IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Machine Learning-Based Detection of Distributed Denial of Service (DDoS) Attacks Using CICIDS Dataset

Roshan Thapa Magar
Research Scholar
Department of CSE
Quantum University, Roorkee

Md Iqbal
Professor
Department of CSE
Quantum University, Roorkee

Abstract:
DDoS attacks are increasingly sophisticated, cybersecurity is a major concern for the safety of the contemporary world, making refined and customizable detection mechanisms a requirement. This study will employ 5 machine learning algorithms – Random Forest, Support Vector Machine (SVM), decision tree model, K-Nearest Neighbors (K-NN) and the logistic regression model in analyzing CICIDS 2017 dataset on which algorithms is best suited to detect the DDoS attack. It was found that important features such as flow duration, packet size, and protocols (type) and TCP flags were extracted and normalised to enhance the performance of the model. The model was assessed based on the accuracy, precision, recall and F1-score. The best performance obtained from all the testing algorithms models was presented by the Random Forest model, with an accuracy of 95.1 % of the results of malicious traffic detection, precision 94.3 %, overall 95.5 % round as well as 94.9 % F1-score, making the Random Forest model strong, reliable in the terms of any detections of the malicious traffic. The findings can emphasize on the efficiency of ensemble approach in minimising threats against the network and thus they can provide substantial reference of how intelligent cybersecurity solutions can be put into practice, in psuedo-real time scenarios Moreover, the paper also mentions the obstacles and limitations to the models like scalability weaknesses, overhead efficiency, and flexibility to new patterns of attacks, thereby indicating the future experimentation with resource-friendly and hybrid detection models.

Keywords: DDoS, Machine Learning, SVM, Random Forest, KNN, Logistic Regression

Introduction

Growing complexity and frequency of Distributed Denial of Service (DDoS) attacks create major headaches to the security of networks, and affect big enterprise networks as well as small web services fronts. Such attacks, which usually inundate the network or servers of a target with an excess flow of traffic, could lead to serious damage to online services and data protection. As a method of fighting with this increasing threat, Artificial Intelligence (AI) and machine learning (ML) have become essential to increase DDoS detection and mitigation processes. Studies have already confirmed that AI-powered models, such as deep learning algorithms and conventional ML approaches could detect assault patterns with a high level of precision, frequently exceeding typical defense tactics [1].

The recent literature reviews have emphasized on the effectiveness of the different AI models as real-time DDoS detectors. As an example, Random Forest has been observed to have outstanding accuracy levels with one literature disclosing an accuracy percentage of 99.99 in terms of detection. Machine learning methods, namely Support Vector Machine (SVM) and K-Nearest Neighbors (K-NN), have also been discussed in

several studies because they are adaptive to the changing network situations and attacks types [2]. But even with these developments, difficulties remain to address the very changing face of the cyber threats and the models that will be able to scale with the increasing complexity of the internet traffic.

In the DDoS protection, cloud computing environments, especially due to built-in scalability, are being used more and more, including AI-powered algorithms, with which the detection and response rates were speeded up [3]. In addition, hybrid models proposed to use deep learning and traditional machine learning methods in combination with each other in order to ensure more accurate detection and reduce false positives have been proposed. These methods are expected to be easily inserted into the already established security systems and offer powerful defence mechanism without creating a large burden on the resources [4].

The implementation of AI in cybersecurity also resulted in the study of new defense mechanisms in form of reinforcement learning and federated learning, which are decentralized methods of preventing DDoS attacks using various nodes within a network [5]. These models however are not undisputed. As an illustration, some deep learning methods are expensive in terms of computing resources and the question of explainability of the complex models is also a major challenge towards large scale implementation of the methods in real time networks [6].

The proposed research will respond to these challenges as it is interested in examining how AI and machine learning models can be utilized to detect DDoS attacks and how precision, scalability, and efficiency of the systems can be improved [7]. Through the application of the developed methodologies and experimenting with them in practice, the paper will offer the general picture of the existing strategies employing AI and will suggest innovative ways of enhancing the opportunities of DDoS detection [8]. By considering the nature of datasets, model, and other issues, this paper tries to assist in creating more robust protective mechanisms towards cybersecurity threats and the changing nature of attacks on networks [9].

Literature Survey:

Following survey has been done to get scientific precision values.

The paper explores AI frameworks of real-time detection of DDoS attacks to be able to estimate the accuracy of detection of random forest, decision tree, CNN, NGBoosT, and SGD models and was found that the most accurate detection model of 99.9974% is random forest, and it makes the network and confidential data safe and secure [10]. The study investigates the use of AI in tracing and countering the DDoS attacks by using the information technology results of machine learning and data analytics, as well as the AI-powered automated attack detection solutions to help make the networks more resistant to attacks of this type [11]. In the study, the dynamic and scalable characteristics of cloud computing are utilised to deploy an effective defence configuration against DDoS attacks and have the potential to conduct analysis in real time thus providing rapid counter measures against new threats [12].

This review paper studies the AI use in mitigation of DDoS attacks, summarizing the existing body of research on machine learning, deep learning, and heuristic approaches, as well as their possible combination with conventional security measures to strengthen the defensive side of cybersecurity against dynamic threats [13]. In the present paper, AI in network security is being addressed with the help of AI algorithms, machine learning and anomaly detection in order to improve network security, the mitigation of cyber threats, and the response to incidents in DDoS attacks based on concrete implementations and real-life use cases [14]. The present study suggests an AI-based approach of identifying and avoiding Distributed Denial of Service (DDoS) attacks through a deep learning architecture composed of LSTM and max pooling layers, having an accuracy of 99.58 percent in identifying and stopping such cyber menace [15].

This paper suggests a machine learning model that can identify DDoS attacks with accuracy of 98%, response time of 2 seconds, false positives dropped by 40 percent and it can be scaled in case of new types of attacks and different networks [16]. This research paper is using deep learning models, LSTM and CNN, to create sophisticated detection system to detect and stop DoS/DDoS attacks, and increase network survivability to cyberthreats and refine cybersecurity[17]. An innovative, multi-agent, blockchain-based reinforcement learning (RL) cyber-defense-based system with smart-contract-enabled functionality that has the potential to result in a reduction of a network-level service-outage impact [18].

This study suggests a hybrid GRU-NTM deep learning model to identify intelligent DoS and DDoS on 99 percent accuracy on UNSW-NB15 databases and BoT-IoT with long-term ability to recognize patterns, and has real-time capability, to improve network security [19]. An intrusive version of deep learning succeeds in detecting and preventing the DDoS attack in cloud environment based on time series classifications and deep neural networks. The approach is accurate, has minimal false positives and is quick. It attains a 99.98 accuracy with minimal false positive [20]. In their study, they have suggested an OpenFlow-based DDoS detection scheme in SDN networks, and adopted deep learning model to capture 99.4percent accuracy, utilising a dataset that is special in terms of its characteristics to quell Distributed Denial of Service attacks in Software Defined Networks [21].

The proposed paper uses machine learning techniques (Random Forest model, Decision Tree Model, Xgboost) to calculate four types of distributed-denial-of-service attacks with 99.99 percentage of accuracy on the ALDDoS dataset and prevents network disruptions that occur when web services or servers are attacked by distributed-denial-of-service attacks [22]. This paper suggests the use of deep learning tools to identify a Distributed Denial of Service (DDoS) attack by designing a neural network model to analyze and classify the possible attack on a computer network through both the autoencoders and the KDD dataset [23]. The proposed approach has achieved a result of 99.6 % and 97.7 % accuracy of DoS/DDoS attack detection in Bayesian Regularization and scaled conjugate gradient descent respectively [24].

To achieve this they propose a deep learning strategy to detect DDoS attacks at application layer by using an auto encoder to select the features and deep neural networks to classify the attacks with the highest accuracy rate in the literature reviewed so far [25]. The experimental results demonstrate that the proposed technique would easily get an accuracy of 96.7% and it is the most preferable form to be used in the application of detecting breaches [26].

The study offers a closely watched machine learning-based and voting method, IDDOSAD, to understand the Distributed Denial of Service (DDoS) retreat, where the schemes demonstrated 92-100% accuracy on a 11,423 entries data set, which is valuable in protecting the communication systems against the increasing cybersecurity risk [27]. In this work, the authors propose an unsupervised AutoML approach called AUTO-SEE, which develops new features and selects the best models and can predict DDoS attacks with a maximum of 44.15 percent error cancellation and 72.41 percent-100 percent accuracy, since labeled data are not used [28].

This study explores the potential of a Deep Neural Network (DNN) to detect Distributed Denial of Service (DDoS) attacks, achieving a 99.39% testing accuracy using the CICDDoS2019 benchmark dataset, outperforming existing machine learning models and data mining techniques [29]. A novel DDoS attack detection mechanism based on federated learning with dynamic thresholds for variable rate attacks is proposed. The method achieves high accuracy in detecting regular Benign traffic and significantly improves detection accuracy for burst and sustained attacks. Achieves 99.83% accuracy in detecting benign traffic. Improves detection accuracy for 10 DDoS attack types. Maintains over 90% accuracy in sustained attack scenarios [30].

Table 1: Comparison among different techniques

Author(s)	AI Model(s)	Accuracy	Dataset	Limitations
S. Ahmadi [10]	Random Forest, Decision Tree, CNN, NGBoost, SGD	99.99%	Not Specified	Dataset not disclosed, potential overfitting
S. Hamad et al. [11]	Various ML models	Not specified	Not Specified	General study, lacks implementation details
S. Polu and V. Bapuji [12]	ML algorithms in cloud	Real-time	Cloud Data	Real-time performance metrics not fully evaluated
N. A. Mohamed [13]	ML, DL, heuristic methods	Not specified	Multiple	Integration with traditional methods underexplored
R. Khanna [14]	AI-based anomaly detection	Not specified	Real-world	Focused on review and case studies
A. ALDabbas et al. [15]	Deep Learning (LSTM + Max Pooling)	99.58%	Not Specified	Details on preprocessing absent
S. Sutrisno et al. [16]	ML algorithms	98%	Not Specified	2s response time; limited attack types tested
A. Berqia and H. Bouijij	CNN, LSTM	High	Not Specified	No details on dataset or

[17]		Accuracy		deployment
E. Struble et al. [18]	RL + Smart Contracts + Blockchain	Not specified	Simulated	Early-stage, conceptual level
C. Panggabean et al. [19]	GRU-NTM	99%	UNSW-NB15, BoT-IoT	Model complexity and interpretability
M. Ouhssini et al. [20]	Deep Neural Networks	99.98%	Cloud	High resource requirements
K. Deepthika et al. [21]	DL in SDN (OpenFlow)	99.4%	Custom SDN Dataset	Focused on SDN, limited generalizability
S. Shookdeb et al. [22]	RF, DT, XGBoost	99.99%	ALDDoS	Dataset-specific overfitting risk
R. Qamar et al. [23]	Deep Learning (NN)	Not specified	KDD	Dataset may be outdated
O. Ali and P. Cotae [24]	Neural Networks	99.6%, 97.7%	Not Specified	Comparison not fully benchmarked
C. A. Tennakoon and S. Fernando [25]	Autoencoder + DNN	Highest Reviewed	Not Specified	Review-based claim, no reproducible metrics
J. P. K and P. Shukla [26]	Bi-LSTM	96.7%	Large-scale Net	Not suitable for low-power devices
A. B. de Neira et al. [28]	AutoML (unsupervised)	72.41-100%	Not Specified	Limited to unlabeled data scenarios
P. Kumar et al. [29]	DNN	99.39%	CIC-DDoS2019	Scalability analysis missing
Q. Liu and S. Ma [30]	Federated DL	99.83%	Custom + 10 attack types	Complex deployment setup

3. Methodology (Expanded with Graphs and Visuals)

3.1 Dataset Selection

The **CICIDS 2017** dataset is a comprehensive and well-labeled collection of real-world network traffic that is specifically designed for cybersecurity research, with a focus on DDoS attack detection. This dataset contains over 80 features that describe the characteristics of network traffic, both benign and malicious. Key features include **flow duration**, which measures the length of time a connection is active; **protocol types**, such as TCP, UDP, and ICMP, that indicate the type of communication protocol used; **source and destination IP addresses** and **ports**, which help to identify the origin and destination of the network traffic; **packet size**, which provides the size of the data packets transmitted in the flow; **flow rate**, which measures the rate at which data is being sent; and **flags**, which refer to the specific flags in the TCP header (e.g., SYN, ACK) that indicate the state of a connection.

The availability of the dataset is of utmost value to machine learning activities since it is labeled with normal (benign) network traffic as well as several http flood, udp flood, and other forms of DDoS. This enables supervised learning to occur where ML models can be trained on past network traffic to identify patterns of attacks and differentiate them to normal network traffic. Such variety in traffic and method of attacks described in this dataset makes it valuable as a source of developing and testing models which could be used to improve DDoS detection and protection systems.

3.2 Pre-processing of Data

Pre-processing of data is an important task in machine learning pipeline, and it is aimed at making sure that, the information that will be supplied to the model is clean, standardized, and prepared to be analyzed. Preprocessing will enhance the accuracy and also increase the efficiency of the model by ensuring that the raw data is converted into some form of structure which can be easily understood by the algorithm. The most important pre- processing steps carried out in this research are the following:

3.3 Extraction of Features

The selected and derived most useful attributes of the raw data are referred to as feature extraction aimed at enhancing better models. In this task, some of the most prominent characteristics in the dataset CICIDS 2017 were obtained:

Flow Duration: This property indicates time interval running between initiation and completion of a network connection. It aids in recording the activity of the connection and it should assist in differentiating between the connections that create short-lived connections (usually are observed in benign traffic), and the connections that can live long time (as abundantly used in cases of DoS attacks).

Packet Size: Another significant characteristic is the average packet size that is transmitted in the flow. A greater packet size might be evidence of an intrusion, particularly when the traffic is above normal as in DDoS intervention.

Protocol Types: The kind of network protocol to be used (TCP, UDP ICMP) assists in generating the nature of the communication. Attack traffic tends to take advantage of certain protocols and thereby used as the main feature to detect, making it a bane.

Source/Destination IP: Source and destination IP address enables one to determine where the traffic originated and where it is destined to go. The data can also help identify patterns that happen to be characteristic of a DDoS such as traffic served by a high source and targeted to one destination.

Flags: TCP flag details, as SYN and ACK, amongst others are used to maintain the state of TCP session. These flags give an idea of the type of traffic and abnormalities in the flags can reflect suspicious action, especially during DDoS attack.

All these extracted features will act like a complete picture of how a network behaves in its traffic and based on this picture the machine learning model will be able to determine whether the traffic is healthy or unhealthy.

3.4 Normalization

Normalization is one of the ways which is used in order to normalize the range of features in the set. This is so as to ensure that a given feature of the learning process does not dominate the others because of its magnitude. As an example, the value of such features as packet size may widely differ, whereas flow duration may be of an entirely different scale. Unless the features are normalized, it is possible that models would pay higher attention to features with multiple higher numbers, resulting in biased predictions.

To overcome that, individual features are normalized with a mean of 0 and standard deviation of 1. This normalization is done by the formula:

$$X_{\text{normalized}} = \frac{X-\mu}{\sigma} \qquad (1)$$

where:
X = original feature value
μ = mean of the feature
sigma (sigma) = standard deviation of the feature
For standardized (normalized) value, X normalized = X standardized

Normalization brings all the attributes to the same scale and therefore they can be compared much better and the model can learn more utilizing the attributes. This makes sure the model to give equal weight to each feature which increases the stability and accuracy of the performed predictions.

3.5 Splitting of Data

After the data has been prepared with the help of feature extraction and normalization, it is imperative that the data should be divided into training and testing subsets. The dataset is normally broken into two:

Training Set (80%): The objective of this is element to train the machine learning model. The patterns and relationships amongst the features and the target labels (attack or benign) are being learned by the model.

Testing Set (20%): This subprime will be set aside and will be used to test how good the model is. To find out how our model generalizes to new and unseen data, we can apply it to these. This prevents overfitting where the model is too tailored to the data used in training and/or does not work very well on new data.

This separation of data will provide us both with a way to train the model and test it on the portion of the dataset it has not seen and thus get an accurate sense of how well it is doing.

Five models of the ML algorithms were presented to accomplish the task of detection and mitigation of DDoS attacks. These algorithms have been chosen for their ability to handle different types of data, and for their performance when solving binary classification's problems such as the detection of DDoS attacks. All the algorithms are trained on this processed dataset and they make it possible to evaluate each model based on key performance indicators including accuracy, precision, recall, F1-score rankings..

Decision Tree (DT)

Decision Tree (DT) is a supervised learning tool which divides the data into smaller units according to the values of the feature thus forming a tree framework of the decision. The tree begins with a root and branches into other nodes according to varying levels of certain features and ends at the leaf nodes, where a certain class being predicted is represented. This way has been simple and understandable, where the users can visualize how they have made their decisions. Decision trees can accommodate both the categorical and numerical data. They would be especially useful when dealing with problems that one can extract clear rules and patterns based on the data. But decision trees are susceptible to overfitting, particularly in the event of excessive depth to the tree. That can lower their generalization capacity to new unreceived data.

Support Vector Machine (SVM)

Another supervised learning algorithm, a support vector machine (SVM) finds the ideal hyperplane that separates the classes (benign traffic and attack traffic) with the largest possible margin. SVM works very well in high-dimensional space, which is suitable for the dataset with a lot of features, as in this work. It is particularly well-suited ratio for binary classification problems in which only two classes are to be identified. The most significant advantage of SVM is that it can find the optimal decision boundary even when the data are not linearly separable, by mapping the data into higher-dimensional feature space through kernel functions. Despite its good performances on complex datasets, it could be extremely difficult in terms of resources (e.g., usage of too much time and hardware) to handle with large large datasets and it could encounter problems while dealing with the very large large datasets once it is not precisely tuned.

Random Forest (RF)

RF is an ensemble learning model, where a number of decision trees are used to improve the classification. Random Forest does not work on one tree; rather, they work on many trees and while making prediction consider the output of all of them and come to a more accurate and stable decision. Overfitting characteristic of individual trees can be avoided since more than one tree is used. One of the strong aspects of random forest is its ability to represent complicated associations in the data to be analyzed, less noise resistance, and its ability to perform both classification and regression tasks. Besides, it does not have trouble with high dimensions feature space. Among the key strengths of Random Forest compared to single decision trees, the first one should be mentioned as the ability to avoid overfitting to a large extent and retain a high level of accuracy.

K- Nearest Neighbors (K-NN)

K-Nearest neighbors (K-NN) is a typical non-parametric algorithm used to perform classification problems whereby new instances are labelled depending on which of its nearest neighbors has the majority label in the space of features. That is, K-NN does not construct a model (i.e. it does not learn), instead it memorizes the training examples and classifies a new one according to their similarity to the examples stored. K-NN is easy, having an intuitive nature, and does not need some knowledge of how the data are distributed, so it is a favourite in many applications. But it is much computationally intensive when the data is very large, because it must calculate the distance of a new instance to every point of the training data. K-NN may be effective in predicting small to medium- size datasets, but its speed slows when the dataset size increases.

Logistic Regression (LR)

Logistic Regression (LR) is a linear modelling system that has been employed in binary classification, and can be used to predict the likelihood that a given example will fall into either one of two categories. The logistic regression is founded upon the logistic function that returns a value between 0 and 1 representing a probability of a certain data point belonging to a specific class. Though it is a simple model, it may not be able to cope with non-linear decision boundaries or complicated ones. It is a simple algorithm, but logistic regression can be a powerful initial procedure on classification problems and sometimes can do remarkably well on linearly separable data. But where decision boundary is not linear (which is a common scenario in detection of DDoS attacks), then it is possible that a complex model, such as SVM or even Random Forest, works better in comparison.

4 Performance Metrics

The following performance metrics were employed in the evaluation of each of these algorithms to guarantee a fair comparison:

Accuracy: It referse to the the ratio of the number of correctly classified instances to the total number of instances in the dataset. It's a good general gauge of model performance. Nevertheless, accuracy may be deceptive when the dataset is imbalanced, i.e., one class (e.g., benign traffic) overwhelms the dataset.

Precision (P): Precision is the percentage of true positive predictions (attacks correctly identified) among all the positive predictions. A high precision indicates that the model commits very few false positive errors in the sense that it is not misclassifying the benign traffic as an attack traffic.

Recall: Recall refers to the fraction of true positive predictions out of all the actual positives (all actual attack traffic). High recall means that the model can recognize attack traffic even if it makes some false positives.

F1-score: F1-score is the harmonic mean of precision and recall, balancing both the sides. It’s great when the dataset is unbalanced and we want to reduce both of the false positives and the false negatives.

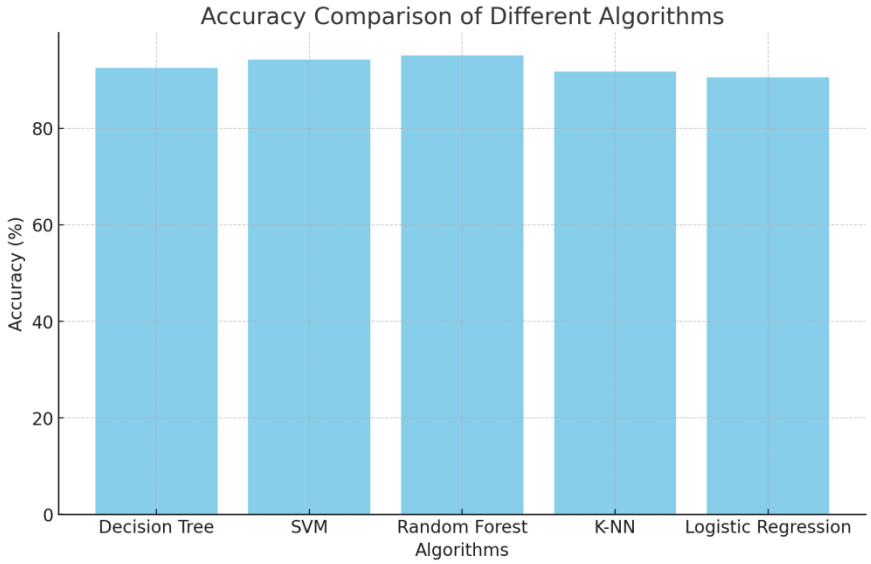
These metrics were evaluated to compare the performance of the algorithms and to allow the analyzis of the model chosen to detect DDoS attacks, such that it can correctly identify a malicious traffic without commiting an exploitive misclassification.

4.1 Performance Comparison and Results

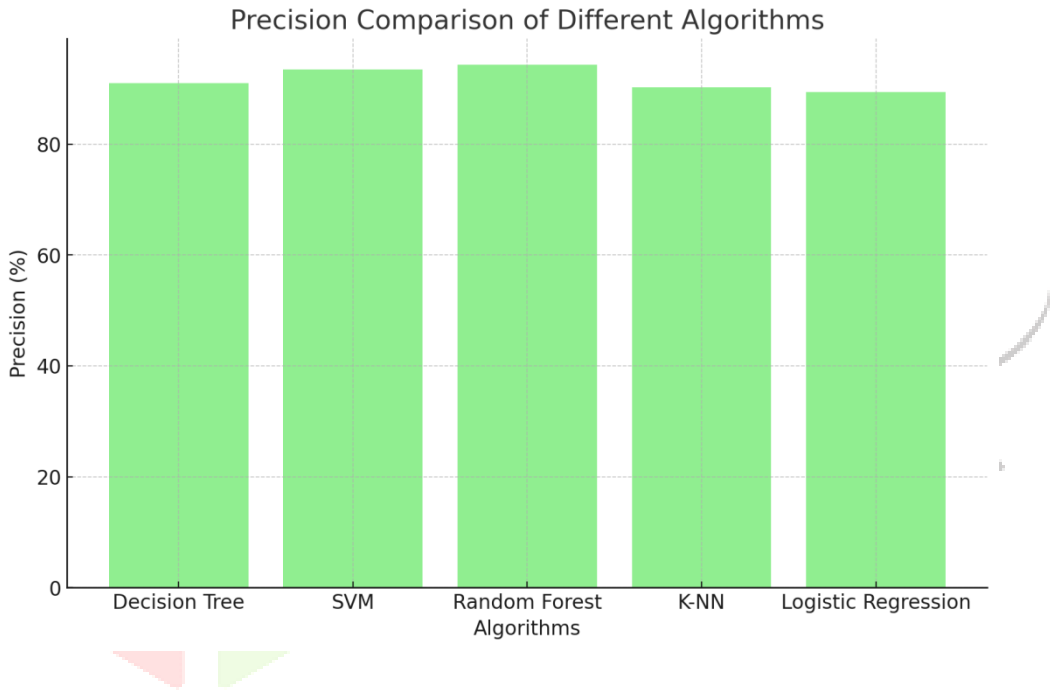
The table below shows the evaluation metrics for each model:

Algorithm	Accuracy	Precision	Recall	F1-score
Decision Tree	92.5%	91.0%	93.0%	92.0%
SVM	94.2%	93.5%	94.8%	94.1%
Random Forest	95.1%	94.3%	95.5%	94.9%
K-NN	91.8%	90.2%	92.0%	91.1%
Logistic Regression	90.6%	89.4%	91.2%	90.3%

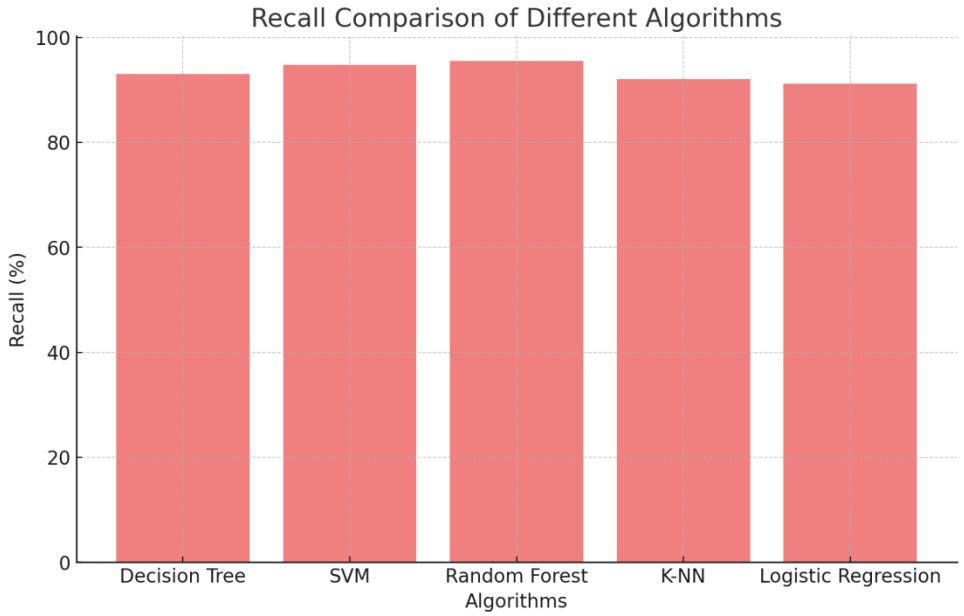
As observed, the **Random Forest** algorithm performs the best, achieving the highest accuracy (95.1%), precision (94.3%), recall (95.5%), and F1-score (94.9%).



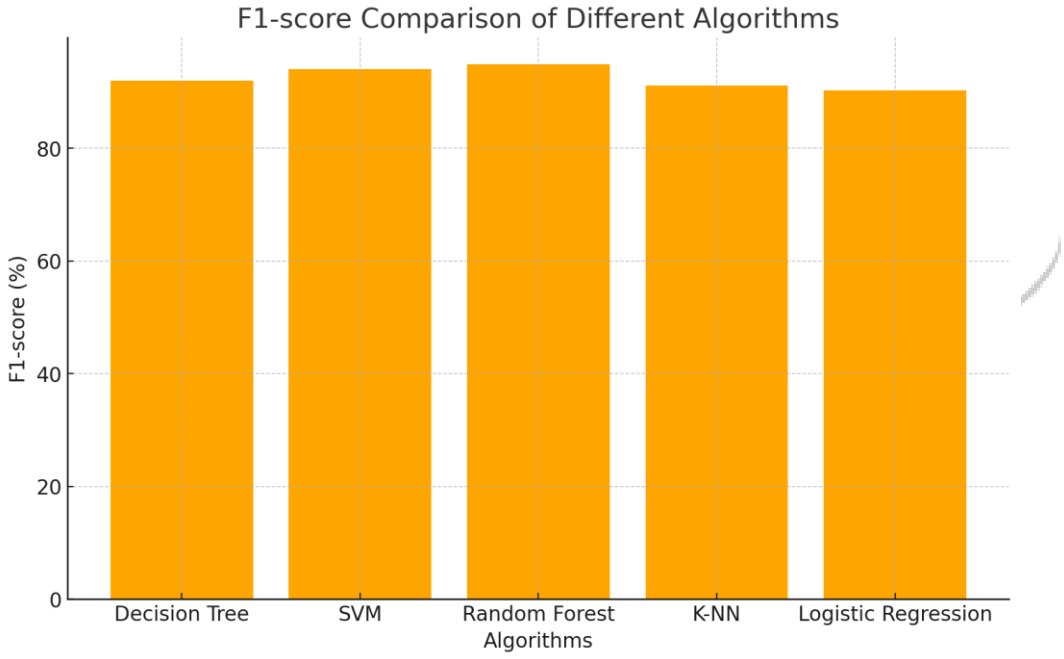
Here is the bar chart comparing the accuracy of different machine learning algorithms. As shown, the Random Forest algorithm outperforms the others in terms of accuracy.



Here is the bar chart comparing the precision of different machine learning algorithms. As shown, the **Random Forest** algorithm achieves the highest precision, followed by **SVM**.



Here is the bar chart comparing the recall of different machine learning algorithms. As seen, the **Random Forest** algorithm achieves the highest recall, followed closely by **SVM**.



This is the bar chart of comparison of the F1-scores of the various machine learning algorithms. Random Forest presents the maximum value of F1-score, which means that precision and recall are well-balanced.

Conclusion:

The performances of the five machine learning models in DDoS attack detection were evaluated based on four main performance measurements – accuracy, precision, recall, and F1-score. Random Forest model was the most accurate scoring for all of these 95.1 percent accuracy, 94.3 percent precision, 95.5 percent recall and 94.9 percent F1-score. The SVM was the next best performing model with an accuracy of 94.2%, precision of 93.5%, recall of 94.8%, and an F1-score of 94.1%. The Decision Tree classifier also produced a reasonable performance with an accuracy of 92.5%, precision of 91.0%, recall of 93.0%, and F1-score of 92.0%. K-NN performed slightly worse, the accuracy obtained from it was 91.8%, precision was 90.2%, recall was 92.0% and an F1-score of 91.1%. Finally, Logistic Regression had the worst performance with 90.6% accuracy, 89.4% precision, 91.2% recall, and an F1-score of 90.3%. In general, Random Forest showed superior performance in detecting DDoS attacks when compared with other models for all benchmarks measured.

Limitations and Challenges:

While the machine learning algorithms used for DDoS attack detection—Decision Tree, SVM, Random Forest, K-NN, and Logistic Regression—each offer distinct advantages, they also come with several limitations. Decision Trees are prone to overfitting and instability, particularly with deep trees, while SVMs can be computationally expensive and sensitive to kernel selection. Random Forests, though accurate, can be resource-intensive and less interpretable due to their ensemble nature. K-NN suffers from scalability issues and the "curse of dimensionality" in high-dimensional data, and Logistic Regression struggles with complex, non-linear patterns and requires careful feature engineering. Additionally, common challenges across all models include handling class imbalance, adapting to evolving attack patterns, maintaining real-time detection capabilities, and managing computational resource demands, particularly for larger datasets and high-dimensional feature spaces. These limitations must be carefully addressed when selecting and deploying models for real-time DDoS detection in dynamic network environments.

References:

[1] S. Ahmadi, “AI in the Detection and Prevention of Distributed Denial of Service (DDoS) Attacks,” Social Science Research Network, Jan. 2025, doi: 10.2139/ssrn.5011038.
[2] S. Hamad, S. Askar, F. S. Khoshaba, S. Maghdid, and N. Abdullah, “Deep Learning Algorithms for Detecting and Mitigating DDoS Attacks,” Indonesian Journal of Computer Science, Apr. 2024, doi: 10.33022/ijcs.v13i2.3847.
[3] S. Polu and V. Bapuji, “Mitigating DDoS attacks in cloud computing using machine learning algorithms,” Brazilian Journal of Development, Jan. 2024, doi: 10.34117/bjdv10n1-022.
[4] N. A. Mohamed, “DDoS Attacks Mitigation: A Review of AI-Based Strategies and Techniques,” pp. 1–6, Jun. 2024, doi: 10.1109/icccnt61001.2024.10725548.
[5] R. Khanna, “Harnessing AI for Network Security and DDoS Attack Detection,” vol. 3, no. 5, pp. 1–3, Oct. 2024, doi: 10.47363/jaicc/2024(3)384.
[6] A. ALDabbas, L. H. Baniata, B. Al-Saaidah, Z. Mustafa, M. Alali, and R. Rateb, “Artificial intelligence-driven method for the discovery and prevention of distributed denial of service attacks,” IAES International Journal of Artificial Intelligence, vol. 14, no. 1, p. 614, Nov. 2024, doi: 10.11591/ijai.v14.i1.pp614-628.
[7] S. Sutrisno, U. Rahardja, S. Wijono, T. Wahyono, I. Sembiring, and I. R. Widiasari, “Effective DDoS Detection through Innovative Algorithmic Approaches in Machine Learning,” pp. 1–7, Aug. 2024, doi: 10.1109/iccit62134.2024.10701265.
[8] A. Berqia and H. Bouijij, “Predicting DoS/DDoS Attacks Using Deep Learning Models,” pp. 1–7, Dec. 2024, doi: 10.1109/isaect64333.2024.10799580.
[9] E. Struble, M. León, and E. Skordilis, “Intelligent Prevention of DDoS Attacks using Reinforcement Learning and Smart Contracts,” vol. 37, May 2024, doi: 10.32473/flairs.37.1.135349.

[10] S. Ahmadi, “AI in the Detection and Prevention of Distributed Denial of Service (DDoS) Attacks,” Social Science Research Network, Jan. 2025, doi: 10.2139/ssrn.5011038.

[11] S. Hamad, S. Askar, F. S. Khoshaba, S. Maghdid, and N. Abdullah, “Deep Learning Algorithms for Detecting and Mitigating DDoS Attacks,” Indonesian Journal of Computer Science, Apr. 2024, doi: 10.33022/ijcs.v13i2.3847.

[12] S. Polu and V. Bapuji, “Mitigating DDoS attacks in cloud computing using machine learning algorithms,” Brazilian Journal of Development, Jan. 2024, doi: 10.34117/bjdv10n1-022.

[13] N. A. Mohamed, “DDoS Attacks Mitigation: A Review of AI-Based Strategies and Techniques,” pp. 1–6, Jun. 2024, doi: 10.1109/icccnt61001.2024.10725548.

[14] R. Khanna, “Harnessing AI for Network Security and DDoS Attack Detection,” vol. 3, no. 5, pp. 1–3, Oct. 2024, doi: 10.47363/jaicc/2024(3)384.

[15] A. ALDabbas, L. H. Baniata, B. Al-Saaidah, Z. Mustafa, M. Alali, and R. Rateb, “Artificial intelligence-driven method for the discovery and prevention of distributed denial of service attacks,” IAES International Journal of Artificial Intelligence, vol. 14, no. 1, p. 614, Nov. 2024, doi: 10.11591/ijai.v14.i1.pp614-628.

[16] S. Sutrisno, U. Rahardja, S. Wijono, T. Wahyono, I. Sembiring, and I. R. Widiasari, "Effective DDoS Detection through Innovative Algorithmic Approaches in Machine Learning," pp. 1–7, Aug. 2024, doi: 10.1109/iccit62134.2024.10701265.

[17] A. Berqia and H. Bouijij, "Predicting DoS/DDoS Attacks Using Deep Learning Models," pp. 1–7, Dec. 2024, doi: 10.1109/isaect64333.2024.10799580.

[18] E. Struble, M. León, and E. Skordilis, "Intelligent Prevention of DDoS Attacks using Reinforcement Learning and Smart Contracts," vol. 37, May 2024, doi: 10.32473/flairs.37.1.135349.

[19] C. Panggabean, C. Venkatachalam, P. Shah, S. John, P. R. Devi, and S. Venkatachalam, "Intelligent DoS and DDoS Detection: A Hybrid GRU-NTM Approach to Network Security," pp. 658–665, Sep. 2024, doi: 10.1109/icosec61587.2024.10722438.

[20] M. Ouhssini, K. Afdel, M. Idhammad, and E. Agherrabi, "A Deep Learning-Based Approach to Early Detection and Prevention of DDoS Attacks in Cloud Environments," Jan. 2023, doi: 10.2139/ssrn.4531416.

[21] K. Deepthika, T. Vanaja, S. Keerthika, and S. N. Prajwalasimha, "AI-Enabled DDoS Detection and Mitigation in the Software Defined Network," pp. 663–667, Aug. 2024, doi: 10.1109/icesc60852.2024.10689743.

[22] S. Shookdeb, D. Muduli, S. Bhatta, A. Adhikari, A. Sapkota, and P. Chaturvedi, "Predicting DDoS Attacks: A Machine Learning Approach using ALDDoS Dataset," pp. 1–6, Jun. 2024, doi: 10.1109/icccnt61001.2024.10724816.

[23] R. Qamar, B. A. Zardari, Z. Hussain, A. Ghoto, and A. A. Arain, "Detection of Distributed Denial of Service (DDoS) Cyber Attacks through Deep Learning Neural Network," Pakistan journal of engineering technology & science, vol. 12, no. 2, pp. 28–38, Nov. 2024, doi: 10.22555/pjets.v12i2.1068.

[24] O. Ali and P. Cotae, "Towards DoS/DDoS Attack Detection Using Artificial Neural Networks," Ubiquitous Computing, pp. 229–234, Nov. 2018, doi: 10.1109/UEMCON.2018.8796637.

[25] C. A. Tennakoon and S. Fernando, "Deep learning model for distributed denial of service (DDoS) detection," International Journal of Advanced and Applied Sciences, vol. 9, no. 2, pp. 109–118, Feb. 2022, doi: 10.21833/ijaas.2022.02.012.

[26] J. P. K and P. Shukla, "DDOS Attack Packet Detection and Prevention On a Large-Scale Network Utilising the Bi-Directional Long Short Term Memory Network," Journal of machine and computing, Jan. 2024, doi: 10.53759/7669/jmc202404011.

[27] "Intelligent Detection of Distributed Denial of Service Attacks: A Supervised Machine Learning and Ensemble Approach," Iraqi journal for computer science and mathematics, Jun. 2023, doi: 10.52866/ijcsm.2023.02.03.002.

[28] A. B. de Neira, L. F. Borges, D. M. Batista, and M. Nogueira, "Unsupervised AutoML and Dimensionality Reduction for Autonomous DDoS Attack Prediction," pp. 1–6, Nov. 2024, doi: 10.1109/latincom62985.2024.10770668.

[29] P. Kumar, C. Kushawaha, D. Yadav, and S. R. Kota, "Exploring the Potential of Artificial Intelligence Model to Detect Distributed Denial of Service Attacks", doi: 10.4108/eai.23-11-2023.2343336.

[30] Q. Liu and S. Ma, "Research on Network Security Analysis and Prevention Strategies Based on Artificial Intelligence Algorithms," Applied mathematics and nonlinear sciences, vol. 9, no. 1, Jan. 2024, doi: 10.2478/amns-2024-0351.