IoT Botnets during the COVID-19 Pandemic

The WHO Emergency Committee declared a global health emergency in January 2020 on the basis of rising case reporting rates for the novel coronavirus that spread to many countries [114]. Due to this worldwide pandemic of COVID-19 and its implications, the use of the Internet has been increased. Hence, every organization today, whether governmental or private, is digital and relies on the Internet and computer networks to exchange business data. There is an immediate need to make full use of available technologies, since there are changes in customer behavior, new ways of working and travel restrictions. Therefore, the Internet of Things (IoT) is considered to be one of the highly innovative technologies with great potential in the fight against coronavirus outbreaks. The IoT consists of a scarce network in which IoT devices sense the world, collect data and send useful data to the Internet.

As IoT is rapidly being adopted in the context of COVID-19 [121], the value of IoT has significantly increased in the presence of this disease, and the number of Web-connected devices has increased, but most devices have little to no security features. The first quarter of 2020 showed a considerable increase in malware. There was a 58% increase in new IoT malware [122]. Consequently, the magnitude and complexity of the IoT botnet threats have gradually increased; IoT botnets exploit more vulnerabilities and cause evermore malicious activities. These activities include information theft and persistence threats, which impact critical systems through exfiltration channels and resource hijacking to convert the IoT devices into bots. This raises the need for similarly complex detection systems. It is projected that the need for IoT botnet detection is increasing at a significant rate due to the COVID-19 pandemic. Various methods, along with sensors and wireless communication techniques, could be used to build secure systems suitable for COVID-19 detection and monitoring.

Many industries are using IoT to meet the requirements of government responses to COVID-19 [114] and are being targeted by attacks as a consequence, including healthcare, education, finance, retail and entertainment industries [122]. Given the importance of managing the COVID-19 pandemic globally and ensuring social distance, healthcare IoT devices have recently become more connected to the Internet as part of the linked health environment. With the aim of automating healthcare procedures, different applications are being employed to retrieve electronic health histories and medical files created by healthcare IoT devices in hospitals. As a result of the widespread outbreak triggered by the human-to-human spread of COVID-19, health officials exploited IoT devices to identify COVID-19 patients. With the intention of enabling faster diagnosis, different models have been utilized, such as X-ray images, ultrasound symptom detection, CT scan images, ICU data gathering, non-intrusive facial-recognition hospital profile examinations and others. Healthcare systems are highly important, as they provide life-critical services. Effective cyber-attacks on healthcare would directly endanger not only the protection of networks and information, but also the health and safety of patients—they may threaten lives. The impacts of cyber-attacks on healthcare facilities are large. They can range from malware that compromises the security of the infrastructure and privacy of patients to distributed denial of service (DDoS) attacks that threaten the ability of the facilities to provide patient care. In the last two quarters of 2020, a high rate of cyber-attacks by various actors against the healthcare sector has been observed. These actors aim to infect vital healthcare networks with various forms of cyber-attacks by using a variety of strategies, techniques and procedures (TTPs) to gain initial access and further exfiltrate sensitive health sector data.

There is a great deal of worry about private data collection; this includes ensuring the quality of the collected data, as well as ethical problems related to the use and storage of data. The data sent from the sensors attached to COVID-19 patients' bodies should be correct; the data should reach the destination successfully; the data should not be forged; the data should not be intercepted along the communication route; and the data should be stored in an IoT computer's memory, which should not be available to all. There are concerns about protecting the collected data from abuse by command and communication channels.

IoT networks have scalability, and conversely, IoT devices are resource limited; hence, conventional cryptographic techniques are not feasible solutions for implementing IoT security. Security solutions should be energy efficient, and algorithms established to secure the IoT network should have less computational complexity to provide end-to-end data protection, user privacy and secure authentication. As a result, lightweight security algorithms need to be built to implement IoT security. With coronavirus outbreaks, the safety criteria of IoT-enabled networks have increased.

Significant challenges include addressing privacy and security concerns when enabling IoT devices to collect personal data needed for the smart management of the pandemic and social distance; and preventing the data theft, resource exploitation and suspension of vital digital services.

Further research and innovations are needed to enhance data protection and privacy for IoT architectures, in order to improve the level of trust between groups involved in data sharing.

Generally, IoT security will be improved by developments in authentication, cryptographic technology and blockchain. In addition, adoption of IoT regulations, policies and frameworks will help strengthen the security of IoT devices and mitigate the risk of IoT botnets.

8. Conclusions

The state-of-the-art methods and techniques for IoT botnet detection were systematically reviewed in this research. As per the conducted SLR on IoT botnet detection methodologies from 2016 to 2020, the number of published studies has been progressively increasing, showing that this topic is being investigated and will continue to gain attention. All these studies were released by noteworthy journals and conferences. The authors assessed the 37 selected studies and classified these studies according to the methods and technologies used. Moreover, we contrasted the selected studies depending on the phase of detection, types of attack and evaluation metrics.

Most of the articles focused on detection in late botnet phases. In addition, depending on the method of classification, artificial intelligence-based solutions are popular in the research field. In brief, this SLR sought to contribute to overcoming the scarcity of present IoT botnet detection methods and provide an opening for supplementary debate so that such detection methods could facilitate tighter IoT security in future. The thrilling areas for research include consolidating machine learning algorithms with trendy technologies such as blockchain and SDN to overcome limitations, and using deep learning for feature engineering with machine learning classifiers. Despite the great number of studies performed, there are still many different trends and open issues—for example, take the need to implement a capable botnet detector in early botnet phases. Additionally, XAI could be used to resolve the problem of excessive false positives. A further possibility is the production of an advanced and comprehensive approach, for instance, integrating more than one level of detection regarding each botnet phase. In the same context, one could integrate machine learning classifiers with other technologies, such as software defined network (SDN) technology, edge computing, blockchain, fog computing and network functions virtualization (NFV).

Author Contributions: Conceptualization, M.W. and D.A.; methodology, M.W.; validation O.B., A.A. and L.C.; formal analysis, M.W.; investigation, O.B., A.A. and L.C.; data curation, M.W.; writing—original draft preparation, M.W.; writing—review and editing, M.W.; visualization, M.W.; supervision, D.A.; project administration, D.A.; funding acquisition, D.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Institutional Fund Projects under grant number IFPRC-106-611-2020. Therefore, the authors gratefully acknowledge the technical and financial support from the Ministry of Education and King Abdulaziz University, Jeddah, Saudi Arabia.

Data Availability Statement: Not applicable.

Acknowledgments: This research was funded by Institutional Fund Projects under grant number IFPRC-106-611-2020. Therefore, the authors gratefully acknowledge the technical and financial support from the Ministry of Education and King Abdulaziz University, Jeddah, Saudi Arabia.

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

References

1. Cisco. Cisco Annual Internet Report (2018–2023). Available online: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf (accessed on 5 January 2021).
2. Hung, M. Leading the IoT. Available online: https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf (accessed on 26 February 2021).
3. Singh, M.; Singh, M.; Kaur, S. Issues and challenges in DNS based botnet detection: A survey. *Comput. Secur.* **2019**, *86*, 28–52. [CrossRef]
4. Koroniotis, N.; Moustafa, N.; Sitnikova, E. Forensics and deep learning mechanisms for botnets in Internet of Things: A survey of challenges and solutions. *IEEE Access* **2019**, *7*, 61764–61785. [CrossRef]
5. Alhajri, R.; Zagrouba, R.; Al-Haidari, F. Survey for anomaly detection of IoT botnets using machine learning auto-encoders. *Int. J. Appl. Eng. Res.* **2019**, *14*, 2417.
6. Ali, I.; Ahmed AI, A.; Almogren, A.; Raza, M.A.; Shah, S.A.; Khan, A.; Gani, A. Systematic literature review on IoT-based botnet attack. *IEEE Access* **2020**, *8*, 212220–212232. [CrossRef]
7. Keele, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; Technical Report, Version 2.3; EBSE: Hajdúszoboszló, Hungary, 2007.
8. Brereton, P.; Kitchenham, B.; Budgen, D.; Turner, M.; Khalil, M. Lessons from applying the systematic literature review process within the software engineering domain. *J. Syst. Softw.* **2007**, *80*, 571–583. [CrossRef]
9. Budgen, D.; Brereton, P. Performing systematic literature reviews in software engineering. In Proceedings of the 28th International Conference on Software Engineering, New York, NY, USA, 20–28 May 2006; pp. 1051–1052.
10. Petticrew, M.; Roberts, H. *Systematic Reviews in the Social Sciences: A Practical Guide*; Blackwell Publishing: Hoboken, NJ, USA, 2005; ISBN 1405121106.
11. Dange, S.; Chatterjee, M. IoT Botnet: The Largest Threat to the IoT Network. In *Advances in Intelligent Systems and Computing*; Springer: Singapore, 2019; pp. 137–157.
12. Sengupta, J.; Ruj, S.; Das Bit, S. A Comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2020**, *149*, 102481. [CrossRef]
13. Ji, Y.; Yao, L.; Liu, S.; Yao, H.; Ye, Q.; Wang, R. The study on the botnet and its prevention policies in the internet of things. In Proceedings of the 2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design (CSCWD), Nanjing, China, 9–11 May 2018; pp. 837–842.
14. Salim, M.M.; Rathore, S.; Park, J.H. Distributed denial of service attacks and its defenses in IoT: A survey. *J. Supercomput.* **2019**, *76*, 5320–5363. [CrossRef]
15. Ashton, K. That 'internet of things' thing. *RFID J.* **2019**, *22*, 97–114.
16. Fraga-Lamas, P. Enabling Technologies and Cyber-Physical Systems for Mission-Critical Scenarios. Ph.D. Thesis, Universidade da Coruña, Coruña, Spain, 2017. [CrossRef]
17. Ahmad, M.; Younis, T.; Habib, M.A.; Ashraf, R.; Ahmed, S.H. A Review of current security issues in internet of things. In *Advanced Controllers for Smart Cities*; Springer Science and Business Media LLC.: Berlin, Germany, 2019; pp. 11–23.
18. Minhaj, K.; Khaled, S. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411.
19. Soe, Y.N.; Feng, Y.; Santosa, P.I.; Hartanto, R.; Sakurai, K. Machine learning-based iot-botnet attack detection with sequential architecture. *Sensors* **2020**, *20*, 4372. [CrossRef]
20. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access* **2019**, *7*, 82721–82743. [CrossRef]
21. Beltrán-García, P.; Aguirre-Anaya, E.; Escamilla-Ambrosio, P.J.; Acosta-Bermejo, R. IoT botnets. In *Communications in Computer and Information Science*; Springer Science and Business Media LLC.: Berlin, Germany, 2019; pp. 247–257.
22. Alzahrani, H.; Abulkhair, M.; Alkayal, E. A multi-class neural network model for rapid detection of IoT botnet attacks. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*. [CrossRef]
23. Bertino, E.; Islam, N. Botnets and internet of things security. *Computer* **2017**, *50*, 76–79. [CrossRef]
24. De Donno, M.; Dragoni, N.; Giaretta, A.; Spognardi, A. Analysis of DDoS-capable IoT malwares. In Proceedings of the 2017 Federated Conference on Computer Science and Information Systems (FedCSIS), Prague, Czech Republic, 3–6 September 2017; pp. 807–816.
25. TrendMicro. Into the Battlefield: A Security Guide to IoT Botnets. 2019. Available online: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/into-the-battlefield-a-security-guide-to-iot-botnets (accessed on 5 March 2021).
26. Manos, A.; April, T.; Bailey, M.; Bernhard, M.; Bursztein, E.; Cochran, J.; Durumeric, Z. Un-derstanding the mirai botnet. In Proceedings of the 26th {USENIX} security symposium ({USENIX} Security 17), Vancouver, BC, Canada, 16–18 August 2017; pp. 1093–1110.
27. Vlajic, N.; Zhou, D. IoT as a land of opportunity for DDoS hackers. *Computer* **2018**, *51*, 26–34. [CrossRef]
28. Paganini, P. The Hajime Botnet Continues to Grow and Implements a New Attack Technique. 2017. Available online: https://securityaffairs.co/wordpress/58415/malware/hajime-botnet.html (accessed on 5 March 2021).
29. Mansfield-Devine, S. Weaponising the internet of things. *Netw. Secur.* **2017**, *2017*, 13–19. [CrossRef]

30. Zheng, S.; Yang, X. Dynashield: Reducing the cost of DDoS defense using cloud services. In Proceedings of the 11th {USENIX} Workshop on Hot Topics in Cloud Computing (HotCloud 19), Boston, MA, USA, 8 July 2019.
31. Soltan, S.; Mittal, P.; Poor, H.V. BlackIoT: IoT botnet of high wattage devices can disrupt the power grid. In Proceedings of the 27th {USENIX} Security Symposium ({USENIX} Security 18), Baltimore, MD, USA, 12–14 August 2018; pp. 15–32.
32. Šimon, M.; Huraj, L.; Horák, T.; Horak, T. DDoS reflection attack based on IoT: A case study. In *Cybernetics and Algorithms in Intelligent Systems*; Springer: Cham, Switzerland, 2018; pp. 44–52.
33. Trendmicro. Mirai Updates: New Variant. 2020. Available online: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/mirai-updates-new-variant-mukashi-targets-nas-devices-new-vulnerability-exploited-in-gpon-routers-upx-packed-fbot (accessed on 5 March 2021).
34. Costin, A.; Zaddach, J. Iot malware: Comprehensive survey, analysis framework and case studies. In Proceedings of the BlackHat, Las Vegas, NV, USA, 3–6 December 2018.
35. Holmes, D.; Shattuck, J. Reaper: The Professional Bot Herder's Thingbot. 2017. Available online: https://www.f5.com/labs/articles/threat-intelligence/reaper-the-professional-bot-herders-thingbo (accessed on 5 January 2021).
36. Vishwakarma, R.; Jain, A.K. A survey of DDoS attacking techniques and defence mechanisms in the IoT network. *Telecommun. Syst.* **2020**, *73*, 3–25. [CrossRef]
37. Nguyen, H.-T.; Ngo, Q.-D.; Nguyen, D.-H.; Le, V.-H. PSI-rooted subgraph: A novel feature for IoT botnet detection using classifier algorithms. *ICT Express* **2020**, *6*, 128–138. [CrossRef]
38. Edwards, S.; Profetis, I. Hajime: Analysis of a decentralized internet worm for IoT devices. *Rapidity Netw.* **2016**, *16*, 1–18.
39. Radware, A. Quick History of IoT Botnets. 2018. Available online: https://blog.radware.com/uncategorized/2018/03/history-of-iot-botnets/ (accessed on 5 March 2021).
40. Mendeley Reference Manager. Available online: https://www.mendeley.com/reference-management/reference-manager/ (accessed on 5 March 2021).
41. Kitchenham, B. *Procedures for Performing Systematic Reviews*; Keele University Technical Report TR/SE-040; Software Engineering Group, Department of Computer Science, Keele University: Keele, UK, 2004.
42. Popoola, S.; Adebisi, B.; Ande, R.; Hammoudeh, M.; Anoh, K.; Atayero, A. SMOTE-DRNN: A Deep Learning Algorithm for Botnet Detection in the Internet-of-Things Networks. *Sensors* **2021**, *21*, 2985. [CrossRef]
43. Popoola, S.I.; Adebisi, B.; Hammoudeh, M.; Gacanin, H.; Gui, G. Stacked recurrent neural network for botnet detection in smart homes. *Comput. Electr. Eng.* **2021**, *92*, 107039. [CrossRef]
44. Lee, S.; Abdullah, A.; Jhanjhi, N.; Kok, S. Classification of botnet attacks in IoT smart factory using honeypot combined with machine learning. *PeerJ Comput. Sci.* **2021**, *7*, e350. [CrossRef] [PubMed]
45. Prokofiev, A.O.; Smirnova, Y.S.; Surov, V.A. A method to detect Internet of Things botnets. In Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), St. Petersburg, Russia, 29 January–1 February 2018; pp. 105–108.
46. McDermott, C.D.; Majdani, F.; Petrovski, A.V. Botnet detection in the internet of things using deep learning approaches. In Proceedings of the 2018 International Joint Conference on Neural Networks (IJCNN), Rio de Janeiro, Brazil, 8–13 July 2018; pp. 1–8.
47. Vishwakarma, R.; Jain, A.K. A Honeypot with machine learning based detection framework for defending iot based botnet DDoS attacks. In Proceedings of the 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 23–25 April 2019; pp. 1019–1024.
48. Tzagkarakis, C.; Petroulakis, N.; Ioannidis, S. Botnet attack detection at the IoT edge based on sparse representation. In Proceedings of the 2019 Global IoT Summit (GIoTS), Aarhus, Denmark, 17–21 June 2019; pp. 1–6.
49. Nguyen, H.-T.; Ngo, Q.-D.; Le, V.-H. IoT Botnet Detection Approach Based on PSI graph and DGCNN classifier. In Proceedings of the 2018 IEEE International Conference on Information Communication and Signal Processing (ICICSP), Singapore, 28–30 September 2018; pp. 118–122.
50. Meidan, Y.; Bohadana, M.; Mathov, Y.; Mirsky, Y.; Shabtai, A.; Breitenbacher, D.; Elovici, Y. N-baiot—network-based detection of iot botnet attacks using deep autoencoders. *IEEE Pervasive Comput.* **2018**, *17*, 12–22. [CrossRef]
51. Nomm, S.; Bahsi, H. Unsupervised anomaly based botnet detection in IoT networks. In Proceedings of the 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA), Orlando, FL, USA, 17–20 December 2018; pp. 1048–1053.
52. Kumar, A.; Lim, T.J. Edima: Early detection of IoT malware network activity using machine learning techniques. In Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 15–18 April 2019; p. 289.
53. Liu, J.; Liu, S.; Zhang, S. Detection of IoT botnet based on deep learning. In Proceedings of the 2019 Chinese Control Conference (CCC), Guangzhou, China, 27–30 July 2019; pp. 8381–8385.
54. Bahsi, H.; Nomm, S.; La Torre, F.B. Dimensionality reduction for machine learning based IoT botnet detection. In Proceedings of the 2018 15th International Conference on Control, Automation, Robotics and Vision (ICARCV), Singapore, 18–21 November 2018; pp. 1857–1862.
55. Li, W.; Jin, J.; Lee, J.-H. Analysis of botnet domain names for IoT cybersecurity. *IEEE Access* **2019**, *7*, 94658–94665. [CrossRef]
56. Nguyen, H.-T.; Nguyen, D.-H.; Ngo, Q.-D.; Tran, V.-H.; Le, V.-H. Towards a rooted subgraph classifier for IoT botnet detection. In Proceedings of the 2019 7th International Conference on Computer and Communications Management, Bangkok, Thailand, 27–29 July 2019; pp. 247–251.

57. Alazzam, H.; Alsmady, A.; Al Shorman, A. Supervised detection of IoT botnet attacks. In Proceedings of the Second International Conference on Data Science, E-Learning and Information Systems, Dubai, United Arab Emirates, 2–5 December 2019; p. 42.
58. Salim, M.M.; Park, J.H. Deep Learning based IoT re-authentication for botnet detection and prevention. In *Advanced Multimedia and Ubiquitous Engineering*; Springer: Singapore, 2019; p. 239.
59. Nguyen, H.-T.; Ngo, Q.-D.; Le, V.-H. A novel graph-based approach for IoT botnet detection. *Int. J. Inf. Secur.* **2019**, *19*, 567–577. [CrossRef]
60. Al Shorman, A.; Faris, H.; Aljarah, I. Unsupervised intelligent system based on one class support vector machine and Grey Wolf optimization for IoT botnet detection. *J. Ambient Intell. Humaniz. Comput.* **2020**, *11*, 2809–2825. [CrossRef]
61. Javed, Y.; Rajabi, N. Multi-layer perceptron artificial neural network based IoT botnet traffic classification. In *Advances in Intelligent Systems and Computing*; Springer Science and Business Media LLC.: Cham, Switzerland, 2019; pp. 973–984.
62. Koroniotis, N.; Moustafa, N.; Sitnikova, E.; Slay, J. Towards developing network forensic mechanism for botnet activities in the IoT based on machine learning techniques. In *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*; Springer Science and Business Media LLC.: Cham, Switzerland, 2018; pp. 30–44.
63. Shire, R.; Shiaeles, S.; Bendiab, K.; Ghita, B.; Kolokotronis, N. Malware squid: A novel iot malware traffic analysis framework using convolutional neural network and binary visualisation. In *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*; Springer: Cham, Switzerland, 2019; Volume 11660, pp. 65–76.
64. Habib, M.; Aljarah, I.; Faris, H.; Mirjalili, S. Multi-objective Particle Swarm Optimization for Botnet Detection in Internet of Things. In *Algorithms for Intelligent Systems*; Springer Science and Business Media LLC.: Singapore, 2019; pp. 203–229.
65. Jung, W.; Zhao, H.; Sun, M.; Zhou, G. IoT botnet detection via power consumption modeling. *Smart Health* **2020**, *15*, 100103. [CrossRef]
66. Koroniotis, N.; Moustafa, N.; Sitnikova, E.; Turnbull, B. Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-IoT dataset. *Future Gener. Comput. Syst.* **2019**, *100*, 779–796. [CrossRef]
67. Shafiq, M.; Tian, Z.; Sun, Y.; Du, X.; Guizani, M. Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city. *Future Gener. Comput. Syst.* **2020**, *107*, 433–442. [CrossRef]
68. Pour, M.S.; Mangino, A.; Friday, K.; Rathbun, M.; Bou-Harb, E.; Iqbal, F.; Samtani, S.; Crichigno, J.; Ghani, N. On data-driven curation, learning, and analysis for inferring evolving internet-of-Things (IoT) botnets in the wild. *Comput. Secur.* **2020**, *91*, 101707. [CrossRef]
69. Karanja, E.M.; Masupe, S.; Jeffrey, M.G. Analysis of internet of things malware using image texture features and machine learning techniques. *Internet Things* **2020**, *9*, 100153. [CrossRef]
70. Spaulding, J.; Park, J.; Kim, J.; Nyang, D.; Mohaisen, A. Thriving on chaos: Proactive detection of command and control domains in internet of things-scale botnets using DRIFT. *Trans. Emerg. Telecommun. Technol.* **2018**, *30*, e3505. [CrossRef]
71. Sagirlar, G.; Carminati, B.; Ferrari, E. AutoBotCatcher: Blockchain-based P2P botnet detection for the internet of things. In Proceedings of the 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC), Philadelphia, PA, USA, 18–20 October 2018; pp. 1–8.
72. Falco, G.; Li, C.; Fedorov, P.; Caldera, C.; Arora, R.; Jackson, K. Neuromesh: Iot security enabled by a blockchain powered botnet vaccine. In Proceedings of the International Conference on Omni-Layer Intelligent Systems, Crete, Greece, 5–7 May 2019; pp. 1–6.
73. Ozawa, S.; Ban, T.; Hashimoto, N.; Nakazato, J.; Shimamura, J. A study of IoT malware activities using association rule learning for darknet sensor data. *Int. J. Inf. Secur.* **2019**, *19*, 83–92. [CrossRef]
74. Hashimoto, N.; Ozawa, S.; Ban, T.; Nakazato, J.; Shimamura, J. A darknet traffic analysis for IoT malwares using association rule learning. *Procedia Comput. Sci.* **2018**, *144*, 118–123. [CrossRef]
75. Özçelik, M.; Chalabianloo, N.; Gür, G. Software-defined edge defense against IoT-based DDoS. In Proceedings of the 2017 IEEE International Conference on Computer and Information Technology (CIT), Helsinki, Finland, 21–23 August 2017; p. 308.
76. Yin, L.; Luo, X.; Zhu, C.; Wang, L.; Xu, Z.; Lu, H. ConnSpoiler: Disrupting C&C communication of IoT-based botnet through fast detection of anomalous domain queries. *IEEE Trans. Ind. Inform.* **2019**, *16*, 1373–1384.
77. Sajjad, S.M.; Yousaf, M. UCAM: Usage, communication and access monitoring based detection system for IoT botnets. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 1547–1550.
78. Hu, J.-W.; Yeh, L.-Y.; Liao, S.-W.; Yang, C.-S. Autonomous and malware-proof blockchain-based firmware update platform with efficient batch verification for Internet of Things devices. *Comput. Secur.* **2019**, *86*, 238–252. [CrossRef]
79. Sun, H.; Wang, X.; Buyya, R.; Su, J. CloudEyes: Cloud-based malware detection with reversible sketch for resource-constrained internet of things (IoT) devices. *Softw. Pr. Exp.* **2016**, *47*, 421–441. [CrossRef]
80. Giachoudis, N.; Damiris, G.-P.; Theodoridis, G.; Spathoulas, G. Collaborative agent-based detection of DDoS IoT botnets. In Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini, Greece, 29–31 May 2019; pp. 205–211.
81. Dietz, C.; Castro, R.L.; Steinberger, J.; Wilczak, C.; Antzek, M.; Sperotto, A.; Pras, A. IoT-botnet detection and isolation by access routers. In Proceedings of the 2018 9th International Conference on the Network of the Future (NOF), Poznań, Poland, 19–21 November 2018; p. 88.

82. Chatterjee, M.; Namin, A.S.; Datta, P. Evidence Fusion for Malicious Bot Detection in IoT. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018; pp. 4545–4548.
83. Yılmaz, Y.; Uludag, S. Timely detection and mitigation of IoT-based cyberattacks in the smart grid. *J. Frankl. Inst.* **2019**, *358*, 172–192. [CrossRef]
84. Li, W.; Wang, P. Two-factor authentication in industrial Internet-of-Things: Attacks, evaluation and new con-struction. *Future Gener. Comput. Syst.* **2019**, *101*, 694–708. [CrossRef]
85. Ekolle, Z.E.; Kimio, K.; Ryuji, K. Intelligent security monitoring in time series of DDoS attack on IoT networks using grammar base filtering and clustering. In Proceedings of the 2018 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), Okinawa, Japan, 27–30 November 2018; pp. 37–42.
86. Wang, A.; Liang, R.; Liu, X.; Zhang, Y.; Chen, K.; Li, J. An inside look at IoT malware. In *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*; Springer Science and Business Media LLC.: Berlin, Germany, 2017; pp. 176–186.
87. Syed, M.H.; Fernandez, E.B.; Moreno, J. A misuse pattern for DDoS in the IoT. In Proceedings of the 23rd European Conference on Pattern Languages of Programs, Irsee, Germany, 4–8 July 2018; p. 34.
88. Pajila, P.J.B.; Julie, E.G. Detection of DDoS attack using SDN in IoT: A survey. In *Advances on P2P, Parallel, Grid, Cloud and Internet Computing*; Springer Science and Business Media LLC.: Cham, Switzerland, 2019; pp. 438–452.
89. Malik, M.; Kamaldeep; Dutta, M. Defending DDoS in the insecure internet of things: A survey. In *Advances in Intelligent Systems and Computing*; Springer Science and Business Media LLC.: Singapore, 2018; pp. 223–233.
90. Pour, M.S.; Bou-Harb, E.; Varma, K.; Neshenko, N.; Pados, D.A.; Choo, K.K.R. Comprehending the IoT cyber threat landscape: A data dimensionality reduction technique to infer and characterize Inter-net-scale IoT probing campaigns. *Digit. Investig.* **2019**, *28*, S40–S49. [CrossRef]
91. Maroof, U.; Shaghaghi, A.; Jha, S. PLAR: Towards a Pluggable Software Architecture for Securing IoT De-vices. In Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things, London, UK, 15 November 2019; pp. 50–57.
92. Hu, H.; Zhai, X.; Wang, M.; Hu, G. Linked-behaviors profiling in IoT networks using Network Connection Graphs (NCGs). In *International Conference on Cloud Computing and Security*; Springer Science and Business Media LLC.: Cham, Switzerland, 2018; pp. 429–439.
93. Moh, M.; Raju, R. Using machine learning for protecting the security and privacy of internet of things (IoT) systems. *Fog Edge Comput.* **2019**, *30*, 223–257. [CrossRef]
94. Banerjee, M.; Lee, J.; Choo, K.-K.R. A blockchain future for internet of things security: A position paper. *Digit. Commun. Netw.* **2018**, *4*, 149–160. [CrossRef]
95. Al-Hayajneh, A.; Bhuiyan, Z.A.; McAndrew, I. Improving Internet of Things (IoT) security with soft-ware-defined networking (SDN). *Computers* **2020**, *9*, 8. [CrossRef]
96. Kumar, A.; Lim, T.J. Early detection of mirai-like IoT bots in large-scale networks through sub-sampled packet traffic analysis. In *Future of Information and Communication Conference*; Springer: Cham, Switzerland, 2019; pp. 847–867.
97. Miettinen, M.; Sadeghi, A.-R. Keynote: Internet of things or threats? On building trust in IoT. In Proceedings of the 2018 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS), Torino, Italy, 30 September–5 October 2018; pp. 1–9.
98. MubarakAli, A.; Srinivasan, K.; Mukhalid, R.; Jaganathan, S.C.B.; Marina, N. Security challenges in internet of things: Distributed denial of service attack detection using support vector machine-based expert systems. *Comput. Intell.* **2020**, *36*, 1580–1592. [CrossRef]
99. Yang, Y.; Wang, J.; Zhai, B.; Liu, J. IoT-Based DDoS Attack Detection and Mitigation Using the Edge of SDN. In *International Symposium on Cyberspace Safety and Security*; Springer: Cham, Switzerland, 2019; p. 3.
100. Parmisano, A.; Garcia, S.; Erquiaga, M.J. *A Labeled Dataset with Malicious and Benign IoT Network Traffic*; Stratosphere Laboratory: Prague, Czech Republic, 2020.
101. Guerra-Manzanares, A.; Medina-Galindo, J.; Bahsi, H.; Nõmm, S. MedBIoT: Generation of an IoT Botnet Dataset in a Medium-sized IoT Network. In Proceedings of the 6th International Conference on Information Systems Security and Privacy, Valletta, Malta, 25–27 February 2020; pp. 207–218.
102. Tambe, A.; Aung, Y.L.; Sridharan, R.; Ochoa, M.; Tippenhauer, N.O.; Shabtai, A.; Elovici, Y. De-tection of threats to IoT devices using scalable VPN-forwarded honeypots. In Proceedings of the 9th ACM Conference on Data and Application Security and Privacy, Dallas, TX, USA, 25–27 March 2019; pp. 85–96.
103. Hakim, M.A.; Aksu, H.; Uluagac, A.S.; Akkaya, K. U-PoT: A Honeypot Framework for UPnP-Based IoT Devices. In Proceedings of the 2018 IEEE 37th International Performance Computing and Communications Conference (IP-CCC), Orlando, FL, USA, 17–19 November 2018.
104. Acien, A.; Nieto, A.; Fernandez, G.; Lopez, J. A Comprehensive methodology for deploying IoT honeypots. In *Proceedings of the International Conference on Trust and Privacy in Digital Business, Regensburg, Germany, 5–6 September 2018*; Springer: Cham, Switzerland, 2018; pp. 229–243.
105. Pauna, A.; Bica, I.; Pop, F.; Castiglione, A. On the rewards of self-adaptive IoT honeypots. *Ann. Telecommun.* **2019**, *74*, 501–515. [CrossRef]

106. Amanullah, M.A.; Habeeb, R.A.A.; Nasaruddin, F.H.; Gani, A.; Ahmed, E.; Nainar, A.S.M.; Akim, N.M.; Imran, M. Deep learning and big data technologies for IoT security. *Comput. Commun.* **2020**, *151*, 495–517. [CrossRef]
107. Otoum, Y.; Liu, D.; Nayak, A. DL-IDS: A deep learning–based intrusion detection framework for securing IoT. *Trans. Emerg. Telecommun. Technol.* **2019**. [CrossRef]
108. Niu, W.; Zhang, X.; Du, X.; Zhao, L.; Cao, R.; Guizani, M. A deep learning based static taint analysis approach for IoT software vulnerability location. *Measurement* **2020**, *152*, 107139. [CrossRef]
109. Almiani, M.; AbuGhazleh, A.; Al-Rahayfeh, A.; Atiewi, S.; Razaque, A. Deep recurrent neural network for IoT intrusion detection system. *Simul. Model. Pr. Theory* **2020**, *101*, 102031. [CrossRef]
110. Parra, G.D.L.T.; Rad, P.; Choo, K.K.R. Implementation of deep packet inspection in smart grids and industrial Internet of Things: Challenges and opportunities. *J. Netw. Comput. Appl.* **2019**, *135*, 32–46. [CrossRef]
111. Akter, M.; Das Dip, G.; Mira, M.S.; Hamid, A.; Mridha, M.F. Construing Attacks of Internet of Things (IoT) and A Prehensile Intrusion Detection System for Anomaly Detection Using Deep Learning Approach. In *Advances in Intelligent Systems and Computing*; Springer: Singapore, 2019; pp. 427–438.
112. Krishnan, P.; Najeem, J.S.; Achuthan, K. SDN Framework for Securing IoT Networks. In *Ubiquitous Communications and Network Computing, Proceedings of the Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Bangalore, India, 3–5 August, 2019*; Springer: Cham, Switzerland, 2018; pp. 116–129.
113. Rathore, S.; Kwon, B.W.; Park, J.H. BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network. *J. Netw. Comput. Appl.* **2019**, *143*, 167–177. [CrossRef]
114. Kamal, M.; Aljohani, A.; Alanazi, E. IoT meets COVID-19: Status, challenges, and opportunities. *arXiv* **2007**, arXiv:2007.12268.
115. Rafique, W.; Khan, M.; Sarwar, N.; Dou, W. A security framework to protect edge supported software defined Internet of Things infrastructure. In *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*; Springer: Cham, Switzerland, 2019; pp. 71–88.
116. Pinno, O.J.A.; Grégio, A.R.A.; De Bona, L.C. ControlChain: A new stage on the IoT access control authorization. *Concurr. Comput. Pr. Exp.* **2020**, *32*, 5238. [CrossRef]
117. Cui, P.; Guin, U.; Skjellum, A.; Umphress, D. Blockchain in IoT: Current trends, challenges, and future roadmap. *J. Hardw. Syst. Secur.* **2019**, *3*, 338–364. [CrossRef]
118. AlRashdi, I.; Alqazzaz, A.; Aloufi, E.; Alharthi, R.; Zohdy, M.; Ming, H. AD-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning. In Proceedings of the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 7–9 January 2019; pp. 305–310.
119. Vahabi, M.; Fotouhi, H.; Björkman, M. FIREWORK: Fog orchestration for secure IoT networks. In *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*; Springer: Cham, Switzerland, 2019; pp. 311–317.
120. Kim, Y.; Nam, J.; Park, T.; Scott-Hayward, S.; Shin, S. SODA: A software-defined se-curity framework for IoT environments. *Comput. Netw.* **2019**, *163*, 106889. [CrossRef]
121. Kumar, K.; Kumar, N.; Shah, R. Role of IoT to avoid spreading of COVID-19. *Int. J. Intell. Netw.* **2020**, *1*, 32–35. [CrossRef]
122. Beek, C. McAfee Labs Covide-19 Threat Report. 2020. Available online: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-july-2020.pdf (accessed on 5 March 2021).