FULafia Journal of Science & Technology
ISSN (print) 2449-0954 \ ISSN (online) 2636-4972
https://lafiascijournals.org.ng/index.php/fjst
Sponsored By TETFUND TERTIARY EDUCATION TRUST FUND
Manuscript => Received: Jan., 2026; Accepted: May, 2026; Published: May, 2026 https://doi.org/10.62050/fjst2026.v10n2.723

A HYBRID ENSEMBLE LEARNING APPROACH FOR ENTERPRISE NETWORK THREAT CLASSIFICATION

Magai Emmanuel Gambo[1]*, Timothy Moses[1], Muhammad Mukhtar Liman[1] and Andrew Ishaku Wreford[2]
[1]*Department of Computer Science, Federal University Lafia, Nigeria*
[2]*Department of Computer Science, Federal University Wukari, Nigeria*
*Corresponding email: magai@fuwukari@edu.ng

ABSTRACT
The increased number of business networks has increased the traffic levels of the networks, which increases the susceptibility to advanced types of cyber-attacks such as Distributed Denial of Service (DDoS). The current intrusion detection systems have not had the capability to address the rising pattern attacks, therefore creating a need to employ the smart data models. The study presents a hybrid model design approach that combines the Support Vector Machine (SVM) algorithm, the Random Forest (RF) algorithm, and the Extreme Gradient Boosting (XGBoost) algorithm. The experiment study is undertaken on the CICDDoS 2019 dataset platform that supports diverse benign and DDoS network attacks. Data processing corresponded to the normalization of data, data ranking through the Information Gain values, and the application of the Synthetic Minority Over-sampling Technique (SMOTE). Each of the algorithms was individually created and evaluated through accuracy, precision, recall, F1 statistics, and AUC-ROC plots. It is clear from this study work that SVM performed best on its own with almost 99.92 % accuracy and Area Under the Curve (AUC) of 0.999 percent, outperforming RF and XG-Boost. The proposed hybrid ensemble model further enhanced these measures with 99.96 % accuracy with added strengths in terms of enhanced model generalization. This study work clearly establishes that the hybrid ensemble design of optimized traditional ML models performs efficiently and is scalable on real-time scales of enterprise network threats.

Keywords: Intrusion detection systems, Hybrid ensemble learning, DDoS attack classification, Feature selection (information gain), Data balancing

INTRODUCTION
The current fast-paced digital evolution of the organizational world has made enterprise networks the backbone for communication, business activities, cloud computing, and mass storage solutions (Afolalu & Tsoeu, 2025). The critical interconnection that has been achieved has increased the overall effectiveness of organizations by enhancing the scalability and effectiveness of global collaboration. On the negative side, the increased interconnection has widened the attack surface for organizations to face well-planned and advanced cybersecurity threats such as malware, phishing, insider threats, data breaches, and denial-of-service attacks in the enterprise network environment (Alotaibi & Ilyas, 2023). The increased velocity and variability associated with network traffic posed greater challenges to ensuring the security of the enterprise network due to the limitations associated with the traditional approach to ensuring network security.

The existing intrusion detection systems (IDSs) mainly rely on pattern-based or rule-based techniques to detect malicious events (Saravanan & Pugalenthi, 2025). Although these techniques have been successful in identifying known attack signatures, they have inherent drawbacks of being static, requiring constant updates to be kept effective. Consequently, traditional IDSs lack the capacity to detect zero-day attacks, advanced persistent threats, and unknown attack types, which keep evolving to evade detection (Ben *et al.*, 2024). The aforementioned challenges have, therefore, triggered a rising demand for intelligent, adaptive, and learned security solutions to identify attack behaviors without relying on any predefined knowledge.

Machine learning (ML) is also an important paradigm that has recently been found very efficient in the context of network intrusion detection, allowing the system to learn from traffic and make decisions based on past and current data (Balta *et al.*, 2024). Supervised learning models such as Support Vector Machine (SVM), Random Forest (RF), and Extreme Gradient Boosting (XGBoost) have shown very promising results in distinguishing between possible and actual network attacks due to the ability to deal with complexities and high-dimensional data (Kavitha *et al.*, 2024). Though very efficient, individual ML models pose certain limitations on their own. For example, SVM is efficient and easy to work with small and regularly structured datasets but may pose scaling issues on larger and complex corporate traffic, whereas RF and XGBoost models are better and efficient when dealing with high-dimensional data and complexities but pose several issues during training and computation due to the requirement of high training parameters and further generate significant overhead due to computations.

With regards to these limitations faced by single model methods, ensemble methods are becoming an influential method for solving issues pertaining to network security. This is because ensemble methods involve several classifiers to harness jointly for the strength and capabilities available, hence providing greater accuracy and capabilities for identifying outcomes (Alharthi *et al.,* 2025). With the utilization of several diverse model outputs, there is potential to achieve smaller variances as well as reducing challenges related to falsification or errors within positive as well as negative outcomes, which are quite imperative within enterprise security (Sharma & Shah, 2025). Additionally, there is an increase in evasion attack resilience.

Despite the growing adoption of machine learning in intrusion detection, existing approaches remain limited in effectively identifying evolving and complex attack patterns within enterprise networks. Traditional intrusion detection systems fail to detect zero-day and sophisticated attacks due to their reliance on static signatures, while individual machine learning models such as SVM, Random Forest, and XG-Boost exhibit performance trade-offs related to scalability, computational cost, and generalization. Furthermore, existing studies have not sufficiently explored how to effectively integrate these models to simultaneously improve detection accuracy, reduce false positives, and maintain computational efficiency, particularly for high-volume DDoS traffic. Therefore, a clear gap exists in the development of a robust, adaptive, and efficient ensemble-based framework tailored for enterprise network intrusion detection.

To address this gap, this study proposes a hybrid ensemble learning framework that combines the complementary strengths of SVM and tree-based models to improve DDoS attack detection in enterprise networks. The framework will be evaluated using the CICDDoS2019 dataset provided by the Canadian Institute of Cybersecurity, with the aim of enhancing detection accuracy, reducing false positives, and improving overall system performance.

A few research studies have attempted to explore the use of ML and ensemble strategies to carry out intrusion detection and threat categorization, primarily with the backdrop of spam categorization and Distributed Denial of Service threats. Early research work carried out by Shajideen and Vijayakumar in 2018 focused on identifying the capability of a range of classifiers under the machine learning approach to classify spam and genuine mails in the Enron spam dataset. The experiment carried out on Enron1 spam with a total of 3,762 spam emails and 5,172 ham emails correspondingly showed that Support Vector Machine (SVM) produced the optimal result with a classification accuracy of 94.06 %.

On the basis of the existing traditional methods for ML, Bolodurina *et al.* (2020) conduct research on the efficiency of data balancing methods in the classification of network traffic for various types of DDoS attacks on the CICDDoS2019 dataset. The models for classification were proposed using TensorFlow and scikit-Learn libraries with the implementation of SVM, RF, and GBM. The parameters taken for testing the efficiency of the proposed models were accuracy, balanced accuracy, completeness, and F1 Score. The experiment revealed the importance of data balancing in the classification of network traffic and was successful in the proposed models ensuring the balanced accuracy of 94.81 % in the case of Port Map attacks. However, the study is limited by its use of individual models and focus on specific attack types, which may reduce generalizability and overall detection performance.

Recently, solutions based on deep learning have also been proposed for enhancing the efficiency of the DDoS attack detection process. Daniyal *et al.* (2021) have proposed a hybrid network based on Convolutional Neural Network (CNN) and Bidirectional Long Short-Term Memory (Bi-LSTM) network with an efficient feature selection scheme. In their proposed network, the features of high importance or of high priority were successfully identified through rank-based methods based on the CICDDoS2019 dataset for better prediction capabilities. In their experiment, the proposed network based on CNN & Bi-LSTM enabled the maximum accuracy of 94.52 % for the testing, validation, or training phases.

Besides DL, another area that has shown considerable potential is the application of models designed using ensemble techniques coupled with feature selection techniques. Hossain *et al.* (2024) designed a hybrid model that integrated feature selection using the correlation approach coupled with gradient boosting for enhancing the detection of the DDoS attack. Upon using it on the CICDDoS 2019 data set, a detection rate of 98.9% was shown with high precision and recall measures. This study demonstrated that high accuracy can be obtained with dimensionality reduction through the adoption of feature selection techniques integrated with ensemble techniques.

Similarly, Abolarinwa *et al.* (2024) proposed an ensemble ML solution for identifying DDoS attack in a dataset of their choice named CICDDoS2019. For evaluation purposes, the datasets are divided into training and testing datasets in a ratio of 70:30. Authors have conducted the experiment with the aid of Python environments named Jupyter Notebook and Anaconda Navigator. Among these proposed ensemble machine learning techniques in the study, bagging is identified as the optimal one with an accuracy of 99.47 %, precision of 96.68 %, recall of 94.88 %, and F1 score of 95.61 %. Just like previous studies, authors concluded again that ensemble machine learning techniques are efficient for identifying the network in intrusion.

In general, existing studies demonstrate that ML, DL and ensemble-based approaches are effective for network threat detection, particularly when combined with feature selection and data balancing techniques. Unfortunately, the methods used in current approaches to network attack detection may face scalability and computational complexity challenges even after using

ensemble methods alone. The above-mentioned needs and challenges lie at the foundation for the current study's use of the hybrid ensemble approach that combines the use of SVM, RF, and XG-Boost algorithms.

MATERIALS AND METHODS

The methodology applied in this research is the quantitative and experimental. It was applied for designing an effective IDS using conventional ML algorithms and ensemble methods. Fig. 1 depicts the research which was divided into several steps such as data processing, feature selection, data balancing, training of models, ensemble model generation, and finally evaluation of models.

At data preprocessing step, the CICDDoS 2019 dataset was adopted as the benchmark dataset owing to the realistic traffic traces and thorough characterization of contemporary Distributed Denial of Service (DDoS) attacks. One-hot encoding was employed for the categorical attributes, and standardization was conducted for the numerical attributes for the sake of uniform scales of the attributes. This was necessary for discouraging the classifiers from favoring the high-magnitude attributes and improving the convergence characteristics of the distance- and margin-based classifiers like the SVM classifier. After the preprocessing step, the dataset was divided into training and testing sets using a stratified approach to maintain the ratio of the original classes. This helped keep the assessment of the generalization abilities of the trained models unbiased. Furthermore, feature selection using Information Gain (IG) was incorporated with the aim to achieve dimensionality reduction as well as to filter out features that are less relevant, Information Gain (IG) was used as a filter method, which is a feature selection technique. IG estimates the reduction in entropy, which is brought about by dividing the dataset using a particular feature, thus estimating its ability to distinguish between a particular class and others. Features with higher IG values were chosen to generate a set with high efficiency features. The use of IG was most advantageous in tree-based models, RF, and XG-Boost, and also helped to optimize the performance of SVM by minimizing noise in high dimensional spaces.

Owing to the nature of class imbalance in intrusion detection datasets, a process called Synthetic Minority Over-sampling Technique (SMOTE) was used to ensure a balance in the training dataset. SMOTE helped in creating virtual data points to supplement minority classes of attacks. This ensured higher sensitivity to vital attack patterns. The use of a balanced dataset helped avoid biases toward majority classes in traffic.

At the model development stage, three supervised machine learning classifiers were designed and developed independently on the balanced and feature-selected dataset. The ML model includes the RF, XG-Boost, and SVM. Furthermore, the models were hybridized using ensemble approach. The ensemble model utilized the soft voting strategy, where the outcome was chosen according to the weighted average of class probability predictions of the models. This was achieved by combining the advantages of each model, which include RF's robustness, SVM's optimization via margins, and the boosting technique of XG-Boost.

The trained models, as well as the hybrid ensemble performances were evaluated on various metrics to obtain a complete understanding of their performance. The metrics taken into consideration were Accuracy, Precision, Recall, F1-Score, and Area Under the Receiver Operating Characteristic Curve (AUC-ROC).

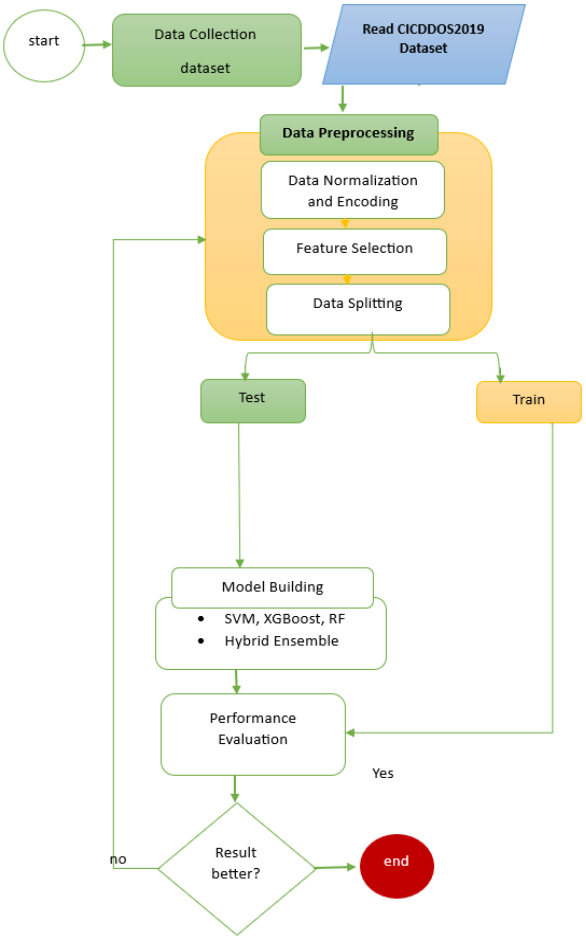


Figure 1: Research design

Dataset Description

The dataset employed in this paper is CIC-DDoS2019 dataset, which is a dataset created to detect DDoS attacks. This dataset has a total of 86 features extracted that relate to network traffic aspects like flow duration, packet size distribution, and packet arrival times. This has been extracted by generating network traffic with the help of open-source tools. It reflects an attack scenario similar to the real world, where attackers emulate reflection-based DDoS attacks on such legitimate services as DNS, NBNS, SNMP, and LDAP to flood and compromise target servers and network availability. Due to the number of attack vectors and benign traffic samples that it covers, the CIC-DDoS2019 is a comprehensive, balanced benchmark for testing next-generation IDSs.

Data Preprocessing

Data preprocessing is a critical phase in the development of an enterprise network threat detection model as the quality of input data directly influences model performance and generalization. Here, preprocessing consists of data cleaning, normalization, feature selection using Information Gain, and class imbalance handling using SMOTE, as illustrated in the proposed methodological flow.

The original CICDDOS2019 dataset has high dimensional network traffic features, and their numerical scales differ. Therefore, to provide uniformity and avoid features of greater absolute values dominating others, numerical attributes underwent standardization, which is defined as:

$$x' = \frac{x-\mu}{\sigma} \quad (1)$$

Where x is the original feature value, μ is the mean of the feature, σ is the standard deviation, and x' is the normalized value

Because of the large dimensional nature of network traffic data, all features in the data do not equally contribute to the identification of an intrusion. Information Gain (IG) is incorporated as a filter method for the selection of features. IG calculates how much this entropy has been reduced after splitting the dataset according to a given feature. Entropy $H(Y)$ of the target class Y is defined as:

$$H(Y) = -\sum_{i=1}^{c} p(y_i)\log_2 p(y_i) \quad (2)$$

Where c is the number of classes, $p(y_i)$is the probability of class y_i. The conditional entropy of Y given a feature X is:

$$H(Y \mid X) = \sum_{x \in X} p(x)H(Y \mid X = x) \quad (3)$$

Information Gain is then computed as:

$$IG(Y,X) = H(Y) - H(Y \mid X) \quad (4)$$

The features with higher Information Gain are of greater importance in class discrimination and hence selected. The feature selection increases the accuracy of detection and at the same time reduces complexity during training for RF, SVM, and XG-Boost.

Handling Class Imbalance using SMOTE

The adapted dataset is imbalanced, where benign traffic dominates attack samples as shown in Fig. 2. This kind of problem usually biases classifiers in favor of the majority classes, which always performs poor detection on minority attack categories. To handle this challenge, the Synthetic Minority Over-sampling Technique is applied after feature selection. SMOTE generates synthetic samples by interpolating between the instances of the minority class. Given a minority class sample $x_i$and one of its k-nearest neighbors x_j, a synthetic sample is created as:

$$x_{\text{new}} = x_i + \lambda(x_j - x_i), \lambda \in (0,1) \quad (5)$$

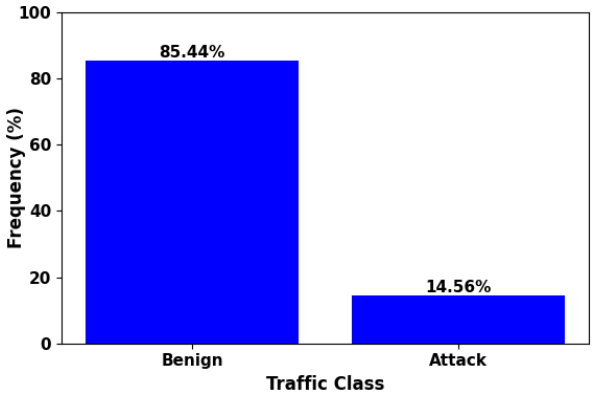


Figure 2: Imbalanced CICDDOS dataset

This approach increases minority class density without duplicating existing samples, thereby improving classifier sensitivity to rare attack patterns. In detail, the CICIDS2019-derived dataset showed a severe class imbalance before balancing, which is representative of most network intrusion detection problems. In the original class distribution, there were 19,566 instances of the Benign class, while there were 3,335 instances in the Attack class as shown in Fig. 3. This imbalance ratio, about 85 % Benign and 15 % Attack, biases learning algorithms toward the majority class (Fig. 2). This demands the application of data balancing technique, hence the adaptation of the SMOTE algorithm.

```
[14]: df['Class'].value_counts()

[14]: Class
      Benign    19566
      Attack     3335
      Name: count, dtype: int64
```

Figure 3: Dataset count prior to SMOTE application

```
[25]: # Check the class distribution after SMOTE
      print(y_resampled.value_counts())

      Class
      0    19566
      1    19566
      Name: count, dtype: int64
```

Figure 4: Dataset count after SMOTE application

After SMOTE application, the dataset was balanced with 19,566 instances in each class as shown in Fig. 4. Instead of repeating any previously existing sample, SMOTE generates synthetic attack samples by interpolating between several minority-class neighbors in feature space. This process of balancing enforces classifiers to learn more discriminative decision boundaries for both benign and attack traffic. As a result, post-SMOTE training increases sensitivity to attacks, enhances recall and F1-score for the minority class, and yields more reliable and generalizable intrusion detection performance.

Random Forest (RF)

Random Forest is an ensemble learning algorithm for classification, and it builds a forest of decision trees via the bootstrapped sample and along the random feature selection (Salman *et al.*, 2024). RF predicts each class independently, and then it combines them via majority votes. Mathematically, given a set of trees $\{T_1, T_2, \dots, T_n\}$, the RF prediction is:

$$\hat{y} = \text{mode}\{T_i(x)\}_{i=1}^{n} \quad (6)$$

One of the strengths of the RF algorithm is in intrusion detection, as it is very efficient in dealing with non-linear relationships and is able to address the noisy and over-fitting challenges in the bagging process. In the environment of CICDDOS 2019, the algorithm is efficient in detecting different types of attacks, such as SYN flood, UDP flood, and application-layer attacks, depending on various traffic types of different packets.

Support Vector Machine (SVM)

Support Vector Machine is a margin-based classifier that seeks to find an optimal hyperplane separating benign and malicious traffic with maximum margin (Alowaidi & Cevik, 2025). For a binary classification problem, SVM solves:

$$\min_{w,b,\xi} \frac{1}{2} \| w \|^2 + C \sum_{i=1}^{n} \xi_i \quad (7)$$

subject to:

$$y_i(w \cdot \phi(x_i) + b) \geq 1 - \xi_i, \xi_i \geq 0$$

Where: $\phi(x)$ is a kernel function that maps input data to a higher dimension. In this research, SVM has a great generalization capability, especially in distinguishing difficult attack patterns from normal connections. The generalization performance in the CICDDOS2019 data comes from its ability to define a decision boundary with a high level of accuracy, even if the behaviors are overlapping between attacks and normal connections

XG-Boost

XG-Boost is a gradient boosting decision tree algorithm that grows a sequence of trees, correcting the mistakes made by previous trees. The objective is defined as:

$$\mathcal{L} = \sum_{i=1}^{n} l(y_i, \hat{y}_i) + \sum_{k=1}^{K} \Omega(f_k) \quad (8)$$

with regularization term:

$$\Omega(f) = \gamma T + \frac{1}{2} \lambda \| w \|^2 \quad (9)$$

This formulation enables XG-Boost to achieve high predictive accuracy while controlling model complexity. For the CICDDOS 2019 dataset, it is conspicuous that the model performs very effectively to identify the subtle and evolving features of DDoS attacks by periodically emphasizing the previously incorrectly classified data flow.

Hybrid Ensemble Strategy

The hybrid ensemble integrates RF, SVM, and XG-Boost to leverage their complementary strengths. The final prediction $\hat{y}_{ensemble}$ is obtained using soft voting, where predicted class probabilities are averaged:

$$\hat{y}_{ensemble} = \arg\max_{c} \left(\frac{1}{M} \sum_{m=1}^{M} P_m (y = c \mid x) \right) \quad (10)$$

Where: M is the number of base models. The ensemble method makes them more robust, less biased, and capable of detecting different DDoS attacks that are present in CICDDOS2019. The combination of tree-based learning methods with Margin-Based Classification is a hybrid model that performs well in enterprises because it is more dynamic, with traffics that are more likely to be attacked by adversaries.

Performance Evaluation Metrics

To evaluate the performance of the models. The metric presented in Table 1 where used base on the definition of the TN, TP, FP and FN variables where:

i. TP (True Positives): Correctly predicted attack cases (malicious traffic detected as attacks).
ii. TN (True Negatives): Correctly predicted normal cases (benign traffic identified as normal).
iii. FP (False Positives): Normal traffic misclassified as attacks.
iv. FN (False Negatives): Attack traffic misclassified as normal.

Table 1: Performance metrics

Metrics	Formulae	Interpretation
Accuracy Score	$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$	Proportion of correctly classified traffic (normal and attack) among all samples.
Precision	$precision = \frac{TP}{TP + FP}$	Of all predicted attacks, precision defines how many were correctly identified as malicious.
Recall	$Recall = \frac{TP}{TP + FN}$	Ability of the model to correctly detect actual attacks.
F1-Score	$F - Measure = 2 \times \frac{Precision \times Recall}{Precision + Recall}$	Harmonic mean of precision and recall, balancing false positives and false negatives.
Area under the Curve	$AUC = \frac{1}{2}\left(1 + \frac{TP}{TP + FN} + \frac{FP}{FP + FN}\right)$	Scalar measure of separability. AUC = 1.0 indicates perfect classification, while AUC = 0.5 corresponds to random guessing.

Environmental Setup

The ML model was developed using the Anaconda computing platform. And the experiment was conducted on Windows operating system with dual-core Intel Core i5 processor and 8 GB RAM. Packages utilized includes standard machine learning libraries Scikit-Learn, TensorFlow, NumPy, and pandas.

Feature Selection

As aforementioned, the research incorporated a FS technique using the IG algorithm. The algorithm 'information gain' allows the specification of the number of features to be selected using a value called the k-threshold. The value of k as a threshold was set to the top 20 during the experiment. Table 2 shows the chosen features of both datasets.

Table 2: Selected Features of the dataset

Feature Index	Feature Name	Information Gain
7	Label	0.554841
52	Avg Packet Size	0.468806
40	Packet Length Mean	0.435146
8	Fwd Packet Length Mean	0.433315
53	Avg Fwd Segment Size	0.433251
39	Packet Length Max	0.424597
38	Packet Length Min	0.420324
7	Fwd Packet Length Min	0.419560
6	Fwd Packet Length Max	0.417627
62	SubflowFwd Bytes	0.416474
4	Fwd Packets Length Total	0.416087
14	Flow Bytes/s	0.384345
16	Flow IAT Mean	0.368214
18	Flow, IAT Max,	0.357049
15	Flow Packets/s	0.356447
36	Fwd Packets/s	0.355390
37	Bwd Packets/s	0.348532
17	Flow IAT Std	0.345089
23	Fwd IAT Max	0.338098
21	Fwd IAT Mean	0.326579

Table 2 above lists the top 20 selected features ranked by their IG values, which is a measure of the importance or relevance of each feature in distinguishing between different classes in network threat detection. The feature index identifies the index of the selected feature from the datasets and their corresponding names next to the index column as the feature names

Experiment Results

This section presents the experimental evaluation of SVM, RF, XG-Boost, and the proposed hybrid ensemble model using the CICDDoS2019 dataset. The performance of the models was assessed using accuracy, precision, recall, F1-score, confusion matrices, and ROC–AUC analysis.

Performance of Individual Models

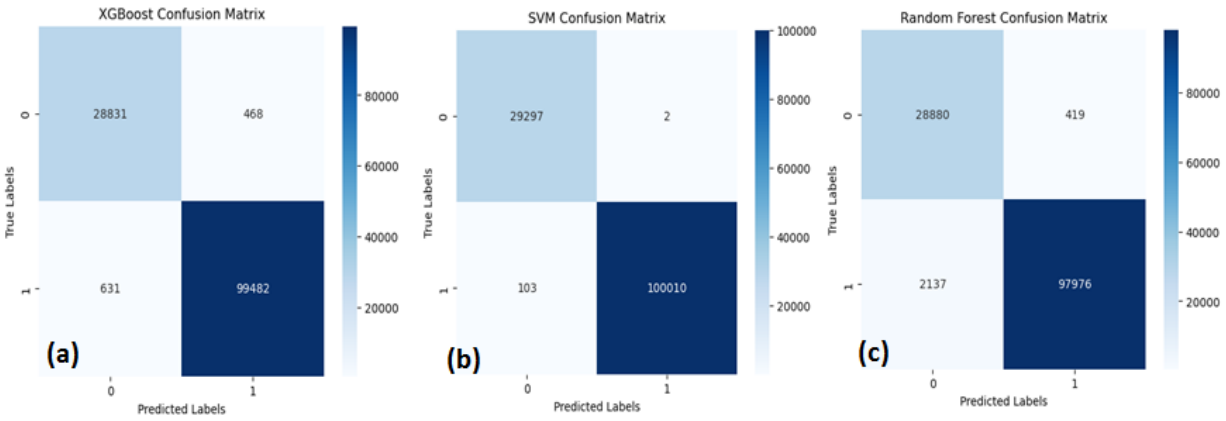
From the experimental result conducted, SVM recorded the highest overall accuracy of 99.92 %, with precision, recall, and F1-values above 99.8 % for both classes, indicating significant discrimination between normal and attack traffic. XG-Boost came second with an overall accuracy of 99.15 %, which recorded high levels of precision and recall for both classes. RF recorded an overall accuracy of 98.02 %, which showed high performance with relatively low precision for normal traffic (Table 3).

Table 3: Summarized classification results of SVM, RF, and XG-Boost for normal (Class 0) and attack (Class 1) traffic

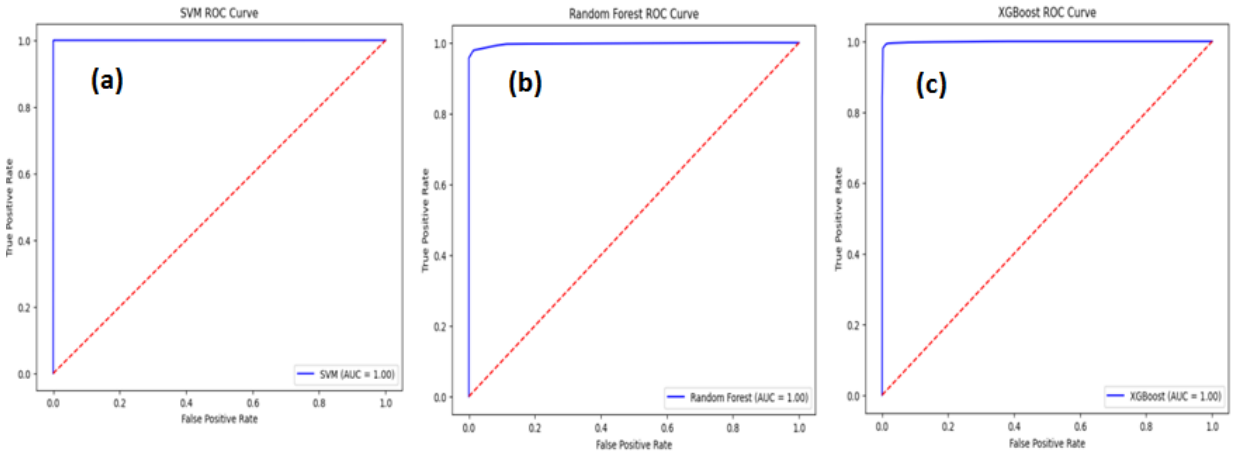
Algorithm	Metric	Class 0 (Normal)	Class 1 (Attack)	Accuracy (%)
RF	Precision	93.11%	99.57%	98.02
	Recall	98.57%	97.87%	
	F1-Score	95.76%	98.71%	
SVM	Precision	99.65%	99.99%	99.92
	Recall	99.99%	99.90%	
	F1-Score	99.82%	99.95%	
XGBoost	Precision	97.86%	99.53%	99.15
	Recall	98.40%	99.37%	
	F1-Score	98.13%	99.45%	

The performance of all models is further investigated via the confusion matrices shown in Fig. 5.

The confusion matrices, given in Fig. 5(a, b, c), further confirm these observations from the classification report from Table 3. The SVM reported the least misclassification rates, with only 2 false positives and 103 false negatives, thus confirming its reliability in minimizing both false alarms and missed attacks. XG-Boost showed strong detection with 468 false positives and 631 false negatives, proving that it is relatively efficient in recognizing attacks but gives minimal errors; while effective, the RF had more false negatives-2,137-established that it has a higher possibility of hidden attacks. These results confirm SVM as the most reliable classifier for intrusion detection in this study.



Figures 5: (a) Confusion matrix of XG-Boost; (b) Confusion matrix of SVM; (c) Confusion matrix of RF



Figures 6: (a) AUC of SVM; (b) AUC of RF; (c) AUC of XG-Boost

In an attempt to rigorously interrogate the model's performance, the ROC-AUC metrics was also considered. The ROC curves and AUC scores (Fig. 6(a, b, c)) highlight the discriminative power of the evaluated models.

In terms of AUC score, SVM recorded the highest result of 0.999; it was closely followed by XG Boost with an AUC score of 0.998 and then by Random Forest that recorded an AUC score of 0.997. The classification ability of each model is excellent; however, marginally.

Hybrid Ensemble Model Performance

"The hybrid ensemble model, which combines SVM, XG-Boost, and Random Forest, obtained 99.96 % accuracy, which is better than the performance of the individual classifiers as listed in Table 4"

Table 4: Hybrid model performance

Algorithm	Metric	Class 0 (Normal)	Class 1 (Attack)	Accuracy (%)
Hybrid	Precision	99.87%	99.95%	99.96
	Recall	99.91%	99.97%	
	F1-Score	99.92%	99.94%	

While SVM still outperformed as an individual model, the results depicted that the ensemble handled stability, generalization, and robustness by behaving complementary to each other to every classifier. The values of precision (99.95 %) and F1-score (99.94 %) of the ensemble indicated near-perfection.

State-of-the-Art Comparison

Table 5: Compares the proposed models with existing state-of-the-art approaches using the CICDDoS2019 dataset

Authors	datasets Used	Algorithm Used	Best Algorithm	Accuracy (%)
Abolarinwa *et al*. (2024)	CIC-DDoS2019	DT, LR, NB, AdaBoost, Gradient Boosting	DT	99.47
Daniyal *et al*. (2021)	CIC-DDoS2019	CNN, BI-LSTM,	CNN-BI-LSTM	94.52
Bolodurina *et al*. (2020)	CIC-DDoS2019	SVM, RF, and GBM	RF	94.81
Current Study	CIC-DDoS2019	SVM, XG-Boost, RF	SVM	**99.92**

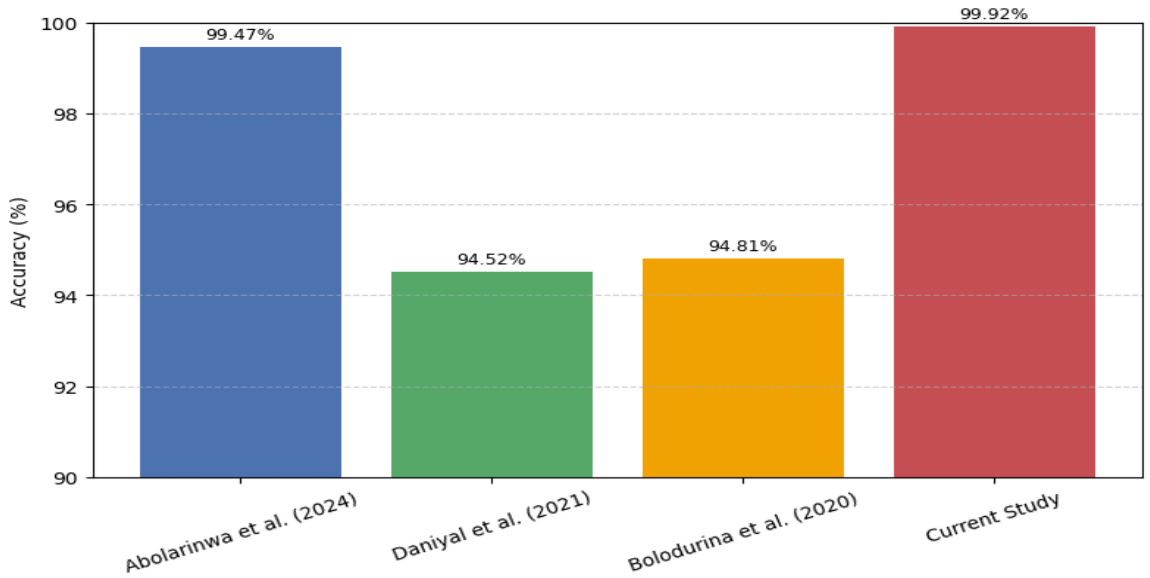


Figure 7: Result Comparison of Best Algorithm for CUC-DDOS2019

Considering the Table 5 and Fig. 7, the SVM model implemented by this study achieved an accuracy of 99.92 %, outperforming prior works, including Decision Tree (99.47 %), CNN–BiLSTM (94.52 %), and RF (94.81 %). These results indicate that optimized conventional machine learning models can outperform more complex deep learning architectures when combined with effective preprocessing and feature selection.

CONCLUSION

In this experiment research, the efficacy of the hybrid ensemble learning method for threat classification on the CICDDoS2019 dataset in the context of the enterprise network has been proved. Based on the thorough preprocessing step of the dataset that included the SMOTE technique and the IG feature selection method, the implemented model improves the classification capability of the general ML algorithm. Among the adapted classification methods, the Support Vector Machine method performed better and reached an accuracy rate of 99.92 %, exhibiting better generalization and classification capability between the normal and the threat traffic correctly. The hybrid ensemble model developed with the soft voting approach further enhanced the performance by effectively combining the unique capabilities of SVM, RF, and XG-Boost. With an accuracy of 99.96 %, the hybrid ensemble model clearly showed better stability, lower variance, and robustness against mis-classification errors in comparison to individual models. The findings clearly show that optimized ML models can perform better when effectively implemented together as an ensemble model with proper feature engineering and balancing of the dataset. As a whole, the hybrid ensemble model proves to be an effective solution with great potential in real-time commercial network environments requiring accurate detection of potential dangers.

Conflict of interest: The authors declare no conflict of interest.

REFERENCE

Abolarinwa, M., Adegoke, E., Adewuya, M. and Ojo, E. (2024). Development of a distributed denial of service detection model *using ensemble machine learning techniques. Adeleke University Journal of Science* (AUJS), 3(1).

Afolalu, O. and Tsoeu, M. S. (2025). Enterprise networking optimization: A review of challenges, solutions, and technological interventions. *Future Internet*, 17(4), 133. https://doi.org/10.3390/fi17040133

Alharthi, H., Medjek, F. and Djenouri, Y. (2025). Hybrid ensemble methods for intrusion detection in enterprise networks. *Computers & Security*, 140, 103746. https://doi.org/10.1016/j.cose.2025.103746

Alotaibi, F. and Ilyas, M. (2023). An ensemble learning framework for IoT device security using SVM and random forest. *International Journal of Information Security Science*, 12(1), 55–70.

Alowaidi, A. E. A. and Cevik, M. (2025). Adaptive volcano support vector machine (AVSVM) for efficient malware detection. *Applied Sci.*, 15(24), 12995. https://doi.org/10.3390/app152412995

Balta, D., Çavuşoğlu, U. and Balta, M. (2024). A comprehensive survey on Machine learning-based intrusion detection systems for vehicular networks: A review. *Düzce University Journal of Science & Technology*, 12, 1536-1556. https://doi.org/10.29130/debited.1372131

Ben, C., HajKacem, M. and Alattas, M. (2024). Enhancing intrution detection performance using explainable ensemble deep learning. *Peerj Comput Sci.*, 10, e2289.doi:10.7717/peerj-cs.2289

Bolodurina, I., Makarov, A., Shukhman, A., Perfenov, D. and Zabrodina. L. (2020). Investigation of the problem of classifying unbalance datasets in identifying DDoS attacks detection using CICDDoS2019 dataset. *Journal of Physics: Conference Series*, 1679, 042020. DOI: 10.1088/1742-6596/1679/4/042020

Daniyal, M., Khan, Z. and Rehman, S. (2021). Efficient detection of DDoS attacks using a hybrid with improved deep learning model with improved feature selection. *International Journal of Applied Science*, *Appl. Sci*., 11, 11634. https://doi.org/10.3390/app112411634

Hossain, M., Rahman, T. and Sultana, N. (2024). Hybrid feature selection and ensemble classification for enhanced DDoS detection. *Computer Networks*, 237, 110023. https://doi.org/10.1016/j.comnet.2024.110023

Kavitha, K., Rajesh, R. and Venkatesh, B. (2024). Hybrid machine learning models for network intrusion detection. *ICT Express*, 10(2).

Salman, H. A., Kalakech, A. and Steiti, A. (2024). Random forest algorithm overview. *Babylonian Journal of Machine Learning*, 69–79.

Saravanan, T. and Pugalenthi, R. (2025). Seismic-driven neural intelligence coupled with hybrid evolution strategy for accurate intrusion detection in cloud-IoT systems. *The Journal of Supercomputing*, 81(16), 1557. https://doi.org/10.1007/s11227-024-05878-3

Shajideen, M. and Bindu, V. (2018). Spam filtering: A comparison between different machine learning classifiers on enron. dataset. *International Conference on Electronics Communication and Aerospace Technology, ICECA, 1919-1922.* DOI: 10.1109/iceca.2028.8474778

Sharma, D. and Shah, S. (2025). Hybrid feature selection and ensemble learning for DDoS detection using CICDDoS2019 dataset. *Journal of Network and Computer Applications.*

Talukder, M. A. and Uddin, M. A. (2023). *CIC-DDoS2019 Dataset (Version 1)* [Data set]. Mendeley Data. https://doi.org/10.17632/ssnc74xm6r.1