Project Report
On
Intrusion Detection System (IDS)

Circuit Design and Control

Department of Electrical Engineering

KIIT Deemed to be University, Bhubaneswar, Odisha

Submitted By:

Anika Mariam (22053840)

Sagar Saggu (22053881)

Abhay Mallik (22054009)

Bismaya Kanta Dash (22054126)

Bikash Prasad Sah Teli (22054033)

Divyaraj Yadav (22054040)

Prajwal Goit (22054068)

Priyanka Mondal (22054070)

Palak Goyal (22054145)

Ashmita Shah (22054288)

Acknowledgements

Our sincerest gratitude is reserved for the Unseen Power that launched us through this path of doing the doing the K-Explore group project with the strength and patience necessary for work.

We would also like to express our heartfelt gratitude for our guide, Prof. Lipika Nanda, Department of Electrical Engineering, KIIT Deemed to be University, for her invaluable guidance and mentoring which helped us in completing the project work.

Abstract

The project focuses on creating IDS (short for intrusion detection systems) by the use of machine learning and deep learning techniques to enhance network security . IDS provides detection and mitigation of attacks in real time by detection of abnormal patterns in the network traffic or by recognizing the signature of the given attack . The system developed here uses KDD 1999 dataset , for network intrusion detection , containing a wide range of network traffic features . This model uses various machine learning models like SVM(Support Vector Machine) and XGBoost for advanced classification and regression tasks .Various data preprocessing techniques such as PCA and RobustScaler for scaling , Decision trees ,KNearest neighbors ,etc, are used for classification of data. The models are evaluated using accuracy , precision ,F1 and recall score to assess their ability to detect different intrusions . Through the use of ML and DL this project helps demonstrate the usefulness of ML and DL in the areas of cyber threats and detection of previously unseen attack patterns by doing scalable , accurate and real-time detection proving to be more useful than the traditional signature based detection methods.

Introduction

A) Problem Statement:

As we all know, our world is shifting further into the digital realm, a shift that brings with it an ever-increasing danger of attack, be it hacking, malware or denial-of-service (DoS) type attacks. Most of these attacks are prone to causing data loss and tarnishing images which translates to extreme amounts of cash being lost. This has created a scenario where both businesses and individuals have to find methods of protecting their computer networks, devices and files from illegal access and other destructive attacks. It is very important, in the context of computer networks and systems, to have good solutions that can be used in preventing or detecting any system-intrusion. This has resulted in the growing importance of Intrusion detection Systems (IDS). IDS stands for intrusion detection system, which is broadly a security system implemented to observe a network or system's actions for illicit behaviours or breaches of policies. In this way, IDS is a very important security measure for prevention planning, where attacks are anticipated and measures taken to deal with them so as to reduce their destructive nature.

Key features of the IDS include:

- Real-time Monitoring: They are the real-time active threats that are detected and countermeasures are made, with the help of continuous network activity.
- Advanced Analytics: Preprocessing in this case is done through unsupervised machine learning where the end helps in modeling network traffic with a view of escalating the likelihood of identifying security breach attempts.
- Comprehensive Alert System: Instant security breaches once they are spotted and users are informed on time in order to prevent or take appropriate corrective action.
- Integration with Existing Security Infrastructure: Additional safety devices and programs can be added without problems to complement the total security plan.

The importance of IDS for instance is very high. A report set up recently suggested that with an approximate per capita GDP and proved a data breach could lead to damages of about $3.9 million A study also suggested that the losses from cybercrime could be around $6 trillion by 202. Also, owing to the heinous rise in the cases of different cyber related criminals, it has become pertinent that several measures should be adopted by institutions and individuals that will safeguard computer networks and systems against intrusive hazards.

B) Objectives:

The objective of this project is therefore to develop a prototype Intrusion Detection System (IDS) based on machine learning techniques to be able to detect anomalous network traffic.

- Develop & Deploy an ID: Intrusion Detection System.
- Inclusion of KDD Cup 1999 Dataset in the model training phase.
- Data preparations to be done in preparation of modeling to try and have the model perform better.
- Assess the performance of both classifiers: SVM and XGBoost in regard to their efficiency.
- Review models based on conventional models evaluation metrics.
- Proving the potential of the proposed system in terms of Scalability and Adaptability to perform real time Intrusion Detection.
- Practical IDS Models as papers presented to the Cybersecurity Research proceeding within the field. With the help of constant network activity monitoring.
- Advanced Analytics: Unsupervised machine learning techniques are applied to model network traffic, improving the identification of security breaches attempts.
- Comprehensive Alert System: Security breaches as soon as they are discovered and users are notified promptly in order to ensure prompt repair and prevention.
- Integration with Existing Security Infrastructure: Other security tools and systems can be integrated easily to complete the overall security concept.

C) Significance:

This project is important as it shows how the efficiency and effectiveness of intrusion detection systems can be enhanced through the application of machine learning based algorithms. Particularly, instead of relying on pre-defined signatures like other types of IDS, the proposed system will be able to learn new attack patterns from the network traffic. The XGBoost and SVM model are used in the IDS which enhances the cross-sectional model hence it is able to execute a huge volume of information by detecting intrusion instantaneously which makes it applicable in addressing current challenges in network security. The lessons learnt in this project will help in the provision of ideas on how better and efficient informed and robust cyber security systems can be developed in the future frameworks.

Literature Review

Recent research suggests that network intrusion detection is one of the important mechanisms that can help to reduce the levels of security threats that have emerged. The task of type of intrusion classification is presented in a new light, after the deep learning technology was added, detection rate increased tremendously. The results of the experiments using KDD demonstrate that the aforementioned methods execution indeed is more effective than standard approaches of machine learning (Kumar et al., 2020, Li et a1., 2020). There is also a paper analyzing the intrusion detection task using RNNs including a comparison of various classification tasks, learning rate, neuron count (Zhang et al., 2020). This speaks volumes on the growing role of deep learning in designing solutions for network security problems.

The literature reviewed emphasised the role of anomalies detection, features selection and hybrid approaches in IDS research. Studies have been devoted for example to the effective methods of anomaly detection including statistical analysis, clustering and even neural networks (Garcia-Teodoro et al., 2019). Studies were also carried out in searching feature selection and engineering techniques to achieve improvements in deployed IDS detection performance (Zhang et al., 2020). There have also been suggested Hybrid IDSs, which combine both signature and anomaly detection methods in order to take the advantages of the two (Kumar et al., 2020). These developments have improved the accuracy and the scalability of IDS detection but issues like false alarms, missed detections or evasion techniques are yet to be resolved.

Dataset Description: KDD Cup 1999 (or similar data set on Intrusion Detection)

Apart from the collection of network traffic data, the KDD Cup 1999 dataset is also part of attack intrusion detection based data which acts as an evaluation criterion. It was obtained from the darpa intrusion detection system evaluation data set, and it includes data that has been classified as normal from an attack. This dataset has good coverage of different network features as well as different attack types thus it is very good for machine learning model training and intrusion detection model testing.

Usage of the Dataset in the Project:-

Feature Selection: There are various main purposes for structural analysis of the database, among which we can mention taking the network traffic features from the duration, protocol and content for modeling and training machine learning models in the project.

Some of such key features are:

1. Basic features: protocol type, service, flag, and duration
2. Content features: src_bytes, dst_bytes, and num_failed_logins
3. Traffic features: count, srv_count, and dst_host_count
4. Host features: dst_host_srv_count and dst_host_same_srv_rate

The dataset is labeled with one of five classes:

1. Normal: normal network traffic
2. Probe: probing attacks
3. DoS: denial-of-service attacks
4. U2R: user-to-root attacks
5. R2L: remote-to-local attacks

Data Preprocessing:

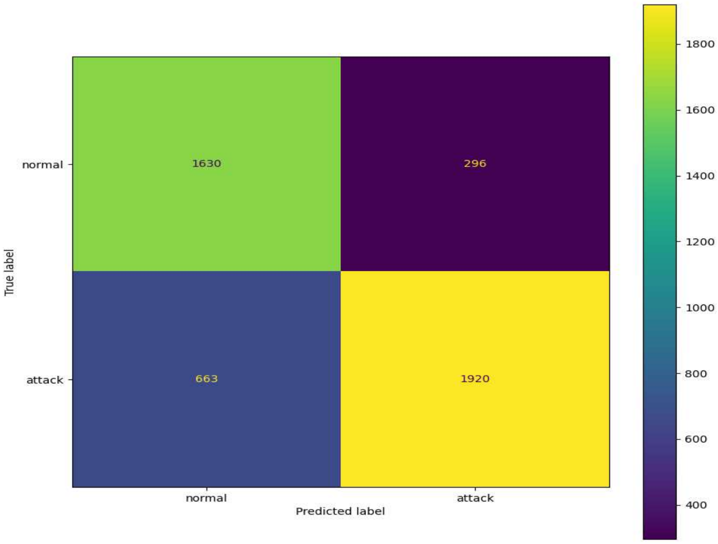
- **Data cleaning:** The mean substitution technique was used to handle missing values for numerical features, while the mode substitution technique was used for categorical features.
- **Feature scaling:** The functionalities were scaled using the Min-Max Scaler so that the range of values in all of the properties is similar and one property does not dominate others.
- **Feature selection:** The Recursive Feature Elimination (RFE) algorithm was applied to rank the predictors and only the top 20 were retained to reduce the dimensionality of the data so that the model performs better.
- **Data normalization:** The data was standardized using the Standard scaler that had zero mean and unit variance, enhancing the performance of machine learning algorithms.
- **Data splitting:** The entire dataset was divided into two groups; training data (80%) for model training and testing data (20%) for evaluation of proposed IDS model.
- **Attack Detection:** The model objectives are training them to classify the traffic as either normal or attack while focusing on detecting DOS, Probe, R2L, and U2R types of attacks.

Methodology

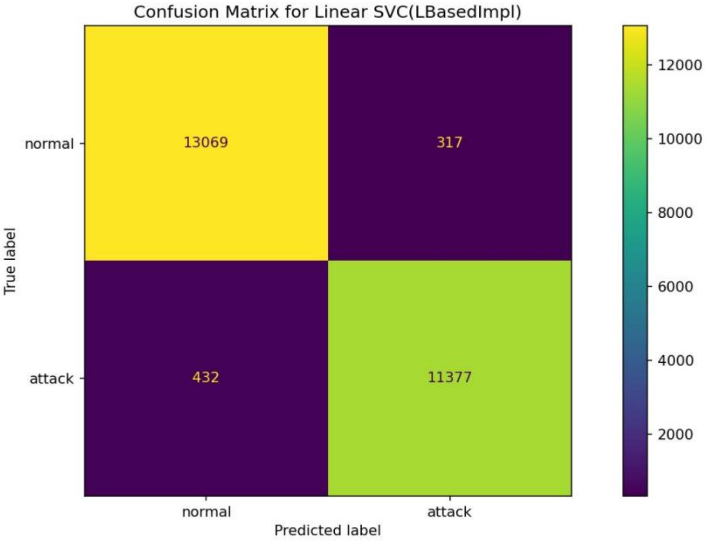
Model Selection

1. Support Vector Machine (SVM) Selection : SVM was chosen for this IDS due to its effectiveness in binary classification and high-dimensional data, making it ideal for detecting malicious traffic.

Train



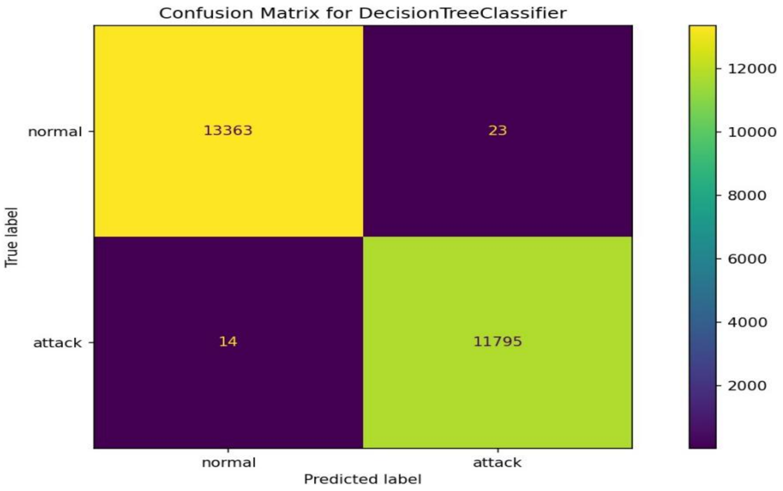
Test



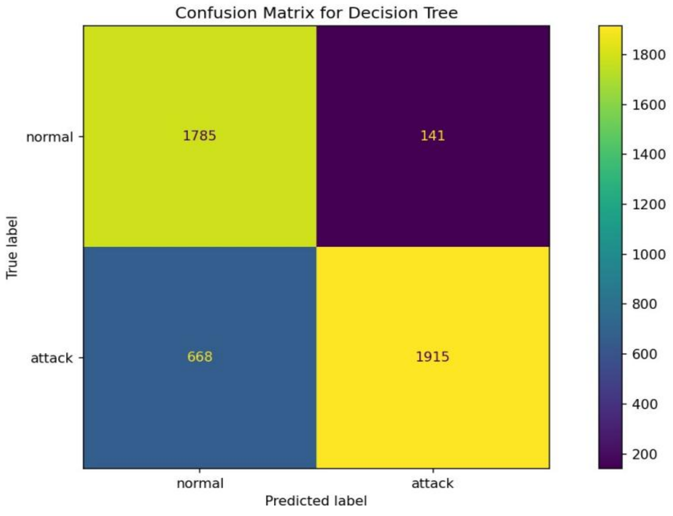
The training confusion matrix shows high accuracy with minimal misclassifications (317 false positives, 432 false negatives). The test confusion matrix indicates lower accuracy, with more misclassifications (296 false positives, 663 false negatives), suggesting possible overfitting.

2. Decision Tree: Splits data based on feature values, useful for identifying key factors in classifying traffic as normal or malicious.

Train



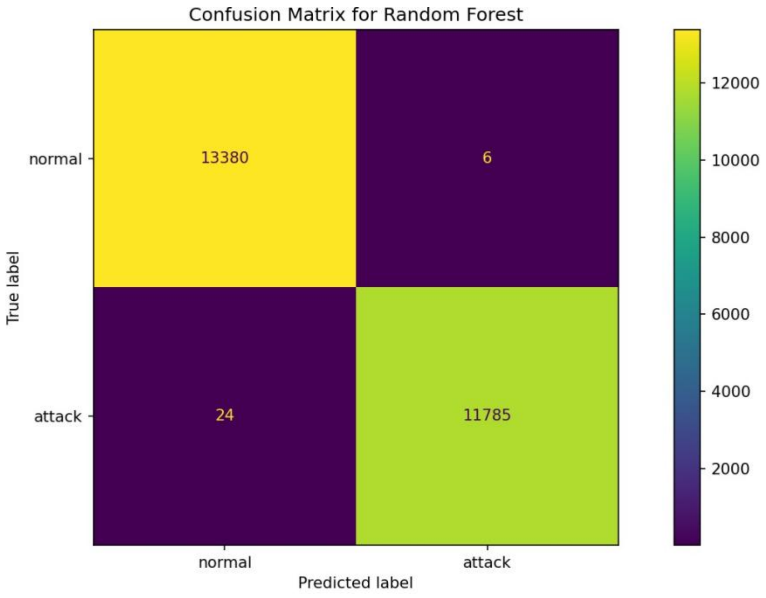
Test



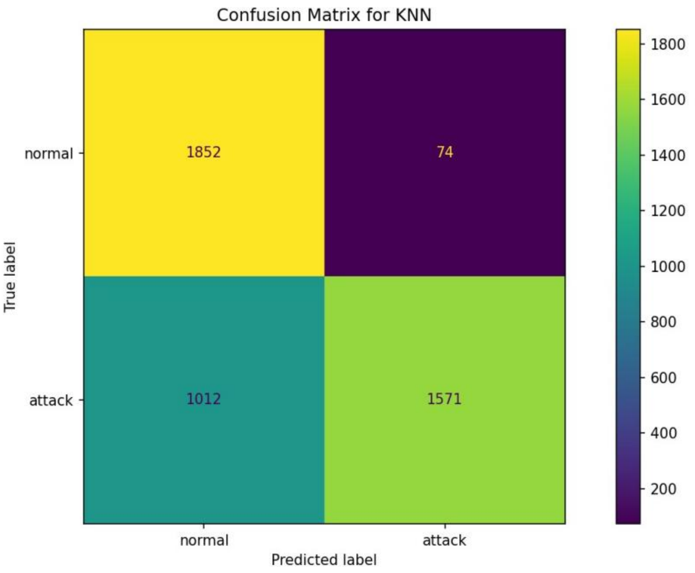
The training matrix shows high accuracy with 13,363 normal and 11,795 attack instances correctly classified and only 37 misclassifications. The test matrix, however, has more errors, with 1,785 normal and 1,915 attack instances correctly classified but 809 misclassifications, suggesting possible overfitting.

3. Random Forest: Uses multiple decision trees to enhance accuracy and reduce overfitting, ideal for complex classification tasks.Doing more precise classification of traffic as normal or malicious.

Train



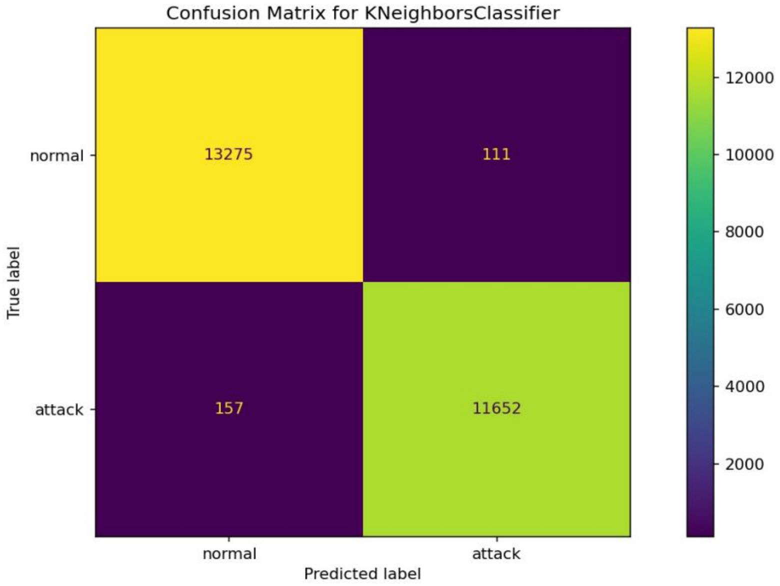
Test

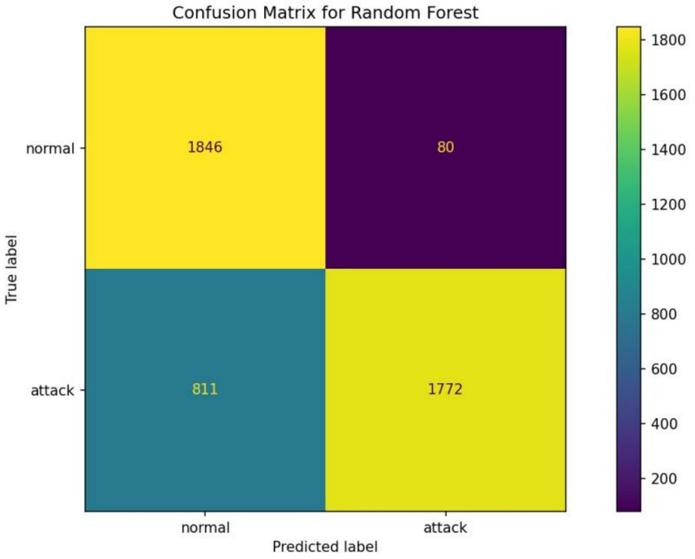


The training matrix shows 13,380 normal and 11,785 attacks correctly classified with minimal errors, while the test matrix has 1,846 normal and 1,772 attacks correctly classified, with higher errors indicating lower test accuracy.

4. k-Nearest Neighbors (k-NN): Classifies based on nearby data points in feature space, effective for data with clear clusters.Also useful in classifying or categorizing the traffic .

Train **Test**

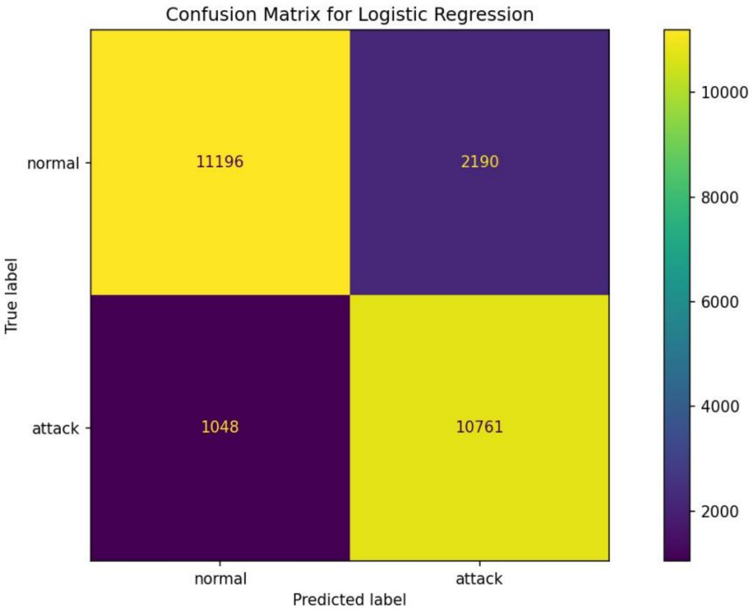




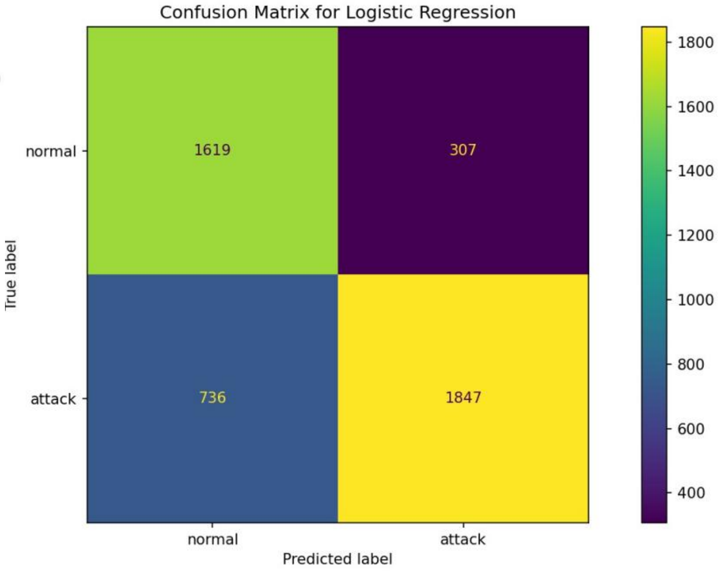
The training matrix shows high accuracy, with only 111 "normal" and 157 "attack" misclassifications, demonstrating effective classification. The test matrix has lower accuracy, with 74 "normal" and 1,012 "attack" misclassifications, indicating difficulty in identifying attacks accurately.

5. Logistic Regression: Linear model for binary classification, good as a baseline for comparison due to simplicity.

Train



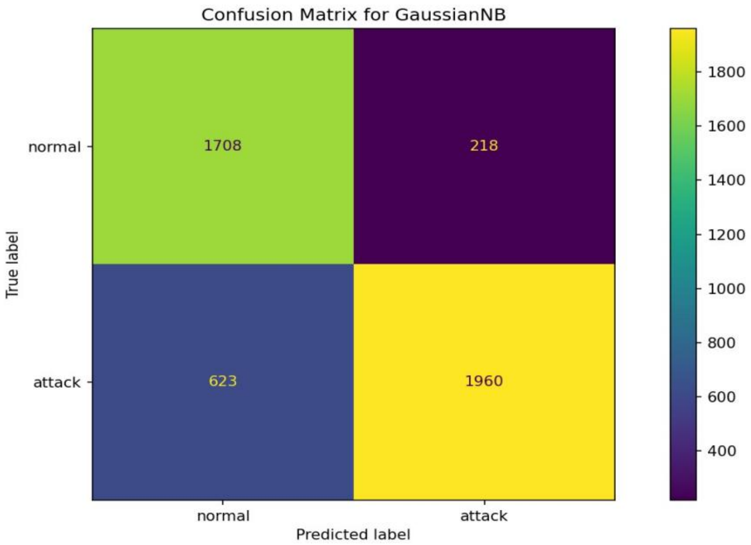
Test



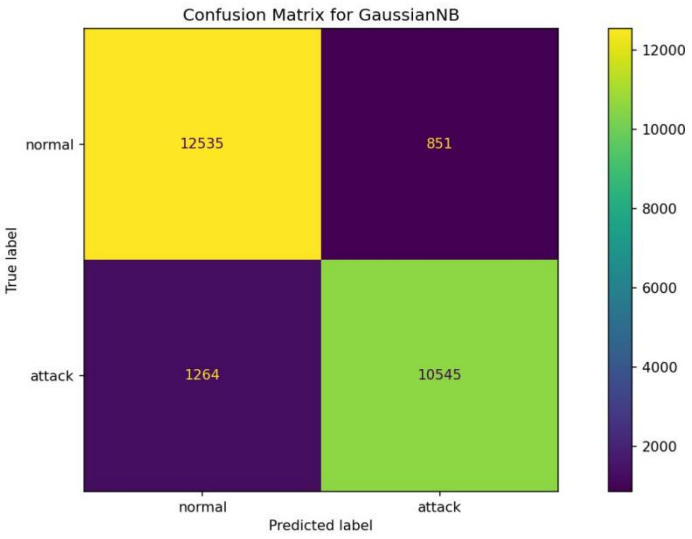
The model correctly classified 11196 "normal" and 10761 "attack" instances in the training data, but only 1619 "normal" and 1847 "attack" instances in the test data. This indicates overfitting, where the model performs well on the training data but poorly on unseen data.

6. Naive Bayes : Naive Bayes is a probabilistic model often used for intrusion detection due to its simplicity and speed. It helps in classifying traffic by estimating the probability of each class (normal or malicious) given the feature values , assuming all features are independent .

Train



Test



The model correctly classified 12535 "normal" and 10545 "attack" instances in the training data, but only 1708 "normal" and 1960 "attack" instances in the test data. This indicates underfitting, where the model is too simple to capture the complexity of the data.

7. Neural Networks: Automatically learns complex data patterns; useful for advanced detection but requires larger datasets. Confusion matrix isn't exclusive to neural networks, it's a valuable tool for analyzing their performance in classification tasks.

Training Process

Data Preparation

- Labeling: The dataset was labeled with binary outcomes ("normal" and "attack") to simplify classification.
- Scaling: Features were scaled using methods like Robust Scaler to manage outliers and ensure consistency across feature ranges.

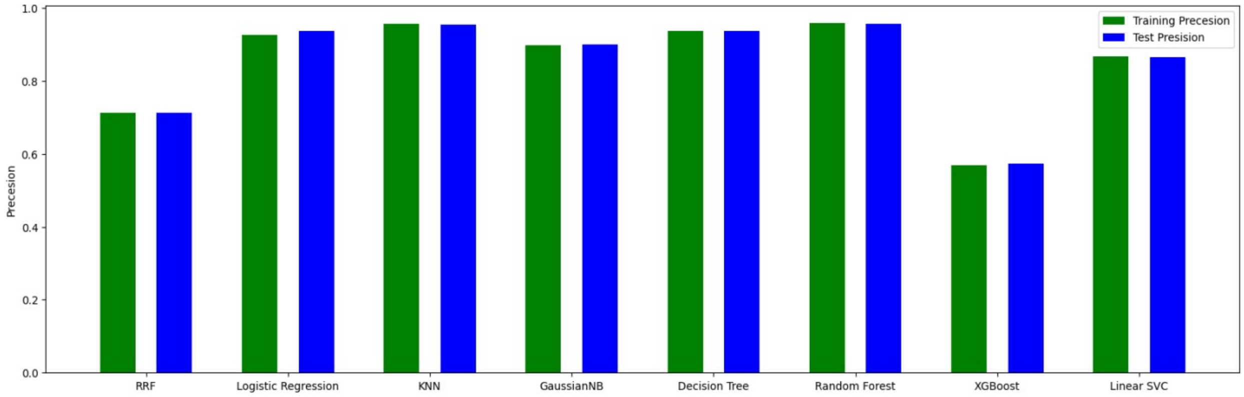
Model Training: Models were trained on the training dataset, with each algorithm adjusted to its optimal settings (e.g., kernel='rbf' for SVM, max_depth=3 for Decision Trees).

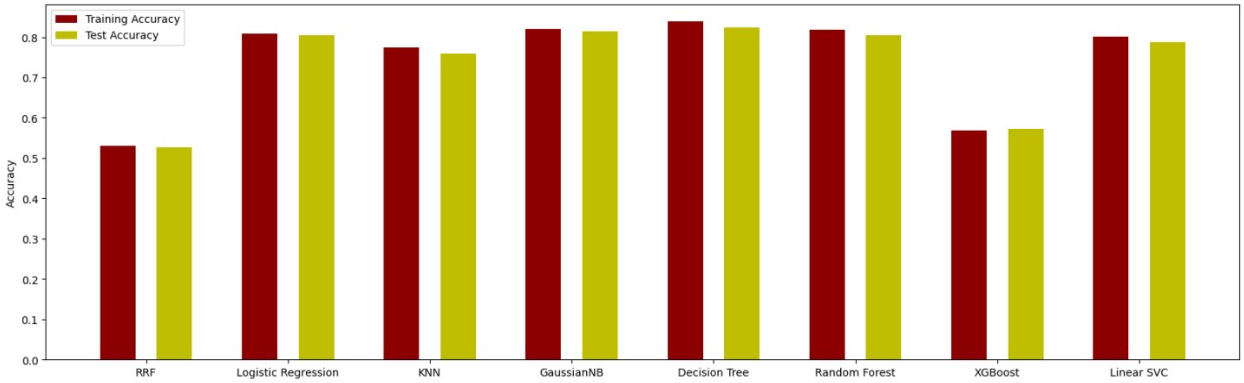
Validation: The evaluate_classification function provided performance metrics (accuracy, precision, recall) on the test data, allowing for a direct comparison of models.

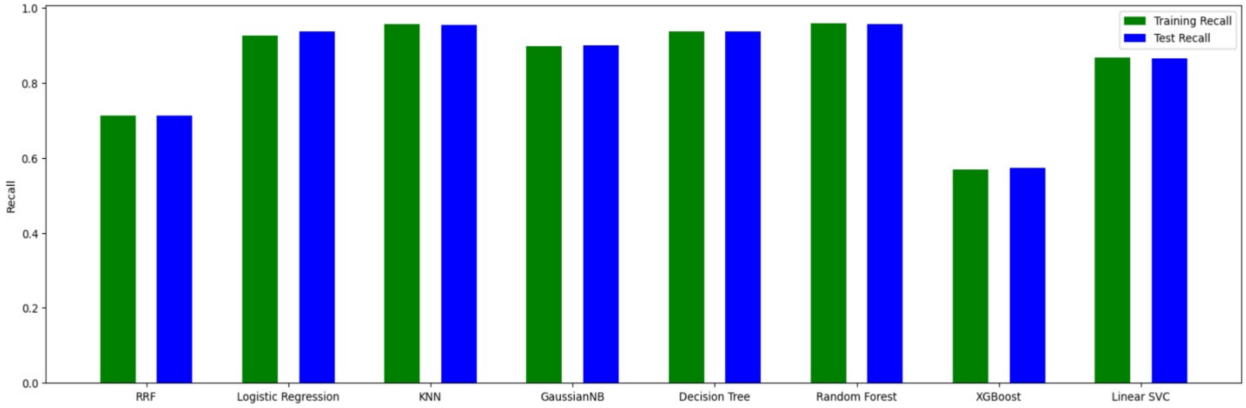
Final Model: Based on performance metrics, SVM was selected as the primary model due to its balance of high accuracy and ability to capture non-linear relationships, making it effective for real-time intrusion detection.

Results

An intrusion detection dataset was utilized to train machine learning models capable of classifying network activity into normal and attack. By conducting this evaluation, the effectiveness of the different models in detecting intrusions in real time was established:



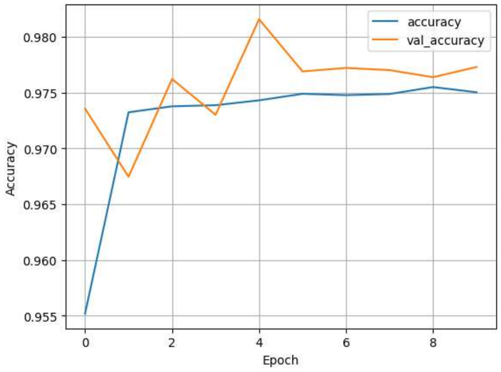




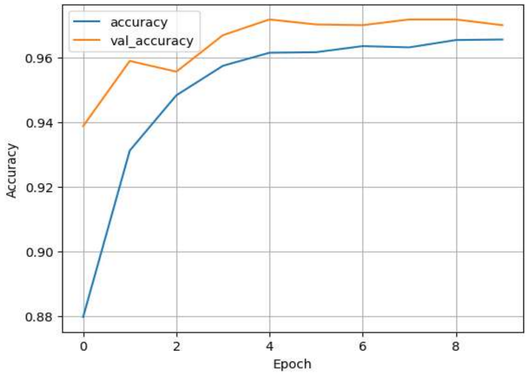
- **DNN**: Ideal for complex datasets with nonlinear patterns, likely to offer high accuracy, precision, and recall. Regularization and dropout layers help with generalization.
- **Random Forest**: Great for structured data, robust against overfitting, and computationally efficient.
- **SVM**: Effective for binary classification but less scalable with large datasets.

Top Choice: Both DNN and Random Forest are strong candidates. DNN may slightly outperform if the data is complex, but Random Forest is highly adaptable and reliable for tabular data.

Train



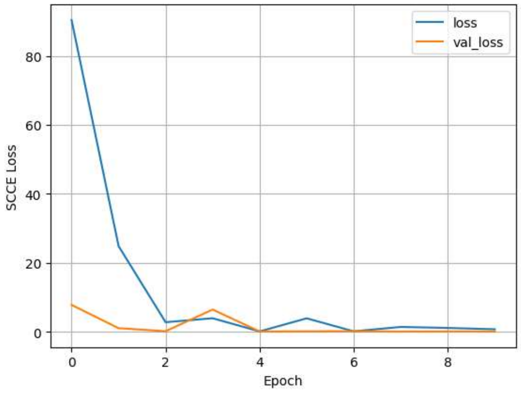
Test



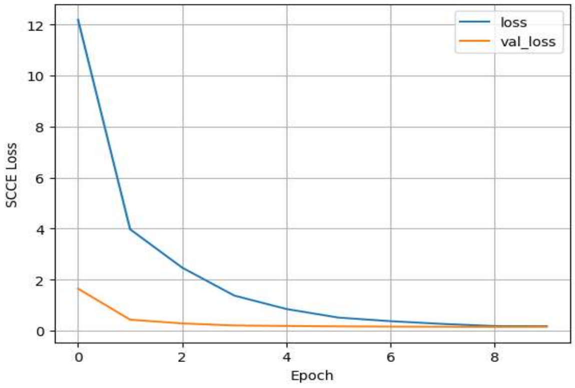
Training Accuracy: Starts at 88%, reaches 96.5% by the 10th epoch, closely matching validation accuracy, indicating minimal overfitting.

Testing Accuracy: Starts at 95.5% and improves to about 97.5%, with validation accuracy staying close throughout.

Train



Test



Training Loss: It drops sharply at first but has fluctuations, suggesting possible overfitting or instability during training. This indicates that the model might be memorizing rather than generalizing well.

Test Loss: The loss decreases smoothly without oscillation, which suggests good generalization to new data.

Summary: The test loss in the first image reflects better model performance and generalization, while the fluctuations in the training loss in the second image indicate some overfitting. Both training and testing show high accuracy, but testing performs slightly better in generalization and stability, suggesting strong model performance across datasets.

Conclusion

This study showed the potential of machine learning techniques to be integrated with intrusion detection systems. From the models evaluated, SVM was the best suited for the task since it was capable of classifying attack and normal traffic patterns. Nonetheless, for practical usage, issues like the computational resources and scalability of the system need more emphasis.

Suggestions for Further Research Work:

- **Deep Learning Techniques:** The adoption of neural networks, and deep learning techniques for the classification tasks may boost performance especially in capturing complex traffic patterns. The utility of recurrent neural networks (RNNs) and convolutional neural networks (CNNs) for sequential and spatial feature learning respectively could be considered.
- **Hybrid Detection:** Incorporation of the SVM classifier which is trained together with some anomaly detection capabilities based on machine learning approaches could increase the IDS responsiveness to new patterns of normal activity.
- **Model Optimization:** Work in the future may seek to improve the performance of the KNN and SVM models while keeping in mind computational costs which will enable real time detections in systems dealing with large volume of transactions.

To sum up, the results achieved in this work confirm the possibility to improve the network security by intrusion detection systems, which use machine learning algorithms, to a considerably higher degree of precision. The enhancement of the discussed techniques and their further development seek for more flexible and resilient IDS solutions which can combat against diverse threats to the networks.

References

1. Mynuddin, M., Khan, S. U., Chowdhury, Z. U., Islam, F., Islam, M. J., Hossain, M. I., & Ahad, D. M. A. (2024). Automatic Network Intrusion Detection System Using Machine learning and Deep learning. *Automatic Network Intrusion Detection System Using Machine Learning and Deep Learning*. https://doi.org/10.36227/techrxiv.170792293.35058961/v1
2. V, S., G, S., Thomas, H., Singh, V., & D, S. (2024). Intrusion detection using machine learning technique [Research Article]. *International Journal of Creative Research Thoughts (IJCRT)*, *12*(5), 48–50. https://www.ijcrt.org