A SURVEY OF AI METHODS FOR DETECTION OF DDoS ATTACKS ON NETWORKS

Abstract

This survey explores various artificial intelligence (AI) methods for detecting Distributed Denial of Service (DDoS) attacks on networks. It classifies these approaches into machine learning, deep learning, and other AI-based techniques, providing a comprehensive overview of current advancements in the field. Numerous research studies in the field of machine learning have evaluated DDoS attack detection performance using various datasets and techniques. Some noteworthy results are the supremacy of the J48 algorithm in SDN networks and the efficacy of the AdaBoost and Gradient Boost classifiers. In other investigations, Random Forest, Support Vector Machine, and Naive Bayes also showed excellent accuracy rates, up to 99.7%. To improve DDoS detection, deep learning techniques introduced autoencoders, hybrid models, and recurrent neural networks. These models achieved accuracy rates as high as 99.99%, frequently outperforming more conventional machine learning techniques. Enhanced detection rates were achieved by the utilization of a varied dataset in conjunction with deep-stacked autoencoders. Artificial intelligence methods such as Fuzzy Logic, Artificial Bee Colony, Ant Colony Optimization, and Whale Optimization Algorithm were used to identify DDoS assaults. These methods demonstrated high accuracy rates, efficient detection of various attack types, and improvements in reducing false positives; the integration of these techniques into intrusion detection systems offers a strong defense against dynamic DDoS threats. The overall survey highlights the effectiveness of AI techniques in DDoS attack detection across various methodologies.

Keywords: Algorithm, artificial intelligence, Denial of Service, Distributed Denial of Service, Malicious Traffic.

1. Introduction

In the constantly changing field of information technology, the growth of linked networks has made resource sharing and communication easier. Distributed Denial of Service (DDoS) assaults are among the most common and destructive types of cyber threats. Still, these networks' interconnection has also made them vulnerable to a wide range of security risks. The goal of denial-of-service (DDoS) assaults is to overload a target system or network with excessive traffic, making it unavailable to authorized users. The need to provide reliable and effective techniques for DDoS attack detection has grown as the frequency and sophistication of these attacks increase (Cisco, 2018). Artificial intelligence (AI) has become a powerful ally in the fight against denial-of-service (DDoS) assaults. AI can provide novel solutions that improve network security systems' detection and mitigation capabilities by utilizing machine learning, data analytics, and other AI approaches. The purpose of this review is to present a thorough analysis of the many AI techniques used to identify DDoS assaults on networks, emphasizing their advantages, disadvantages, and possible directions for further study (Karim, & Ge, 2017). Proactive security methods that can adjust to changing

attack patterns are essential due to the increasing complexity and scope of DDoS attacks. Although they can be somewhat successful, traditional rule-based and signature-based techniques frequently find it difficult to keep up with the changing nature of DDoS attacks. AI-driven methods, on the other hand, use machine learning algorithms to analyze massive volumes of network data in real-time and spot patterns and abnormalities that point to DDoS assaults. These AI techniques improve detection accuracy while also helping to lower false positives, which is important for preserving network service availability (Rass, & Mooney, 2007).

2. Background

Due to attackers' continuous adaptation and strategy improvement, the danger environment surrounding DDoS assaults is dynamic. Novel and complex DDoS assaults are sometimes difficult to spot using traditional signature-based detection techniques, which rely on predetermined patterns of existing attacks. Due to this constraint, methods must change to become more intelligent and adaptable, with AI technologies playing a key role. Since AI techniques like machine learning and deep learning are effective at extracting patterns and anomalies from massive datasets, they are a good fit for the dynamic and intricate nature of DDoS attacks (Bhatia *et al.*, 2018). Being able to differentiate between malicious and genuine traffic is a major difficulty when it comes to detecting DDoS attacks, especially in situations with large traffic volumes. After being trained on previous network data, machine learning algorithms are able to distinguish between abnormalities that might be signs of a DDoS assault and patterns associated with typical behavior. AI-based systems may continually grow and increase their detection accuracy over time because to this adaptive learning capability (Najar, 2024). Conventional detection techniques frequently fail to counteract the dynamic nature of DDoS threats. For example, signature-based strategies depend on established attack patterns, which leaves them vulnerable to new attack vectors and zero-day vulnerabilities. Herein lays the justification for investigating AI techniques, which exhibit the capacity to learn and adjust in real-time, providing a more proactive protection against the constantly changing strategies utilized by cyber attackers.

3. Artificial Intelligence in DDoS Attack Detection

Many AI methods that make use of various facets of machine learning and data analysis have been put forth and put into practice to detect DDoS assaults. Models for machine learning, such as Random Forests, Support Vector Machines (SVMs), and Neural Networks, have demonstrated potential in detecting patterns suggestive of DDoS attacks. Furthermore, anomaly detection algorithms, which are grounded on unsupervised learning seek to detect irregularities in network activity, offering a flexible and dynamic security system (Arshi *et al.*, 2020). AI methods, including Machine Learning (ML) and Deep Learning (DL), have drawn interest because to their capacity to evaluate large datasets, spot trends, and adjust to changing threats. Even in situations when traditional approaches are ineffective, these techniques can identify unusual activity suggestive of a DDoS assault (Ozkan *et al.*, 2024). Anomaly detection in network traffic analysis has been approached using machine learning methods including Support Vector Machines (SVM), Random Forests, and

Neural Networks. These algorithms can recognize departures from typical network activity that might indicate a DDoS assault by mastering usual patterns of behavior (Thwaini, 2022). Deep learning has shown potential in DDoS detection due to its autonomous learning of hierarchical characteristics from raw data. To extract complex patterns and temporal relationships in network traffic and increase detection accuracy, Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) have been used (Yuan *et al.*, 2017).

4. Related Works

The literature reviewed in this survey is organized into key approaches that have been employed in the detection of Distributed Denial of Service (DDoS) attacks on networks. These include the machine learning approach, deep learning approach, and artificial intelligence-based techniques. Each of these methodologies offers unique advantages in identifying and mitigating DDoS threats, as they leverage various algorithms and models to analyze network traffic patterns and detect anomalies indicative of attacks.

A. Machine learning approaches

Meti *et al.*, (2017) explored various AI methods for detecting DDoS attacks by applying machine learning algorithms such as Logistic Regression, Decision Tree, Random Forest, Ada Boost, Gradient Boost, K-Nearest Neighbors (KNN), and Naive Bayes to the CIC-DDoS2019 dataset. This dataset includes eleven distinct DDoS attacks with 87 features. Their study evaluated the performance of these classifiers using multiple metrics. Results demonstrated that AdaBoost and Gradient Boost provided superior classification performance, while Logistic Regression, KNN, and Naive Bayes were moderately effective. However, Decision Tree and Random Forest were shown to perform poorly in identifying DDoS attacks.

Zekri *et al.*, (2017) examined several machine learning algorithms, including J48, Random Forest (RF), Support Vector Machine (SVM), and K-Nearest Neighbors (K-NN), to detect and mitigate DDoS attacks in Software Defined Networks (SDN). They employed DDoS packet datasets consisting of ICMP and TCP floods to train and select optimal models for real-time implementation in a prevention script. The study demonstrated that J48 outperformed the other algorithms in terms of both training and testing time, highlighting its potential for effective DDoS attack detection in SDN environments.

Bindra & Sood (2019) sought to identify the most accurate machine learning algorithm for detecting DDoS attacks, focusing on the effectiveness of supervised learning models. Their analysis of the Random Forest Classifier yielded an accuracy rate exceeding 96%, confirmed using two metrics. The study underscored the strength of Random Forest in detecting DDoS attacks, while comparisons with other methods demonstrated that it provided more reliable performance when trained on actual datasets.

Wani *et al.*, (2019) investigated DDoS attacks in a cloud computing environment by applying machine learning techniques through an intrusion detection system (IDS) and utilizing the Tor Hammer tool to simulate attacks. The study introduced a new dataset and employed several classifiers, including Support Vector Machine, Random Forest, and Naive Bayes, achieving high classification accuracy rates of 99.7%, 97.6%, and 98.0%, respectively. These

results indicated the high effectiveness of machine learning approaches for DDoS detection in cloud environments.

Lima *et al.,* (2019) proposed a machine learning-based system to detect denial-of-service (DoS) attacks using four contemporary benchmark datasets. Their system inferred attack signatures from network traffic samples and achieved an online detection rate above 96%, with high precision and low false alarm rates. A key aspect of their approach was the use of a 20% sampling rate, which enabled effective real-time DDoS detection.

Tuan *et al.*, (2020) analyzed various machine learning methods for detecting Botnet-induced DDoS attacks, applying techniques such as Support Vector Machine (SVM), Artificial Neural Network (ANN), Naïve Bayes (NB), Decision Tree (DT), and Unsupervised Learning (USML) using datasets like UNBS-NB15 and KDD99. Their study revealed that the KDD99 dataset yielded better detection outcomes than UNBS-NB15, underscoring the importance of dataset selection in DDoS attack detection. Metrics such as Accuracy, Sensitivity, Specificity, and False Positive Rate (FPR) were used to assess the performance of these models, with results indicating that machine learning is crucial in enhancing DDoS detection in computer security.

Perez-Diaz *et al.,* (2020) employed six machine learning models, J48, Random Tree, REP Tree, Random Forest, Multi-Layer Perceptron (MLP), and Support Vector Machine (SVM) to train an intrusion detection system (IDS) using the DoS dataset from the Canadian Institute of Cybersecurity (CIC). Despite the challenges posed by low-rate DoS (LR-DoS) attacks, their approach achieved a detection rate of 95%, indicating the efficacy of the proposed machine learning models in detecting and mitigating DDoS attacks in network environments.

Sarraf (2020) examined a subset of the CICIDS2017 dataset, applying machine learning models such as Decision Tree and Support Vector Machine to detect DDoS attacks. Key features, including "Flow ID," "SYN Flag Cnt," and "Dst IP," were found to have the most significant impact on attack detection. The study achieved nearly 100% accuracy in classifying DDoS attacks, with Decision Tree slightly outperforming linear SVM in terms of overall classification performance.

Santos *et al.,* (2020) explored the use of machine learning algorithms SVM, MLP, Random Forest, and Decision Tree in categorizing DDoS attacks in a simulated SDN environment. By simulating DDoS attacks using the Scapy program, the study demonstrated that both Random Forest and Decision Tree achieved high accuracy and optimal processing times. The research also identified essential features for classifying various types of DDoS attacks, such as bandwidth, controller, and flow-table attacks, although some limitations were noted in detecting these attack types using a classifier.

Saini et al. (2020) proposed a machine learning-based approach for detecting and categorizing different network traffic flows, focusing on attacks like HTTP flood and SID DoS. The researchers employed the WEKA tool and compared machine learning models, with the J48 algorithm outperforming Random Forest and Naive Bayes in terms of accuracy. The study emphasized the importance of contemporary datasets and tools like WEKA in enhancing the detection capabilities for diverse DDoS attack types.

Miranda *et al.,* (2021) evaluated the performance of four machine learning

techniques Multinomial Naive Bayes (MNB), K-Nearest Neighbors (K-NN), Support Vector Machine (SVM), and Multi-Layer Perceptron (MLP) in detecting DDoS attacks. The study proposed a strategy that combined Euclidean Distance (ED), Fuzzy Logic (FL), and MLP, achieving F1-scores exceeding 98% for simulated traffic and nearly 100% for real traffic. However, the superior classification performance came at the cost of increased processing time, particularly for the MLP model, highlighting the trade-offs involved in using certain machine learning methods for DDoS attack detection.

Pande *et al.,* (2021) employed the WEKA tool to detect DDoS attacks using the NSL-KDD dataset. Their study applied the Random Forest algorithm to classify normal and attack samples, achieving an impressive classification accuracy of 99.76%. The study highlighted the reliability of Random Forest in detecting DDoS attacks in large-scale datasets.

B. Deep Learning Approaches

A recurrent deep neural network was designed by Yuan *et al.* (2017) in order to trace network attack activities and learn patterns from sequences of network traffic. The experimental results show that the designed model performs better than conventional machine learning models; in their research, they reduced the error rate from 7.517% to 2.103% in comparison with the conventional machine learning method in the larger data set.

An Intrusion Detection System (IDS) utilizing a mix of deep Autoencoders (AE) and the Random Forest (RF) machine-learning approach was presented by Shone et al. (2018). Experimental analyses were carried out with the KDD Cup '99 and NSL-KDD datasets for multiclass classification situations. When it came to evaluating the results, the models did rather well.

A very efficient two-stage model using deep-stacked Autoencoders (AE) was presented by Khan et al. (2019). The used datasets for the model's performance evaluation were UNSW-NB15 and KDD Cup'99. The attack class's Detection Rate (DR) efficiency was much improved by this dataset preparation, especially in situations when there were less training examples. Based on the simulation results, the authors suggested model was able to attain 99.996% accuracy for the KDD99 dataset and 89.134% accuracy for the UNSW-NB15 dataset.

Asad et al. (2020) presented a unique feed-forward back-propagation-based deep neural network-based detection technique that can effectively identify numerous application layer DDoS assaults. On the most recent dataset with a variety of DDoS attack types, the suggested neural network architecture can detect and utilize the most pertinent high level aspects of packet flows with an accuracy of 98%.

DDoSNet was a proposed intrusion detection system by Elsayed et al. (2020) that protects SDN environments from DDoS assaults. Their approach included an autoencoder with a recurrent neural network (RNN) and was based on the Deep Learning (DL) technology. The recently published dataset CICDDoS2019, which fills in the gaps in the current datasets and includes a wide range of DDoS assaults, was used to test their approach. They achieve a notable enhancement in attack identification when compared to alternative benchmarking techniques. As a result, their methodology

offered a high level of assurance about network security.

Al-Daweri *et al.*, (2020) conducted a thorough examination of the characteristics of the KDD99 and UNSW-NB15 datasets to determine their significance in their work on intrusion detection systems. They employed a discrete version of the cuttlefish method (D-CFA), a back-propagation neural network (BPNN), and rough-set theory (RST). The outcome of their experiment suggested that a classification accuracy of more than 84% might be attained by utilizing a few characteristics in the KDD99 dataset. Furthermore, it was discovered that a small number of characteristics from both datasets significantly improved the performance of the categorization. These features were included in a feature combination that produced a high accuracy; also, the features were regularly chosen by the authors during the feature selection procedure.

Using a sample of packets taken from network traffic, *Cil et al.*, (2021) employed a deep learning model based on the deep neural network (DNN) to identify DDoS assaults. The CICDDoS2019 dataset, which comprises the current DDoS attack types developed in 2019, was used for testing. The findings showed that attacks on network traffic were identified with 99.99% success rate and that the attack types were categorized with 94.57% accuracy rate. The deep learning model's excellent accuracy values demonstrate its efficacy in thwarting DDoS attacks.

In 2021, Ortet *et al.*, introduced CyDDoS, an integrated intrusion detection system (IDS) architecture that integrates a deep neural network with a collection of feature engineering methods. Five machine learning classifiers were utilized in the ensemble feature selection process to find and extract the most pertinent features for the prediction model. By analyzing only a subset of pertinent characteristics, this method reduced computing requirements and enhanced model performance. They used CICDDoS2019, a current and realistic dataset made up of DDoS and regular attack traffic, to assess the model's performance. One of the limitations of CyDDoS's technology is that it only detected DDoS assaults.

Shieh *et al.*'s (2021) investigation looked into how the OSR issue affected DDoS assault detection. They suggested a novel DDoS detection system using incremental learning, a Gaussian Mixture Model (GMM), and bi-directional long short-term memory (BI-LSTM) in answer to this issue. Traffic engineers classified and discriminated unknown traffic that the GMM had gathered, and then they put the data back into the framework as more training samples. The suggested BI-LSTM-GMM can achieve recall, precision, and accuracy up to 94%, according to experiment findings using the training, testing, and evaluation data sets CIC-IDS2017 and CIC-DDoS2019. This outcome showed that the suggested methodology may offer a useful way to identify DDoS assaults that aren't well-known.

In 2021, Gopalakrishnan *et al.*, presented a novel multistage model that uses Autoencoders (AE). Two stacked fully connected layers plus an Intrinsic Dimension (ID) convolution layer make up this model. The datasets from KDD Cup'99, UNSW-NB15, and CICIDS2017 were subjected to experimental assessments. The suggested approach outperformed several Deep Learning (DL) models in terms of

performance. Specifically, the MINDFUL (Auto-Encoder with 1D-CNN) model achieved 92.49% accuracy on the KDD Cup'99 dataset, 93.40% accuracy on the UNSW-NB15 dataset, and 97.90% accuracy on the CICIDS2017 dataset, outperforming NN, ANN, CNN, and CANN.

In order to successfully anticipate DDoS assaults utilizing benchmark data, Alghazzawi *et al.*, (2021) used a hybrid deep learning (DL) model, specifically a CNN with BiLSTM (bidirectional long/short-term memory). Only the most relevant aspects were selected for their investigation by rating and selecting those that had the greatest scores in the given data set. Results of the experiment showed that the CNN-BI-LSTM that was suggested was able to achieve up to 94.52 percent accuracy in training, testing, and validation using the CIC-DDoS2019 data set.

A "Long Short-Term Memory (LSTM)" based model was created by Kumar et al. (2023) to detect DDoS attacks on a sample of network traffic packets. being aware that an algorithm for feature selection and extraction is a part of the LSTM deep learning approach. Once trained, it updates itself; LSTM operates quickly and accurately even with fewer data points. The recommended LSTM model obtained an accuracy of up to 98 percent in their work using the "CICDDoS2019 dataset" for training and testing. Deep learning outperforms machine learning on the CICDDoS2019 dataset.

Ahmed *et al*., (2023) assessed the efficacy of metrics-based attack detection using actual weblogs (dataset), the CTU-13 dataset, and standard datasets in a multilayer perceptron (MLP) deep learning algorithm. The suggested MLP classification system has a 98.99% detection effectiveness for DDoS assaults, according to simulation findings. When compared to conventional classifiers such as Naïve Bayes, Decision Stump, Logistic Model Tree, Naïve Bayes Updateable, Naïve Bayes Multinomial Text, AdaBoostM1, Attribute Selected Classifier, Iterative Classifier, and OneR, the performance of the proposed technique yielded the lowest value of false positives, at 2.11%.

C. Artificial Intelligence Approach

Weller-Fahy *et al*., (2014) applied neural networks combined with the Bees Algorithm (BA) to detect Distributed Denial of Service (DDoS) attacks on networks. The BA was employed to train the neural network by learning attack patterns from the training dataset, and the system subsequently identified anomalous behaviors in real-time using a filtering decision method. The Desirable-Present (DP) detector was applied to model normal network behavior, while the Undesirable-Absent (UA) detector identified fresh intrusions as they emerged. Using the KDD'99 dataset, the proposed Intrusion Detection System (IDS) demonstrated high accuracy in identifying various attack types with a low false positive rate, highlighting the potential of neural networks in DDoS detection.

Aroora *et al*., (2015) developed an Ant-Based Routing Algorithm to detect DDoS attacks in wireless sensor networks. Their approach factored in node age, energy, and reliability, making it a novel contribution compared to earlier research that mainly focused on energy, hop, and distance. By considering these additional factors, the ant-based algorithm efficiently identified congestion in the network, which could be linked to DDoS attacks. This method enhanced the detection accuracy in wireless sensor networks by

addressing critical factors previously overlooked in DDoS detection.

In 2016, Chen *et al*. designed an LDDoS attack detection system using the Ant Colony Optimization (ACO) algorithm. This system was tested with DARPA and KDD repository datasets, and the simulation results demonstrated that the proposed DDIACS framework outperformed existing approaches. The adaptive metaheuristic algorithm was particularly effective in resisting LDDoS attacks, achieving an accuracy rate above 83% and a detection rate around 89%. The success of this method underscores the effectiveness of ACO in defending against DDoS attacks in network environments.

Sharma *et al.*, (2016) employed an artificial bee colony (ABC) algorithm to create an intrusion detection system aimed at identifying denial-of-service (DoS) attacks in cloud environments. By leveraging CloudSim's background traffic data, the swarm-based ABC algorithm was tested for its efficacy in detecting DoS attacks. The results indicated that this approach surpassed the quantum-inspired PSO algorithm, achieving detection rates of 72.4% and 68.3% in the ABC and PSO models, respectively. This finding solidifies the role of swarm intelligence in identifying DDoS attacks on cloud platforms.

Mondal *et al*., (2017) developed a fuzzy logic-based system to detect DDoS attacks in cloud computing environments. The fuzzy system proved to be effective at early-stage DDoS detection, reducing the attack's impact as it progressed over time. Their study proposed extending the fuzzy system by incorporating additional variables, which would improve the overall robustness and adaptability of the system. This approach provided a dynamic and reliable mechanism for safeguarding cloud infrastructures from DDoS threats.

Ali *et al*., (2018) integrated backpropagation artificial neural networks with the artificial bee colony (ABC) algorithm to create a hybrid method for detecting DDoS attacks in cloud computing. The ABC algorithm was responsible for selecting the initial weights and thresholds using the least mean square error, while the backpropagation network conducted the training. This hybrid approach improved both the speed and accuracy of detecting DDoS attacks, offering a significant improvement over existing techniques in cloud environments.

Seth & Chandra (2018) introduced the CDOSD model, a cloud-based DDoS attack detection system that used a binary version of the Artificial Bee Colony Optimization (BABCO) algorithm combined with a decision tree (DT) classifier. By constructing a custom DOS dataset in a private cloud, they demonstrated that CDOSD achieved high accuracy in detecting DDoS attacks while maintaining a low false positive rate. BABCO reduced the dataset's dimensionality, allowing for more efficient training and classification. This approach outperformed existing models, offering a promising solution for cloud-based DDoS detection.

Yu *et al*., (2019) implemented an intelligent bee colony algorithm to develop a system for DDoS detection. By combining traffic reduction techniques with swarm intelligence, the system reduced network traffic while detecting DDoS attacks more effectively. Using traffic feature distribution entropy and probability comparison discrimination factors, the system achieved higher accuracy and reduced time consumption compared to traditional algorithms. This method illustrates the

potential of integrating swarm intelligence with traffic reduction algorithms for efficient DDoS detection.

Ateş *et al.*, (2020) employed fuzzy clustering to classify traffic and identify potential DDoS attacks by examining the relationship between IP addresses and port numbers. Their method modeled attack and non-attack traffic using a fuzzy relevance function, which was tested on real data from Boğaziçi University. This approach improved DDoS detection accuracy by addressing traffic uncertainty, making it an effective solution for real-world DDoS detection in network environments.

Ravi *et al.*, (2021) applied the Whale Optimization Algorithm (WOA) for feature reduction in detecting DDoS attacks. The algorithm optimized the selection of features from the CICDDoS2019 dataset, reducing the number from 80 to 11 without sacrificing accuracy. The experiment showed that the Random Forest classifier achieved a detection accuracy of 99.94% after feature reduction, compared to 99.92% with the full feature set. This work demonstrated that WOA can effectively reduce computational complexity while maintaining high detection accuracy for DDoS attacks.

Abdulkareem & Zeebaree (2022) explored the Whale Optimization Algorithm (WOA) for improving load balancing in the context of DDoS attack prevention. They compared WOA with Round-Robin, Particle Swarm Optimization (PSO), and Genetic Algorithms (GA), showing that WOA performed better in terms of response time and traffic management. By distributing client requests evenly across servers, WOA enhanced the system's resilience against DDoS attacks, making it a valuable tool for mitigating unexpected traffic surges.

Table 1. Summary of Machine Learning Approaches

Author/Year	Dataset	Method	Result
Meti et al. (2017)	CIC-DDoS2019 dataset	Logistic Regression, Decision Tree, Random Forest, Ada Boost, Gradient Boost, KNN, and Naive Bayes	AdaBoost and Gradient Boost perform the best in terms of classification; Logistic Regression, KNN, and Naive Bayes perform well; while Decision Tree and Random Forest perform poorly
Zekri et al. (2017)	DDoS packets (ICMP and TCP floods) dataset	J48, Random Forest (RF), Support Vector Machine (SVM), and K-Nearest Neighbors (K-NN)	The outcomes demonstrated that J48 outperforms the other algorithms under evaluation, particularly when it comes to training and testing time
Bindra & Sood (2019)	Actual datasets	Random Forest Classifier	They confirmed their results using two metrics and attained an accuracy rate of over 96%
Wani et al. (2019)	Developed a new dataset	Support Vector Machine, Random Forest, and Naive Bayes	The total accuracy of this study was 99.7%, 97.6%, and 98.0% for Support Vector Machine, Random Forest, and Naive Bayes, respectively
Lima et al. (2019)	Four contemporary benchmark datasets	Machine learning (ML) based DoS detection system	The results demonstrate an online detection rate (DR) of attacks above 96%, with high precision (PREC) and low false alarm rate (FAR) using a sampling rate (SR) of 20% of network traffic
Tuan et al. (2020)	UNBS-NB 15 and KDD99	Support Vector Machine (SVM), Artificial Neural Network (ANN), Naïve Bayes (NB), Decision Tree (DT), and Unsupervised Learning (USML) (K-means, X-means)	It was demonstrated through experimentation that the KDD99 dataset performs better than the UNBS-NB 15 dataset.
Perez-Diaz et al. (2020)	DoS dataset from the Canadian Institute of Cybersecurity (CIC)	J48, Random Tree, REP Tree, Random Forest, Multi-Layer Perceptron (MLP), and Support Vector Machines (SVM)	The evaluation's results showed that their strategy produced a 95% detection rate.

Sarraf, (2020)	A subset of the CICIDS2017 dataset	Decision tree and linear support vector machines	The decision tree models outperformed linear support vector machines by a little margin
Santos et al.(2020)	A list of legitimate IP addresses	SVM, MLP, Random Forest, and Decision Tree	Study identified the key characteristics for categorizing denial-of-service (DDoS) assaults
Saini et al. (2020)	A novel dataset containing a blend of contemporary attack types, including HTTP flood, SID DoS, and regular traffic	J48 algorithm, Random Forest and Naïve Bayes	J48 algorithm outperformed the Random Forest and Naïve Bayes algorithms in terms of outcomes
Miranda et al. (2021)	Real traffic datasets	Multinomial Naive Bayes (MNB), K-Nearest Neighbors (K-NN), Support Vector Machine (SVM), and Multi-Layer Perceptron (MLP) neural network with backpropagation	better performance of the approach based on FL, MLP and ED was obtained at the cost of larger execution time, since MLP required 0.74 ms and 0.87 ms for classification of the emulated and real traffic datasets
Pande et al. (2021)	NSL-KDD dataset	Random Forest	In 99.76% of the samples, the classification was accurate

Table 2. Summary of Related Works on Deep Learning Approach

Author/Year	Dataset	Method	Result
Yuan et al. (2017)	Network traffic larger data set	Recurrent deep neural network	Performs better than conventional machine learning models; in their research, they reduced the error rate from 7.517% to 2.103% in comparison with the conventional machine learning method
Shone et al. (2018)	KDD Cup '99 and NSL-KDD datasets	Deep Autoencoders (AE) and the Random Forest (RF) machine-learning approach	When it came to evaluating the results, the models did rather well

Khan et al. (2019)	UNSW-NB15 and KDD Cup'99	Deep-stacked Autoencoders (AE)	Model was able to attain 99.996% accuracy for the KDD99 dataset and 89.134% accuracy for the UNSW-NB15 dataset
Asad et al. (2020)	Most recent dataset with a variety of DDoS attack types	Unique feed-forward back-propagation-based deep neural network	The proposed neural network architecture can detect and utilize the most pertinent high-level aspects of packet flows with an accuracy of 98%
Elsayed et al. (2020)	CICDDoS2019 dataset	Autoencoder with a recurrent neural network (RNN)	They achieve a notable enhancement in attack identification when compared to alternative benchmarking techniques
Al-Daweri et al. (2020)	KDD99 and UNSW-NB15 datasets	Cuttlefish method (D-CFA), a back-propagation neural network (BPNN), and rough-set theory (RST)	Their experiment acheived a classification accuracy of more than 84%, it was discovered that a small number of characteristics from both datasets significantly improved the performance of the categorization
Cil et al. (2021)	CICDDoS2019 dataset	Deep neural network (DNN)	The findings showed that attacks on network traffic were identified with 99.99% success rate and that the attack types were categorized with 94.57% accuracy rate
Ortet et al. (2021)	CICDDoS2019 dataset	Deep neural network	This method reduced computing requirements and enhanced model performance
Shieh et al.'s (2021)	CIC-IDS2017 and CIC-DDoS2019 dataset	Incremental learning, a Gaussian Mixture Model (GMM), and bi-directional long short-term memory (BI-LSTM)	This outcome showed that the suggested methodology offered a useful way to identify DDoS assaults that aren't well-known
Gopalakrishnan et al. (2021)	KDD Cup'99, UNSW-NB15, and CICIDS2017 dataset	Autoencoders (AE)	MINDFUL (Auto-Encoder with 1D-CNN) model achieved 92.49% accuracy on the KDD Cup'99 dataset, 93.40% accuracy on the UNSW-NB15 dataset, and 97.90% accuracy on the CICIDS2017 dataset, outperforming NN, ANN, CNN, and CANN

Alghazzawi et al. (2021)	CIC-DDoS2019 data set	ybrid deep learning (DL) model, specifically a CNN with BiLSTM (bidirectional long/short-term memory)	CNN-BI-LSTM that was suggested was able to achieve up to 94.52 percent accuracy in training, testing, and validation
Kumar et al. (2023)	CICDDoS2019 dataset	Long Short-Term Memory (LSTM)	The recommended LSTM model obtained an accuracy of up to 98 percent in their work using the "CICDDoS2019 dataset" for training and testing
Ahmed et al. (2023)	Actual weblogs (dataset), the CTU-13 dataset, and standard datasets	Multilayer perceptron (MLP) deep learning algorithm	MLP classification system has a 98.99% detection effectiveness for DDoS assaults, according to simulation findings

Table 3. Summary of Related Works Using Artificial Intelligence Approach

Author/Year	Dataset	Method	Result
Weller-Fahy et al., (2014)	KDD'99 dataset	Bees Algorithm (BA)	The trials demonstrated the effective use of the suggested method, which can identify a wide variety of incursion types with a low false positive rate.
Aroora et al. (2015)	KDD'99 dataset	Ant-Based Routing Algorithm	An ant-based routing method that takes into account age, energy, and reliability was successfully implemented
Chen et al. (2016)	DARPA and KDD repository datasets	Ant Colony Optimization Algorithms	The adaptive metaheuristic algorithm beats other ways in resisting an LDDoS assault. The accuracy was higher than 83% and the detection rate was around 89%.
Sharma et al. (2016)	Data generated by CloudSim's background traffic	Artificial bee colony	The results show that the strategy is effective in combating these types of attacks. When their method was contrasted with quantum-inspired PSO, it was discovered to be superior. The testing and training data sets yielded 72.4 and 68.3% of the desired outcomes for ABC and QPSO
Mondal et al. (2017)	KDD repository datasets	Fuzzy logic	Employed fuzzy logic to safeguard the cloud environment

Ali et al. (2018)		A hybrid strategy (backpropagation artificial neural networks with artificial bee colonies)	It improved the DDoS attack detection process's speed and precision
Seth & Chandra (2018)	DOS cloud dataset in a private cloud environment	Artificial bee colony optimization (BABCO) and a decision tree (DT) classifier	BABCO considerably reduced the dataset's characteristics and offered a low-dimensional computing space for training and classification.
Yu et al. (2019)	Real-world data	Intelligent bee colony algorithm	The demand for traffic detection in this system was significantly reduced
Ateş et al., (2020)	Real data collected from Boğaziçi University network	Fuzzy clustering	This algorithm was tested as it performed relatively well
Ravi et al. (2021)	CICDDOD2019 dataset	Whale optimization method for feature reduction	Random forest yielded the greatest accuracy of 99.94%, whereas the accuracy of the complete feature was measured at 99.92%.
Abdulkareem, & Zeebaree, (2022)	DARPA	Whale Optimization Algorithm (WOA), Round-Robin (RR), Particle Swarm Optimization (PSO), and Genetic Algorithms (GA)	The whale optimization algorithm can prevent unexpected traffic and block the regular operation of Internet websites by providing a proper plan for distributing requests between servers and reducing the average response speed.

5. Challenges and Open Issues

Despite the potential benefits, the adoption of AI methods for DDoS detection poses the following challenges among many others:

a. Adversarial Attacks and Evasion Techniques: DDoS attackers employ adversarial attacks to manipulate input data and trick AI-based detection systems. Therefore, developing robust models that can resist adversarial attacks and evasion techniques is a critical challenge.
b. Dynamic and Evolving Attack Patterns: DDoS attack patterns are in constant change, making it challenging for static AI models to adapt. There is a need for dynamic and adaptive AI models that can learn and update their knowledge to effectively detect new and emerging DDoS attack strategies.
c. Handling Encrypted Traffic**:** DDoS attacks are increasingly utilizing encrypted traffic to evade detection. Developing AI models capable of analyzing encrypted traffic without compromising user privacy is a significant challenge that needs to be addressed.
d. Interoperability with Existing Security Infrastructure: Integrating AI-based DDoS detection systems with existing security infrastructure and protocols can be a complex task. Ensuring seamless interoperability and compatibility with diverse network environments, firewalls, and intrusion prevention systems is a current challenge.

6. Conclusion

Based on the review conducted in this study, deep learning techniques especially those that use autoencoders, recurrent neural networks, and LSTM-based models perform better than more conventional machine learning techniques. Higher accuracy rates are demonstrated by these deep learning models, which are especially useful in managing intricate and dynamic DDoS assault patterns. Using hybrid models, which fuse machine learning and deep learning methods, also improves detection performance. Innovative solutions are provided by artificial intelligence techniques, such as neural networks trained on bio-inspired algorithms like Ant Colony Optimization and Bees Algorithm. These methodologies exhibit the potential to detect an extensive array of threats with minimal false positive rates, showcasing the versatility of bio-inspired optimization methods in augmenting intrusion detection systems. This extensive survey reveals how useful AI methods are for identifying and classifying DDoS assaults, particularly deep learning models. The results underscore the ongoing development and modification of AI-driven techniques to tackle the ever-changing DDoS attacks, resulting in enhanced precision, effectiveness, and durability in preserving network security. Findings from this survey have also revealed how crucial it is to use cutting-edge AI algorithms for reliable and effective DDoS attack detection, as this lays the groundwork for further advancements in cyber security.

Disclaimer (Artificial intelligence)

Option 1:

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.

Option 2:

Author(s) hereby declare that generative AI technologies such as Large Language Models, etc. have been used during the writing or editing of manuscripts. This explanation will include the name, version, model, and source of the generative AI technology and as well as all input prompts provided to the generative AI technology

Details of the AI usage are given below:

1.

2.

3.

References

Abdulkareem, N. M., & Zeebaree, S. R. (2022). Optimization of load balancing algorithms to deal with ddos attacks using whale optimization algorithm. *Journal of Duhok University*, *25*(2), 65-85.

Ahmed, S., Khan, Z. A., Mohsin, S. M., Latif, S., Aslam, S., Mujlid, H., ... & Najam, Z. (2023). Effective and Efficient DDoS Attack Detection Using Deep Learning Algorithm, Multi-Layer Perceptron. *Future Internet*, *15*(2), 76.

Al-Daweri, Muataz & Zainol Ariffin, Khairul Akram & Abdullah, Salwani & Senan, Mohamad. (2020). An analysis of the KDD99 and UNSW-NB15 datasets for the intrusion detection system. Symmetry. 12. 1666. 10.3390/sym12101666.

Alghazzawi, D., Bamasag, O., Ullah, H., & Asghar, M. Z. (2021). Efficient detection of DDoS attacks using a hybrid deep learning model with improved feature selection. *Applied Sciences*, *11*(24), 11634.

Ali, U., Dewangan, K. K., & Dewangan, D. K. (2018). Distributed denial of service attack detection using ant bee colony and artificial neural network in cloud computing. In *Nature Inspired Computing: Proceedings of CSI 2015* (pp. 165-175). Springer Singapore.

Aroora, N., Junaeja, D., & Bannsal, S. (2015). An Ant-Based Routing Algorithm for Detecting Attacks in Wireless Sensor Networks.

Arshi, M & Nasreen, MD & Karanam, Madhavi. (2020). A Survey of DDOS Attacks Using Machine Learning Techniques. E3S Web of Conferences. 184. 01052. 10.1051/e3sconf/202018401052.

Asad, M., Asim, M., Javed, T., Beg, M. O., Mujtaba, H., & Abbas, S. (2020). Deepdetect: detection of distributed denial of service attacks using deep learning. *The Computer Journal*, *63*(7), 983-994.

Ateş Ç., S. Özdel and E. Anarim, (2020). "DDoS Detection Algorithm Based on Fuzzy Logic," *28th Signal Processing and Communications Applications Conference (SIU)*, Gaziantep, Turkey, 2020, pp. 1-4, doi: 10.1109/SIU49456.2020.9302139.

Bhatia, Sajal & Behal, Sunny & Ahmed, Irfan. (2018). Distributed Denial of Service Attacks and Defense Mechanisms: Current Landscape and Future Directions. 10.1007/978-3-319-97643-3_3.

Bindra, N., & Sood, M. (2019). Detecting DDoS attacks using machine learning techniques and contemporary intrusion detection dataset. *Automatic Control and Computer Sciences*, *53*, 419-428.

Chen, H. H., & Huang, S. K. (2016). LDDoS Attack Detection by Using Ant Colony Optimization Algorithms. *Journal of Information Science & Engineering*, *32*(4).

Cil, A. E., Yildiz, K., & Buldu, A. (2021). Detection of DDoS attacks with feed forward based deep neural network model. *Expert Systems with Applications*, *169*, 114520.

Cisco. (2018). Cisco 2018 Annual Cybersecurity Report. Retrieved from https://www.cisco.com/c/en/us/products/security/annual-cybersecurity-report-2018/index.html

Elsayed, M. S., Le-Khac, N. A., Dev, S., & Jurcut, A. D. (2020). Ddosnet: A deep-learning model for detecting network attacks. In *2020 IEEE 21st International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)* (pp. 391-396). IEEE.

Gopalakrishnan, Mahalakshmi & Elangovan, Uma & M, Aroosiya & M, Vinitha. (2021). Intrusion Detection System Using Convolutional Neural Network on UNSW NB15 Dataset. 10.3233/APC210116.

Karim, A., & Ge, X. (2017). A survey of big data architectures and machine learning algorithms in healthcare. Journal of King Saud University - Computer and Information Sciences.

Khan, Farrukh & Gumaei, Abdu & Derhab, Abdelouahid & Hussain, Amir. (2019). A Novel Two-Stage Deep Learning Model for Efficient Network Intrusion Detection. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2899721.

Kumar, D., Pateriya, R. K., Gupta, R. K., Dehalwar, V., & Sharma, A. (2023). DDoS Detection using Deep Learning. *Procedia Computer Science*, *218*, 2420-2429.

Lima Filho, F. S. D., Silveira, F. A., de Medeiros Brito Junior, A., Vargas-Solar, G., & Silveira, L. F. (2019). Smart detection: an online approach for DoS/DDoS attack detection using machine learning. *Security and Communication Networks*, *2019*, 1-15.

Meti, N., Narayan, D. G., & Baligar, V. P. (2017). Detection of distributed denial of service attacks using machine learning algorithms in software defined networks. In *2017 international conference on advances in computing, communications and informatics (ICACCI)* (pp. 1366-1371). IEEE.

Miranda de Rios, V., Inácio, P. R., Magoni, D., & Freire, M. M. (2021). Detection of reduction-of-quality DDoS attacks using Fuzzy Logic and machine learning algorithms. *Computer Networks*, *186*, 107792.

Mondal H. S., M. T. Hasan, M. B. Hossain, M. E. Rahaman and R. Hasan, (*2017*). "Enhancing secure cloud computing environment by Detecting DDoS attack using fuzzy logic," *3rd International Conference on Electrical Information and Communication Technology (EICT)*, Khulna,

Bangladesh, 2017, pp. 1-4, doi: 10.1109/EICT.2017.8275211.

Najar, A. A. (2024). Cyber-Secure SDN: A CNN-Based Approach for Efficient Detection and Mitigation of DDoS Attacks. *Computers & Security*, 103716.

Ortet Lopes, I., Zou, D., Ruambo, F. A., Akbar, S., & Yuan, B. (2021). Towards effective detection of recent DDoS attacks: A deep learning approach. *Security and Communication Networks*, *2021*, 1-14.

Ozkan Okay, Merve & Akin, Erdal & Aslan, Ömer & Kosunalp, Selahattin & Iliev, Teodor & Stoyanov, Ivaylo & Beloev, Ivan. (2024). A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. IEEE Access. PP. 10.1109/ACCESS.2024.3355547.

Pande, S., Khamparia, A., Gupta, D., & Thanh, D. N. (2021). DDOS detection using machine learning technique. In *Recent Studies on Computational Intelligence: Doctoral Symposium on Computational Intelligence (DoSCI 2020)* (pp. 59-68). Springer Singapore.

Perez-Diaz, J. A., Valdovinos, I. A., Choo, K. K. R., & Zhu, D. (2020). A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning. *IEEE Access*, *8*, 155859-155872.

Rass, S., & Mooney, P. (2007). Artificial Immune Systems for Intrusion Detection: A Brief Overview and Recent Advances. Artificial Intelligence Review, 27(1), 1-18.

Ravi Kiran Varma, P., Subba Raju, K. V., & Ruthala, S. (2021). Application of whale optimization algorithm in DDOS attack detection and feature reduction. In *Inventive Computation and Information Technologies: Proceedings of ICICIT 2020* (pp. 93-102). Springer Singapore.

Saini, P. S., Behal, S., & Bhatia, S. (2020). Detection of DDoS attacks using machine learning algorithms. In *2020 7th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 16-21). IEEE.

Santos, R., Souza, D., Santo, W., Ribeiro, A., & Moreno, E. (2020). Machine learning algorithms to detect DDoS attacks in SDN. *Concurrency and Computation: Practice and Experience*, *32*(16), e5402.

Sarraf, S. (2020). Analysis and detection of ddos attacks using machine learning techniques. *Am. Sci. Res. J. Eng. Technol. Sci*, *66*(1), 95-104.

Seth, J. K., & Chandra, S. (2018). An effective DOS attack detection model in cloud using artificial bee colony optimization. *3D Research*, *9*, 1-13.

Sharma, S., Gupta, A., & Agrawal, S. (2016). An intrusion detection system for detecting denial-of-service attack in cloud using artificial bee colony. In *Proceedings of the International Congress on Information and Communication Technology: ICICT 2015, Volume 1* (pp. 137-145). Springer Singapore.

Shieh, C. S., Lin, W. W., Nguyen, T. T., Chen, C. H., Horng, M. F., & Miu, D. (2021). Detection of unknown ddos attacks with deep learning and gaussian mixture model. *Applied Sciences*, *11*(11), 5213.

Shone, Nathan & Tran Nguyen, Ngoc & Vu Dinh, Phai & Shi, Qi. (2018). A Deep Learning Approach to Network Intrusion

Detection. IEEE Transactions on Emerging Topics in Computational Intelligence. 2. 41-50. 10.1109/TETCI.2017.2772792.

Thwaini, Mohammed. (2022). Anomaly Detection in Network Traffic using Machine Learning for Early Threat Detection. Data and Metadata. 1. 34. 10.56294/dm202272.

Tuan, T. A., Long, H. V., Son, L. H., Kumar, R., Priyadarshini, I., & Son, N. T. K. (2020). Performance evaluation of Botnet DDoS attack detection using machine learning. *Evolutionary Intelligence*, *13*, 283-294.

Wani, A. R., Rana, Q. P., Saxena, U., & Pandey, N. (2019). Analysis and detection of DDoS attacks on cloud computing environment using machine learning techniques. In *2019 Amity International conference on artificial intelligence (AICAI)* (pp. 870-875). IEEE.

Weller-Fahy, D. J., Borghetti, B. J., & Sodemann, A. A. (2014). A survey of distance and similarity measures used within network intrusion anomaly detection. *IEEE Communications Surveys & Tutorials*, *17*(1), 70-91.

Yu, X., Han, D., Du, Z., Tian, Q., & Yin, G. (2019). Design of DDoS attack detection system based on intelligent bee colony algorithm. *International Journal of Computational Science and Engineering*, *19*(2), 223-232.

Yuan, X., Li, C., & Li, X. (2017). DeepDefense: identifying DDoS attack via deep learning. In *2017 IEEE international conference on smart computing (SMARTCOMP)* (pp. 1-8). IEEE.

Yuan, Xiaoyong & Li, Chuanhuang & Li, Xiaolin. (2017). DeepDefense: Identifying DDoS Attack via Deep Learning. 1-8. 10.1109/SMARTCOMP.2017.7946998.

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