Detection Systems for Distributed Denial-of-Service (DDoS) Attack Based on Time Series: A Review

1nd Ahmed Adil Nafea
dept. Artificail inteligence, College of Computer Science and Information Technology
University of Anbar
Ramadi, Iraq
ahmed.a.n@uoanbar.edu.iq

2nd Mustafa Maad Hamdi
dept. of Computer Science, College of Computer Science and IT
University of Anbar
Ramadi, Iraq
mustafa.maad.hamdi@uoanbar.edu.iq

3th , Baraa saad abdulhakeem
dept. of Information System,College of Computer Science and IT,
University of Anbar
Ramadi, Iraq
Baraasaad@uoanbar.edu.iq

4th , Ahmed Thair Shakir
dept. of Biophysics, College of Applied Sciences
University of Anbar
Ramadi, Iraq
ahmedth16@gmail.com

5th , Mustafa S. Ibrahim Alsumaidaie
dept. of Biophysics, College of Applied Sciences
University of Anbar
Ramadi, Iraq
mustafa.s.alsomadae@uoanbar.edu.iq

6th , Ali Muwafaq Shaban
dept. Information System,College of Computer Science and Information Technology
University of Anbar
Ramadi, Iraq
ali.m.shaban@uoanbar.edu.iq

2024 21st International Multi-Conference on Systems, Signals & Devices (SSD) | 979-8-3503-7413-1/24/$31.00 ©2024 IEEE | DOI: 10.1109/SSD61670.2024.10548796

***Abstract*— The Distributed Denial-of-Service (DDoS) attacks are one of the most critical threats to the stability and security of the Internet. With the increasing number of devices connected to the Internet, the frequency and severity of DDoS attacks are also increasing. To mitigate the impact of DDoS attacks, intelligent detection systems are becoming increasingly important. This paper reviews the recent literature on intelligent techniques, including machine learning (ML), Deep Learning (DL), and artificial intelligence (AI), for detecting DDoS attacks. We will provide an overview of the existing research in the field and analyse the trends in using time series data analysis for DDoS attack detection. A taxonomy and conceptual framework for DDoS mitigation are presented. This study highlights the use of several intelligent techniques for detecting DDoS attacks and evaluates the performance utilizing real datasets and also discusses future research directions in this field.**

Keywords—Distributed Denial-of-Service (DDoS) attack, detection system, time series analysis, machine learning, deep learning, fuzzy logic, extreme learning machines, clustering, deep reinforcement learning

I. INTRODUCTION

Cloud computing presents a large-scale Internet-based platform, which supports to lower infrastructure costs in order to provide computing services such as servers, databases, and networking to users and companies [1], [2]. The ability to deploy distributed denial-of-service (DDoS) attacks is one security risk that affects how the Internet and computer systems are used. The DDoS attack tries to overwhelm the target system with a high volume of traffic, making it impossible to authorised users [3] As a outcome, its position is a serious danger to the availability and stability of online services and networks. Time series analysis has developed as one of the most indicating methodologies for DDoS attack detection as a result of the frequency and power of DDoS attack growing over time. The DDoS attack could be detected using time series analysis, which can describe dynamic patterns and trends in network traffic [4]. Based on the aim and performance, the DDoS attack may be separated into three primary categories, such as bandwidth attacks, traffic attacks, and application attacks. In traffic-based attacks, the performance of the object server is decreased by the attackers' sending a lot of TCP or UDP packets to it. In bandwidth attacks, attackers send a lot of anonymous data to use up more bandwidth and cause congestion. Application attacks are difficult to prevent since they target a particular system [5]. Machine learning-based prediction models are used to identify DDoS attacks.

The Internet of Things is a developing network of physically linked and networked devices with Internet connectivity that enables the interchange of digital data from any location and at any time. This network is composed of several different device types, ranging in size from tiny to huge, and is fully autonomous. Cisco estimates that there are 50 billion connected devices worldwide [6], [7], [8]. IoT device examples are shown in "Fig 1". These devices are distinguished by their constrained memory, processing power, and computational capabilities. A variety of technologies, including wireless sensor networks, radio frequency identification, and cloud computing, assist the growth of the IoT paradigm [5].

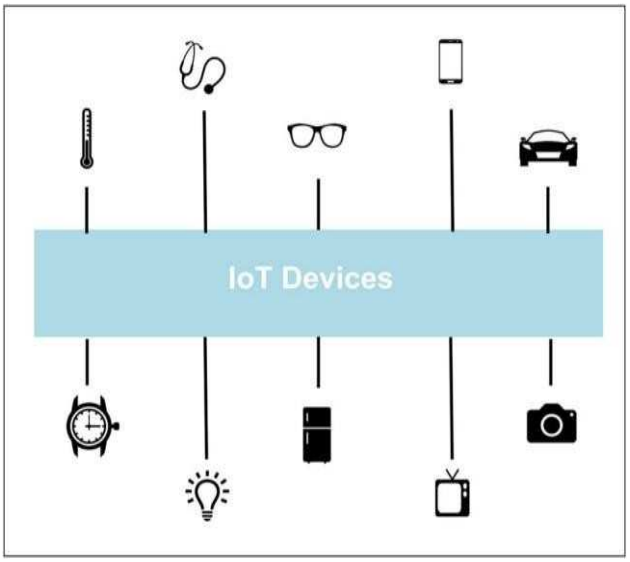

Fig. 1. IoT Devices Example.

DDoS attacks may take many different shapes and sizes, employing tactics similar to DoS attacks but on a larger scale and with a more sophisticated approach, making them challenging to defend against and seriously harming networks and information systems [9],[10]. It is possible to remotely control thousands of infected devices and use them to conduct attacks against the target that overload and paralyse it. The framework of a DDoS attack is shown in "Fig 2". The attacked IoT devices are made into slaves under the attacker's control, forming a network like an army that makes erroneous requests to the intended victim, leading to a complete shutdown. DDoS attacks may be executed in a variety of methods, as the graphic illustrates. Dos assaults find Internet-connected devices an appealing target, since they can be hacked and become zombie without the owner's knowledge. These zombies use Trojan horses, malware, and backdoors to aid DDoS attacks. They can be spread through emails, kept on unpatched websites, or displayed as adverts. Trojan software has even been known to be concealed in the pixel structure such that it opens as a regular image [11]. The programme, which is commonly built in JavaScript, downloads payloads to the unaware user's device when it is opened.

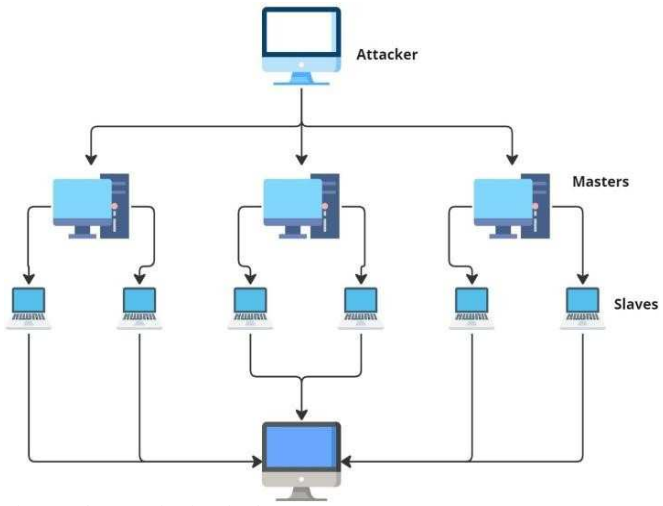

Fig. 2. The organizational scheme

Different DDoS attack detection techniques have been developed as a result of the increase in frequency and intensity of DDoS attacks rising [12] ,[13]. Time series analysis, which can identify dynamic patterns and trends in network traffic, is one of the most promising methods for detecting DDoS attacks[14]. Several research has suggested DDoS attack detection systems based on time series analysis and other machine learning methods in this area. These methods include clustering, deep reinforcement learning, graph neural networks, support vector machines (SVM), deep neural networks (DNNs), fuzzy logic, extreme learning machines (ELM), and transfer learning. The purpose of these investigations is to create methods to quickly and correctly detecting DDoS assaults with the least possible impact on the stability and availability of online services and networks.

This paper aims to review the latest advances in DDoS attack detection systems that use time series analysis as the basis. The purpose of this review is to give a complete understanding of the current state of the art in this field and to highlight the important issues and potential future directions for research.

II. WHAT IS DISTRIBUTED DENIAL OF SERVICE ATTACK

Distributed Denial of Service (DDoS) attacks aim to disrupt network services by inundating targeted servers with an excessive amount of traffic from multiple dispersed sources [15], [16]. These sources may include hacked web-connected bots or the attacker's PCs [17]. In today's technologically dependent society, DDoS attacks are a frequent type of attack that frequently targets virtual servers or web servers of large corporations like banks, governments, or e-commerce websites [18]. By quietly installing malicious scripts on compromised workstations, attackers build a botnet network and leverage the combined efforts of several machines to produce harmful traffic [19]. Although individual bot machines only send a small amount of bandwidth, the combined effect of this traffic could impair a service's availability [20]. Attackers also take advantage of holes in the protocols used by the Open Systems Interconnection (OSI) reference model [21]. The DDoS attack puts online businesses at risk since even a short period of outage can harm their bottom line or reputation.

III. COMMON DDOS ATTACK TYPES

DDoS attacks can be divided into four categories:

- Volume-based attacks
- Protocol layer attacks
- Application-layer attacks
- Zero-day attacks

A. Attacks Based on Volume

Attacks relying on volume have as their objective exceeding the target system's bandwidth capacity, expressed in bits per second. UDP floods, ICMP floods, and other phoney packet floods are examples of this kind of attack. We list a few typical instances of volume-based assaults. [22], [23].

1) UDP Floods: In a DDoS assault, the goal of a UDP flooding attack is to overload the target server with an overwhelming amount of traffic, leading the host to continuously look for an application on particular ports. The host responds with an ICMP (Desination Unreachable) packet if no application is found, which depletes host resources and can make the host unavailable [24].

2) ICMP floods: Like a UDP flooding attack, an ICMP flooding attack includes bombarding the target

with a large number of 'ICMP Echo Request"/ping packets in quick suc- cession. This kind of assault can consume both incoming and outgoing bandwidth, severely affecting the entire system [25].

B. Protocol Layer Attacks

This type of attack is measured in packets per second and uses server resources or intermediary communication infrastructures like firewalls and packet filtering (Pps). SYN flood, fragmented assaults, such as Smurf DDoS, death ping, and others are included in this kind of attack [26]. The following describes a few typical forms of protocol assaults.

1) SYN floods: By repeatedly sending SYN requests to establish a TCP connection with a host, while failing to acknowledge the host's SYN-ACK response, or making the requests from a fictitious IP address, the SYN flood DDoS assault takes advantage of a flaw in the TCP connection process. The host server uses resources while it waits for each request to be approved, resulting in a denial of service because new connections can be made [27].

2) Ping of Death: A Ping-of-Death attack involves the attacker repeatedly calling a computer with harmful or phoney intentions. The largest frame size is often limited by the data link layer, for instance, 1.5K bytes on an Ethernet network, despite the fact that an IP packet can have a maximum of 65,54 bytes in length. The destination server reassembles the fragments into the whole IP packet when a larger IP packet is split into numerous smaller IP packets (known as fragments). However, in this attack, the alteration of malicious fragment content causes the victim to receive an IP packet that is greater than 65,54 bytes when put together. Due to the influx of memory barriers allocated for the packet, this may result in genuine packets being denied service [26], [27].

C. Application-Layer Attacks

An application layer DDoS attack aims to flood a web server with many requests per second that appear to be safe and legal (Rps). Assaults of this kind target flaws in Windows, Apache, or OpenBSD, truncated, and sluggish attacks, POST or GET floods. Below is a description of a few typical application-layer DDoS attack types.

1) Slowloris: In a slowloris DDoS assault, the attacker can destroy a web server by keeping as many connections open as possible to the target server. The attack persuades the target server to retain these phoney connections by opening connections with it while only sending a part of the information that was requested. Therefore, it is likely that the highest synchronised link pool is filled to the point where only unauthorised users may join [24].

2) NTP Amplification: In an HTTP flooding attack, the hacker uses seemingly legitimate HTTP POST or GET queries to attack a web server or even an application [25], [27]. This kind of attack uses less bandwidth to damage the victim's system since it does not employ reflection, spoofing, or malformed packet attacks. The attack works best when the server or application is forced to use all of its resources in response to each request.

D. Zero-Day Attacks

Zero-day attacks are those that take advantage of recently discovered or newly known vulnerabilities for which there is now no suitable fix. The phrase has become more well-known among hackers, who frequently engage in the practice of exploiting zero-day flaws.

In "Fig 3", the various DDoS attack types are enumerated.

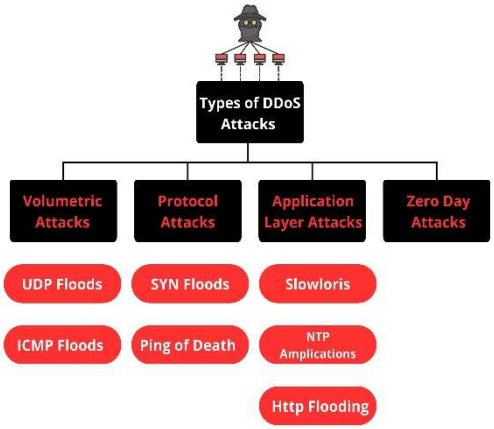

Fig. 3. Common types of DDoS attacks.

IV. LITERATURE SURVEY

Recent years have seen a substantial increase in interest in DDoS attack detection utilising time series data analysis, especially from 2016 to 2023.

This study by [28] conducted an analysis of the difficulties in identifying DoS and DDoS attacks in 2016. The time series was made utilising two metrics, the quantity of packets and the quantity of source IP addresses, extracted from network traffic per minute to predict the number of packets, this time series was converted utilizing the Box-Cox transformation and modelled using the ARIMA technique. The highest Lyapunov exponent was calculated to evaluate the confused nature of the prediction errors. In order to attacks the degree of chaos and non-chaos in the data, the local Lyapunov exponent was also computed to distinguish between normal traffic and attack traffic, the authors developed a set of standards based on the repeatability of chaotic behaviour and the exponential development in the ratio of the number of packets to the number of source IP addresses during attack stages. The simulation results showed that 99.5% of traffic experiences were appropriately classified by the proposed approach.

This study by [29] proposed a DDoS detection mechanism. This system used signature detection approaches to produce an automated decision tree for the efficient detection of signature-based flooding attacks, and it utilized the C.4.5 algorithm to lessen the danger of DDoS attacks by choosing various machine learning techniques and contrasting the outcomes; the authors put the system to the test.

This paper [30] proposed a cutting-edge method for identifying botnets in DDoS assaults in 2018. They proposed a theoretical model for the type of attack in which the botnet imitates regular traffic by continuously picking up acceptable patterns from its environment. The researchers created an inference technique that offers a reliable estimate of the botnet's existence in the network, and it was discovered that this algorithm eventually converged to the correct answer. They tested their suggested method for detecting botnets and discovered that, in a variety of implementation settings, it can quickly and reliably identify virtually all bots without interfering with the actions of regular users.

In this work by [31] they focused their attention in 2019 on drawing attention to the DDoS attack and its preventative strategy to make the server side less vulnerable. The authors discussed the problem of DDoS attacks, which involve sending massive volumes of packets at cloud-based websites and are made possible by piratelike operating systems. The most efficient algorithms for detection and prevention, Nave Bayes and Random Forest, are used in the final phase. This study also included several types of cloud computing attacks.

In 2020, the authors introduced a DDoS detection system based on ML with excellent accuracy and low false positive rates [32]. On the basis of signatures obtained from samples of network traffic, the system offers inductions. To counter four main forms of DDoS attacks, the authors conducted tests utilising four benchmark datasets and four ML algorithms. The results show maximum accuracy when compared to other powerful ML methods.

This paper by [33] proposed using ML techniques in 2021 to distinguish DDoS assaults from innocuous traffic. They evaluated their suggested methodology using the four major types of DDoS attack, UDP, DNS, SYN, and NetBIOS, after selecting 19 unique characteristics from the CIC 2019 DoS dataset. The results demonstrated that KNN and DT worked best, with accuracy rates of 100% and 98%, respectively. Nave Bayes, on the contrary, only obtained an accuracy rate of 29%.

This proposed by [34] utilised the CICDDOS2019 dataset to evaluate and develop ML models for the detection of DDoS attacks. To shorten training time, they used random sample collection and feature engineering to create a balanced data set with 360,000 records and the 15 most important characteristics. This study proposed ML models such as RF, Naive Bayes, Stochastic GB, KNN, and DT to train and evaluate predection. The finding shows that RF achieved the best, with an accuracy rate of more than 99% in both the original and balanced datasets. This study has shown that ML algorithms can accurately identify DDoS attacks.

This work by [35] proposed a bidirectional CNN-BiLSTM DDoS detection, which combines three deep learning algorithms like RNN, LSTM-RNN, and CNN. They compared the performance of these three models on the detection evaluation dataset (CICID2017) to determine the most effective one in detecting DDoS attacks from real traffic.

The evaluation of this study was based on four commonly utilised metrics as accuracy, precision, recall, and F-measure. The results showed that the models were highly efficient, with an accuracy of 99.00%, while for the CNN model (98.82%). The best results achieved by CNN-BiLSTM, with an accuracy of 99.76% and precision of 98.90%.

The comparison of stadies shown in Table 1 highlights the need to develop effective ways to recognize distributed denial of Service (DDoS) attacks. There are several methods, including time series analysis, ML algorithm, and signature-based detection, have been utilised to study these strategies. The results show that combining these strategies can produce very high levels of DDoS attack detection accuracy. These findings highlight the ability of machine learning techniques to identify DDoS attacks with precision and swiftness. However, as DDoS attacks develop, it is critical to constantly improve and adjust the technologies used for detection.

V. CONCLUSION

Current studies have shown supporting findings about DDoS attack detection systems based on time series data analysis. The Internet is more secure and stable because of these technologies capacity to identify DDoS attacks. However, there is still a chance of advancement, and more study is required to keep improving the functionality and ability of these systems.

TABLE I: LITERATURE REVIEW FROM 2016 TO 2023

Ref	Method	Accuracy	Key Finding
[28]	ARIMA	99.5%	The proposed system uses a combination of the Box-Cox transformation, the ARIMA model and local Lyapunov exponent to classify network traffic as normal or attack.
[29]	C4.5 algorithm	98.8%	DDoS detection system using the C45 algorithm and signature detection is proposed and verified to be effective with ML.
[30]	Inference algorithm,		A model for DDoS attacks by botnets and an inference algorithm to estimate botnets in a network is proposed. The algorithm consistently estimates botnets with only one minute of observation time.
[31]	RF & Naive bays	98.2%	A preventive approach to reducing server-side susceptibility to DDoS attacks. The method is presented using Naive Bayes and RF algorithms for detection and prevention.
[32]	ML algorithms	99.63%	A high accuracy, low false positive rate DDoS detection technique using ML is proposed and evaluated by four datasets and four ML techniques.
[33]	DT, KNN	99%	ML-based classification system is proposed to differentiate benign traffic from DDoS attacks.
[34]	ML algorithms	99%	DDoS detection using ML algorithms and the CICDDOS2019 dataset with feature engineering for efficient training, resulting in 99% accuracy with RF.
[35]	CNN-BiLSTM	99.76	A bidirectional CNN-BiLSTM DDoS detection model that combines three deep learning algorithms was proposed. The performance of the models was tested and compared on the CICID2017 dataset. The best results were achieved by the National Institutes of Health CNN-BiLSTM with an accuracy of 99.76% and a precision of 98.90%.

REFERENCES

[1] N. Malik, M. Sardaraz, M. Tahir, B. Shah, G. Ali, and F. Moreira, "Energy-efficient load balancing algorithm for workflow scheduling in cloud data centers using queuing and thresholds," *Appl. Sci.*, vol. 11, no. 13, p. 5849, 2021.

[2] H. Y. Khdier, W. M. Jasim, and S. A. Aliesawi, "Deep learning algorithms based voiceprint recognition system in noisy environment," in *Journal of Physics: Conference Series*, 2021, vol. 1804, no. 1, p. 12042.

[3] Q. Yan and F. R. Yu, "Distributed denial of service attacks in software-defined networking with cloud computing," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 52–59, 2015.

[4] F. Lau, S. H. Rubin, M. H. Smith, and L. Trajkovic, "Distributed denial of service attacks," in *Smc 2000 conference proceedings. 2000 ieee international conference on systems, man and cybernetics.'cybernetics evolving to systems, humans, organizations, and their complex interactions'(cat. no. 0*, 2000, vol. 3, pp. 2275–2280.

[5] S. Sambangi and L. Gondi, "A machine learning approach for ddos (distributed denial of service) attack detection using multiple linear regression," in *Proceedings*, 2020, vol. 63, no. 1, p. 51.

[6] N. M. Alfahad, S. A. Aliesawi, and F. S. Mubarek, "Enhancing AODV routing protocol based on direction and velocity for real-time urban scenario," *J. Theor. Appl. Inf. Technol.*, 2018.

[7] Z. K. Maseer, R. Yusof, S. A. Mostafa, N. Bahaman, O. Musa, and B. A. S. Al-rimy, "DeepIoT. IDS: hybrid deep learning for enhancing IoT network intrusion detection," *Comput. Mater. Contin*, vol. 69, no. 3, pp. 3945–3966, 2021.

[8] S. A. Aliesawi, D. S. Alani, and A. M. Awad, "Secure image transmission over wireless network," *Int. J. Eng. Technol.*, vol. 7, no. 4, pp. 2758–2764, 2018.

[9] Y. Al-Hadhrami and F. K. Hussain, "DDoS attacks in IoT networks: a comprehensive systematic literature review," *World Wide Web*, vol. 24, no. 3, pp. 971–1001, 2021.

[10] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: a classification," in *Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology (IEEE Cat. No. 03EX795)*, 2003, pp. 190–193.

[11] B. A. Khalaf, S. A. Mostafa, A. Mustapha, M. A. Mohammed, and W. M. Abduallah, "Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods," *IEEE Access*, vol. 7, pp. 51691–51713, 2019.

[12] M. H. Wasmi, S. A. Aliesawi, and W. M. Jasim, "Distributed semi-clustering protocol for large-scale wireless sensor networks," *Int. J. Eng. Technol.*, vol. 7, no. 4, pp. 3119–3125, 2018.

[13] M. J. Awan *et al.*, "Real-time DDoS attack detection system using big data approach," *Sustainability*, vol. 13, no. 19, p. 10743, 2021.

[14] H. Abusaimeh, "Distributed denial of service attacks in cloud computing," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 6, 2020.

[15] R. F. Fouladi, O. Ermiş, and E. Anarim, "A DDoS attack detection and defense scheme using time-series analysis for SDN," *J. Inf. Secur. Appl.*, vol. 54, p. 102587, 2020.

[16] S. Aliesawi, C. C. Tsimenidis, B. S. Sharif, and M. Johnston, "Performance comparison of IDMA receivers for underwater acoustic channels," in *2010 7th International Symposium on Wireless Communication Systems*, 2010, pp. 596–600.

[17] S. Yu, *Distributed denial of service attack and defense*. Springer, 2014.

[18] M. Fabian and M. A. Terzis, "My botnet is bigger than yours (maybe, better than yours): why size estimates remain challenging," in *Proceedings of the 1st USENIX Workshop on Hot Topics in Understanding Botnets, Cambridge, USA*, 2007, vol. 18.

[19] B. McCarty, "Botnets: Big and bigger," *IEEE Secur. Priv.*, vol. 1, no. 4, pp. 87–90, 2003.

[20] H. N. Thanh and T. Van Lang, "Use the ensemble methods when detecting DoS attacks in Network Intrusion Detection Systems," *EAI Endorsed Trans. Context. Syst. Appl.*, vol. 6, no. 19, pp. e5–e5, 2019.

[21] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE Commun. Surv. tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.

[22] D. Chaudhary, K. Bhushan, and B. B. Gupta, "Survey on DDoS attacks and defense mechanisms in cloud and fog computing," *Int. J. E-Services Mob. Appl.*, vol. 10, no. 3, pp. 61–83, 2018.

[23] T. Kawamura, M. Fukushi, Y. Hirano, Y. Fujita, and Y. Hamamoto, "An NTP-based detection module for DDoS attacks on IoT," in *2017 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)*, 2017, pp. 15–16.

[24] A. M. da Silva Cardoso, R. F. Lopes, A. S. Teles, and F. B. V. Magalhães, "Real-time DDoS detection based on complex event processing for IoT," in *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 2018, pp. 273–274.

[25] R. Yaegashi, D. Hisano, and Y. Nakayama, "Light-weight DDoS mitigation at network edge with limited resources," in *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, 2021, pp. 1–6.

[26] D. Yin, L. Zhang, and K. Yang, "A DDoS attack detection and mitigation with software-defined Internet of Things framework," *IEEE Access*, vol. 6, pp. 24694–24705, 2018.

[27] Y. Jia, F. Zhong, A. Alrawais, B. Gong, and X. Cheng, "Flowguard: An intelligent edge defense mechanism against IoT DDoS attacks," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9552–9562, 2020.

[28] S. M. T. Nezhad, M. Nazari, and E. A. Gharavol, "A novel DoS and DDoS attacks detection algorithm using ARIMA time series model and chaotic system in computer networks," *IEEE Commun. Lett.*, vol. 20, no. 4, pp. 700–703, 2016.

[29] M. Zekri, S. El Kafhali, N. Aboutabit, and Y. Saadi, "DDoS attack detection using machine learning techniques in cloud computing environments," in *2017 3rd international conference of cloud computing technologies and applications (CloudTech)*, 2017, pp. 1–7.

[30] V. Matta, M. Di Mauro, and M. Longo, "DDoS attacks with randomized traffic innovation: Botnet identification challenges and strategies," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 8, pp. 1844–1859, 2017.

[31] A. Amjad, T. Alyas, U. Farooq, and M. A. Tariq, "Detection and mitigation of DDoS attack in cloud computing using machine learning algorithm," *EAI Endorsed Trans. Scalable Inf. Syst.*, vol. 6, no. 23, pp. e7–e7, 2019.

[32] A. U. Sudugala, W. H. Chanuka, A. M. N. Eshan, U. C. S. Bandara, and K. Y. Abeywardena, "WANHEDA: a machine learning based DDoS detection system," in *2020 2nd International Conference on Advancements in Computing (ICAC)*, 2020, vol. 1, pp. 380–385.

[33] R. J. Alzahrani and A. Alzahrani, "Security analysis of ddos attacks using machine learning algorithms in networks traffic," *Electronics*, vol. 10, no. 23, p. 2919, 2021.

[34] A. Bandi, L. Sherpa, and S. M. Allu, "Machine learning algorithms for DDoS attack detection in cybersecurity," in *Modern Approaches in Machine Learning & Cognitive Science: A Walkthrough*, Springer, 2022, pp. 269–281.

[35] F. M. Aswad, A. M. S. Ahmed, N. A. M. Alhammadi, B. A. Khalaf, and S. A. Mostafa, "Deep learning in distributed denial-of-service attacks detection method for Internet of Things networks," *J. Intell. Syst.*, vol. 32, no. 1, p. 20220155, 2023.