UNIABUJA Journal of Engineering and Technology

https://ujet.uniabuja.edu.ng/

ISSN: 2714-3236 (Online); 2714-3228 (Print)

Volume 2, Issue 1, 2025; 51-68

Systematic Literature Review on Distributed Denial of Service Attack

Rukayat B. AHMED[1], Olawale S. ADEBAYO[2], Sulieman AHMAD[3], Peter C. ANYAORA[4*], Mustapha ATIKU[5], Nafisa D. ADELEKE[6], Meshach BABA[7]

[1,2,3,4 6,7]*Department of Cybersecurity Science, Federal University of Technology, Minna, Nigeria*
[5]*Department of information technology, Federal University of Technology, Minna, Nigeria*

[*]*Corresponding Author: p.anyaora@futminna.edu.ng*

Abstract
Distributed Denial of Service (DDoS) attacks are one of the more sophisticated threats that have been targeting the internet and systems in recent years. Traditional machine learning-based intrusion detection systems (IDSs) frequently do not detect these attacks effectively when they are trained on unbalanced datasets. This work provides a system literature review (SLR) on Distributed Denial of Service (DDoS) attack detection, by presenting a detailed assessment of the approaches and methodologies taken throughout the nine years, emphasizing machine learning and deep learning techniques. The review examines various approaches, including token embedding for feature extraction, transformer-based models, and hybrid detection techniques. Despite improvements, the study highlights ongoing challenges, such as computational complexity and the need for enhanced solutions like blockchain-based detection systems. Open research gaps and future directions, including the refinement of detection algorithms for evolving DDoS tactics, are also discussed, offering a comprehensive resource for researchers aiming to improve DDoS mitigation.

Keywords: *Denial of service attack, deep learning, distributed denial of service attack, machine learning.*

1.0 Introduction

One cannot fathom living in today's fast-paced world without the Internet, which is necessary for a wide range of purposes, including business purchasing, education, communication, and more. Notwithstanding its many benefits, several crimes, such as attacks, hacking, and the dissemination of false information, have increased online. When legitimate users are unable to access a service, system, or network, this is known as a denial of service (DoS) attack. DDoS attacks are a subset of DoS attacks that happen when an attacker hacks several computer devices in order to disrupt a targeted victim's normal traffic. Emphasizes the need for sophisticated models that can manage the intricacies of contemporary network traffic, especially models that make use of more recent datasets that mirror current attack trends. In contrast to earlier datasets like KDD99, this study suggests adopting the UNSW-NB15 dataset, which contains contemporary attack vectors and is more representative of current network conditions.

Nazih *et al.* (2020) formulated the detection of DDoS attacks as a classification problem and proposed an approach using token embedding to enhance extracted features from SIP messages. The authors discussed a deep learning model based on Recurrent Neural Networks (RNNs) developed to detect DDoS attacks with low and high-rate intensity. For validation, a balanced real traffic dataset was built containing three attack scenarios with different attack durations and intensities.

In order to detect distributed denial-of-service (DDoS) attacks on SDN, Wang and Li (2021) developed a hybrid neural network DDoSTC structure that combines scalable and effective transformers with a convolutional neural network (CNN). This structure was tested on the most recent dataset, CICDDoS2019. They also built upon a transformer-based DDoSTC model based on the most recent DDoS attack dataset. In order to improve verification, a number of experiments were carried out by segmenting the dataset and comparing it with the most recent deep learning detection method used in DDoS intrusion detection. Additionally, Wang et al. (2021) developed a DDoS attack detection system to protect in a software-defined Internet of Things (SD-IoT) environment in real time. In their study, the authors utilized an improved firefly algorithm to optimize the convolutional neural network (CNN), for detecting DDoS attacks in their proposed SD-IoT framework. Amma (2022) proposed a Tuned Vector Convolutional Deep Neural Network (TVCDNN) by optimizing the structure and parameters of the deep neural network using binary and real Cumulative Incarnation (CuI), respectively. The CuI is a genetic-based optimization technique which optimizes the tuning process by providing values generated from best-fit parents. DDOS classification and detection using data mining technique is a significant area in the detection of DDoS attack. This technique of detection can be

Received: 03-01-2025 / Accepted: 26-01-2025 /Published: 31-03-2025

classified into supervised and unsupervised learning strategies and several techniques (Roiger and Geatz, 2003).

This paper's focus is on employing convolutional neural networks (CNNs) to detect Distributed Denial of Service (DDoS) attacks, which are one of the biggest security risks now facing the world. Thousands of infected computers, known as "zombies," initiate DDoS attacks, and these machines collectively form a "zombie" network. These zombies carry out extensive attacks on a victim, exhausting its network resources and bandwidth. History-based Internet Protocol (IP) filtering and the traffic entropy model are popular DDoS detection models (Maranhão et al., 2020). Such conventional network intrusion detection systems, however, are unable to handle contemporary DDoS assault tactics, which are more difficult to identify and stop, due to the advancement of cloud computing, the Internet of Things (IoT), and artificial intelligence approaches (Jiang et al., 2018). One deep learning technique, CNN, is utilized because it is suitable for identifying DDoS attacks due to its dual capabilities of feature extraction and data classification. A detection system that can deal with data unavailability is required in the modern world. According to Marianhão et al. (2020), damaging traffic labels are less common than legitimate traffic labels. (Mebawondu *et al*., 2020) outlines current methods for intrusion detection systems (IDS), emphasizing the drawbacks of conventional rule-based systems and the expanding application of machine learning techniques to increase detection precision.

Research Questions Concerns

1) Which deep learning and machine learning methods have been applied recently to identify Distributed Denial of Service (DDoS) assaults, and what is their efficacy?
2) How do different types of datasets, such as CICDDoS2019 and NSL-KDD, impact the performance of DDoS detection models?
3) What are the emerging challenges and potential future solutions in enhancing DDoS detection systems, particularly in IoT and cloud environments?

The purpose of this review is to provide a clear understanding of DDoS attacks, including their approaches and techniques used in the field of internet security. Additionally, this review examines previous research efforts to facilitate the improvement of existing DDoS attack detection methods.

The remainder of this paper is organized as follows: Section Two presents a detailed analysis of previous related literature. Section Three outlines the methodology used in this research, while Section Four discusses the results and findings. Section Five provides the conclusion, and Section Six explores future research directions for advancing DDoS attack detection.

2.0 Related Work

Seo and Lee (2016) conducted a study focused on the detection of IP-spoofed DDoS attacks. They employed a method that involved calculating the frequency of network-based packet attributes and analysing anomalies in these attributes. Aljumah (2017) suggested a DDoS detection system that uses artificial neural networks to identify and flag harmful and legitimate data traffic, preventing the network from experiencing performance issues. The author assessed and contrasted their suggested system with the current models of the relevant work based on accuracy, sensitivity, and precision. To identify and mitigate DDoS attacks in a large-scale network, including a smart city constructed on SDN infrastructure, Bawany *et al.* (2017) developed a unique framework (ProDefense). Application-specific DDoS attack, detection and mitigation needs can be satisfied by the author's framework. Gondim *et al.* (2016) introduced a novel approach aimed at empirically assessing the threat posed by conducting controlled tests of attacks on IoT devices. Their methodology considered the perspective of potential attackers and actively sought vulnerabilities within computer systems. Jia (2017) developed a hybrid heterogeneous multiclassifier ensemble learning-based DDoS assault detection technique and built the detection system using a heuristic detection approach based on Singular Value Decomposition (SVD). The experimental findings demonstrated the superior TNR, accuracy, and precision of their detection technique. By employing system packet analysis to identify DDoS attack patterns and machine learning techniques to investigate these patterns, Nayaki and Kumar (2017) created an intelligent detection system for DDoS attacks. The Center for Applied Internet Data Analysis supplied the author with a significant quantity of network packets to analyse, and the author used the detection system using Ad-hoc On-demand Distance Vector (AODV) and Adaptive Information Dissemination (AID) protocols. When it comes to DDoS detection, the discovery mechanism is accurate.

Adebayo *et al.* (2018) conducted a study in which they applied six widely recognized classification algorithms—Random Forest, Decision Stump, NNge, OneR, RART, and Naïve Bayes: to the NSL-KDD dataset got an optimised accuracy of 98.58 with a reduced 0.351 false positive rate. Shaaban and Hussein (2019) presented a Convolutional Neural Network (CNN) technique to detect and classify DDoS traffic into normal and malicious information with an accuracy of 99% using two different datasets. One was captured from a simulated MCC network by Wireshark and the other one was a predefined open-source dataset. Dantas Silva

et al. (2020) developed a taxonomy to classify and describe strategies for mitigating DDoS attacks using SDN technologies in IoT environments. Their contributions include a comprehensive review of DDoS mitigation strategies in IoT scenarios, a classification guide considering various parameters, an overview of existing mitigation techniques, a comparative analysis using established criteria, and discussions on open issues and research challenges in this domain. Gadzama and Adebayo (2020) proposed a method for classifying distributed denial of service (DDOS) attacks using a genetic algorithm-based neural network (NNGA). They employed a genetic algorithm to enhance the neural network's capabilities for DDoS attack detection, aiming to enhance classification accuracy and overall efficiency. Maranhão *et al.* (2020) introduced a novel method for DDoS attack detection that involves extracting average common features from the dataset. Initially, to remove the average value of common features across instances in the dataset, they used Higher-Order Singular Value Decomposition (HOSVD). They then classified the data as either DDoS attacks or benign traffic using machine learning algorithms including gradient boosting, decision trees, and random forests. In the framework of the COVID-19 scenario, Grey *et al.* (2020) presented a novel technique for identifying DDoS attacks that is especially suited for small business owners. Support Vector Machine (SVM), Linear Regression (LR), Gradient Boosting, Decision Tree Classifiers, and Random Forest were among the machine learning algorithms they used.

Even when trained with damaged data, Maranhao *et al.* (2021) suggested a noise-robust multilayer perceptron (MLP) architecture for identifying DDoS attacks. Their method uses Higher Order Singular Value Decomposition (HOSVD) techniques, which have a higher computational complexity, to iteratively filter out the average values of similar features among dataset instances. By increasing CNN's computational complexity for DDoS assault model detection, this research's drawback was lessened. Subairu *et al.* (2020) suggested and created design frameworks to address this reported issue with convolutional neural networks used in image classification models. The results the authors got after proper implementation of the proposed CNN design framework showed an insignificant misclassification as the false positive rate was extremely low, likewise the false negative. Ahmad *et al.* (2021) conducted a study focusing on enhancing the detection of Denial-of-Service (DoS) anomalies in Wireless Sensor Networks (WSNs) while maintaining power reservation balance within the network. They introduced a novel clustering technique called the CH_Rotations algorithm, designed to improve the efficiency of anomaly detection throughout the lifetime of a WSN. The study also investigated the impact of feature selection techniques in conjunction with various machine learning algorithms for analysing WSN node traffic and their influence on the network's lifespan. Ko *et al.* (2021) presented an Intelligent Attack Mitigation (IAM) system, which adopts an ensemble approach by utilizing basic learners combined with a majority voting scheme. Within this framework, they introduced the Reference Adaptation Algorithm (RAA), which is a target-driven, distribution-enabled, and specialized clustering algorithm designed to cooperate with an ISP's blackholing mechanism for mitigating Distributed Denial of Service (DDoS) attacks. Chen *et al.* (2021) introduced the Flow Differentiation Detector (FDD) to detect Hybrid DDoS attacks effectively. The FDD employs a fuzzy-based mechanism called Target Link Selection to identify critical links for DDoS attacks and statistically evaluate the traffic patterns on these links. Notably, they implemented the FDD within the SDN controller OpenDayLight to create a Hybrid DDoS attack detection system. Wang and Li (2021) proposed the DDosTC model, a transformer-based approach for detecting distributed denial-of-service (DDoS) attacks on SDN (Software-Defined Networking) systems. They utilized the latest DDoS attack dataset, CICDDoS2019, and designed a hybrid neural network structure that combines efficient transformers and a convolutional neural network (CNN). Wang *et al.* (2022) proposed a DDoS attack detection scheme tailored for real-time security in the Software-Defined Internet of Things (SD-IoT) environment. Amma (2022) proposed a Tuned Vector Convolutional Deep Neural Network (TVCDNN), optimizing the deep neural network's structure and parameters using both binary and real Cumulative Incarnation (CuI). Guo *et al.* (2022) proposed a novel deep learning approach called GLD-Net for DDoS attack detection. This method simultaneously extracts flow and topological features from time-series flow data and leverages a Graph Attention Network (GAT) to uncover correlations between non-Euclidean features, effectively fusing flow and topological information. *Li et al.* (2022) proposed a two-stage intelligent detection mechanism for identifying various types of DDoS attacks. The approach combines similarity-based prior knowledge with CNN-based attention. An enhanced ANN model with data dimension reduction features was developed by Rasheed *et al.* (2022) for the implementation of an attack detection system, particularly for DDoS attacks, which have become a threat in recent years. Almaraz-Rivera *et al.* (2022) conducted research utilizing the Bot-IoT dataset, a comprehensive resource for safeguarding IoT networks. Their methodology aimed to address the class imbalance issue in the original dataset without introducing synthetic data or class weights. Aslam *et al.* (2022) proposed introduced an Adaptive Machine Learning-based framework called AMLSDM, designed for detecting and mitigating Distributed Denial-of-Service (DDoS) attacks in Software-Defined Networking (SDN) environments. By combining SDN technology with adaptive machine learning, this framework seeks to improve the security of IoT devices. A mathematical model for distributed denial-of-

service assaults was put forth by Kumari and Mrunalini in 2022. Attacks and typical situations are detected using machine learning methods like Naive Bayes and Logistic Regression. The CAIDA 2007 dataset was used for the experimental study. Mishra *et al.* (2022) presented introduced a novel approach called "perplexed-based classification with feature selection" for identifying and distinguishing attacks within data. They specifically focused on detecting Distributed Denial-of-Service (DDoS) attacks. The approach involved selecting a dataset containing features related to the attacks, and from these features, actionable characteristics were extracted by assessing their correlation with the target variable. Patil (2022) proposed introduced a novel distributed classification system called SSK-DDoS, which utilizes Spark Streaming and Kafka to classify various types of Distributed Denial-of-Service (DDoS) attacks and legitimate network flows. A machine learning-based approach to smart grid DoS attack detection was presented by Reddy *et al.* in 2022. The technique gathered real-time network communication data between the data server and the smart meter. The trained SVM classifier model was used to detect and classify DoS assaults by using PCA dimension reduction and feature selection to select more representative characteristics.

Saha *et al.* (2022) conducted a complete evaluation of various Feature Set (FS) methods, employing three primary categories of AI techniques. They examined a total of 15 individual feature sets, one ensemble feature set (EnFS), and the original feature set to identify the optimal feature set. Prasad and Chandra (2022) proposed the Voting-Based Multimode Framework to Counter Volumetric DDoS (VMFCVD) attacks, comprising three modes: Fast Detection Mode (FDM), Defensive Fast Detection Mode (DFDM), and High Accuracy Mode (HAM). Abu Bakar et al. (2023) suggested an intelligent agent system that uses automatic feature extraction and selection to detect DDoS attacks. In their trial, the authors employed a custom-generated dataset called CICDDoS2019, and the system outperformed the most advanced machine learning-based DDoS attack detection methods by 99.7%. Ali et al. (2023) examined the performance of several classification techniques, such as support vector machines (SVMs), convolutional neural networks (CNNs), multiple layer perceptrons (MLP), decision trees (DTs), and K-nearest neighbors (KNNs). Aswad *et al.* (2023) proposed a combined three deep learning algorithms, namely recurrent neural network (RNN), long short-term memory (LSTM)-RNN, and convolutional neural network (CNN), to build a bidirectional CNN-BiLSTM DDoS detection model. The RNN, CNN, LSTM, and CNN-BiLSTM were implemented and tested to determine the most effective model against DDoS attacks that can accurately detect and distinguish DDoS from legitimate traffic. The intrusion detection evaluation of the Canadian Institute of Cyber Security Intrusion Detection System 2017(CICIDS2017) dataset was used to provide more realistic detection. The CICIDS2017 dataset closely matched real-world Packet Capture data by providing safe and current samples of common attacks. Confusion Metrix was used to test and evaluate the four models concerning the four widely used criteria: accuracy, precision, recall, and F-measure. Except for the CNN model, which achieves an accuracy of 98.82%, the models' performance was fairly successful, achieving an accuracy rate of about 99.00%. The highest accuracy of 99.76% and precision of 98.90% are attained by the CNN-BiLSTM.

Galeano-Brajones *et al.* (2020) proposed an experimental assessment of an entropy-based approach for detecting and mitigating DoS and DDoS attacks within IoT scenarios, utilizing a stateful SDN data plane. Huraj and Šimon (2020) conducted a case study on the impact of DDoS attacks on IoT devices in a smart home environment. They investigated how these attacks affected communication and control of IoT sensors from the user's perspective while using smart home services. Hsu *et al.* (2021) introduced a novel mechanism called Migration Sensor (MS) aimed at enhancing TCP/IP connection establishment and detecting Distributed Denial of Service (DDoS) attacks. This mechanism addresses the challenge of setting up a new TCP/IP connection for a host under attack. Mishra *et al.* (2021) proposed a novel solution aimed at detecting volume-based Distributed Denial of Service (DDoS) attacks efficiently. This solution, called the identification-pattern mechanism using a threshold scheme, serves as a pre-emptive measure for DDoS attack detection while maintaining low latency and high throughput.

Wang and Wang (2022) developed an online SDN-based defence system for detecting and mitigating attacks. This system comprises two main components: (i) an anomaly detection module and (ii) a mitigation module. The anomaly detection module employs a lightweight hybrid deep learning approach called Convolutional Neural Network and Extreme Learning Machine (CNN-ELM) to identify traffic anomalies. Najafimehr *et al.* (2022) proposed an innovative approach for detecting novel DDoS attacks, employing a hybrid machine learning strategy that combines both supervised and unsupervised techniques. Ibrahim *et al.* (2022) proposed an Ethereum blockchain-based model designed to identify and prevent Distributed Denial of Service (DDoS) attacks against IoT systems. This system not only serves to thwart DDoS attacks but also addresses issues like single points of failure, privacy concerns, and security vulnerabilities in IoT systems. Shah *et al.* (2022) conducted a comprehensive review of different Blockchain-based approaches aimed at countering DDoS attacks in IoT environments. The study began by examining the vulnerabilities of IoT networks to DDoS attacks, exploring the consequences of these attacks on IoT networks and their associated services. Yin *et al.* (2022) proposed a trusted multi-domain DDoS attack detection approach based on federated

learning. They categorized DDoS attack types into sub-attacks and created domain-specific federated learning datasets to achieve comprehensive detection while preserving data privacy. Roy *et al.* (2022) introduced a novel network architecture designed to combat the threat of DDoS attacks. They have harnessed Physically Unclonable Functions (PUFs) as a promising security solution. Zhang *et al.* (2022) devised a space-time graph model to pinpoint critical nodes within Low Earth orbit satellite constellation networks (LSCNs). They conducted DDoS attacks as the first method to target these crucial nodes. AlArnaout *et al.* (2023) proposed the Robust Attack Path Tracing (RAPT) algorithm as an efficient solution for countering SYN-Flood Distributed Denial of Service (DDoS) attacks. This algorithm is implemented on both edge and core routers, allowing them to initiate trace packets in response to attacks. Shieh *et al.* (2023) provided an effective solution for identifying and alleviating DDoS. The module continuously improves the model's performance by incorporating new knowledge and adapting to new attack patterns.

Hossain and Islam, (2024) proposed an enhanced approach for detecting DDoS attacks using a hybrid feature selection technique in combination with an ensemble-based classifier. The ensemble-based approach aggregated many decision trees to increase classification accuracy and reduce overfitting and model robustness. The feature selection technique used correlation analysis, mutual information, and principal component analysis to identify the most useful characteristics for attack detection. The ensemble-based Random Forest classifier from the various ensemble-based approaches with the specified relevant features produces the best detection rates. Many datasets related to identifying DDoS attacks were used to evaluate the proposed model, and experimental findings demonstrated that it surpasses existing techniques in terms of accuracy, recall, precision, f1-score, and false positive rate with other evaluation metrics. The proposed approach achieves almost 99.93 % accuracy and 0 % error rate making it a promising solution for DDoS attack detection. Dash *et al.* (2024) proposed two approaches, one utilizing Principal Component Analysis (PCA) and another without PCA, to compare their performance. Robust scaling and encoding techniques are applied as preprocessing steps. The experiment outcomes demonstrate a noteworthy improvement in the accuracy of DDoS attack detection in IoT devices by integrating PCA and Robust Scaler. Notably, the Random Forest and KNN classifiers demonstrate exceptional performance with an accuracy of 99.87% and 99.14%, respectively, while Naïve Bayes showed a lower accuracy of 87.14%. Their experiment's results provided important information for improving IoT device security against DDoS attacks. The suggested method demonstrated how crucial suitable preprocessing methods are to building reliable intrusion detection systems for Internet of Things settings. The DeepDefend framework was used by Ouhssini *et al.* (2024) to detect and stop DDoS attacks in cloud environments in real-time. To forecast network traffic entropy and identify possible threats, the authors used deep learning techniques, particularly CNN-LSTM-Transformer networks. The framework improved the AutoCNN-DT model's ability to differentiate between attack and legitimate traffic by using a genetic method for optimal feature selection. DeepDefend showed excellent entropy predicting accuracy and quick, accurate DDoS attack detection when tested on the CIDDS-001 traffic dataset. By integrating deep learning, genetic algorithms, and time series analysis, this integrated strategy provides a strong defence against DDoS attacks for cloud computing infrastructure.

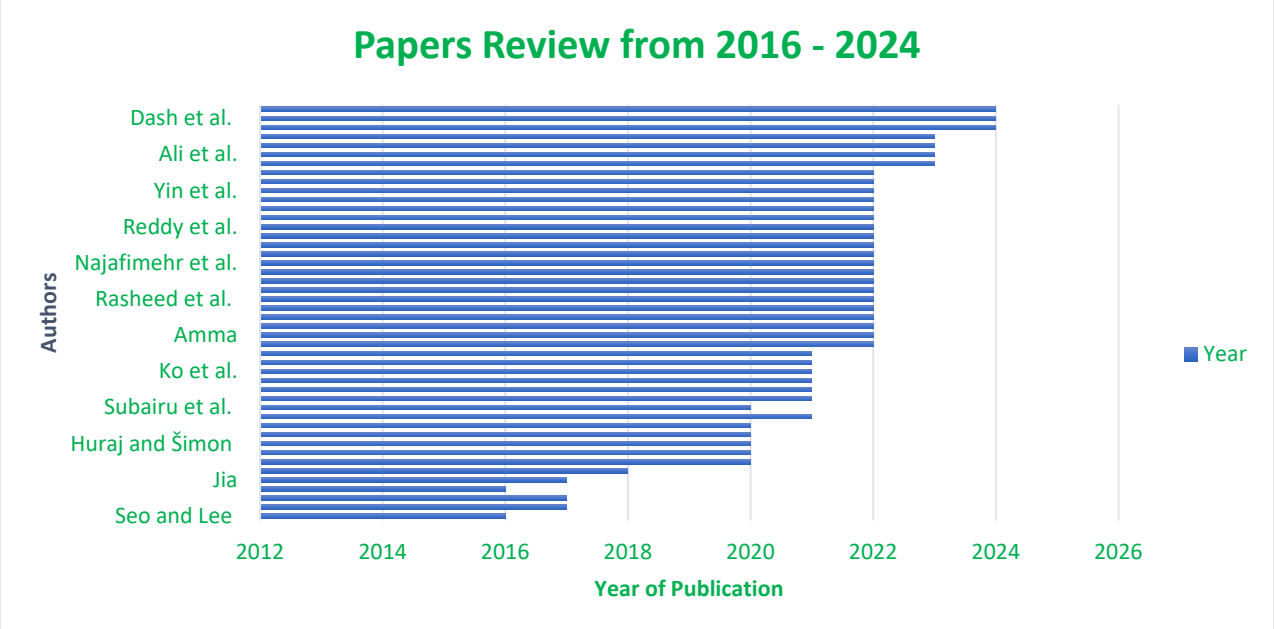

Figure 1: A Visual summary chart of the related words

Received: 03-01-2025 / Accepted: 26-01-2025 /Published: 31-03-2025

3.0 Methodology

The research procedures used to examine the body of work in the field of DDoS attack detection techniques are presented in this part. It was also revealed how the pre-existing studies were chosen using predetermined inclusion and exclusion criteria.

3.1 Protocol and Phases of the Study

The Preferred Reporting Items for Systematic Reviews and Analyses (PRISMA), (Moher *et al*., 2009) and the established guidelines in the work of (Kitchenham *et al*., 2009) were adopted in this review.

3.2 Source of Data

Reputable academic research databases covering computational disciplines with a good publication reputation are necessary to obtain data from trustworthy sources. As indicated in Table 1, these databases included, but were not limited to, Science Direct, Springer, IEEE Xplorer, Academia, and Research-gate. The study's main source of data came from conference proceedings and journals published by such organizations. Since they are deemed unreliable, papers from unreliable sources, including Wikipedia, were not taken into consideration.

Table 1: Database search sources

S/N	Database Sources	No. of Articles
1.	Science Direct	213
2.	Springer	259
3.	IEEE Xplorer	269
4.	Academia	117
5.	Research gate	100
	Total	958

3.2 Keywords for Search

In this study, the literature search methodology of Kitchenham *et al.* (2009) was applied. The core search terms were carefully selected to identify the most relevant search phrases. Using the review's stated objectives, the following search phrases were utilized to find pertinent content in a few esteemed academic archives: DDoS assault plus identification.

3.3 Inclusion and Exclusion Criteria for Paper Selection

A set of criteria was used to choose the papers for this investigation. Only papers that fit and fulfilled these requirements were chosen. Table 2 displays the criteria together with the corresponding rationale.

Table 2: Inclusion/Exclusion Criteria of research publications

S/N	Criteria	Explanation/Justification
1.	The original research publication was not a survey or review paper.	The research papers are expected to focus on the DDoS attack detection techniques.
2.	The proposed solutions must be on the methodologies/techniques/processes of DDoS attack detection.	This research aims to aid newer and expert researchers in the development of better techniques and approaches.
3.	The publication must be a full-length paper.	Short papers are insufficient in providing relevant information on the proposed solution.
4.	The language chosen for writing the research paper must be written in the English language.	The publication must be written in English language.
5.	The paper must be published between 2015-2024	The coverage of the Systematic Literature Review is 9 years, from 2016-2024.

Received: 03-01-2025 / Accepted: 26-01-2025 /Published: 31-03-2025

3.4 Study Selection Process

A study 510 identified by the initial keyword searches on the chosen database platforms. After eliminating the duplicate research, the number was drastically reduced to 150. The research papers that match the inclusion/exclusion criteria were thoroughly examined, and 117 publications were left over for reading. Only papers written in English and published between 2011-2023 were chosen. After reading all 117 papers in detail and using the inclusion/exclusion criteria again, 26 papers were left for the systematic literature review. The identification, screening, eligibility and included phases are presented in Figure 2.

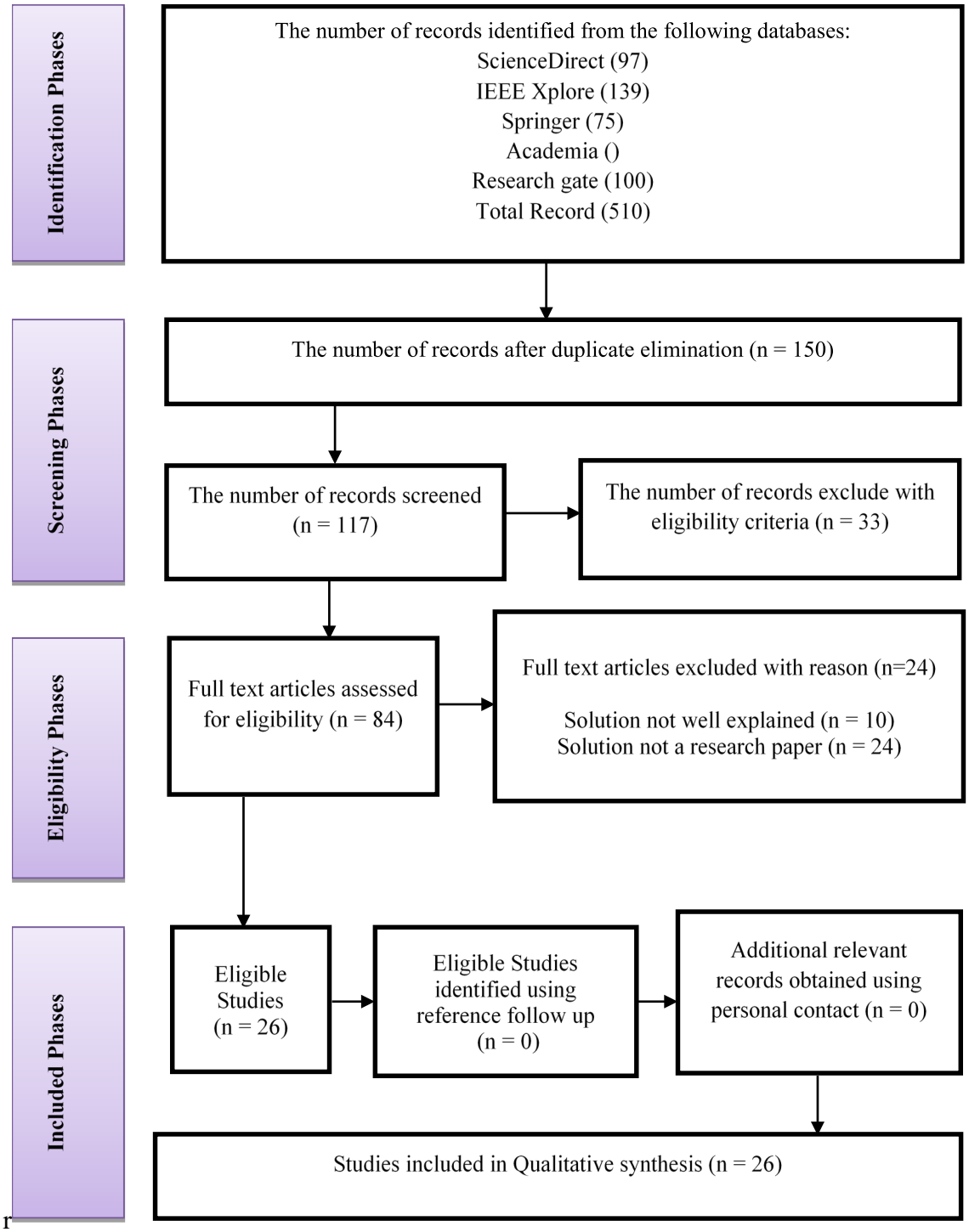

Figure 2: The Study Selection Workflow with PRISMA

4.0 Result and Discussion

Peer-reviewed works published between 2016 and 2024 were the subject of this study. This was due to the fact that the objective was to determine which models and frameworks were utilized in the past years for

the identification of DDoS attacks. A total of fifty (50) articles were assessed after the pertinent review papers published between 2016 and 2024 were screened. There were two (2) reviews in 2016, four (4) reviews in 2017, two (2) reviews in 2018, two reviews in 2019, nine reviews in 2020, six reviews in 2021, eighteen reviews in 2022, and just four reviews in 2023. Lastly, as indicated in Table 3, three were published in 2024. Table 3 summarizes the selected reviewed articles. As previously mentioned, 50 papers were reviewed. Table 3 includes the names of the authors, the year and title of the publications, the problems the authors addressed, the methodology or framework they used to address those problems, the datasets they used, and, finally, the research gap of the authors. Some writers offered a DDoS attack detection methodology, while others suggested a model or framework for DDoS attack prevention and mitigation. A blockchain approach to DDoS attack detection was one of the novel models that was suggested. It was challenging to describe the methods employed in some of the research publications, and several of the researchers failed to explicitly explain the limitations of their study. According to the study survey, more work is still needed on the blockchain method for DDoS attack detection because there are not as many papers on it as there are on the machine and deep learning approaches.

Table 3: Number of DDoS attack detection reviewed published articles per year

Number of Published Papers	Publication Year
2	2016
4	2017
2	2018
2	2019
9	2020
6	2021
18	2022
4	2023
3	2024

Received: 03-01-2025 / Accepted: 26-01-2025 /Published: 31-03-2025

Table 4: Summarized the above selected reviewed article

Authors	Problem Addressed	Methodology	Dataset Used	Performance Metrics	Research Gap
Seo and Lee, 2016	Calculated the frequency of network-based packet attributes and analysed the anomalies of the attributes in order to detect IP-spoofed DDoS attacks.	ML	Not stated	1. Accuracy 2. Error Ratio	
Gondim *et al.*, 2016	Presented a novel approach used to empirically examine the threat represented by running the attack over a controlled environment, with IoT devices, considered from the perspective of an attacker.	-			The main limitation of this work relies on the fact that the approach used is novel, not only in its application to IoT but for availability in general.
Grey *et al.*, 2020	suggested a unique method for small business owners to detect DDoS attacks in the COVID-19 scenario.	ML		1. Recall 2. Accuracy 3. Precision 4. F-1 Score	
Maranhão *et al.*, 2020	suggested a brand-new average common feature extraction method for detecting DDoS attacks.	ML	CICDDoS2019 and CICIDS2017	Accuracy (98.94%), Detection Rate (97.70%), False Alarm Rate (4.35%) Area Under the Precision-Recall Curve (0.9937) Matthews Correlation Coefficient (0.9663)	Their suggested scheme's greater computational complexity, which represents the trade-off between time cost and more precise DDoS attack detection, is a significant disadvantage.
Galeano-Brajones *et al.*, 2020	Proposed an entropy-based to detect and mitigate DoS and DDoS attacks in IoT scenarios using a stateful SDN data plane.	An Entropy-Based Algorithms	Stateful Software Defined Networking (SDN) data plane.	1. Detection Rate 2. False Positive Rate 3. Mean (ms) 4. Standard Deviation (ms)	

Received: 03-01-2025 / Accepted: 26-01-2025 /Published: 31-03-2025

Huraj and Šimon	Described a case study of a DDoS attack on IoT devices in a smart home environment and the impact of the attack on the communication and control of IoT sensors from the perspective of a user using smart home services	-			
(Nazih *et al.*, 2020	developed a method to improve retrieved features from SIP communications by employing token embedding and formulated the detection of DDoS attacks as a classification problem.	DL		1. Accuracy 2. F1 Score	RNN is not very effective for parallel processing because of recurrent connections. In their final scenario, RNN-LSTM fared better than other classifiers but was unable to identify low-rate attacks, such as L and VL attacks. When employing character-based features, RNN-GRU and l1-SVM seem to have struggled to handle lengthy sequences, as evidenced by their notably reduced detection rates.
Danta Silva *et al.*, 2020	A comprehensive review of the state-of-the-art DDoS attack mitigation strategies featured by SDN technologies in IoT scenarios.	Hybrid			
Hsu *et al.*, 2021	Proposed a kernel module-based mechanism to establish a new TCP/IP connection by the host that is under attack (the clients did not know the location of the host at first). Also designed a novel component, Client Connection Handler (CCH), to make another three-way handshake to establish a new connection for the destination transferring.	-		1. Convergence Time 2. Path Reconstruction Cost	Previous work lacked this novel mechanism and usually required more resources than their system, were often complicated, and either had huge hardware resources or a few fragile servers to support the system.
Ahmad *et al.*, 2021	Examined techniques for improving DoS anomaly detection along with power reservation in Wireless Sensor Networks (WSNs) to balance them.	ML	CICDDoS2019 and BoT-IoT datasets	Accuracy	

Received: 03-01-2025 / Accepted: 26-01-2025 /Published: 31-03-2025

Wang *et al,*2022	Proposed a transformer-based DDosTC model based on the latest DDoS attack dataset, and also designed a hybrid neural network DDosTC structure to detect distributed denial-of-service (DDoS) attacks on SDN.	DL	CICDDoS2019	1. Accuracy 2. Recall 3. F1 score 4. The area under the ROC curve	This model was not optimal in terms of recall rate
Ko *et al.*, 2021	Presented an Intelligent Attack Mitigation (IAM) system, which takes an ensemble approach by employing Recurrent Autonomous Autoencoders (RAA) as basic learners with a majority voting scheme and also proposed Estimated Evaluation Metrics (EEM) to evaluate the performance of unsupervised models. A novel Comparison-Max Random Walk algorithm was used to determine the Reference Target (RT)	EL	Not clearly stated	1. Estimated Accuracy (EA) 2. Estimated Recall (ER)	While the average Recall of the system was over 0.98, the amount of computing power and training time required could be high. Even though adjusting the N value for the Top-N, Max-N, and EnsembleN can deal with the performance and resources trade-off.
Mishra *et al.*, 2021	Proposed a novel solution; identification-pattern mechanism using a threshold scheme for detecting volume-based DDoS attacks.	Identification-pattern mechanism	Not clearly stated		
Maranhão *et al.*, 2021	Suggested a multilayer perceptron (MLP) architecture that is noise-robust and is trained using damaged data to identify DDoS attacks.	DL	(1) NSL-KDD, and (2) CIC-IDS2017	1. Accuracy (98.95%), 2. Detection Rate (98.31%), 3. False Alarm Rate (0.015%)	An important drawback of their proposed scheme is its higher computational complexity, which reflects the trade-off between the more accurate DDoS attack detection and the time cost.
Chen and Lai, 2021	Proposed a novel approach called Flow Differentiation Detector (FDD), to detect Hybrid DDoS attacks.	-		1. Accuracy, 2. False-Positive Rate (FPR), 3. False-Negative Rate (FNR	

Roy *et al.*, 2022	Proposed a network architecture based on the capability to address the threat of DDoS attacks.	-	Self-generated	1. Computational complexity 2. Communication overhead 3. Storage constraints.	
Li *et al.*, 2022	Proposed a two-stage intelligent detection DDoS attack mechanism that combines similarity-based prior knowledge and CNN-based attention to detect various DDoS attack types	DL	Self-generated	1. Detection Rate. 2. Accuracy 3. Precision 4. Recall	
Wang and Li(2021)	Designed and implemented an online attack detection and mitigation Software Defined Networking (SDN) defence system.	DL	CICIDS-2017 and InSDN	1. Accuracy 2. Precision 3. Recall 4. F1-Score	The disadvantage is that the cost of labelling the required data is very high.
Saha *et al.*, 2022	used the three primary categories of AI methods feature (EnFS) set to conduct a thorough examination of a significant number of FS approaches.	ML	UNSW-NB15 dataset		NSL-KDD, CICIDS, and other well-known cyberattack datasets ought to be used to verify the proposed model. They can grid search the hyper-parameters for the feature selection techniques and use dynamic selection to optimize feature selection and achieve better results.
Najafimehr *et al.*, 2022	suggested a hybrid machine-learning approach that combines supervised and unsupervised algorithms to detect hitherto unheard-of DDoS attacks.	ML	CICIDS2017 and CICDDoS2019	1. Accuracy 2. Precision 3. Recall 4. False Positive Rate 5. Positive likelihood ratio	
Mishra *et al.*,	Presented a novel approach, perplexed-based classification with feature selection, to extract actionable characteristics and differentiate attacks from data.	ML	NSLKDD+	1. Accuracy 2. Recall 3. Specificity	

Received: 03-01-2025 / Accepted: 26-01-2025 /Published: 31-03-2025

Amma, 2022	suggested a Tuned Vector Convolutional Deep Neural Network (TVCDNN) by employing binary and real Cumulative Incarnation (CuI) to optimize the deep neural network's parameters and structure.	DL	KDD Cup and NSL KDD	1. Accuracy 2. Precision 3. Error rate	
Patil, 2022	Proposed a novel Spark Streaming and Kafka-based distributed classification system, named SSK-DDoS, for classifying different types of DDoS attacks and legitimate network flows.	Spark Streaming and Kafka-based distributed classification.	CICDDoS2019	1. Accuracy 2. Recall 3. Precision 4. F1 score	
Zhang *et al.*, 2022	A DDoS attack was chosen as the primary method of attacking the critical nodes in Low Earth orbit satellite constellation networks (LSCNs) after a space-time graph model was constructed to locate the nodes.	Space-Time Graph Model			
Yin *et al.*, 2022	Proposed a trusted multi-domain DDoS detection method based on federated learning.			1. Accuracy 2. Recall 3. Precision	
Ibrahim *et al.*, 2022	Proposed an Ethereum blockchain model to detect and prevent DDoS attacks against IoT systems.	Blockchain Approach		Time complexity	
Guo *et al.*, 2022	suggested a deep learning technique based on topological and flow features (GLD-Net), which uses Graph Attention Networks (GAT) to mine correlations between non-Euclidean features in order to merge topological and flow information. GLD-Net simultaneously extracts topological and flow features from time-series flow data.	DL	KDD2009 and CIC-IDS2017	1. Accuracy 2. Recall 3. Precision 4. F1 Score	• Because GAT's neighbourhood computation efficiency is low, it cannot handle real-time training, and it is unable to identify unknown traffic, including 0-day attacks.

Received: 03-01-2025 / Accepted: 26-01-2025 /Published: 31-03-2025

Prasad and Chandra, 2022	Proposed a Voting-Based Multimode Framework to Combat Volumetric DDoS (VMFCVD) attacks.	ML	CICIDS2017, CSE-CIC-IDS2018, CICDDoS2019, DoHBrw2020, NBaIoT2018, UNSW2018 BoTIoT, and UNSW NB15	1. Accuracy 2. Dimensional Reduction	
Shah *et al.*, 2022	conducted a thorough analysis of several Blockchain-based ways to lessen DDoS attacks on the Internet of Things.	Blockchain-Based Solutions	UNSW-NB15	1. Accuracy 2. F1 Score 3. Precision 4. Recall 5. Time (s)	This study restricts its analysis to security concerns on the Internet of Things network layer and does not categorize current solutions that deal with security concerns, pertaining to the application and sensor levels.
Almaraz-Rivera *et al.*, 2022	Resolved the original dataset's class imbalance issue (by excluding synthetic data and class weights), which resulted in the development of a revolutionary IDS based on AI models that target DDoS and DoS attacks.	ML and DL	Bot-IoT dataset		Directly detecting anomalies on sensor nodes—which have little processing power and little memory—is challenging in heterogeneous sensor networks, such as the Bot-IoT testbed.
Aslam *et al.*, 2022	Proposed an Adaptive Machine Learning based SDN-enabled Distributed Denial-of-Services attacks Detection and Mitigation (AMLSDM) framework.	ML		1. Accuracy 2. F1 Score 3. Precision 4. Recall	
AlArnaout *et al.*, 2023	The Robust Attack Path Tracing (RAPT) technique was proposed as an effective solution to the SYN-Flood DDoS attacks.	Robust Attack Path Tracing (RAPT) algorithm.		1. Detection time: 2. Number of SYN packets destined to the victim 3. Tracing Time 4. Total Processing Time 5. Convergence Time	Low computation and message overhead, efficient detection, and tracing time, and converges in near optimal time. The results are validated using extensive simulation runs.

Received: 03-01-2025 / Accepted: 26-01-2025 /Published: 31-03-2025

Aswad *et al.*, 2023	Proposed the CNN-BiLSTM model for DDoS detection, and the results show that the CNN-BiLSTM model surpasses other tested models.	DL	CICIDS2017	1. Accuracy 2. Precision 3. Recall 4. F-measure.	
Dash *et al.*, 2024	Proposed two approaches, one utilizing Principal Component Analysis (PCA) and another without PCA, to compare their performance. Robust scaling and encoding techniques are applied as preprocessing steps.	ML	NSL-KDD Dataset	1. Accuracy 2. Precision 3. Recall 4. F1 score	
Hossain & Islam, 2024	Suggested a better method for identifying DDoS attacks that combines an ensemble-based classifier with a hybrid feature selection strategy.	ML	CIC-DDoS2019	1. Accuracy 2. recall 3. precision 4. f1-score, 5. false positive rate	
Ouhssini *et al.*, 2024	Proposed an advanced DeepDefend framework for real-time detection and prevention of DDoS attacks in cloud environments.	ML & DL	CIDDS-001	1. Accuracy 2. recall 3. precision 4. f1-score,	DeepDefend framework was not implemented in real-world cloud settings to test its adaptability and resilience under varied and unpredictable conditions.

Received: 03-01-2025 / Accepted: 26-01-2025 /Published: 31-03-2025

Conclusion

A thorough literature evaluation on DDoS attack detection was presented in this study. Articles from 2016 to 2024 were the only ones taken into account. Researchers' various approaches, methods, and strategies were examined and documented. The study ended with a summary of all the findings from the previous review, which may be used as a guide by anyone interested in learning more about the various facets of the DDoS assault area. It is also expected to spur research efforts toward the development of comprehensive solutions that give equal weight to the technological and standardized components.

Future work

This study summarized some of the future work from the papers reviewed for future researchers in the domain of DDoS attack detection. They are as follows:

1. To be extended to generalize other types of (D)DoS attacks and also to include different statistical-based metrics that could help in the detection process.
2. To experiment with more complex cases outside Mininet and even make use of other proposals in the stateful SDN literature.
3. It is necessary to use intelligent methods, such as machine learning approaches that enable the algorithm parameters—namely, θ and window size to be self-configured.
4. Working on a (D)DoS attack detector as a Network Function (NF) that could be deployed in the network as a standalone module. To give flexibility to the detection process and would be in line with other 5G technology pillars such as NFV.
5. Based on the particular resource constraints of the IoT infrastructure, appropriate Key Performance Indicators (KPIs) are needed to provide optimal assessment measuring.
6. Since DDOS attacks have a significant impact on IP source address, acknowledgement, reset, finished, TCP/IP, ICMP segments, and ports, future studies may employ an optimized approach to evaluate these parameters more effectively.
7. Self-generated datasets ought to be investigated as well.
8. By examining how other IoT protocols behave under different DDoS attacks in such real-world circumstances, the conducted pilot testing can be expanded in the future and used as basic research for more studies.
9. To expand their research into Artificial Intelligence (AI) technology and investigate the ideal moderator K configuration in their suggested FDD. To confirm that the artificial intelligence model has been thoroughly trained to guarantee robustness and efficacy, they will also investigate the feasibility of creating an AI robustness test technique.
10. Blockchain can be employed for data analytics applications and cyber-attacks in communicating data, such as data compressing algorithms for transactive energy management framework and for healthcare security analytics.
11. Tracing packet authentication, in which a hacker might insert fake packets that could implicate trustworthy hosts. Furthermore, the approach calls for changes to the Autonomous Systems (AS) routers' operation.

References

Abu Bakar, R., Huang, X., Javed, M. S., Hussain, S., & Majeed, M. F. (2023). An Intelligent Agent-Based Detection System for DDoS Attacks Using Automatic Feature Extraction and Selection. *Sensors*, *23*(6). https://doi.org/10.3390/s23063333

Ahmad, R., Wazirali, R., Bsoul, Q., Abu-Ain, T., & Abu-Ain, W. (2021). Feature-selection and mutual-clustering approaches to improve dos detection and maintain wsns' lifetime. *Sensors*, *21*(14). https://doi.org/10.3390/s21144821

AlArnaout, Z., Mostafa, N., Alabed, S., Aly, W. H. F., & Shdefat, A. (2023). RAPT: A Robust Attack Path Tracing Algorithm to Mitigate SYN-Flood DDoS Cyberattacks. *Sensors*, *23*(1). https://doi.org/10.3390/s23010102

Ali, T. E., Chong, Y. W., & Manickam, S. (2023). Comparison of ML/DL Approaches for Detecting DDoS Attacks in SDN. *Applied Sciences (Switzerland)*, *13*(5). https://doi.org/10.3390/app13053033

Almaraz-Rivera, J. G., Perez-Diaz, J. A., & Cantoral-Ceballos, J. A. (2022). Transport and Application Layer DDoS Attacks Detection to IoT Devices by Using Machine Learning and Deep Learning Models. *Sensors*, *22*(9). https://doi.org/10.3390/s22093367

Amma, N. G. B. (2022). Optimization of vector convolutional deep neural network using binary real cumulative incarnation for detection of distributed denial of service attacks. *Neural Computing and Applications*, *34*(4), 2869–2882. https://doi.org/10.1007/s00521-021-06565-8

Aslam, M., Ye, D., Tariq, A., Asad, M., Hanif, M., Ndzi, D., Chelloug, S. A., Elaziz, M. A., Al-Qaness, M. A. A.,

& Jilani, S. F. (2022). Adaptive Machine Learning Based Distributed Denial-of-Services Attacks Detection and Mitigation System for SDN-Enabled IoT†. *Sensors*, *22*(7). https://doi.org/10.3390/s22072697

Chen, Y. H., Lai, Y. C., & Zhou, K. Z. (2021). Identifying hybrid ddos attacks in deterministic machine-to-machine networks on a per-deterministic-flow basis. *Micromachines*, *12*(9). https://doi.org/10.3390/mi12091019

Dantas Silva, F. S., Silva, E., Neto, E. P., Lemos, M., Venancio Neto, A. J., & Esposito, F. (2020). A taxonomy of DDoS attack mitigation approaches featured by SDN technologies in IoT scenarios. In *Sensors (Switzerland)* (Vol. 20, Issue 11, pp. 1–28). https://doi.org/10.3390/s20113078

Galeano-Brajones, J., Carmona-Murillo, J., Valenzuela-Valdés, J. F., & Luna-Valero, F. (2020). Detection and mitigation of DoS and DDoS attacks in iot-based stateful SDN: An experimental approach. *Sensors (Switzerland)*, *20*(3), 1–18. https://doi.org/10.3390/s20030816

Gondim, J. J. C., de Oliveira Albuquerque, R., Nascimento, A. C. A., Villalba, L. J. G., & Kim, T. H. (2016). A methodological approach for assessing amplified reflection distributed denial of service on the internet of things. *Sensors (Switzerland)*, *16*(11), 1–31. https://doi.org/10.3390/s16111855

Guo, W., Qiu, H., Liu, Z., Zhu, J., & Wang, Q. (2022). GLD-Net: Deep Learning to Detect DDoS Attack via Topological and Traffic Feature Fusion. *Computational Intelligence and Neuroscience*, *2022*. https://doi.org/10.1155/2022/4611331

Hossain, M. A., & Islam, M. S. (2024). Enhancing DDoS attack detection with hybrid feature selection and ensemble-based classifier: A promising solution for robust cybersecurity. *Measurement: Sensors*, *32*(February), 101037. https://doi.org/10.1016/j.measen.2024.101037

Ko, I., Chambers, D., & Barrett, E. (2021). Recurrent autonomous autoencoder for intelligent DDoS attack mitigation within the ISP domain. *International Journal of Machine Learning and Cybernetics*, *12*(11), 3145–3167. https://doi.org/10.1007/s13042-021-01306-8

Li, M. (2022). *DDoS Behavior*.

Maranhão, J. P. A., da Costa, J. P. C. L., de Freitas, E. P., Javidi, E., & de Sousa Júnior, R. T. (2020). Error-robust distributed denial of service attack detection based on an average common feature extraction technique. *Sensors (Switzerland)*, *20*(20), 1–21. https://doi.org/10.3390/s20205845

Mebawondu, J. O., Alowolodu, O. D., Mebawondu, J. O., & Adetunmbi, A. O. (2020). Network intrusion detection system using supervised learning paradigm. *Scientific African*, *9*. https://doi.org/10.1016/j.sciaf.2020.e00497

Mishra, N., Pandya, S., Patel, C., Cholli, N., Modi, K., Shah, P., Chopade, M., Patel, S., & Kotecha, K. (2021). Memcached: An experimental study of ddos attacks for the wellbeing of iot applications. *Sensors*, *21*(23), 1–22. https://doi.org/10.3390/s21238071

Mishra, N., Singh, R. K., & Yadav, S. K. (2022). Detection of DDoS Vulnerability in Cloud Computing Using the Perplexed Bayes Classifier. *Computational Intelligence and Neuroscience*, *2022*. https://doi.org/10.1155/2022/9151847

Najafimehr, M., Zarifzadeh, S., & Mostafavi, S. (2022). A hybrid machine learning approach for detecting unprecedented DDoS attacks. *The Journal of Supercomputing*, *78*(6), 8106–8136. https://doi.org/10.1007/s11227-021-04253-x

Nazih, W., Hifny, Y., Elkilani, W. S., Dhahri, H., & Abdelkader, T. (2020). Countering ddos attacks in sip based voip networks using recurrent neural networks. *Sensors (Switzerland)*, *20*(20), 1–15. https://doi.org/10.3390/s20205875

Patil, N. V. (2022). SSK-DDoS : distributed stream processing framework based classification system for DDoS attacks. *Cluster Computing*, *25*(2), 1355–1372. https://doi.org/10.1007/s10586-022-03538-x

Roy, S., Singh, J., & Mathew, J. (2022). Design and analysis of DDoS mitigating network architecture. *International Journal of Information Security*. https://doi.org/10.1007/s10207-022-00635-1

Saha, S., Priyoti, A. T., Sharma, A., & Haque, A. (2022). Towards an Optimized Ensemble Feature Selection for DDoS Detection Using Both Supervised and Unsupervised Method †. *Sensors*, *22*(23). https://doi.org/10.3390/s22239144

Shaaban, A. R. (2019). DDoS attack detection and classification via Convolutional Neural Network (CNN). *2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS)*, *November 2020*, 233–238. https://doi.org/10.1109/ICICIS46948.2019.9014826

Shah, Z., Ullah, I., Li, H., Levula, A., & Khurshid, K. (2022). Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey. *Sensors*, *22*(3). https://doi.org/10.3390/s22031094

Shieh, C. S., Nguyen, T. T., & Horng, M. F. (2023). Detection of Unknown DDoS Attack Using Convolutional Neural Networks Featuring Geometrical Metric. *Mathematics*, *11*(9). https://doi.org/10.3390/math11092145

Wang, H., & Li, W. (2021). DDosTC: A transformer-based network attack detection hybrid mechanism in SDN.

Sensors, *21*(15). https://doi.org/10.3390/s21155047

Wang, J., Liu, Y., & Feng, H. (2022). IFACNN: Efficient DDoS attack detection based on improved firefly algorithm to optimize convolutional neural networks. *Mathematical Biosciences and Engineering*, *19*(2), 1280–1303. https://doi.org/10.3934/mbe.2022059

Yin, Z., Li, K., & Bi, H. (2022). Trusted Multi-Domain DDoS Detection Based on Federated Learning. *Sensors*, *22*(20). https://doi.org/10.3390/s22207753

Zhang, Y., Wang, Y., Hu, Y., Lin, Z., Zhai, Y., Wang, L., Zhao, Q., Wen, K., & Kang, L. (2022). Security Performance Analysis of LEO Satellite Constellation Networks under DDoS Attack. *Sensors*, *22*(19). https://doi.org/10.3390/s22197286

Received: 03-01-2025 / Accepted: 26-01-2025 /Published: 31-03-2025