Building of Informatics, Technology and Science (BITS)
Volume 6, No 4, March 2025 Page: 2335−2344
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i4.6727

Impact of SMOTE for Imbalance Class in DDoS Attack Detection Using Deep Learning MLP

Zidni Ilma, Wildanil Ghozi*, Fauzi Adi Rafrastara

Faculty of Computer Science, Informatics Engineering, Universitas Dian Nuswantoro, Semarang, Indonesia
Email: [1]111202113932@mhs.dinus.ac.id, [2,*]wildanil.ghozi@dsn.dinus.ac.id, [3]fauziadi@dsn.dinus.ac.id
Correspondence Author Email: wildanil.ghozi@dsn.dinus.ac.id
Submitted: **14/01/2025**; Accepted: **26/02/2025**; Published**: 01/03/2025**

Abstract−DDoS attacks, which are becoming increasingly complex and frequent, pose significant challenges to network security, particularly with the rise of cyber exploitation of infrastructure. A major issue in detecting these attacks is the imbalance between normal traffic and attack data, which causes machine learning models to be biased toward the majority class. To address this, this study proposes the use of the Synthetic Minority Over-sampling Technique (SMOTE) to balance the CIC-DDoS2019 dataset, successfully enhancing the performance of a Multi-Layer Perceptron (MLP) in detecting various types of attacks. Analysis results indicate that, on the original dataset without SMOTE, the model achieved high accuracy but low F1-Score for minority classes, highlighting difficulties in recognizing underrepresented attack patterns. After applying SMOTE, the F1-Score significantly improved for minority classes, demonstrating the model's enhanced ability to identify attack patterns. All dataset subsets showed improved performance across key evaluation metrics, indicating that SMOTE effectively expanded the model's decision boundary for minority classes, enabling MLP to detect DDoS attacks more accurately in previously challenging data patterns. This approach illustrates increased model sensitivity to minority feature distributions without significantly compromising performance on majority classes.

Keywords: DDoS; Anomaly Detection; SMOTE; Multi-Layer Perceptron; CIC-DDoS2019

1. INTRODUCTION

The rapid development of information and communication technology has significantly influenced global geography. In the 21st century, the world has become increasingly interconnected through the internet, shaping communication in commercial, political, economic, and socio-cultural fields [1]. The advancement of network technology has been driven by continuously evolving computers and diverse user segments [2]. However, the widespread use of network technology has introduced critical security challenges. Numerous efforts have been made to establish a secure cyber environment to protect institutional, organizational, and individual assets. DDoS attacks often exploit cloud infrastructure services such as pay-as-you-go, auto-scaling, and multi-tenancy by overloading traffic, disrupting service access for legitimate users. According to data from Cloudflare and Gcore in Q1 2024, DDoS attacks surged by 46% compared to the same period in 2023 [3]. The motive behind these attacks, termed Economical Denial of Sustainability (EDoS), involves attackers persistently triggering resource usage, forcing cloud services to automatically scale capacity, thereby significantly increasing user costs [4].

The evolution of DDoS attacks has led to more sophisticated techniques, such as amplified reflection DDoS (AR-DDoS). This attack exploits the connectionless nature of UDP protocols by sending spoofed requests to misconfigured open servers, which then respond excessively, targeting the victim [5]. Recent reports from NETSCOUT revealed a sharp 34% increase in Amplified Reflection DDoS attacks in the first half of 2024 compared to the same period the previous year, making them increasingly difficult to detect [6]. The success of such attacks is driven by poorly managed reflector servers, minimal effort required to execute the attack, and the challenge of distinguishing attack traffic from normal traffic, as attackers use third-party servers to mask the source of the attack [7].

Data imbalance poses a significant challenge in detecting DDoS attacks, particularly in network security systems. This imbalance occurs when attack traffic data dominates the dataset compared to normal traffic, making it difficult for machine learning models to learn effectively. Models tend to be biased toward the majority class, reducing sensitivity to the minority class, which is the primary focus of detection. This imbalance often results in high false-negative rates, where DDoS attacks go undetected and are classified as normal traffic, allowing the attacks to continue unnoticed [8]. Additionally, models with high accuracy on the majority class can create an illusion of good performance while failing to detect critical patterns in the minority class [9]. Such misclassification not only increases network vulnerability but also reduces the reliability of detection systems in complex environments [10]. Addressing data imbalance is a crucial step in enhancing the efficiency and accuracy of attack detection systems.

To address this imbalance, solutions such as Synthetic Minority Over-sampling Technique (SMOTE) are crucial for enhancing the effectiveness of detection systems, particularly against cyberattacks like DDoS. SMOTE has proven to be an effective technique for balancing datasets by systematically adding synthetic samples to the minority class, overcoming the limitations of traditional methods like Random Undersampling (RUS), which often remove important information from the majority class [11]. By balancing data distribution, SMOTE enables machine learning models to focus more on minority class patterns without compromising majority class information. This technique works by generating synthetic samples through interpolation between existing minority data points, expanding the model's decision space and ensuring that unique minority class patterns can be effectively learned [12]. Integrating

Building of Informatics, Technology and Science (BITS)
Volume 6, No 4, March 2025 Page: 2335−2344
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i4.6727

SMOTE with algorithms like Multi-Layer Perceptron (MLP) is significant, as MLP requires sufficient data to optimally detect non-linear patterns. SMOTE enhances sensitivity to attack variations, reduces false-negative rates, and maintains performance on the majority class while minimizing overfitting risks typically associated with scarce minority data.

Several previous studies support the effectiveness of deep learning in detecting DDoS attacks, Sharmin Aktar and Abdullah Yasin Nur (2023) [13] proposed a Deep Contractive Autoencoder (DCAE) model for detecting network anomalies based on reconstruction error. This semi-supervised learning approach used only normal data for training, improving the detection of previously unknown attacks. Compared to LSTM AE, Variational Autoencoder (VAE), and Basic Autoencoder (Basic AE), DCAE demonstrated superior performance with 97.58% accuracy on the CIC-DDoS2019 dataset. DCAE also excelled in handling non-linear and complex data through contractive regularization, enhancing the model's resilience to minor variations in input data. The study employed a stochastic threshold method to minimize detection errors, including false positives and false negatives. Evaluations on other datasets, such as NSL-KDD and CIC-IDS2017, also showed consistent performance with accuracies of 96.08% and 92.45%, respectively, outperforming other approaches.

A study conducted by Rissal Efendi in 2024 [14] proposed an efficient strategy for detecting DDoS attacks by combining SMOTE (Synthetic Minority Over-sampling Technique) with Long Short-Term Memory (LSTM) models. The study focused on addressing data imbalance in network datasets by applying SMOTE to increase minority class samples, enabling the model to better learn temporal patterns and network anomalies. Experimental results indicated that applying SMOTE to LSTM models significantly improved DDoS attack detection performance, reducing validation loss from 0.1934 to 0.0428 and increasing validation accuracy from 97.50% to 99.50%. Additionally, the F1-Score for minority classes increased from 93.4% to 98.3%, reflecting enhanced model capability in recognizing rare and complex attack patterns. This study highlights the importance of data balancing techniques like SMOTE in improving the performance of deep learning models for network security applications, particularly on imbalanced data.

This study aims to address the identified research gap by integrating the Synthetic Minority Over-sampling Technique (SMOTE) with the Multi-Layer Perceptron (MLP) model to enhance the detection of DDoS attacks in complex and imbalanced network environments. Building upon prior research that has demonstrated the efficacy of SMOTE in addressing data imbalance and the capability of MLP in capturing non-linear relationships. Combination of these methods advances the field by specifically addressing the challenges posed by minority attack classes. Evaluation results showed that the MLP model trained with a balanced dataset through SMOTE achieved increased sensitivity to minority class attack patterns that were previously difficult to detect. Evaluation metrics such as precision, recall, and F1-Score improved significantly for minority attacks, while performance on majority classes remained stable without significant decline. By achieving a more balanced data distribution, SMOTE enables models to detect DDoS attacks more accurately and effectively, reducing false-negative risks and enhancing the reliability of detection systems in addressing dynamic attack patterns.

2. RESEARCH METHODOLOGY

The study commenced with data collection from the CIC-DDoS2019 dataset. Preprocessing involved several steps, including removing duplicate entries to ensure the dataset contained only unique records, thereby avoiding redundancy and bias in the analysis. Additionally, features were normalized to ensure uniform scaling, and data quality was addressed by eliminating invalid and missing values. These steps were crucial to preparing the dataset for effective and reliable analysis. To address data imbalance, SMOTE was applied to balance the class distribution. The modeling phase utilized the MLP algorithm for DDoS attack detection, with evaluation metrics including accuracy, F1-Score, recall, and a confusion matrix. These stages ensured the reliability of the DDoS detection system, as illustrated in Figure 1.

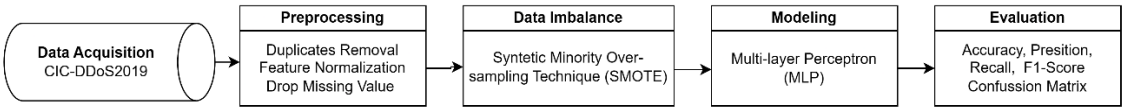

Figure 1. The Proposed Methodology

2.1 Data Acquisition

In the initial stage, a study was conducted on the dataset under investigation, including its characteristics and feature structure. The Canadian Institute for Cybersecurity collected the CICDDoS2019 dataset using Wireshark in a simulated environment. This dataset includes two types of attacks: reflection-based and exploitation-based attacks [15]. Reflection-based attacks leverage TCP, UDP, or a combination of both protocols, while exploitation-based attacks employ methods exploiting TCP connection mechanisms and open UDP ports. The dataset contains 88 network traffic features generated using CICFlowMeter-V3 [16] and is stored in CSV format. This study examines

Building of Informatics, Technology and Science (BITS)
Volume 6, No 4, March 2025 Page: 2335−2344
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i4.6727

seven different types of attacks, namely MSSQL, SYN, PortMap, LDAP, NetBIOS, UDP-Lag, and UDP, as shown in Table 1.

Table 1. CIC-DDoS2019 Subset

Dataset	Total Label	Flows
MSSQL	3	5775786
SYN	2	4320541
PortMap	2	191694
LDAP	3	2113234
NetBIOS	2	3455899
UDPLag	4	725165
UDP	3	3782206

2.2 Preprocessing Data

Data preparation is a critical process for understanding and preparing data for use in a model, encompassing several essential stages, including data cleaning, addressing class imbalance, and feature extraction to obtain relevant information from the dataset. The preprocessing process involves crucial steps to ensure the data is ready for model training. First, we removed duplicate data and irrelevant columns for classification, such as Flow ID, Source IP, Source Port, Destination IP, Destination Port, Protocol, and Timestamp, to prevent overfitting caused by network variations [17].

Label Encoding was applied for binary classification or ordinal categorical data, where categories are assigned integer values. For instance, the label "Normal" may be encoded as 0 and "Attack" as 1, simplifying the model's interpretation. For non-ordinal categorical features, One-Hot Encoding was employed, creating binary vectors for each category. For example, protocol types such as TCP, UDP, and ICMP were encoded as (1,0,0), (0,1,0), and (0,0,1), respectively. Similarly, features like "flag" and "services," which contain multiple categories, were expanded into multiple binary features. This process ensures the model treats categories as distinct entities without introducing ordinal bias, thereby enhancing feature representation during training.

To maintain the dataset's integrity and ensure meaningful feature calculations, all rows containing NaN or Inf values were removed. These invalid values can arise due to issues in data collection or feature computation and can negatively impact model performance, leading to errors during computation. By removing these rows, the dataset was cleaned to ensure the input data remained valid and did not introduce bias or inconsistencies during the training process. The numerical features in the dataset were normalized using a Standard Scaler, ensuring each feature has a mean of 0 and a standard deviation of 1. This standardization process is crucial for machine learning models sensitive to the scale of input features, such as models that use gradient-based optimization.

$$z = \frac{x - \mu}{\sigma} \tag{1}$$

Where x represents the feature value, μ is the mean, and σ is the standard deviation of the feature. By standardizing the dataset, model convergence during training is improved, and the influence of features with larger scales on the loss function is minimized. This ensures that all features contribute equally during the training process, enhancing the model's robustness in detecting anomalies and variations in the data.

2.3 Data Imbalance with SMOTE

In network attack datasets, the number of abnormal samples is significantly larger than the number of normal samples, resulting in severe data imbalance that hinders the performance of classification models during the detection training process. To address this issue, an over-sampling method is applied with the aim of increasing the minority class samples by generating new synthetic samples rather than merely duplicating them, as seen in methods like Random Over-Sampling (ROS). This approach reduces the risk of overfitting during the development of classification models [18]. The technique operates by creating synthetic points between minority class samples and their nearest neighbors, using Euclidean distance as a reference to expand the decision boundary of the minority class. This enhances class representation and ultimately improves the generalization ability of the classification model [19].

$$Enew = Ei + (Ei - Ej)\delta \tag{2}$$

In this formula, Ei represents an original data point from the minority class, while Ej is the nearest neighbor of Ei, also from the minority class. The combination of these two points generates a new synthetic sample between them, thereby expanding the representation of the minority class in the feature space. This process is designed to improve data distribution, enabling the classification model to learn minority class patterns more effectively and reducing bias toward the majority class.

2.4 Modeling with Deep Learning MLP

Modeling in data and analytics involves creating mathematical or statistical models to identify patterns and make predictions based on data [20]. This study employs a Multilayer Perceptron (MLP), an artificial neural network

Building of Informatics, Technology and Science (BITS)
Volume 6, No 4, March 2025 Page: 2335−2344
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i4.6727

consisting of an input layer, three hidden layers with 15, 10, and 8 neurons, and an output layer with 6 neurons. MLP is particularly effective for structured datasets, like those analyzed in this research, due to its ability to uncover complex patterns and relationships, making it suitable for detecting network attacks, including DDoS [21, 22]. The model utilizes ReLU as the activation function for hidden layers and Softmax for the output layer. The output of each layer is computed through the forward pass equation :

$$a^1 = \phi(W^1.a^{1-1} + b^1) \tag{3}$$

Forward pass calcultates the output of each layer, where W^1 and b^1 are the weights and biases, a^{1-1} is the previous layer's output and ϕ is the activation function.

$$W^1 \leftarrow W^1 - \eta.\frac{\widehat{m}_t}{\sqrt{\widehat{v}_t+\epsilon}} \tag{4}$$

Adam optimizer updates weights W^1 by combining momentum-based methods for efficient convergence, where η is the learning rate, $\widehat{m}_t$ is the bias-corrected first moment estimate and $\widehat{v}_t$ is the bias-corrected second moment estimate.

$$\mathcal{L}(y, \hat{y}) = -\frac{1}{N}\sum_{i=1}^{N} \sum_{k=1}^{C} yik \log \hat{y}ik \tag{5}$$

CrossEntropyLoss measures the difference between the predicted probabilities $\hat{y}$ and the true labels y in classification tasks, where N is the number of samples, C is the number of classes, yik is the true label, and $\hat{y}ik$ is the predicted probability for class k of sample i
The model's hyperparameters, including 10 epochs, a batch size of 300, and the use of Adam optimizer and CrossEntropyLoss, are detailed in Table 2.

Table 2. Hyperparameters of our model

Parameter	Value
Epoch & Batch Size	10 / 300
Activation Function	ReLU(Hidden) / Softmax(Output)
Optimizer	Adam
Loss Function	CrossEntropyLoss
No of Hidden Layers	3
Hidden Neuron Size	15 / 10 / 8 / 6

2.5 Performance Evaluation

The model evaluation is conducted to measure the effectiveness of the model in detecting DDoS intrusions using the Classification Report and Confusion Matrix as the primary methods. Four key performance metrics are utilized: Accuracy, Precision, Recall, and F1-Score, which are calculated based on the values of True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN). TP refers to positive data correctly identified as positive, while TN refers to negative data correctly identified as negative. Conversely, FP occurs when negative data is incorrectly classified as positive, and FN occurs when positive data is mistakenly classified as negative. These metrics provide a comprehensive overview of the model's ability to accurately detect attacks, avoid detection errors, and maintain a balance between precision and sensitivity. The following are the formulas for calculating these evaluation metrics :

$$Accuracy = \frac{TP}{TP+TN+FP+FN} \tag{6}$$

Accuracy: The ratio of the number of anomalous and normal instances correctly classified to the total number of all instances.

$$Precision = \frac{TP}{TP+FP} \tag{7}$$

Precision: The ratio of the number of attack samples correctly classified to the total number of instances classified as attacks.

$$Recall = \frac{TP}{TP+FN} \tag{8}$$

Recall: The ratio of the number of anomalous instances correctly classified to the total number of actual anomalous instances.

$$F1 - Score = \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{9}$$

F1-Score: The harmonic mean between precision and recall metrics, representing the overall performance of the model.

Building of Informatics, Technology and Science (BITS)
Volume 6, No 4, March 2025 Page: 2335−2344
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i4.6727

These formulas are utilized to quantitatively interpret the model's performance and provide a more accurate evaluation of the model's effectiveness in intrusion detection.

3. RESULT AND DISCUSSION

This section elaborates on the research findings and experimental analysis conducted using the Multi-Layer Perceptron (MLP) model combined with the Synthetic Minority Over-sampling Technique (SMOTE) to rapidly and accurately detect anomalies in DDoS attacks. The integration of MLP and SMOTE aims to enhance anomaly detection capabilities, particularly in imbalanced datasets, by automatically identifying attack patterns with high precision.

3.1 Class Distribution Comparison

In the CIC-DDoS2019 dataset, a significant data imbalance is observed, where attack labels dominate the dataset with far more samples compared to the Benign (normal traffic) label. This condition indicates that the dataset is heavily skewed towards attack patterns, while normal traffic data is underrepresented. Such an imbalance can introduce bias into the detection model, making it more accurate in identifying attack patterns but less effective in detecting normal traffic. This limitation may reduce the model's generalization ability, particularly when applied to more diverse real-world network data. The class distribution in the CIC-DDoS2019 dataset is illustrated in Figure 2.

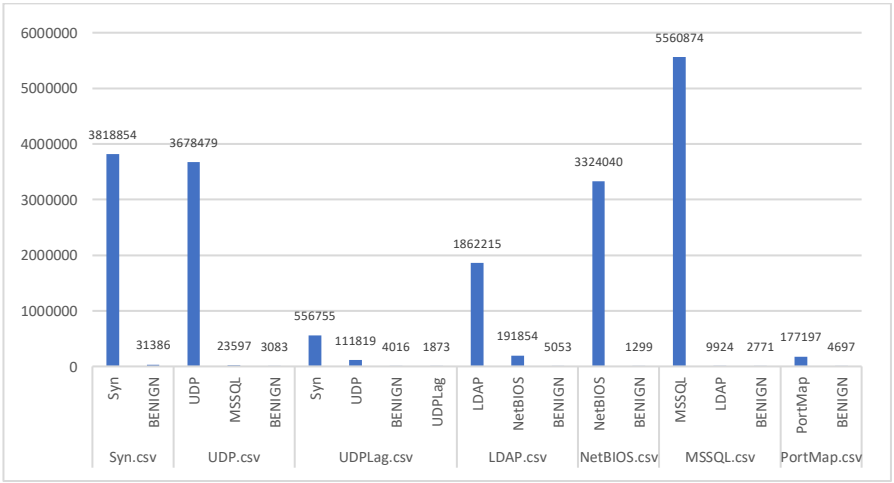

Figure 2. Class Distribution Before SMOTE

From the diagram in Figure 2, it is evident that the dataset exhibits significant class imbalance among various types of attacks. The MSSQL class has the highest number of samples, reaching 5,787,453, followed by the SYN, UDP, and NetBIOS classes, each with millions of samples. Conversely, classes such as UDPLag, PortMap, and Benign have significantly fewer samples, with UDPLag having only 1,873 samples. This imbalance indicates that the dataset is dominated by a few majority classes, while minority classes are underrepresented.

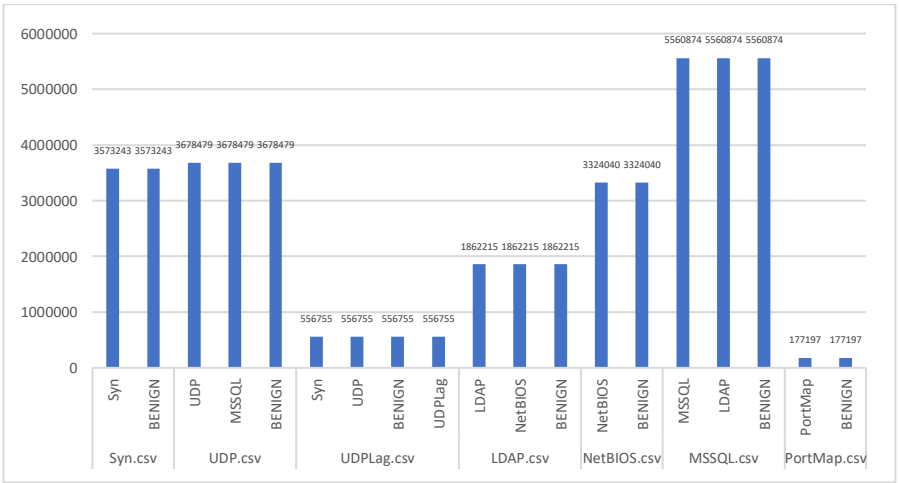

Figure 3. Class Distribution After SMOTE

In Figure 3, it is shown that after applying the proposed method, SMOTE, the dataset distribution was successfully balanced for each attack label in their respective subsets. The data underwent preprocessing steps, including the removal of NaN and Inf values, to ensure the data was clean and suitable for training purposes. The final

Building of Informatics, Technology and Science (BITS)
Volume 6, No 4, March 2025 Page: 2335−2344
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i4.6727

results indicate that each attack label, such as SYN, UDP, UDPLag, LDAP, NetBIOS, MSSQL, and PortMap, as well as the BENIGN label, achieved equal distribution after SMOTE was applied. For instance, in the Syn.csv subset, both the SYN and BENIGN labels have a balanced distribution of 3,818,854 samples. Similar balancing was observed in other subsets, such as UDP.csv and UDPLag.csv, where all classes were equalized, as depicted in Figure 3.

The approach of modeling datasets separately for each subset ensures that the specific characteristics of each attack type can be thoroughly learned by the model. Each subset, such as Syn.csv, UDP.csv, and others, represents unique network traffic patterns and features tailored to the specific type of attack. Combining all subsets into one large dataset could blend these unique patterns, potentially reducing the model's ability to identify distinctive characteristics of each attack. By separating the dataset based on attack types, the model can focus on relevant features for detecting specific patterns, such as those in SYN and LDAP attacks, which may differ significantly from patterns in UDPLag or PortMap attacks. Additionally, this separation helps mitigate bias that might arise if the majority class dominates a combined dataset, even with the application of SMOTE. Practically, this approach enables more controlled testing, targeted performance evaluation for each attack type, and minimizes the risk of overfitting, allowing the model to capture relevant patterns for each attack type more effectively.

3.2 Metric Evaluation Comparison

The purpose of this comparative evaluation is to analyze the model's performance in detecting DDoS attacks on an imbalanced dataset and after applying the SMOTE technique as the proposed method. The evaluation is conducted using accuracy, precision, recall, and F1-Score metrics across seven tested attack types. The comparison aims to identify the impact of data distribution on the model's ability to recognize attack patterns, as shown in Table 3.

Table 3. Evaluation Without SMOTE

Attack Name	Accuracy	Precision	Recall	F1-Score
Syn	0.9995	0.9663	1	0.9853
UDP	0.9993	0.6534	0.6663	0.6663
UDPLag	0.9996	0.7256	0.7554	0.7354
LDAP	0.9996	0.9996	1	0.9996
NetBIOS	1	0.9997	0.9997	0.9997
MSSQL	0.9982	0.6564	0.6677	0.6545
PortMap	0.9990	0.9890	0.9990	0.9990

In Table 3, the evaluation without using SMOTE shows that the model performs fairly well for most types of attacks. Attacks such as NetBIOS and LDAP demonstrate optimal results with accuracy, precision, recall, and F1-Score each reaching 1 or close to 1. This indicates that the model can effectively recognize attack patterns in both majority and minority classes. However, for certain types of attacks, such as UDP and MSSQL, despite the accuracy metrics showing good results, the F1-Scores for these attacks reflect poor performance, scoring 0.6663 and 0.6545 respectively. This situation likely arises from the data imbalance in the dataset, causing the model to struggle in recognizing attack patterns in minority classes. The model tends to prioritize majority classes, leading to reduced performance in detecting other classes.

Table 4. Evaluation with Purpose Method

Attack Name	Accuracy	Precision	Recall	F1-Score
Syn	0.9991	0.9991	0.9991	0.9991
UDP	0.9828	0.9828	0.9828	0.9828
UDPLag	0.9519	0.9532	0.9519	0.9517
LDAP	0.9992	0.9992	0.9992	0.9992
NetBIOS	0.9999	0.9999	0.9999	0.9999
MSSQL	0.9898	0.9898	0.9898	0.9898
PortMap	0.9985	0.9985	0.9985	0.9985

In Table 4, after applying SMOTE, the evaluation shows significant changes in several attack types. UDP and MSSQL, which previously had lower F1-Scores compared to other attacks, experienced an overall improvement in metrics. Although UDP exhibited a decrease in accuracy by 0.0102, its F1-Score increased significantly by 0.3168, from 0.66 to 0.9828. Similarly, MSSQL demonstrated an F1-Score improvement, achieving 0.9898. Additionally, attack types such as NetBIOS, LDAP, and PortMap maintained excellent performance with metrics close to perfection, indicating that majority class data was still well-accommodated by the model despite the application of SMOTE. For UDPLag, the F1-Score increased to 0.9517, suggesting that SMOTE effectively enhanced the model's ability to recognize minority class data more accurately.

Although a decrease in accuracy was observed across all attack types, improvements in precision and recall indicate that the model was able to reduce detection errors, both in terms of False Positives and False Negatives. These improvements suggest that the synthetic data distribution from SMOTE expanded the decision boundary of the model,

Building of Informatics, Technology and Science (BITS)
Volume 6, No 4, March 2025 Page: 2335−2344
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i4.6727

enabling it to recognize UDPLag attack patterns more effectively, although there is still room to improve generalization for more complex data characteristics.

This evaluation demonstrates that the application of SMOTE impacts the model's performance differently depending on the characteristics of each attack type. For minority class data, SMOTE enhances data representation and helps the model recognize attack patterns, although synthetic distributions can occasionally introduce noise that affects the model's generalization ability. Meanwhile, performance on majority class data remains stable, indicating that the method does not significantly negatively impact majority classes.

3.3 Confussion Matrix

The confusion matrix provides an overview of the model's performance, including correct predictions (True Positives and True Negatives) and errors (False Positives and False Negatives). This analysis helps in understanding detection patterns for majority and minority labels, as well as the challenges in identifying attacks with overlapping data or limited samples. The visualization in Figure 4 is used to evaluate the model's accuracy across each subset of the dataset.

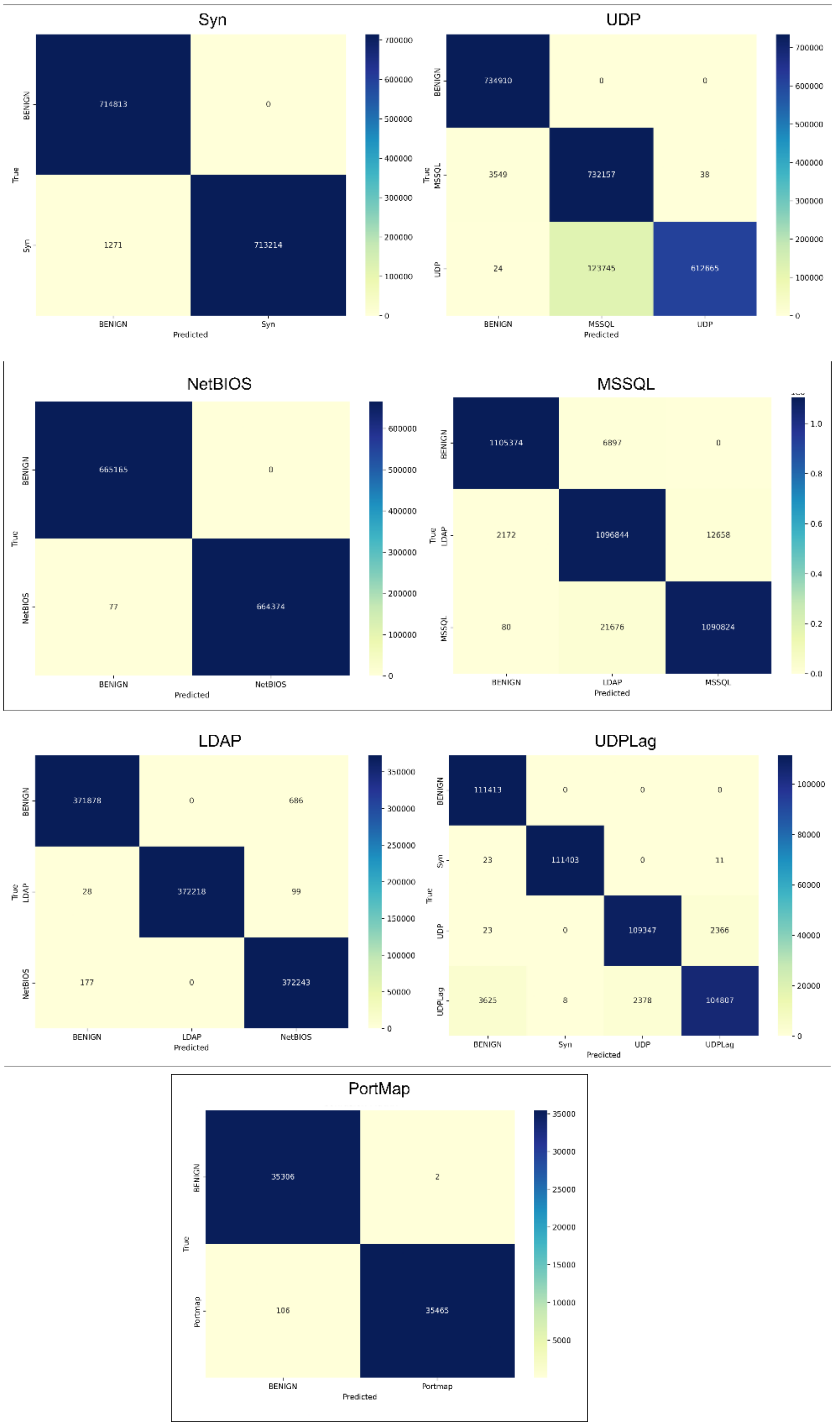

Figure 4. Confussion Matrix Visualization

Building of Informatics, Technology and Science (BITS)
Volume 6, No 4, March 2025 Page: 2335−2344
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i4.6727

The confusion matrix visualization in Figure 4 illustrates the model's performance in detecting seven types of DDoS attacks across dataset subsets, including SYN, UDP, MSSQL, NetBIOS, LDAP, UDPLag, and PortMap, as well as BENIGN traffic. The model demonstrates a high capability in identifying majority labels like SYN, UDP, MSSQL, and NetBIOS, as evidenced by dominant True Positives and True Negatives. However, for minority classes such as UDPLag and PortMap, some False Positives and False Negatives were observed, indicating challenges in recognizing underrepresented or overlapping attack patterns. Despite this, subsets like PortMap still exhibited reasonably good performance, even with limited data. This analysis highlights the model's accuracy in recognizing majority patterns while addressing challenges associated with minority classes.

3.4 Comparison to Previous Research

Previous research has employed various deep learning-based methods to detect DDoS attacks on the CIC-DDoS2019 dataset. For instance, Sharmin Aktar and Abdullah Yasin Nur (2023) [13] proposed a Deep Contractive Autoencoder (DCAE)-based approach for detecting network anomalies. The study compared the performance of DCAE with other deep learning methods, including LSTM AE, VAE, and Basic AE. Experimental results indicate that MLP combined with SMOTE outperformed these methods, achieving higher accuracy in detecting attacks on the CIC-DDoS2019 dataset, as demonstrated in Table 5.

Table 5. Accuracy Evaluation with Purpose Method

Algorithm	LDAP	UDP	MSSQL	PortMap	Syn	UDPLag	NetBIOS
LSTM AE	94.10	87.98	95.33	88.60	95.40	70.46	78.32
VAE	90.20	70.46	84.48	77.15	78.35	70.50	79.50
Sharmin Approach	95.86	97.58	97.33	95.97	95.12	93.41	93.88
Basic AE	93.09	87.56	80.39	87.27	82.01	75.82	86.17
Zidni Approach	**99.92**	**98.28**	**98.98**	**99.85**	**99.91**	**95.19**	**99.99**

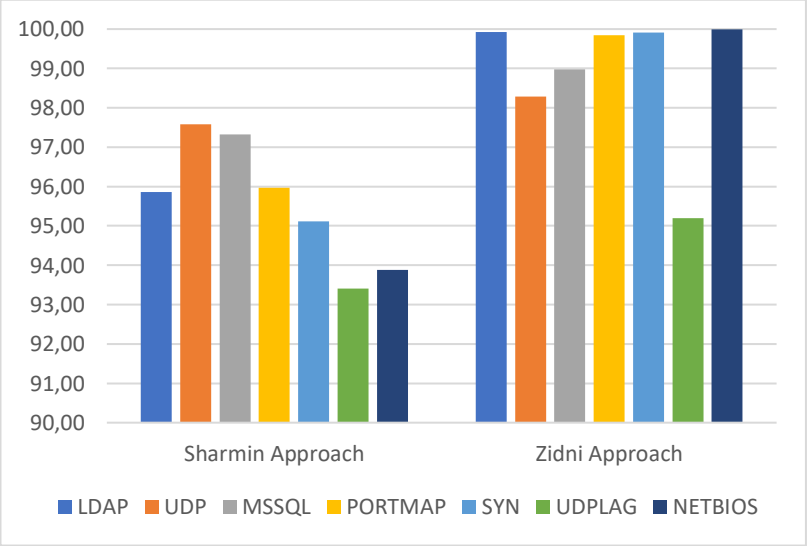

Figure 5. Comparison Visualization

The graph in Figure 5 demonstrates that the Zidni Approach consistently outperforms the Sharmin Approach across all attack categories, achieving near-perfect accuracy in most categories, such as LDAP (99.92%), UDP (98.28%), MSSQL (98.98%), PORTMAP (99.85%), SYN (99.91%), UDPLAG (95.19%), and NETBIOS (99.99%). The Zidni Approach records a significant improvement of up to +6.11% in certain categories, attributed to its combination of deep learning and data optimization techniques like SMOTE. These results highlight the superiority of the Zidni Approach in detecting anomalous patterns within complex and imbalanced data, establishing it as a more reliable solution for DDoS attack detection across various categories.

4. CONCLUSION

This study confirms the effectiveness of Multi-Layer Perceptron (MLP) combined with Synthetic Minority Over-sampling Technique (SMOTE) as an approach to address class imbalance in DDoS attack detection. The evaluation results demonstrate that SMOTE significantly enhances the model's performance in detecting various types of attacks, especially within minority classes. On the original imbalanced dataset, the model struggled to detect minority class attacks, such as UDPLag and PortMap, as indicated by low precision and recall values. However, after applying

Building of Informatics, Technology and Science (BITS)
Volume 6, No 4, March 2025 Page: 2335−2344
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i4.6727

SMOTE, performance improvements were evident across all key evaluation metrics. For example, in the SYN attack category, the model achieved an accuracy of 99.91%, precision of 99.91%, recall of 99.91%, and an F1-score of 99.91%. Similarly, for UDPLag attacks, significant improvements were observed, with accuracy reaching 95.19%, recall 95.19%, and an F1-score of 95.17%. Although some labels, like UDPLag, still presented challenges with minor false positives, these results demonstrate that SMOTE successfully enhances the model's ability to recognize attack patterns in minority classes while maintaining high performance on majority classes. This improvement indicates that SMOTE aids the model in learning from a more representative dataset, reducing bias toward majority classes and providing better generalization capability. This approach has practical implications for real-time DDoS attack detection, enabling more reliable network security by minimizing undetected threats. However, this study also has limitations, such as potential overfitting on certain synthetic data and increased computational time due to data augmentation. Future research could explore alternative data augmentation techniques, optimize SMOTE parameters, or apply similar approaches to other types of attacks to generalize these findings. This strategy holds promise for developing more advanced and adaptive intrusion detection systems to counter evolving security threats.

REFERENCES

[1] A. Maslan, K. M. Bin Mohamad, and F. Binti Mohd Foozy, "Feature selection for DDoS detection using classification machine learning techniques," IAES Int. J. Artif. Intell. IJ-AI, vol. 9, no. 1, p. 137, Mar. 2020, doi: 10.11591/ijai.v9.i1.pp137-145.

[2] M. Shurman, R. Khrais, and A. Yateem, "DoS and DDoS Attack Detection Using Deep Learning and IDS," Int. Arab J. Inf. Technol., vol. 17, no. 4A, pp. 655–661, Jul. 2020, doi: 10.34028/iajit/17/4A/10.

[3] A. Bonguet and M. Bellaiche, "A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing," Future Internet, vol. 9, no. 3, p. 43, Aug. 2017, doi: 10.3390/fi9030043.

[4] M. N. Faiz, O. Somantri, A. R. Supriyono, and A. W. Muhammad, "Impact of Feature Selection Methods on Machine Learning-based for Detecting DDoS Attacks : Literature Review," J. Inform. Telecommun. Eng., vol. 5, no. 2, pp. 305–314, Jan. 2022, doi: 10.31289/jite.v5i2.6112.

[5] M. A. Sotelo Monge, J. Maestre Vidal, and G. Martínez Pérez, "Detection of economic denial of sustainability (EDoS) threats in self-organizing networks," Comput. Commun., vol. 145, pp. 284–308, Sep. 2019, doi: 10.1016/j.comcom.2019.07.002.

[6] X. Z. Khooi, L. Csikor, D. M. Divakaran, and M. S. Kang, "DIDA: Distributed In-Network Defense Architecture Against Amplified Reflection DDoS Attacks," in 2020 6th IEEE Conference on Network Softwarization (NetSoft), Ghent, Belgium: IEEE, Jun. 2020, pp. 277–281. doi: 10.1109/NetSoft48620.2020.9165488.

[7] H. Polat, O. Polat, and A. Cetin, "Detecting DDoS Attacks in Software-Defined Networks Through Feature Selection Methods and Machine Learning Models," Sustainability, vol. 12, no. 3, p. 1035, Feb. 2020, doi: 10.3390/su12031035.

[8] M. Šimon and L. Huraj, "A Study of DDoS Reflection Attack on Internet of Things in IPv4/IPv6 Networks," in Software Engineering Methods in Intelligent Algorithms, vol. 984, R. Silhavy, Ed., in Advances in Intelligent Systems and Computing, vol. 984. , Cham: Springer International Publishing, 2019, pp. 109–118. doi: 10.1007/978-3-030-19807-7_12.

[9] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," IEEE Access, vol. 7, pp. 41525–41550, 2019, doi: 10.1109/ACCESS.2019.2895334.

[10] M. P. Novaes, L. F. Carvalho, J. Lloret, and M. L. Proenca, "Long Short-Term Memory and Fuzzy Logic for Anomaly Detection and Mitigation in Software-Defined Network Environment," IEEE Access, vol. 8, pp. 83765–83781, 2020, doi: 10.1109/ACCESS.2020.2992044.

[11] P. Devan and N. Khare, "An efficient XGBoost–DNN-based classification model for network intrusion detection system," Neural Comput. Appl., vol. 32, no. 16, pp. 12499–12514, Aug. 2020, doi: 10.1007/s00521-020-04708-x.

[12] D. Alghazzawi, O. Bamasag, H. Ullah, and M. Z. Asghar, "Efficient Detection of DDoS Attacks Using a Hybrid Deep Learning Model with Improved Feature Selection," Appl. Sci., vol. 11, no. 24, p. 11634, Dec. 2021, doi: 10.3390/app112411634.

[13] S. Aktar and A. Yasin Nur, "Towards DDoS attack detection using deep learning approach," Comput. Secur., vol. 129, p. 103251, Jun. 2023, doi: 10.1016/j.cose.2023.103251.

[14] R. Efendi, T. Wahyono, and I. R. Widiasari, "LSTM SMOTE: An Effective Strategies for DDoS Detection in Imbalanced Network Environments," Jul. 24, 2024, Computer Science and Mathematics. doi: 10.20944/preprints202407.1825.v1.

[15] "University of New Brunswick. DDoS Evaluation Dataset (CIC-DDoS2019). 2019." Access Date Dec 2024, [Online]. Available: https://www.unb.ca/cic/

[16] "CIC Flow Meter. 2020." Canadian Institute for Cybersecurity, Access Date Dec 2024, [Online]. Available: https://github.com/CanadianInstituteForCybersecurity/ CICFlowMeter."

[17] N. M. Yungaicela-Naula, C. Vargas-Rosales, and J. A. Perez-Diaz, "SDN-Based Architecture for Transport and Application Layer DDoS Attack Detection by Using Machine and Deep Learning," IEEE Access, vol. 9, pp. 108495–108512, 2021, doi: 10.1109/ACCESS.2021.3101650.

[18] H. Zhang, L. Huang, C. Q. Wu, and Z. Li, "An effective convolutional neural network based on SMOTE and Gaussian mixture model for intrusion detection in imbalanced dataset," Comput. Netw., vol. 177, p. 107315, Aug. 2020, doi: 10.1016/j.comnet.2020.107315.

[19] T. Wu, H. Fan, H. Zhu, C. You, H. Zhou, and X. Huang, "Intrusion detection system combined enhanced random forest with SMOTE algorithm," EURASIP J. Adv. Signal Process., vol. 2022, no. 1, p. 39, Dec. 2022, doi: 10.1186/s13634-022-00871-6.

[20] D. Kumar, R. K. Pateriya, R. K. Gupta, V. Dehalwar, and A. Sharma, "DDoS Detection using Deep Learning," Procedia Comput. Sci., vol. 218, pp. 2420–2429, 2023, doi: 10.1016/j.procs.2023.01.217.

Building of Informatics, Technology and Science (BITS)
Volume 6, No 4, March 2025 Page: 2335−2344
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i4.6727

[21] J. A. Perez-Diaz, I. A. Valdovinos, K.-K. R. Choo, and D. Zhu, "A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning," IEEE Access, vol. 8, pp. 155859–155872, 2020, doi: 10.1109/ACCESS.2020.3019330.

[22] M. S. E. Sayed, N.-A. Le-Khac, M. A. Azer, and A. D. Jurcut, "A Flow-Based Anomaly Detection Approach With Feature Selection Method Against DDoS Attacks in SDNs," IEEE Trans. Cogn. Commun. Netw., vol. 8, no. 4, pp. 1862–1880, Dec. 2022, doi: 10.1109/TCCN.2022.3186331.