Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 47 No. 4 (2026)

A Hybrid Intrusion Detection Framework Integrating Mutual Information-based Feature Selection with Stacking-based Ensemble Learning

Venkatesh Eluru[1] and Jayavarapu Karthik[2]

[1]*Department of CSE, Koneru Lakshmaiah Educational Foundation, Guntur, AP, India;* evenkatesh027@gmail.com

[2]*Department of CSE, Koneru Lakshmaiah Educational Foundation, Guntur, AP, India;* jayavarapukarthik@kluniversity.in

Abstract:- Intrusion Detection Systems (IDS) are crucial for protecting modern computer networks against the ever-evolving landscape of cyber threats. But there are certain challenges that are hard for many machine learning based intrusion detection systems, such as high dimensional data, class imbalance and the detection of unknown attacks. To solve these problems, this study suggests a hybrid stacking-based intrusion detection system combining the feature selection method named Mutual Information (MI) and supervised and anomaly-based learning. In the proposed framework, logistic regression (LR) is proposed to be used as a meta-classifier, which takes predictions from Random Forest (RF) and Isolation Forest (IF) as base learners. Once the data has been processed, the features have been selected, and the model has been trained, the UNSW-NB15 data set is used to test the framework. The results of the experiments demonstrate that the proposed approach can achieve an accuracy of 97.72%, with precision and recall (and F1-scores) close to 0.98 for both attack and normal classes. The proposed system has been proved to achieve improved performance on a regular basis compared to individual classifiers and existing intrusion detection systems. The outcomes illustrate that feature selection combined with a hybrid ensemble learning technique boosts the accuracy of intrusion detection, its robustness, and its practical usability, thus showing the viability of the proposed framework in the context of modern network security scenarios.

Keywords*: Intrusion Detection System, Mutual Information, Stacking Ensemble.*

1. Introduction

With the rapid growth of computer networks and Internet-based services, contemporary information systems are far more susceptible to cyberattacks, such as malware, denial-of-service attacks, unauthorised access, and data breaches. These attacks are becoming more sophisticated and more common, and are now a top concern of the businesses, governments and even the scientific community [1]. With the growth of network size and complexity, traditional security systems are no longer sufficiently effective to defend against a variety of attacking strategies [3].

While significant advances have been made in the field of cybersecurity research, current intrusion detection systems (IDS) face several challenges. These involve handling high-dimensional network traffic data, detecting new or zero day attacks, and maintaining a reliable performance when traffic is class imbalanced [4, 5]. Furthermore, existing IDS architectures often are not adaptable and are unable to be generalized properly in real-world scenarios, making it critical to develop more effective and data-driven detection techniques [6].

In order to continuously monitor network activity and spot hostile behaviours that jeopardise system availability, confidentiality, and integrity, intrusion detection systems are crucial. IDS solutions are generally classified into two types: Anomaly-based and Signature-based. Signature based intrusion detection systems (IDS) are known to be effective in detecting known attacks, and are inadequate against novel attacks because they are based on predefined

patterns of attacks [2]. However, anomaly-based IDS is able to identify zero-day attacks and deviations from normal behaviour, but may generate more false alarms [14]. Hybrid IDS approaches aim at combining the merits of both approaches to achieve better detection accuracy and robustness [6].

Many current IDS implementations continue to use rule-based mechanisms or small statistical models, even though the use of hybrid architectures has been beneficial. As a consequence, the application of machine learning (ML) techniques for intrusion detection has gained popularity. This has led to the emergence of using machine learning (ML) techniques for intrusion detection becoming popular. An ML-based intrusion detection system can be trained to detect complex patterns directly from network traffic and adapt to new attack methods. Many studies have explored traditional machine learning techniques, like Random Forest, Support Vector Machine (SVM), Naïve Bayes, k-Nearest Neighbours and Logistic Regression, which gave promising results on several benchmark datasets such as UNSW-NB15 [1] and [4].

However, existing research on IDS using ML techniques has certain drawbacks. IDS frameworks that rely on ensemble and stacking are primarily based on supervised models and are lacking of anomaly detection mechanisms in the ensemble structure [7]. Besides, most of the existing works are concentrated on binary classification which limits the applicability to realistic network scenario with multiple attack categories [13]. Moreover, the feature selection is often performed separately from the ensemble learning flows [11]. These drawbacks inspire the development of a hybrid stacking-based IDS that combines both supervised and anomaly-based learning, as well as good feature selection.

Feature selection plays an important role to improve IDS performance by reducing the dimensionality of data, removing redundant features and enhancing the learning efficiency. MI is a popular feature selection technique which quantifies the dependency between input features and classes. It is particularly effective for datasets such as UNSW-NB15, as it is able to detect non-linear relationships, and it is independent of any classifier, thus it is ideal for high dimensional network traffic data sets [3, 5]. MI is used to select the most informative features, thus enhancing the detection accuracy and decreasing the computation overhead.

Mostly, current IDS frameworks are based on the feature selection and ensemble learning, but a few stacking-based IDS utilize supervised learning models and do not explicitly consider anomaly detection in the ensemble design. Furthermore, feature selection is often treated as a separate preprocessing step and not as a part of the learning process. To address these limitations, this paper suggests a hybrid framework of intrusion detection system (IDS) based on stacking ensembles of Random Forest, Isolation Forest and Logistic Regression with Mutual Information (MI) feature selection is presented. This is done using a combination of supervised and anomaly-based learning to enhance the accuracy, robustness and generalization of detection.

The following is a summary of the main contributions of this work:

1. A good framework for developing intrusion detection systems using stacking ensemble learning with Mutual Information (MI) feature selection.
2. A new unified stacking framework based on both supervised and anomaly learning, combining the Random Forest and Isolation Forest algorithms.
3. Logistic regression is a light-weight meta-classifier, which is also very effective in fusing base learner predictions.
4. Experimental results on the UNSW-NB15 dataset demonstrate superior detection performance when compared to the baseline models and existing approaches [4], [12].
5. A practical framework suitable for practical network security applications which is computationally efficient.

2. Objectives

The main aim of this research is to create a hybrid intrusion detection system that combines Mutual Information (MI)-driven feature selection with both supervised and anomaly-based ensemble learning to enhance the identification of harmful network traffic. The research intends to determine the most relevant characteristics from the UNSW-NB15 dataset through MI-based feature selection and create a stacking ensemble model that integrates Random Forest and Isolation Forest as base learners with Logistic Regression as the meta-classifier. Additionally, the research assesses the suggested framework through accuracy, precision, recall, and F1-score, and it contrasts its effectiveness with standalone machine-learning classifiers such as Random Forest, Isolation Forest, Logistic Regression, Support Vector Machine, and XGBoost. Ultimately, the research examines the impact of feature selection and the integration of supervised and anomaly-based learning on enhancing intrusion detection effectiveness.

3. Methods

This study is based on the UNSW-NB15 dataset to design a hybrid intrusion detection system which is comprised of the stacking ensemble learning technique for classification of network traffic into harmful and normal [4]. Supervised and anomaly-based learning paradigms are combined to achieve the suggested approach that improves the accuracy of detection and generalization over different attack types. The predictions of the two base learners, Random Forest [3] and Isolation Forest [14] are used as a meta-classifier in logistic regression.

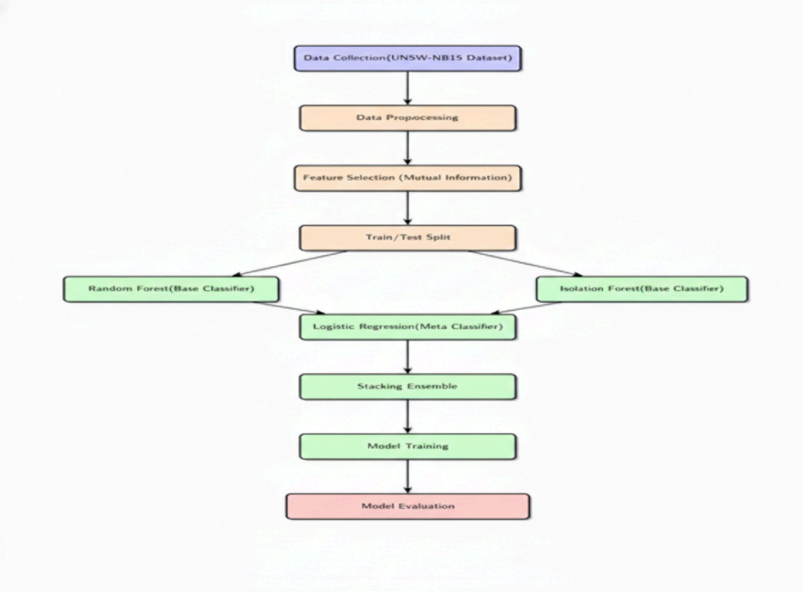


Figure 1: Workflow of the suggested Intrusion Detection System

3.1 Dataset Description

The UNSW-NB15 dataset [4] is one of the widely used datasets for intrusion detection studies. It is composed of real network traffic data from which features are extracted that describe the flow behavior, the characteristics of the packets and information about the protocols. These records include various forms of attack that include DoS, exploits, reconnaissance, worms and normal network traffic. The dataset is well-known with problems such as class imbalance and feature redundancy which make the task of accurate intrusion detection difficult. Such properties call for effective preprocessing, feature selection, and effective learning strategies.

The UNSW-NB15 dataset was chosen because it is appropriate for assessing contemporary intrusion detection frameworks since it includes actual network traffic that includes both typical activities and a variety of sophisticated cyberattacks. The data set is complex enough to evaluate the effectiveness of various feature selection techniques and hybrid ensemble learning models as it provides a number of network traffic variables describing packet characteristics, flow characteristics and protocol information. It has high dimension, high redundancy and high imbalance, making it an appropriate test set for the effectiveness and robustness of the proposed hybrid intrusion detection architecture.

3.2 Data Preprocessing

The preprocessing procedures were performed to prepare the data for training the model before it was trained. To keep just important network traffic aspects, non-essential attributes were first eliminated, such as the redundant `label` and `id` fields. The category attributes proto, service and state were then encoded as numerical values using Label Encoding. To make multiclass classification easier, the target variable `attack_cat`, which represents the attack categories, was also encoded into numerical form.

For numerical features, they were scaled to zero mean and unit variance using z-score normalisation to ensure the numerical features contributed uniformly in the learning process of the model. This normalisation improved the behaviour of the learning algorithms due to its lack of influence over the learning process while features with a wider numerical range were present. Overall, these preprocessing steps reduced redundant data, improved numerical consistency and provided a good foundation for the next step of feature selection using the Mutual Information method and stacking ensemble learning.

3.3 Feature Selection Using Mutual Information

High dimensional data in network traffic could have redundant features that may affect the learning performance. The proposed approach is chosen to reduce this problem: Mutual Information (MI) is used as a feature selection method in the proposed approach, [3] and [11] are adopted. MI is a measure of statistical dependence between the input features and the target classes that was selected because it can detect linear and non-linear relationships between the features and the class attribute. As opposed to the original feature space and dimensionality reduction techniques such as Principal Component Analysis (PCA), the MI can provide a more flexible way of measuring the relevance of features. In the proposed framework the top 10 most informative features were selected for further model training, which involved ranking features through a combination of feature importance scores obtained by the Random Forest algorithm and Mutual Information score. The suggested intrusion detection framework's computational efficiency and classification performance were enhanced by this method, which also minimised redundant information and decreased dimensionality.

The mutual information between a feature Xand the target variable Yis calculated as:

$$I(X;Y) = \sum_{x\in X}\sum_{y\in Y} p(x,y)\log log\left(\frac{p(x,y)}{p(x)p(y)}\right) \quad (1)$$

3.4 Dataset Splitting Strategy

The preprocessed data is divided into 80% training and 20% testing. The training subset defines the parameters of the model and the testing subset is used to test the generalization ability of the proposed IDSs on the data that were not used for training. This will enable an objective evaluation of the efficiency of the model.

3.5 Stacking Ensemble Architecture

For enhancing detection robustness, a stacking ensemble architecture is used [7]. The overall generalisation and classification results of the stacking approach are better than the classification results obtained using individual models, which have complementary properties and are merged into a single predictive modelling system. The framework recommends to combine the predictions of two base classifiers (Random Forest, Isolation Forest) using Logistic Regression as the meta-classifier.

3.6 Base Learners

3.6.1Random Forest (RF)

A supervised ensemble technique called Random Forest uses random feature selection and bootstrap sampling to build several decision trees. It can handle high dimensional data, it is noise robust and is useful for models for complicated decision boundaries. Each tree gets a vote to determine the ultimate class prediction by majority voting:

$$H(x) = majority_vote\{h_1(x), h_2(x), ..., h_n(x)\} \quad (2)$$

For each decision tree, there is a prediction $h_i(x)$ and the final prediction is $H(x)$ by majority voting.

In the proposed architecture, the main supervised base learner is the Random Forest that is responsible for learning complex decision boundaries from the selected network traffic data and for providing reliable classification predictions to the stacking ensemble.

3.6.2 Isolation Forest (IF)

Isolation Forest is an unsupervised anomaly detection technique that isolates the data points by splitting on random features and values. Shorter path lengths are a consequence of the fact that the anomalous samples are typically easier to isolate in fewer splits. The anomaly score of an instance x is set to:

$$s(x, n) = 2^{-\frac{E(h(x))}{c(n)}} \quad (3)$$

where E(h(x)) is the average path length of the successful searches in a binary tree of size n, and c(n) is the average path length of unsuccessful searches in a binary tree of size n. If an instance has a high anomaly score then it is more likely to be anomalous.

In the proposed framework, the base learner is an isolation forest, which can detect unusual and unknown attack patterns that supervised learning models may not be able to learn well. Its forecasts enhance the Random Forest classifier's predictions and add to the stacking ensemble's overall resilience.

3.6.3 Meta-Classifier

Logistic Regression (LR) is suggested as the meta-classifier [6]. To develop the final classification it trains the Random Forest and Isolation Forest base learners to learn the optimal combination of their predictions. Logistic Regression is effective in mitigating overfitting at the meta-learning stage and improving the overall performance of the stacking ensemble due to its computational efficiency, interpretability, and good generalization power.

A sample's probability of being in the attack class is calculated as:

$$P(X) = \frac{1}{1+e^{-(\beta_0+\beta_1 x_1+\beta_2 x_2+\cdots+\beta_n x_n)}} \quad (4)$$

β_1, ..., β_n coefficients refer to the outputs of the base learners and β_0 is the intercept.

The proposed intrusion detection architecture benefits from the complementary features of the supervised and anomaly-based base classifiers, to improve the overall classification accuracy and generalisation skills of the meta-classifier.

3.7 Stacking Training Strategy

The suggested stacking ensemble structure uses an 80:20 train-test split for model building and performance evaluation. The testing subset is utilized to test the performance of the entire stacking structure, and the training subset is utilized to train the basic learners [7]. The first step is to partition the data into training and testing sets at 80:20 ratio. The training data is used to train the base learners, Random Forest and Isolation Forest, whose predictions are fed into the Logistic Regression meta-classifier for training. In this training method, the meta-classifier can successfully fuse the benefits of ANNs and supervised learning, while retaining separate training and testing data sets. This means that information leakage is decreased and the framework's ability to generalise can be evaluated more trustworthily. Training and test sets are clearly separated, which helps to avoid information leakage and fair assessment of generalization capability.

3.8 Model Training and Evaluation

The ability of the stacking ensemble to generalize to never-seen-before network traffic was evaluated by testing on the independent testing subset after training on the training subset.The proposed framework was evaluated using several performance metrics like precision, accuracy, recall, and F1-score. The accuracy of the results was obtained by calculating:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (5)$$

TP, TN, FP and FN stand for true positive, true negative, false positive and false negative respectively.

In order to provide a comprehensive evaluation of the proposed framework particularly in an imbalanced setting, accuracy, precision, recall and F1-score were also determined. These metrics collectively help measure the accuracy of the system at detecting fraudulent traffic and minimizing false positives. The addition of supervised learning and anomaly detection to the stacking ensemble enhances the resilience and performance of the proposed intrusion detection system when tested on the UNSW-NB15 dataset, resulting in better detection of common and new attack patterns.

4. Results

This section presents the classification results and analysis of different machine learning models using UNSW-NB15 intrusion detection dataset[4]. The performance of the models is assessed with widely used performance measures like F1 score, accuracy, precision and recall. The performance of three classifiers – Random forest (RF), Isolation forest (IF), Logistic regression (LR) is observed first, followed by a detailed evaluation of the proposed stacking ensemble model. The discussion focuses on robustness with respect to class imbalance, detection reliability and applicability in real network scenarios.

4.1 Performance of Individual Classifiers

4.1.1 Random Forest Classifier

Table 1. Classification report of Random Forest Classifier

Class	Precision	Recall	F1-Score	Support
0	0.92	0.94	0.93	7418
1	0.95	0.93	0.94	9049
accuracy			0.93	16467
macro avg	0.93	0.93	0.93	16467
weighted avg	0.93	0.93	0.93	16467

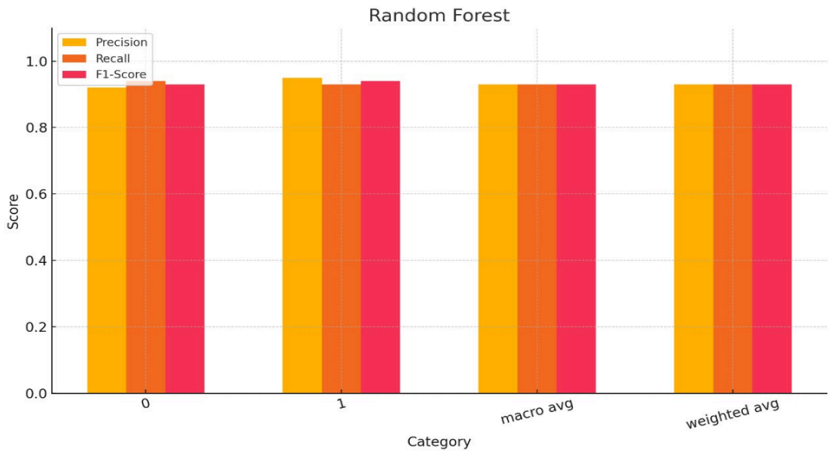


Figure 2. Comparison of Classification Metrics for Random Forest Classifier

The classification results by the Random Forest model are summarized in Table 1 and the corresponding performance measures are shown in figure 2. The classifier shows good balanced behavior on both the normal traffic (Class 0) and attack traffic (Class 1), with 0.92–0.94 and 0.95–0.93 precision–recall values, respectively. The resulting F1 scores of 0.93 and 0.94 indicate good selective ability.

Macro and weighted F1-scores of 0.93 indicate that the model performs well even with class imbalance. The impressive performance of Random Forest is due to its ensemble tree-based structure capable of representing complex and non-linear relationships in network traffic data. The multiple decision trees used by the classifier help to avoid overfitting and enhance the tolerance for noise, which is very suitable for high dimensional feature space intrusion detection applications.

4.1.2 Isolation Forest

Table 2. Classification report of Isolation Forest

Class	Precision	Recall	F1-Score	Support
0	0.91	0.96	0.93	7418
1	0.96	0.92	0.94	9049
accuracy			0.94	16467
macro avg	0.94	0.94	0.94	16467
weighted avg	0.94	0.94	0.94	16467

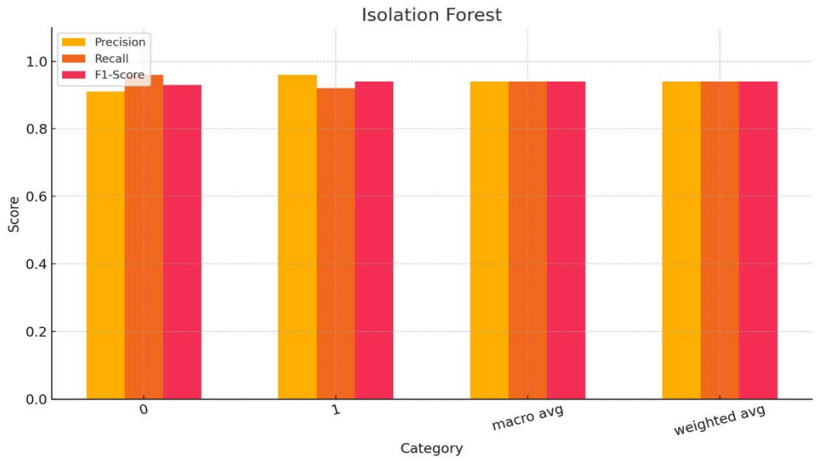


Figure 3. Comparison of Classification Metrics for Isolation Forest

Table 2 shows the results achieved by the Isolation Forest classifier and Figure 3 displays this classification. When compared to Random Forest, the overall performance of Isolation Forest is slightly better, and the macro F1-scores and weighted F1-scores are approximately 0.94. Interestingly, it achieves good precision in attack traffic (0.96) as well as good recall in the normal traffic (0.96). This implies that the model performs well in cases of low numbers of false alarms (precision) in anomaly detection.

Isolation Forest's ability to detect rare and irregular patterns is especially beneficial for intrusion detection systems where unseen or infrequent attacks might emerge. These results validate the use of an anomaly-based approach to augment supervised learning by enhancing its ability to detect abnormal behaviors.

Anomaly based learning is the main reason behind the anomaly detection capability of Isolation Forest, as it is able to isolate data anomalies from the structural differences rather than relying on attack patterns marked by labels. This allows for increased sensitivity to rare and unknown attacks, a very valuable characteristic in a dynamic cyber security environment.

4.1.3 Logistic regression

Table 3. Classification report of Logistic Regression

Class	Precision	Recall	F1-Score	Support
0	0.78	0.60	0.68	7418
1	0.72	0.86	0.79	9049
accuracy			0.74	16467
macro avg	0.75	0.73	0.73	16467
weighted avg	0.75	0.74	0.74	16467

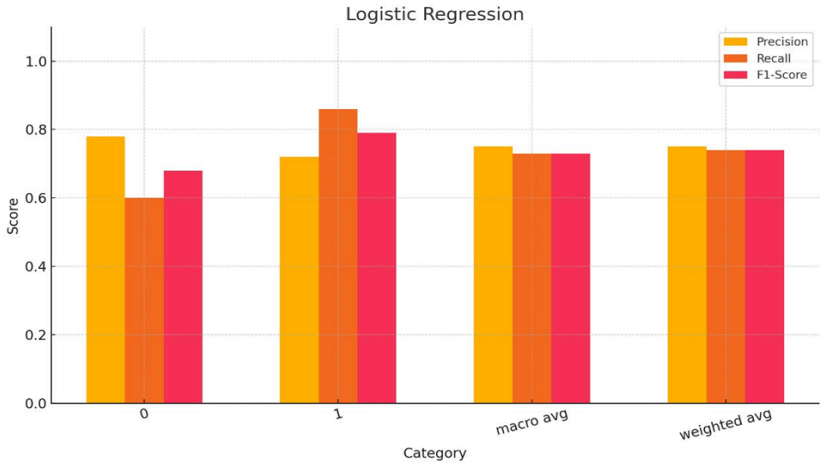


Figure 4. Comparison of Classification Metrics for Logistic Regression

Table 3 and Figure 4 show the performance of the Logistic Regression classifier. LR is less accurate than RF and IF, but has good recall for attack traffic (0.86), making it effective at detecting malicious traffic. But the lower recall for normal traffic (0.60) means that there is a higher false positive rate.

Despite these limitations, logistic regression is useful as a baseline model because it is simple, easy to understand and has a low processing cost. It may be suitable for learning combinations of base model outputs, as a meta-classifier in ensemble methods, due to these properties. While performance-wise logistic regression is not as good as ensemble-based methods, its ease of use and interpretability make it a good option for combining the base learners' predictions in the stacking framework. However, its ability to learn an extremely complicated intrusion pattern is restricted because of its linear decision boundary.

4.1.4 Support Vector Machine

To make the evaluation of the machine learning models comparable, the Support Vector Machine (SVM) model was evaluated with the same preprocessed dataset and selected features. The overall accuracy obtained by the classifier was found to be 73.46%, which is less than what is obtained by the ensemble-based methods. The UNSW-NB15 dataset's complex and high-dimensional features hindered SVM's ability to create the best decision boundaries for both linearly and non-linearly separable data. Furthermore, its ability to perform well in generalisation was further reduced due to the presence of class imbalance and attack categories. The results indicate that the proposed hybrid

stacking approach is more suitable for the complex intrusion detection problem than the conventional single-classifier approach.

4.1.5 XGBoost Classifier

Preprocessed data and selected features were also used to evaluate the XGBoost classifier. It performed better than a few traditional classifiers such as Support Vector Machine and Logistic Regression with 93.64% overall accuracy. The gradient boosting technique of XGBoost efficiently captures complex feature interactions and improves prediction accuracy, by repeatedly minimizing classification errors. However, despite its great performance, XGBoost failed to perform better than the proposed stacking ensemble. The combination of the complementary benefits of anomaly-based learning via the Isolation Forest and supervised learning via the Random Forest is the key to the achievement of better results, giving the proposed model more robustness and generalisation ability.

4.2 Performance of the Stacking Ensemble Classifier

Table 4. Classification report of Stacking Classifier

Class	Precision	Recall	F1-Score	Support
0	0.97	0.98	0.97	7418
1	0.98	0.97	0.98	9049
accuracy			0.9772	16467
macro avg	0.98	0.98	0.98	16467
weighted avg	0.98	0.98	0.98	16467

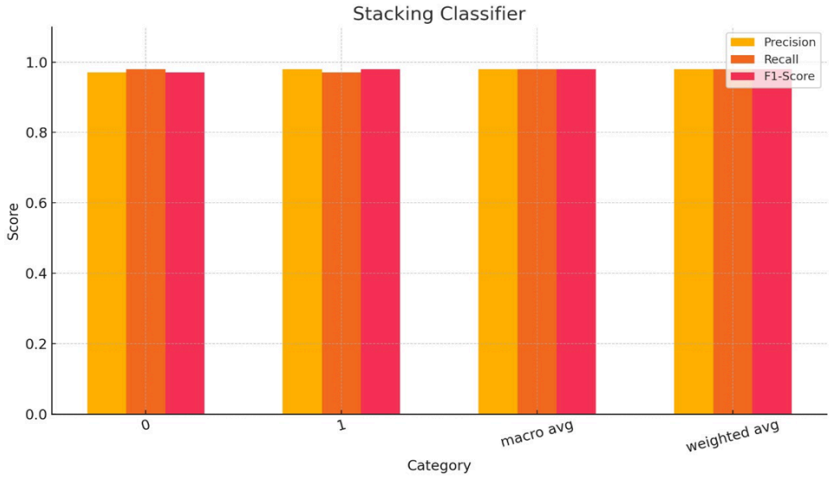


Figure 5. Comparison of Classification Metrics for Stacking Classifier

The classification accuracy of the proposed stacking ensemble is shown in Table 4, and illustrated in Figure 5. The ensemble model achieves the highest precision, recall and F1-scores of around 0.98 for both classes, far exceeding the performance of all other classifiers. It has a high detecting capability that is reflected in its total accuracy of 97.72%.

Macro and weighted averages are close to each other (0.98) and this results in good robustness to class imbalance. With the high precision and recall, the stacking ensemble effectively reduces false positives and false negatives, a critical factor for a realistic IDS deployment.

In this regard, the integrated learners' complementary characteristics are the principle reasons for the performance advantage of the proposed stacking ensemble. Isolation Forest boosts the sensitivity to unusual and less frequent attack patterns, and Random Forest is capable of efficiently detecting organized and non-linear traffic activity. The predictions are fused using Logistic Regression as a meta-classifier for better generalization and reduction of classification errors.

4.3 Comparitive Results

Table 5. Comparative Accuracy of Baseline Models and the Proposed Stacking Framework

Model	Accuracy
Logistic Regression	74%
SVM	73.46%
Random Forest	93%
Isolation Forest	94%
XGBoost	93.64%
Proposed Stacking	97.72%

The study shows that SVM and XGBoost models are competitive models but not as good as proposed stacking ensemble. This is because the stacking model is able to combine supervised and anomaly based learning to help achieve high performance, allowing for the recognition of both common and uncommon attack patterns.

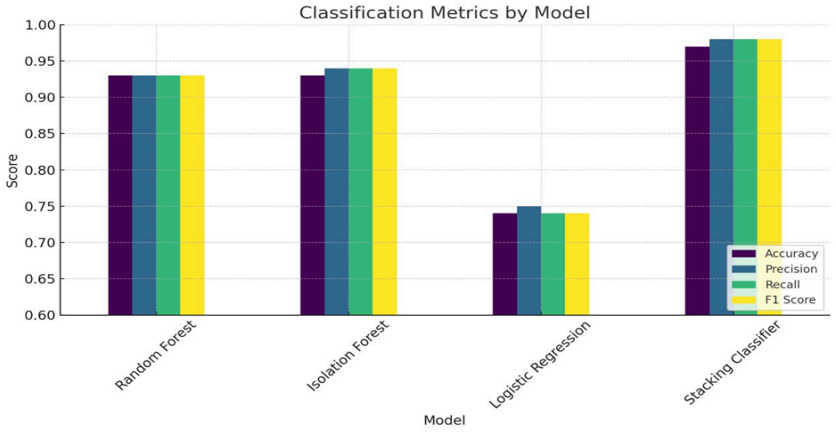


Figure 6. Comparison of classification metrics for each model

The improvement observed is the result of the complementing features of the basic learners in the stacking framework in figure 6. Isolation Forest enhances the ability to detect the atypical and previously unknown attack patterns, while Random Forest is able to learn a complex supervised decision boundary from the selected network traffic attributes. As the meta-classifier, logistic regression reduces false positives and false negatives by learning the best mix of these complementing predictions. Therefore, the proposed stacking model always achieves better accuracy, precision, recall and F1-score than the single classifiers and shows better robustness when the classes are imbalanced. These results show that a unified stacking architecture that incorporates supervised and anomaly-based learning offers a more successful intrusion detection method than depending just on separate machine learning models.

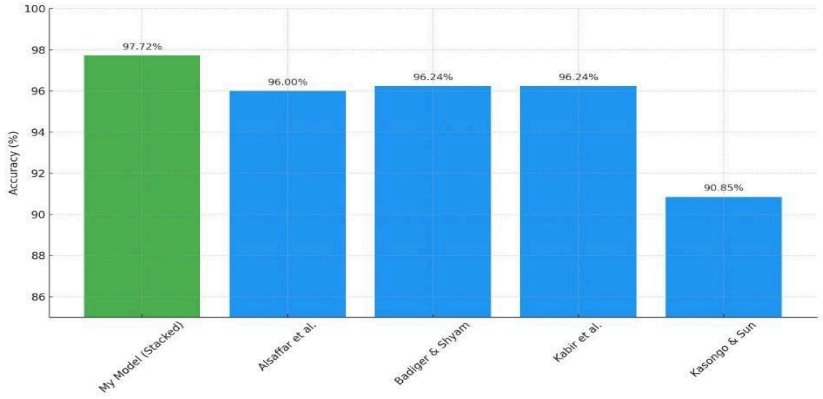


Figure 7. Comparison of different models

The accuracy of the suggested model is compared to more modern IDS techniques assessed using the UNSW-NB15 dataset in Figure 7. With the suggested stacking ensemble, we obtained 97.72% accuracy, which is higher than many of the previous methodologies published. Alsaffar et al. have achieved high accuracy over 96% by base learners RF, XGBoost and MLP with a hybrid stacking approach using feature selection by MI-Boruta [11]. In their work, Badiger et al. obtained 96.24% accuracy using the hybrid feature selection with stacking ensemble technique [12] and Kabir et al. obtained a similar level of accuracy with Extra Trees and Mutual Information Gain in a binary class classification scenario [8].

However, Kasongo and Sun used the traditional classifiers SVM and Decision Trees with XGBoost based feature selection, resulting in an accuracy of 90.85% [4]. The results demonstrate that the stacking ensemble, with hybrid learning and efficient feature selection, enhances intrusion detection capability.

Table 6. Comparison with Existing Studies

Study	Method	Dataset	Accuracy
Kasongo & Sun (2020)	SVM + Feature Selection	UNSW-NB15	90.85%
Kabir et al. (2022)	Stacking Ensemble	UNSW-NB15	96.24%
Badiger et al. (2024)	Hybrid Ensemble Learning	UNSW-NB15	96.24%
Alsaffar et al. (2024)	MI + Stacking Ensemble	UNSW-NB15	96%

Study	Method	Dataset	Accuracy
Proposed Model	RF + IF + LR (Stacking)	UNSW-NB15	97.72%

The results show the proposed model is better than different intrusion detection techniques in the UNSW-NB15 dataset. Supervised and anomaly learning in the stacking framework largely contribute to the improvement. In contrast to the previous research which focused on supervised ensemble approaches, the authors combine the Isolation Forest with other methods to enhance the detection of rare and unseen attack patterns which further boosts the performance.

The results indicate that the integration of feature selection and anomaly-based detection in an architecture (not just ensemble learning) is to blame for this improvement. The combination results in a balanced intrusion detection in a variety of attack categories, and improved robustness when the data are imbalanced.

5. Discussion

5.1 Interpretation of Classifier Performance

The efficacy of the separate classifiers illustrates the varying learning traits of the models when utilized on the chosen network traffic attributes. Random Forest establishes a solid baseline as its collection of decision trees can identify intricate and non-linear patterns in network traffic while remaining resilient to noise. Isolation Forest offers an additional function by detecting outliers through anomaly isolation instead of solely depending on predefined attack patterns. This trait is especially important for intrusion detection, as unusual or irregular traffic might not be sufficiently captured by standard supervised learning models. Logistic Regression, while easy to compute and understand, struggles to model highly complex intrusion patterns due to its linear decision boundary. Likewise, the reduced performance of SVM highlights the challenge of establishing effective decision boundaries for the dataset's complex and imbalanced network traffic characteristics. XGBoost exhibits enhanced learning ability by capturing intricate feature interactions via gradient boosting. The variations between the individual classifiers indicate that the models grasp different facets of network traffic, offering a basis for integrating complementary learning strategies within the suggested framework.

5.2 Effectiveness of Proposed Stacking Architecture

The proposed architecture's effectiveness can be credited to the supportive functions of its individual learners. Random Forest offers supervised classification by leveraging the learned connections between the features of network traffic and attack labels, whereas Isolation Forest adopts an anomaly detection approach that emphasizes recognizing atypical traffic patterns. The outputs produced by these two base learners are then merged using Logistic Regression, offering a simple method for learning how to combine their results. As a result, the stacking architecture can utilize information from both supervised classification and anomaly detection instead of relying on just one learning approach. The analysis of individual components suggests that Mutual Information-driven feature selection enhances this architecture by minimizing redundant data and preserving valuable network traffic features. The integrated design consequently offers a cohesive structure where feature selection and supplementary learning techniques enhance the overall detection effectiveness.

5.3 Comparison with Existing Studies

The evaluation against current research shows that the suggested framework delivers competitive results on the UNSW-NB15 dataset compared to the methods explored in this study. The detected enhancement can be linked to the incorporation of Mutual Information-driven feature selection and the blend of supervised and anomaly detection learning within a stacking framework. Unlike methods that mainly depend on supervised ensemble models, the suggested framework integrates Isolation Forest to offer an extra perspective on anomaly detection. Nonetheless, comparisons with findings from earlier studies need to be approached carefully, as variations in preprocessing

techniques, feature selection strategies, model settings, data divisions, and evaluation criteria may affect the performance reported. Consequently, the comparison offers proof of the proposed framework's competitiveness within the assessed conditions, instead of proving a general performance superiority in all intrusion-detection situations.

5.4 Component -wise Analysis of the Proposed Framework

A component-wise analysis is provided in order to have a better understanding of each component's contribution within the suggested framework. The discussion emphasizes the special contributions of the Random Forest, Isolation Forest, Logistic Regression and Mutual Information-based feature selection algorithms to boosting overall intrusion detection performance. Random Forest and Isolation Forest individually provide a good accuracy, but they are used together in stacking and show very high accuracy. Furthermore, the inclusion of Mutual Information–based feature selection brings efficiency and generalization by eliminating irrelevant features. The possibility to retain useful features while pruning redundant features, along with adding to the efficiency of the learning process without compromising interpretability, also supports the effectiveness of feature selection using MI.

The excellent ensemble performance is due to the complementary nature of base learners. Random Forest is able to detect complex supervised attacks while Isolation Forest shows higher sensitivity to rare and unknown attacks.Random Forest is capable of detecting complex supervised attacks, and Isolation Forest shows higher sensitivity to rare and unknown attacks. The base classifiers learn to make predictions, which are used as the basis of the classification, and Logistic Regression, as a meta-classifier, learns optimal weights for combining all base predictions, thus achieving a robust and balanced classification.

5.5 Computational Complexity and Deployment Considerations

However, when it comes to practical intrusion detection systems, computational efficiency is as critical as the detection performance. Mutual Information-based feature selection reduces the dimensionality of the input data which is beneficial for the proposed framework. This reduction maintains good classification performance while reducing the computing load during model training and inference.

The suggested system makes use of computationally effective machine learning methods, such as Random Forest, Isolation Forest, and Logistic Regression, which together keep the computational cost of model training and inference below manageable bounds. Furthermore, Logistic Regression serves as a simple meta-classifier and the predictions of the base learners can be effectively combined with computational cost.

These properties make the proposed framework suitable for practical network applications where speed and accuracy of detection are important, and enable its deployment.

5.6 Discussion on Practical Applicability

The proposed IDS achieved very high accuracy and good precision–recall values in all trials, demonstrating its feasibility for use in a real network environment. The model can help security analysts more effectively detect malicious activities by reducing the number of false alarms and increasing the detection accuracy. Moreover, the networks implemented by the selected classifiers have moderate computational complexity, ensuring the scalability and flexibility of the framework in large-scale network infrastructure implementations. By using suitable deployment and optimisation techniques, the suggested architecture also offers a versatile basis for next studies on online network monitoring and real-time intrusion detection.

Refrences

[1] Kiran, A., Prakash, S. W., Kumar, B. A., Likhitha, Sameeratmaja, T., & Charan, U. S. S. R. (2023, January). Intrusion detection system using machine learning. In 2023 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1–4). IEEE. https://doi.org/10.1109/ICCCI56745.2023.10128363

[2] Sharma, V., & Shah, D. J. (2024, December). A novel approach to intrusion detection systems using hybrid machine learning techniques. In 2024 International Conference on Artificial Intelligence and Quantum Computation-Based Sensor Application (ICAIQSA) (pp. 1–6). IEEE. https://doi.org/10.1109/ICAIQSA64000.2024.10882184

[3] Hossain, M. A., & Islam, M. S. (2023). Ensuring network security with a robust intrusion detection system using ensemble-based machine learning. Array, 19, 100306. https://doi.org/10.1016/j.array.2023.100306

[4] Kasongo, S. M., & Sun, Y. (2020). Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset. Journal of Big Data, 7(1), 105. https://doi.org/10.1186/s40537-020-00379-6

[5] Zhao, R., Mu, Y., Zou, L., & Wen, X. (2022). A hybrid intrusion detection system based on feature selection and weighted stacking classifier. IEEE Access, 10, 71414–71426. https://doi.org/10.1109/ACCESS.2022.3186975

[6] Mananayaka, A. K., & Chung, S. S. (2023). Network intrusion detection with two-phased hybrid ensemble learning and automatic feature selection. IEEE Access, 11, 45154–45167. https://doi.org/10.1109/ACCESS.2023.3274474

[7] Parashar, A., Saggu, K. S., & Garg, A. (2022). Machine learning based framework for network intrusion detection system using stacking ensemble technique. Indian Journal of Engineering and Materials Sciences. https://doi.org/10.56042/ijems.v29i4.46838

[8] Kabir, M. H., Rajib, M. S., Rahman, A. S. M. M., Rahman, M. M., & Dey, S. K. (2022). Network intrusion detection using UNSW-NB15 dataset: Stacking machine learning based approach. In 2022 International Conference on Advancement in Electrical and Electronic Engineering (ICAEEE) (pp. 1–6). https://doi.org/10.1109/ICAEEE54957.2022.9836404

[9] Santhosh Kumar, V., Saiharish, S., & Dinesh Kumar, A. (2024). Network intrusion detection through stacked machine learning models on UNSW-NB15 dataset. In Proceedings of the 2024 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES) (pp. 1–7). https://doi.org/10.1109/ICSES63760.2024.10910677

[10] Sidharth, V., & Kavitha, C. (2021). Network intrusion detection system using stacking and boosting ensemble methods. In 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 357–363). https://doi.org/10.1109/ICIRCA51532.2021.9545022

[11] Alsaffar, A. M., Nouri-Baygi, M., & Zolbanin, H. M. (2024). Shielding networks: Enhancing intrusion detection with hybrid feature selection and stack ensemble learning. Journal of Big Data, 11(1), 133. https://doi.org/10.1186/s40537-024-00994-7

[12] Badiger, V. S., & Shyam, G. K. (2024). Ensemble technique to detect intrusion in a network based on the UNSWB-NB15 dataset. In S. Kumar, S. Hiranwal, R. Garg, & S. D. Purohit (Eds.), Proceedings of International Conference on Communication and Computational Technologies. ICCCT 2023 (Lecture Notes in Networks and Systems, Vol. 1121). Springer. https://doi.org/10.1007/978-981-97-7423-4_35

[13] Badiger, V. S., & Shyam, G. K. (2025). A multiclass network intrusion detection system using stacking ensemble technique with hybrid feature selection. Journal of Advances in Information Technology, 16(3), 342–356. https://doi.org/10.12720/jait.16.3.342-356

[14] Shanthi, K., & Maruthi, R. (2023, August). Machine learning approach for anomaly-based intrusion detection systems using Isolation Forest model and Support Vector Machine. In 2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 136–139). IEEE. https://doi.org/10.1109/ICIRCA57980.2023.10220620

[15] Megantara, A. A., & Ahmad, T. (2021). A hybrid machine learning method for increasing the performance of

network intrusion detection systems. Journal of Big Data, 8(1), 142. https://doi.org/10.1186/s40537-021-00531-w

[16] Das, A., Pramod, & Sunitha, B. S. (2022). Anomaly-based network intrusion detection using ensemble machine learning approach. International Journal of Advanced Computer Science and Applications, 13(2), 236–243. https://doi.org/10.14569/IJACSA.2022.0130275

[17] Apruzzese, G., Pajola, L., & Conti, M. (2022). The cross-evaluation of machine learning-based network intrusion detection systems. IEEE Transactions on Network and Service Management, 19(4), 5152–5169. https://doi.org/10.1109/TNSM.2022.3157344

[18] M.V., H. V., & Jarin, T. (2025). A hybrid model for detecting intrusions using stacked autoencoders and extreme gradient boosting. Computers & Security, 150, 104212. https://doi.org/10.1016/j.cose.2024.104212

[19] Hammad, M., El-Medany, W. M., & Ismail, Y. (2020). Intrusion detection system using feature selection with clustering and classification machine learning algorithms on the UNSW-NB15 dataset. In 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT) (pp. 1–6). https://doi.org/10.1109/3ICT51146.2020.9312002

[20] Hossen, M. S., Hossain, M. J., Masud, M. A., Samsuzzaman, M., & Bepery, C. (2022). Anomaly based network intrusion detection using ensemble classifiers. 2022 4th International Conference on Sustainable Technologies for Industry 4.0 (STI), 1–6. IEEE. https://doi.org/10.1109/STI56238.2022.10103301