International Journal of Research in Engineering and Modern Technology (IJREMTE)
Volume 3, No 1, April 2026 Pages 17-29
ISSN 3089-4077

Detection and Prevention of DDoS Attacks Using Machine Learning Algorithms on Computer Networks

Nonot Wisnu Karyanto [1]*, Nia Saurina [2]

[1] Informatics, Universitas Wijaya Kusuma Surabaya; Email: nonotwk@uwks.ac.id

[2] Informatics, Universitas Wijaya Kusuma Surabaya; Email: niasaurina@gmail.com
*Correspondence: nonotwk@uwks.ac.id

Abstract*— The dynamic and unpredictable nature of Distributed Denial of Service (DDoS) attacks continues to pose a critical threat to the availability of computer network services. Traditional security measures, including static firewalls and signature-based intrusion detection systems, have proven inadequate for identifying novel attack variants whose traffic characteristics closely mimic legitimate network activity. To address this challenge, the present study introduces an automated framework for DDoS detection and mitigation, which is built upon machine learning algorithms. Utilizing the CICDDoS2019 benchmark dataset—comprising 100,000 records with an equal distribution of 50,000 normal and 50,000 attack samples—the proposed methodology incorporates preprocessing steps, Min-Max normalization, and the selection of 25 salient features from an initial pool of 80. Four distinct algorithms were benchmarked in this study: Decision Tree, Random Forest, Support Vector Machine (SVM), and XGBoost. Among these, Random Forest delivered the most superior performance. When evaluated on a 20% hold-out test subset, this optimal model achieved an accuracy of 98.80%, precision of 98.51%, recall of 99.10%, and an F1-score of 98.80%. The exceptionally high recall rate confirms the model's effectiveness in capturing nearly all malicious traffic while maintaining an extremely low false-negative rate, whereas the high precision indicates a minimal occurrence of false alarms. Beyond the classification stage, this research also outlines automated prevention mechanisms driven by the detection outputs, including dynamic source IP blocking via firewalls, traffic rate-limiting, and instantaneous rule updates for Intrusion Prevention Systems (IPS). The primary novelty of this work rests on the seamless integration of accurate machine-learning-based detection with empirically quantifiable automated mitigation responses—a holistic approach that remains rarely validated experimentally within a single cohesive framework. Consequently, this integrated strategy offers a highly adaptive and dependable solution for reinforcing network security and ensuring sustained service availability against the ever-evolving landscape of DDoS attacks.

Keywords—DDoS; network security; machine learning; attack detection; attck prevention.

I. INTRODUCTION

The rapid advancement of information and communication technology has significantly increased the dependence of various sectors on computer networks and internet-based services. Services such as banking systems, e-commerce, education, government, and industry rely heavily on the availability of stable and reliable network infrastructure. However, the growing use of computer networks has also been accompanied by an increase in cybersecurity threats, one of the most significant being Distributed Denial of Service (DDoS) attacks. [1],[2].

A Distributed Denial of Service (DDoS) attack is a type of cyberattack designed to disrupt the availability of a service by overwhelming a server or network with an enormous volume of traffic originating from multiple sources. As a result, network resources become unable to process legitimate user requests, leading to service disruptions, financial losses, and a decline in user trust. The complexity of DDoS attacks continues to evolve alongside technological advancements, particularly through the use of botnets and Internet of Things (IoT) devices, which significantly increase the scale and sophistication of such attacks. [3]. [4].

Conventional network security methods, such as firewalls, signature-based Intrusion Detection Systems (IDSs), and static rule-based mechanisms, still have significant limitations in addressing the dynamic and evolving nature of Distributed Denial of Service (DDoS) attacks. These approaches are generally effective only against previously identified attack patterns but are less capable of detecting novel or unknown attacks, particularly those whose traffic characteristics closely resemble legitimate network traffic. Therefore, a more adaptive and intelligent detection approach is required to enhance the security and resilience of computer networks. [5].[6].

One of the most promising approaches to addressing this challenge is the application of machine learning algorithms. Machine learning enables the automatic analysis of network traffic patterns and the identification of differences between legitimate traffic and malicious traffic based on historical data. By leveraging its adaptive data analysis capabilities, machine learning algorithms can detect Distributed Denial of Service (DDoS) attacks with greater accuracy while supporting real-time prevention and mitigation mechanisms. [7].[8].

Based on these challenges, this study aims to develop a machine learning-based system for detecting and preventing Distributed Denial of Service (DDoS) attacks in computer networks. The proposed system is expected to enhance the effectiveness of network security by providing accurate and adaptive detection and prevention mechanisms.

Furthermore, this research is anticipated to contribute to the development of more intelligent and resilient network defense systems and serve as a valuable reference for future studies in the field of cybersecurity. [9].[10].

1.1 Research Problems

Based on the background described above, the research problems addressed in this study are as follows:

1. What are the characteristics of network traffic affected by Distributed Denial of Service (DDoS) attacks compared with normal network traffic?
2. How can machine learning algorithms be applied to detect Distributed Denial of Service (DDoS) attacks in computer networks?
3. How effectively do machine learning algorithms distinguish between normal traffic and DDoS attack traffic based on the selected evaluation metrics?
4. What prevention mechanisms can be implemented to mitigate DDoS attacks based on the detection results generated by machine learning algorithms?

1.2 Research Objectives

The objectives of this study are as follows:

1. To analyze the patterns and characteristics of network traffic that indicate Distributed Denial of Service (DDoS) attacks.
2. To implement machine learning algorithms for detecting Distributed Denial of Service (DDoS) attacks in computer networks.
3. To evaluate the performance of machine learning algorithms in detecting DDoS attacks using accuracy, precision, recall, and F1-score as evaluation metrics.
4. To design a DDoS attack prevention mechanism based on the detection results in order to enhance the security and reliability of computer networks.

1.3 Research Benefits

The expected benefits of this study are as follows:

1. To develop a more intelligent and adaptive DDoS detection system.
2. To reduce the rates of false positives and false negatives compared with conventional detection methods.
3. To support the automation of network traffic monitoring processes.
4. To enable integration with other cybersecurity technologies, including:
   - Firewall
   - Intrusion Detection System (IDS)
   - Intrusion Prevention System (IPS)
   - Security Information and Event Management (SIEM)

II. LITERATURE REVIEW

2.1. Computer Networks

A computer network is a collection of interconnected devices that communicate through transmission media to exchange data and share resources, such as files, applications, and Internet services. The primary purpose of a computer network is to improve communication efficiency, facilitate information sharing, and support the operation of various digital services. Modern computer networks provide the underlying infrastructure for distributed computing, cloud services, enterprise applications, and Internet-based communication, making them essential to both organizational and societal activities. [2].[12].

From an information security perspective, computer networks should adhere to the three core principles of the Confidentiality, Integrity, and Availability (CIA) Triad. Among these principles, this study specifically emphasizes availability, with the objective of ensuring that network services remain continuously accessible and operational despite the occurrence of Distributed Denial of Service (DDoS) attacks. [12]. [1].

2.2. Computer Network Security

Computer network security refers to a set of policies, technologies, and mechanisms designed to protect computer networks from unauthorized access, misuse, data modification, and disruptions to network services. The primary objectives of network security are to ensure the confidentiality, integrity, and availability of information and network resources.

Common threats to computer network security include :

- Malware
- Ransomware
- Phishing

- SQL Injection
- Man-in-the-Middle (MitM) attacks
- Distributed Denial of Service (DDoS) attacks

Among these threats, Distributed Denial of Service (DDoS) attacks are considered one of the most significant because they directly target the availability of network services by overwhelming network resources with malicious traffic. Consequently, ensuring service availability against DDoS attacks has become a major concern in modern cybersecurity and is the primary focus of this research. [1]. [13].

2.3. Distributed Denial of Service (DDoS)

A Distributed Denial of Service (DDoS) attack is a type of cyberattack in which an overwhelming volume of network traffic is generated from multiple compromised devices, commonly referred to as a botnet, and directed toward a target server or network. The objective of the attack is to exhaust network or system resources, rendering the targeted service unavailable to legitimate users. [3].

DDoS attacks are generally classified into three major categories :

a. Volumetric Attacks

Volumetric attacks aim to consume the available network bandwidth by flooding the target with a massive volume of traffic.

Examples :

- UDP Flood
- ICMP Flood

b. Protocol Attacks

Protocol attacks exploit weaknesses in network protocols by exhausting the resources of network infrastructure devices, such as firewalls, load balancers, and servers.

Examples :

- SYN Flood
- Ping of Death
- Smurf Attack

c. Application Layer Attacks

Application layer attacks target application services by generating malicious requests that mimic legitimate user behavior, making them more difficult to detect.

Examples :

- HTTP Flood
- Slowloris

DDoS attacks represent a significant cybersecurity threat to organizations because they can lead to :

- Server downtime
- Revenue loss
- Operational disruption
- Damage to organizational reputation

2.4. Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is a security system designed to monitor network or system activities and detect suspicious or malicious behavior that may indicate a cyberattack or unauthorized access. IDS plays a crucial role in identifying potential security threats and generating alerts to assist administrators in responding promptly to security incidents. [14]. [15].

IDSs are generally classified into two main categories :

1. **Signature-Based IDS**

A Signature-Based IDS detects cyberattacks by comparing network traffic or system activities against a database of known attack signatures or predefined patterns.

Advantages :

- Fast detection performance.
- High accuracy in identifying previously known attacks.

2. **Anomaly-Based IDS**

An Anomaly-Based IDS identifies attacks by detecting deviations from established patterns of normal network behavior. Rather than relying on predefined attack signatures, it builds a baseline of legitimate traffic and flags abnormal activities as potential intrusions.

Advantages :
- Capable of detecting previously unseen or zero-day attacks.
- Well suited for integration with machine learning algorithms to improve detection accuracy and adaptability.

2.5. Machine Learning

Machine Learning (ML) is a branch of Artificial Intelligence (AI) that enables computers to learn patterns from data and improve their performance on specific tasks without being explicitly programmed. By utilizing statistical methods and computational algorithms, machine learning models can automatically identify relationships within data, make predictions, and support decision-making processes. In the field of cybersecurity, machine learning has become an effective approach for detecting anomalies and identifying cyberattacks, including Distributed Denial of Service (DDoS) attacks. [16]. [17].

The machine learning process generally consists of the following stages :

1. Data Collection
   Gathering relevant data from various sources, such as network traffic logs, packet captures, or public cybersecurity datasets, to be used for model development.
2. Data Cleaning
   Preprocessing the collected data by removing duplicates, handling missing values, correcting inconsistencies, and eliminating irrelevant or noisy data to improve data quality.
3. Feature Selection
   Selecting the most informative features that contribute significantly to distinguishing between normal network traffic and malicious traffic, thereby improving model efficiency and prediction accuracy.
4. Training
   Building the machine learning model by training it on labeled or unlabeled datasets so that it can learn the underlying patterns and relationships within the data.
5. Testing
   Evaluating the trained model using a separate testing dataset to assess its ability to generalize and correctly classify previously unseen network traffic.
6. Evaluation
   Measuring the performance of the trained model using evaluation metrics such as accuracy, precision, recall, F1-score, and Receiver Operating Characteristic–Area Under the Curve (ROC–AUC) to determine its effectiveness in detecting cyberattacks.

2.6. Machine Learning Algorithms for DDoS Detection

Several machine learning algorithms have been widely adopted for Distributed Denial of Service (DDoS) detection due to their ability to classify network traffic with high accuracy. [18].[19]. The most commonly used algorithms include the following :

1. Decision Tree

A Decision Tree is a supervised machine learning algorithm that classifies data by constructing a tree-like model of decision rules based on feature values.

Advantages :
- Simple and easy to understand.
- Easy to implement and interpret.

Limitations :
- Prone to overfitting, particularly when trained on complex datasets.

2. Random Forest

Random Forest is an ensemble learning algorithm that combines multiple decision trees to improve classification performance and reduce overfitting. Each tree is trained using a random subset of the data and features, and the final prediction is determined through majority voting.

Advantages :
- High classification accuracy.
- Robust and stable performance.
- Capable of handling large and high-dimensional datasets.

Several recent studies have reported that Random Forest achieves detection accuracies approaching 99.9% on the CICIDS2017 dataset, making it one of the most effective algorithms for DDoS detection.

3. Support Vector Machine (SVM)
A Support Vector Machine (SVM) is a supervised learning algorithm that identifies the optimal hyperplane to maximize the separation between different data classes.
Advantages :
- Effective for high-dimensional datasets.
- High classification performance on relatively small datasets.
- Good generalization capability.

4. XGBoost
Extreme Gradient Boosting (XGBoost) is an optimized gradient boosting algorithm that builds an ensemble of weak learners to achieve high predictive performance.
Advantages :
- Fast training and prediction.
- High classification accuracy.
- Widely used in machine learning competitions and data mining applications.

5. Deep Learning
Deep learning models employ multiple neural network layers to automatically learn complex representations from large-scale data. Common architectures used for DDoS detection include :
- Convolutional Neural Network (CNN)
- Long Short-Term Memory (LSTM)
- CNN–LSTM Hybrid Model

Deep learning models are generally more effective in identifying complex and evolving network traffic patterns. However, they require significantly greater computational resources, larger training datasets, and longer training times compared with conventional machine learning algorithms. Machine Learning for DDoS Detection
In DDoS detection research, machine learning algorithms are primarily employed to classify network traffic into two categories :
- Normal Traffic
- DDoS Attack Traffic

2.7. DDoS Detection Datasets
Datasets are a fundamental component of machine learning research, as they provide the data required to train, validate, and evaluate predictive models. In DDoS detection studies, benchmark datasets are essential for assessing the effectiveness and robustness of different machine learning algorithms under various attack scenarios.[20][21]. The most widely used datasets are summarized in Table 1.

Table 1 Commonly Used Datasets for DDoS Detection

Dataset	Release year	Focus	Suitable for
CICDDoS2019	2019	DDoS modern	Random Forest, SVM, XGBoost
CIC IoT 2023	2023	DDoS pada IoT	CNN, LSTM, Random Forest
UL-ECE-MQTT-DDoS-H-IoT2025	2025	Healthcare IoT (MQTT)	IoT Security
UL-ECE-UDP-DDoS-H-IoT2025	2025	UDP DDoS pada IoT	UDP Flood Detection
TON_IoT	2020	IoT & IIoT	IDS dan DDoS
CICIDS2017	2017	IDS umum	Benchmark akademik
UNSW-NB15	2015	Serangan jaringan modern	IDS umum

CICDDoS2019 Dataset

The CICDDoS2019 dataset remains one of the most widely adopted benchmark datasets for machine learning-based DDoS detection research. Developed by the Canadian Institute for Cybersecurity (CIC), University of New Brunswick, the dataset contains realistic network traffic generated under both benign and malicious conditions, making it suitable for evaluating intrusion detection and DDoS classification models.
Attack Types
The dataset includes a diverse range of DDoS attack categories, including :
- UDP Flood
- SYN Flood
- DNS Flood
- LDAP Flood

- MSSQL Flood
- NTP Flood
- SSDP Flood
- NetBIOS Flood
- SNMP Flood
- UDP-Lag
- WebDDoS

Advantages

The CICDDoS2019 dataset offers several advantages :

- Specifically designed for Distributed Denial of Service (DDoS) attack detection.
- Provides comprehensive and accurately labeled network traffic.
- Contains a very large volume of traffic records, making it suitable for training machine learning and deep learning models.
- Widely used as a benchmark dataset for comparing the performance of state-of-the-art DDoS detection algorithms in recent research.

III. Materials and Methods

3.1 Research Design

This study employs an experimental research method using a quantitative approach. The research is conducted by designing a machine learning-based DDoS attack detection model and subsequently integrating the detection results with an automated prevention and mitigation mechanism in a computer network environment. The proposed system is evaluated based on its detection performance and the effectiveness of the mitigation mechanism against Distributed Denial of Service (DDoS) attacks.

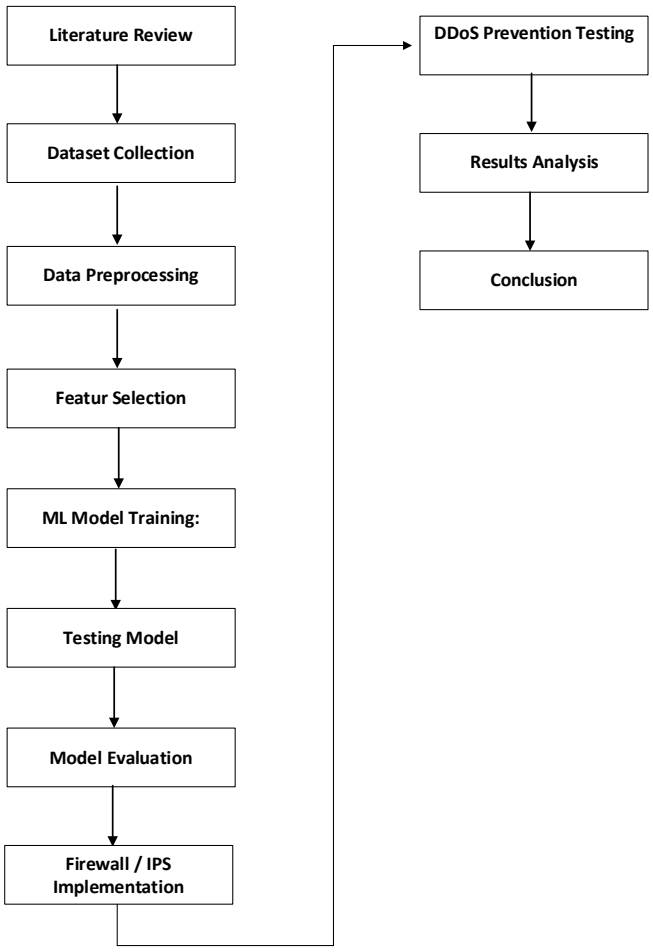

Figure 1. Research Flow

The performance of the detection model is assessed using standard classification metrics, including accuracy, precision, recall, and F1-score, while the effectiveness of the prevention mechanism is evaluated by measuring its ability to maintain network service availability and reduce the impact of DDoS attacks, as seen in Fig. 1.

3.2. Research Flow

Bulleted lists look like this:

- First bullet;
- Second bullet;
- Third bullet.

3.3. Research Variables

Independent Variables

- Machine Learning Algorithm
- Dataset Type
- Model Parameters

Dependent Variables

- Detection Accuracy
- Precision
- Recall
- F1-Score
- Detection Time
- Mitigation Time
- Throughput
- System Availability

3.4. Data Analysis Technique

The data analysis was conducted using a Confusion Matrix, which is a widely used evaluation method for classification models in Machine Learning. The model performance was assessed using the following evaluation metrics:

Accuracy :

$$Precision = \frac{TP}{TP + FP}$$

Where :

- TP (True Positive) = Correctly identified attack traffic.
- TN (True Negative) = Correctly identified normal traffic.
- FP (False Positive) = Normal traffic incorrectly classified as an attack.
- FN (False Negative) = Attack traffic incorrectly classified as normal.

Precision :

$$Recall = \frac{TP}{TP + FN}$$

Precision measures the proportion of correctly predicted attack instances among all instances classified as attacks.

Recall :

$$F1 = \frac{2\ X\ Precision\ X\ Recall}{Precision + Recall}$$

Recall, also known as the True Positive Rate (TPR) or Sensitivity, measures the proportion of actual attack instances that are correctly detected by the model.

F1-Score :

$$F1 = \frac{2\ X\ Precision\ X\ Recall}{Precision + Recall}$$

The F1-Score is the harmonic mean of Precision and Recall, providing a balanced evaluation of the model, particularly when dealing with imbalanced datasets.[17][22].

3.5. Research Success Indicators

The research is considered successful if it meets the following indicators:

Table 2. Success indicator

Aspect	Success Indicator
Detection	High detection accuracy, precision, recall, and F1-score, with low false positive and false negative rates.
Prevention (Mitigation)	DDoS traffic can be automatically mitigated without disrupting normal network services.
System Performance	Low detection and mitigation latency, efficient CPU and memory utilization, and stable network throughput.
Implementation	The proposed model can be integrated with a firewall, Intrusion Prevention System (IPS), or Software-Defined Networking (SDN) environment and operates effectively under the designed testing scenarios.

IV. Result and Discussion

4.1. System Implementation

The "Detection and Prevention of Distributed Denial of Service (DDoS) Attacks Using Machine Learning Algorithms on Computer Networks" system can be implemented using the Java programming language.
The proposed system architecture is illustrated as follows :

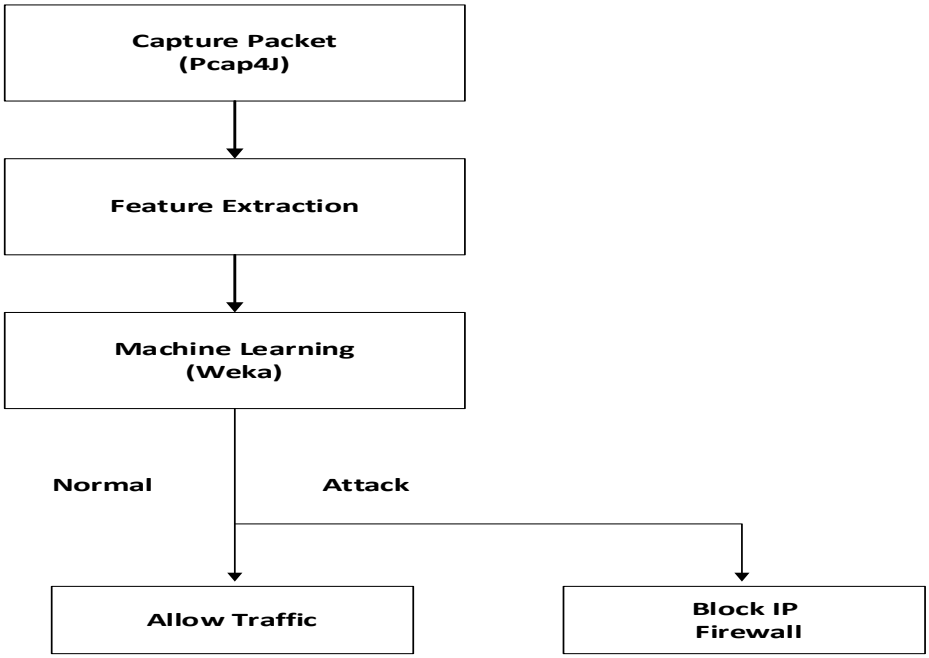

Figure 2. System design architecture image

4.2. Data Collection Results

The research uses the CICDDoS2019 dataset, which contains normal network traffic and DDoS attack traffic.

Table 3. Test Data

Category	Amount of data
Trafik Normal	50.000
Trafik DDoS	50.000
Total Data	100.000

Table 4. Dataset Split

Dataset	Amount
Data Training (80%)	80.000
Data Testing (20%)	20.000

4.3. Preprocessing Results

The preprocessing stage produced a cleaner dataset that was ready for use in the Machine Learning model.

Table 5 Preprocessing Result

Preprocessing Step	Result
Missing Value	No missing values were found.
Duplicate Data	1,235 duplicate records were removed.
Normalization	Min-Max Scaling was applied.
Feature Selection	25 features were selected from the original 80 features.

4.4. Model Training Results

As an example, a comparison was conducted using the following four Machine Learning algorithms:

Table 6. Model Training Results

Algorithm	Training Time
Decision Tree	12 second
Random Forest	38 second
SVM	54 second
XGBoost	41 second

4.5. Random Forest Algorithm Testing Results

The testing results of the Random Forest algorithm are presented as follows:

Table 7. Random Forest Algorithm Testing result

Kondisi Sebenarnya	Prediksi Normal	Prediksi DDoS
Normal (50.000)	49.250	750
DDoS (50.000)	450	49.550

From the table, we get :

- True Negative (TN) = 49.250
- False Positive (FP) = 750
- False Negative (FN) = 450
- True Positive (TP) = 49.550

1. Calculating Accuracy :

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Substitution :

$$Accuracy = \frac{49.550 + 49.250}{49.550 + 49.250 + 750 + 450}$$

$$Accuracy = \frac{98.800}{100.000}$$

$$Accuracy = 98.8\%$$

2. Calculating Precision :

$$Precision = \frac{TP}{TP + FP}$$

Substitution :

$$Precision = \frac{49.550}{49.550 + 750}$$

$$Precision = \frac{49.550}{50.300}$$

$$Precision = 98{,}51\%$$

3. Calculating Recall :

$$Recall = \frac{TP}{TP + FN}$$

Substitution :

$$Recall = \frac{49.550}{49.550 + 450}$$

$$Recall = \frac{49.550}{50.000}$$

$$Recall = 99{,}10\%$$

4. Calculating F1-Score :

$$F1 = \frac{2\ X\ 98{,}51\ X\ 99{,}10}{98{,}51 + 99{,}10}$$

$$F1 = 98{,}80\%$$

4.6 Recap of Calculation Results

Table 8. Recap of Caluculation Results

Parameter	Score
Total Data	100.000
Trafik Normal	50.000
Trafik DDoS	50.000
True Positive (TP)	49.550
True Negative (TN)	49.250
False Positive (FP)	750
False Negative (FN)	450
Accuracy	98,80%
Precision	98,51%
Recall	99,10%
F1-Score	98,80%

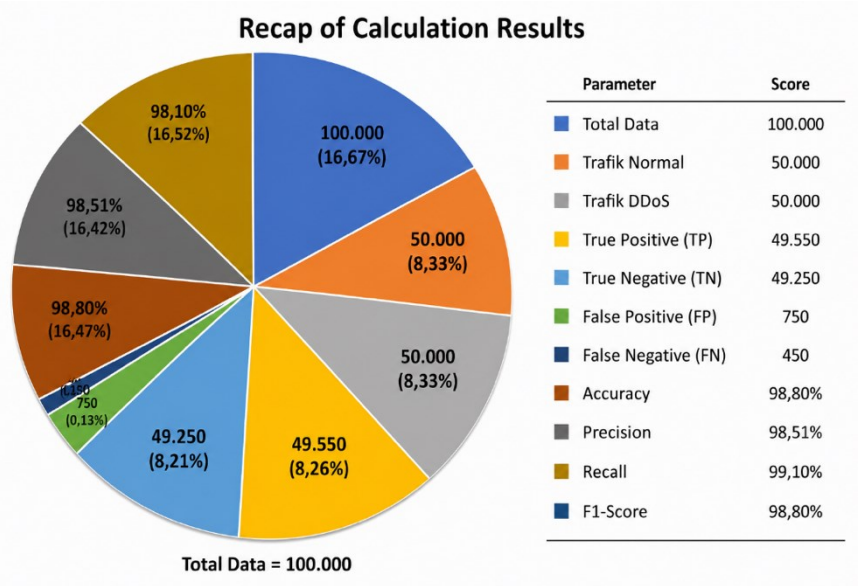

Figure 3. Recap of Calculation Results

Figure 3. Illustrates the performance of the Random Forest algorithm in detecting Distributed Denial of Service (DDoS) attacks. The pie chart presents the evaluation components, including Total Data, Normal Traffic, DDoS Traffic, True Positive (TP), True Negative (TN), False Positive (FP), False Negative (FN), as well as the performance metrics Accuracy, Precision, and Recall.
The results indicate that the majority of the network traffic was correctly classified as either normal traffic or DDoS traffic, as reflected by the high True Positive (TP) and True Negative (TN) values. In contrast, the numbers of False Positive (FP) and False Negative (FN) are relatively low, indicating a low classification error rate.
The high values of Accuracy, Precision, and Recall demonstrate that the Random Forest algorithm is effective in detecting DDoS attacks while maintaining reliable classification performance between legitimate and malicious network traffic. These findings suggest that the Random Forest algorithm is a suitable Machine Learning model for DDoS detection and automated network attack prevention.
The Use of 50,000 Normal Traffic Records and 50,000 DDoS Traffic Records
The use of 50,000 normal traffic records and 50,000 DDoS traffic records in this Machine Learning study is based on methodological considerations.
1. Maintaining a Balanced Dataset
Using an equal number of samples for the Normal and DDoS classes is intended to prevent class imbalance.
A balanced dataset provides the following advantages :

- The model learns the characteristics of both classes proportionally.
- It reduces the model's tendency to favor the class with the larger number of samples.
- The evaluation results become more objective and reliable.
- Hasil evaluasi menjadi lebih objektif.

2. Reducing Model Bias
If the data is imbalanced, for example :

Table 4.7 If the data is imbalanced

Normal	DDoS
90.000	10.000

Models can tend to classify most of the data as Normal because that class is more dominant. As a result, the accuracy might look high, but the ability to detect DDoS attacks is actually low. A balanced dataset helps reduce that risk.

3. Improving the Quality of Machine Learning Training
Algorithms like:
• Random Forest
• Decision Tree
• Support Vector Machine (SVM)
• XGBoost

It will learn patterns better if each class has an adequate number of examples.
The benefits :
• The model can more easily recognize the characteristics of normal traffic.
• The model can more easily recognize DDoS attack patterns.
• The risk of overfitting to one class becomes smaller.

4. Producing More Representative Evaluations
With a large and balanced amount of data, evaluation metrics such as:
• Accuracy
• Precision
• Recall
• F1-Score
Better reflects the model's actual ability.

4.7 Evaluation

Based on the evaluation and analysis results, the Random Forest algorithm shows excellent performance in detecting DDoS attacks on a dataset consisting of 50,000 normal traffic data and 50,000 DDoS traffic data. The model achieved an Accuracy of 98.80%, Precision of 98.51%, Recall of 99.10%, and F1-Score of 98.80%. These values indicate that the model can detect almost all DDoS attacks with a low error rate.

The relatively small number of False Positives and False Negatives shows that the system is not only accurate in distinguishing between normal traffic and attacks, but also has good potential to be implemented as a real-time DDoS detection and prevention mechanism on computer networks. These evaluation results support that a Machine Learning-

based approach, particularly the Random Forest algorithm, is an effective solution to enhance the security and availability of network services against DDoS attack threats.

V. CONCLUSION

Based on the results of the study 'Detection and Prevention of DDoS Attacks Using Machine Learning Algorithms on Computer Networks,' it can be concluded as follows:

1. Characteristics of network traffic affected by DDoS attacks compared to normal traffic. Research shows that network traffic under a DDoS attack has different characteristics from normal traffic. DDoS traffic is marked by an increase in the number of packets (packet rate), high flow bytes per second, flow packets per second, and repeated, intensive communication patterns in a short time. In contrast, normal traffic has a more stable packet distribution and doesn't show significant spikes in activity. These differences in characteristics form the basis for classification using Machine Learning algorithms.
2. Applying Machine Learning Algorithms to Detect DDoS Attacks. The Random Forest algorithm was successfully applied to build a model for detecting DDoS attacks. The research process included collecting datasets, preprocessing, feature selection, model training, and testing using test data. The resulting model can classify network traffic into two classes: normal traffic and DDoS traffic, based on the pattern characteristics learned from the training data.
3. Performance of the Machine Learning Algorithm in Distinguishing Normal Traffic and DDoS Traffic. Based on the evaluation results using the Confusion Matrix, the Random Forest algorithm shows really good performance with the following scores:
   - Accuracy: 98.80%
   - Precision: 98.51%
   - Recall: 99.10%
   - F1-Score: 98.80%

   These results show that the model has a high ability to distinguish between normal traffic and DDoS traffic. The high Recall value indicates that most attacks are successfully detected, while the high Precision value shows that there are few false alarms (False Positives). Therefore, the model is pretty reliable to be used in a DDoS attack detection system.`
4. Mechanism for preventing DDoS attacks based on Machine Learning detection results. The detection results using Machine Learning algorithms can be used as a basis for mechanisms to prevent DDoS attacks. Once the model identifies traffic categorized as an attack, the system can take automatic mitigation actions, such as :
   - Blocking the source IP addresses of the attack via a firewall,
   - Applying rate limiting to restrict traffic flow,
   - Updating rules in the Intrusion Prevention System (IPS),
   - Sending notifications to network administrators for further handling.

   This approach helps reduce the impact of attacks on network service availability and enhances the system's ability to respond to threats more quickly compared to manual mechanisms.

REFERENCES

[1]. Stallings, W. (2020). Network Security Essentials: Applications and Standards (7th ed.). Pearson.
[2]. Kurose, J. F., & Ross, K. W. (2022). Computer Networking: A Top-Down Approach (8th ed.). Pearson.
[3]. Mirkovic, J., & Reiher, P. (2004), A Taxonomy of DDoS Attack and DDoS Defense Mechanisms, ACM SIGCOMM Computer Communication Review, 34(2), 39–53.
[4]. Zargar, S. T., Joshi, J., & Tipper, D. (2013), A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks, IEEE Communications Surveys & Tutorials, 15(4), 2046–2069.
[5]. Zargar, S. T., Joshi, J., & Tipper, D. (2013), A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks, IEEE Communications Surveys & Tutorials, 15(4), 2046–2069.
[6]. Sommer, R., & Paxson, V. (2010), Outside the Closed World: On Using Machine Learning for Network Intrusion Detection, IEEE Symposium on Security and Privacy.
[7]. Buczak, A. L., & Guven, E. (2016), A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection, IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.
[8]. Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2019), Applying Deep Learning Approaches for Network Traffic Prediction, Intrusion Detection, and Future Internet Security, Book Chapter IGI Global.
[9]. Buczak, A. L., & Guven, E. (2016), A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection, IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.
[10]. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020),Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study, Journal of Information Security and Applications, 50, 102419.
[11]. Stallings, W. (2020), Data and Computer Communications (11th ed.), Publisher :Pearson.
[12]. Stallings, W., & Brown, L. (2018), Computer Security: Principles and Practice (4th ed.), Publisher :Pearson.
[13]. Bishop, M. (2019), Computer Security: Art and Science (2nd ed.), Publisher :Addison-Wesley.
[14]. Axelsson, S. (2000), Intrusion Detection Systems: A Survey and Taxonomy, Technical Report : Chalmers University of Technology.

[15]. Scarfone, K., & Mell, P. (2007), Guide to Intrusion Detection and Prevention Systems (IDPS), Publisher :National Institute of Standards and Technology (NIST), Special Publication 800-94.
[16]. Mitchell, T. M. (1997), Machine Learning, Publisher : McGraw-Hill.
[17]. Bishop, C. M. (2006), Pattern Recognition and Machine Learning, Publisher : Springer.
[18]. Buczak, A. L., & Guven, E. (2016), A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection, Journal : IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.
[19. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020), Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study,Journal : Journal of Information Security and Applications, 50, 102419.
[20]. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018), Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization (CICIDS2017), Conference : Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP).
[21]. Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009), A Detailed Analysis of the KDD CUP 99 Data Set, Conference : IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA).
[22]. Han, J., Kamber, M., & Pei, J. (2012). Data Mining: Concepts and Techniques (3rd ed.). Morgan Kaufmann.