International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Tackling DDOS Attacks in IoT: Asynthesis of Literature 2018 to 2022

Syaifuddin[1], Sri Suning Kusumawardani*[2], Widyawan[3]

Submitted: 29/08/2023 **Revised**: 26/10/2023 **Accepted**: 02/11/2023

Abstract: Currently, the Internet of Things is expanding into all computing-reliant domains. Fog computing is a key ally of the Internet of Things. It brings cloud computing and services to the network's edge. IoT makes smart surroundings a reality and a possibility. However, they are not immune to security weaknesses and threats. Therefore, specialized security measures are necessary. Security is one of the greatest obstacles to achieving an ideal IoT and Fog environment. This reality, coupled with the enormous harm caused by application attacks, necessitates the concentration of efforts in this area. Existing studies of the state of the art have demonstrated this requirement by highlighting a number of unresolved issues requiring additional investigation. This article presents a Systematic Literature Review (SLR) that takes into account the context of intrusion detection and prevention in IoT-based environments. This review examines more than 73 papers that passed a rigorous inclusion/exclusion procedure with well stated criteria. Information was gathered from these studies to construct a picture of the present state of the art and answer the study's research goals. Thus, we identify the state of the art, outstanding questions, and future potential.

Keywords: *Detecting, Identifying, DDOS, IoT*

1. Introduction

IoT will influence various sectors like healthcare, energy management, manufacturing, surveillance, retail, urban development, and transportation. The Internet of Things (IoT) represents a step forward in networking technology, allowing simple devices to connect directly to the worldwide web. At its core, a unit, termed "things," can carry out specific tasks like collecting environmental data, taking actions based on certain conditions, or even forecasting results from the data it accumulates [1]. IoT's integration into our daily routines leads to a system that acts as a smart ecosystem, minimizing human physical interaction with the surroundings or the device itself, often referred to as Machine to Machine Communication [2]. IoT will influence various sectors like healthcare [3], energy management [4], manufacturing, surveillance [5], retail, smart city, and transportation [6].

The growth of the conventional network also influenced the IoT. But because IoT devices have limited resources, they're susceptible to attacks that aim to drain their resources. Attackers can send malicious packets to overwhelm the communication link. As a result, service disruptions, commonly known as Distributed Denial of Service Attacks (DDoS), are inevitable. Botnet IP packets were generated.

[1]*Department of Electrical and Information Technology, Jl. Grafika 2, Universitas Gadjah Mada, Yogyakarta 55281, Indonesia. Email: saifuddin@umm.ac.id*
[2]*Department of Information Technology, Jl. Raya Tlogomas 246, Universitas Muhammadiyah Malang, Malang 65144, Indonesia. Email: suning@ugm.ac.id*
[3]*Department of Electrical Engineering and Information Technology, Jl. Grafika No.2, Universitas Gadjah Mada, Daerah Istimewa Yogyakarta 55281, Indonesia*
** Corresponding Author Email: author@email.com*

Several studies have previously been conducted to study the feasibility of mitigating and resolving DDoS attacks in IoT utilizing the SD-IoT paradigm. Paper [7] presented a similar solution based on SD-IoT entropy. However, the value should be modified dynamically as system traffic grows.

Similarly, the authors in used entropy in [8] Although a threshold value was specified to categorize the traffic, the application was unable to pinpoint the exact location of each malicious IP address. The cosine similarity approach is also used by [9]. The authors used this strategy to distinguish between DDoS and normal flows by counting the Packet-IN messages that entered the controller. In [10], The authors created the ENeFS neuro-fuzzy algorithm, which differentiates DDoS using an inference rule. Researchers from [11] were using the counter-method. Based on flow counters, packet payload counters, node-based packet counters, node transmission/receiving power, and traffic load counters, this article offered various factors to detect DDoS attacks. The findings demonstrate the effectiveness of identifying a zero-day attack. Based on the results of the statistical method, it emerged that this strategy could detect DDoS attacks quickly. Nonetheless, it was unable to identify the static variables used to detect DDoS that varied significantly.

Some articles also discussed how to detect DDoS assaults in SD-IoT using Machine Learning (ML) and Deep Learning (DL). [12] Semi-supervised techniques were utilized to identify the DDoS attack known as LEDEM. The researchers designed a dataset based on the UDP flooding method and tested it on emulation and test-bed platforms, achieving a 96.28% accuracy rate. Additionally, they introduced the SD-IoT system, which leverages Logistic

Regression, Random Forest, and the XGB algorithm to spot and classify DDoS attacks. For this system, they adapted the ISCXIDS2012 dataset by tweaking some features and opted not to use the controller as the main detection point for the assault [13]. The authors used Support Vector Machine (SVM), RF, and Neural Network (NN) as key classification modules to construct DDoS assaults (ICMP and TCP SYN flood) over ordinary IoT traffic. [14] The DDoS attack was categorized using Stacked Auto Encoder (SAE) alongside Snort IDS. Features from the dataset were derived from the Snort rule for ICMP, TCP, and UDP traffic. The research showed a high accuracy of 95% for True Positive outcomes. Past studies using ML/DL for classification didn't specify a dataset focused on IoT scenarios. To better mimic real-world IoT scenarios, the researchers could consider expanding their dataset to include recognized application-layer protocols like MQTT, CoAP, and HTTP.

Several prior research attempted to combine the statistics and ML methods. [15] To detect and identify the DDoS assault and lower the False Positive Rate (FPR), we used information entropy and machine learning methods. Other than the similar research, the accuracy indicated in the outcomes was higher. The authors performed the categorization using UNB-ISCX, CTU-13, and ISOT datasets, which do not fully represent the IoT environment's actual data transit. Likewise, paper [16] To detect and classify the attack, a statistical and Multi-Layer Perceptron (MLP) combination was used. To generate UDP flood assaults, Trinoo DDoS tools were used. Flow statistics from the IoT gateway were used in the feature extraction procedure.

Preliminary questions

A systemized review method is designed and necessary to discover the fundamental insight behind the specific subject. We generated some review questions, which are included in Table 1, and planned the review work such that we will be able to answer the review questions before the end of the paper. The Review Questions (RQ) questionnaire was created to handle the review problem in the specific field of IoT, detection, and classification.

Table 1. Review Questions

RQ No	Review Question	Motivation
RQ1	What are the vulnerabilities and potential attack vectors in the Internet of Things?	To comprehend the threat to key cyber infrastructure posed by potentially vulnerable embedded devices, as well as the motivation for attacks.
RQ2	How is threat data gathered from diverse sources?	To investigate various threat data collection methodologies.
RQ3	What forms of data are analyzed and where are detection solutions deployed?	The location of IDS deployment is an important issue that must be taken into account when developing any IDS in the IoT-Fog-Cloud setting, whether it is an NIDS or a HIDS.
RQ4	What characteristics are included in attack data packets aimed at IoT networks?	Understanding what features can be converted into information for detection and mitigation.
RQ5	Which evaluation methods are utilized to validate detection methods?	The great majority of datasets used are old and based on different types of network traffic; finding an appropriate reference dataset to apply detections in IoT security is tough. In this approach, we hope to review the validation procedures employed in the state-of-the-art and present a newly updated list of current datasets that can serve as a foundation for future researchers, indicating which dataset is most appropriate for the context of their particular works.

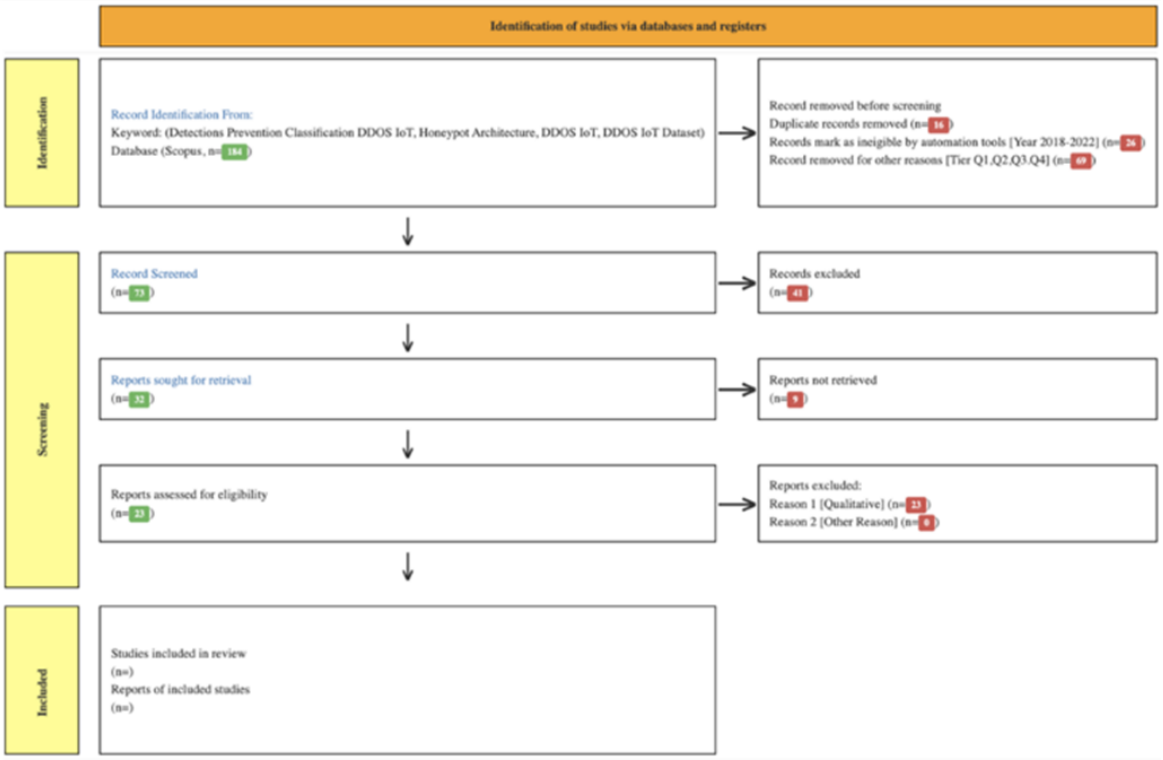
This study was divided into three sections: describing the publication selection process utilized as a reference, conducting literature investigations with supporting data, and presenting the findings.

2. Research Method

The following procedures were used: (1) creating research questions, (2) determining criteria, (3) developing searching techniques, (4) assessments, (5) data extraction, (6) data analysis, and (7) reporting the findings. Figure 2 depicts the flow of the literature review.

2.1. Search Strategy and Exclusion Criteria

The search and selection of studies is a critical phase in the systematic review. Your goal is to collect a collection of articles related to mapping.



The research was initially conducted in databases like ACM, IEEE, ScienceDirect, Springer, Wiley, and MDPI on September 15, 2022. These were selected due to their extensive collection of proceedings and journals relevant to the subject, their consistent updates, the precision of their search results, user-friendly interfaces, and the availability of full-text articles. To refine the search, certain criteria were set to exclude irrelevant papers. The keywords used during the search included terms related to IoT security like "Detections AND Prevention AND Classification", "DDOS-IoT", "Honeypot AND Architecture", and "Dataset". Using this methodology, 185 papers from publishers such as Elsevier, Springer, IEEE Journal, Wiley, and ScienceDirect were identified. However, certain articles were omitted based on criteria such as language (non-English), publication date (before 2018), unavailability of full text, format discrepancies, specific tier exclusions [Tier Q1, Q2, Q3, Q4], or absence from Scimago.

3. Data Analysis

To determine the eligibility of the paper, the title, abstract, and entire text are screened. If an article is irrelevant, it is not used. The NVivo 12 application was used to do the article analysis. The "Synthesis Without Meta-Analysis" manual is applicable. Meta-analysis is not required for synthesis [17] to use tables and graphs to summarize the findings.

4. Results

The following are study questions that were addressed in compliance with the research goals based on the findings of a literature review. RQ1, RQ2, RQ3, RQ4, and RQ5 were produced as research questions. RQ 1 delves into the vulnerabilities and possible attack avenues in IoT, RQ 2 focuses on gathering data about threats, RQ 3 identifies applied solutions and the nature of data analyzed, RQ 4 addresses attacks on IoT networks via packet data, and RQ 5 touches on the methods used to confirm the detection approach. Detailed answers for each research question follow below.

4.1. RQ1. What are the vulnerabilities and potential attack vectors in IoT?

This inquiry seeks to comprehend the threats to key cyber infrastructure posed by potentially vulnerable embedded devices and the motivations behind assaults. A literature search yielded 31 papers that fulfilled the requirements. Several articles highlight potential IoT vulnerabilities and attack routes. DDoS attacks pose a threat to every IoT segment, from smartphones and transport systems to smart homes, medical facilities, manufacturing units, educational infrastructures, and government entities. As IoT adoption accelerates, its security measures lag behind. Consequently, IoT is vulnerable to DDoS attacks, a situation further exacerbated by the expansion of 5G networks [18], [19], [28]-[31], [20]-[27]. IoT devices are susceptible to unauthorized access due to their ability to conduct widespread attacks unnoticed, leading to the creation of botnets [32]. By taking advantage of and dominating IoT, one can initiate DDoS attacks [33]. These attacks aim for

personal benefits, targeting military operations, influencing financial systems, damaging the economy's service sector, and advancing in areas like cyber espionage, warfare, and terrorism while enhancing security [34]-[41]. A major vulnerability of IoT to DDoS attacks stems from the limited capacities of most devices in terms of processing power, storage, and energy [42]. These restricted resources primarily serve to send data for processing and storage online. During this data management in IoT, significant amounts of data lead to congestion between the cloud and the devices [43].

4.2. RQ2. How threat data is collected from various sources?

Research gathers threat data from diverse sources to study various methods of data collection. There are several techniques to categorize this data. Notable tools and methods include J48, KNN, CNN, Naive Bayes, and more, like REP Tree, SVM, and LSTM. Additionally, techniques like IoTBoT-IDS, SIEM, and Stochastic Markov Chains help analyze this data [18], [21], [40], [41], [44]-[48], [22]-[24], [27]-[29], [32], [39], Other methods cited include R-IDPS, Snort, [42], Online Discrepancy Test [49], combined autoencoder (AE) and multi -layer perceptron (MLP) [50], a blend of autoencoder and multi-layer perceptron, and hybrid methods such as DNN-PCA and LSTM-CNN [51], NIDS-based PCCNN [43], self-exposing node (SEN) [52], Some tools, like the self-exposing node, add security features by blocking threats using the FLEAM method, enhancing the functionality of BBSC-SDN networks. Various optimizers like Adam, RMSProp, and SGD are also mentioned [25], [35], [36], [53].

4.3. RQ3. Where are detection solutions deployed and what types of data are analysed?

Detection tools were employed, and various data types were analyzed (RQ3). The systems were set up on IDS network areas, IoT emulation services, and feature extraction platforms [45], [19], [22], [23]. Both NIDS and HIDS determined the location for detection. NIDS incorporated network simulations into its detection mechanism [42], [43], [54]. monitoring all IoT network traffic and noting any anomalies. HIDS, on the other hand, focuses on detection within the host-managed network [32], [47], [50]–[52], [47]. Various data examples include port scanning, Ack flooding, and several other network attacks. Factors taken into account include download and upload delays, server response time, bandwidth consumption, and more. Several procedures like C&C, C&C-HeartBeat, and file downloads are also noted [22], [35], [36], [40], [41], [44].

4.4. RQ4. What features are present in attack data packets against IoT networks?

The properties of attacks on IoT networks via packet data are examined to identify which attributes can be used for spotting and counteracting these threats. These traits are typically categorized into different types. Commonly referenced categories encompass flow-based, content-based, time-based, essential, time-based, and active-flow attributes [19], [20], [42], [45], [43], [47], [48], [50], [54], [24]–[26], [28], [32], [36], [40], [41] The flow-based attack method is rapidly emerging as the standard technique used by attackers to overwhelm a service by sending massive traffic, leading to blockages and stopping legitimate data from reaching its destination. This involves flooding the system with unnecessary data to hamper or damage targets, and inundating devices with packets to exhaust their processing capacity, causing service denial to genuine traffic.

4.5. RQ5. Which evaluation strategies are used to validate detection approaches?

The evaluation process is utilized to validate the detection method. Various methodologies are adopted in assessing detection capabilities. Some commonly used metrics for this evaluation include Classification Accuracy (CA), F1-Score, Precision, Recall, Receiver Operating Characteristics (ROC), False Discovery Rate (FDR), False Omission Rate (FOR), False Positive Rate (FPR), and True Positive Rate (TPR). Additionally, assessments are based on Detection Time, Detection Accuracy, sensitivity, specificity, accuracy, F-measure, and the Matthew Correlation Coefficient. Each of these metrics offers a distinct perspective on the effectiveness of a given detection method [18], [20], [23], [26], [27], [32], [34], [35], [37], [41]–[43], [46], [49]–[52].

5. Discussion

The Internet of Things is one of today's most adaptable technologies. Because it has taken over our daily routines, it has a plethora of applications aimed to make life easier and simpler. Industry 4.0, as a paradigm implying the use of the Internet of Things idea to optimize business, manufacturing, and logistical processes, necessitates an upgrade in the employee work environment with the goal of improving employee comfort, safety, and productivity. IoT devices are easy targets for fraudsters and other aggressors due to a lack of fundamental security safeguards and the connection of real-world things with the Internet. These flaws allow hacking, improving Botnet networks, and ultimately launching DoS and DDoS attacks against companies. As a result, data leaks, phishing and spam campaigns, DDoS attacks, as well as security breaches can occur. Other motivations include cyber espionage, cyber warfare, and terrorism, as well as attempts to hack government and corporate systems to impede military capabilities, disrupt financial markets, and damage the economy's service sector. DDoS attacks can damage servers and devices on the internet, preventing legitimate system users from accessing resources or services. The existence of 5G services and IoT

devices with 5G capabilities further exacerbates this DDoS attack. IoT devices with 5G capabilities offer enhanced and interconnected connectivity scale, allowing them to be remotely controlled to form botnets and launch large-scale security attacks. Unfortunately, many IoT devices today are not designed with security in mind. With the number of exploitable IoT devices rapidly increasing, the attack surface for IoT systems is expanding. Another important factor is that the information passed on by these devices is often used in decision-making, so if fake data is sent quickly over 5G, this could seriously impact users. However, another reason behind DDoS attacks is to explore potential vulnerabilities to improve IoT security.

DDoS attacks can be detected through several methods like machine learning, deep learning, and federated learning. DNN, a popular machine learning tool, can perform intricate operations by integrating more layers and units in its network. It can identify normal and unusual traffic flows hidden in large structured datasets. Apart from DNN, there are other classifiers such as J48, KNN, CNN, Nave Bayes, REP Tree, Decision trees, Random Forest, SVM, LIBSVM, VAE, MLP, LSTM, etc. Additionally, studying DDoS attacks can help uncover weak points to enhance IoT security. According to Ashraf et al. (2021) the IoTBoT-IDS, integrated with BMM and Correntropy models, is believed to outperform other IDSs tailored for IoT networks like those in smart cities. The stochastic Markov serves as a predictor and detector in the fifth-generation network, showcasing impressive results with minimal errors, high detection, and a rapid decline in attacks [53], [27]. Various models and methods are blended in detection techniques. By pairing the DNN model with principal component analysis (PCA), security and efficiency are heightened [19]. A combined LSTM-CNN model excels in detecting attack categories, boasting a 99.92% accuracy, 99.85% precision, and an extremely low false positive rate for multiclass categorization. This hybrid approach outstrips the individual performances of both LSTM and CNN. Furthermore, SIEM-based detection can counteract DDoS attacks originating from compromised IoT gadgets [54], [34]. SIEM-based detection may also be used to stop DDoS attack traffic from hacked IoT devices [23].

FLEAM, short for A Federated Learning Empowered Architecture, not only serves to identify attacks but also becomes the main key to overcoming them. Another advantage of FLEAM is its ease of implementation. In addition, FLEAM has the ability to mitigate attacks directly from the source, thereby reducing delays in handling and increasing costs for attackers. In fact, FLEAM has the potential to eliminate zombie-type attacks before they can attack the second target of the alliance [43]. Increasing IoT network security by providing authentication access on the SDN network is thought to be capable of protecting data during transmission by broadcasting keys in parallel to the SDN switch [41]. In a study conducted by Alotaibi in 2020, network optimization was carried out using various types of optimizers. Among the optimizers examined such as Adam, RMSProp, SGD, and AdaGrad, it was found that Adam's optimizer performed best. Furthermore, Adam offers advantages over RMSProp and AdaGrad optimizers.

This location will implement IDS platforms, IoT service simulations, and feature extraction tools. IDS, which identifies abnormal network activities, comes in two main forms: NIDS and HIDS. NIDS oversees traffic for all network devices from a central point, while HIDS monitors both inbound and outbound traffic on individual devices, alerting administrators to unusual activities. HIDS looks at specifics like packet content, duration, and power efficiency. One attack tactic is the "network flooding attack", aiming to overwhelm a server by sending massive amounts of traffic, making genuine requests unprocessed or slowing server responses. Another tactic targets all open ports of a server, impacting its response to genuine traffic. Various evaluation metrics are employed to validate detection methods, including CA, F1-Score, Precision, Recall, ROC, FDR, and many more. Out of these, accuracy, F1-Score, precision, and recall are the most popular. A higher accuracy, calculated as the ratio of correctly identified records to total records, indicates a better machine-learning model. F1-Score, another name for F1-Measure, is the harmonic mean of precision and recall. A higher F1-Score suggests a superior model. Precision looks at the proportion of accurately identified attack records, while recall measures the rate of correct attack detection against the actual attacks.

6. Conclusion

Thanks to its adaptability, the Internet of Things (IoT) plays a pivotal role in refining various operations like commerce, manufacturing, and logistics. Designed to simplify and enhance everyday life, the benefits of IoT are undeniable. However, intertwined with these advantages are pressing security issues. Cyber attackers can exploit vulnerabilities in the system to compromise networks, amplify Botnets, and then launch DoS and DDoS attacks on businesses. These breaches can manifest in various forms, including data exposure, phishing campaigns, spamming, and direct DDoS attacks. Such malicious activities span a spectrum of motives, from mere spamming to graver intentions. Integrating 5G networks further amplifies the security challenges posed by DDoS threats. Fortunately, multiple strategies and techniques for DDoS attack detection are tailored based on network specifics, implementation site, and data variety. We can bolster IoT security and optimize overall network performance by identifying and countering these attacks.

Additionally, as technological advancements continue, it's imperative for businesses and individuals to remain vigilant

about their IoT devices. With the expansion of 5G and the ever-increasing number of connected devices, the potential attack surface grows larger. Proactive measures, such as consistent updates, encryption, and stringent authentication protocols, are necessary to safeguard data and maintain the integrity of operations. Collaborative efforts among tech firms, governments, and communities are crucial in developing robust and adaptable defense mechanisms against these threats. Furthermore, with the ongoing development of machine learning and AI technologies, there's potential for creating smarter, more adaptive security solutions. By harnessing these innovations' collective strength, we can confidently navigate the digital landscape, ensuring the promise of IoT is realized without compromising safety and security.

References

[1] O. Vermesan *et al.*, "Internet of robotic things-converging sensing/actuating, hyperconnectivity, artificial intelligence and IoT platforms," in *Cognitive hyperconnected digital transformation: Internet of things intelligence evolution*, 2017. doi: 10.1201/9781003337584-4.

[2] A. Nag, A. Kesharwani, B. Sharma, I. Gupta, A. Tiwari, and A. K. Singh, "Potential and Extention of Internet of Things," in *Lecture Notes on Data Engineering and Communications Technologies*, vol. 44, 2020. doi: 10.1007/978-3-030-37051-0_61.

[3] S. Selvaraj and S. Sundaravaradhan, "Challenges and opportunities in IoT healthcare systems: a systematic review," *SN Applied Sciences*, vol. 2, no. 1. 2020. doi: 10.1007/s42452-019-1925-y.

[4] Y. Liu, C. Yang, L. Jiang, S. Xie, and Y. Zhang, "Intelligent Edge Computing for IoT-Based Energy Management in Smart Cities," *IEEE Netw.*, vol. 33, no. 2, 2019, doi: 10.1109/MNET.2019.1800254.

[5] J. Arshad, M. A. Azad, M. M. Abdeltaif, and K. Salah, "An intrusion detection framework for energy constrained IoT devices," *Mech. Syst. Signal Process.*, vol. 136, 2020, doi: 10.1016/j.ymssp.2019.106436.

[6] M. D. Lytras, K. T. Chui, and A. Visvizi, "Data analytics in smart healthcare: The recent developments and beyond," *Applied Sciences (Switzerland)*, vol. 9, no. 14. 2019. doi: 10.3390/app9142812.

[7] D. Yin, L. Zhang, and K. Yang, "A DDoS Attack Detection and Mitigation with Software-Defined Internet of Things Framework," *IEEE Access*, vol. 6, 2018, doi: 10.1109/ACCESS.2018.2831284.

[8] M. Begović, S. Čaušević, B. Memić, and A. Hasković, "AI-aided traffic differentiated qos routing and dynamic offloading in distributed fragmentation optimized SDN-IoT," *Int. J. Eng. Res. Technol.*, vol. 13, no. 8, 2020, doi: 10.37624/ijert/13.8.2020.1880-1895.

[9] X. You, Y. Feng, and K. Sakurai, "Packet in Message Based DDoS Attack Detection in SDN Network Using OpenFlow," in *Proceedings - 2017 5th International Symposium on Computing and Networking, CANDAR 2017*, 2018, vol. 2018-January. doi: 10.1109/CANDAR.2017.93.

[10] P. J. B. Pajila, J. P, K. C, A. V. Sweet, and R. M. Lakshmi, "Software Defined Networking Based Protection against DDOS in IoT," *Int. J. Innov. Technol. Explor. Eng.*, vol. 9, no. 5, pp. 739–745, 2020, doi: 10.35940/ijitee.e2521.039520.

[11] J. David and C. Thomas, "DDoS attack detection using fast entropy approach on flow-based network traffic," in *Procedia Computer Science*, 2015, vol. 50. doi: 10.1016/j.procs.2015.04.007.

[12] N. Ravi and S. M. Shalinie, "Learning-Driven Detection and Mitigation of DDoS Attack in IoT via SDN-Cloud Architecture," *IEEE Internet of Things Journal*, vol. 7, no. 4. Institute of Electrical and Electronics Engineers (IEEE), pp. 3559–3570, 2020. doi: 10.1109/jiot.2020.2973176.

[13] G. C. Fernandez and S. Xu, "A Case Study on using Deep Learning for Network Intrusion Detection," in *Proceedings - IEEE Military Communications Conference MILCOM*, 2019, vol. 2019-November. doi: 10.1109/MILCOM47813.2019.9020824.

[14] R. M. A. Ujjan, Z. Pervez, K. Dahal, A. K. Bashir, R. Mumtaz, and J. González, "Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN," *Futur. Gener. Comput. Syst.*, vol. 111, 2020, doi: 10.1016/j.future.2019.10.015.

[15] J. A. Perez-Diaz, I. A. Valdovinos, K. K. R. Choo, and D. Zhu, "A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning," *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3019330.

[16] L. Van Efferen and A. M. T. Ali-Eldin, "A multi-layer perceptron approach for flow-based anomaly detection," in *2017 International Symposium on Networks, Computers and Communications, ISNCC 2017*, 2017. doi: 10.1109/ISNCC.2017.8072036.

[17] M. Campbell *et al.*, "Synthesis without meta-analysis (SWiM) in systematic reviews: Reporting guideline," *BMJ*, vol. 368, pp. 1–6, 2020, doi: 10.1136/bmj.l6890.

[18] A. Mihoub, O. Ben Fredj, O. Cheikhrouhou, A. Derhab, and M. Krichen, "Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques," *Comput. Electr. Eng.*, vol. 98, no. June 2021, p. 107716, 2022, doi: 10.1016/j.compeleceng.2022.107716.

[19] M. Al-Fawa'reh, M. Al-Fayoumi, S. Nashwan, and S. Fraihat, "Cyber threat intelligence using PCA-DNN model to detect abnormal network behavior," *Egypt.*

Informatics J., vol. 23, no. 2, pp. 173–185, 2022, doi: 10.1016/j.eij.2021.12.001.

[20] N. Mahajan, A. Chauhan, H. Kumar, S. Kaushal, and A. K. Sangaiah, "A Deep Learning Approach to Detection and Mitigation of Distributed Denial of Service Attacks in High Availability Intelligent Transport Systems," *Mob. Networks Appl.*, vol. 27, no. 4, pp. 1423–1443, 2022, doi: 10.1007/s11036-022-01973-z.

[21] I. Cvitić, D. Peraković, M. Periša, and M. Botica, "Novel approach for detection of IoT generated DDoS traffic," *Wirel. Networks*, vol. 27, no. 3, pp. 1573–1586, 2021, doi: 10.1007/s11276-019-02043-1.

[22] W. Li, Y. Wang, and J. Li, "Enhancing blockchain-based filtration mechanism via IPFS for collaborative intrusion detection in IoT networks," *J. Syst. Archit.*, vol. 127, no. April, p. 102510, 2022, doi: 10.1016/j.sysarc.2022.102510.

[23] H. Moudoud, L. Khoukhi, and S. Cherkaoui, "Prediction and Detection of FDIA and DDoS Attacks in 5G Enabled IoT," *IEEE Netw.*, vol. 35, no. 2, pp. 194–201, 2021, doi: 10.1109/MNET.011.2000449.

[24] J. G. Almaraz-Rivera, J. A. Perez-Diaz, and J. A. Cantoral-Ceballos, "Transport and Application Layer DDoS Attacks Detection to IoT Devices by Using Machine Learning and Deep Learning Models," *Sensors*, vol. 22, no. 9, 2022, doi: 10.3390/s22093367.

[25] Z. Shah, I. Ullah, H. Li, A. Levula, and K. Khurshid, "Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey," *Sensors*, vol. 22, no. 3, 2022, doi: 10.3390/s22031094.

[26] I. Ullah, B. Raza, S. Ali, I. A. Abbasi, S. Baseer, and A. Irshad, "Software Defined Network Enabled Fog-to-Things Hybrid Deep Learning Driven Cyber Threat Detection System," *Secur. Commun. Networks*, vol. 2021, 2021, doi: 10.1155/2021/6136670.

[27] Y. Labiod, A. Amara Korba, and N. Ghoualmi, "Fog Computing-Based Intrusion Detection Architecture to Protect IoT Networks," *Wirel. Pers. Commun.*, vol. 125, no. 1, pp. 231–259, 2022, doi: 10.1007/s11277-022-09548-7.

[28] N. Mazhar, R. Saleh, R. Zaba, M. Zeeshan, M. Muzaffar Hameed, and N. Khan, "R-IDPS: Real Time SDN-Based IDPS System for IoT Security," *Comput. Mater. Contin.*, vol. 73, no. 2, pp. 3099–3118, 2022, doi: 10.32604/cmc.2022.028285.

[29] M. A. Haq, M. A. R. Khan, and T. AL-Harbi, "Development of pccnn-based network intrusion detection system for edge computing," *Comput. Mater. Contin.*, vol. 71, no. 1, pp. 1769–1788, 2022, doi: 10.32604/cmc.2022.018708.

[30] T. Gaber, A. El-Ghamry, and A. E. Hassanien, "Injection attack detection using machine learning for smart IoT applications," *Physical Communication*, vol. 52. Elsevier BV, p. 101685, 2022. doi: 10.1016/j.phycom.2022.101685.

[31] P. Kumar, H. Bagga, B. S. Netam, and V. Uduthalapally, "SAD-IoT: Security Analysis of DDoS Attacks in IoT Networks," *Wirel. Pers. Commun.*, vol. 122, no. 1, pp. 87–108, 2022, doi: 10.1007/s11277-021-08890-6.

[32] S. P. K. Gudla, S. K. Bhoi, S. R. Nayak, and A. Verma, "DI-ADS: A Deep Intelligent Distributed Denial of Service Attack Detection Scheme for Fog-Based IoT Applications," *Mathematical Problems in Engineering*, vol. 2022. Hindawi Limited, pp. 1–17, 2022. doi: 10.1155/2022/3747302.

[33] M. Aslam *et al.*, "Adaptive Machine Learning Based Distributed Denial-of-Services Attacks Detection and Mitigation System for SDN-Enabled IoT†," *Sensors*, vol. 22, no. 7, 2022, doi: 10.3390/s22072697.

[34] J. Ashraf *et al.*, "IoTBoT-IDS: A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities," *Sustain. Cities Soc.*, vol. 72, no. April, p. 103041, 2021, doi: 10.1016/j.scs.2021.103041.

[35] M. Roopak, G. Y. Tian, and J. Chambers, "Multi-objective-based feature selection for DDoS attack detection in IoT networks," *IET Networks*, vol. 9, no. 3. Institution of Engineering and Technology (IET), pp. 120–127, 2020. doi: 10.1049/iet-net.2018.5206.

[36] A. Mehmood, M. Mukherjee, S. H. Ahmed, H. Song, and K. M. Malik, "NBC-MAIDS: Naïve Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks," *J. Supercomput.*, vol. 74, no. 10, pp. 5156–5170, 2018, doi: 10.1007/s11227-018-2413-7.

[37] R. Kalathiripi and N. Venkatram, "Regression coefficients of traffic flow metrics (RCTFM) for DDOS defense in IoT networks," *Int. J. Commun. Syst.*, vol. 34, no. 6, pp. 1–14, 2021, doi: 10.1002/dac.4330.

[38] K. Doshi, Y. Yilmaz, and S. Uludag, "Timely Detection and Mitigation of Stealthy DDoS Attacks via IoT Networks," *IEEE Trans. Dependable Secur. Comput.*, vol. 18, no. 5, pp. 2164–2176, 2021, doi: 10.1109/TDSC.2021.3049942.

[39] T. Liu, F. Sabrina, J. Jang-Jaccard, W. Xu, and Y. Wei, "Artificial intelligence-enabled ddos detection for blockchain-based smart transport systems," *Sensors*, vol. 22, no. 1, pp. 1–22, 2022, doi: 10.3390/s22010032.

[40] M. Ibrahim *et al.*, "SDN based DDos mitigating approach using traffic entropy for IoT network," *Comput. Mater. Contin.*, vol. 70, no. 3, pp. 5651–5665, 2022, doi: 10.32604/cmc.2022.017772.

[41] M. M. Cherian and S. L. Varma, "Mitigation of DDOS and MiTM Attacks using Belief Based Secure Correlation Approach in SDN-Based IoT Networks,"

Int. J. Comput. Netw. Inf. Secur., vol. 14, no. 1, pp. 52–68, 2022, doi: 10.5815/ijcnis.2022.01.05.

[42] E. Chovancová and N. Ádám, "A clustered hybrid honeypot architecture," *Acta Polytech. Hungarica*, vol. 16, no. 10, pp. 173–189, 2019, doi: 10.12700/APH.16.10.2019.10.11.

[43] J. Li, L. Lyu, X. Liu, X. Zhang, and X. Lyu, "FLEAM: A Federated Learning Empowered Architecture to Mitigate DDoS in Industrial IoT," *IEEE Trans. Ind. Informatics*, vol. 18, no. 6, pp. 4059–4068, 2022, doi: 10.1109/TII.2021.3088938.

[44] B. Alotaibi and M. Alotaibi, "A Stacked Deep Learning Approach for IoT Cyberattack Detection," *J. Sensors*, vol. 2020, 2020, doi: 10.1155/2020/8828591.

[45] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 3, pp. 2671–2701, 2019.

[46] B. Al-Duwairi, W. Al-Kahla, M. A. AlRefai, Y. Abdelqader, A. Rawash, and R. Fahmawi, "SIEM-based detection and mitigation of IoT-botnet DDoS attacks," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 2, pp. 2182–2191, 2020, doi: 10.11591/ijece.v10i2.pp2182-2191.

[47] Y. E. Kim, Y. S. Kim, and H. Kim, "Effective Feature Selection Methods to Detect IoT DDoS Attack in 5G Core Network," *Sensors*, vol. 22, no. 10, 2022, doi: 10.3390/s22103819.

[48] K. Malik, F. Rehman, T. Maqsood, S. Mustafa, O. Khalid, and A. Akhunzada, "Lightweight Internet of Things Botnet Detection Using One-Class Classification," *Sensors*, vol. 22, no. 10, pp. 1–17, 2022, doi: 10.3390/s22103646.

[49] P. Chaudhary, B. Gupta, and A. K. Singh, "Implementing attack detection system using filter-based feature selection methods for fog-enabled IoT networks," *Telecommunication Systems*, vol. 81, no. 1. Springer Science and Business Media LLC, pp. 23–39, 2022. doi: 10.1007/s11235-022-00927-w.

[50] R. F. Hayat, S. Aurangzeb, M. Aleem, G. Srivastava, and J. C. W. Lin, "ML-DDoS: A Blockchain-Based Multilevel DDoS Mitigation Mechanism for IoT Environments," *IEEE Trans. Eng. Manag.*, pp. 1–14, 2022, doi: 10.1109/TEM.2022.3170519.

[51] W. Fan, Z. Du, M. Smith-Creasey, and D. Fernandez, "HoneyDOC: An Efficient Honeypot Architecture Enabling All-Round Design," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 3, pp. 683–697, 2019, doi: 10.1109/JSAC.2019.2894307.

[52] Y. Sun, Z. Tian, M. Li, S. Su, X. Du, and M. Guizani, "Honeypot Identification in Softwarized Industrial Cyber-Physical Systems," *IEEE Trans. Ind. Informatics*, vol. 17, no. 8, pp. 5542–5551, 2021, doi: 10.1109/TII.2020.3044576.

[53] M. Usama *et al.*, "Unsupervised machine learning for networking: Techniques, applications and research challenges," *IEEE access*, vol. 7, pp. 65579–65615, 2019.

[54] B. Miller and X. Zhang, "A Multi-Layer Approach To Detecting And Preventing Iot-Based Botnet Attacks," *Issues Inf. Syst.*, vol. 21, no. 3, 2020.