Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14502
e-ISSN : 2541-2019
p-ISSN : 2541-044X

The Efficiency of Machine Learning Techniques for DDoS Attack Detection: Random Forest, Logistic Regression, and Neural Networks

Syauqii Fayyadh Hilal Z[1)*], Rushendra[2)]
[1)2)]Informatics, Faculty of Computer Science, Universitas Mercu Buana, Jakarta, Indonesia
[1)]syauqiifayyad13@gmail.com, [2)]rushendra@mercubuana.ac.id

Submitted :Jan 20, 2025 | **Accepted** : Feb 11, 2025 | **Published** : Feb 22, 2025

Abstract: Distributed Denial of Service (DDoS) attacks are one of the most common cybersecurity concerns brought on by the quick development of digital technology. By flooding servers with too many requests, these assaults interfere with online services, highlighting the necessity of strong detection systems. Using the well-known CIC-DDoS2019 dataset, this study explores the use of machine learning algorithms—Random Forest (RF), Logistic Regression (LR), and Neural Networks (NN)—to improve DDoS assault detection. A comprehensive preprocessing procedure that comprised feature selection, normalization, and duplication removal was applied to dataset in order to ensuring optimal algorithm performance. With an accuracy of 97% on the entire test dataset and 99.13% on the training and validation datasets, RF showed exceptional performance. While NN successfully managed intricate data patterns, attaining an accuracy of roughly 94%, LR demonstrated impressive results with an accuracy of 98.65%. Because of its ensemble method, which minimizes overfitting and improves model generalization, the RF algorithm performed better than the others. This study highlights how machine learning may be used to solve practical cybersecurity issues by offering insightful information about how to optimize algorithms for real-time DDoS detection. The results improve the stability and resilience of digital infrastructures by aiding in the creation of effective intrusion detection systems. Future research can explore integrating advanced neural network architectures and hybrid methods to further improve detection rates and adaptability to evolving cyber threats.
Keywords: Machine learning, cybersecurity, DDoS detection, Random Forest, Logistic Regression, and Neural Network

INTRODUCTION

Many real-world transactions have been able to move significantly into the digital sphere thanks to technological improvements, making them easily accessible online (Karatas, Demir, and Sahingoz 2020). However, this shift has also brought about serious challenges, as cybersecurity threats have become one of the most critical issues faced globally in the current era (Dasari and Devarakonda 2021). As digital systems evolve, the growing risk of attacks, particularly Distributed Denial of Service (DDoS) attacks, which overwhelm central servers with excessive requests to disrupt services and cause shutdowns, has emphasized the urgent need for effective defense mechanisms to protect sensitive data and ensure the continuity of online services (Al-Shareeda, Manickam, and Saare 2023).

An Intrusion Detection System (IDS) is essential for ensuring the protection of data against security threats that may inject unauthorized information through standard communication channels, whether the data is at rest or in transit (Rushendra et al. 2021). However, while some systems can detect DDoS attacks, many lack the scalability required to manage large-scale attacks in real time, especially in cloud environments or large enterprise networks. Additionally, the constantly evolving nature of DDoS attack vectors demands continuous adaptation of detection systems, which can be resource-intensive and costly (Dr. Sheshang Degadwala and Verma Jyoti Sukhdev Sushila 2024).

Due to the frequent changes in attack styles and patterns by DDoS attackers, it is crucial to carefully analyze the nature and characteristics of these attacks, making the development of detection mechanisms a challenging task (Malliga, Nandhini, and Kogilavani 2022).

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14502
e-ISSN : 2541-2019
p-ISSN : 2541-044X

In today's technology-driven era, machine learning has emerged as a powerful tool with diverse applications in addressing real-world challenges. It is widely applied in areas such as medical image processing (Barragán-Montero et al. 2021), sentiment analysis (Jain, Pamula, and Srivastava 2021), and cloud resource utilization prediction (Malik et al. 2022). Furthermore, intrusion detection systems in cloud computing settings heavily rely on machine learning (Ali, Chong, and Manickam 2023; Malik et al. 2022; Rushendra et al. 2021). Methods like deep learning (DL) and machine learning (ML) have gained popularity as efficient ways to counteract distributed denial-of-service (DDoS) attacks on many kinds of networks (Ali et al. 2023). We tested the proposed model using the CIC-DDoS2019 dataset, which is commonly used in the literature.

We evaluated the proposed model using the widely recognized CIC-DDoS2019 dataset. To achieve optimal model performance and accurate findings, this dataset was subjected to a number of preprocessing methods, including feature elimination, random subset selection, feature selection, duplication removal, and normalization (Devrim Akgun and Cavusoglu 2022).

The authors aim to enhance DDoS attack detection by leveraging various machine learning algorithms, including Random Forest, Logistic Regression, and Neural Network. The Random Forest model achieved an accuracy of 99.13% on both the training and validation datasets, and 97% on the full test dataset (Najar, A.A., Manohar Naik 2022). The Logistic Regression model demonstrated strong performance, achieving an accuracy, precision, and recall of 98.65% (Alkasassbeh et al. 2016). The Neural Network model, while slightly lower in performance, achieved an accuracy of approximately 94%, showcasing its potential in handling complex data patterns (Chartuni and Márquez 2021).

Detecting DDoS attacks is challenging due to their evolving nature. Attackers constantly modify patterns, making static detection systems inadequate. Distinguishing between normal and malicious traffic is also difficult due to high network data volume. This highlights the need for adaptive, real-time detection systems powered by machine learning. Intrusion Detection Systems (IDS) increasingly rely on machine learning (ML) to detect anomalies in network traffic. Algorithms such as Random Forest (RF), Logistic Regression (LR), and Neural Networks (NN) have shown potential in improving detection accuracy. This research uses the CIC-DDoS2019 dataset to evaluate these algorithms for DDoS attack detection.

However, many systems lack scalability to handle large-scale attacks in real-time, particularly in cloud environments and large networks. The ever-changing nature of DDoS attacks demands continuous adaptation, which is resource-intensive and costly. This study aims to offer a scalable and reliable solution for DDoS detection, contributing to better intrusion detection systems and faster response to modern cyberattacks. Unlike previous studies focused on statistical methods, this research explores ensemble techniques like Random Forest to address overfitting and improve accuracy in detecting DDoS attacks.

LITERATURE REVIEW

Studies on the application of machine learning in detecting Distributed Denial of Service (DDoS) attacks show significant progress in mitigating cybersecurity threats. With the rise of increasingly complex cyber-attacks, traditional approaches such as statistical-based techniques or simple neural networks are starting to be replaced by more advanced machine learning methods, such as ensemble algorithms and deep learning (Malliga et al. 2022).

Research using the CIC-DDoS2019 dataset, which includes normal network traffic and modern DDoS attacks, is an important reference due to the accuracy of the data and its ability to reflect real-world conditions (Al-Shareeda et al. 2023).

This dataset provides an ideal framework for testing various machine learning algorithms, including Random Forest, Logistic Regression, and Neural Network. The results show that the Random Forest algorithm excels with 99.99% accuracy, followed by Neural Network (98.07%) and Logistic Regression (93.89%) (Chartuni and Márquez 2021; Najar, A.A., Manohar Naik 2022).

Random Forest-based approaches are considered effective due to their ability to overcome overfitting and produce 100% precision. In contrast, Logistic Regression, while showing strong performance in recall (98.75%), has lower precision (91.20%), making it less ideal in conditions where false positives should be minimized (Kshirsagar and Kumar 2021).

This study fills a gap in existing literature by focusing on Random Forest as an ensemble method to improve DDoS detection accuracy. Unlike previous research that often emphasizes individual algorithms, this approach provides better generalization and real-time application potential in industrial environments. The findings offer practical value in enhancing DDoS attack detection and mitigation in large-scale network systems.

METHOD

The phases of the DDoS attack detection methodology utilizing the CIC-DDoS2019 dataset (DDoS Evaluation Dataset (CIC-DDoS2019), n.d.) are described in this section. Extracting and getting the dataset ready for analysis is the first step in the procedure. Preprocessing, which includes feature selection, cleaning, and normalization, is then applied to ensure the data is ready for use with machine learning algorithms. In the third stage, DDoS attacks

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14502
e-ISSN : 2541-2019
p-ISSN : 2541-044X

are successfully identified and categorized using a variety of machine learning techniques. Finally, various metrics such as accuracy, precision, recall and F1 score are used to evaluate the effectiveness of the methodology. Figure 1 shows the workflow, and each step is explained in depth in the following subsections.

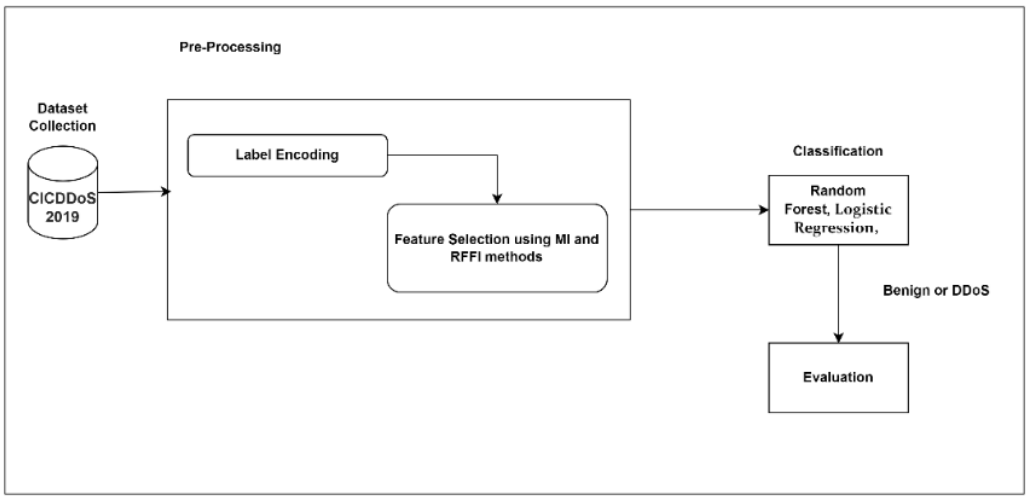

Fig 1. Design DDoS attack detection.

Datasets

Dataset from CICDDoS2019, obtained from its official source (Anon n.d.). includes both benign traffic and modern DDoS attack traffic. Among the more than 12 attack types it offers are PortMap, NetBIOS, LDAP, MSSQL, UDP, SYN, and others. Spanning two days of network traffic, the dataset provides raw PCAP files and event logs, along with over 80 extracted features per traffic flow, stored in CSV format for easier analysis. A particular file, DrDoS_NTP, has been chosen from the collection for this investigation. 1,209,961 occurrences with 84 cleaned input characteristics are included in this file. There are two labels for the binary class attribute: DDoS (attack traffic) and benign (regular traffic). While the full dataset includes records of various attack types, this study focuses solely on detecting DDoS attacks. The dataset's large sample size makes it ideal for assessing detection accuracy and has been widely used in previous research on DDoS detection.

Data Preprocessing

Preparing unprocessed information into a format that may be used is known as data preparation. This involves employing label encoding to translate category class labels into numerical values (0 and 1), where "0" stands for benign traffic and "1" for DDoS attack.

Feature Selection

Training process becomes increasingly more complex as the dimensionality of the data increases, and the chosen datasets are high-dimensional. Numerous research employing these datasets have employed feature selection to improve the detection of different forms of assault (Afsaneh Banitalebi Dehkordi 2021; Kshirsagar and Kumar 2021).

Ddos Attack Classification

Evaluation measures are essential for determining how well prediction models work. Machine learning algorithms' performance in detecting DDoS attacks was evaluated in this study using metrics like accuracy, precision, recall, and F1 score.

Random Forest

Using random node splitting and random node resampling, the Random Forest method is an ensemble machine learning technique that builds decision trees. Voting across several decision trees determines the ultimate classification outcome (Dhanabal and Shantharajah 2015). On systems like Spark, Random Forest enables concurrent training by separately training a group of decision trees. Large-scale data management is made possible by processing the datasets as RDDs (Resilient Distributed Datasets). Setting the number and depth of the trees with the right parameters is crucial to achieving the best possible results.

In this study, the Random Forest model was trained with 50 decision trees (n_estimators=50), and feature importance was analyzed to identify the most influential features.

Parameters used:

Number of estimators (n_estimators) : 50
Random state (random_state) : 42

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14502
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Logistic Regression

Logistic regression is a method of machine learning designed for classification tasks, particularly effective for binary class labels. It operates by multiplying input features with their corresponding weights and processing the result through a sigmoid activation function (Larasati, DeYong, and Slevitch 2012). In this study, logistic regression is applied to a set of selected features for detecting DDoS attacks. The model's weights are fine-tuned using the lbfgs optimizer with a regularization parameter set to C = 0.2.

Parameters used:
Regularization strength (C) : 0.2
Solver : lbfgs
Maximum iterations : 200

Neural Network

Neural networks, particularly deep learning architectures, have demonstrated significant effectiveness in detecting Distributed Denial of Service (DDoS) attacks. These models are adept at capturing intricate patterns within network traffic data, enabling the differentiation between legitimate and malicious activities (Batchu et al. 2024).

We use a neural network model in this study to detect DDoS attacks. The optimizer with a learning rate of 0.001 is used to optimize the model's parameters. The input, hidden, and output layers are among the several layers that make up the neural network, and each one is intended to represent different degrees of data abstraction. Rectified Linear Units (ReLU) are the activation functions utilized in the hidden layers. By adding non-linearities to the model, ReLU enables it to recognize intricate patterns. The output layer generates a probability score that indicates the possibility of an input being malicious by using a sigmoid activation function.

Several neural network designs have been investigated recently for DDoS detection. As an illustration of how deep learning might improve cybersecurity measures, a paper that was published in Scientific Reports presented a unique optimization-driven deep learning framework for identifying DDoS attacks.

Parameters used:
Hidden layer sizes (hidden_layer_sizes) : (10,)
Maximum iterations (max_iter) : 10
Random state (random_state) : 42

Measures for Assessment

Metrics from performance evaluation are essential for determining how well predictive models work. Metrics such as accuracy, precision, recall and F1 score are used in this study to evaluate the efficiency of machine learning techniques in identification of DDoS attacks.

a. Accuracy

The main evaluation metric, accuracy, determines the ratio of correctly predicted observations to the total number of observations. Although a useful metric, accuracy works best when the data set is balanced and the ratio of false positives to false negatives is fairly close. According to the corresponding equation, this metric indicates how well the classifier predicts the data points.

$$Accuracy=TP/(TP+TN+FP+FN) \quad (1)$$

Where:
TP (True Positives)
TN (True Negatives)
FP (False Positives)
FN (False Negatives)

b. Precision

The percentage of successfully identified positive instances to all anticipated positive cases is measured by a metric known as precision. A higher precision value indicates a lower false positive rate, reflecting the clarity of the model in identifying true positives. Essentially, precision measures the likelihood that a prediction classified as positive is indeed correct. This metric can be calculated using a specific formula, often provided alongside its application.

$$Precision=TP/(TP+FP) \quad (2)$$

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14502
e-ISSN : 2541-2019
p-ISSN : 2541-044X

c. Recall

In a dataset, recall is defined as the proportion of correctly identified positive events to all actual positive cases. It demonstrates how effectively the model can detect real positives inside the class. Recall assesses the classifier's ability to accurately represent the positive class using a given equation.

$$Recall=TP/(TP+FN) \quad (3)$$

d. F1 Score

A balanced score that accounts for both false positives and false negatives is the F1 Score. It is the precision and recall harmonic mean. Because it provides a more insightful assessment than accuracy alone, this metric is especially useful when addressing unequal class distributions. The F1 Score combines precision and recall into a single value, emphasizing their relationship, as expressed through a defined equation.

$$Fmeasure=PR/((P+R)) \quad (4)$$

Where:
P (Precision)
R (Recall)

RESULT

Before diving into the detailed performance metrics of the models, it is essential to establish the context of the analysis. The CICDDoS2019 dataset was selected for its comprehensive representation of network traffic, including both benign and malicious activity. The dataset's features were preprocessed to ensure compatibility with machine learning algorithms, and several models were trained and evaluated to identify the most effective approach for DDoS attack detection.

Table 1. The CICDDos2019 Datasets

Features	Mean	Std	...	Min	Max
Destination Port	8879.62	19754.64740	…	0.00000	65532.00000
Flow Duration	1.624165e+07	3.152437e+07	…	1.000000e+00	1.199999e+08
Total Fwd Packets	4.874916	15.422874	…	1.000000	1932.000000
Total Backward Packets	4.572775	21.755356	…	0.000000	2942.000000
Total Length of Fwd Packets	939.463346	3249.403484	…	0.000000	183012.000000
Fwd Packet Length Max	538.535693	1864.128991	…	0.000000	11680.000000
Idle Mean	1.032214e+07	2.185303e+07	…	0.000000e+00	1.200000e+08

In this work, evaluation measures such as accuracy, F1 score, recall, precision, and confusion matrix are used to give a multidimensional picture of the models' capabilities. Furthermore, ROC curves and other visual aids shed light on the trade-offs between true positive and false positive rates for each model. A thorough evaluation of the models' performance is guaranteed by this methodical methodology.

Model Performance Overview

a. Accuracy

Accuracy measures the overall correctness of the model. The model of Random Forest scored better than the others with an accuracy of 99.99%, followed by the Neural Network (98.07%) and Logistic Regression (93.89%). These results suggest that ensemble methods, like Random Forest, perform exceptionally well on this dataset.

Table 2. Comparison of Model Accuracy for DDoS Detection.

Model	Accuracy
Random Forest	0.9999
Logistic Regression	0.9389
Neural Network	0.9807

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14502
e-ISSN : 2541-2019
p-ISSN : 2541-044X

b. F1 Score

Particularly crucial for unbalanced datasets is the F1 Score, which strikes a compromise between precision and recall. The Random Forest model showed its effectiveness in controlling the trade-off between false positives and false negatives with an F1 Score of 99.99%. The neural network and logistic regression had respective F1 values of 98.30% and 94.83%.

Table 3. Comparison of Model F1S Score for DDoS Detection.

Model	F1 Score
Random Forest	0.9999
Logistic Regression	0.9483
Neural Network	0.9830

c. Recall

The model's recall shows how well it can detect every incident of DDoS attacks. With a 99.98% recall, the Random Forest model performed exceptionally well, guaranteeing that the majority of assault occurrences were identified. With a recall of 98.04%, the Neural Network came next, followed by Logistic Regression with 98.75%.
Table 4. Comparison of Model Recall for DDoS Detection.

Model	Recall
Random Forest	0.9998
Logistic Regression	0.9875
Neural Network	0.9804

d. Precision

The percentage of genuine positives among all anticipated positives is known as precision. With a precision of 100.00%, Random Forest once again took the lead, proving its resilience in reducing false positives. The Logistic Regression scored 91.20%, whereas the Neural Network earned 98.55%.

Table 5. Comparison of Model Precision for DDoS Detection.

Model	Precision
Random Forest	1.0000
Logistic Regression	0.9120
Neural Network	0.9855

Confusion Matrix

The distribution of true positives, true negatives, false positives, and false negatives is shown by the confusion matrices for each model. The Random Forest model's strong recall and precision were highlighted by its low number of false negatives (7) and lack of erroneous positives.

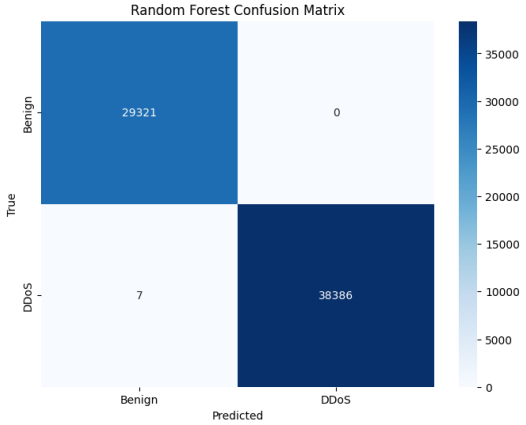

Fig 2. Random Forest Confussion Matrix

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14502
e-ISSN : 2541-2019
p-ISSN : 2541-044X

The Logistic Regression model exhibited a relatively higher rate of false positives (3,617), which affected its precision, and had 481 false negatives.

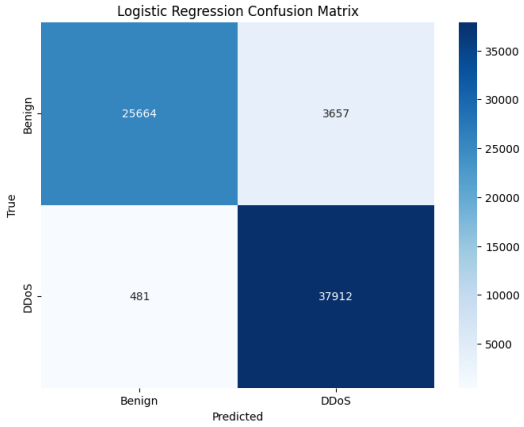

Fig 3. Logistic Regression Confusion Matrix

The Neural Network model, on the other hand, had excellent precision and recall performance with 532 erroneous positives and 753 false negatives.

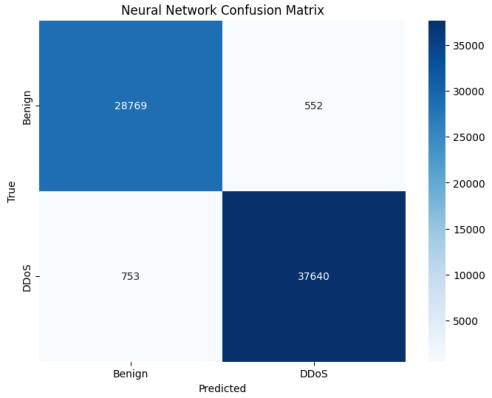

Fig 4. Neural Network Confusion Matrix

Model Comparison

ROC curves for Random Forest, Logistic Regression, and Neural Network models. Random Forest has the highest AUC (1.00), followed by Neural Network (0.99) and Logistic Regression (0.99). These graphs demonstrate how well the model can differentiate between malicious and benign network data.

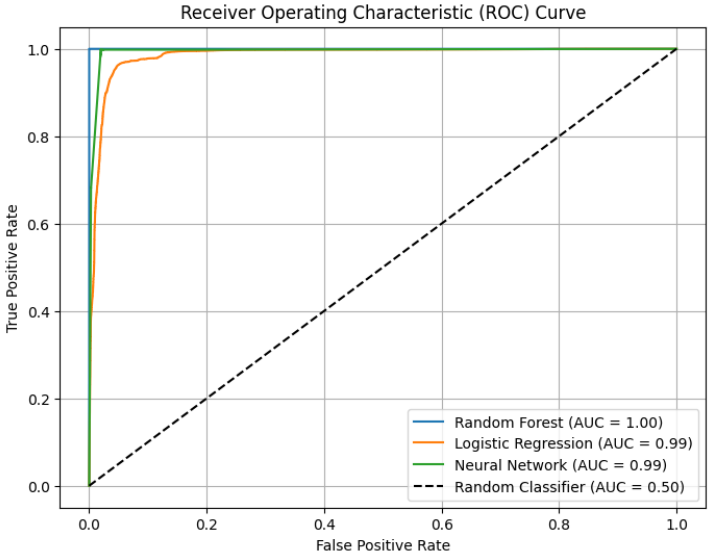

Fig 5. Curve of the Receiver Operating Characteristic (ROC)

*name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

DISCUSSIONS

Using the CIC-DDoS2019 dataset, the study's findings demonstrate how well machine learning systems detect DDoS attacks. Among the algorithms analyzed, the Random Forest method outperformed Logistic Regression and Neural Networks with regard to of recall, accuracy, F1 score, and precision. Its ensemble learning methodology, which reduces overfitting and improves model generalization, is responsible for this.

The Neural Network, although slightly less accurate, demonstrated robustness in capturing complex data patterns. Its performance could be further enhanced with advanced architectures or larger datasets. Logistic Regression, while simpler and faster, exhibited lower precision due to a relatively higher false-positive rate, making it less suitable for real-time applications where accuracy is critical.

The comparison with existing literature confirms that our Random Forest implementation achieves state-of-the-art performance for DDoS detection. However, the study acknowledges limitations such as dataset dependency and the computational complexity of some algorithms, which may affect real-world deployment.

CONCLUSION

This study shows how machine learning methods, in particular Random Forest, might improve DDoS assault detection. The findings show that ensemble-based approaches are an attractive option for intrusion detection systems since they provide higher accuracy and dependability. Neural Networks also show great promise in handling complex data patterns, while Logistic Regression remains a viable option for scenarios requiring simplicity and speed.

To increase flexibility to changing cyberthreats, future research should investigate the combination of sophisticated neural network topologies, hybrid approaches, and real-time implementation. Additionally, expanding the scope to include other attack types and datasets could provide a more comprehensive evaluation.

ACKNOWLEDGMENT

The authors express their gratitude to Universitas Mercu Buana for providing the resources and support necessary for this research. We also thank the developers of the CIC-DDoS2019 dataset for making their data publicly available, enabling this study.

REFERENCES

Afsaneh Banitalebi Dehkordi, MohammadReza Soltanaghaei &. Farsad Zamani Boroujeni. 2021. “The DDoS Attacks Detection through Machine Learning and Statistical Methods in SDN.” *The Journal of Supercomputing* 77:2383–2415.

Al-Shareeda, Mahmood A., Selvakumar Manickam, and Murtaja Ali Saare. 2023. “DDoS Attacks Detection Using Machine Learning and Deep Learning Techniques: Analysis and Comparison.” *Bulletin of Electrical Engineering and Informatics* 12(2):930–39. doi: 10.11591/eei.v12i2.4466.

Ali, Tariq Emad, Yung Wey Chong, and Selvakumar Manickam. 2023. “Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review.” *Applied Sciences (Switzerland)* 13(5). doi: 10.3390/app13053183.

Alkasassbeh, Mouhammd, Ghazi Al-Naymat, Ahmad B.A, and Mohammad Almseidin. 2016. “Detecting Distributed Denial of Service Attacks Using Data Mining Techniques.” *International Journal of Advanced Computer Science and Applications* 7(1). doi: 10.14569/ijacsa.2016.070159.

Anon. n.d. “DDoS Evaluation Dataset (CIC-DDoS2019).” Retrieved December 11, 2024 (https://www.unb.ca/cic/datasets/ddos-2019.html).

Barragán-Montero, Ana, Umair Javaid, Gilmer Valdés, Dan Nguyen, Paul Desbordes, Benoit Macq, Siri Willems, Liesbeth Vandewinckele, Mats Holmström, Fredrik Löfman, Steven Michiels, Kevin Souris, Edmond Sterpin, and John A. Lee. 2021. “Artificial Intelligence and Machine Learning for Medical Imaging: A Technology Review.” *Physica Medica* 83(May):242–56. doi: 10.1016/j.ejmp.2021.04.016.

Batchu, Raj Kumar, Thulasi Bikku, Srinivasarao Thota, Hari Seetha, and Abayomi Ayotunde Ayoade. 2024. “A Novel Optimization-Driven Deep Learning Framework for the Detection of DDoS Attacks.” *Scientific Reports* 14(1). doi: 10.1038/s41598-024-77554-9.

Chartuni, Andrés, and José Márquez. 2021. “Multi-Classifier of DDoS Attacks in Computer Networks Built on Neural Networks.” *Applied Sciences (Switzerland)* 11(22). doi: 10.3390/app112210609.

Dasari, Kishore Babu, and Nagaraju Devarakonda. 2021. “Detection of Different DDoS Attacks Using Machine Learning Classification Algorithms.” *Ingenierie Des Systemes d’Information* 26(5):461–68. doi: 10.18280/isi.260505.

Devrim Akgun, Selman Hizal, and Unal Cavusoglu Cavusoglu. 2022. “A New DDoS Attacks Intrusion Detection Model Based on Deep Learning for Cybersecurity.” 118:101021. doi: https://doi.org/10.1016/j.cose.2022.102748.

Dhanabal, L., and S. P. Shantharajah. 2015. “A Study on NSL-KDD Dataset for Intrusion Detection System Based

*name of corresponding author

on Classification Algorithms." *International Journal of Advanced Research in Computer and Communication Engineering* 4(6):446–52. doi: 10.17148/IJARCCE.2015.4696.

Dr. Sheshang Degadwala, and Verma Jyoti Sukhdev Sushila. 2024. "Detection and Mitigation of DDoS Attacks : A Review of Robust and Scalable Solutions." *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* 10(5):12–23. doi: 10.32628/cseit2410582.

Jain, Praphula Kumar, Rajendra Pamula, and Gautam Srivastava. 2021. "A Systematic Literature Review on Machine Learning Applications for Consumer Sentiment Analysis Using Online Reviews." *Computer Science Review* 41:100413. doi: 10.1016/j.cosrev.2021.100413.

Karatas, Gozde, Onder Demir, and Ozgur Koray Sahingoz. 2020. "Increasing the Performance of Machine Learning-Based IDSs on an Imbalanced and Up-to-Date Dataset." *IEEE Access* 8:32150–62. doi: 10.1109/ACCESS.2020.2973219.

Kshirsagar, Deepak, and Sandeep Kumar. 2021. "An Efficient Feature Reduction Method for the Detection of DoS Attack." *ICT Express* 7(3):371–75. doi: 10.1016/j.icte.2020.12.006.

Larasati, Aisyah, Camille DeYong, and Lisa Slevitch. 2012. "The Application of Neural Network and Logistics Regression Models on Predicting Customer Satisfaction in a Student-Operated Restaurant." *Procedia - Social and Behavioral Sciences* 65:94–99. doi: 10.1016/j.sbspro.2012.11.097.

Malik, Sania, Muhammad Tahir, Muhammad Sardaraz, and Abdullah Alourani. 2022. "A Resource Utilization Prediction Model for Cloud Data Centers Using Evolutionary Algorithms and Machine Learning Techniques." *Applied Sciences (Switzerland)* 12(4). doi: 10.3390/app12042160.

Malliga, S., P. S. Nandhini, and S. V. Kogilavani. 2022. "A Comprehensive Review of Deep Learning Techniques for the Detection of (Distributed) Denial of Service Attacks." *Information Technology and Control* 51(1):180–215. doi: 10.5755/j01.itc.51.1.29595.

Najar, A.A., Manohar Naik, S. 2022. "DDoS Attack Detection Using MLP and Random Forest Algorithms." *Int. j. Inf. Tecnol* 14:2317–2327. doi: 10.1007/s41870-022-01003-x.

Rushendra, Kalamullah Ramli, Nur Hayati, Eko Ihsanto, Teddy Surya Gunawan, and Asmaa Hani Halbouni. 2021. "Development of Intrusion Detection System Using Residual Feedforward Neural Network Algorithm." *2021 4th International Seminar on Research of Information Technology and Intelligent Systems, ISRITI 2021* (April 2022):539–43. doi: 10.1109/ISRITI54043.2021.9702773.

*name of corresponding author