Journal of Information Systems Engineering and Management
2025, 10(15s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Security Issues in IoT Applications

Happy[1*], Dr. Neeti Kashyap[2], Dr. Rita Chhikara[3]
[1]*Research Scholar, Dept. of Computer Science & Engineering, The NorthCap University* Gurugram, Haryana, India
[2]*Assistant Professor, Dept. of Computer Science & Engineering, The NorthCap University* Gurugram, Haryana, India
[3]*Professor, Dept. of Computer Science & Engineering, The NorthCap University* Gurugram, Haryana, India
**Correspondence author E*-mail: happy22csd004@ncuindia.edu

ARTICLE INFO

Received : 18 Nov 2024
Revised : 01 Dec 2024
Revised : 26 Jan 2025
Accepted : 05 Feb 2025

ABSTRACT

The 21st century witnessed the appearance of the Internet of Things (IoT), which completely shifted the realm of innovations by enabling connectivity and communication between multiple devices. Constantly interdependent infrastructure that incorporates sensor equipment with information sharing and processing abilities has transformed everyone's lives, enabling seamless intercontinental interaction and information evaluation. The IoT remains vulnerable to security incidents regardless of its widespread utilization, partially due to risks ranging from obsolete firmware or software, inadequate authorization procedures, resources, and bandwidth restrictions. The expansion of IoT botnets, a trend that has appeared designed to attack the noted deficiencies, is particularly concerning, which renders them a significant threat to cybersecurity. Efficient surveillance tactics are mandatory due to the probable consequences of IoT malware attacks, which typically involve financial losses, service interruptions, and information breaches. The main objective of this research is to provide comprehensive evaluations of security deficiencies within IoT equipment, highlighting the disruptive consequences of botnets and investigating distinct prevention strategies, particularly those utilizing machine learning procedures. Furthermore, we endeavor to carry out a case investigation that employs a real-world IoT industry database (CICIOT2023) to identify botnet assaults on IoT applications, subsequently providing fruitful insights. Furthermore, the investigation intends to discuss forthcoming threats in the IoT prevention scenario as well as develop prevention methods, culminating in a philosophical stance on IoT protective paradigms.

Keywords: IoT/Internet of Things, Security, Botnet, CICIOT2023, Botnet Detection, Malware, IoT Security, DDoS, Cyber-attacks.

INTRODUCTION

Contemporary innovation breakthroughs, especially in affordable prices, low energy utilization, cloud computing, machine learning, and artificial intelligence, have drastically influenced many aspects of everyday life [1]. These advancements have made it possible for even smaller devices to connect to the internet, motivating manufacturers to build a wide range of low-cost IoT devices for direct customers, commercial, military, and industrial uses. IoT devices have transformed personal lives and mechanized countless sectors, playing a critical role in the industrial revolution [2]. The Internet of Things (IoT) ecosystem is expected to rapidly expand, with 41.6 billion linked devices forecast by 2025 [3]. According to a Statista analysis, the IoT segment is anticipated to achieve an astounding expansion of 1,387 billion US dollars by the end of 2024 in this automotive IoT-dominant market, totaling 494.20 billion US dollars. Looking ahead, the IoT market is projected to grow at a compound annual growth rate (CAGR) of 12.57% from 2024 to 2028. By the end of 2028, its market gross revenue is expected to exceed 2,227 billion US dollars [4].

Countless vital factors demonstrate the importance of IoT protections. First, the absence or variations of security upgrades for IoT appliances exposes them to vulnerabilities. Second, monetary elements usually highlight cost effectiveness instead of satisfactory security measures during development, causing them to be inadequately protected. Moreover, traditional strategies such as leaving ports open and accessible with standard authentication details and employing exposed authorization information further raise legitimacy hazards. Equipment obstacles create barriers to applying encryption, rendering systems accessible to information vulnerable. Additionally, exposed network interfaces and standards establish opportunities for illegal access.

Sooner or later, vulnerabilities during the data exchange phases expose the possibility of abuse by malicious users, which leads to comprehensive safety standards to prevent IoT applications [3] and [5]. These sorts of devices, which have constrained processing power and memory, cannot rely on conventional security procedures [5]. Unlicensed attackers use IoT security holes to get access to sensitive information, using hazards such as botnets, crypto-miners, and ransomware [6]. The IoT industry emphasizes extensive device manufacturing, constantly overlooking security precautions, leading to vulnerabilities such as session hijacking, XSS (cross-site scripting), DDoS assaults, SQL injection, and others [1]. Further, transmission channels, applications, and software are all attack vectors, with DoS/DDoS, password assaults, and malware injections being the most frequent [6].

The infamous Mirai attack in September 2016 unleashed a 620 Gbps denial-of-service onslaught against Brian Krebs' website [7], followed by a record-breaking 1.1 Tbps assault on OVH in France [14], and a 1.2 Tbps onslaught on Dyn Service providers' servers in October 2016 [8]. Plenty of popular internet sites encountered extended downtime, which included Netflix, Amazon, Twitter, Reddit, and GitHub [8] [9]. The consequences of Mirai's botnet attack and, afterwards, the release of its source code in 2017, caused a spike in IoT malware propagation [10]. Despite advances in machine learning and deep learning techniques for threat detection and mitigation [1], as well as research into intrusion detection methods and virus detection [5], there is still a lack of comprehensive understanding and technical depth regarding IoT botnet detection, prevention, and mitigation strategies. Recently released research demonstrate the necessity for deeper investigation and improvement of IoT security frameworks, especially in terms of tackling new risks and expanding detection effectiveness.

Referring to Kaspersky's 2023 security advisory, the primary attack methods are SSH and Telnet. Strong IoT security measures are critical, as illustrated by the fact that China and India were among the top two countries where these attacks were carried out [11]. Moreover, according to a poll performed by "Spamhaus" on the botnet threat report for Q4-2023, botnet C&C has grown to 8,147, up 16% from 7,052 the previous quarter. This highlights the significance of a comprehensive defensive approach for growing cyber threats in IoT security. It also shows that the pen testing framework, remote access Trojan (RAT), Android backdoor, loader/downloader, credential stealer, and ransomware were the most famous malware families associated with these malwares. It shows that India is the top country in which most domain registrars abuse [12]. These findings highlight the significance of a comprehensive defensive approach for growing cyber threats in IoT security.

Our investigation aims to significantly improve IoT integrity by addressing deficiencies in several important IoT application sectors. We carried out a meticulous evaluation of IoT safeguard barriers, analyzing penetration surfaces and equipment architectures. We simultaneously examined multiple techniques for tracking IoT botnets and recognized obstacles and irregularities. Subsequently, a case study was conducted on the CICIoT2023 dataset to explore the numerous characteristics of IoT botnet datasets and the consequences of machine learning (ML) techniques on detecting malware in real-world scenarios. Moreover, our assessment applies to emerging botnet hazards and tracking techniques within the changing IoT prospect. To achieve this, key publications were chosen and summarized to emphasize the study's contributions. The review presents an in-depth examination of current IoT botnet research, including the latest articles and sophisticated methodology, as well as rigorous study selection criteria. We critically evaluate each survey's merits and limitations, highlight research gaps, and offer future botnet detection and prevention tactics, which may shape future studies and help address IoT botnet security problems.

Further, this paper is structured as follows: Section II discusses the methodology utilized to conduct this investigation, followed by Section III, which deals with a literature analysis on various security issues in IoT applications and addresses security issues. Section III: Demonstrate case study to understand the various attributes and attack parameters on the real-world CICIoT2023 dataset, while Section IV: Discusses the findings, followed by Section V: Conclusion summarizes our findings, and the study is closed with Section VI by future research directions.

METHODOLOGY

This review follows Wohlin's et. al., and Petersen et al. three-stage methodology of planning, conducting, and reporting [13]. During the planning stage, research inquiries are identified, review processes are created, and the methodology is assessed [14]. Research identification, search strategy, primary research selection, inclusion and exclusion practices, study quality assessment, data synthesis, and extraction are all included in the conducting phase. The reporting process includes an evaluation phase, a dissemination strategy, and a report format. Figure 1 outlines various component of these steps thoroughly.

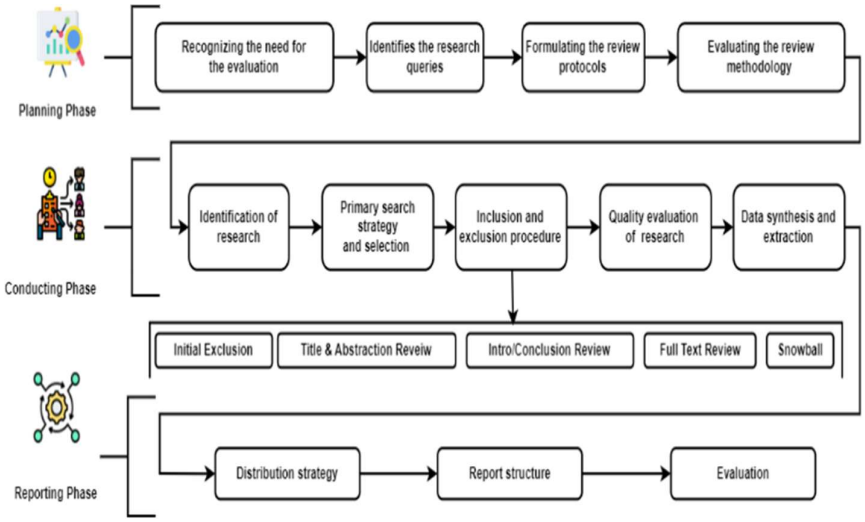

Fig. 1. Component of planning, conducting, and reporting phases

In this research, we adopted the PICO framework [13], which encompasses population (IoT device networks), intervention (IoT botnet detection techniques), comparison (with other methods or baseline metrics), and outcome (detection effectiveness). We also formulate tailored investigation queries to accomplish our aim. After gathering and screening research based on inclusion and exclusion criteria, we step into the planning stage. The planning stage begins the evaluation process, building a thorough framework for future phases. It includes recognizing possible investigation needs, integrating prior studies, and evaluating existing abilities and deficiencies to determine future study guidance. We apply rigorous full-text screening, which is conducted after the initial title and abstract screening, to ensure the papers fit the criteria for inclusion. We also extracted data on study design, sample size, interventions, and evaluated outcomes.

In the execution stage, we managed multiple stages to ensure the accuracy and reliability of the acquired data. This obtained data is essential for evaluating the effectiveness of the studies carried out. This assessment guarantees that relevant, excellent studies are studied. We achieved that by building a comprehensive searching approach that we used in a number of digital libraries, such as Wiley Online Library (WOL), IEEE Xplore (IEEE), Science Direct (SCI), Google Scholar (GS), ACM DL, and Google Scholar (GS), to get the desired high quality results. Further, we utilized Zotero to manage the extracted research and other tools to refine search queries and access research findings from various platforms like Springer, Hindawi, MDPI, and Taylor and Francis (T&F). We developed the search query utilizing multiple Boolean variables, (("Internet of Things" OR "IoT") AND ("Security" OR "IoT security" OR "security issues" OR "attack vectors" OR "architecture issues") AND ("Botnet" OR "Botnet architecture" OR "attack" OR "attack methods" OR "Detection" OR "Detection methods" OR "Detection techniques" OR "Emerging techniques" OR "Machine learning")), that could be incorporated as they are or as a portion of them in every selected online research database sites. After screening, 48 papers were chosen from 67,596 results, ensuring research integrity with exclusion criteria in which studies before 2017, unrelated work, and other language studies were removed and backward snowball sampling. Table 1 illustrates the initial output after search query (IOASQ), results after first level filtering (RAFLF), initial selected papers before final assessment (ISPBFA), and final selected paper after snowball process (FSPASP) corresponding to each database.

Table I. Database's Phase Wise Selected Studies

Database	IOASQ	RAFLF	ISPBFA	FSPASP
Springer	402	107	5	6
SCI	31633	3143	9	9
IEEE	10698	2079	25	25
ACMDL	6025	684	1	1
Hindawi	8412	3467	2	3
WOL	7865	4363	1	1
MDPI	308	230	4	5
T&F	2253	546	1	1
Total	**67596**	**14619**	**48**	**51**

Out of the total 67,596 cumulative results of the initial query on each dataset, only 14,619 were selected after first level filtering, which is 21.63% of the initial outcome, followed by only 48 selected after initial selection before final assessment, i.e., 0.071% of the initial and 0.33% of the first level filtering. After the snowball process, three new studies were incorporated into this review, resulting in a final total of 51, which is 0.075% of the initial and 0.35 of the first level filtered results. This rigorous selection process demonstrates our dedication to identifying high-quality studies for our research. Furthermore, Fig. 2 depicts a specific publisher's year wise contributions.

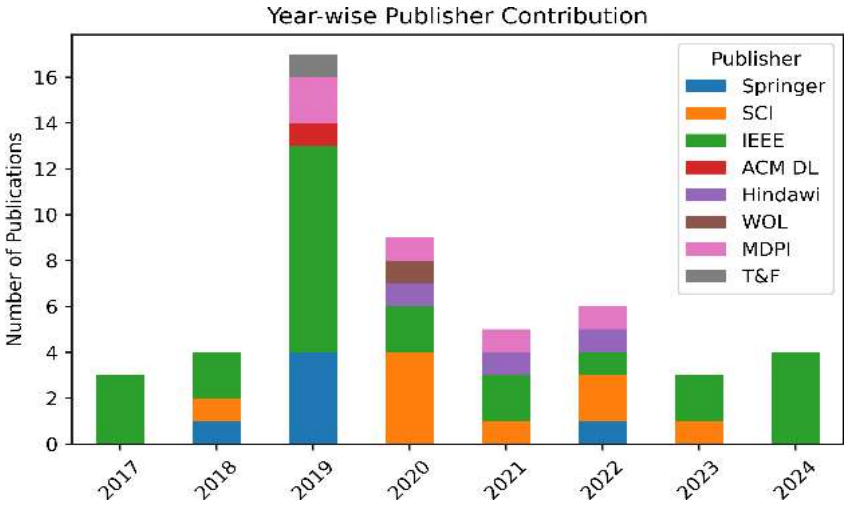

Fig. 2. Year-wise publisher contribution

To determine the validity and reliability of the initial chosen studies, we conduct a quality assessment of our methodology, meticulously evaluating variables including methods, data analysis, study design, sample size, and reporting. Utilizing high-quality studies for the final analysis, we improve the overall validity and reliability of our findings, assisting in identifying knowledge gaps and guiding future research. To achieve this, each research study received a rating between 1 and 12, with 1 representing the lowest score and 12 the highest. The score for each rule can be either '0' (not implying EC), '0.5' (partially implying EC), or '1' (fully implying EC). In this analysis, only papers with a quality value of at least 50% were considered. Study participants who did not meet this criteria were not used further in this research. The chosen research paper's quality was ensured using the evaluation criteria (EC) listed below.

EC 1: Will the research investigate IoT application design or related integrity threats throughout different layers?

EC 2: Did the research thoroughly address illicit behavior and incidents that occurred in IoT botnets?

EC 3: Should the investigation involve multiple strategies and techniques for finding and classifying integrity deficiencies in IoT applications in order to identify IoT botnets?

EC 4: Does the study include the most recent research findings on machine learning-based botnet detection in IoT systems?

EC 5: Does the study discuss emerging botnet threats and detection strategies in the IoT ecosystem?

EC 6: Is the study's methodology appropriate for the research aim?

EC 7: Does the study provide relevant and clear research findings?

EC 8: Does the study provide recommendations for future research in IoT botnet security?

EC 9: Are the data sources and collection methods appropriate for the research aim?

EC 10: Are the data analysis techniques appropriate for the research aim?

EC 11: Are the results and findings presented clearly and concisely?

EC 12: Does the paper discuss the findings' implications and significance?

Choosing or refusing certain research is determined by the proposed research commutative score (PRCS), which determines the quality of individual papers, as shown in (i). If the SSCS is ≥ 0.5, the study is suitable for selection. Otherwise, it is refused. Where ECi is the score for evaluation criterion i (ranging from 0 to 1), NEC is the total number of evaluation criteria, i.e., 12 in our case.

$$\text{PRCS} = \frac{\sum_{i=1}^{12} EC_i}{N_{EC}} \quad (1)$$

Similarly, the impact score (IS) of this research using the following method, where N_{SP} is the number of selected papers, i.e., 47, and N_{EC} is the number of evaluation criteria, i.e., 12 in our case, EC_{ij} represents the score for evaluation criterion *i* for paper *j*.

$$\text{IS} = \frac{\sum_{j=1}^{N_{SP}} \left(\frac{\sum_{i=1}^{N_{EC}} EC_i j}{N_{EC}} \right)}{N_{SP}} \quad (2)$$

Table 2 illustrates a thorough evaluation criteria matrix for the chosen studies, showcasing comprehensive evaluations and impact scores. This enables us to determine the standard and relevance of the research studies used in this investigation, providing perspectives on their particular consequences. In our investigation, data extraction and synthesis serve crucial roles, including the organized collection and gathering of statistics from our chosen studies. Using this, we include the examination and evaluation of the acquired analysis to draw significant conclusions. The varied styles of data offered by the preferred studies allow us to tackle concerns identified during prior stages of the research. The several procedures employed in this assessment are portrayed in Figure 3.

Fig. 3. Various Techniques employed in this review

The first column of the table, "Ref/Pub/Year," indicates the reference number and publisher name, in which 'SPRI' indicates Springer, 'HIND' indicates Hindawi, and 'Year' indicates publication year, respectively. For the 51 identified studies, the respective impact scores (IS) of EC1 to EC12 are, in order, 0.73, 0.8, 0.79, 0.65, 0.89, 0.79, 0.71, 0.88, 0.83, 0.83, and 0.86. With 0.075% of selected studies, we achieved a comprehensive impact score close to 9.61, reflecting a considerable magnitude of significance within the domain. Considering the evaluation criteria (EC), our selected study assessment has achieved around 80.08% of its maximum potential impact. This accomplishment demonstrates our study's commendable contribution, reflecting its relevance, rigor, and significance, especially in light of our extensive comprehension and expertise.

LITERATURE REVIEW

In this section, our intent is to try to identify gaps, difficulties, and possibilities in existing research and provide a theoretical framework and research technique, focusing on organized literature on IoT application security challenges, botnets, and solutions. The primary emphasis of this review is to deliver the latest solutions to solve security challenges in IoT devices, ensuring the research findings and conclusions' authenticity, reliability, and importance.

Sarker et al. [1] highlight the importance of adequate data simulation for optimal IoT security. They additionally highlight potential exploration possibilities in IoT safety, notably in the formation of efficient ML and DL algorithms for security solutions. Nguyen et al. [2] offer a distributed ML framework procedure that extends beyond conventional full-time sequence data-based processes, attaining a superior performance score of 99.37% for the early recognition of IoT malware attacks. They additionally carried out a thorough study by employing ML methods such as SVM, KNN, DT, and RF to evaluate attributes associated with network data, system resources, and malware behavior. Employing ML procedures deployed for network-edge communication in home networks, Kumar et al. [3] present a distinctive methodology called EDIMA, which uses a two-stage ML-based detection technique for precise bot detection and bot-CnC communication identification. This is beneficial for the initial identification of IoT botnets. When deployed on resource-restrained devices like the Raspberry Pi, the methodology outperforms existing procedures in terms of performance and identification effectiveness, with low false-positive rates.

Table II. Evaluation Matrix for Selected Studies

Ref/Pub/Year	EC1	EC2	EC3	EC4	EC5	EC6	EC7	EC8	EC9	EC10	EC11	EC12	PRCS
[1]/SPRI/2022	1	1	1	0.5	1	1	1	0.5	1	0.5	1	1	**10.5**
[2]/SCI/2022	1	1	1	0.5	0.5	1	1	1	0.5	1	1	0.5	**10**
[3]/SCI/2022	1	1	0.5	1	1	0.5	1	0.5	1	1	1	1	**10.5**
[6]/IEEE/2020	1	1	1	1	1	1	1	0.5	0.5	0.5	0.5	0.5	**9.5**
[8]/IEEE/2021	0.5	0.5	1	1	1	1	0.5	1	1	0.5	1	0.5	**9.5**
[9]/IEEE/2017	1	1	1	1	1	1	0.5	0.5	1	0.5	0.5	0.5	**9.5**
[10]/IEEE/2019	1	1	1	1	0.5	1	0.5	0.5	1	1	0.5	1	**10**
[15]/IEEE/2024	0.5	1	1	1	1	1	1	0.5	1	0.5	1	1	**10.5**
[16]/IEEE/2024	0.5	1	1	0.5	1	1	0.5	0.5	1	0.5	0.5	1	**9**
[17]/IEEE/2024	0.5	1	1	1	1	1	0.5	1	1	1	0.5	0.5	**10**
[18]/IEEE/2024	1	0.5	1	0.5	1	1	1	0.5	1	1	1	1	**10.5**
[19]/IEEE/2019	1	1	1	0.5	1	0.5	1	0.5	0.5	0.5	1	1	**9.5**
[20]/IEEE/2022	1	1	1	0.5	1	0.5	0.5	0.5	1	0.5	0.5	1	**9**
[21]/IEEE/2023	0.5	0.5	1	0.5	0.5	1	0.5	1	1	1	0.5	1	**9**
[22]/IEEE/2023	0.5	1	1	0	0.5	1	1	0.5	1	1	1	1	**9.5**
[23]/IEEE/2018	0.5	1	0	0.5	1	1	0.5	0.5	1	1	1	1	**9**
[24]/IEEE/2019	1	1	1	0	1	1	0.5	0.5	1	1	1	1	**10**
[25]/IEEE/2019	0	1	0.5	1	0.5	1	1	0.5	1	1	1	1	**9.5**
[26]/IEEE/2019	1	0.5	0	0	1	1	0.5	0.5	1	1	1	1	**8.5**
[27]/IEEE/2018	0.5	0.5	1	0.5	1	1	1	1	1	1	1	1	**10.5**
[28]/IEEE/2020	0.5	0.5	1	0.5	1	0.5	1	0.5	1	0.5	1	0.5	**8.5**
[29]/IEEE/2019	0.5	1	1	1	1	1	1	0.5	1	1	1	1	**11**
[30]/IEEE/2017	0.5	1	1	0	1	1	1	0.5	1	0.5	1	1	**9.5**
[31]/IEEE/2017	0.5	1	0.5	1	1	0.5	1	1	0.5	1	0.5	1	**9.5**
[32]/IEEE/2019	0.5	1	1	1	1	1	0.5	0.5	1	1	1	0.5	**10**
[33]/IEEE/2019	0.5	0	0.5	0.5	1	1	1	1	1	1	1	1	**9.5**
[34]/IEEE/2019	0.5	1	1	0.5	1	1	0.5	1	0.5	1	1	1	**10**
[35]/IEEE/2021	1	1	0.5	1	0.5	1	0.5	1	1	0.5	0.5	1	**9.5**
[36]/SPRI/2019	0.5	1	0.5	0.5	0.5	1	0.5	0.5	1	1	1	1	**9**
[37]/SCI/2020	0.5	1	0.5	1	0.5	1	1	0.5	1	0.5	0.5	0.5	**8.5**
[38]/SCI/2020	1	1	1	0.5	0.5	1	0.5	1	1	0.5	1	1	**10**
[39]/SCI/2021	1	0.5	1	0.5	0.5	1	1	0.5	1	1	0.5	0.5	**9**
[40]/SPRI/2019	0.5	1	0.5	1	1	0.5	1	0.5	1	1	0.5	1	**9.5**
[41]/SPRI/2019	0.5	1	0.5	0	1	1	1	0.5	1	1	1	1	**9.5**
[42]/ACM/2019	0.5	0.5	1	0.5	0	1	1	0.5	1	1	1	1	**9**
[43]/T&F/2019	0.5	0.5	1	0.5	1	0.5	1	1	1	1	1	0.5	**9.5**
[44]/SCI/2018	0.5	1	1	1	0.5	1	0.5	1	0.5	0.5	0.5	0.5	**8.5**
[45]/MDPI/2022	1	1	1	0.5	0.5	1	0.5	0.5	0.5	1	0.5	1	**9**
[46]/SCI/2020	0.5	1	0.5	1	1	1	1	0.5	1	1	1	1	**10.5**
[47]/HIND/2022	1	1	0	1	0.5	1	1	1	0.5	1	0.5	1	**9.5**
[48]/SPRI/2018	0.5	1	0.5	1	1	1	1	0	1	1	1	1	**10**
[49]/MDPI/2020	1	1	0.5	1	0.5	1	0.5	1	0.5	1	0.5	0.5	**9**
[50]/SCI/2020	0.5	0.5	1	1	0.5	1	1	1	1	0.5	1	0.5	**9.5**
[51]/SCI/2023	0.5	0	0.5	1	1	1	1	1	1	1	1	1	**10**
[52]/MDPI/2019	1	0.5	1	0.5	0.5	0.5	1	1	0.5	1	1	1	**9.5**
[53]/MDPI/2019	1	1	1	0.5	1	0.5	1	1	0.5	0.5	1	1	**10**
[54]/HIND/2021	1	1	0.5	0.5	1	0.5	1	1	0.5	0.5	1	1	**9.5**
[55]/MDPI/2021	1	0.5	0.5	0.5	0.5	1	1	0.5	1	1	1	0.5	**9**
[56]/SPRI/2019	1	0.5	1	0	0.5	1	0.5	1	1	1	1	1	**9.5**
[57]/HIND/2020	1	1	1	0.5	1	0.5	0.5	1	1	1	0.5	1	**10**
[58]/WOL/2020	1	1	1	0.5	1	1	0.5	1	1	1	1	1	**11**
Impact Score	**0.73**	**0.8**	**0.79**	**0.65**	**0.8**	**0.89**	**0.79**	**0.71**	**0.88**	**0.83**	**0.83**	**0.86**	**9.61**

Here, score of '1' means that the paper meets the criteria of the assessment rule, '0.5' means that it partially meets the criteria, and '0' means that it does not meet the criteria.

Shafee [6] addresses a range of identification procedures for different types of botnets, especially mobile botnets, RAT bots, and botnets used for cryptocurrency mining. Since botnet vulnerabilities have a significant impact on cybersecurity, they highlight how essential it is to discover and eliminate them. They also propose a range of strategies, such as host-based identification, neural networks, clustering methods, and bitcoin malware detection frameworks, to effectively combat malware activities. Using a distinct Bot-IoT dataset, Chopra et al. [8] evaluate and select attributes for attack data through the PCA feature extraction method, and the result is confirmed using a 10-fold cross-validation approach. The proposed DDoS attack recognition system is accomplished by implementing Random Forest, J48, Naïve Bayes, and Bayes Net supervised classification algorithms. Kumar & Lim [10] describe EDIMA, a universal approach to classifying IoT malware into separate categories, the efficiency of employing ML methods for early identification of IoT malware network activity, and the necessity of examining communication behaviours for malware tracking. The investigation emphasizes the importance of identifying malware activity during the scanning/infection stage in order to avoid attacks and encourages a holistic approach involving IoT device fingerprinting, awareness of anomalies, and IoT infection inspection traffic identification.

Sutheekshan et al. [15] explore the complex development of IoT botnets and malware, and they offer perceptive approaches to both detection and mitigation. Their research highlights the critical requirement for strong protection against the constantly changing threats found in IoT environments. The critical roles that network segmentation, cooperative defensive strategies, and low-weight security solutions play in bolstering IoT security are also highlighted. In contrast to ANN, CNN, LSTM, and RNN models, Ali et al. [16] recommended an ACLR framework that outscored existing research, obtaining the highest accuracy score of 96.98% and demonstrating superior outcomes in respect of precision, recall, and F1 scores. The study demonstrates the effectiveness of hybrid methods in detecting botnet attacks as well as how critical it is to utilize a comprehensive range of deep learning techniques to boost IoT defenses Research conducted by Rahim et al.'s [17] focuses on enhancing IoT protection by evaluating NIDS (network-based intrusion detection systems) targeted at the IoT infrastructure through ML approaches. Their findings illustrate how important it is to identify security vulnerabilities in IoT ecosystem before implementing proactive measures. The research by Goyal and Mittal [18] focuses on the necessity of applying effective recognition techniques leveraging cutting-edge technology, such as artificial neural networks (ANN) , LSTM, GRU, and anomaly-based recognition approaches, to combat botnet assaults that represent a vital risk to IoT and IIoT systems. Security techniques used in well-known IoT communication protocols, which consist of LoRaWAN, 6LoWPAN, Zigbee, and Bluetooth Low Energy, are examined by Meneghello et al. [19].

In addition to emphasizing the significance of safe authentication techniques in cloud-driven IoT ecosystems and the importance of distributed intelligence and machine learning in strengthening IoT security, Deshmukh et al. [20] provide exhaustive insight on the security problems that IoT-based smart environments face. In order to ensure security and reliability, Sharma & Babbar [21] emphasize the need for detecting anomalies and vulnerabilities in IoT systems. The results illustrate how effectively ML techniques such as LR, DT, and RF recognize irregularities in IoT devices. Using ML models such as sequential, SVM, KNN, DT, RF, and GNB, Sharma et al. [22] achieve the best accuracy of 99% in multiclass classification on the N-BaIoT dataset. They also emphasized the risks that come with man-in-the-middle, botnet, physical manipulation, eavesdropping, and malicious code injection attacks, which are all types of IoT threats. "The Gunner System" is a revolutionary elimination methodology that Alieyan et al. [23] recommend to boost DNS-based botnet detection truthfulness. The research demonstrates the importance of establishing a technique that uses a distinct selection procedure to detect DNS-based botnets that match their attributes.

Aleksieva et al. [24] provide a host-based intrusion detection system (IDS) that uses a genetic algorithm to identify botnet breaches. They talk about how important network safety techniques are to counter modern threats like botnets and emphasize how important it is to create a normal behavior profile so that anomalies may be identified early on. According to Sudhakar & Kumar [25], keeping careful monitoring of communication patterns, using multipurpose methodologies, and employing protocol-specific detection algorithms are crucial for accurately identifying botnets. Through a simulation-based Java platform for confirming IP origins and collecting network packets, Shurman et al. [26] designed a hybrid intrusion detection system (IDS) that incorporates signature-based and anomaly-based detection. This strategy minimizes false positives and improves the efficiency of detecting new attacks, with an emphasis on reducing denial-of-service (DoS) attacks. Establishing a permissioned Byzantine Fault Tolerant (BFT) blockchain for interconnected botnet detection, Sagirlar et al. [27] proposed a methodological strategy called

AutoBotCatcher that utilizes network traffic analysis, community recognition algorithms, and blockchain technology to track and reduce botnet activities in IoT environments.

Adopting a data-driven methodology, Sriram et al. [28] capture network communication packets in PCAP form and convert them into connection details for review. They build several DNNs and conventional ML procedures, then manually identify the linking data. To identify the optimal hyperparameters for the DNN model, which comprises various hidden layers, neurons, stimulating functions, and normalization strategies, grid exploration is used. To generate conflicting communication streams, Wu et al. [29] employed a deep reinforcement learning technique. In an effort to alter communication flows, this involves employing a reinforcement learning program that is fed sequences of behaviors and feedback from the intended model, regardless of whether it is benign or malicious. By replicating actual assault scenarios, the investigation uses the identification model as a black box, thereby improving the evasion technique's precision. Zhuang & Chang [30] used a data-driven methodology to assess PeerHunter's effectiveness by combining synthetic and actual network datasets. They used a Map-Reduce architecture to construct a P2P host recognition component, which allowed them to drastically lower the number of hosts that needed to be analyzed.

An exhaustive two-stage botnet recognition strategy is offered by Wang & Paschalidis [31]. For flow-level and packet-level data, they first employ the big variation theory to keep an eye out for unusual patterns in network activity. To further enhance bot identification, they use anomaly evaluation in conjunction with network surveillance in the second phase to recognize highly engaging nodes related to both victims and bot-masters. Zha et al. [32] introduce BotSifter, a novel system designed to accurately identify bot activity in data centers. In an SDN configuration, distributed edge-assisted detection is combined with centralized learning via software switches. This integration enables real-time detection of VM-based bots in cloud systems. A blockchain trust model (BTM) was developed by She et al. [33] to identify malicious nodes in wireless sensor networks (WSNs). They simulated and validated the BTM using Truffle, Ganache-cli, and OPNET, allowing sensor devices to cast votes for malevolent ones by applying trust criteria set by smart contracts. The aforementioned framework handles trust and accurately detects rogue nodes, leveraging blockchain technology to improve privacy in WSNs.

In an attempt to construct and evaluate a surveillance model, Khan et al. [34] employed a data-driven methodology that utilized network traffic details from numerous sources. In order to distinguish between P2P botnet activity and regular P2P communication, they adopted ML techniques for attribute mining and classification, emphasizing session attributes and traffic distribution. In attempts to investigate ML approaches for IoT botnet detection, Garg et al. [35] provide a substantial focus on quantitative research techniques. The UNSW-NB15 dataset, which contains marked network traffic data, is used to evaluate algorithm performance. Eustis [36] highlights the significance of IoT gadget protection while describing the Mirai Botnet. They propose the establishment of an Industry Security Association to formulate security guidelines and impose emphasis on manufacturers to prioritize security first. In an attempt to investigate attack vectors, integrity risks, and shortcomings at the equipment and network levels, Rizvi et al. [37] split the IoT framework into trust zones. To tackle security problems, they map threats to devices, link attacks with gaps, and recommend safety measures.

By exploring the crucial facets of safety, security, and confidence within the IoT framework, Tewari & Gupta [38] point out the necessity of addressing privacy issues to preserve user trust and compliance with legislation. Active and passive attacks in WSNs, such as node duplication, information gathering, fake nodes, replay attacks, rushing attacks, clock skewing, and vampire attacks, are examined by Keerthika & Shanmugapriya [39], along with related defenses. They list the essential security needs for WSNs, including confidentiality, integrity, availability, authorization, and authentication. With a concentration on HTTP and TCP-based models, Prasad & Rohokale [40] concentrate on botnets and their detection techniques. The work highlights the use of principal component analysis, multi-agent systems, and cooperative game theory models in the identification and comprehension of botnets. According to Beltrán-García et al. [41], IoT botnets are susceptible to individual points of failure because of their concentrated topologies caused by IoT device restrictions.

Wainwright and Kettani [42] examine current botnet models and their role in improving mitigation strategies. Their identification of several botnet types offers unique perspectives on botnet behavior and strategies for mitigating its impact. In an effort to increase precision and reduce false positives in the currently available detection techniques, Alieyan et al. [43] provide a DNS rule-based botnet detection strategy by looking for unusual queries and response behavior in DNS. In order to identify botnets, Mathur et al. [44] recommend employing the WEKA tool to analyze network traffic data. They highlight its wide range of ML algorithms, which can build models with low false-positive

rates and high accuracy. In order to enhance intrusion detection, Baz [45] utilized supervised and unsupervised learning to establish the SEHIDS model employing a constructive neural network technique. SEHIDS prioritizes decentralization and resource efficiency, which are crucial for IoT setups, by using AI models on IoT devices for intrusion detection.

BotMark is a novel method that Wang et al. [46] propose for locating bots in network data. To improve accuracy, they mix graph-based and flow-based functions, which helps them identify emerging threats like Black Energy, Athena, and Mirai. Detection models are built using ML techniques such as local outlier factor (LOF) and k-means clustering. In order to overcome the challenges posed by the intricate communication patterns of P2P botnets, Xing et al. [47] developed the Peertrap framework, which uses network traffic data and ML to detect unstructured P2P botnets using the SAW (Shared Neighbor Analysis) community discovery method over the CTU-13 dataset. For P2P botnet identification, Alauthaman et al. [48] integrate decision trees with neural networks, using a CART method for reducing feature sets to increase classification accuracy and efficiency. Their approach is resistant to encryption techniques because it addresses P2P bot connections without examining payload information. Aldhaheri et al. [49] developed the DeepDCA framework by combining artificial immune system (AIS) techniques with deep learning in a hybrid fashion. DeepDCA improves signal extraction, attribute identification, and comprehensive detection efficiency by fusing the Dendritic Cell Algorithm (DCA) with a self-normalizing neural network (SNN).

With an 8-layer CNN and a deep learning technique, Jung et al. [50] are able to classify data based on patterns of power usage with 96.5% accuracy. The model exhibits excellent accuracy rates when examined on voice assistant appliances, routers, and security cameras. The use of AI in botnet surveillance is explored by Moorthy and Nathiya [51]. They emphasize network-based passive tracking methods for exploring traffic data and bi-directional net streams. It uses a variety of AI models, such as NN, SVM, RF, and DT, to detect botnets using the CTU-13 dataset and achieves 92% accuracy in recognizing malware packets. A collaborative blockchain-based method for recognizing DDoS attempts in IoT applications is offered by Spathoulas et al. [52]. On IoT gateways, several sensors securely transmit communication data via blockchain, enabling integration with internally generated measures to identify potential DDoS events. A qualitative study using ML classifiers to examine network traffic data was conducted by Khan et al. [53]. For attribute filtering and categorization, they used a DT strategy with the goal of distinguishing P2P and non-P2P communication.

A thorough review given by Xing et al. [54] emphasizes standards and classifying systems. They propose a typical bot detection evaluation system (CBDES) that uses qualitative analysis to identify the best strategies, including PRCL, BotSifter, PeerHunter, and Bot Catcher. The Wazzan et al. [55] research seeks to draw conclusions about the stages of IoT botnets, types of attacks using IoT botnets, identification difficulties, and techniques to improve detection processes. Aswale et al. [56] point out the necessity of expandability, trustworthiness, economy, governance, interoperability, and mobility in IoT systems. They also highlight the importance of establishing new standards such as Co-AP, MQTT, mDNS, DNS-SD, IEEE, and more to meet the distinctive needs of IoT appliances with low memory, reduced battery capability, and prone radio conditions. Almutairi et al. [57] propose a hybrid detection method called HANABot, which seeks to identify P2P, IRC, HTTP, and IP fluxing events from bot behaviors in network monitoring. By leveraging ML methods and feature reduction from host processes, the suggested technique improves botnet screening capabilities. BotDetector is offered by Xudong et al. [58] as an efficient means to track botnet behavior on IoT devices. For botnet identification, the experts utilized the Extreme Learning Machine (ELM) technique in the BotDetector framework.

The literature review reveals several notable shortcomings in the current landscape of IoT botnet investigation research. Firstly, multiple research studies typically concentrate primarily on theoretical concepts rather than actual applications or case studies, restricting the validation of recommended remedies in real-world scenarios. Secondly, reliance on individual datasets and assessment techniques may limit the adaptability and expandability of identification models across a variety of IoT environments. Furthermore, there is a predominant focus on traditional techniques, possibly overlooking complementary recognition techniques and emerging threats. Additionally, the reliance on hypothetical or synthetic data may not fully reflect the enormity of real-world IoT grids, necessitating verification using empirical investigations. Tackling these shortcomings through interdisciplinary research, empirical validation, and a deeper study of classification strategies with machine learning is critical for improving the performance and practicality of IoT botnet detection remedies. Further, Table III displays a summary of the prior studies, and the presented study is mainly based on experimental (Expmt), comparative (Cmprt), observational (Obsrv) types of studies, and [TR] represent this review.

ANALYSIS

In the prior sections, we described our research methodology and reviewed associated literature. Here, we'll deliver our results in an organized manner, aiding comprehension and achieving research goals.

Primarily based on the prior study statistics presented in Table III, it is evident that experimental (Expmt) studies predominate in the landscape (average of 100%), indicating a substantial concentration on empirical research in the fields of IoT. But there seems to be a considerable difference between observational (Obsrv) studies, which average 47%, and comparative (Cmprt) studies, which average 49%. This indicates a potential gap in the kinds of research carried out, with comparative analysis and observational studies getting less attention than they should. In order to enhance the academic discourse and expand the discipline's expertise, subsequent research endeavors should aim to attain a more equal proportion across all study formats to acquire a more thorough understanding of IoT botnet dynamics.

Table III. Type of Study utilised in this study vs. this Review

	Study Type				Study Type				Study Type		
Ref	**Expmt**	**Cmprt**	**Obsrv**	**Ref**	**Expmt**	**Cmprt**	**Obsrv**	**Ref**	**Expmt**	**Cmprt**	**Obsrv**
[1]	✓			[25]	✓	✓	✓	[42]	✓	✓	✓
[2]	✓	✓	✓	[26]	✓			[43]	✓	✓	✓
[3]	✓	✓	✓	[27]	✓	✓	✓	[44]	✓		
[6]	✓	✓	✓	[28]	✓			[45]	✓		
[8]	✓	✓		[29]	✓			[46]	✓		
[9]	✓	✓	✓	[30]	✓			[47]	✓		
[10]	✓			[31]	✓			[48]	✓		
[15]	✓	✓	✓	[32]	✓	✓	✓	[49]	✓		
[16]	✓			[33]	✓	✓	✓	[50]	✓		✓
[17]	✓	✓	✓	[34]	✓			[51]	✓		
[18]	✓			[35]	✓			[52]	✓		
[19]	✓	✓	✓	[36]	✓	✓	✓	[53]	✓		
[20]	✓	✓	✓	[37]	✓	✓	✓	[54]	✓	✓	✓
[21]	✓	✓		[38]	✓	✓	✓	[55]	✓	✓	✓
[22]	✓			[39]	✓	✓	✓	[56]	✓	✓	✓
[23]	✓			[40]	✓	✓	✓	[57]	✓	✓	✓
[24]	✓			[41]	✓			[58]	✓		
								[TR]	✓	✓	✓

Table IV provides an insightful overview of the IoT threat landscape, focusing on targeted operating systems, attack types, and malicious activity categories. Targeted OS categories include IoT, Linux (Lin), and Windows (Win), while attack types encompass Denial of Service and Distributed Denial of Service Attacks (D(DoS)), Data-related Attacks (DRA), Unauthorized Access and Intrusion Attacks (UA&IA), Network Scanning and Reconnaissance Attacks (NS&R), Botnet-related Attacks (BRA), Evasion Attacks and Exploits (EA&E), and Other Attacks. Moreover, malicious activity types are further delineated into Denial of Service and Distributed Denial of Service Attacks (D(DoS)), Unauthorized Access and Intrusion Attacks (UA&IA), Data-related Attacks (DRA), Botnet-related Attacks (BRA), Malware-related Attacks (MRA), Network Disruption and Manipulation (ND&M), Spam and Deception (S&D), and Other Attacks. The discoveries unambiguously show that operation system deviations in vulnerability are demonstrated in the occurrence of specific attack categories, which differ significantly across them.

The attacks classified as Distributed Denial of Service (D/DoS) have the highest average presence (92%), indicating that they constitute a threat to all operating systems. With an average existence of 80%, it is noteworthy that IoT devices and applications are particularly targeted. On the other hand, breaches particular to Windows have a substantially lower average presence (14%), indicating that attackers are not as keen on them. This indicates that attackers would alternatively target other systems, such as Linux and IoT (61% and 80%), respectively. The functioning of IoT applications is extremely impacted by D/DoS attacks, which have the greatest impact and are followed in significance by data-related assaults (DRA) at 71%. Evasion attacks and exploits, on the other hand, have minimal impact (0.06%), indicating that vulnerabilities are exploited less frequently. The threat landscape emphasizes the vital significance of the malicious activity categories UA&IA and DRA, which exhibit substantial effects at 61% and 65%, respectively.

Table IV. IoT Threat Landscape: Targeted Operating Systems, Attack Types, And Malicious Activity Types.

	Targeted OS			Attack Type							Malicious Activity Type							
Ref	**IoT**	**Lin**	**Win**	**D(DoS)**	**DRA**	**UA&IA**	**NS&R**	**BRA**	**EA&E**	**Other**	**D(DoS)**	**UA&IA**	**DRA**	**BRA**	**MRA**	**ND&M**	**S&D**	**Other**
[1]	✓	✓		✓		✓					✓			✓				
[2]	✓			✓	✓						✓	✓				✓		
[3]	✓	✓	✓				✓	✓			✓	✓	✓	✓	✓			
[6]	✓	✓		✓	✓	✓					✓	✓	✓	✓				
[8]	✓			✓				✓			✓			✓				
[9]	✓	✓		✓							✓							
[10]	✓	✓					✓		✓			✓	✓					
[15]	✓			✓	✓	✓					✓	✓						✓
[16]	--	--	--			✓	✓		✓	✓	✓	✓	✓					
[17]		✓		✓	✓	✓					✓	✓	✓	✓				
[18]		✓		✓		✓	✓				✓	✓				✓		✓
[19]	✓	✓		✓	✓	✓		✓			✓	✓	✓		✓			
[20]	✓	✓		✓	✓	✓		✓			✓	✓	✓	✓				
[21]	✓			✓	✓	✓	✓				✓	✓	✓			✓		
[22]	✓				✓	✓		✓		✓	✓	✓	✓					
[23]	--	--	--	✓	✓						✓						✓	
[24]		✓	✓	✓							✓	✓				✓		
[25]	✓	✓		✓	✓	✓		✓			✓	✓	✓		✓			
[26]	✓	✓		✓		✓					✓	✓						
[27]	✓	✓	✓	✓	✓						✓		✓		✓			
[28]	✓			✓				✓			✓			✓				
[29]	✓			✓					✓		✓	✓	✓					
[30]		✓		✓	✓					✓	✓	✓	✓					✓
[31]	✓	✓	✓	✓	✓					✓	✓						✓	
[32]	✓	✓	✓	✓	✓			✓			✓		✓	✓	✓			
[33]	✓	✓	✓	✓	✓	✓		✓			✓	✓	✓		✓			
[34]	✓			✓						✓	✓						✓	
[35]	✓			✓	✓						✓		✓				✓	
[36]	✓	✓		✓	✓			✓			✓			✓	✓			
[37]	✓	✓		✓	✓	✓		✓		✓	✓	✓	✓	✓				✓
[38]	✓	✓		✓	✓			✓			✓	✓	✓	✓	✓			
[39]	✓	✓		✓	✓		✓	✓			✓	✓	✓	✓	✓	✓		
[40]	✓			✓	✓			✓			✓	✓	✓			✓		
[41]	✓	✓		✓		✓		✓			✓	✓						
[42]		✓		✓	✓			✓		✓	✓				✓		✓	
[43]	✓			✓			✓				✓		✓	✓				✓
[44]		✓		✓	✓	✓					✓		✓	✓				
[45]	✓	✓	✓	✓	✓		✓	✓			✓	✓	✓	✓		✓		
[46]	✓			✓	✓	✓					✓		✓					
[47]		✓		✓	✓						✓			✓				
[48]	✓			✓	✓			✓					✓	✓				
[49]	✓			✓	✓						✓		✓					
[50]	✓			✓	✓		✓					✓			✓			
[51]	--	--	--	✓	✓	✓	✓						✓		✓			
[52]	✓			✓							✓							
[53]	✓			✓	✓						✓	✓	✓					
[54]	✓	✓		✓	✓			✓			✓	✓	✓	✓	✓			
[55]	✓	✓		✓	✓	✓	✓	✓			✓	✓	✓	✓	✓			
[56]	✓	✓		✓	✓			✓			✓	✓	✓					
[57]	✓	✓		✓	✓			✓			✓	✓	✓	✓				
[58]	✓	✓		✓	✓	✓	✓	✓			✓	✓	✓					

Here, ✓ signifies applicability, while '--', denotes "not specified" in this table.

Table V provides the numerous malware overviews identified using the existing review, which include the types, architectures, impacts, and detection methods of these malicious activities. The malware type is further categorized into IoT-based malware (IOTBM), Linux-based malware (LBM), Windows-based malware (WBM), and network-based malware (NBM) sub-classes. Malware architecture is also further divided into centralized architecture (CENT), peer-to-peer architecture (P2P), and hierarchical architecture (HIER). Malware impacts are also classified as disruption and congestion (D&C), data compromise and leakage (DC&L), unauthorized access and control (UA&C), and security and malware-related (S&MR). Further, detection methods are also classified into BBD (behavior-based detection), DDD (data-driven detection), & IBD (infrastructure-based detection).

The facts presented in Table V indicate that malware targeting Linux-based systems and IoT platforms is comparatively more common, with rates of 0.76 and 0.67, respectively, while malware based on Windows is far less common, with an average of 0.12 and an average of 0.61. Peer-to-peer and centralized architecture (CENT) are the most widespread threat architectures, with hierarchical structures only averaging 0.39. The vital botnet impact is disruption and congestion (D&C), with an average of 0.86, 0.69, 0.51, and 0.47, respectively, subsequently followed by DC&L, U&AC, and S&MR. In contradistinction, infrastructure-based detection (IBD) techniques have the minimum apparent at 0.27, compared to the median of 0.61 and 0.57 for BBD and DDD, respectively. These findings highlight the importance of robust security defenses, particularly the ones intended for Linux and IoT systems, in trying to mitigate the rising risk of botnet attacks. It is further crucial to emphasize surveillance strategies that tackle disruption-related impacts and centralize malware networks in efforts to enhance global privacy stability in emerging IoT device surroundings.

Further, Table VI compares the different botnet strategies available in the IoT environment in different situations, such as known bot detection (KBD), unknown bot detection (UBD), encrypted traffic detection (ETD), structure and protocol independence detection (S&PID), and real-time detection (RTD). It demonstrates how machine learning-based approaches excel at covering all detection situations because of their adaptability. While promising, data mining and anomaly-based methods might not be able to detect encrypted communication. Heuristic and signature-based approaches have greater limitations, particularly when dealing with encrypted communications and unknown bots. The efficiency of DNS-based and honeypot-based techniques varies depending on the situation. In general, we find that a mix of methods, emphasizing machine learning, seems most promising for thorough botnet identification in Internet of Things settings.

For the use case analysis, we adopted the CICIoT2023 dataset [62] to apply experimental, observational, and comparative studies to understand the concepts much better. This real-time dataset, developed by the Canadian Institute for Cybersecurity, represents an extensive examination of large-scale assaults on the IoT ecosystem. The initiative encompassed the exploitation of 105 IoT devices to simulate 33 types of attacks, collect data on the activities of these devices during the attacks, and classify that in seven different categories, such as DDoS (ACK fragmentation, Slow Loris, RSTFIN flood, HTTP flood, TCP flood, UDP flood, ICMP flood, Synonymous IP flood, SYN flood, UDP fragmentation, and PSHACK flood), Spoofing (ARP spoofing and DNS spoofing), Brute force (dictionary brute force attack), DoS (TCP floods, HTTP floods, SYN floods, and UDP floods), recon (Ping, sweep, OS scan, vulnerability scan, port scan, host discovery), Mirai (GREIP flood, the Greeth flood, and the UDP Plain), web-based (SQL injection, command injection, backdoor malware, uploading attacks, XSS, and browser hijacking).

Various PCAP files were captured throughout the execution of these 33 types of attacks on 105 different devices. Using these files, various attributes were extracted, and a total of 169 comma-separated value (CSV) files were generated, which is a total of 12.8 GB. Each CSV file contains 47 attribute values. That contains a total of 4,66,86,579 entries, out of which only 2.35 percent, i.e., 10,98,195, are benign and 4,55,88,384 are malicious entries, which are subsequently broken down into the aforementioned subcategories. Due to the hardware limitations in this use case study, we were only able to select 3% of the total CSV files. To conduct the case study, we started reading the first 5 files and merged them into a combined data frame. In the merged data frame, we introduce a new attribute 'benign' using the exiting attribute 'label'. After that, we check if there is any kind of bias present in the data or not, and we find out that the data is highly imbalanced towards malicious traffic with 11,63,394 entries as compared to 27,870 benign entries. It shows that the dataset is not properly balanced, and malicious traffic entries are 97.66%, compared to 2.34% of benign traffic entries.

Table V. Malware Overview: Types, Architectures, Impact, Detection Methods

	Malware Type				Malware Architecture			Malware Impact				Detection Method		
Ref	**IOTBM**	**LBM**	**WBM**	**NBM**	**CENT**	**P2P**	**HIER**	**D&C**	**DC&L**	**UA&C**	**S&MR**	**BBD**	**DDD**	**IBD**
[1]	✓	✓			✓	✓	✓	✓	✓	✓		✓	✓	✓
[2]	✓	✓			✓	✓		✓		✓		✓		✓
[3]	✓	✓			✓			✓	✓		✓		✓	
[6]	✓	✓			✓	✓	✓	✓	✓	✓	✓		✓	
[8]	✓				✓			✓	✓				✓	
[9]	✓	✓			--	--	--	✓	✓			--	--	--
[10]	✓	✓			✓	✓		✓			✓		✓	
[15]	✓	✓			✓	✓	✓	✓		✓	✓	✓	✓	
[16]	--	--	--	--	--	--	--	--	--	--	--		✓	
[17]	✓	✓			✓	✓	✓	✓	✓	✓		✓	✓	✓
[18]	✓	✓			✓	✓		✓		✓		✓		
[19]	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓		
[20]	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	
[21]	--	--	--	--	--	--	--	✓	✓	✓	✓	✓	✓	
[22]	✓	✓			--	--	--	--	--	--	--		✓	
[23]			✓	✓	--	--	--	✓			✓			✓
[24]	--	--	--	--	--	--	--	--	--	--	--	✓		
[25]	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	
[26]	✓	✓			✓	✓		✓		✓			✓	
[27]	✓	✓			✓	✓	✓	✓	✓	✓		✓	✓	✓
[28]	✓	✓			--	--	--	✓					✓	
[29]		✓	✓	✓	--	--	--	--	--	--	--	--	--	--
[30]				✓		✓		✓			✓	✓		
[31]	✓	✓			✓	✓		✓	✓			✓		
[32]	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓		
[33]	✓	✓			✓	✓	✓	✓	✓	✓	✓	--	--	--
[34]				✓			✓	✓			✓		✓	
[35]	✓						✓	✓	✓			--	--	--
[36]	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	
[37]	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
[38]	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
[39]	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓		
[40]	✓	✓			✓	✓		✓	✓			✓		
[41]	✓	✓			✓			✓		✓		✓		
[42]	✓	✓			✓	✓		✓	✓		✓	✓	✓	
[43]	✓					✓	✓	✓	✓					✓
[44]	✓	✓			✓			✓	✓	✓			✓	✓
[45]	✓				✓				✓	✓		✓		
[46]	✓	✓	✓	✓	--	--	--	✓	✓			✓		
[47]			✓			✓		✓	✓			✓		
[48]			✓	✓		✓		--	--	--	--	✓		
[49]	✓				--	--	--	✓	✓			✓	✓	
[50]	✓				--	--	--		✓		✓	✓	✓	
[51]	--	--	--	--	--	--	--	✓	✓	✓				✓
[52]	--	--	--	--	--	--	--	✓			✓			✓
[53]				✓		✓		✓	✓				✓	
[54]	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
[55]	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
[56]	✓	✓			✓	✓	✓	✓	✓		✓	✓	✓	✓
[57]	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	
[58]	✓	✓			✓	✓		✓	✓	✓			✓	

Here, ✓ signifies applicability, while '--', denotes "not specified" in this table.

Table VI. Botnet Detection Strategies Comparison

Detection Technique	KBD	UBD	ETD	S&PID	RTD
Signature Based	Y	N	N	N	N
Data Mining	Y	N	N	Y	N
DNS Based	Y	Y	N	N	N
Honeypot Based	Y	Y	N	N	Y
Heuristic-based	N	Y	P	N	Y
Anomaly Based	Y	Y	P	Y	N
Machine Learning	Y	Y	Y	Y	Y

Here, Y, N, *and* P *Signifies 'Yes', 'No', & 'Partially', respectively.*

This tragic data imbalance may impact the reliability of the system. To handle this problem, we balance the dataset with the lower-class entries, i.e., the benign class. To achieve this, we first split the data frame into benign and malicious subsets, and then for each unique 'label' attribute value from the malicious data frame, we did a random sample of malicious traffic for each unique label and shuffled the rows to ensure randomness. After ensuring a balanced dataset with 27,870 and 27,852 for both benign and malicious traffic, respectively, we split the dataset into training and testing sets with a ratio of 80:20, respectively. Then we apply various machine learning algorithms, such as DT, SVM, KNN, RF, NB, LR, and ANN. Table VII illustrates the comparison metrics of different machine learning algorithms (ALGO) based on accuracy (ACC) in percentage, precision (PRE), recall (REC), F1 score (F1S), ROC-AUC (ROC), training time (TRTs), testing time (TETs), and execution time (EXTs) in seconds.

TABLE VII. CICIoT2023 Case Study Comparison Matrices

ALGO	ACC	PRE	REC	F1S	ROC	TRTs	TETs	EXTs
Random Forest (RF)	98.11	0.97	0.99	0.98	0.98	11.43	0.16	11.58
Decision Tree (DT)	97.02	0.97	0.97	0.97	0.97	0.8	0.02	0.82
k-nearest neighbors (KNN)	93.97	0.92	0.96	0.94	0.94	0.02	1.52	1.54
Artificial neural network (ANN)	83.74	0.87	0.79	0.83	0.84	9.4	0.02	9.41
Support Vector Machine (SVM)	79.54	0.71	1	0.83	0.8	548.84	22.4	571.24
Linear Regression (LR)	76.31	0.8	0.7	0.74	0.76	0.24	0	0.24
Naive Bayes (NB)	73.67	0.82	0.6	0.69	0.73	0.04	0	0.04

Based on several measures, especially outstanding accuracy (98.11%), precision (97.11%), recall (99.11%), and F1 score (98.10%), RF is the best-performing algorithm. Additionally, it demonstrates excellent abilities in distinguishing across both categories, with a ROC-AUC score of 98.12%. Considering an overall execution time of 11.58 seconds, RF is noteworthy for having a slightly greater training duration than DT, KNN, ANN, LR, and NV algorithms. With a success rate of 97.02%, comparable precision of 97.29%, recall of 96.65%, and F1 score of 96.77%, the DT performs well across the parameters. In contrast to the RF, it demonstrates much lesser testing (0.016 seconds) and training (0.80 seconds) time, which renders it a more effective choice in circumstances with limited computational resources. Even though KNN attains a respectable accuracy rate of 93.97%, it performs less effectively than RF and DT in regards to precision and recall. It furthermore exhibits a significantly longer period for testing (1.52 seconds), emphasizing scalability challenges in real-time applications using massive datasets.

With an accuracy of 83.74%, ANN performs significantly worse than ensemble approaches like RF and DT. SVM outperforms RF and DT in terms of recall, achieving a remarkable recall of 100%, proving its effectiveness in identifying positive occurrences, but at the expense of precision, yielding a lower F1 score. Additionally, SVM takes the longest for testing and training (548.84 seconds and 22.40 seconds, respectively). This raises concerns about scalability for large datasets. Among the measures, LR and NB fare the worst, with accuracy scores of 76.31% and 73.67%, respectively. Although LR outperforms NB in terms of precision, both algorithms have poorer recall rates, which lowers their total F1 scores. However, application-specific needs determine which ML algorithm is best. This involves striking a balance between performance measures and factors like computing power, the capacity to analyze data in real-time, and the model's interpretability. Due to their stable performance and relatively cheap execution rates, ensemble approaches such as Random Forest and Decision Tree appear as viable alternatives for IoT botnet detection tasks. Figure 4 further illustrates the ROC curve for this use case research.

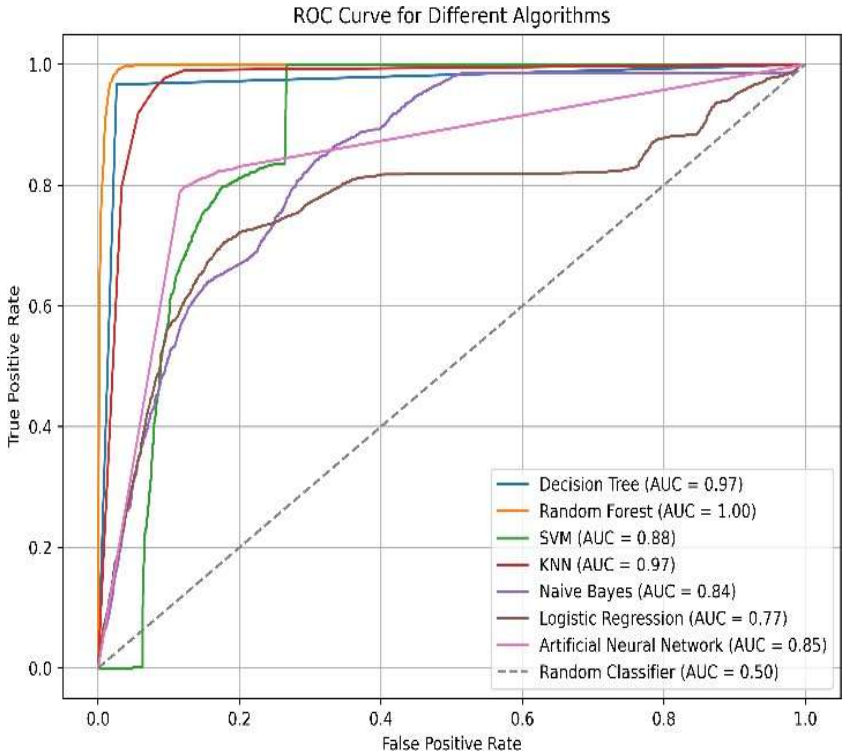

Fig. 4. CICIoT 2023 use Case study ROC curve

Emerging threats to IoT gadgets pose a diversified panorama of challenges, stretching from the flourishing of crypto-mining botnets to the insidious penetration of in-browser mining activities, both of which abuse IoT appliance computing bandwidth for illicit gains [59]. As IoT malware evolves in sophistication, perpetrators employ a plethora of methods involving sophisticated deception strategies, encrypted communications, and the deployment of unidentified botnets to conceal their activities from flagging mechanisms. Strategies, including fast-flux and P2P communications, further elevate the difficulties of recognizing and combating these vulnerabilities. Energy and resource-draining assaults attack the capabilities of IoT devices, hindering their intended activities and potentially throttling crucial services. The appearance of cross-device assaults within IoT networks raises further challenges, elevating the scope and consequences of illicit activities.

These vulnerabilities, coupled with intentions influenced by cyber-espionage and financial gain, demonstrate the critical need for robust security precautions to safeguard IoT grids. Additionally, the emergence of zero-day exploits, diverse integration issues, and the deception of botnets using encryption and obfuscation methods strengthen the imperative for perpetual surveillance and adaptive defences. Including the discussed new kind of self-issuing command attacks by IoT attacks on other IoT devices, for example, Alexa vs. Alexa (AvA) [60] and SMS-based cellular botnet attacks [61] may increase the worries for security researchers. It is imperative for security investigators to remain abreast of emerging concerns and regularly strengthen their safety mechanisms. As per our analysis throughout this research, we can conclude that the panorama of emerging hazards in IoT botnets poses a significant obstacle to the privacy and reliability of interrelated systems. The emergence of IoT appliances, together with the expertise of hackers, has culminated in an unprecedented rise in the magnitude and extent of malware activity. From DDoS attacks to information breaches, resource exploitation, and privacy infringement, the consequences of botnet-driven cyberattacks are extensive.

As emerging threats evolved very drastically, security researchers also offered emerging solutions to handle them, ranging from effective detection techniques utilizing collaborative machine learning to neural network methods designed for mobile botnet identification. Dynamic pattern modifications enable equipment to respond quickly to new malware variants, while auto encoders strengthen anomaly recognition capacities. Secure recognition strategies in cloud-driven IoT environments eliminate the risk of unauthenticated access, augmented by rule-based DNS attribute filtering engines like the Gunner System [23]. Blockchain-based recognition strategies offer flexible P2P botnet surveillance [27], while deep learning-based procedures evaluate network flow data for botnet screening with

unprecedented truthfulness. GPU hardware support increases computational efficiency [28], while multi-modal learning approaches improve detection systems.

The adversarial traffic flows generated by deep reinforcement learning frameworks facilitate robust testing, and mutual contact graph creation and community behavior analysis make P2P botnet detection more efficient. Destination diversity ratio adoption covers complex P2P activity trends, and two-stage detection techniques combine sophisticated frameworks such as BotSifter with the big deviations theory [32]. In order to defend against host-based infiltration, the SEHIDS system [45] dynamically changes, and hybrid analytic techniques provide thorough insights. Security protections are strengthened by real-time detection systems that use network traffic analysis and power consumption simulation, while interactive blockchain-based detection techniques improve efficiency and scalability. Defences against sophisticated botnet versions and hybrid detection approaches are strengthened by improved encryption techniques, robust authentication procedures, and secure communication protocols. Power consumption estimation system [50], like out-of-the-box techniques, is one example of an emerging solution to mitigate the emerging threats in the IoT ecosystem.

CONCLUSION

Based on this study, we emphasize the growing danger posed by distributed networks, resource-constrained hardware, and many attack vectors. The IoT brings substantial security challenges due to its confidentiality and verification limitations, as well as its exposure to denial-of-service attacks. These shortcomings typically result in the propagation of malware, which is exceptionally hazardous for both consumers and businesses. One of the significant features our investigation intends to demonstrate is the evolving nature of these threats. Botnets continually evolve, utilizing distributed P2P set-ups, fast-flux methods, and encrypted interaction methods to hinder identification and elimination endeavors. Additionally, the establishment of innovative malware variants with flexible C&C systems raises the threat of efficiently combating these threats. Traditional recognition methods are eventually inadequate to tackle emerging malware tactics, resulting in a conceptual transition regarding adaptable and innovative intrusion detection systems. Further, we notice that the rapid evolution of botnet behavior presents its own set of challenges, requiring continuous refinement and adaptation of detection algorithms to keep pace with emerging threats. IoT-specific botnets, AI-based attacks, and zero-day vulnerabilities are some of the most recent threats in the IoT botnet space.

Recognizing IoT malware is difficult due to diverse device characteristics, evolving methodologies, and data encryption issues. Host-based and network-based recognition techniques have restrictions, while behavioral-based approaches such as anomaly-based techniques and machine learning enhance accuracy but demand substantial resources. In our case study, we also employed machine learning techniques and achieved 98.11 percent accuracy by random forest for IoT botnet detection using the CICIoT2023 dataset. Static signature-based techniques are inefficient for discovering covert malware and encrypted traffic, forcing regular procedural advancements. To enhance identification performance, diverse knowledge resources, such as network communication, system logs, and consumer behavior, are being studied. By developing secure firmware, hardware-level privacy controls, user-centric design, and employing blockchain techniques for rapid surveillance and threat intelligence, we can also strengthen the security of the IoT ecosystem to the next extent. Future developments will involve the development of strong defence systems, real-time scanning, multi-modal data analysis, privacy-preserving detection approaches, flexible security systems, and cooperative defence strategies.

Furthermore, this investigation emphasizes the significant demand for hardware safety for IoT devices as a crucial component in minimizing malware risks. Secure authentication protocols, secure transmission methods, and firmware-legitimate authentication are indispensable in strengthening the durability of IoT frameworks against malicious encroachments. In order to combat these emerging threats, stakeholders from academia, industry, and government must work together to develop comprehensive tactics that include proactive threat intelligence, robust safeguarding methods, and legislative procedures that emphasize safeguarding and privacy. We can only hope to successfully safeguard the emerging IoT environment from the negative impacts of botnet-driven malware by putting integrated efforts and interdisciplinary collaboration into action. At the end, we can say that the aforementioned solutions may enhance IoT infrastructure security against emerging botnet assaults, highlighting the need for interdisciplinary approaches to protecting IoT ecosystems.

FUTURE WORK

In this review, we identify various issues present in IoT devices, including emerging threats and solutions. Furthermore, we recommend behavioral-based approaches, such as anomaly-based techniques and machine learning, to identify these attacks. In our case study, we also use various machine learning techniques and do a comparative analysis of those. In our future work, we will focus on developing a dataset, particularly for IoT applications, and identifying a set of attributes that can be used to detect these emerging threats in the IoT ecosystem. Using that database, we will also develop a hybrid system that uses multiple detection techniques to identify both existing and emerging botnet threats more efficiently.

Author Contributions: Conception and methodology, all authors participated mutually; investigation and writing—original draft formulation, Happy; writing—editing and review, all authors participated equally; supervision, R.C., and N.K.; project administration, R.C., N.K, and Happy.

Funding: Not applicable; the study has not received funding from any agency or organization.

Data Availability Statement: Not applicable; the research does not report any data.

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

REFERENCES

[1] Sarker, I.H., Khan, A.I., Abushark, Y.B. et al. Internet of Things (IoT) (2022). Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions. Mobile Netw Appl (2022). https://doi.org/10.1007/s11036-022-01937-3

[2] Nguyen, G. L., Dumba, B., Ngo, Q.-D., Le, H.-V., & Nguyen, T. N. (2022). A collaborative approach to early detection of IoT Botnet. Computers & Electrical Engineering, 97, 107525. https://doi.org/10.1016/j.compeleceng.2021.107525

[3] Kumar, A., Shridhar, M., Swaminathan, S., & Lim, T. J. (2022). Machine Learning-Based Early Detection of IoT Botnets Using Network-Edge Traffic, Computers & Security, Volume 117, 2022, 102693, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2022.102693.

[4] Statista "Internet of Things - Worldwide" acessed Feb 2024 [Online] Available: https://www.statista.com/outlook/tmo/internet-of-things/worldwide

[5] Mishra, N., & Pandya, S. (2021). Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review. IEEE Access, 9, 59353–59377. https://doi.org/10.1109/ACCESS.2021.3073408

[6] Shafee, A. (2020). Botnets and their detection techniques. 2020 International Symposium on Networks, Computers and Communications (ISNCC), 1–6. https://doi.org/10.1109/ISNCC49221.2020.9297307

[7] Zhao, H., Shu, H., & Xing, Y. (2021). A Review on IoT Botnet. The 2nd International Conference on Computing and Data Science, 1–7. https://doi.org/10.1145/3448734.3450911

[8] Chopra, A., Behal, S., & Sharma, V. (2021). Evaluating Machine Learning Algorithms to detect and classify DDoS attacks in IoT. IEEE Conference ID: 51348 2021 8th International Conference on "Computing for Sustainable Global Development", 17th - 19th March 2021

[9] Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and Other Botnets. Computer, 50(7), 80–84. https://doi.org/10.1109/MC.2017.201

[10] A. Kumar and T. J. Lim, "EDIMA: Early Detection of IoT Malware Network Activity Using Machine Learning Techniques," 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 2019, pp. 289-294, doi: 10.1109/WF-IoT.2019.8767194.

[11] Kaspersky "Kaspersky 2023 security bulletin" acessed Feb 2024 [Online] Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2023/11/28102415/KSB_statistics_2023_en.pdf

[12] spamhaus "Spamhaus Botnet Threat Update Q3 2023" acessed Feb 2024 [Online] Available: https://info.spamhaus.com/botnet-threat-updates

[13] Petersen, K., Vakkalanka, S., & Kuzniarz, L. (2015). Guidelines for conducting systematic mapping studies in software engineering: An update. Information and Software Technology, 64, 1–18. https://doi.org/10.1016/j.infsof.2015.03.007

[14] Wohlin, C. (2014). Guidelines for snowballing in systematic literature studies and a replication in software engineering. Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering, 1–10. https://doi.org/10.1145/2601248.2601268

[15] Sutheekshan, B., Basheer, S., Thangavel, G., & Sharma, O. P. (2024). Evolution of Malware Targeting IoT Devices and Botnet formation. In 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT). 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT). IEEE. https://doi.org/10.1109/ic2pct60090.2024.10486705

[16] Ali, M., Shahroz, M., Mushtaq, M. F., Alfarhood, S., Safran, M., & Ashraf, I. (2024). Hybrid Machine Learning Model for Efficient Botnet Attack Detection in IoT Environment. In IEEE Access (Vol. 12, pp. 40682–40699). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/access.2024.3376400

[17] R. Rahim, M. A. Chishti and M. M. Raheem, "Improving the security of Internet of Things (IoT) using Intrusion Detection System(IDS)," 2024 21st Learning and Technology Conference (L&T), Jeddah, Saudi Arabia, 2024, pp. 290-295, doi: 10.1109/LT60077.2024.10469668

[18] Goyal, M., & Mittal, S. (2024). Review for Prevention of Botnet Attack Using Various Detection Techniques in IoT and IIoT. In 2024 2nd International Conference on Disruptive Technologies (ICDT). 2024 2nd International Conference on Disruptive Technologies (ICDT). IEEE. https://doi.org/10.1109/icdt61202.2024.10489168

[19] Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019). IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices. IEEE Internet of Things Journal, 6(5), 8182–8201. https://doi.org/10.1109/JIOT.2019.2935189

[20] Deshmukh, A., Sreenath, N., Tyagi, A. K., & Jathar, S. (2022). Internet of Things Based Smart Environment: Threat Analysis, Open Issues, and a Way Forward to Future. 2022 International Conference on Computer Communication and Informatics (ICCCI), 1–6. https://doi.org/10.1109/ICCCI54379.2022.9740741

[21] Sharma, A., & Babbar, H. (2023). Machine Learning-Based Anomaly Detection in the Internet of Things. In 2023 3rd Asian Conference on Innovation in Technology (ASIANCON). 2023 3rd Asian Conference on Innovation in Technology (ASIANCON). IEEE. https://doi.org/10.1109/asiancon58793.2023.10270100

[22] Sharma, Y., Kumar, V., & Chaudhary, H. (2023). Attack Detection on Internet of Things Devices using Machine Learning Techniques. In 2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS). 2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS). IEEE. https://doi.org/10.1109/iciccs56967.2023.10142701.

[23] Alieyan, K., Anbar, M., Almomani, A., Abdullah, R., & Alauthman, M. (2018). Botnets Detecting Attack Based on DNS Features. 2018 International Arab Conference on Information Technology (ACIT), 1–4. https://doi.org/10.1109/ACIT.2018.8672582

[24] Aleksieva, Y., Valchanov, H., & Aleksieva, V. (2019). An approach for host based botnet detection system. 2019 16th Conference on Electrical Machines, Drives and Power Systems (ELMA), 1–4. https://doi.org/10.1109/ELMA.2019.8771644

[25] Sudhakar, & Kumar, S. (2019). Botnet Detection Techniques and Research Challenges. 2019 International Conference on Recent Advances in Energy-Efficient Computing and Communication (ICRAECC), 1–6. https://doi.org/10.1109/ICRAECC43874.2019.8995028

[26] Shurman, M. M., Khrais, R. M., & Yateem, A. A. (2019). IoT Denial-of-Service Attack Detection and Prevention Using Hybrid IDS. 2019 International Arab Conference on Information Technology (ACIT), 252–254. https://doi.org/10.1109/ACIT47987.2019.8991097

[27] Sagirlar, G., Carminati, B., & Ferrari, E. (2018). AutoBotCatcher: Blockchain-Based P2P Botnet Detection for the Internet of Things. 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC), 1–8. https://doi.org/10.1109/CIC.2018.00-46

[28] Sriram, S., Vinayakumar, R., Alazab, M., & Kp, S. (2020). Network Flow based IoT Botnet Attack Detection using Deep Learning. IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 189–194. https://doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162668

[29] Wu, D., Fang, B., Wang, J., Liu, Q., & Cui, X. (2019). Evading Machine Learning Botnet Detection Models via Deep Reinforcement Learning. ICC 2019 - 2019 IEEE International Conference on Communications (ICC), 1–6. https://doi.org/10.1109/ICC.2019.8761337

[30] Zhuang, D., & Chang, J. M. (2017). PeerHunter: Detecting peer-to-peer botnets through community behavior analysis. 2017 IEEE Conference on Dependable and Secure Computing, 493–500. https://doi.org/10.1109/DESEC.2017.8073832

[31] Wang, J., & Paschalidis, I. Ch. (2017). Botnet Detection Based on Anomaly and Community Detection. IEEE Transactions on Control of Network Systems, 4(2), 392–404. https://doi.org/10.1109/TCNS.2016.2532804

[32] Zha, Z., Wang, A., Guo, Y., Montgomery, D., & Chen, S. (2019). BotSifter: An SDN-based Online Bot Detection Framework in Data Centers. 2019 IEEE Conference on Communications and Network Security (CNS), 142–150. https://doi.org/10.1109/CNS.2019.8802854

[33] She, W., Liu, Q., Tian, Z., Chen, J.-S., Wang, B., & Liu, W. (2019). Blockchain Trust Model for Malicious Node Detection in Wireless Sensor Networks. IEEE Access, 7, 38947–38956. https://doi.org/10.1109/ACCESS.2019.2902811

[34] Khan, R. U., Kumar, R., Alazab, M., & Zhang, X. (2019). A Hybrid Technique To Detect Botnets, Based on P2P Traffic Similarity. 2019 Cybersecurity and Cyberforensics Conference (CCC), 136–142. https://doi.org/10.1109/CCC.2019.00008

[35] Garg, U., Kaushik, V., Panwar, A., & Gupta, N. (2021). Analysis of Machine Learning Algorithms for IoT Botnet. 2021 2nd International Conference for Emerging Technology (INCET), 1–5. https://doi.org/10.1109/INCET51464.2021.9456246

[36] Eustis, A.G. (2019). The Mirai Botnet and the Importance of IoT Device Security. In: Latifi, S. (eds) 16th International Conference on Information Technology-New Generations (ITNG 2019). (Vol. 800, pp. 85–89). Springer International Publishing. https://doi.org/10.1007/978-3-030-14070-0_13

[37] Rizvi, S., Orr, R., Cox, A., Ashokkumar, P., & Rizvi, M. R. (2020). Identifying the attack surface for IoT network. Internet of Things, 9, 100162. https://doi.org/10.1016/j.iot.2020.100162

[38] Tewari, A., & Gupta, B. B. (2020). Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. Future Generation Computer Systems, 108, 909–920. https://doi.org/10.1016/j.future.2018.04.027

[39] Keerthika, M., & Shanmugapriya, D. (2021). Wireless Sensor Networks: Active and Passive attacks - Vulnerabilities and Countermeasures. Global Transitions Proceedings, 2(2), 362–367. https://doi.org/10.1016/j.gltp.2021.08.045

[40] Prasad, R., & Rohokale, V. (2020). BOTNET. In R. Prasad & V. Rohokale, Cyber Security: The Lifeline of Information and Communication Technology (pp. 43–65). Springer International Publishing. https://doi.org/10.1007/978-3-030-31703-4_4

[41] Beltrán-García, P., Aguirre-Anaya, E., Escamilla-Ambrosio, P. J., & Acosta-Bermejo, R. (2019). IoT Botnets. In M. F. Mata-Rivera, R. Zagal-Flores, & C. Barría-Huidobro (Eds.), Telematics and Computing (Vol. 1053, pp. 247–257). Springer International Publishing. https://doi.org/10.1007/978-3-030-33229-7_21

[42] Wainwright, P., & Kettani, H. (2019). An Analysis of Botnet Models. Proceedings of the 2019 3rd International Conference on Compute and Data Analysis, 116–121. https://doi.org/10.1145/3314545.3314562

[43] Alieyan, K., Almomani, A., Anbar, M., Alauthman, M., Abdullah, R., & Gupta, B. B. (2021). DNS rule-based schema to botnet detection. Enterprise Information Systems, 15(4), 545–564. https://doi.org/10.1080/17517575.2019.1644673

[44] Mathur, L., Raheja, M., & Ahlawat, P. (2018). Botnet Detection via mining of network traffic flow. Procedia Computer Science, 132, 1668–1677. https://doi.org/10.1016/j.procs.2018.05.137

[45] Baz, M. (2022). SEHIDS: Self Evolving Host-Based Intrusion Detection System for IoT Networks. Sensors, 22(17), 6505. https://doi.org/10.3390/s22176505

[46] Wang, W., Shang, Y., He, Y., Li, Y., & Liu, J. (2020). BotMark: Automated botnet detection with hybrid analysis of flow-based and graph-based traffic behaviours. Information Sciences, 511, 284–296. https://doi.org/10.1016/j.ins.2019.09.024

[47] Xing, Y., Shu, H., Kang, F., & Zhao, H. (2022). Peertrap: An Unstructured P2P Botnet Detection Framework Based on SAW Community Discovery. Wireless Communications and Mobile Computing, 2022, 1–18. https://doi.org/10.1155/2022/9900396

[48] Alauthaman, M., Aslam, N., Zhang, L., Alasem, R., & Hossain, M. A. (2018). A P2P Botnet detection scheme based on decision tree and adaptive multilayer neural networks. Neural Computing and Applications, 29(11), 991–1004. https://doi.org/10.1007/s00521-016-2564-5

[49] Aldhaheri, S., Alghazzawi, D., Cheng, L., Alzahrani, B., & Al-Barakati, A. (2020). DeepDCA: Novel Network-Based Detection of IoT Attacks Using Artificial Immune System. Applied Sciences, 10(6), 1909. https://doi.org/10.3390/app10061909

[50] Jung, W., Zhao, H., Sun, M., & Zhou, G. (2020). IoT botnet detection via power consumption modeling. Smart Health, 15, 100103. https://doi.org/10.1016/j.smhl.2019.100103

[51] Moorthy, R. S. S., & Nathiya, N. (2023). Botnet Detection Using Artificial Intelligence. Procedia Computer Science, 218, 1405–1413. https://doi.org/10.1016/j.procs.2023.01.119

[52] Spathoulas, G., Giachoudis, N., Damiris, G.-P., & Theodoridis, G. (2019). Collaborative Blockchain-Based Detection of Distributed Denial of Service Attacks Based on Internet of Things Botnets. Future Internet, 11(11), 226. https://doi.org/10.3390/fi11110226

[53] Khan, R. U., Zhang, X., Kumar, R., Sharif, A., Golilarz, N. A., & Alazab, M. (2019). An Adaptive Multi-Layer Botnet Detection Technique Using Machine Learning Classifiers. Applied Sciences, 9(11), 2375. https://doi.org/10.3390/app9112375

[54] Xing, Y., Shu, H., Zhao, H., Li, D., & Guo, L. (2021). Survey on Botnet Detection Techniques: Classification, Methods, and Evaluation. Mathematical Problems in Engineering, 2021, 1–24. https://doi.org/10.1155/2021/6640499

[55] Wazzan, M., Algazzawi, D., Bamasaq, O., Albeshri, A., & Cheng, L. (2021). Internet of Things Botnet Detection Approaches: Analysis and Recommendations for Future Research. Applied Sciences, 11(12), 5713. https://doi.org/10.3390/app11125713

[56] Aswale, P., Shukla, A., Bharati, P., Bharambe, S., & Palve, S. (2019). An Overview of Internet of Things: Architecture, Protocols and Challenges. In S. C. Satapathy & A. Joshi (Eds.), Information and Communication Technology for Intelligent Systems (Vol. 106, pp. 299–308). Springer Singapore. https://doi.org/10.1007/978-981-13-1742-2_29

[57] Almutairi, S., Mahfoudh, S., Almutairi, S., & Alowibdi, J. S. (2020). Hybrid Botnet Detection Based on Host and Network Analysis. Journal of Computer Networks and Communications, 2020, 1–16. https://doi.org/10.1155/2020/9024726

[58] Dong, X., Dong, C., Chen, Z., Cheng, Y., & Chen, B. (2020). BotDetector: An extreme learning machine-based Internet of Things botnet detection model. In Transactions on Emerging Telecommunications Technologies (Vol. 32, Issue 5). Wiley. https://doi.org/10.1002/ett.3999

[59] Saad, M., & Mohaisen, D. (2024). Analyzing In-browser Cryptojacking. In IEEE Transactions on Dependable and Secure Computing (pp. 1–13). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/tdsc.2024.3377533

[60] Esposito, S., Sgandurra, D., & Bella, G. (2022, May 30). Alexa versus Alexa. Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security. Presented at the ASIA CCS '22: ACM Asia Conference on Computer and Communications Security, Nagasaki Japan. doi:10.1145/3488932.3497766

[61] Kitana, Traore, & Woungang. (2020). Towards an epidemic SMS-based cellular botnet. Journal of Internet Services and Information Security, 10(4), 38–58. doi:10.22667/JISIS.2020.11.30.038

[62] Neto, E. C. P., Dadkhah, S., Ferreira, R., Zohourian, A., Lu, R., & Ghorbani, A. A. (2023). CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment. Sensors (Basel, Switzerland), 23(13). doi:10.3390/s23135941