IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 28, 2020, accepted November 16, 2020, date of publication November 24, 2020,
date of current version December 8, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3039985

Systematic Literature Review on IoT-Based Botnet Attack

IHSAN ALI[1], (Senior Member, IEEE), ABDELMUTTLIB IBRAHIM ABDALLA AHMED[1], AHMAD ALMOGREN[2], (Senior Member, IEEE), MUHAMMAD AHSAN RAZA[3], SYED ATTIQUE SHAH[4], ANWAR KHAN[5], AND ABDULLAH GANI[1,6], (Senior Member, IEEE)

[1]Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur 50603, Malaysia
[2]Chair of Cyber Security, Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11633, Saudi Arabia
[3]Department of Information Technology, Bahauddin Zakariya University, Multan 60000, Pakistan
[4]Department of Computer Science, Balochistan University of IT, Engineering and Management Sciences, Quetta 87300, Pakistan
[5]Department of Electronics, University of Peshawar, Peshawar 25120, Pakistan
[6]Faculty of Computing and Informatics, University Malaysia Sabah, Labuan 88400, Malaysia

Corresponding authors: Ahmad Almogren (ahalmogren@ksu.edu.sa), Ihsan Ali (ihsanalichd@siswa.um.edu.my), and Abdullah Gani (abdullahgani@ums.edu.my)

The authors are grateful to the Deanship of Scientific Research, King Saud University for funding through Vice Deanship of Scientific Research Chairs and Faculty of Computer Science and Information Technology, University of Malaya, through Postgraduate Research Grant PG035-2016A.

ABSTRACT The adoption of the Internet of Things (IoT) technology is expanding exponentially because of its capability to provide a better service. This technology has been successfully implemented on various devices. The growth of IoT devices is massive at present. However, security is becoming a major challenge with this growth. Attacks, such as IoT-based botnet attacks, are becoming frequent and have become popular amongst attackers.IoT has a resource constraint and heterogeneous environments, such as low computational power and memory. Hence, these constraints create problems in implementing a security solution in IoT devices. Therefore, various kind of attacks are possible due to this vulnerability, with IoT-based botnet attack being one of the most popular.In this study, we conducted a comprehensive systematic literature review on IoT-based botnet attacks. Existing state of the art in the area of study was presented and discussed in detail. A systematic methodology was adopted to ensure the coverage of all important studies. This methodology was detailed and repeatable. The review outlined the existing proposed contributions, datasets utilised, network forensic methods utilised and research focus of the primary selected studies. The demographic characteristics of primary studies were also outlined.The result of this review revealed that research in this domain is gaining momentum, particularly in the last 3 years (2018-2020). Nine key contributions were also identified, with Evaluation, System, and Model being the most conducted.

INDEX TERMS IoT, botnet, systematic review.

I. INTRODUCTION

The general idea of the Internet of Things (IoT) is to allow for communication between human-to-thing or thing-to-thing(s) [1]. Things denote sensors or devices, whilst human or an object is an entity that can request or deliver a service [2]. The interconnection amongst the entities is always complex. IoT is broadly acceptable and implemented in various domains, such as healthcare, smart home and agriculture. However, IoT has a resource constraint and heterogeneous environments, such as low computational power and memory. These constraints create problems in providing and implementing a security solution in IoT devices. These constraints further escalate the existing challenges for IoT environment. Therefore, various kinds of attacks are possible due to the vulnerability of IoT devices. IoT-based botnet attack is one of the most popular, spreads faster and create more impact than other attacks. In recent years, several works have been conducted to detect and avoid this kind of attacks [3]–[4] by using novel approaches.Hence, a plethora of relevant of relevant models, methods, and etc. have been introduced over the past few years, with quite a reasonable number of studies reported in the research domain. Various review and survey papers have also been published in this

The associate editor coordinating the review of this manuscript and approving it for publication was Nabil Benamar.

area of research Section (II). However, from our knowledge, systematic literature review (SLR) on IoT-based botnet attack is lacking. Thus, this study will fill the research gap.

In this work, studies were collected from the year 2016 to 2020 using an adopted evidence-based systematic methodology. With the guide of an evidence-based method utilised, 5465 studies were initially collected. Through the formulated inclusion and exclusion criteria, we ultimately selected 34 studies that are related to our defined research questions. The results based on our selected primary studies were outlined, and challenges and future research directions were given.

The contributions of this study are threefold, and these contributions are stated as follows:

- The conduction of a comprehensive SLR on IoT-based botnet attacks.
- A detailed analysis and discussion of the primary studies based on the defined research questions.
- The identification of key research challenges with future research directions.

This SLR is planned as follows. The related works are given in Section II. Section III presents the research method utilised for this study, which is in-line with Keele *et al.* [5] and Petersen *et al.* [6]'s general principles of conducting systematic reviews. In Section IV, the results of the study with respect to the defined research questions are given. The discussion of the analysed result is given in Section V. The study is concluded in Section VI.

II. RELATED WORK

In this section, we have highlighted all the identified related works that are in-line to our work. Hence, with this, the paper contribution is further emphasis. The existing survey and review papers are highlighted and discussed in this section. The papers discussed in this section are review and survey papers that are done in relation to IoT botnet attacks.

Ji *et al.* conducted a study to analyse and understand botnet and its prevention policies in IoT [7]. The authors specifically analysed mirai architecture and its components. Furthermore, botnet propagation model attack processes and impact factor were all studied. The challenges and existing solutions for deep learning and forensics mechanisms for botnet in IoT were surveyed by Koroniotis *et al.* [8]. The authors further investigated the utilisation of deep learning in network forensics. Existing issues and future research directions were outlined as well. Alhajri *et al.* surveyed anomaly detection of IoT botnets using machine learning [9]. The authors investigated the possibility of utilising autoencoders to detect IoT botnets. The authors outlined future research directions for the utilisation of machine learning in this domain. Salim *et al.* surveyed distributed denial of service (DDoS) attacks and conducted their defences in IoT [10]. The authors also outlined the reasons why attackers prefer IoT devices for DDoS attacks. Key methods used for defence in the existing works against DDoS attacks were presented. Singh *et al.* comprehensively surveyed domain name system (DNS)-based botnet detection [11]. The work provides a new classification of DNS-based botnet detection techniques with thorough analysis of each technique. Dange and Chatterjee also reviewed the distinct kinds of potential attack on IoT and the considerable attention of attackers to botnet [2]. The authors further outlined the main differences between traditional botnet and IoT botnet. Lastly, Sengupta surveyed attacks, security issues in IoT, industrial IoT and blockchain [12]. By examining all the review studies, we find no SLR in the research domain that focused on IoT-based botnet attacks. Thus, this study is eminent to help researchers in understanding the research area. Table 1 highlights the identified current survey and review papers in the research domain.

TABLE 1. Existing review and survey studies in the research domain.

Studies	Type of study	Year of publication
[7]	Review	2018
[8]	Survey	2019
[9]	Survey	2019
[10]	Survey	2019
[11]	Survey	2019
[2]	Review	2020
[12]	Survey	2020

III. RESEARCH METHOD

This section outlines the method used for this study. The method is in-line with Keele *et al.* [5] and Petersen *et al.* [6]'s general principles of conducting systematic reviews. The methodology is composed of planning and the execution of the review. Thus, the methodology utilized five clear steps as follows:

- The formulation of key research questions.
- The formulation of the search processes.
- The formulation of the general criteria for the selection of articles.
- The data extraction process, and
- The execution of analysis and classification.

This section further discusses each of these individual steps outlining the decisions and application of the methodology.

A. RESEARCH QUESTIONS

In defining research questions, the entire research field has to be considered. This consideration will be regarding how studies explored these research fields and their common characteristics. This process is composed of a process of breaking down a prime research question into many. Our main research question is 'What is the state of the art in the field of study of IoT-based botnet attacks'. This study aims to investigate the existing research conducted in the field of study. Thus, the following research questions were put forward to achieve the objective of this study.

- RQ1: What are the contributions of the primary studies?
- RQ2: What are the network forensic methods utilised by the primary studies? Do the studies focus on IoT botnet attack detection or avoidance?

- RQ3: What are the datasets utilised by the primary studies?
- RQ4: What are the evaluation metrics utilised by the primary studies?
- RQ5: What are the demographic characteristics of the primary studies?

1) DATA SOURCES AND SEARCH STRATEGY

In this study, we selected five data sources for the retrieval of important articles from the literature. These data sources are Science Direct (http://sciencedirect.com/), Springer Link (http://link.springer.com/), IEEE Xplore (http://ieeexplore.ieee.org/), ACM (http://dl.acm.org/), and Wiley (http://onlinelibrary.wiley.com/). In these data sources, the queries considered filtering by title (either document or publication), abstract, metadata and keywords. Utilising these filters the right way helps in obtaining a reasonable number of studies without missing key works. With respect to our search strategy, this SLR utilised some selected keywords for primary studies search in our selected data sources. Thus, in choosing the keywords, we opted to be as broad and specific as possible with respect to our formulated research questions. We chose keywords, such as botnet attack, Internet of things and IoT, to formulate our search string. The search string for this study was 'botnet attack OR IoT AND Internet of Things'. This search string will be used in all the selected data sources for the retrieval of primary studies.

B. STUDY SELECTION AND QUALITY ASSESSMENT

For primary study selection, we utilised a set of inclusion and exclusion criteria. These criteria were used on all the studies collected in the distinct stages of the study selection process, as presented in Table 2. For study inclusion criteria, we selected studies that achieve the following criteria:

- ICR1: A study has to be in a journal or proceedings.
- ICR2: A study must focus on IoT-based botnet attack.
- ICR3: A study must be written in the English language.
- ICR4: A study must be published from 2016 to 2020.

For study exclusion criteria, a given study was excluded if it meets one of the following criteria.

- ECR1: A study that is unavailable in hard or electronic format.
- ECR2: A study with duplicate copy reporting the same results.
- ECR3: A study that is not written in English.
- ECR4: The study does not relate to IoT-based botnet attack.

With respect to quality assessment, we assessed the quality of each primary study based on our set of quality criteria. Thus, the quality criteria of this study were based on a formulated quality assessment questions presented in Table 3. For the result in Table 3, YES carries 1 point, Partial carries 0.5 points, and NO carries 0 points. Thus, for each quality assessment question, the score obtained by a given study will be recorded and tallied to obtain the overall score.

TABLE 2. Study selection process.

Data Source ID	Data Source Name	Initial Results of the Search	Final Selected Studies based on Fulfilment of our Criteria
D1	IEEE Xplore	610	20
D2	Science direct	2889	2
D3	ACM	1670	5
D4	Springer Link	244	5
D5	Wiley	52	2

C. DATA EXTRACTION

In the process of data extraction, we collected important data of the primary studies for analysis.Thus, the analysis considered each research question. In Table 4, we present the information fields and their association with the respective research questions. Firstly, data that identify the article uniquely were extracted.Then, the articles were reviewed manually by the respective researchers to answer the research questions.

D. ANALYSIS AND CLASSIFICATION

The primary studies were classified into different facets on the basis of the analysis of the results obtained. Thus, the classification was performed in relation to the individual research question. This way enabled summarisation of results to obtain the answers for the questions. Therefore, the classification of the primary studies was broken down into various categories with respect to the research questions. These categories were the contributions of the primary studies, the network forensic methods utilised, the dataset used and the evaluation metric used. The contribution facets composed of proposals such as approach, software architecture, techniques, model, algorithm, evaluation/investigation, method, mechanism, dataset and framework. This classification was inspired by the researcher in [5], who recommended this kind of classification. The second facets was the classification based on network forensic methods. These methods, as classified,

TABLE 3. Quality assessment questions.

QA	Questions
1	Does the study clearly state the objective of the research?
2	Does the topic of the study cover the answers to our research questions?
3	Is the study result evaluated?
4	Is the study well referenced?
5	Is the method proposed or used in the study well described?

TABLE 4. Data extraction form.

Data Item	Values	Question
Headers		
Id	Integer	
Title	Title of paper	
Authors First name	The first author name	Q5
Name of Publication	The publication venue name	Q5
Focused questions		
Contribution	The contribution of the study	Q1
Network Forensic Method	The network forensic method used	Q2
Dataset	The dataset utilized	Q3
Evaluation Metric	The evaluation metric used	Q4
Statistical questions		
Publication Year	Year	Q5
Publication Type	Venue and research data sources	Q5
Citation Count	Citation	Q5

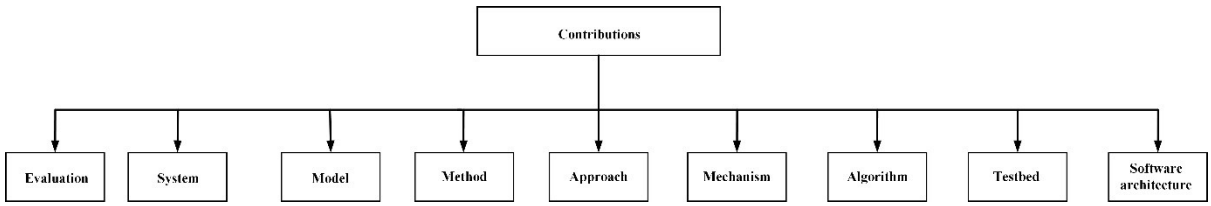

FIGURE 1. Classification of the Research Contributions by the Primary Studies.

were honeypot, network flow analysis and intrusion detection system. We classified the utilised datasets by the primary studies with the evaluation metrics used as well.

IV. RESULTS

In this section, we discuss the results of each research question in detail.

A. RQ1:WHAT ARE THE CONTRIBUTIONS OF THE PRIMARY STUDIES?

This section provides a general overview of the research contributions proposed by the primary studies. Thus, in answering this research question, all the studies that proposed these contributions will be discussed in each paragraph.We identify nine contributions proposed by the primary studies in this domain. These contributions are classified and highlighted in Figure 1. Therefore, Evaluation was conducted by 26.47% of the primary studies (the most conducted), followed by System with 17.65%, Model (17.65%), Method (14.71%), Approach (11.76%), Mechanism (2.94%), Algorithm (2.94%), Testbed (2.94%) and Software architecture (2.94%). Thus, the following paragraphs discuss the studies that proposed these contributions. With respect to Evaluation, we identify 9 studies (26.47% of the primary studies) that conduct it. Gopal *et al.* analysed mirai malware with its exploitation techniques to stop IoT botnet from spreading. The experimental results indicated the successes of blocking mirai malware [19].Nomm and Bahsi evaluated the use of unsupervised learning models with reducing feature set sizes to help decrease computational resource utilisation [14]. The study showed that training a single model for all IoT devices is better than training specific model for each IoT device. Hallman *et al.* explored the existing challenges to cybersecurity in the environment of IoT. The authors further examined the general utilisation of IoT botnets [35]. An evaluation study on mirai botnet was conducted by Margolis *et al.* [31]. The authors examined mirai capabilities, its spread to new devices and their impact. Furthermore, the authors proposed a set of mitigation solutions to help mitigate future attacks. Tanabe *et al.* analysed IoT botnet infrastructure by focusing on bashlite, mirai and tsunami [37]. The evaluation results showed a good outcome and provided a clear insight into IoT

TABLE 5. Overview of selected studies.

Identifier	Study reference	Publication year	Publication channel	Citation count	Contribution
A1	[13]	2019	IEEE	1	Method
A2	[14]	2018	IEEE	17	Evaluation
A3	[15]	2018	IEEE	5	Algorithm
A4	[16]	2018	IEEE	1	Model
A5	[17]	2018	Springer	2	Testbed
A6	[18]	2019	Springer	3	Mechanism
A7	[19]	2018	IEEE	10	Evaluation
A8	[20]	2018	IEEE	49	Model
A9	[21]	2020	Springer	4	Method
A10	[22]	2019	Springer	4	System
A11	[23]	2020	Springer	15	Method
A12	[3]	2019	ACM	4	Approach
A13	[24]	2019	ACM	7	Evaluation
A14	[25]	2019	ACM	0	Model
A15	[26]	2019	ACM	12	Model
A16	[27]	2018	IEEE	19	System
A17	[28]	2019	IEEE	1	System
A18	[29]	2019	IEEE	13	Model
A19	[30]	2018	IEEE	39	Evaluation
A20	[31]	2017	IEEE	17	Evaluation
A21	[32]	2019	IEEE	1	Approach
A22	[33]	2018	IEEE	15	Approach
A23	[34]	2018	IEEE	6	Approach
A24	[35]	2017	Wiley	49	Evaluation
A25	[36]	2018	Wiley	4	System
A26	[37]	2020	ACM	0	Evaluation
A27	[38]	2019	Science Direct	1	Software architecture
A28	[39]	2020	Science Direct	2	Evaluation
A29	[40]	2016	IEEE	14	System
A30	[4]	2018	IEEE	214	Method
A31	[41]	2019	IEEE	6	Evaluation
A32	[42]	2017	IEEE	20	Model
A33	[43]	2018	IEEE	3	System
A34	[44]	2018	IEEE	15	Method

botnet anatomy. Marzano *et al.* studied mirai and bashlite botnets [30]. They mainly focused on the evolution of malware and the changes in botnet operator behaviour. The results indicated that mirai botnet is more resilient and supports more effective attacks. An evaluation on how users perceive security and privacy in IoT devices with respect to botnet activities was conducted by McDermott *et al.* [24]. The authors utilised experiments to examine users' ability to detect threats. The results showed that the user finds it difficult to detect and be aware of threats in the absence of clear signs. Zhang *et al.* conducted a digital forensic case study on mirai botnet. The authors further discussed database servers, command and control servers, forensic artefacts on the attacker's terminal and the network packet for the attacks [39]. The authors outlined how a forensic expert can remotely obtain some of these artefacts without physical access to botnet servers.An analysis of Rustock botnet domain names was conducted on multiple aspects by Li *et al.* [41].The authors attempted to understand botnet detection in these domain names. The results of an experiment guides future botnet

detection. With regard to System proposal, we identify six studies that proposed it, which amount to 17.65% of the primary studies. A system named AutoBotCatcher was proposed by Sagirlar *et al.* [27]. The system aims to detect P2P botnets in IoT. The key idea behind the system design is the concern that bots related to the same botnet converse often with each other and create clusters. Sajjad and Yousaf proposed a system for botnet detection [43]. The system has three key modules, which are monitor, descriptor and comparator. The results showed that the system can detect mirai IoT malware. A solution was proposed in [40] to detect and prevent malicious connections by utilising machine learning. The newly proposed solution combines key features that mine correlations from packet history for servers and hosts. The results signified that the proposed solution can successfully detect network intrusions and botnet communication with high precision. An adaptive filter was proposed by Kumar and Bhama [22]. The proposed system helps in avoiding DDoS attacks from various vulnerable IoT bots. The experimental results showed that IoT botnet detection is achieved with high accuracy. Yin *et al.* proposed a system named ConnSpoiler to detect IoT-based botnets. This detection was conducted by identifying algorithmically generated domains effectively [28]. The results on an evaluation of DNS traffic showed that the proposed system identifies the devices compromised by unidentified botnets. Spaulding *et al.* proposed a new system named DRIFT [36]. The system helps in identifying command and control domain names in IoT botnets. The results showed that the system is effective with good accuracy of malware detection. Model contributes 17.65% of the primary studies. McDermott *et al.* proposed the use of deep learning to build a detection model [20]. The results established the efficacy of the proposed model with regard to botnet detection. Hachinyan *et al.* proposed a mathematical model of attack on IoT devices [16]. This model was built to stop the attempt of cracking IoT devices. In a study by Irfan *et al.*, a model was proposed, which was devised to classify incoming data in IoT devices to specifically check if the data contain malware [25]. On the basis of an experiment conducted with a traffic data taken from UCI machine learning depository's website, the results showed a good outcome. Gardner *et al.* proposed a model to explain the spread of IoT worms [42]. The model uses SEIRs (susceptible-exposed-infected-recoverysusceptible) epidemic model. The results showed that IoTBAI can reduce or mitigate IoT botnet attacks. An analytical model was proposed by Farooq and Zhu [29]. The model aims to study the device-to-device spread of malware in IoT wireless networks. The results showed that the proposed model is critical in assisting with planning, design and defence of vulnerable IoT wireless networks. Acarali *et al.* proposed a new propagation model coined as IoTSIS [26]. The model considers specific characteristics of IoT, such as limited energy, restricted processing power and node density, when arranging botnet. The proposed model was built to examine the dynamics of the attack spread by mitigating simulations. The results showed some progress. Method contributes 14.71% of the primary studies, where only five studies out of the 34 primary studies proposed it. Tzagkarakis *et al.* proposed a method used to identify IoT botnet attack [13]. A sparse representation framework with reconstruction error thresholding rule was utilised to identify malicious network traffic. The proposed method is more effective than the existing methods. Bahsi *et al.* proposed the use of a machine learning method in detecting IoT bots [44]. With the utilisation of feature selection, the authors showed that fewer features can archive very high accuracy. Meidan *et al.* proposed a new network-based anomaly detection method [4]. The method retrieves behaviour snapshots of a given network and utilises autoencoders to detect suspicious network traffic from suspicious IoT devices. The evaluation results demonstrated that the proposed method can accurately detect attacks when they are initiated from suspicious IoT devices. Nguyen *et al.* proposed a new lightweight method used to detect IoT botnet [21]. The results showed improvements in terms of accuracy of detection. Al Shorman *et al.* proposed a new unsupervised method for IoT botnet attack detection. The proposed method helps in detecting IoT botnet attack that is launched in a compromised IoT device. The experimental results established that the method is better than the compared state of the art. Another contribution is Approach, which was proposed by four studies (11.76% of the primary studies). A new approach was proposed by Giachoudis *et al.* [32]. The approach was built for IoT security that is based on distributed multiagent system. Thus, a lightweight agent was utilised in each multiple IoT installation to detect security instances and prevent potential attacks. The simulation results signified that the proposal minimises the effect of DDoS attacks done with IoT device botnets. Dietz *et al.* proposed an IoT botnet detection and isolation approach at access router level [34]. The approach helps in preventing the compromise IoT devices to be compromised without technical, administrative knowledge. Nguyen *et al.* proposed a new approach for Linux IoT botnet detection [33]. The approach combines CNN graph and PSI classifier. The results indicated that the proposed approach performs better and achieves good outcome in terms of accuracy and F-measure. Ceron *et al.* introduced a new approach that handles network traffic that is generated by IoT malware. The proposed approach was designed to modify traffic at the network layer based on the actions conducted by the malware [3]. The authors investigated mirai and bashlite botnets. The experimental results indicated that the proposed approach can handle malicious network traffic and can be utilised to modify botnet instruction messages and manipulate the network flow. The rest of the contributions by the primary studies are Mechanism (2.94%), Algorithm (2.94%), Testbed (2.94%) and Software architecture (2.94%). Shah and Venkatesan proposed a mechanism to alter the intricacy of the puzzle after every login try. This mechanism ensures that, if all the IoT devices have utilised the login puzzle, then mirai attack will require two months to be affected [18]. The results showed some progress. Gurulakshimi and Nesarani

TABLE 6. Contributions of the primary studies.

Contribution	Studies	Number	Percentage
Evaluation	A31, A28, A26, A24, A20, A19, A13, A7, A2	9	26.47%
System	A33, A29, A25, A17, A16, A10	6	17.65%
Model	A32, A18, A15, A14, A8, A4	6	17.65%
Method	A34, A30, A11, A9, A1	5	14.71%
Approach	A23, A22, A21, A12	4	11.76%
Mechanism	A6	1	2.94%
Algorithm	A3	1	2.94%
Testbed	A5	1	2.94%
Software architecture	A27	1	2.94%

TABLE 7. Network forensic method.

Network forensic method	Studies	Number	Percentage
Network flow analysis	A4, A8, A14, A15, A18, A32, A12, A21, A22, A23, A3, A5,A10, A16, A17, A25, A29, A33, A6, A1, A9, A11, A30, A34, A2, A7, A13, A20, A24, A28, A31	31	91.18%
Honeypot	A27, A19, A26	3	8.82%

TABLE 8. Research focus.

Research Focus	Studies	Number
Detection	A19, A26, A27, A8, A21, A22, A23, A3, A16, A17, A25, A29, A33, A1, A9, A11, A30, A34, A2, A13, A28, A31	22
Avoidance	A4, A14, A15, A18, A32, A12, A5, A10, A6, A7, A20, A24	12

used support vector machine (SVM) algorithm to predict earlier abnormal activities [15]. Thus, the authors classified normal and abnormal traffic flow with the aid of the SVM algorithm. The results showed some improvements. Kumar and Lim built a testbed that will be used to evaluate IoT botnets. The authors further designed a mitigation technique that will be used against them [17]. The name of this testbed proposed is DETERLAB-based IoT testbed. The authors highlighted some key features of the proposed testbed with its capabilities. In a study by Oliveri and Lauria, a software architecture named Sagashi was proposed to infiltrate IoT botnets [38]. The results showed some promise. Table 6 presents and categorises the contributions with regard to the studies that proposed them.

B. RQ2. WHAT ARE THE NETWORK FORENSIC METHODS UTILISED BY THE PRIMARY STUDIES? DO THE STUDIES FOCUS ON BOTNET ATTACK DETECTION OR AVOIDANCE?

To answer this research question, we adopted the categorisation of the network forensic methods from [8] with respect to botnet investigation. In this previous study, the authors investigated botnet and its attack and further classified the network forensic methods utilised in the research domain. Therefore, in the current study, we identify two forensic methods used by our primary studies. These methods are network flow analysis and honeypot, which are highlighted in Table 7 and the studies that utilised them. Some studies have used network flow to analyse IoT botnet malware attacks, whilst other studies have used honeypot systems for the same purpose. Network flow analysis was used by 91.18% of the primary studies, whilst 8.82% of the primary studies used Honeypot systems. Thus, we observe that researchers find network flow analysis to be more appealing and realistic in terms of real-time attack detection and avoidance. From Figure 2, we highlight each forensic method with respect to the year and studies that utilised it in each year. For network flow analysis, we observe that 2018 was the most active year of its utilisation, followed by the year 2019. For the honeypot system, the utilisation is flat, with one study published each year from 2018 to 2020. Thus, this yearly analysis shows that researchers lean more on network flow analysis in this research domain. We further categorised the primary studies based on the studies research focus, specifically whether the studies focused on IoT botnet attack detection or avoidance. Table 8 highlights the studies with respect to their focus. We observe that 22 studies are focused on the detection of IoT botnet attacks, whilst 12 studies are focused on avoiding the attacks rather than detecting them. This finding is disadvantageous to the organisation experiencing such attack. Researchers should focus more on IoT botnet attack avoidance because as the saying goes, 'prevention is better than cure'. We believe organisations will save a large amount of financial expenditure if they focus more on attack avoidance than on detection. Figure 3 provides

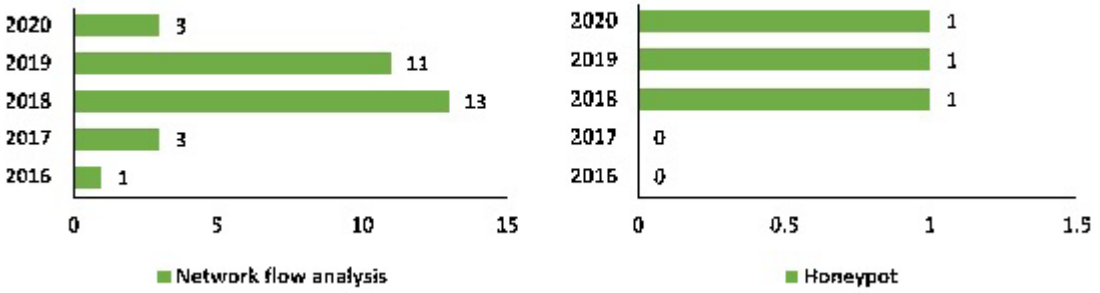

FIGURE 2. Yearly analysis of the network forensic methods utilised by the primary studies.

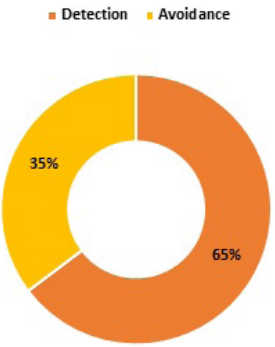

FIGURE 3. Primary studies focus on both botnet detection and avoidance.

a pictorial representation, percentage-wise, of the research focus utilisation.

C. RQ3. WHAT ARE THE DATASETS UTILISED BY THE PRIMARY STUDIES?

From Table 9, we highlight all the datasets used by each of the primary studies. We identify seven unique datasets used by 30 studies, which amount to 88.24% of the primary studies. Four studies did not clearly state which dataset they utilised (A18, A20, A23 and A24). The results demonstrate that 13 (38.24%) of the primary studies used Network traffic as their form of a dataset, which is the most utilised. By contrast, 9 (26.47%) of the primary studies utilised DNS traffic for their experiment. The two datasets were utilised by 64.71% of the primary studies

D. RQ4. WHAT ARE THE EVALUATION METRICS UTILIZED BY THE PRIMARY STUDIES?

Table 9 shows all the evaluation metrics utilised by the primary studies. We observe that seven studies, namely, A6, A16, A20, A23, A24, A26 and A28, did not identify which evaluation metric they utilised. We further identify three primary evaluation metrics that were used in this research domain for evaluating proposals. These metrics are Accuracy with nine (9) studies, followed by Precision (6) and Performance (5). These metrics were often used together with other sub-metrics to evaluate a given proposal. However, overall, these metrics were the most used by the primary studies.

E. RQ5. WHAT ARE THE DEMOGRAPHICS AND CHARACTERISTICS OF THE SELECTED STUDIES?

From the overall studies that were retrieved and studied based on all the defined criteria, 34 studies were finally selected for this study. The 34 studies were analysed to answer our defined research questions, which are outlined in Section III. In this section, the demographic characteristics are outlined and discuss. In Table 5, we show all the primary studies and their details.

1) PUBLICATION OVER TIME

Figure 4 presents the general evolution of the primary studies from 2016 to 2020. The figure shows that the research in this domain is more active, starting from 2018, where 14 studies were published, which amount to 41.18% of the primary studies. Moreover, 2016 is the year that has the lowest amount of studies with only one study published in that year (A29). In the year 2016, 2017, 2018, 2019 and 2020, the total number of works published are 1, 3, 14, 12 and 4. Thus, we expect more studies to be published in the year 2020 before the year ends.

2) PUBLICATION CHANNEL AND QUALITY SCORES

With regard to publication channels, we identify three key publication channels, as highlighted in Figure 5. These are Conference, Journal and Symposium. From our findings, we observe that Conferences are the most active publication channels in the research domain with 20 (58.82%) studies published in them, followed by Journal with 13 (38.24%) studies and lastly Symposium with 1 (2.94%) study. The quality of the primary studies is relatively low because only 38.24% of the primary studies were published in Journals. This situation is due to that publishing a paper in Journals is harder than that in other publication sources in most cases. As shown in Table 10, studies published in Journals mostly have a higher quality score. Publication sources are not presented in this section because all the sources published only one paper each. Therefore, these sources cannot be ranked and classified.

The result of the quality assessment of the primary studies is presented in Table 10. The table displays the individual score of each quality assessment question and the cumulative score of all studies individually. The results demonstrate that studies such as A8, A15, A17, A25, A27, A30 and A31 have

TABLE 9. Studies based on the dataset and evaluation metrics utilised.

Datasets	Evaluation metric	Study focus	Quality score	Study identifier
N-Balot dataset	Performance	Detection	3	A1
Network traffic	Performance	Detection	3.5	A2
Normal and abnormal data traffic	Precision, recall, and accuracy	Detection	4.5	A3
Network traffic	Performance	Avoidance	2	A4
DNS traffic	Transmission time of bots	Avoidance	3.5	A5
Network traffic	Nil	Avoidance	2	A6
DNS traffic	Performance	Avoidance	3	A7
DNS traffic	Accuracy, precision, recall, and F1 score	Detection	5	A8
Network traffic	Accuracy	Detection	4.5	A9
DNS traffic	Accuracy	Avoidance	4.5	A10
Network traffic	Accuracy and precision	Detection	4.5	A11
Network traffic	Number of packets per hour	Avoidance	4.5	A12
DNS traffic	Accuracy and detection rate	Detection	4.5	A13
UCI machine learning depository's website (traffic dataset)	Accuracy, precision, recall, and F1 score	Avoidance	4.5	A14
Network traffic	Node density and time	Avoidance	5	A15
DNS traffic	Nil	Detection	2.5	A16
DNS traffic	Effectiveness	Detection	5	A17
Nil	Time evolution and total cost of patching	Avoidance	4	A18
Data collected from monitors that connect to command and control servers (C and Cs)	Session durations and intersession times	Detection	3.5	A19
Nil	Nil	Avoidance	2	A20
Network traffic	Packet rate	Detection	3	A21
DNS traffic	Accuracy and F-measure	Detection	4	A22
Nil	Nil	Detection	2	A23
Nil	Nil	Avoidance	2	A24
NXDomain traffic	Accuracy	Detection	5	A25
Data collected from monitors that connect to command and control servers (C and Cs)	Nil	Detection	2.5	A26
Data collected from monitors that connect to command and control servers (C and Cs)	Mean duration of attack and payload size of the attack	Detection	5	A27
Data collected from monitors that connect to command and control servers (C and Cs)	Nil	Detection	4	A28
Network traffic	Precision	Detection	4	A29
Network traffic	Detection accuracy and detection time	Detection	5	A30
DNS traffic	Precision, recall, and F-measure	Detection	5	A31
Network traffic	Botnet reduction time	Avoidance	4	A32
Network traffic	Captured packets	Detection	3.5	A33
Network traffic	Accuracy	Detection	3.5	A34

the maximum quality score, which is 5 points. Notably, 6 of these studies were published in Journals. We further observe that studies such as A3, A9, A10, A11, A12, A13 and A14 have a total quality score of 4.5. Thus, with respect to our devised quality assessment question, 41.18% of the primary studies score 4.5 or above. Thus, this outcome is

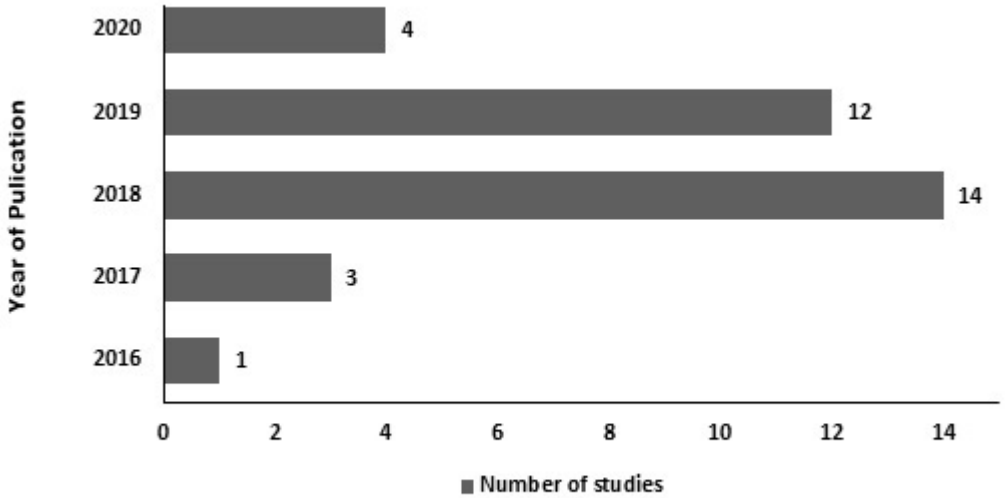

FIGURE 4. Publication Over time.

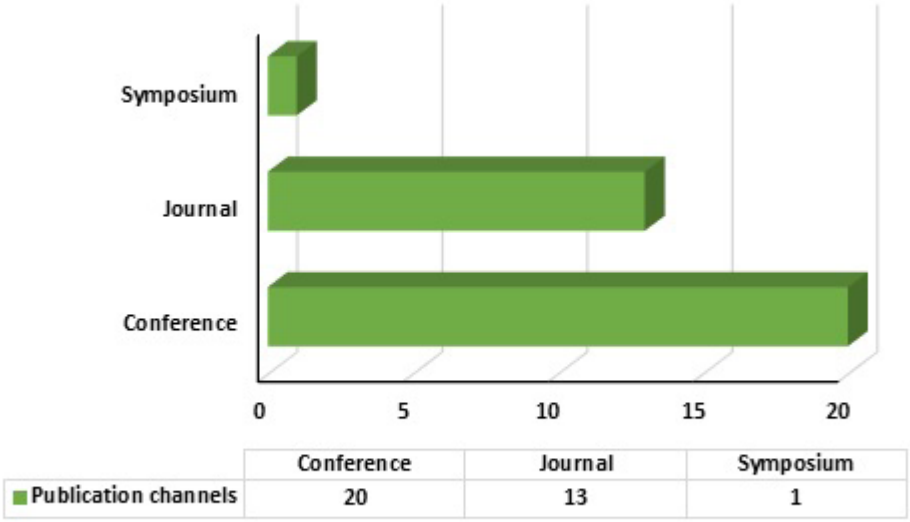

FIGURE 5. Publication Channel.

generally reasonable. However, 10 studies score 3 or less than 3, and they amount to 29.41% of the primary studies.

3) CITATION IMPACT

Table 11 shows the top 15 most cited articles from the primary studies. The citation count is bound to change with time; thus, it can change any point in time. The total citation count of all the 15 most cited papers in this domain is 518. However, the remaining articles that have less than 10 citations each cumulatively have a total citation count of 55. Thus, the overall citation count for all the primary studies is 573. Studies such as A30, A8 and A24 are the most influential with 214, 49 and 49 citations each, respectively.

4) GEOGRAPHICAL DISTRIBUTION

The top 10 most active countries in this research domain are presented in Table 12. We identify 17 active countries from primary studies. The United States (USA) with 6 studies is the most active, followed by United Kingdom (UK) with 4 studies. We barely see any study published from the African continent. This trend is normal in nearly every domain. However, more diversity is needed to further have more contribution from various continents.

V. DISCUSSION

This section outlines the research findings with respect to the answered research questions. The section further provides the identified study limitations that researchers need to focus on in future works. The threat to the validity of this study is also presented for transparency.

- The distribution of study contribution: The results analysed for research question 1 show that the contributions proposed by the primary studies are balanced in the sense that 5 out of 9 identified contributions are in total amount to 88.24% of the primary studies. The five contributions all have nothing less than 11% of the total

TABLE 10. Quality evaluation of the selected studies.

Study	QA1	QA2	AQ3	QA4	AQ5	Total Score
A1	0	1	1	0.5	0.5	3
A2	0.5	1	1	0.5	0.5	3.5
A3	1	1	1	0.5	1	4.5
A4	0.5	0.5	0	0.5	0.5	2
A5	1	1	1	0.5	0	3.5
A6	0.5	0.5	0	0.5	0.5	2
A7	1	1	0.5	0.5	0	3
A8	1	1	1	1	1	5
A9	0.5	1	1	1	1	4.5
A10	1	1	1	1	0.5	4.5
A11	1	0.5	1	1	1	4.5
A12	1	0.5	1	1	1	4.5
A13	1	1	1	1	0.5	4.5
A14	1	1	1	0.5	1	4.5
A15	1	1	1	1	1	5
A16	1	0.5	0	0.5	0.5	2.5
A17	1	1	1	1	1	5
A18	1	0.5	1	0.5	1	4
A19	0.5	1	1	0.5	0.5	3.5
A20	1	0.5	0	0.5	0	2
A21	1	0.5	0.5	0.5	0.5	3
A22	1	1	1	0.5	0.5	4
A23	0.5	0.5	0	0.5	0.5	2
A24	0.5	0.5	0	0.5	0.5	2
A25	1	1	1	1	1	5
A26	0.5	0.5	0.5	0.5	0.5	2.5
A27	1	1	1	1	1	5
A28	1	0.5	0.5	1	1	4
A29	0.5	1	1	0.5	1	4
A30	1	1	1	1	1	5
A31	1	1	1	1	1	5
A32	0.5	1	1	0.5	1	4
A33	0.5	1	1	0.5	0.5	3.5
A34	1	1	0.5	0.5	0.5	3.5

distribution of the primary studies. Another observation is that Evaluation is the most conducted with 9 (26.47%) studies conducting it. This result is not surprising because the research domain is very young. Thus, having more evaluation studies is expected. This situation will also further help researchers in the domain to understand the existing phenomenon in the domain better.

- Proportionality of the network forensic methods utilised Network forensic methods are vital in this domain. In this study, the categorisation is made based on an existing study [8]. From the primary studies, two forensic methods, namely, network flow analysis and honeypot systems, are identified. These methods were used to analysed IoT botnet attack detection or avoidance in a given network. We find that network flow analysis is the most used with 91.18% of the primary studies utilising it. On the contrary, only 8.82% of the studies utilised honeypot.
- IoT botnet attack detection or avoidance From our analysis, 22 (65%) studies focused on IoT botnet attack detection, whilst 12(35%) studies focused on avoidance. In normal circumstances, we believe that researchers should focus more on attack avoidance to save financial waste for organisations.
- Vastness and adequacy of the datasets utilised From the analysis, seven datasets are identified, and they were used by 30 studies. Four studies were unclear of the dataset they used (Table 6). The results demonstrate that 13 (38.24%) of the primary studies used Network traffic as their form of the dataset, which is the most utilised. By contrast, 9 (26.47%) of the primary studies utilised DNS traffic for their experiment. The two datasets were utilised by 64.71% of the primary studies.
- The evaluation metrics utilised Three major evaluation metrics are further identified, and they were utilised in this research domain for evaluating proposals. These metrics are Accuracy with 9 studies, followed by Precision (6) and Performance (5). These metrics were often used together with other sub-metrics to evaluate a given proposal. However, overall, these metrics were the most used by the primary studies.

TABLE 11. Top 15 most cited articles.

Identifier	Year of publication	Citation count
A30	2018	214
A8	2018	49
A24	2017	49
A19	2018	39
A32	2017	20
A16	2018	19
A2	2018	17
A20	2017	17
A22	2018	15
A11	2020	15
A34	2018	15
A29	2016	14
A18	2019	13
A15	2019	12
A7	2018	10

TABLE 12. Top 10 most active countries.

Countries	Studies	Number	Percentage
USA	A18, A20, A24, A6, A28, A25	6	17.65%
UK	A15, A32, A8, A13	4	11.76%
Greece	A1, A21	2	5.88%
India	A10, A3	2	5.88%
Pakistan	A7, A33	2	5.88%
Netherlands	A12, A23	2	5.88%
China	A31, A17	2	5.88%
Estonia	A34, A2	2	5.88%
Vietnam	A22, A9	2	5.88%
Singapore	A5	1	2.94%

A. CHALLENGES AND DIRECTION FOR FUTURE WORK

From our findings, few research challenges are identified. Therefore, in this sub-section, the recognised challenges are discussed and suggestions on ways to address the outlined challenges are given. We find that network flow analysis is the most utilised, with 91.18% of the primary studies utilising it. The high utilisation of this network forensic method is a concern. Even though its high utilisation is reasonable, a little diversity in network forensic methods utilisation is vital. Therefore, we recommend the research community to use more of honeypot systems and intrusion detection systems in their future research.

A total of 65% of the primary studies focused on IoT botnet attack detection, whilst 12(35%) focused on attack avoidance. This finding is not ideal for the organisation experiencing such attack. Researchers should focus more on IoT botnet attack avoidance because as the saying goes, 'prevention is better than cure'. We believe organisations will save much financial expenditure if they focus more on attack avoidance than detection. Therefore, the research community have to look into this matter and work more on IoT botnet attack avoidance.

B. LIMITATIONS

IoT-botnet attack is currently one of the most critical threat on the internet. Despite much research and law enforcement works and attempts to reduce the menance. Botnets are still in existence around the wolds. The existing limitations identified are discussed in this section.

- The unavailability of propose dataset and implementation description. makes IoT-based botnet attacks comparison challenging.
- C&C server detection and removal of blacklisted domains record limited success [11]. Hence, the existence of vulnerabilities in normal domains gives botmasters idea to utilize current domains instead of new domains. Therefore, detection and removal of domain is still an issue.
- Due to constant evolving of IoT-botnets with new capabilities, blacklisting is not enough to stop the communication of known bots. Hence, existing solutions are not built in a way to deal with such evolving bots. Therefore, new improve bots are always needed.

C. THREAT TO VALIDITY

This section outlines the observed threats that can hinder the validity of this study.

- The difficulty in identifying all articles that are related to this study: This problem is identified and was considered to be a key problem of SLR studies [45]. In this study, we adopt key data sources that were utilised by [46] in the search for relevant and important articles. Keywords are also utilised for the search of relevant articles on IoT-based botnet attacks. Thus, if we observe that a given study does not fall under the scope of this SLR, then we exclude it by utilising our formulated and well-defined inclusion and exclusion criteria for paper selection. This criteria further help in selecting the best articles for this study.
- The primary studies are classified into different facets on the basis of the analysis of the result obtained. Thus, the classification is conducted concerning the individual research question. This classification is challenging in some studies, such as the studies may unclearly state their contribution. However, the researchers look at the methodology of these kinds of studies thoroughly and make a consensus decision on which contribution a given study proposed.
- Data extraction is often tricky and challenging when no comprehensive search terminologies and data sources are utilised. In mitigating this challenge, this study uses five key data sources and comprehensive search terminology for the extraction of data.

VI. CONCLUSION

Security-related challenges in the IoT should be handled effectively, efficiently and thoughtfully to actualise the vision of IoT. Therefore, IoT devices and networks should have a degree of confidence with respect to features such as security, trust and privacy. Various potential attacks may occur on IoT devices; however, IoT-based botnet attack is the most popular. The reason is that IoT botnet spreads faster and create more impact than other attacks. In this study, we conducted an SLR on IoT-based botnet attacks. The existing literature was reviewed. With the guide of an evidence-based method utilised, 5465 studies were initially collected. Through the formulated inclusion and exclusion criteria, we finally selected 34 studies that are relevant to our defined research questions. The primary studies selected were thoroughly analysed, and the results based on the research questions were presented. Thus, the results were augmented with scientific findings and identified challenges from the primary studies. We identified nine contributions proposed by the primary studies in this domain. Evaluation, System, Model, Method and Approach are the mostly proposed with 26.47%, 17.65%, 17.65%, 14.71% and 11.76% of the primary studies, respectively. We further observed that network flow analysis is the most used with 91.18% of the primary studies utilising it. On the contrary, only 8.82% of the studies utilised honeypot. From our analysis, 22 (65%) of the primary studies focused on IoT botnet attack detection, whilst 12(35%) focused on avoidance. The identified research challenges were also highlighted with future research recommendations on ways to mitigate them (Section V-A)). This work presents an outline for many works to be conducted in this research domain. Thus, we expect key solutions in tackling IoT-based botnet attacks in future works. For future work, we will conduct a systematic mapping study that is focused on other aspect of IoT-botnet, such as IoT botnet detection. and avoidance which will aid in understanding the general trends and overall research productivity in the research domain.

REFERENCES

[1] D. Singh, G. Tripathi, and A. J. Jara, "A survey of Internet-of-Things: Future vision, architecture, challenges and services," in *Proc. IEEE world forum Internet Things (WF-IoT)*, Mar. 2014, pp. 287–292.

[2] S. Dange and M. Chatterjee, "Iot botnet: The largest threat to the iot network," in *Data Communication and Networks*. Cham, Switzerland: Springer, 2020, pp. 137–157.

[3] J. Ceron, K. Steding-Jessen, C. Hoepers, L. Granville, and C. Margi, "Improving IoT botnet investigation using an adaptive network layer," *Sensors*, vol. 19, no. 3, p. 727, Feb. 2019.

[4] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, "N-baiot-network-based detection of iot botnet attacks using deep autoencoders," *IEEE Pervas. Comput.*, vol. 17, no. 3, pp. 12–22, 2018.

[5] S. Keele, "Guidelines for performing systematic literature reviews in software engineering," EBSE, Goyang-si, South Korea, Tech. Rep. EBSE 2007-001, 2007.

[6] K. Petersen, S. Vakkalanka, and L. Kuzniarz, "Guidelines for conducting systematic mapping studies in software engineering: An update," *Inf. Softw. Technol.*, vol. 64, pp. 1–18, Aug. 2015.

[7] Y. Ji, L. Yao, S. Liu, H. Yao, Q. Ye, and R. Wang, "The study on the botnet and its prevention policies in the Internet of Things," in *Proc. IEEE 22nd Int. Conf. Comput. Supported Cooperat. Work Design (CSCWD)*, May 2018, pp. 837–842.

[8] N. Koroniotis, N. Moustafa, and E. Sitnikova, "Forensics and deep learning mechanisms for botnets in Internet of Things: A survey of challenges and solutions," *IEEE Access*, vol. 7, pp. 61764–61785, 2019.

[9] R. Alhajri, R. Zagrouba, and F. Al-Haidari, "Survey for anomaly detection of iot botnets using machine learning auto-encoders," *Int. J. Appl. Eng. Res.*, vol. 14, no. 10, pp. 2417–2421, 2019.

[10] M. M. Salim, S. Rathore, and J. H. Park, "Distributed denial of service attacks and its defenses in iot: A survey," *J. Supercomput.*, vol. 10, pp. 1–44, Jul. 2019.

[11] M. Singh, M. Singh, and S. Kaur, "Issues and challenges in DNS based botnet detection: A survey," *Comput. Secur.*, vol. 86, pp. 28–52, Sep. 2019.

[12] J. Sengupta, S. Ruj, and S. Das Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *J. Netw. Comput. Appl.*, vol. 149, Jan. 2020, Art. no. 102481.

[13] C. Tzagkarakis, N. Petroulakis, and S. Ioannidis, "Botnet attack detection at the IoT edge based on sparse representation," in *Proc. Global IoT Summit (GIoTS)*, Jun. 2019, pp. 1–6.

[14] S. Nomm and H. Bahsi, "Unsupervised anomaly based botnet detection in IoT networks," in *Proc. 17th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2018, pp. 1048–1053.

[15] K. Gurulakshmi and A. Nesarani, "Analysis of IoT bots against DDOS attack using machine learning algorithm," in *Proc. 2nd Int. Conf. Trends Electron. Informat. (ICOEI)*, May 2018, pp. 1052–1057.

[16] O. Hachinyan, A. Khorina, and S. Zapechnikov, "A game-theoretic technique for securing IoT devices against mirai botnet," in *Proc. IEEE Conf. Russian Young Researchers Electr. Electron. Eng. (EIConRus)*, Jan. 2018, pp. 1500–1503.

[17] A. Kumar and T. J. Lim, "A secure contained testbed for analyzing iot botnets," in *Proc. Int. Conf. Testbeds Res. Infrastruct.* New York, NY, USA: Springer, 2018, pp. 124–137.

[18] T. Shah and S. Venkatesan, "A method to secure iot devices against botnet attacks," in *Proc. Int. Conf. Internet Things*, 2019, pp. 28–42.

[19] T. S. Gopal, M. Meerolla, G. Jyostna, P. Reddy Lakshmi Eswari, and E. Magesh, "Mitigating mirai malware spreading in IoT environment," in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Sep. 2018, pp. 2226–2230.

[20] C. D. McDermott, F. Majdani, and A. V. Petrovski, "Botnet detection in the Internet of Things using deep learning approaches," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Jul. 2018, pp. 1–8.

[21] H.-T. Nguyen, Q.-D. Ngo, and V.-H. Le, "A novel graph-based approach for IoT botnet detection," *Int. J. Inf. Secur.*, vol. 19, no. 5, pp. 567–577, Oct. 2020.

[22] C. U. Om Kumar and P. R. K. Sathia Bhama, "Detecting and confronting flash attacks from IoT botnets," *J. Supercomput.*, vol. 75, no. 12, pp. 8312–8338, Dec. 2019.

[23] A. Al Shorman, H. Faris, and I. Aljarah, "Unsupervised intelligent system based on one class support vector machine and grey wolf optimization for IoT botnet detection," *J. Ambient Intell. Hum. Comput.*, vol. 11, no. 7, pp. 2809–2825, Jul. 2020.

[24] C. D. McDermott, J. P. Isaacs, and A. V. Petrovski, "Evaluating awareness and perception of botnet activity within consumer Internet-of-Things (iot) networks," in *Informatics*, vol. 6. Spain, China: Multidisciplinary Digital Publishing Institute, 2019, p. 8.

[25] Irfan, I. M. Wildani, and I. N. Yulita, "Classifying botnet attack on Internet of Things device using random forest," *IOP Conf. Ser., Earth Environ. Sci.*, vol. 248, Apr. 2019, Art. no. 012002.

[26] D. Acarali, M. Rajarajan, N. Komninos, and B. B. Zarpeláo, "Modelling the spread of botnet malware in IoT-based wireless sensor networks," *Secur. Commun. Netw.*, vol. 2019, pp. 1–13, Feb. 2019.

[27] G. Sagirlar, B. Carminati, and E. Ferrari, "Auto bot catcher: Blockchain-based P2P botnet detection for the Internet of Things," in *Proc. IEEE 4th Int. Conf. Collaboration Internet Comput. (CIC)*, Oct. 2018, pp. 1–8.

[28] L. Yin, X. Luo, C. Zhu, L. Wang, Z. Xu, and H. Lu, "ConnSpoiler: Disrupting C&C communication of IoT-based botnet through fast detection of anomalous domain queries," *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 1373–1384, Feb. 2020.

[29] M. J. Farooq and Q. Zhu, "Modeling, analysis, and mitigation of dynamic botnet formation in wireless IoT networks," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 9, pp. 2412–2426, Sep. 2019.

[30] A. Marzano, D. Alexander, O. Fonseca, E. Fazzion, C. Hoepers, K. Steding-Jessen, M. H. P. C. Chaves, I. Cunha, D. Guedes, and W. Meira, "The evolution of bashlite and mirai IoT botnets," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jun. 2018, p. 00.

[31] J. Margolis, T. T. Oh, S. Jadhav, Y. H. Kim, and J. N. Kim, "An in-depth analysis of the mirai botnet," in *Proc. Int. Conf. Softw. Secur. Assurance (ICSSA)*, Jul. 2017, pp. 6–12.

[32] N. Giachoudis, G.-P. Damiris, G. Theodoridis, and G. Spathoulas, "Collaborative agent-based detection of DDoS IoT botnets," in *Proc. 15th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, May 2019, pp. 205–211.

[33] H.-T. Nguyen, Q.-D. Ngo, and V.-H. Le, "IoT botnet detection approach based on PSI graph and DGCNN classifier," in *Proc. IEEE Int. Conf. Inf. Commun. Signal Process. (ICICSP)*, Sep. 2018, pp. 118–122.

[34] C. Dietz, R. L. Castro, J. Steinberger, C. Wilczak, M. Antzek, A. Sperotto, and A. Pras, "IoT-botnet detection and isolation by access routers," in *Proc. 9th Int. Conf. Netw. Future (NOF)*, Nov. 2018, pp. 88–95.

[35] R. Hallman, J. Bryan, G. Palavicini, J. Divita, and J. Romero-Mariona, "Ioddos-the Internet of distributed denial of sevice attacks," in *Proc. 2nd Int. Conf. Internet Things, Big Data Secur.*, 2017, pp. 47–58.

[36] J. Spaulding, J. Park, J. Kim, D. Nyang, and A. Mohaisen, "Thriving on chaos: Proactive detection of command and control domains in Internet of Things scale botnets using DRIFT," *Trans. Emerg. Telecommun. Technol.*, vol. 30, no. 4, Apr. 2019, Art. no. e3505.

[37] R. Tanabe, T. Tamai, A. Fujita, R. Isawa, K. Yoshioka, T. Matsumoto, C. Gañán, and M. van Eeten, "Disposable botnets: Examining the anatomy of IoT botnet infrastructure," in *Proc. 15th Int. Conf. Availability, Rel. Secur.*, Aug. 2020, pp. 1–10.

[38] A. Oliveri and F. Lauria, "Sagishi: An undercover software agent for infiltrating IoT botnets," *Netw. Secur.*, vol. 2019, no. 1, pp. 9–14, Jan. 2019.

[39] X. Zhang, O. Upton, N. L. Beebe, and K.-K.-R. Choo, "IoT botnet forensics: A comprehensive digital forensic case study on mirai botnet servers," *Forensic Sci. Int., Digit. Invest.*, vol. 32, Apr. 2020, Art. no. 300926.

[40] I. Indre and C. Lemnaru, "Detection and prevention system against cyber attacks and botnet malware for information systems and Internet of Things," in *Proc. IEEE 12th Int. Conf. Intell. Comput. Commun. Process.*, Dec. 2016, pp. 175–182.

[41] W. Li, J. Jin, and J.-H. Lee, "Analysis of botnet domain names for iot cybersecurity," *IEEE Access*, vol. 7, pp. 94658–94665, 2019.

[42] M. T. Gardner, C. Beard, and D. Medhi, "Using seirs epidemic models for iot botnets attacks," in *Proc. 13th Int. Conf. Des. Reliable Commun. Netw.*, 2017, pp. 1–8.

[43] S. M. Sajjad and M. Yousaf, "UCAM: Usage, communication and access monitoring based detection system for IoT botnets," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Aug. 2018, pp. 1547–1550.

[44] H. Bahsi, S. Nomm, and F. B. La Torre, "Dimensionality reduction for machine learning based IoT botnet detection," in *Proc. 15th Int. Conf. Control, Autom., Robot. Vis. (ICARCV)*, Nov. 2018, pp. 1857–1862.

[45] B. Kitchenham, "Systematic literature reviews in software engineering–a tertiary study," *Inf. Softw. Technol.*, vol. 52, no. 8, pp. 792–805, 2010.

[46] B. H. Mohammed, N. Safie, H. Sallehuddin, and A. H. B. Hussain, "Building information modelling (bim) and the Internet-of-Things (iot): A systematic mapping study," *IEEE Access*, vol. 8, pp. 155171–155183, 2020.