Published *online* on the journal's web page : http://innovatics.unsil.ac.id

Innovation in Research of Informatics (INNOVATICS)

| ISSN (Online) 2656-8993 |

Robust DDoS Detection in Software-Defined Networks: A Comparative Analysis of RBF-SVM and Gaussian Naïve Bayes with Feature Management Strategies

Putri Maharani.S[1], Ramdan Satra[2], Huzain Azis[3,4]

[1]Faculty of Computer Science, Universitas Muslim Indonesia Makassar, Indonesia.
[2]Malaysian Institute of Information Technology, Universiti Kuala Lumpur, Kuala Lumpur, Malaysia.

[1]13020220036@student.umi.ac.id, [2]ramdan@umi.ac.id, [3]huzain.azis@umi.ac.id, [4]huzain.azis@s.unikl.edu.my.

ARTICLE INFORMATION

Article History:
Received: February 17th, 2026
Last Revision: March 17th, 2026
Published *Online*: March 30th, 2026

KEYWORDS

DDoS Attack Detection,
Software-Defined Network,
Support Vector Machine,
Gaussian Naïve Bayes,
Feature Selection,
Dimensionality Reduction

CORRESPONDENCE

Phone: +6282271092204
E-mail: 13020220036@student.umi.ac.id

ABSTRACT

Distributed Denial of Service (DDoS) attacks pose a serious risk to network reliability, particularly within Software-Defined Networking (SDN) architectures that rely on centralized control. This research analyzes the effectiveness of Gaussian Naïve Bayes (GNB) and Support Vector Machine (SVM) with a Radial Basis Function (RBF) kernel for identifying DDoS attacks using an SDN traffic dataset consisting of 104,345 flow records. Three different feature-handling strategies are explored: using the complete feature set without reduction, applying feature selection through SelectKBest, and performing dimensionality reduction with Principal Component Analysis (PCA). Model validation is carried out using Stratified K-Fold Cross-Validation with K values of 2, 5, and 10. Predictions obtained from each fold are merged into a single aggregated confusion matrix to compute classification accuracy. Experimental results demonstrate that RBF-SVM without feature reduction delivers the highest detection performance, reaching an accuracy of up to 96.9%, while GNB provides lower accuracy but operates with greater computational efficiency. These findings indicate that an evaluation framework based on aggregated confusion matrices can provide more dependable performance estimates for DDoS detection systems deployed in SDN environments.

1. INTRODUCTION

Distributed Denial of Service (DDoS) attacks are widely recognized as one of the major threats to today's network infrastructures, especially in Software Defined Networking (SDN) environments [1]. By overwhelming network resources with massive volumes of malicious traffic, DDoS attacks can significantly reduce service availability and disrupt critical digital operations [2][3]. Although SDN offers centralized and flexible network control capabilities, its architecture also introduces new security gaps that require effective and adaptive detection mechanisms [4].

Traditional DDoS detection methods generally rely on rule-based or signature-based approaches [5]. While effective in identifying known attack patterns, these approaches are less adaptive and often fail to detect new or evolving attack variants [6]. To overcome these challenges, machine learning–based techniques are being adopted more frequently, as they can automatically identify complex patterns within network traffic [7]. Previous research has demonstrated that machine learning approaches are effective in detecting DDoS attacks, particularly within SDN environments [8]. Different machine learning algorithms demonstrate distinct performance characteristics when evaluated under the same experimental conditions, highlighting the importance of comparative performance analysis to determine the most effective classification approach[9]. Comparative studies have shown that different classification models can produce varying performance depending on feature representation and model architecture [10].

One study compared several classification algorithms such as K-Nearest Neighbors (KNN), TabNet, and Wide & Deep Learning using an SDN based dataset [11]. The results showed that KNN, despite its simplicity, was able to achieve a detection accuracy of up to 98% under certain conditions. This indicates that even lightweight algorithms can yield strong performance when supported by

appropriate data management [12]. However, that study focused primarily on deep learning models and did not thoroughly examine the role of preprocessing strategies such as feature selection and dimensionality reduction [13]. In addition, research into the performance of simple classifiers such as Gaussian Naïve Bayes (GNB) when combined with such feature-management strategies remains limited.

Other studies involving classifiers such as SVM and GNB also show that SVM generally performs well on high-dimensional data, while GNB provides computational efficiency despite its sensitivity to feature correlation. However, most of these works still rely on single train test splits, which may result in biased estimates that do not fully reflect real world generalization capability. This approach is intended to better represent real world generalization capability. The overall research procedure adopted in this study is presented in Figure 1, describing the sequential phases of data collection, preprocessing, feature processing, model development, cross-validation, and performance assessment.

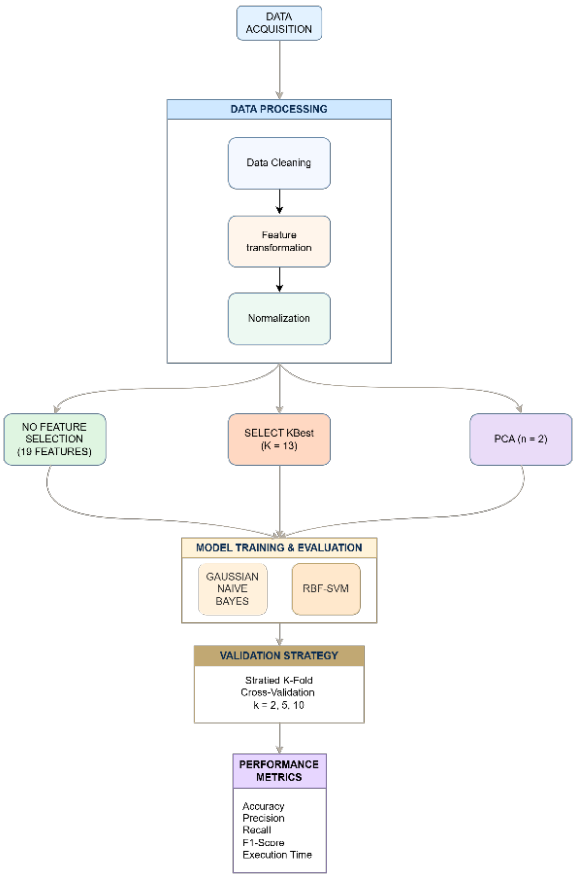

FIGURE 1. RESEARCH DESIGN

Moreover, the influence of feature management strategies, including feature selection and dimensionality reduction, has not been systematically compared across different types of classifiers. In particular, the performance of simple probabilistic models like GNB when combined with aggressive dimensionality reduction such as PCA has been evaluated in recent studies[14].

To address these research gaps, this study evaluates the performance of GNB and RBF-SVM in detecting DDoS attacks using an SDN-based dataset. Three feature-management scenarios are analyzed: using all features without reduction, feature selection using SelectKBest, and dimensionality reduction using PCA. Model evaluation is carried out using a stratified cross-validation procedure with three different fold settings (K = 2, 5, and 10) to maintain balanced class representation. Instead of assessing each fold separately, the predictions are pooled and summarized within a single confusion matrix, allowing performance to be measured in a more consistent and unbiased manner.

This research contributes by providing a structured comparative evaluation of GNB and RBF-SVM under multiple feature-management strategies within a multi-fold stratified cross-validation framework using aggregated confusion matrix analysis to obtain more stable performance estimation in SDN-based DDoS detection.

2. METHODOLOGY

2.1 Research Design

An experimental research approach is adopted in this study to systematically evaluate the performance of multiple machine learning methods for detecting DDoS attacks within SDN environments. The experimental workflow is structured into several sequential and interrelated stages to ensure methodological consistency and reproducibility. The process begins with data acquisition, followed by data preprocessing and feature preparation, model development, validation, and ultimately performance evaluation. Each stage is designed to ensure that the classifiers are trained and tested under controlled conditions, allowing a fair comparison between the selected algorithms. This structured design enables the investigation of how different modeling configurations influence detection capability in SDN-based traffic environments.

Prior to model training, the dataset undergoes comprehensive preprocessing, including the removal of irrelevant attributes, handling of missing or infinite values, conversion of all features into numerical format, and feature standardization. Once the dataset is properly prepared, three distinct feature-handling strategies are applied: training with the complete feature set, selecting the most relevant features using SelectKBest, and reducing dimensionality through PCA. Each feature configuration is evaluated using both GNB and SVM with an RBF kernel to analyze differences in learning behavior. To ensure balanced class distribution during validation, a Stratified K-Fold cross-validation scheme with K values of 2, 5, and 10 is implemented. Model performance is evaluated using classification accuracy derived from the aggregated confusion matrix to ensure consistent and stable performance estimation.

2.2 Data Section

This study utilizes the SDN-based DDoS Dataset obtained from a publicly accessible repository on Kaggle (https://www.kaggle.com/datasets/putrimaharanii/datasetforpaper). The dataset consists of 104,345 labeled network flow records collected from a Software-Defined Networking (SDN) environment. Each instance is classified as either normal traffic (0) or DDoS attack traffic (1), making it suitable for supervised machine learning approaches. The class distribution consists of 63,561 normal traffic instances (60.9%) and 40,784 DDoS attack instances (39.1%), providing a moderately balanced dataset for classification tasks.

Each flow record represents aggregated network behavior over a specific communication session and is described using various statistical indicators, including packet counts, byte counts, flow duration, transmission rate, and switch-related activity metrics. These features are designed to reflect traffic dynamics within the SDN architecture, capturing behavioral differences between legitimate traffic patterns and malicious DDoS activities. The availability of labeled data enables the classification models to learn discriminative patterns that distinguish attack traffic from normal network operations.

During preprocessing, non-behavioral attributes such as IP addresses and timestamps are excluded to prevent potential data leakage and to ensure that the models focus solely on generalized traffic characteristics rather than identity-based information. Although the original dataset contains 23 attributes, several identity-related fields are removed during preprocessing, resulting in 19 traffic-related features used for machine learning modeling. All retained attributes are converted into numerical format to meet the input requirements of machine learning algorithms, while the binary class label is preserved as the target variable.

This structured and cleaned dataset serves as the foundation for implementing the three feature management strategies, including full-feature utilization, SelectKBest-based feature selection, and PCA-based dimensionality reduction, as well as for conducting cross-validation and performance evaluation. By establishing a consistent and well-prepared dataset, the study ensures that the comparative analysis between classifiers is conducted under controlled and reliable experimental conditions.

2.3 Data Processing

Data preprocessing is conducted to ensure that the dataset is consistent, clean, and suitable for machine learning modeling. This stage plays a crucial role in improving data quality and preventing misleading patterns from influencing the learning process. Non-informative identity attributes, such as source IP address, destination IP address, and timestamp information, are removed because they do not directly represent traffic behavior characteristics. Retaining such attributes could introduce bias or unintended data leakage, especially if the model learns patterns tied to specific identities rather than generalizable traffic behavior. By eliminating these attributes, the model is encouraged to focus solely on statistical and behavioral features that are more relevant for distinguishing between normal and DDoS traffic.

After removing irrelevant fields, all remaining features are converted into numerical format to ensure compatibility with machine learning algorithms, which require structured numeric input. Missing values and non-finite values, including infinite or undefined entries, are replaced with zero to maintain dataset integrity and prevent computational errors during training. This replacement strategy is applied to maintain numerical consistency and prevent computational instability during model training, particularly for algorithms that cannot handle undefined or infinite values. Since such entries occur rarely in the dataset and do not represent meaningful traffic behavior, replacing them with zero is considered a practical preprocessing approach. Furthermore, feature standardization is incorporated into the training pipeline, particularly for algorithms that are sensitive to feature scale, such as SVM. Standardization ensures that each feature contributes proportionally to the learning process by transforming them into a comparable scale, thereby improving convergence stability and classification performance.

2.4 Feature Selection and Dimensionality Reduction

Three feature management strategies are implemented in this study to systematically evaluate how different feature handling approaches influence classification performance in detecting DDoS attacks within SDN environments. In the first scenario, all 19 original features are directly utilized for model training without applying any selection or dimensionality reduction technique. This full-feature configuration preserves the complete set of statistical and behavioral traffic characteristics, allowing the classifiers to learn from the entire information space and capture potentially complex interactions among variables. However, while retaining all features ensures that no potentially relevant information is discarded, it may also introduce redundancy, correlated attributes, and noise that can increase computational complexity and affect model stability, particularly for algorithms sensitive to feature scale and interdependence.

The second strategy applies SelectKBest based on Mutual Information to retain the 13 most relevant features by measuring the dependency between each feature and the target class. This relevance-based selection aims to eliminate less informative attributes while preserving discriminative information that is important for classification. By focusing on the most informative features, this approach can potentially improve model efficiency and reduce the impact of noisy or redundant attributes. In contrast, PCA performs dimensionality reduction by transforming the original feature set into a smaller number of orthogonal components; in this study, the 19-dimensional feature space is compressed into two principal components. The selection of two principal components was intended to evaluate the impact of aggressive dimensionality reduction on classification performance. By compressing the original feature space into a minimal number of components, the experiment highlights how much discriminative information is preserved when the dimensionality is significantly reduced. While this approach simplifies the feature representation and improves computational efficiency, it may also lead to the loss of class-specific information, since PCA prioritizes variance preservation rather than direct relevance to DDoS detection.

Together, these approaches enable a structured comparison between full-feature training, relevance-based feature selection, and substantial dimensional compression within the proposed detection framework.

2.5 Classification

2.5.1 Gaussian Naïve Bayes

GNB is a probabilistic classification method based on Bayes' Theorem and built on the assumption that features are conditionally independent given the class label. In this study, GNB is used as a simple baseline

approach because of its low computational requirements and fast processing speed[15]. Despite its simple independence assumption, GNB is still able to model probabilistic relationships in network-traffic data [16], and provides useful insight into the behaviour of probabilistic classifiers in SDN-based DDoS detection. However, the strong assumption of feature independence may reduce its effectiveness when dealing with correlated data; consequently, GNB's performance largely relies on the properties of the input features [17][18].

The probabilistic structure of GNB used in this study is illustrated in Figure 2 where the class label Yacts as the parent variable of all features $x_1, x_2, \ldots, x_n$. Under the conditional independence assumption, the likelihood of each class given the observed feature vector X is expressed in Equation (1).

$$\mathrm{P}(Y = y \mid \mathrm{X}) = \frac{P\,(Y = \gamma)\prod_{i=1}^{n} P\,(x_i \mid Y = y)}{P\,(X)} \quad (1)$$

$$\hat{\mathrm{Y}} = \arg max_{\{y\in\{0,1\}\}} \left[P(Y = y) \prod_{i=1}^{n} P(x_i|Y = y) \right] \quad (2)$$

The predicted class is determined by selecting the category that yields the highest posterior probability value after applying Bayes' Theorem to the observed feature vector. As illustrated in Figure 2, $P\,(Y = \gamma)$ represents the prior probability of each class, reflecting the overall distribution of normal and DDoS traffic in the dataset, while $P(x_i|Y = y)$ denotes the likelihood of observing feature (x_i) given a particular class label. In the GNB model, each feature is assumed to follow a Gaussian (normal) distribution within each class, and under the conditional independence assumption, the joint likelihood of all features is computed as the product of their individual likelihoods. This probabilistic formulation enables efficient parameter estimation and fast classification, although its effectiveness depends on how closely the actual feature distributions conform to the Gaussian assumption and the degree to which feature dependencies are limited.

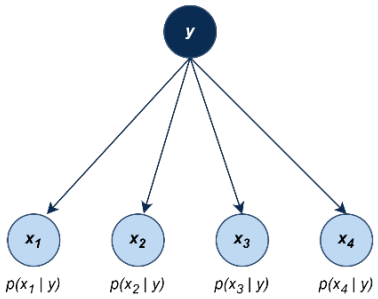

FIGURE 2. GRAPHICAL REPRESENTATION OF THE NAÏVE BAYES CLASSIFIER

2.5.2 Support Vector Machine with RBF Kernel

SVM is a supervised learning technique that determines an optimal separating hyperplane for differentiating data points across classes. It has been extensively adopted in classification problems because of its strong generalization ability and its effectiveness in modeling complex data distributions[19].

In this study, the RBF kernel is used to enable non-linear separation in the feature space [20][21]. RBF kernel projects the initial network traffic features into a higher-dimensional feature space, which helps the model learn intricate non-linear boundaries separating legitimate traffic from attack flows. This capability makes RBF-SVM highly suitable for detecting DDoS traffic behaviour, which typically exhibits irregular and overlapping feature distributions[22][23].

The overall classification workflow of the RBF-SVM model used in this study is illustrated in Figure 3. The input features are first transformed through the RBF kernel function, and the resulting kernel outputs are then passed into the SVM decision function to determine the final class label.

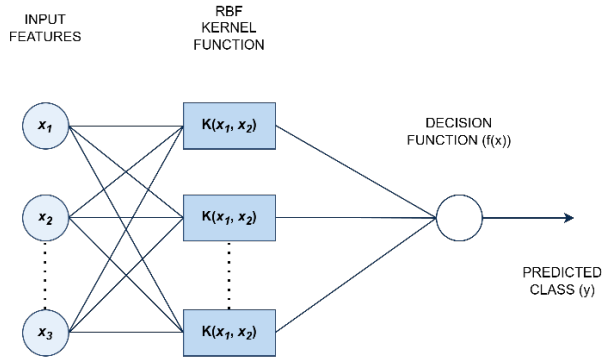

FIGURE 3. BLOCK DIAGRAM OF SVM USING RADIAL BASIS FUNCTION KERNEL (RBF)

For a given input sample x, the SVM decision function is defined as:

$$\hat{\mathrm{Y}} = sign\left(\sum_{i=1}^{N} \propto_i y_i\, exp(-\gamma \parallel x_i - x \parallel^2) + b\right) \quad (3)$$

In Equation (3), x_i represents the support vectors selected during the training process, which are the critical data points located near the decision boundary and directly influence the construction of the optimal separating hyperplane. The term y_i denotes the corresponding class label of each support vector, while α_i refers to the learned Lagrange multipliers that determine the contribution weight of each support vector in the final decision function. The bias term b adjusts the position of the decision boundary within the transformed feature space, and the parameter γ controls the width of the RBF kernel. Specifically, γ determines how far the influence of a single training sample reaches, thereby affecting the flexibility of the decision boundary. A higher γ value results in a more localized and complex boundary, whereas a lower value produces a smoother and more generalized separation.

In this study, the SVM classifier employs the RBF kernel with two important hyperparameters: the regularization parameter C and the kernel coefficient γ (gamma). The parameter C controls the trade-off between maximizing the decision margin and minimizing classification errors. The hyperparameter values follow the default configuration provided by the Scikit-learn implementation to ensure consistent and reproducible experimentation across all feature-management scenarios. Specifically, the regularization parameter is set to C = 1.0,

while the kernel coefficient is defined as γ = "scale", which automatically adjusts the gamma value based on the feature variance and number of features. This configuration allows the model to adapt to the scale of the dataset while maintaining stable decision boundaries during classification. In this formulation, a positive output of the decision function corresponds to the DDoS attack class, while a negative output indicates normal network traffic.

SVM is selected in this study due to its strong generalization capability and its effectiveness in handling high-dimensional and non-linearly separable data. The incorporation of the RBF kernel enables the classifier to project the original traffic features into a higher-dimensional space, where complex and overlapping traffic patterns can be more effectively separated. This characteristic is particularly important in real-world DDoS detection scenarios, where attack traffic often exhibits irregular, dynamic, and non-linear behavior that cannot be adequately captured by linear decision boundaries. As a result, RBF-SVM can model intricate traffic distributions more accurately than linear classifiers and simple probabilistic approaches, contributing to improved detection performance and more reliable classification outcomes.

2.6 Performance Evaluation

Cross-validation is widely applied to obtain dependable and unbiased performance measurements in classification tasks. In this study, a stratified K-Fold cross-validation scheme with three-fold configurations (K = 2, 5, and 10) is implemented to preserve balanced class representation across all folds. Rather than evaluating each fold independently, predictions from all folds are aggregated into a single comprehensive confusion matrix from which classification accuracy is calculated. Instead of reporting fold-level variability statistics such as mean and standard deviation, the evaluation metrics are derived from this aggregated confusion matrix constructed from predictions across all cross-validation folds. This aggregated evaluation approach emphasizes overall classification stability across all validation folds and provides a consolidated performance estimation derived from the complete validation process. As illustrated in Figure 4, the dataset is partitioned into K equal subsets while maintaining consistent class distribution, thereby reducing inter-fold variability, mitigating the influence of random data partitioning, and ensuring a more stable and representative estimation of the model's generalization capability under different validation granularities.

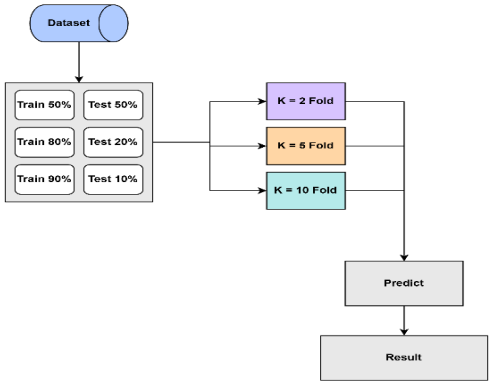

FIGURE 4. DATA SPLITTING SCHEME WITH K-FOLD CROSS VALIDATION

Predictions generated from all validation folds are systematically aggregated into a single unified confusion matrix, which serves as the primary basis for computing standard classification performance metrics, including accuracy, precision, recall, and F1-score, alongside computational processing time, thereby establishing a comprehensive and structured evaluation framework. By consolidating classification outcomes from all folds into one aggregated representation, this approach captures the cumulative distribution of true positives, true negatives, false positives, and false negatives across the entire validation cycle rather than relying on isolated fold-level measurements.

Consequently, it reduces inter-fold variability, mitigates the influence of random data partitioning, and minimizes the risk of performance fluctuation caused by sample imbalance or distributional variation within individual folds. This unified evaluation strategy not only enhances statistical robustness but also improves the reproducibility of experimental results, as performance is derived from the complete validation process. Precision, recall, and F1-score are also derived from the aggregated confusion matrix to provide additional insights into classification performance. However, in this study, classification accuracy is used as the primary metric for comparing model performance across different feature management strategies and Cross-Validation configurations.

Ultimately, it provides a more consistent, stable, and less biased estimation of overall model effectiveness while offering a more realistic approximation of the classifier's generalization capability in practical, real-world DDoS detection scenarios within SDN environments.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (4)$$

$$Precission = \frac{TP}{TP + FP} \quad (5)$$

$$Recall = \frac{TP}{TP + FN} \quad (6)$$

$$F1 - Score = \frac{Precission \times Recall}{Precission + Recall} \quad (7)$$

Equations (4)-(7) are formulated based on the four fundamental components of the confusion matrix, TP (true positives), TN (true negatives), FP (false positives), and FN (false negatives), which collectively represent the core elements for evaluating classification performance in DDoS detection; Accuracy, as defined in Equation (4), measures the overall proportion of correctly classified instances among all predictions, reflecting the general effectiveness of the model, while Precision in Equation (5) quantifies the proportion of instances predicted as DDoS that are actually attacks, thereby indicating the model's reliability in minimizing false alarms; Recall, introduced in Equation (6), evaluates the model's ability to correctly identify actual DDoS instances from the total number of true attack samples, emphasizing detection sensitivity; finally, Equation (7) presents the F1-score as a harmonic mean of Precision and Recall, providing a balanced and more informative performance metric, particularly in scenarios where class distribution may be uneven or when

both false positives and false negatives carry significant consequences.

3. RESULT

This section presents and analyzes the experimental findings of DDoS detection using GNB and RBF-SVM under three distinct feature management configurations: full-feature training without feature reduction (AK, representing the use of all features), feature selection using SelectKBest (KB), and dimensionality reduction using PCA. Although several evaluation metrics are calculated, the analysis in this study primarily focuses on classification accuracy as the main indicator for comparing the effectiveness of different models and feature management strategies. The evaluation is conducted using a Stratified K-Fold cross-validation framework with K values of 2, 5, and 10 to ensure balanced class representation and to obtain robust, stable, and unbiased performance estimates across different validation scenarios. By employing multiple fold settings, the study evaluates classification accuracy and analyzes the consistency of each model under varying validation granularities. The resulting classification accuracies of both GNB and RBF-SVM under each feature management strategy and cross-validation configuration are summarized in Table 1, providing a structured comparative overview of how different preprocessing approaches influence detection effectiveness, model stability, and overall learning behavior within the SDN-based DDoS detection framework.

TABLE 1. CLASSIFICATION ACCURACY (%) OF GNB AND RBF-SVM UNDER DIFFERENT FEATURE MANAGEMENT SCENARIOS.

Method		Gaussian Naïve Bayes	RBF SVM
CV K = 2	AK	66.42%	96.62%
	KB	66.98%	95.93%
	PCA	65.77%	84.38%
CV K = 5	AK	66.36%	96.89%
	KB	66.97%	96.21%
	PCA	65.77%	84.40%
CV K = 10	AK	66.36%	96.96%
	KB	66.98%	96.27%
	PCA	65.78%	84.41%

GNB exhibits relatively stable performance across all K-values and feature-management scenarios, with accuracy ranging from 65.77% to 66.98%. The highest accuracy is obtained in the SelectKBest scenario, reaching 66.98% at K = 2 and K = 10. This indicates that eliminating less-relevant features can partially mitigate the impact of feature dependence on the Naïve Bayes independence assumption. Nevertheless, overall GNB performance remains constrained by the inherent complexity and correlation of SDN traffic features, as highlighted in prior studies on machine-learning-based traffic classification in SDN environments[24],[25].

In contrast, RBF-SVM demonstrates significantly higher and more consistent performance across all settings. The highest accuracy is achieved in the full-feature scenario (AK), reaching 96.62% at K = 2, 96.89% at K = 5, and 96.96% at K = 10. This suggests that RBF-SVM effectively leverages the complete feature set to model non-linear network-traffic relationships and capture complex interactions among traffic attributes. Feature selection results in a slight decrease in accuracy to around 95.93%–96.27%, indicating that although less relevant features are removed, some excluded attributes still contribute meaningful discriminative information to the decision boundary.

Performance declines more substantially in the PCA scenario, where accuracy drops to approximately 84%, suggesting that aggressive dimensionality reduction may eliminate essential class-specific information and weaken separability between normal and attack traffic. Despite these variations across feature-management strategies, the observed differences between K = 2, 5, and 10 remain minimal, indicating that the stratified multi-fold validation framework provides stable and consistent performance estimation. Overall, these findings confirm that RBF-SVM without feature reduction offers the most robust and reliable detection capability within the evaluated SDN-based DDoS dataset.

A deeper analysis of the results shows that the relatively low performance of GNB, which remains around 66% across all configurations, can be explained by the strong conditional independence assumption inherent in the Naïve Bayes model. In SDN traffic environments, many network features such as packet counts, byte counts, flow duration, and transmission rates tend to exhibit significant correlations. These dependencies violate the independence assumption of GNB, limiting its ability to accurately capture complex relationships among traffic attributes. In contrast, RBF-SVM can model non-linear decision boundaries and interactions between correlated features, which explains its substantially higher performance in detecting DDoS traffic patterns. Furthermore, the significant accuracy reduction observed in the PCA scenario indicates that aggressive dimensionality compression may remove discriminative information necessary for distinguishing between normal and attack traffic flows.

Variations in K values (2, 5, and 10) cause only minor fluctuations in accuracy across all models and scenarios, confirming that the Stratified K-Fold cross-validation framework is stable and unbiased. Overall, the results demonstrate that RBF-SVM without feature reduction is the most optimal approach for DDoS detection on the evaluated SDN dataset. Feature selection may be useful when balancing computational efficiency and accuracy, while PCA significantly degrades performance[26]. GNB is computationally efficient but generally achieves lower accuracy, which makes it more suitable for resource-constrained environments where maximum detection performance is not the primary concern [27].

4. Conclusion

This research evaluates the effectiveness of GNB and kernel RBF-SVM in detecting DDoS attacks within SDN environments under three different feature management strategies. To ensure a fair, systematic, and dependable comparison, a Stratified K-Fold cross-validation procedure is implemented with K values of 2, 5, and 10. The stratified mechanism preserves balanced class distribution between normal and attack traffic across all folds, thereby reducing the risk of biased performance estimation caused by uneven attack-to-normal traffic ratios. This is particularly

important in intrusion detection scenarios, where class imbalance may distort evaluation results. Furthermore, aggregating predictions across all folds into a unified evaluation structure provides a more stable and representative assessment of model generalization capability compared to single train–test splits, which are more susceptible to randomness and sampling variation.

The experimental results indicate that RBF-SVM consistently outperforms GNB across all feature-handling configurations and validation settings. In the full-feature scenario without dimensionality reduction, RBF-SVM achieves the highest detection accuracy, reaching up to 96.96%, demonstrating its strong ability to exploit the complete feature space and model complex traffic patterns. When SelectKBest feature selection is applied, a slight decrease in accuracy is observed, suggesting that although irrelevant features are removed, some eliminated attributes still contribute meaningful discriminative information to the classification boundary.

A more substantial decline in performance occurs in the PCA scenario, where aggressive dimensionality reduction compresses the feature space into only two principal components, potentially eliminating class-relevant information and weakening the separability between attack and normal traffic. In contrast, GNB produces relatively stable but significantly lower performance, with an average accuracy of approximately 66% across all configurations. Although GNB benefits from low computational complexity and rapid processing time, its strong assumption of conditional independence among features limits its effectiveness in handling correlated and high-dimensional SDN traffic attributes.

Overall, the findings demonstrate that RBF-SVM without feature reduction provides the most robust, consistent, and reliable performance for DDoS detection in the evaluated SDN dataset. The capability of the RBF kernel to project data into a higher-dimensional space and capture intricate non-linear traffic distributions appears to play a crucial role in achieving superior classification accuracy. While feature selection may offer a practical trade-off between computational efficiency and detection performance, excessive dimensionality reduction can significantly degrade classification capability by discarding critical structural information embedded in the original feature space.

Future research is encouraged to explore ensemble learning strategies, hybrid models, and deep learning approaches that may further enhance detection accuracy while preserving computational efficiency. Additionally, validating the proposed framework on diverse SDN datasets and real-world traffic environments, including varying attack intensities and dynamic network conditions, would strengthen the generalizability, scalability, and practical applicability of the findings.

REFERENCES

[1] F. Ahmed, I. A. Sumra, and U. Jamil, "A Comprehensive Review on DDoS Attack in Software-Defined Network (SDN): Problems and Possible Solutions," *J. Comput. &Biomedical ...*, vol. 07, no. 01, 2024.

[2] Y. Su, D. Xiong, K. Qian, and Y. Wang, "A Comprehensive Survey of Distributed Denial of Service Detection and Mitigation Technologies in Software-Defined Network," 2024. doi: 10.3390/electronics13040807.

[3] R. Sommese *et al.*, "Investigating the impact of DDoS attacks on DNS infrastructure," in *Proceedings of the 22nd ACM Internet Measurement Conference*, New York, NY, USA: ACM, Oct. 2022, pp. 51–64. doi: 10.1145/3517745.3561458.

[4] D. S. Ahmed, A. A. Abdulhameed, and M. T. Gaata, "A Systematic Literature Review on Cyber Attack Detection in Software-Define Networking (SDN)," 2024. doi: 10.58496/MJCS/2024/018.

[5] S. A. Khan, S. I. Hussain, and J. Iqbal, "From Signatures to AI: A Comprehensive Review of DDoS Detection Strategies in IoT & SDN," *Int. J. Robot. Autom. Sci.*, vol. 7, no. 1, 2025, doi: 10.33093/ijoras.2025.7.1.3.

[6] M. Ouhssini, K. Afdel, M. Akouhar, E. Agherrabi, and A. Abarda, "Advancements in detecting, preventing, and mitigating DDoS attacks in cloud environments: A comprehensive systematic review of state-of-the-art approaches," 2024. doi: 10.1016/j.eij.2024.100517.

[7] A. A. Bahashwan, M. Anbar, S. Manickam, T. A. Al-Amiedy, M. A. Aladaileh, and I. H. Hasbullah, "A Systematic Literature Review on Machine Learning and Deep Learning Approaches for Detecting DDoS Attacks in Software-Defined Networking," 2023. doi: 10.3390/s23094441.

[8] J. Bhayo, S. A. Shah, S. Hameed, A. Ahmed, J. Nasir, and D. Draheim, "Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks," *Eng. Appl. Artif. Intell.*, vol. 123, p. 106432, Aug. 2023, doi: 10.1016/j.engappai.2023.106432.

[9] H. Azis, Nirmala, L. Syafie, Herman, F. Fattah, and T. Hasanuddin, "Unveiling Algorithm Classification Excellence: Exploring Calendula and Coreopsis Flower Datasets with Varied Segmentation Techniques," in *2024 18th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, IEEE, Jan. 2024, pp. 1–7. doi: 10.1109/IMCOM60618.2024.10418246.

[10] P. Purnawansyah *et al.*, "Comparative Study of Herbal Leaves Classification using Hybrid of GLCM-SVM and GLCM-CNN," *Ilk. J. Ilm.*, vol. 15, no. 2, pp. 382–389, Aug. 2023, doi: 10.33096/ilkom.v15i2.1759.382-389.

[11] R. Satra, I. A. Dahlan, H. Darwis, Purnawansyah, S. Mujaddid, and F. Fattah, "A Comparison of Accuracy: KNN, TabNet, and Wide & Deep Learning for DDoS Attack Detection in Software Defined Network," in *2025 19th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, IEEE, Jan. 2025, pp. 1–8. doi: 10.1109/IMCOM64595.2025.10857511.

[12] S. Sadhwani, B. Manibalan, R. Muthalagu, and P.

Pawar, "A Lightweight Model for DDoS Attack Detection Using Machine Learning Techniques," *Appl. Sci.*, vol. 13, no. 17, p. 9937, Sep. 2023, doi: 10.3390/app13179937.

[13] V. Atluri, K. Heidary, and J. Bland, "Performance Evaluation of Machine Learning Algorithms in Reduced Dimensional Spaces," *J. Cyber Secur.*, vol. 6, no. 1, pp. 69–87, 2024, doi: 10.32604/jcs.2024.051196.

[14] J. García, J. Entrena, and Á. Alesanco, "Empirical evaluation of feature selection methods for machine learning based intrusion detection in IoT scenarios," *Internet Things (The Netherlands)*, vol. 28, 2024, doi: 10.1016/j.iot.2024.101367.

[15] D. Gudipudi, R. E. Srinivasa, and B. D. Bujji, "DDoS attacks detection using naive bayes classifier," *i-manager's J. Inf. Technol.*, vol. 13, no. 3, 2024, doi: 10.26634/jit.13.3.21109.

[16] A. Aksoy, L. Valle, and G. Kar, "Automated Network Incident Identification through Genetic Algorithm-Driven Feature Selection," *Electronics*, vol. 13, no. 2, p. 293, Jan. 2024, doi: 10.3390/electronics13020293.

[17] Nurul A'ayunnisa, Y. Salim, and H. Azis, "Analisis Performa Metode Gaussian Naïve Bayes untuk Klasifikasi Citra Tulisan Tangan Karakter Arab," *Indones. J. Data Sci.*, vol. 3, no. 3, pp. 115–121, Dec. 2022, doi: 10.56705/ijodas.v3i3.54.

[18] P. Subarkah, W. R. Damayanti, and R. A. Permana, "Comparison of Correlated Algorithm Accuracy Naive Bayes Classifier and Naive Bayes Classifier for Classification of heart failure," *Ilk. J. Ilm.*, vol. 14, no. 2, pp. 120–125, Aug. 2022, doi: 10.33096/ilkom.v14i2.1148.120-125.

[19] M. K. Anam, T. A. Fitri, A. Agustin, L. Lusiana, M. B. Firdaus, and A. T. Nurhuda, "Sentiment Analysis for Online Learning using The Lexicon-Based Method and The Support Vector Machine Algorithm," *Ilk. J. Ilm.*, vol. 15, no. 2, pp. 290–302, Aug. 2023, doi: 10.33096/ilkom.v15i2.1590.290-302.

[20] Y. Irawan, R. Pramitasari, W. M. Ashari, A. Nur, and H. Yansyah, "Support Vector Machine Classification Algorithm for Detecting DDoS Attacks on Network Traffic," 2025. [Online]. Available: http://jurnal.polibatam.ac.id/index.php/JAIC

[21] Q. A. Thanni and P. de Boves Harrington, "Self-Optimizing Radial Basis Function Support Vector Classifier (SO-RBFSVC)," *J. Chemom.*, vol. 39, no. 6, Jun. 2025, doi: 10.1002/cem.70038.

[22] G. O. Anyanwu, C. I. Nwakanma, J. M. Lee, and D. S. Kim, "RBF-SVM kernel-based model for detecting DDoS attacks in SDN integrated vehicular network," *Ad Hoc Networks*, vol. 140, 2023, doi: 10.1016/j.adhoc.2022.103026.

[23] V. Hnamte, A. A. Najar, H. Nhung-Nguyen, J. Hussain, and M. N. Sugali, "DDoS attack detection and mitigation using deep neural network in SDN environment," *Comput. Secur.*, vol. 138, p. 103661, Mar. 2024, doi: 10.1016/j.cose.2023.103661.

[24] H. Azis, "Assessing the Performance of Logistic Regression in Heart Disease Detection through 5-Fold Cross-Validation," *Int. J. Artif. Intell. Med. Issues*, vol. 2, no. 1, pp. 1–11, May 2024, doi: 10.56705/ijaimi.v2i1.137.

[25] D. Nuñez-Agurto, W. Fuertes, L. Marrone, and M. Macas, "Machine Learning-Based Traffic Classification in Software-Defined Networking: A Systematic Literature Review, Challenges, and Future Research Directions."

[26] Ö. TONKAL and H. POLAT, "Traffic Classification and Comparative Analysis with Machine Learning Algorithms in Software Defined Networks," *Gazi Üniversitesi Fen Bilim. Derg. Part C Tasarım ve Teknol.*, vol. 9, no. 1, pp. 71–83, Mar. 2021, doi: 10.29109/gujsc.869418.

[27] M. S. Sawah, H. Elmannai, A. A. El-Bary, K. Lotfy, and O. E. Sheta, "Distributed denial of service (DDoS) classification based on random forest model with backward elimination algorithm and grid search algorithm," *Sci. Rep.*, vol. 15, no. 1, Dec. 2025, doi: 10.1038/s41598-025-03868-x.

AUTHORS

Putri Maharani.S

She is currently pursuing a bachelor's degree in informatics engineering. She has an interest in cybersecurity. Her current research focuses on the implementation of deep learning models for detecting Distributed Denial-of-Service (DDoS) attacks in Software-Defined Networking (SDN) environments. She is committed to developing her knowledge and expertise in the field of cybersecurity.

Ramdan Satra

He is a Lecturer at the Faculty of Computer Science. He earned his doctoral degree in Electrical Engineering and Informatics from Universitas Negeri Malang. His research interests include computer networking, embedded systems, Internet of Things (IoT), and wireless sensor networks. He has published various scientific papers in national and international journals and is actively involved in research related to Internet of Things, Wireless Sensor Networks, Computer Networks, Network Security.

Huzain Azis

He is a Lecturer at the Faculty of Computer Science. He obtained his master's degree in computer science and is currently pursuing a Ph.D. at the Malaysian Institute of Information Technology (MIIT), Universiti Kuala Lumpur (UniKL). His research interests include data science, artificial intelligence, and computer security. He actively conducts research and has contributed to several scientific

publications focusing on intelligent systems and cybersecurity solutions.