RESEARCH ARTICLE

INTERNATIONAL RESEARCH JOURNAL OF
MULTIDISCIPLINARY TECHNOVATION

Asian Research Association

DOI: 10.54392/irjmt25411

Detection of Distributed Denial of Service Attacks Based on Deep Learning Approaches: A Survey, Taxonomy, and Challenges

G. Vidhya [a, *], M. Jagadheeswari [a]

[a] Department of Computer Science, Kongunadu Arts and Science College, Coimbatore, Tamil Nadu, India

* Corresponding Author Email: vidhyaphd.2022@gmail.com

DOI: https://doi.org/10.54392/irjmt25411

Received: 15-10-2024; Revised: 12-06-2025; Accepted: 27-06-2025; Published: 18-07-2025

Abstract: DDoS attacks are among the most dangerous dangers to the digital world, according to recent theoretical and empirical research. Over time, DDoS attack mitigation strategies have developed to guarantee security. In the past, several traditional techniques, including heuristics and signatures, were employed to detect DDoS attacks encoded with different characteristics. The advanced obfuscation strategies used by new generations of DDoS attackers were too formidable for detection tools designed for traditional DDoS attacks. Since DL-based systems beat traditional DDoS attack detection techniques in discovering novel DDoS attack variations, Deep Learning (DL) is being employed more and more in DDoS attacks. Additionally, DL-based methods offer quick DDoS attack prediction together with superior detection rates and DDoS attack analysis. Thus, this work is interested in examining recently suggested DL-based DDoS attack detection systems and their development. It provides a comprehensive examination of the most current advances in DL-based detection methods. This survey's main objective is to give readers a thorough grasp of the applications of DL for detection. The outcome of this review discusses various DL methods, their strengths and weaknesses, datasets, challenges of recent research work, and future enhancements of present works.

Keywords: DDoS Attack Detection, Network Security, Computer Network, Deep Learning

1. Introduction

Computer networks are important for enabling collaboration, resource sharing, and communication between people and devices. Computer networks play a wide range of roles in contemporary computing and communication. Numerous industries, including banking, e-governments, business, education, and healthcare, are prime examples of our heavy reliance on the Internet [1]. A DDoS attack is a deliberate attempt to disrupt normal network, server, or service traffic by overloading the target's infrastructure or that of its surroundings with traffic. Usually, these attacks involve flooding the targeted system with pointless traffic until it stops responding [2]. It is more challenging to protect against due to the usage of several compromised devices to overwhelm the target with fake traffic. The main goal is to disrupt the normal operation of a network, service, or website. DDoS attacks have been carried out by attackers using a range of techniques [3].

With advancements in detection and mitigation techniques, new attack types have emerged. These attacks can be categorized in a variety of ways, depending on factors like attack frequency and mechanism. Malicious traffic is sent to the target slowly in a low-rate DDoS attack [4]. This attack makes use of a weakness in TCP's congestion management system. Malicious communication is transmitted either steadily at a low pace, referred to as a "continuous attack," or often during brief intervals, known as a "pulsing attack. "Six If a DDoS attack makes up 15% to 25% of the target's background network traffic, or if its rate is less than 1000 bps, it is deemed low-rate. On the other hand, high-rate attacks entail the attacker sending a large number of packets to the target in an attempt to jeopardize the availability of its services. Because of the massive amount of malicious traffic they create, these operations are frequently referred to as volumetric or flooding attacks [5]. The Figure 1 shows the framework of DDoS attack.

Network topology-based DDoS detection techniques are divided into three main categories: source, destination, and network-based techniques. The destination-based methods are deployed within the attack's destination network near the target. The source-based methods locate and function from the attack's point of origination near the attacker. Conversely, network-based techniques operate within the Internet's infrastructure, sitting in between the victim and the attacker [6].

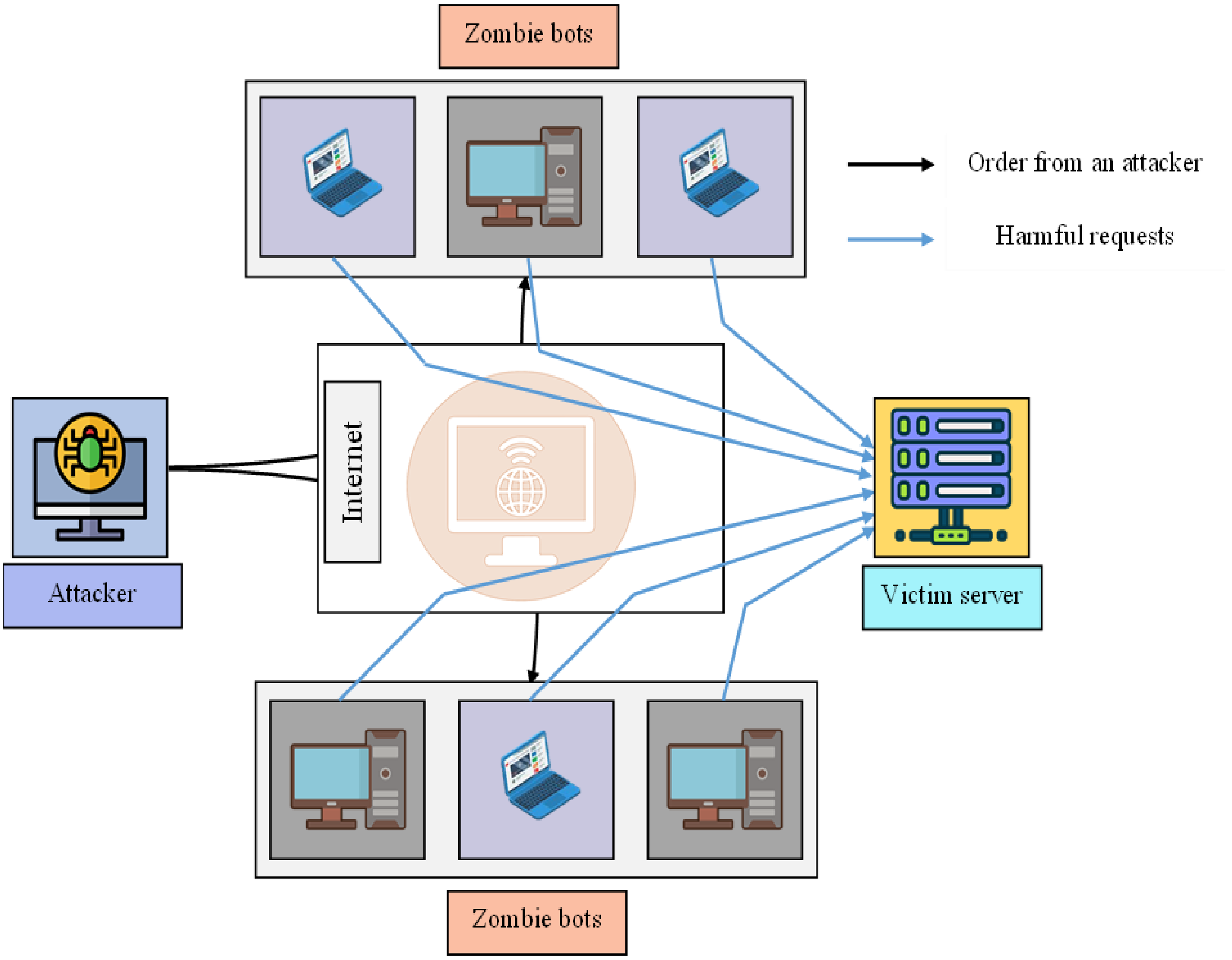

Figure 1. Framework of DDoS attack

There are several methods available to prevent, detect, and reduce DDoS attacks. There are two main approaches to detection methods: signature-based and anomaly detection methods. Signature-based techniques are ineffective against new or zero-day attacks and can only identify known attacks for which the signature is already known. However, by recognizing the aberrant circumstances brought on by the attack, the anomaly detection approach can identify new and unknown attacks [7]. In the anomaly detection strategy, statistical techniques like entropy analysis and DL techniques are commonly used. Although protection systems are becoming more effective, attack tactics are also becoming more sophisticated, leaving a substantial research gap in countering DDoS attacks. As a result, new types of DDoS attacks can appear that are harder for current detection techniques to stop. For example, the largest DDoS attack to date is said to have occurred on GitHub in 2018. Millions of engineers use the network to write and discuss code, and the hack increased traffic to it dramatically. In 2020, New Zealand's Exchange was the subject of a volumetric DDoS attack that knocked it offline for a few days. A website that was used to plan pro-democracy demonstrations in Hong Kong was the subject of China's Great Cannon DDoS operation in 2019, which caused traffic congestion on the website.

According to the DDoS recent threat report 2023- Q4 [8], network-layer DDoS attacks have surged by 117% over the year while DDoS activity targeting websites related to public relations, shipping, and retail has increased overall during and around Black Friday and the holiday season. Targeting traffic from DDoS attacks Despite the impending general election and rumored tensions with China, Taiwan saw a 3,370% increase in GDP compared to the previous year. As Israel and Hamas continued their military conflict, the percentage of DDoS attack traffic directed at Israeli websites increased by 27% and the percentage of DDoS attack traffic directed at Palestinian websites increased by 1,126% over the same period. Related to the previous year, the 28th United Nations Climate Change Conference saw a startling 61,839% increase in DDoS attack traffic directed at Environmental Services websites. Nearly 57,116 DDoS attacks were reported, per Kaspersky's quarterly report. According to Cloudflare, ransom DDoS attacks increased by 67% in 2022. Globally, attacks between 100 Gbps and 400 Gbps increased by 776% year over year between 2018 and 2019, and by 2023, there will be twice as many DDoS attacks (2018) (7.9 million versus 15.4 million). Radware's 2024 Global Threat Analysis Report [8] states that DDoS attacks are moving and that hackers are adapting their strategies to thwart mitigation measures: Following a 99% rise in 2022, the number of DDoS attacks per customer improved by 94% in 2023. In 2023, there were 48% more attacks than in 2022. In 2023, a 150% rise in main attacks peaking above 500 Mbps, a 177% increase in attacks topping between 100 and 250 Mbps, and a 63% increase in attacks with traffic below 1 GB. From 106 attacks per month or 3.48 attacks per day in 2021 to an average of 49 attacks per day in 2023, the number of attacks per client has improved.

DDoS attacks are frequently employed in social movements by hacktivists, government-affiliated organizations, and hackers alike. DDoS attacks are a useful tool for drawing attention to a particular cause or group among the public [9]. Threat actor groups Armada Collective and Fancy Bear both threatened to use DDoS attacks against other companies in 2020 unless a Bitcoin ransom was paid [10, 11]. The efficacy of DL-based detection techniques for actual DDoS attacks is a crucial research topic. Traditional techniques including decision trees (DT), support vector machines (SVMs), and k-nearest neighbors (KNNs) were frequently employed in the early stages (2014-2017) of DDoS attack detection. These techniques, however, necessitated a great deal of feature engineering. Later (2017-present), DL, which offers automated feature extraction, real-time investigation, and adaptive learning, has developed as a key tool in the detection of DDoS attacks. DL models can distinguish intricate patterns in network data and detect threats more precisely than typical ML techniques, which depend on manual feature engineering. However, the developed DL methods are very accurate in prepared datasets and simulated testbeds, their effectiveness may be hampered by the differences between lab testbed conditions and real-world situations. The literature that is now available still has several shortcomings despite the many studies that have been done on DDoS attacks and associated detection techniques:

- Numerous research endeavors have concentrated on detecting DDoS attacks inside particular domains, so limiting their extent and efficacy.
- Some research has overlooked the importance of providing significant datasets and their attributes that can be used to compare detection algorithms across different investigations.
- Several research has not concentrated on this contemporary strategy due to the growing use of DL techniques in the DDoS detection space.
- The ability of DL-based detection techniques to be systematically categorized makes it difficult for researchers to compare and assess various strategies.
- Some research has not included illustrations of the most prevalent kinds of DDoS attacks, which makes it challenging for readers to comprehend the strategies used by attackers in these attacks.

This work attempts to thoroughly examine DDoS attack detection methods and an emphasis on DL-based strategies, to overcome these shortcomings. We offer a thorough taxonomy of these techniques, allowing scholars to methodically categorize and assess various methodologies. Furthermore, we present noteworthy datasets together with their salient features, which will aid in the cross-validation of detection techniques. To aid readers in understanding the strategies used by attackers in these attacks, we present and illustrate the most common kinds of DDoS attacks. Because our study condenses DL-based DDoS detection techniques into a single publication, it offers a substantial theoretical contribution that will aid scholars in understanding the state of the field at this time. Additionally, we offer tables that allow for a useful comparison of the outcomes from the various DL techniques used in DDoS detection. We assist researchers in understanding the limitations of the current methodologies by talking about the flaws of the offered methods and the ongoing difficulties in DDoS detection. Lastly, to fill in the gaps and overcome the shortcomings in the current DDoS detection literature, we provide several recommendations for future research. Figure 2 shows the steps of DDoS attack detection framework.

1.1 Types of DDoS Attacks

The goal of a DDoS attack is to burden a target's server, network, or application with too much traffic, disrupting or stopping it from functioning. Based on their attack method and the network layer they target, DDoS attacks can be separated into three groups such as application layer, protocol, and volumetric attacks. Figure 3 shows the types DDoS attacks. Application layer is the attack targets layer 7, where webpages are built in response to requests from end users, under the OSI model. The process of producing a request by a client is not burdensome, and it may effortlessly generate several requests to the server. Conversely, the server must work very hard to fulfill requests as it must generate all of the pages, do any necessary calculations, and load the database's contents by the request [12]. Three types of major attacks come under the application layer such as HTTP Flood, slowloris, and zero-days attack. *HTTP*: It overloads web servers with a lot of HTTP requests to attack them. Attacks aim to eat up server resources, which causes the website to develop sluggish or broken for authorized users. *Slowloris:* Web servers are the target of the low-and-slow Slowloris DDoS attack and it preserves connections open for as long as possible.

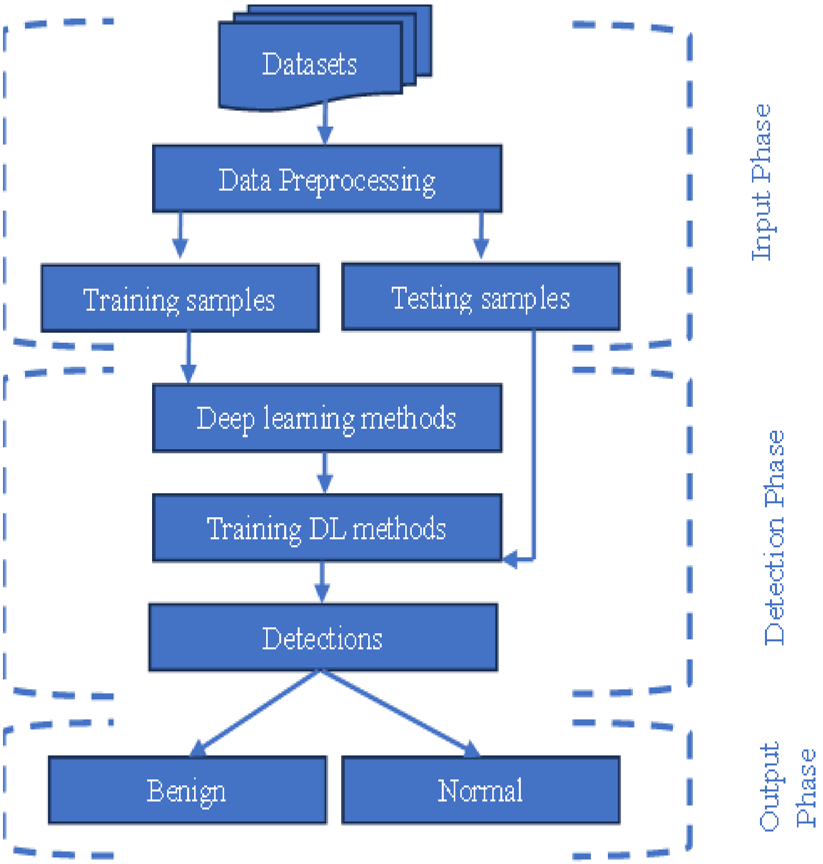

Figure 2. Framework for DDoS attack detection using DL methods

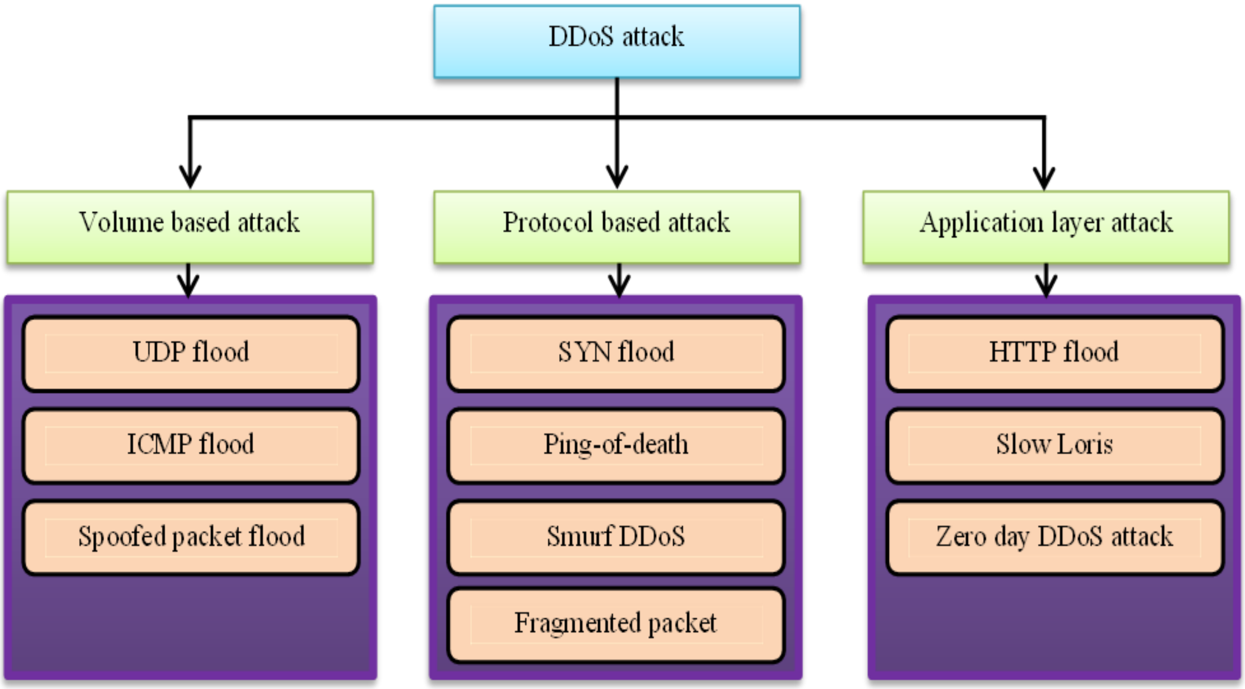

Figure 3. Types of attacks

It doesn't need a lot of bandwidth as traditional volumetric attacks do; instead, it slowly reduces the server's resources until it is unable to process valid requirements [13]. *Zero-days attack:* it is a cyberattack that exploits an earlier unidentified vulnerability in software and hardware before the developer has had a chance to develop a patch. Since the susceptibility is not openly identified, there are no defenses accessible at the time of the attack, making it enormously dangerous [14]. *Protocol attacks is called the* state-exhaustion attacks and layers 3 and 4 of the protocol stacks are the main targets of these attacks. Resources are used up by these kinds of attacks. SYN flood, ping of death, smurf attack, and fragment packet are examples of protocol attacks. An *SYN Flood* attack exploits the TCP handshake process to overload a target's server with half-open connections. This prevents legitimate users from establishing connections, leading to service disruption. *Ping of Death* takes advantage of how some systems respond to large ICMP messages. An attacker may cause vulnerable systems to crash, freeze, or reboot by sending ping packets that are distorted or excessively large. *Smurf Attack* uses ICMP requests to flood a network by tricking it into responding to the target [15]. The *Volumetric attack's* goal is to impede user access to the network by filling it with traffic and overloading it through botnets or amplification. They may be easily produced by sending a large volume of traffic to the intended server. *UDP Flood* is sends a huge amount of UDP packets to random ports, killing bandwidth and system resources. ICMP (Ping) Flood is an overload the target with ICMP Echo Request (ping) packets [16]. *SYN Flood* exploits the TCP handshake by sending numerous SYN requests but never completing the handshake. A DDoS attack known as a *"spoof packet flood"* occurs when an attacker conveys a large volume of packets with spoofed source IP addresses. This causes the target's network to become overloaded, which results in DoS and makes it challenging to identify the attacker.

1.2 Searching strategy

Forming an appropriate search strategy is the first step in starting a systematic survey. Any research project must begin with a well-thought-out search strategy. To find the relevant literature, a suitable selection of databases has been chosen. The search was conducted in two stages for the current study, from 2018 to 2023. Four digital libraries were used in Phase 1 of the search: the ACM Digital Library, IEEE Explore, Springer, and Science Direct; Phase 2 of the search also included the academic search engine Google Scholar. The inclusion of Google Scholar has made it possible to avoid overlooking any pertinent material. Pilot research was also conducted to improve the search string. The best articles have been chosen from a list of previously gathered.

Articles that were stored in the database throughout the trial project. One such search phrase that was applied sparingly to several digital libraries is: "DDoS attack detection + Computer networks + Deep learning techniques". We primarily composed more than 140 research papers related to DDoS attack detection. Out of these, 27 papers were omitted as they were survey or review articles, and another 66 papers were removed for focusing primarily on traditional machine learning methods rather than deep learning approaches. After this filtering process, a total of 47 relevant papers were selected for detailed comparison and analysis. The present paper reviewed the DDoS attack detection system based on DL techniques in this study and offered the following conclusions.

- A thorough analysis of the traditional shortcomings and advantages of DDoS detection methods
- A thorough analysis of the DL methodology for several DDoS attack detection methods
- An analysis of current DDoS attacks on computer networks

2. Deep Learning approaches

The research community has focused especially on using cutting-edge DL models for identifying DDoS traffic as a result of the difficulties mentioned above [17]. DL offers a variety of cutting-edge tools and methods to anticipate cyberattacks quickly and automatically. The quantity of data that traditional DL approaches can manage, however, is one of their main drawbacks. DL, in comparison, can process and identify patterns from enormous amounts of data. DDoS attacks based on DL have shown to be quite successful and efficient in spotting anomalies in network traffic. DL is an artificial intelligence subset of DL that can learn from both supervised and unstructured data [18]. DL is also known as deep neural network (DNN) as it makes use of multilayer networks. Neurons connect the layers, symbolizing the learning processes mathematical. DL algorithms take as input the preprocessed data, perform feature extraction and classification, and as an output, classify the samples as benign or malignant. DL has three types of learning methods such as supervised, semi-supervised, and hybrid methods. Figure 4 represent overview of the DL methods for DDoS attack detection.

2.1 Supervised Method

The capacity of supervised deep learning models to learn from vast quantities of labeled traffic data makes them effective tools for identifying DDoS attacks. Depending on the traffic and attack patterns, different techniques—such as DNNs, CNNs, LSTMs, and hybrid models—offer varying benefits [19]. Real-time performance and generalization to novel attacks, however, are still being researched and improved [20]. Several fully connected layers that learn abstract representations from input information make up a DNN in most cases [21]. CNNs can be utilized for DDoS detection by treating network traffic data as a 2D matrix, even though they are best known for image classification [22]. Analysis of sequential data is a strong suit for RNNs, particularly LSTMs. The time-dependent nature of network traffic makes these models appropriate for identifying trends in traffic flows across time [23]. LSTM and CNN models are sometimes used by academics to extract both temporal and spatial information from traffic data. When dealing with complicated assault detection circumstances, hybrid techniques typically produce superior results. The effectiveness of GRU (Gated Recurrent Unit) at handling sequential data makes it a potent tool for DDoS attack detection. GRU networks can recognize the temporal patterns in network data that DDoS attacks frequently display to differentiate between benign and malevolent activities [24, 25].

- ***Deep neural networks (DNN):*** An artificial neural network having more than two hidden layers between the input and output layers is called a DNN. Feedforward neural networks without feedback links are combined to create the DNN model. The input, output, and hidden layers—which may consist of multiple layers—are the primary parts of the FNN. Each layer comprises units with weights. The activation procedures of the units originating from the preceding layer are made by these units [26].
- ***CNN :*** Convolutional, pooling, flattening, and FC layers make up the CNN. The primary building block of CNN is the convolutional layer. By put on the filters to the input, the convolution layer carries out the mathematical operation and creates a feature map or convoluted feature. The input's height, breadth, and depth are all affected by the filters' moving window application. The convolution layer was followed by the pooling layer. By selecting the highest or least value from a specified region, feature maps' dimensionality can be decreased. The multidimensional data in the pooling layer is converted to a 1-D vector by the flattening layer before being fed into an FC layer. The FC layer classifies the data according to the likelihood of each class label.
- ***Recurrent neural network:*** RNN can anticipate the next word in a phrase by keeping the previous information because it receives the output from the previous phase in addition to the current input. However, the drawbacks of RNN include the inability to analyze lengthy sequential input and gradient disappearing and exploding issues.
- The LSTM is the solution to the RNN problem and made up of various memory cells or blocks. The following cell obtains the two states—the hidden state and the cell state. The three processes known as gates—forget, input, and output gates—allow the memory blocks to choose which information to retain or discard. The information that is no longer required for the LSTM is uninvolved from the cell state by a forget gate. The output gate is in charge of extracting significant information from the current cell state and treating it as an output, whereas the input gate adds the information to the cell state.
- The GRU associations with the input and forget gates into an update gate consolidated the hidden and cell states, and made a few other adjustments.

2.2 Unsupervised Method

Since unsupervised deep learning techniques do not require labeled data—which is frequently hard to come by or might not cover all possible attack variations—they are becoming more and more popular for DDoS attack detection [27]. These techniques concentrate on finding unusual network traffic patterns that differ from typical behavior and may be signs of a DDoS attack. GANs are an effective method for identifying anomalies. When it comes to DDoS detection, the discriminator in a GAN seeks to discern between created traffic and genuine (regular) traffic, while the generator aims to create samples of normal traffic. The discriminator may recognize traffic that deviates from typical patterns once the GAN has been trained [28]. A VAE is a generative method that restructures input data equally to a conventional AE. However, it integrates a probabilistic element, which permits the model to better generalize to unseen traffic patterns and capture uncertainty [29]. SOMs can be used to group associated traffic patterns collected and spot anomalies that don't belong in any of the recognized clusters [30]. A Deep Belief Network (DBN) can also be used to distinguish DDoS attacks by using its capacity to complex data distributions and learn features without supervision. DBNs are a kind of GANs that can learn hierarchical illustrations from data. Network traffic samples can be captured by DBNs, which can then recognize anomalies that are suggestive of DDoS attacks. The use of Restricted Boltzmann Machines (RBMs) for DDoS attack finding makes use of their capacity to extract data from network traffic samples and simulate complicated probability distributions. RBMs, or GANs, are helpful for both supervised classification tasks in DDoS detection [31].

- ***Autoencoder:*** AE is employed for extracting optimal features and dimensionality reduction. An AE consists of input and output layers in addition to the hidden layer and uses back-propagation to train both the encoder and the decoder concurrently. The inputs are converted into low-dimensional by the encoder which extracts the raw features. Then, the decoder uses the low-dimensional notion to collect the original features.

2.3 Hybrid Method

DL models are combined in a hybrid DL approach for DDoS attack detection to increase detection accuracy, robustness, and generalization. The goal of hybrid models is to overcome the drawbacks of utilizing a single model by utilizing the advantages of several approaches. When it comes to detecting DDoS attacks, hybrid approaches can perform better in identifying intricate attack patterns, managing massive network traffic, and reducing false positives and negatives. In addition to integrating various DL architectures like CNNs, RNNs, or autoencoders, these approaches frequently blend supervised and unsupervised learning approaches. Researchers occasionally use CNN and LSTM models in tandem to extract temporal and geographical information from traffic data. Hybrid methods typically perform better in instances involving complicated attack detection [32] such as deep belief networks with GRU (DBN-GRU) [33], DBN-LSTM [34], and AE-MLP [35].

3. DDoS Detection Methods Based on DL

Research has been done on how to identify, prevent, and mitigate DDoS attacks. These surveys range from full narrative studies covering various attack kinds, obstacles, and countermeasure strategies to papers that concentrate on certain parts of the issue. This section offers a review of the literature on these works, evaluating and comparing their contributions to the current survey [36]. The use of DL as an anomaly detection technique to differentiate between benign and hostile traffic is a current research topic with promising results. One approach is to use a physical network as a testbed, where the victim and the attacking computers are present and multiple attacks are conducted in an orchestrated fashion. The produced traffic records can be used to train supervised learning algorithms that distinguish between benign and malicious traffic.

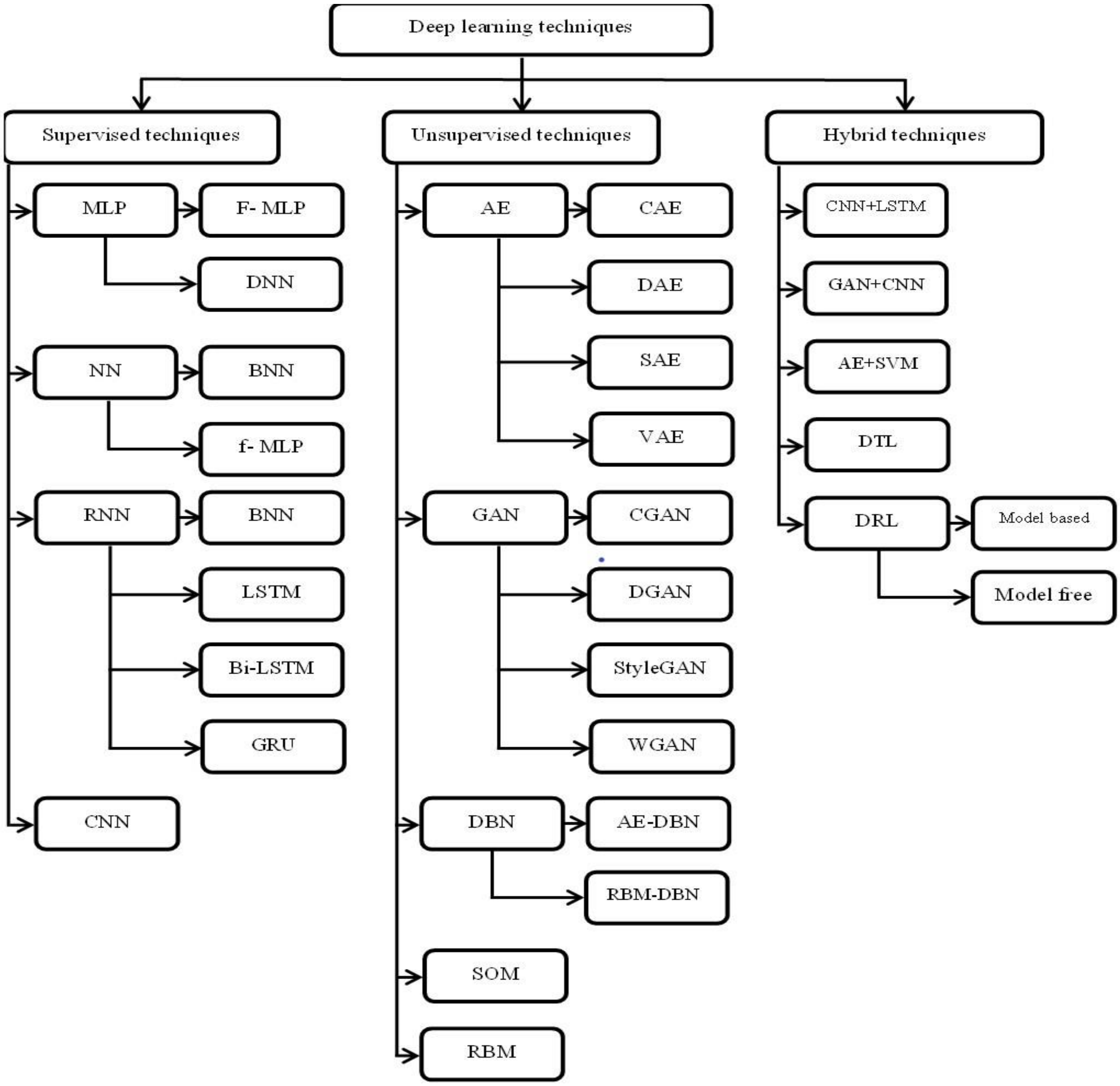

Figure 4. Overview of DL methods

Alternatively, unsupervised learning algorithms that differentiate between valid and malicious communication based on behavioral and feature qualities can be used to cluster real-time incoming traffic. Both approaches depict the traffic packets using crucial parameters like packet size, protocol, and packet interval [37].

Key concepts and findings will be further discussed in this paper in the section that follows. Along with some recent research initiatives, it will also cover all of the categories of DL-based detection algorithms that have been discussed. A tabulation of all the suggested DL-based detection techniques that have been studied is also provided in Table 1.

Mittal *et al*. (2023) [38] created a DL-2P-DDoSADF-based, two-phase DL-based detection system. The autoencoder (AE) was trained using genuine traffic, and the threshold value was adjusted using the reconstruction error (RE). Test data containing attack and legitimate traffic has been used to validate the efficacy of the proposed approach. The first stage is to let projected valid traffic pass across the network using a trained AE model. However, the expected attack traffic proceeds to the second stage to be identified as the specific type of attack that it is.

Ortega-Fernandez *et al.* (2023) [39] suggested an NIDS design with the benefit of not requiring prior information on the network topology. The architecture is built on a deep AE (DAE) trained on network flow data. According to experimental data, in an unsupervised learning context, the suggested model can identify abnormalities brought on by DDoS attacks with a high detection rate and few false alarms. Moreover, following an attack, the DAE model can identify unusual activity in devices that are not compromised. Also illustrated the applicability of the suggested NIDS in an actual industrial plant in the food industry by examining the false positive rate and the feasibility of the data collection, filtering, and preprocessing process for a situation that would occur in almost real-time.

Benmohamed *et al.* (2023) [40] developed a half-AE-Stacked DNN (HAE-SDNN) for DDoS attack detection. HAE enables feature selection from a pre-processed sample, creating a final collection of important features. The DNNs that are loaded together are then trained using these features, and their outputs are joined via the Softmax layer. The outcomes show that the new approach reached a 99.95% accuracy rate. The HAE-SDNN model proceeded better than previous approaches, indicating its supremacy in exactly classifying attacks. Mousa (2023) [41] presented a hybrid DL for DDoS detection and checkpoint network failure tolerance. The findings prove that the proposed method performs remarkably well, attaining 99.99% and 99.92% for both training and validation.

Benmohamed *et al.* (2024) [42] propose a novel DDoS attack detection method using Encoder-Stacked DNN (E-SDNN) for accurately detecting DDoS attacks. The suggested encoder picks relevant features from a pre-processed dataset to permit correct attack detection. The experimental results illustrate how much better the E-SDNN method is than the most cutting-edge methods. Batchu *et al.* (2023) [43] established a two-stage hybrid method for detecting DDoS. The Deep Sparse AE (DSAE) first retrieves the features using Elastic Net regularization. Moreover, numerous learning methods are adjusted to classify attacks according to the feature sets that are mined.

Balasubramaniam *et al.* (2023) [44] suggested a Gradient hybrid leader optimization (GHLBO) for detecting DDoS attacks. It is tuned to train a DSAE that can identify the attack effectively. In this instance, the oversampling procedure augments the data while the deep max-out network (DMN) with an overlap coefficient fuses the features. Additionally, merging the hybrid LBO (HLBO) and gradient descent algorithms yields the suggested GHLBO. The true positive rate (TPR) (0.909), true negative rate (TNR) (0.909), and accuracy (0.917) are three more performance metrics that are used to evaluate this suggested procedure. Akana *et al.* (2023) [45] recommended there DL -based models that are combined in a hybrid technique termed DFNN-SAE-DCGAN for DDoS attack detection. Without the need for human intervention, the Deep Feed-Forward Neural Network (DFNN) and SAE provide an effective way to extract features that find the most relevant feature sets. The DCGAN component uses the restricted and minimized characteristic sets produced by the DFNN-SAE as inputs to classify the attacks into different DDoS attack types to avoid the operational overhead and assumptions associated with processing massive sets of features with distortion and redundant characteristic values. The experimental findings exhibit an F1-score of 98.5%, greater than the performance of other techniques, and a very high and robust accuracy rate.

Kandiero *et al.* (2023) [46] presented the VAE-DNN classifier, a variational AE (VAE) based DNN that does not require feature engineering and can be trained on an unbalanced dataset. A variational AE is a kind of DNN that replicates how the DDoS and benign classes were created by learning the underlying distribution of computer network flows. A VAE model learns how to distinguish between classes because it discovers the distribution of those classes within the sample. Scaling to any size of data is possible with the variational auto-encoder-based classifier. Classifying the flows in the latent representation of network traffic involves applying the decision boundaries of a DNN, QDA, and LDA. Among the three classifiers, the DNN has the best recall and precision. Shrivastav *et al*. (2023) [47] suggested a Double AE model auto-encoder-based method for DDoS detection that combines the strengths of supervised and unsupervised learning. It can differentiate between

DDoS and normal traffic using the reconstructed error values. Additionally, the suggested technique exhibits good generalization across various datasets, indicating its potential for practical use. Hossain *et al.* (2023) [48] developed a new detection technique for attacks based on ensembles. Principal component analysis (PCA), mutual information (MI), and correlation analysis are used to regulate which features are most applicable for DDoS. The detection technique using numerous ensemble methods establishes that the suggested approach based on the RF outperforms existing methods. To improve the effectiveness of network IDS a DNN with independent feature extraction and DL was built for DDoS attack detection.

Hu *et al*. (2020) [49] developed an innovative method of attack detection using an improved CNN and adaptive synthetic sampling called ADASYN. The ADASYN method is used to first stabilize the sample movement, which successfully prevents the method from being overly sensitive to large examples and undervaluing small ones. Secondly, the progressed CNN may expand feature diversity and diminish the influence of data redundancy thanks to the split difficulty component (SPCCN). An AS-CNN model with ADASYN and SPC-CNN is employed for DDoS attack detection. Doriguzzi-Corin *et al.* (2020) [50] suggested a lightweight DDoS detection method based on the features of CNNs called LUCID. The use of a CNN to distinguish DDoS traffic with minimal computing time, the preprocessing of the dataset to produce traffic explanations for online attack detection, and the activation analysis to clarify DDoS attacks Catak *et al.* (2019) [51] developed AE-based DL methods to classify network traffic. To improve the classification performance, a DNN-based method has been used. The objective is to exactly classify malicious network traffic from packets by using a hybrid approach. The AE layer takes up the illustration of the network flows. The second layer's sDNN explorations for certain types of unsafe behavior.

Thangasamy *et al*. (2023) [52] established new detection techniques using a hybrid LSTM based on DBN for feature extraction. The Hybrid LSTM reduces prediction error by combining the PSO with LSTM. The DBN technique detects DDoS attacks by extracting IP packet properties. It also notices anomalies brought on by DDoS attacks and anticipates network traffic with accuracy. A new and enhanced LSTM (ILSTM) was proposed by Awad *et al.* (2023) for IDS [53]. To improve the LSTM approaches' precision, the PSO and chaotic butterfly optimization algorithm (CBOA) were hybrid to make an efficient ILSTM. Next, an effective IDS detection method was constructed using the ILSTM. The hybrid swarm algorithms, PSO and CBOA, to adjust the LSTM weights to enhance accuracy. Nine performance metrics were used to measure the efficiency of the ILSTM. The ILSTM obtained 93.09 % of accuracy and a 96.86 % of precision. Laghrissi *et al.* (2021) [54] considered a DL method to detect attacks based on LSTM. The optimal features are selected by PCA and MI. The experimental results demonstrate that for both training and testing in classification, PCA-based methods accomplish the highest levels of accuracy.

Sumathi *et al.* (2022) [55] employed a gradient descent learning rule-based DL approach based on LSTM, AE, and DE. The network parameters, including weight and bias are optimized by using a hybrid method based on Harris Hawks optimization (HHO) and PSO. The results exposed that the proposed LSTM achieved better than all other methods. Alom *et al.* (2017) [56] developed an AE and RBM-based DDoS attack detection method. The inputs are arithmetically encoded then AE and RBM are used for reducing the dimensional and feature extraction. The methods produced detection correctness values of almost 91.86% and 92.12%, correspondingly. Vinayakumar *et al.* (2019) [57] proposed an efficient detection method based on DNN to identify unpredictable cyberattacks. By feeding the data into many hidden layers, their DNN can learn the intellectual and high-dimensional feature illustration of the data. It has been recognized through extensive investigational testing that DNNs outperform conventional classifiers. An extremely scalable hybrid DNN that can be used to efficiently monitor host-level activities and network traffic in real-time, to anticipate and warn in contradiction of upcoming cyber-attacks. Su *et al.* (2020) [58] developed a BAT-based traffic anomaly recognition method using a combination of Bi-LSTM and the attention mechanism (AM). Using AM, the network traffic data made up of packets perverse by the BLSTM is separated to extract the important features to classify network traffic. Furthermore, numerous convolutional layers were used to extract the regional features from the traffic data. The BAT is mentioned to as BAT-MC since numerous convolutional layers are working to process traffic samples. Network traffic is categorized using the softmax method. The proposed end-to-end approaches can repeatedly recognize the salient features and do not need any knowledge of feature engineering. It can significantly improve anomaly detection competencies and offer a clear explanation of network traffic behavior. The experimental results demonstrate that it performs better than other comparison methods. Akgun *et al.* (2022) [59] developed a detection method that uses a DL method to detect attack and info gain attribute evaluation (IGAE) for preprocessing. Better appreciation performance was thus reached for the testing and training valuations.

Shende *et al.* (2020) [60] developed an attack detection method based on LSTM to perform. This technique is used to categorize data into binary and multiclass classes. It offers an accuracy of 99.2% for binary and 96.9% for multiclass classification. Y. Imrana *et al.* (2021) [61] established a new detection method based on BiDLSTM was suggested. Moreover, the BiDLSTM method outperforms the LSTM in terms of detection accuracy. Halbouni et al. (2022) [62] utilized the capacity of the LSTM to extract temporal features and the CNN to extract spatial characteristics to build a hybrid IDS model. Added dropout layers and batch normalization to the model to improve its efficiency. Pooja *et al*. (2021) [63] used the DL technique based on Bi-LSTM. The proposed method produced excellent results with 99% accuracy using the Bi-directional LSTM model. By changing the network's activation functions, the work was done again. Softmax and relu produced outstanding results for both datasets, averaging 99.5% accuracy. The outcomes were contrasted with the most recent techniques. We can infer from the comparison that BiLSTM outperforms other relevant efforts in the literature.

Gwon *et al.* (2019) [64] provide LSTM network-based models for IDS that use sequential information and embedding technique-based models that use categorical information. LSTM has used UNSW-NB15, a large-scale network traffic dataset, to test the models. The experiment results, which show a 99.72% binary classification accuracy, validate that the suggested strategy improves performance. Khan *et al.* (2019) [65] suggest a scalable and hybrid IDS based on Spark DL and the LSTM network. This is a two-stage ID system using the Spark DL-based anomaly detection module in the first stage. Based on the Conv-LSTM network, the second stage serves as a misappropriation detection module that addresses latent threat signatures that are both local and global. Our hybrid IDS beats state-of-the-art methods in 10-fold cross-validation testing and can accurately identify network misuses in 97.29% of cases, according to evaluations of different baseline models. Assy *et al.* (2023) [66] proposed a new one-dimensional CNN-based IDS model is put forth that has a 93.2% accuracy rate and a 93.1% F1 score for detecting anomalies. To train this model, the entire NSL-KDD benchmark dataset was utilized. The comparative analysis of the obtained findings using DL techniques such as CNN, LSTM, RNN, and others is then used to illustrate the advantage of the proposed model over existing models in the literature.

Elmasry *et al.* (2020) [67] suggested a twofold PSO-based approach that allows for the simultaneous selection of the feature subset and hyperparameters. During the pre-training stage, the previously mentioned algorithm is utilized to automatically choose the model's hyperparameters and optimum features. To explore the variations in performance, we employed three DL models: Deep DNN, LSTM, and DBN. Based on the equivalent values of the same models without pre-training on the same dataset, experimental results demonstrate a considerable increase in network intrusion detection when utilizing this strategy, improving DR by 4% to 6% and reducing FAR by 1% to 5%. Zhang *et al.* (2022) [68] developed a new network IDS based on AE and LSTM. To map high-dimensional data to low-dimensional space, multiple AE networks are superimposed to create an AE. Then, to extract features, train data, and forecast the types of intrusion detection, the LSTM optimized the cell structure. The experimental outcomes prove a 2% average improvement in network IDS accuracy and a decrease in FAR when compared to multiple classical methods.

Kasongo (2023) [69] developed a new DL technique used to create an IDS framework which makes use of three different RNN methods such as Simple RNN, LSTM, and GRU. The significance of features was calculated using an XGBoost approach. Kumar *et al.* (2024) [70] proposed a new detection method based on Deep Residual CNN (DCRNN) which is optimized by Improved Gazelle Optimization Algorithm (IGOA. The Binary Grasshopper Optimization Algorithm (NBGOA) is used to choose optimal features. The results show how precisely and proficiently the proposed technique detects different of attacks. Khan *et al*. (2019) [71] recommend a CNN-based IDS method based on optimal features. To efficiently categorize intrusion samples, the model can automatically extract the real features. Experimental results prove that the developed method can meaningfully increase detection accuracy. Abusitta *et al.* (2019) [72] developed a cooperative IDS based on DL that efficiently uses past feedback data to allow proactive decision-making. To be more precise, the suggested model is built on a Denoising AE (DAE), which is an important component of a DNN. The ability of DAE to reconstruct traffic data feedback from imperfect feedback is what gives it its control. This allows us to choose on suspicious intrusions proactively even when the IDSs do not deliver us with all of their data sample. TensorFlow with GPU support was used to develop the proposed model, and a real-world dataset was used for assessment. According to experimental outcomes, the approach can attain up to 95% detection accuracy.

Al *et al.* (2021) [73] proposed a new classification-based IDS method using hybrid CNN and LSTM. Furthermore, data imbalance was achieved based on the Synthetic Minority Oversampling Technique (SMOTE) and Tomek-Links sampling methods known as STL to reduce the effect of data imbalance on system performance. De Carvalho Bertoli *et al.* (2023) [74] a new IDS to generalize on a cross-silo setup for a flow based on stacked-unsupervised federated learning (FL). In an ensemble learning challenge, a deep AE and an energy flow classifier are part of the suggested strategy that has been studied. This method outperforms naive cross-evaluation and conventional local learning. Surprisingly, the suggested method performs admirably when it comes to non-IID data silos. It is suggested that the FL-based NIDS produces a workable method for generalization across heterogeneous networks when combined with an instructive feature.

Ieracitano *et al.* (2020) introduce an intelligent IDS driven by AE and statistical analysis. In particular, the suggested IDS extracts optimized and more associated features by combining statistical methods, data analytics, and recent developments in DL theory. According to experimental data, the developed IDS outperforms deep and standard shallow DL as well as recently suggested state-of-the-art methods [75]. Lopes *et al.* (2023) [76] create, apply, and evaluate the classification performance of four temporal-based convolutional models for NIDs. Using the test dataset, all models have produced excellent evaluation performances, falling between 98.07% and 99.99% for the majority of the measures taken into consideration. The models with the greatest evaluation scores in terms of effectiveness measures were MiniRocket and OS-CNN. The positive evaluation outcomes imply that they can raise the efficacy of methods for defining network intrusion detection as a time series task. Pingale *et al.* (2022) [77] created a powerful hybrid deep model for intrusion detection called the Remora Whale Optimization (RWO) based Hybrid deep model. Here, preprocessing is done on the incoming data before data transformation is carried out. Effective CNN features are extracted from the changed data, and feature conversion is done to turn the features into vector form. Additionally, the RV-coefficient is utilized to carry out the feature selection process, and in the end, the Hybrid Deep Model—which combines the Deep Maxout Network and AE—effectively detects network intrusions.

Thakkar *et al.* (2023) [78] focus on improving the DNN-based IDS's performance by introducing a novel feature selection method that uses Standard Deviation and Difference of Mean and Median to fuse statistically significant features. Performance comparison is given in terms of execution time in addition to evaluation indicators. Additionally, the Wilcoxon Signed Rank test is used to statistically test the results obtained. Alsirhaniet *et al.* (2023) [79] suggest a novel IDS for intelligent grids that combines feature-based and DL-based methods. The dataset is pre-processed for this purpose, and min-max normalization is used to do this. Next, features are retrieved, such as data percentiles, correlation coefficient, and information gain, mean, median, mode, standard deviation, and autoregressive data. After that, feature selection is arranged by the African Vulture Optimization Algorithm. Lastly, a DBN-LSTM classification algorithm is used to distinguish between attack and normal packets. When compared to other current strategies, the new method performs better. Therefore, the results show that the AVOA-DBN-LSTM technique has a good chance of detecting cyber security intrusions. Lan *et al.* (2022) [80] suggest MEMBER, a multi-task learning model with hybrid deep features, as a solution to the problems outlined above. Based on a CNN with integrated spatial and channel attention mechanisms, MEMBER creatively adds two auxiliary tasks (a distance-based prototype network and an AE enhanced with a memory module) to expand the model's capability to simplify and mitigate the performance degradation experienced in unbalanced network environments. Our suggested MEMBER is superior and resilient, as shown by extensive experimentation on many benchmark datasets.

Ayo *et al.* (2023) [81] created a rule-based hybrid feature selection-optimized DL model-based network IDS. The three stages of the architecture are detection, rule evaluation, and hybrid feature selection. The suggested method beats related methods with lower false alarm rates, higher accuracy rates, and shorter training and testing times of 1.2%, 98.8%, 7.17s, and 3.11s, respectively, according to the results of the performance comparison. Ultimately, the suggested approach is appropriate for attack classification in NIDS, as demonstrated by the simulation experiments conducted using conventional assessment criteria. Li *et al.* (2024) [82] suggested a novel IDS built on a GAN and VAE. To balance the initial training dataset, the VAE-WGAN model was first introduced. This model combines the benefits of VAE and GAN and allows for the generation of data with predetermined labels. A hybrid neural network model based on stacked LSTM and Multi-Scale MSCNN was employed in the intrusion detection phase. Network attack detection rates can be raised by using feature fusion after stacked LSTM and MSCNN networks can extract network characteristics at various depths and sizes. With 83.45% accuracy and 83.69% f1-score, the model performs better than other intrusion detection techniques currently. Additionally, on the AWID dataset, it achieves an accuracy and f1-score of above 98.9%. Ur Rehman *et al*. (2021) [83] developed a brand-new, highly effective method called DIDDOS is put forth to defend against actual DDoS attacks by utilizing GRUs, a subset of RNNs.

Al-zubidi *et al.* (2024) [84] presents a novel and efficient method for forecasting DoS and DDoS attacks using an efficient model termed CNN-LSTM-XGBoost, a cutting-edge hybrid technique made for network security intrusion detection. Authors handle imbalanced data, eliminate null and duplicate data, and use correlation-based feature selection to choose the most pertinent features as part of our preprocessing steps. Additionally, the method uses the most vital features to reduce the model's overfitting. Issa *et al.* (2020) [85] propose a DL-based IDS that expands detection accuracy by removing temporal and geographical information from network traffic data based on hybrid CNN and LSTM. According to the developed approach, DL-IDS got the best fallouts across all methods, with an overall high accuracy. Bamber *et al.* (2025) [86] proposed a hybrid detection technique based on LSTM with CNN based on the feature selection technique. The most informative features are extracted the use of Recursive Feature Elimination (RFE), which drops dimensionality and reduces overfitting.

Table 1. Summary of DL-based DDoS detection methods including model architectures, datasets used, detection accuracy, and identified limitations

Ref. No.	Approaches	Implementation Focus	Dataset	Merits	Demerits
[38]	AE+RF	Feature selection	CICDDoS2019 DDoS-AT-2022	The model produced high detection accuracy	High computation cost
[39]	ADE	Feature selection	ICS	The method is scalable and cost-effective	The model lacks in accuracy
[40]	HDE + SDNN	Feature selection	CICDDoS2017	The model achieved Low computational time	The model is high cost-effective
[41]	Hybrid CNN+LSTM	Features extractions	UNSW 2018 Mandalay dataset	The approach gives better results	High computational time
[42]	E-SDNN	Selecting pertinent features	CICDS2017 CICDDoS2019	Model produced high accuracy	The model is ineffective
[43]	DSAE+Elastic net	Feature selection Hyperparameter optimization	CICDS2017 CICDDoS2019	Enhanced detection accuracy	The model can manage fewer datasets
[44]	GHLBO +DSA	Training approaches	BoT-IoT	Finding optimal hyperparameters	The method achieved low accuracy
[45]	DVGAN	Feature selections	CICDDoS2019	Reduce operational overhead	The method is incompetence
[46]	VAE-DNN	Latent representation	CICIDS 2017	Model achieved highest precision	The method issues in scalability
[47]	SVM-AE	Imbalanced datasets	CICDDoS2019	Managing new types of attacks	The model falls into underfitting
[48]	GRU+DLP+Softmax	Classifications	SIMARGL21 UNR-IDD NF-ToN-IoT 2021, UKM-IDS20 2020, CIC–IDS2018, WSN-DS, UNSW-NB15 2015, NSL-KDD, KDD Cup	The model achieved high Accuracy	The method falls into local optima
[49]	CNN	Hyperparameter optimization	NSL-KDD	The model has low computational time	The model lacks into execution efficiency
[50]	CNN	Network optimization	ISCX2012 CIC2017 CSECIC2018 UNB201X	High computational time	The model achieved low accuracy
[51]	AE	Feature selection	KDDCUP99	The model discovers meaningful feature	The method falls into overfitting
[52]	LSTM + DBN with PSO	Feature selection	NSL-KDD	Enhanced feature learning and better convergence	High computation time due to sensitive to initial settings
[53]	CBOA + PSO-based LSTM	Hyperparameter optimization	NSL-KDD LITNET-2020	The model produced high accuracy	The model achieved high computation time

[54]	PCA+MI based LSTM	Features selection	KDD99	High correlation between features	Lack of multiple variant investigation in LSTM
[55]	HHO+PSO based LSTM	Weights and biases optimization	NSL-KDD	The model achieved fast convergence rate	High computational time, and lack of automatic updating during attacks.
[56]	USELM	Dimensionality reduction	KDD-99	The model produced high accuracy	Lack of inline detection
[57]	DNN	Weights and bias optimization	DARPA, KDD Cup 88, KDD Cup 99, NSL-KDD, CICIDS 2017	The model convergence quickly	Lack of accuracy, not able to work on complex data.
[58]	Bi-LSTM + AM	Feature engineering	NSL-KDD	Improve the ability to detect the rate	Lack of feature implementation
[59]	DL methods	Feature selections	CIC-DDoS2019	Low computational cost	The model lacks in accuracy
[60]	LSTM	Online alert	NSL-KDD	High accuracy with low computation cost	Low convergence rate
[61]	BiDLSTM	Concentrate on different attacks	NSL-KDD	The model achieved high accuracy	Requires much training time
[62]	Hybrid CNN-LSTM	Feature extractions	CIC-IDS 2017, UNSW-NB15, and WSN-DS.	The model achieved high accuracy	High computation complexity
[63]	Bi-LSTM	Analysis of activation functions	KDD CUP-99 UNSW-NB-15	High accuracy when using offline datasets	Lack of online detection
[64]	LSTM	Feature embedding	UNSW-NB15	The model achieved high accuracy	Lack of online detection
[65]	CNN-LSTM	Spark platform	ISCX-IDS 2012	The model convergence quickly	The model produced low accuracy
[66]	CNN1D	Feature selection	NSL-KDD	High accuracy achieved by model	Class imbalance problem
[67]	DNN, LSTM, and DBN.	Feature selection	NSL-KDD, CICIDS2017	High detection accuracy produced by the model	The model lacks when handling new datasets
[68]	AE+LSTM	Dimensionality reduction	KDDcup99	Mapping datasets with large dimensions to datasets with reduced dimensions	Encoding and decoding process takes high computational time
[69]	XGBoost + GRU+LSTM	Feature selection	UNSW-NB15, NSL-KDD	High detection accuracy	Failure to find global optima
[70]	IGOA+DL	Hyperparameters optimization + feature selections	UNSW-NB-15, CICDDOS2019, CIC-IDS-2017	Low computation time	The model produced low accuracy
[71]	CNN	Automatic feature extractions	KDD 99	The model achieved high accuracy	Low efficient performance

[72]	AE	Denoising the data	KDD Cup 99	Real-time environment	Model convergence quickly
[73]	CNN+LSTM	Filling the missing values	CIDDS-001, UNSW-NB15	The learning process is high	Data unbalancing causes a problem
[74]	AE	Federated unsupervised learning	Customized	Model can handle complex data	The model lacks in accuracy
[75]	fuzzy logic + CNN	Handing the uncertainty	NSL-KDD	The model achieved low computation time	The model produced low accuracy
[76]	OS-CNN	Hyperparameter optimization	CICDDoS2019, CSE-CIC-IDS2018	Detection accuracy is high	High computation time
[77]	Deep Maxout Network (DMN) and AE	Network optimization	NSL-KDD	The model convergence quickly	Failure to recent datasets
[78]	DNN	Statistical feature selection	NSL-KDD, UNSW_NB-15, CIC-IDS-2017.	The model convergence quickly	the model stuck in the real-time dataset
[79]	DBN-LSTM with AVO	Feature extraction and selection	NSL-KDD	High detection accuracy obtained	AVO affects the duplicability
[80]	CNN+AM	embedded spatial and channel	Bot-IoT, UNSW-NB15, CIC-IDS2017, ISCX2012	The model convergence quickly	The model produced low accuracy
[81]	GA with ANNs	Feature selection	UNSW-NB15	High accuracy obtained with low computation time	More iterations are required to get convergence
[82]	VAE	Hyperparameters optimization	NSL-KDD AWID	The approach produced high accuracy	Low convergence rate
[83]	GRU	Real-time data generations	CICDDoS2019	The model can manage the different layers	Low convergence rate
[84]	CNN-LSTM-XGBoost	Feature selection	CICIDS-001 CIC-IDS2017 CIC-IDS2018	The model can manage overfitting	The model produced low accuracy
[85]	CNN+LSTM	Extract the spatial and temporal features of network traffic	CICIDS2017	Reduce the influence of an unbalanced number of samples	Lacks in computation time
[86]	CNN+LSTM based on RFE	Feature selection	NSL-KDD	Reduce the chance of an overfitting and computational complexity	The model lacks in accuracy
[87]	CNN + BiLSTM	Feature extractions and ranking	CIC-DDoS2019	Low computation time	The learning process of model falls into overfitting
[88]	Hybrid-optimized LSTM and CNN	Feature extraction and hyperparameters tunning	NSL-KDD BoT-IoT	Features are extracted from dimension-transformed data	The model produced low accuracy

The proposed technique makes use of sophisticated DL methods, mostly the CNN-LSTM model. The hybrid detection method addresses overfitting, computational complexity, and assuring better scalability by combining CNNs for efficient feature extraction and LSTMs for capturing temporal trends. Alghazzawi (2021) [87] recommend utilizing a hybrid DL model, specifically a CNN with BiLSTM to predict DDoS attacks. According to experiment outcomes, the proposed CNN-BI-LSTM attained up to 94.52 % accuracy.

4. Discussions

DL approaches have formed a big influence on DDoS attack detection. Some DL approaches have established excellent accuracy and real-time detection abilities, while others have had problems with deployment, simplification, and adversarial attacks. The CNN [71], LSTM [64], and AE [82] (AEs), and hybrid models are some of the most significant models. Some have suffered with scalability, false positives, and adversarial attacks, while others have flourished in real-time performance and high accuracy. An LSTM-based approach was used in an actual network monitoring scheme to classify both high-rate and slow-rate attacks. By identifying long-term dependencies in network data, LSTM was able to identify complex slow-rate DDoS attacks [89]. The accuracy of the model in detecting covert DDoS patterns was 98.7%. However, High false positive rate (10%+) due to normal traffic variations misclassified as DDoS, Poor generalization to diverse traffic patterns, and computationally expensive for slow-rate attacks. The AE detected previously unseen DDoS attacks with high accuracy, learned typical traffic behavior, and highlighted aberrant DDoS patterns without the need for labeled data, decreasing reliance on manual attack signatures. However, when tested on real-world traffic, detection accuracy fell below 10%, it produced too many false alarms, resulting in needless mitigation, and it had trouble distinguishing DDoS attacks from typical high-traffic spikes. CNN was unable to generalize to attack vectors that were altered and attackers made small changes to the characteristics of network traffic, the detection rate decreased from 97% to 43% after undergoing adversarial training.

Much research work is carried out using hybrid methods such as CNN [71], LSTM [64], and AE [82]. Some papers use CNN to extract the spatial features from the traffic data to enhance the accuracy of the detection method such as LSTM [62, 90] and AE [35] etc. CNN and AE are used to extract the features and LSTM method for capturing temporal features from the traffic data and helping distinguish slow-and-low DDoS attacks. The hybrid methods achieved more than 98 % accuracy with low false positives. A CNN-LSTM [85] hybrid model was created for volumetric and application-layer DDoS detection. LSTMs perform well in sequential DDoS patterns, but they have trouble in a variety of settings. Although they need strong feature engineering, autoencoders are excellent for detecting zero-day attacks. CNNs are good at fast detection, but they can be attacked by adversaries.

Table 2. Overview of publicly available DDoS-related datasets with their characteristics and relevance to real-world detection scenarios

Dataset	Description	Relevance with Real-time
KDD	An intended for assessing DDoS and other intrusions included Both anomaly-based and signature-based detection are possible. It contains four attacks including “DoS/DDoS, Probe, User to Root (U2R), and Remote to Local (R2L)”	It aids in the training of intrusion prevention and detection systems (IDS and IPS)
NSL-KDD	Reduced instances of duplicates in an enhanced KDD99 dataset and it contains such as “Teardrop, Neptune, and Smurf”	It is appropriate for traditional ML models and less reflective of contemporary DDoS attack designs but useful for benchmarking.
CICIDS2017	Despite being mainly an intrusion detection dataset, it covers DDoS attacks like DoS Hulk and Port Scan.	It depicts both attack and benign network activity realistically. It is beneficial for model training in hybrid attack detection settings.
CIC-IDS2018	It is designed to evaluate IDS and cover a range of cyberattacks, including DDoS attacks. Five days' worth of realistic network traffic, including both attack and regular circumstances such as “UDP Flood, SYN Flood, HTTP Flood, and Botnet-based DDoS”	It is extremely indicative of traffic in the real world because it was recorded from a testbed that replicates a corporate network. It contains harmless traffic, enabling DDoS detection based on anomalies.
CICDDoS2019	It contains actual DDoS attack traffic produced in a controlled situation. It covers a variety of DDoS	It reflects current attack patterns, such as DDoS attacks at the application layer and volumetric attacks. It is appropriate for

	attacks which contain UDP flood, SYN flood, and HTTP flood.	machine learning-based detection since it includes tagged network traffic with a variety of attack kinds.
BoT-IoT	Considered to signify IoT-related cyberattacks with large-scale DDoS attacks.	It can detect botnet-driven DDoS attacks and features both normal and attack traffic from IoT devices.
UNSW-NB15	An extensive dataset was created using the IXIA Perfect Storm program that includes a variety of attack types, including DDoS.	It is perfect for AI-based DDoS detection because it has 49 features. It beneficial for multi-stage and hybrid attack analysis.
ISCX2012	It contains a target system that is inundated with traffic from numerous infected servers. It records application-layer attacks (like HTTP flooding) as well as volumetric DDoS attacks (like UDP flood).	The dataset helps simulate real-world attacks since it replicates the behaviors of enterprise networks. It is perfect for anomaly-based detection because it incorporates typical user activities.

Although they require adjustment for real-time performance, hybrid CNN-LSTM [85] models perform better than standalone DL models. Large, high-quality datasets are necessary for DL models to identify DDoS attacks and identify trends in network traffic. Many datasets are available with their separate characteristics for detecting attacks in their environments. Table 2 shows the overview of available DDoS attack datasets.

5. Challenges

Despite the potential advantages of applying advanced DL methods, detecting DDoS attacks using DL approaches faces various difficulties. Datasets for DDoS attacks are sometimes quite unbalanced, with a large percentage of cases representing regular traffic and a disproportionately small percentage representing attack instances. DL approaches require balanced datasets to work well, and biased methods might outcome from imbalanced data. The size of the collection should permit for a thorough depiction of the DDoS attacks. Make certain the datasets are large and diverse when developing methods to classify and mitigate DDoS attacks. . The diversity of attacks contains a range of attack types, pathways, and intensities. Because various kinds of DDoS attacks are involved in the training data, the produced models can identify and respond to a wider range of attack types. As a result, they may be significantly more precise and capable of generalization, making them more resilient to various types of attacks. Because of this, it's significant to frequently update the datasets with fresh attacks to assurance that the models continue to function well and can identify even the most complicated and sophisticated attack patterns. The excellence and applicability of the input data have an important impact on the efficiency of DL models. To classify significant patterns in network traffic data, feature engineering is important. Designing effective features for DDoS attack detection is problematic, particularly given how frequently DDoS attacks variation. The developed models for one network may not generalize effectively to another due to its dynamic nature. It can be problematic to adjust DL models to various network setups and behaviors, especially in real-time situations. DDoS attacks may start very rapidly and overwhelm a network in an instant of minutes. Due to their computational expense, DL methods, mostly sophisticated ones, may not be suitable for real-time detection. For prompt detection and reaction, effective application and optimization are compulsory. An interpretability can be interesting to comprehend the logic behind the predictions made by DL models, especially DNN, which are sometimes referred to as "black boxes." Understanding why a particular traffic instance was labeled as an attack or normal in the context of DDoS attack detection might be critical for network managers.

6. Conclusions

One of the most important lessons securities teaches us is to be proactive rather than reactive. These days, creating a DDoS attack detection system is difficult, particularly when dealing with attacks that are of a new generation. New DDoS attack generations have been able to evolve thanks to advanced evasion techniques, which have had extremely serious consequences. On the other hand, DDoS attack detection technology based on DL lessens the shortcomings of both conventional and traditional approaches. This study offers a thorough analysis of DL methods for DDoS attack detection. Research taxonomy is proposed based on the development of DL-based methodologies. There is also an exploration and comparison of recent methods for identifying DDoS attacks on computer network systems. Lastly, this study will point researchers in the right direction for creating mitigation strategies for both common and sophisticated malware by providing them with a comprehensive grasp of DDoS attack analysis.

A few feature enhancements are discussed as follows:

- Create a new DL model that is domain-adaptive so they can simplify to a variety of network circumstances and traffic patterns.

- Examine transfer learning approaches to adjust models established on a single dataset to fit novel or changing assault scenarios.
- For hybrid detection frameworks, combine rule-based or signature-based techniques with anomaly detection based on deep learning.
- To increase the accuracy of detection, combine information from several sources such as network flow, system logs, and endpoint behavior.

References

[1] P. Bojović, I. Bašičević, S. Ocovaj, M. Popović, A practical approach to detection of distributed denial-of-service attacks using a hybrid detection method. Computers & Electrical Engineering, 73, (2019) 84-96. https://doi.org/10.1016/j.compeleceng.2018.11.004

[2] J. Lansky, S. Ali, M. Mohammadi, M.K. Majeed, S.H.T. Karim, S. Rashidi, M. Hosseinzadeh, A. M. Rahmani, Deep learning-based intrusion detection systems: a systematic review. IEEE Access, 9, (2021) 101574-101599. https://doi.org/10.1109/ACCESS.2021.3097247

[3] T. A. Tuan, H. V. Long, L. H. Son, R. Kumar, I. Priyadarshini, N.T.K. Son, Performance evaluation of Botnet DDoS attack detection using machine learning. Evolutionary Intelligence, 13, (2020) 283-294. https://doi.org/10.1007/s12065-019-00310-w

[4] M.T. Hussan, G. V. Reddy, P. Anitha, A. Kanagaraj, P. Naresh, DDoS attack detection in IoT environment using optimized Elman recurrent neural networks based on chaotic bacterial colony optimization. Cluster Computing, 27(4), (2024) 4469-4490. https://doi.org/10.1007/s10586-023-04187-4

[5] Y. Wu, D. Wei, J. Feng, Network attacks detection methods based on deep learning techniques: A survey. Security and Communication Networks, 2020(1), (2020) 8872923. https://doi.org/10.1155/2020/8872923

[6] A.A. Habib, A. Imtiaz, D. Tripura, M. O. Faruk, M.A. Hossain, I. Ara, S. Sarker, A.F.Z. Abadin, Distributed denial-of-service attack detection short review: issues, challenges, and recommendations. Bulletin of Electrical Engineering and Informatics, 14(1), (2025) 438-446. https://doi.org/10.11591/eei.v14i1.8377

[7] N. K. Almazmomi, Long short-term memory-based intrusion detection system using hybrid grid search and sequential chimp optimization algorithm-based hyperparameter tuning. Intelligent Decision Technologies, 19(2), (2025) 18724981241291422. https://doi.org/10.1177/18724981241291422

[8] Y. Omer, P. Jorge, (2023). DDoS threat report for 2023 Q4. The Cloudflare Blog. https://blog.cloudflare.com/ddos-threat-report-2023-q4/

[9] Q.A. Al-Haija, A. Droos, A comprehensive survey on deep learning-based intrusion detection systems in Internet of Things (IoT). Expert Systems, 42(2), (2025) e13726. https://doi.org/10.1111/exsy.13726

[10] K.M. Abuali, L. Nissirat, A. Al-Samawi, Advancing Network Security with AI: SVM-Based Deep Learning for Intrusion Detection. Sensors, 23(21), (2023) 8959. https://doi.org/10.3390/s23218959

[11] L.D. Tsobdjou, S. Pierre, A. Quintero, An online entropy-based DDoS flooding attack detection system with dynamic threshold. IEEE Transactions on Network and Service Management, 19(2), (2022) 1679-1689. https://doi.org/10.1109/TNSM.2022.3142254

[12] M. Solanki, S. Chaudhari, VLMDALP: design of an efficient VARMA LSTM-based model for identification of DDoS attacks using application-level packet analysis. International Journal of Electronic Security and Digital Forensics, 17(1-2), (2025) 149-168. https://doi.org/10.1504/IJESDF.2025.143476

[13] R. Alguliyev, R. Shikhaliyev, Computer Networks Cybersecurity Monitoring Based on Deep Learning Model," Security and Privacy, 8(1), (2025) e459. https://doi.org/10.1002/spy2.459

[14] S. Kansal, Utilizing Deep Learning Techniques for Effective Zero-Day Attack Detection. Economic Sciences, 21(1), (2025) 246-257. https://doi.org/10.69889/m3jzbt24

[15] Z. Xu, Deep Learning Based DDoS Attack Detection. in ITM Web of Conferences, 70, (2025) 03005. https://doi.org/10.1051/itmconf/20257003005

[16] J. Yan, H. Zhou, W. Wang, Intelligent Network Element: A Programmable Switch Based on Machine Learning to Defend Against DDoS Attacks. Information Systems Frontiers, (2025) 1-20. https://doi.org/10.1007/s10796-024-10577-9

[17] S. Aktar, A.Y. Nur, Towards DDoS attack detection using deep learning approach. Computers & Security, 129, (2023) 103251. https://doi.org/10.1016/j.cose.2023.103251

[18] M. Mittal, K. Kumar, S. Behal, Deep learning approaches for detecting DDoS attacks: A systematic review. Soft computing, 27(18), (2023) 13039-13075. https://doi.org/10.1007/s00500-021-06608-1

[19] M.A. Al-Shareeda, S. Manickam, M.A. Saare, DDoS attacks detection using machine learning and deep learning techniques: Analysis and comparison. Bulletin of Electrical Engineering and Informatics, 12(2), (2023) 930-939. https://doi.org/10.11591/eei.v12i2.4466

[20] S. Hosseini, M. Azizi, The hybrid technique for DDoS detection with supervised learning algorithms. Computer Networks, 158, (2019) 35-45. https://doi.org/10.1016/j.comnet.2019.04.027

[21] V. Hnamte, A.A. Najar, H. Nhung-Nguyen, J. Hussain, M.N. Sugali, DDoS attack detection and mitigation using deep neural network in SDN environment. Computers & Security, 138, (2024) 103661. https://doi.org/10.1016/j.cose.2023.103661

[22] D. Krishnan, S. Hemamalini, P. Cheraku, K. H. Priya, S. Ganesan, R. Balamanigandan, Attack detection using DL based feature selection with improved convolutional neural network. International Journal of Electrical and Electronics Research, 11(2), (2023) 308-314. https://ijeer.forexjournal.co.in/archive/volume-11/ijeer-110209.html

[23] H. Aydın, Z. Orman, M. A. Aydın, A long short-term memory (LSTM)-based distributed denial of service (DDoS) detection and defense system design in public cloud network environment. Computers & Security, 118, (2022) 102725. https://doi.org/10.1016/j.cose.2022.102725

[24] N.A. Bajao, J.a. Sarucam, Threats Detection in the Internet of Things Using Convolutional neural networks, long short-term memory, and gated recurrent units. Mesopotamian journal of cybersecurity, 2023, (2023) 22-29. https://doi.org/10.58496/MJCS/2023/005

[25] D.M.B. Lent, M.P. Novaes, L.F. Carvalho, J. Lloret, J.J. Rodrigues, M.L. Proença, A gated recurrent unit deep learning model to detect and mitigate distributed denial of service and portscan attacks. IEEE Access, 10, (2022) 73229-73242. https://doi.org/10.1109/ACCESS.2022.3190008

[26] A.E. Cil, K. Yildiz, A. Buldu, Detection of DDoS attacks with feed forward based deep neural network model. Expert Systems with Applications, 169, (2021) 114520. https://doi.org/10.1016/j.eswa.2020.114520

[27] D. C. Le, N. Zincir-Heywood, M. I. Heywood, "Unsupervised monitoring of network and service behaviour using self-organizing maps. Journal of Cyber Security and Mobility, (2019) 15-52.

[28] D. M. B. Lent, V. G. D. S. Ruffo, L. F. Carvalho, J. Lloret, J. J. Rodrigues, M. L. Proença, An Unsupervised Generative Adversarial Network System to Detect DDoS Attacks in SDN. IEEE Access, (2024) 70690-70706. https://doi.org/10.1109/ACCESS.2024.3402069

[29] R.F. Fouladi, O. Ermiş, E. Anarim, A DDoS attack detection and countermeasure scheme based on DWT and auto-encoder neural network for SDN. Computer Networks, 214, (2022) 109140. https://doi.org/10.1016/j.comnet.2022.109140

[30] X. Qu, L. Yang, K. Guo, L. Ma, M. Sun, M. Ke, M. Li, A survey on the development of self-organizing maps for unsupervised intrusion detection. Mobile networks and applications, 26, (2021) 808-829. https://doi.org/10.1007/s11036-019-01353-0

[31] S. Velliangiri, H.M. Pandey, Fuzzy-Taylor-elephant herd optimization inspired Deep Belief Network for DDoS attack detection and comparison with state-of-the-arts algorithms. Future Generation Computer Systems, 110, (2020) 80-90. https://doi.org/10.1016/j.future.2020.03.049

[32] M. Aamir, S.M.A. Zaidi, Clustering based semi-supervised machine learning for DDoS attack classification," Journal of King Saud University-Computer and Information Sciences, 33(4), (2021) 436-446. https://doi.org/10.1016/j.jksuci.2019.02.003

[33] A.A. Samsu Aliar, M. Agoramoorthy, An automated detection of DDoS attack in cloud using optimized weighted fused features and hybrid DBN-GRU architecture. Cybernetics and Systems, 55(7), (2024) 1469-1510. https://doi.org/10.1080/01969722.2022.2157603

[34] L. Chen, Z. Wang, R. Huo, T. Huang, An adversarial DBN-LSTM method for detecting and defending against DDoS attacks in SDN environments. Algorithms, 16(4), (2023) 197. https://doi.org/10.3390/a16040197

[35] Y. Wei, J. Jang-Jaccard, F. Sabrina, A. Singh, W. Xu, S. Camtepe, Ae-mlp: A hybrid deep learning approach for ddos detection and classification. IEEE Access, 9, (2021) 146810-146821. https://doi.org/10.1109/ACCESS.2021.3123791

[36] B. Hussain, Q. Du, B. Sun, Z. Han, Deep learning-based DDoS-attack detection for cyber–physical system over 5G network. IEEE Transactions on Industrial Informatics, 17(2), (2020) 860-870. https://doi.org/10.1109/TII.2020.2974520

[37] M. Ramzan, M. Shoaib, A. Altaf, S. Arshad, F. Iqbal, Á.K. Castilla, I. Ashraf, Distributed denial of service attack detection in network traffic using deep learning algorithm. Sensors, 23(20), (2023) 8642. https://doi.org/10.3390/s23208642

[38] M. Mittal, K. Kumar, S. Behal, DL-2P-DDoSADF: Deep learning-based two-phase DDoS attack detection framework. Journal of Information Security and Applications, 78, (2023) 103609. https://doi.org/10.1016/j.jisa.2023.103609

[39] I. Ortega-Fernandez, M. Sestelo, J.C. Burguillo, C. Piñón-Blanco, Network intrusion detection system for DDoS attacks in ICS using deep autoencoders. Wireless Networks, 30, (2023) 1-17. https://doi.org/10.1007/s11276-022-03214-3

[40] E. Benmohamed, A. Thaljaoui, S. El Khediri, S. Aladhadh, M. Alohali, DDoS attacks detection with half autoencoder-stacked deep neural network. International Journal of Cooperative

Information Systems, 33(3), (2023) 2350025. https://doi.org/10.1142/S0218843023500259

[41] A.K. Mousa, M.N. Abdullah, An improved deep learning model for DDoS detection based on hybrid stacked autoencoder and checkpoint network. Future Internet, 15(8), (2023) 278. https://doi.org/10.3390/fi15080278

[42] E. Benmohamed, A. Thaljaoui, S. Elkhediri, S. Aladhadh, M. Alohali, E-SDNN: encoder-stacked deep neural networks for DDOS attack detection. Neural Computing and Applications, 36, (2024) 10431–10443. https://doi.org/10.1007/s00521-024-09622-0

[43] R.K. Batchu, H. Seetha, A hybrid detection system for DDoS attacks based on deep sparse autoencoder and light gradient boost machine. Journal of Information & Knowledge Management, 22(1), (2023) 2250071. https://doi.org/10.1142/S021964922250071X

[44] S. Balasubramaniam, C. Vijesh Joe, T.A. Sivakumar, A. Prasanth, K. Satheesh Kumar, V. Kavitha, R.K.Dhanaraj, Optimization enabled deep learning-based ddos attack detection in cloud computing. International Journal of Intelligent Systems, 2023(1), (2023) 2039217. https://doi.org/10.1155/2023/2039217

[45] C.M.V.S. Akana, A. Kumar, M. Tiwari, A.Z. Yunus, E. Vijayakumar, M. Singh, (2023) An Optimized DDoS Attack Detection Using Deep Convolutional Generative Adversarial Networks. International Conference on Inventive Research in Computing Applications (ICIRCA), IEEE, India. https://doi.org/10.1109/ICIRCA57980.2023.10220745

[46] A. Kandiero, P. Chiurunge, J. Munodawafa, Detection of DDoS Attacks Using Variational Autoencoder-Based Deep Neural Network. Privacy Preservation and Secured Data Storage in Cloud Computing: IGI Global, (2023) 365-404. https://doi.org/10.4018/979-8-3693-0593-5.ch017

[47] U. Shrivastav, M. Kumar, S. Kumar, An Autoencoder-based Efficient Scheme for DDoS Detection. International Conference on Computer, Electronics & Electrical Engineering & their Applications (IC2E3), IEEE, India. https://doi.org/10.1109/IC2E357697.2023.10262806

[48] M.A. Hossain M.S. Islam, Ensuring network security with a robust intrusion detection system using ensemble-based machine learning. Array, 19, (2023) 100306. https://doi.org/10.1016/j.array.2023.100306

[49] Z. Hu, L. Wang, L. Qi, Y. Li, W. Yang, A novel wireless network intrusion detection method based on adaptive synthetic sampling and an improved convolutional neural network. IEEE Access, 8, (2020) 195741-195751. https://doi.org/10.1109/ACCESS.2020.3034015

[50] R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J. Martinez-del-Rincon, D. Siracusa, LUCID: A practical, lightweight deep learning solution for DDoS attack detection. IEEE Transactions on Network and Service Management, 17(2), (2020) 876-889. https://doi.org/10.1109/TNSM.2020.2971776

[51] F.O. Catak, A.F. Mustacoglu, Distributed denial of service attack detection using autoencoder and deep neural networks. Journal of Intelligent & Fuzzy Systems, 37(3), (2019) 3969-3979. https://doi.org/10.3233/JIFS-190159

[52] A. Thangasamy, B. Sundan, L. Govindaraj, A Novel Framework for DDoS Attacks Detection Using Hybrid LSTM Techniques. Computer Systems Science & Engineering, 45(3), (2023) 2553-2567. https://doi.org/10.32604/csse.2023.032078

[53] A.A. Awad, A.F. Ali, T. Gaber, An improved long short term memory network for intrusion detection. Plos one, 18(8), (2023) e0284795. https://doi.org/10.1371/journal.pone.0284795

[54] F. Laghrissi, S. Douzi, K. Douzi, B. Hssina, Intrusion detection systems using long short-term memory (LSTM). Journal of Big Data, 8(1), (2021) 65. https://doi.org/10.1186/s40537-021-00448-4

[55] S. Sumathi, R. Rajesh, S. Lim, Recurrent and deep learning neural network models for DDoS attack detection. Journal of Sensors, (2022). https://doi.org/10.1155/2022/8530312

[56] M.Z. Alom, T.M. Taha, Network intrusion detection for cyber security using unsupervised deep learning approaches. IEEE national aerospace and electronics conference (NAECON), IEEE, USA. https://doi.org/10.1109/NAECON.2017.8268746

[57] R. Vinayakumar, M. Alazab, K. Soman, P. Poornachandran, A. Al-Nemrat, S. Venkatraman, Deep learning approach for intelligent intrusion detection system. Ieee Access, 7 (2019) 41525-41550. https://doi.org/10.1109/ACCESS.2019.2895334

[58] T. Su, H. Sun, J. Zhu, S. Wang, Y. Li, BAT: Deep learning methods on network intrusion detection using NSL-KDD dataset. IEEE Access, 8 (2020) 29575-29585. https://doi.org/10.1109/ACCESS.2020.2972627

[59] D. Akgun, S. Hizal, U. Cavusoglu, A new DDoS attacks intrusion detection model based on deep learning for cybersecurity. Computers & Security, 118, (2022) 102748. https://doi.org/10.1016/j.cose.2022.102748

[60] S. Shende, S. Thorat, Long short-term memory (LSTM) deep learning method for intrusion detection in network security. International Journal of Engineering Research and Technology, 9(6), (2020).

https://doi.org/10.17577/IJERTV9IS061016

[61] Y. Imrana, Y. Xiang, L. Ali, Z. Abdul-Rauf, A bidirectional LSTM deep learning approach for intrusion detection. Expert Systems with Applications, 185, (2021) 115524. https://doi.org/10.1016/j.eswa.2021.115524

[62] A. Halbouni, T.S. Gunawan, M.H. Habaebi, M. Halbouni, M. Kartiwi, R. Ahmad, CNN-LSTM: hybrid deep neural network for network intrusion detection system. IEEE Access, 10, (2022) 99837-99849. https://doi.org/10.1109/ACCESS.2022.3206425

[63] T. Pooja, P. Shrinivasacharya, Evaluating neural networks using Bi-Directional LSTM for network IDS (intrusion detection systems) in cyber security. Global Transitions Proceedings, 2(2), (2021) 448-454. https://doi.org/10.1016/j.gltp.2021.08.017

[64] H. Gwon, C. Lee, R. Keum, H. Choi, (2019) Network intrusion detection based on LSTM and feature embedding. arXiv preprint arXiv:1911.11552. https://doi.org/10.48550/arXiv.1911.11552

[65] M.A. Khan, M.R. Karim, Y. Kim, A scalable and hybrid intrusion detection system based on the convolutional-LSTM network. Symmetry, 11(4), (2019) 583. https://doi.org/10.3390/sym11040583

[66] A.T. Assy, Y. Mostafa, A. Abd El-khaleq, M. Mashaly, Anomaly-Based Intrusion Detection System using One-Dimensional Convolutional Neural Network. Procedia Computer Science, 220, (2023) 78-85. https://doi.org/10.1016/j.procs.2023.03.013

[67] W. Elmasry, A. Akbulut, A.H. Zaim, Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic. Computer Networks, 168, (2020) 107042. https://doi.org/10.1016/j.comnet.2019.107042

[68] Y. Zhang, Y. Zhang, N. Zhang, M. Xiao, A network intrusion detection method based on deep learning with higher accuracy. Procedia Computer Science, 174, (2020) 50-54. https://doi.org/10.1016/j.procs.2020.06.055

[69] S.M. Kasongo, A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework. Computer Communications, 199, (2023) 113-125. https://doi.org/10.1016/j.comcom.2022.12.010

[70] G.S.C. Kumar, R.K. Kumar, K.P.V. Kumar, N.R. Sai, M. Brahmaiah, Deep residual convolutional neural Network: An efficient technique for intrusion detection system. Expert Systems with Applications, 238, (2024) 121912. https://doi.org/10.1016/j.eswa.2023.121912

[71] R.U. Khan, X. Zhang, M. Alazab, R. Kumar, (2019) An improved convolutional neural network model for intrusion detection in networks. Cybersecurity and cyberforensics conference (CCC), IEEE, Australia. https://doi.org/10.1109/CCC.2019.000-6

[72] A. Abusitta, M. Bellaiche, M. Dagenais, T. Halabi, A deep learning approach for proactive multi-cloud cooperative intrusion detection system. Future Generation Computer Systems, 98, (2019) 308-318. https://doi.org/10.1016/j.future.2019.03.043

[73] S. Al, M. Dener, STL-HDL: A new hybrid network intrusion detection system for imbalanced dataset on big data environment. Computers & Security, 110, (2021) 102435. https://doi.org/10.1016/j.cose.2021.102435

[74] G. de Carvalho Bertoli, L. A. P. Junior, O. Saotome, A. L. dos Santos, Generalizing intrusion detection for heterogeneous networks: A stacked-unsupervised federated learning approach. Computers & Security, 127, (2023) 103106. https://doi.org/10.1016/j.cose.2023.103106

[75] C. Ieracitano, A. Adeel, F.C. Morabito, A. Hussain, A novel statistical analysis and autoencoder driven intelligent intrusion detection approach. Neurocomputing, 387, (2020) 51-62. https://doi.org/10.1016/j.neucom.2019.11.016

[76] I.O. Lopes, D. Zou, I.H. Abdulqadder, S. Akbar, Z. Li, F. Ruambo, W. Pereira, Network intrusion detection based on the temporal convolutional model. Computers & Security, 135, (2023) 103465. https://doi.org/10.1016/j.cose.2023.103465

[77] S.V. Pingale, S.R. Sutar, Remora whale optimization-based hybrid deep learning for network intrusion detection using CNN features. Expert Systems with Applications, 210, (2022) 118476. https://doi.org/10.1016/j.eswa.2022.118476

[78] A. Thakkar R. Lohiya, Fusion of statistical importance for feature selection in Deep Neural Network-based Intrusion Detection System. Information Fusion, 90, (2023) 353-363. https://doi.org/10.1016/j.inffus.2022.09.026

[79] A. Alsirhani, M. M. Alshahrani, A.M. Hassan, A.I. Taloba, R.M. Abd El-Aziz, A.H. Samak, "Implementation of African vulture optimization algorithm based on deep learning for cybersecurity intrusion detection. Alexandria Engineering Journal, 79, (2023) 105-115. https://doi.org/10.1016/j.aej.2023.07.077

[80] J. Lan, X. Liu, B. Li, J. Sun, B. Li, J. Zhao, MEMBER: A multi-task learning model with hybrid deep features for network intrusion detection. Computers & Security, 123, (2022) 102919. https://doi.org/10.1016/j.cose.2022.102919

[81] F.E. Ayo, S.O. Folorunso, A.A. Abayomi-Alli, A.O. Adekunle, J.B. Awotunde, Network intrusion

detection based on deep learning model optimized with rule-based hybrid feature selection. Information Security Journal: A Global Perspective, 29(6), (2020) 267-283. https://doi.org/10.1080/19393555.2020.1767240

[82] Z. Li, C. Huang, W. Qiu, An intrusion detection method combining variational auto-encoder and generative adversarial networks. Computer Networks, (2024) 110724. https://doi.org/10.1016/j.comnet.2024.110724

[83] S. Ur Rehman, M. Khaliq, S.I. Imtiaz, A. Rasool, M. Shafiq, A.R. Javed, Z. Jalil, A.K. Bashir, DIDDOS: An approach for detection and identification of Distributed Denial of Service (DDoS) cyberattacks using Gated Recurrent Units (GRU). Future Generation Computer Systems, 118, (2021) 453-466. https://doi.org/10.1016/j.future.2021.01.022

[84] A.F. Al-zubidi, A.K. Farhan, S.M. Towfek, Predicting DoS and DDoS attacks in network security scenarios using a hybrid deep learning model. Journal of Intelligent Systems, 33(1), (2024) 20230195. https://doi.org/10.1515/jisys-2023-0195

[85] P. Sun, P. Liu, Q. Li, C. Liu, X. Lu, R. Hao, J. Chen, DL-IDS: Extracting Features Using CNN-LSTM Hybrid Network for Intrusion Detection System. Security and communication networks, 2020(1), (2020) 8890306. https://doi.org/10.1155/2020/8890306

[86] S.S. Bamber, A.V.R. Katkuri, S. Sharma, M. Angurala, A hybrid CNN-LSTM approach for intelligent cyber intrusion detection system. Computers & Security, 148, (2025) 104146. https://doi.org/10.1016/j.cose.2024.104146

[87] D. Alghazzawi, O. Bamasag, H. Ullah, M. Z. Asghar, Efficient detection of DDoS attacks using a hybrid deep learning model with improved feature selection. Applied Sciences, 11(24), (2021) 11634. https://doi.org/10.3390/app112411634

[88] B. Deore, S. Bhosale, Hybrid optimization enabled robust CNN-LSTM technique for network intrusion detection. Ieee Access, 10, (2022) 65611-65622. https://doi.org/10.1109/ACCESS.2022.3183213

[89] J. Kaur, B.S. Khehra, A. Singh, Back propagation artificial neural network for diagnose of the heart disease. Journal of Reliable Intelligent Environments, 9(1), (2023) 57-85. https://doi.org/10.1007/s40860-022-00192-3

[90] A.S.A. Issa, Z. Albayrak, DDoS attack intrusion detection system based on hybridization of CNN and LSTM. Acta Polytechnica Hungarica, 20(2), (2023) 105-123. https://doi.org/10.12700/APH.20.2.2023.2.6

Authors Contribution Statement

G. Vidhya and M. Jagadheeswari both equally contributed and approved the final version of this manuscript.

Funding

The authors declare that no funds, grants or any other support were received during the preparation of this manuscript.

Competing Interests

The authors declare that there are no conflicts of interest regarding the publication of this manuscript.

Data Availability

The data supporting the findings of this study can be obtained from the corresponding author upon reasonable request.

Has this article screened for similarity?

Yes

About the License