**Cybersecurity (Intrusion Detection System)**

***By***

## **Ojaswa Awasthi [BT23CSA060]**

## **Mangesh Thale [BT23CSA065]**

## **Vivek Yadav [BT23CSA035]**

## 

## **Semester: 4 th Branch: CSA**

## 

**Course Name: Machine Learning**

***Under the guidance of***

# **Dr. Pooja Jain**

|  |  |
| --- | --- |
|  |  |

**Department of Computer Science and Engineering Indian Institute of Information Technology Nagpur - 441108 (India)**

**April – 2025**

**© Indian Institute of Information Technology (IIIT) 2025**

**Abstract**

Cybersecurity is a major concern around the world. Intrusion Detection Systems (IDS) play a crucial role in safeguarding networks from malicious attacks by identifying abnormal activities. This study explores the effectiveness of various machine learning models Logistic Regression, K-Nearest Neighbors (KNN) Classifier, Random Forest Classifier, Decision Tree Classifier, and Support Vector Classifier on the NSL-KDD dataset. Among the models tested, Random Forest and KNN classifiers achieved the highest accuracies of 99.92% and 99.88% respectively, demonstrating their superior performance in detecting intrusions. The results underscore the potential of ensemble and distance-based methods in enhancing IDS accuracy.These insights could help build smarter, more reliable intrusion detection systems that better protect today’s increasingly complex digital environments.

**Introduction**

Cybersecurity is not just about protecting data; it's about protecting trust. In the emerging era where data is the new currency, data protection needs to be a major concern in the field of cybersecurity, hence we need better systems which can protect data from unwanted, unauthorized interference. These interferences can vary from data threats and data breaches

and could undermine the integrity and smooth functionality of systems. Safeguarding against such threats is at most an area of importance in cybersecurity.

Intrusion Detection Systems(IDS) has traditionally served as a cornerstone of network security.

An Intrusion Detection is a software/hardware that identifies suspicious activities and potential risks within a network or interconnected networks. In a very basic sense it is like a security guard that constantly watches your digital infrastructure and prevents intrusions of unauthorised access towards data.

Traditional intrusion detection systems (IDS) mainly rely on known patterns or signatures to spot threats, which means they often miss new or unknown attacks. They also need regular manual updates, which can be time-consuming and not always practical. Attackers can hide their actions by making them look like normal activity, making it harder for traditional systems to catch them. These systems don’t learn or adapt on their own, so they become outdated unless someone updates them manually.

On the other hand, machine learning (ML) methods offer smarter and more flexible solutions. ML models can spot unusual behavior, even if the threat has never been seen before. They can learn from new data and improve over time, helping them stay up to date with new types of attacks. ML systems can also analyze large amounts of data quickly, detecting threats in real time. Once they’re set up, they need less hands-on work and can handle complex, large networks much more effectively.

In our suggested Intrusion Detection System (IDS) model, we initially applied a heatmap to examine feature correlations and chose only the most significant ones. We dropped features with a correlation of less than 0.15 with the target column since they were less predictive. We then scaled the chosen features with Standard Scaler so that all values were on the same scale. Our target column initially had a single "normal" class and numerous various categories of anomalies. To make it easier, we categorized all the anomalies into one "anomaly" label. We trained our model and tested it for binary classification (normal vs. anomaly) as well as multi-class classification (normal vs. types of attacks).

**Literature Review**

Intrusion Detection Systems (IDS) are pivotal in ensuring network security through identifying malicious behavior and policy breaches. The NSL-KDD dataset, a refined extension of the KDDCup'99 dataset, resolves the latter's redundancy and imbalance, hence serving as a widely used benchmark for testing IDS models. This paper reviews recent work that utilizes machine learning (ML) and deep learning (DL) methods in intrusion detection using the NSL-KDD dataset and identifies their approaches, achievements, and shortcomings.

**1. Machine Learning Approaches**

Machine learning models are commonly applied to IDS because of their ability to learn from past attack patterns and generalize to identify novel threats. Most studies that use ML algorithms tend to focus on feature selection, preprocessing, and tuning for improving detection rates.

Patel et al. (2020) applied a Random Forest classifier to the NSL-KDD dataset with an accuracy of 85.34%. Their contributions highlighted the significance of ranking feature importance towards enhancing detection rates and model simplicity. Correspondingly, Bansal and Garg (2021) examined using Support Vector Machines (SVM) in conjunction with Principal Component Analysis (PCA) for reducing dimensionality, achieving a detection accuracy of 83.91%. Though these approaches provide interpretability and satisfactory performance, they tend to be weak in discovering minority class intrusions like U2R (User to Root) and R2L (Remote to Local).

Ensemble methods have also been investigated for their stability. Gupta and Kaur (2021) suggested a voting ensemble of Decision Trees, K-Nearest Neighbors (KNN), and Naïve Bayes, which provided a better accuracy of detection at 87.16%. Their model was, however, the subject of careful tuning of individual learners and adjustment of class weights to counter overfitting.

**2. Deep Learning Approaches**

Deep learning models have the advantage over conventional ML approaches of learning hierarchical representations automatically from raw input features. Deep models have been found to perform well in dealing with large, intricate network traffic data like NSL-KDD.

Tavallaee et al. (2017) used a Deep Belief Network (DBN) with 89.92% accuracy, citing superior generalization as well as feature extraction automatically, as the greatest advantages. Yet another prominent paper by Yin et al. (2017) used a deep neural network (DNN) and reached a 82.66% accuracy, although the training time took much longer when compared to other traditional ML methodologies.

Recurrent Neural Networks (RNNs), especially Long Short-Term Memory (LSTM) networks, have also been explored for temporal dependencies in network traffic. Kim et al. (2019) utilized an LSTM-based IDS and achieved 91.21% accuracy, beating shallow models in identifying sequential patterns of attacks. Their research, nonetheless, noted the requirement of heavy computational resources as well as hyperparameter adjustment.

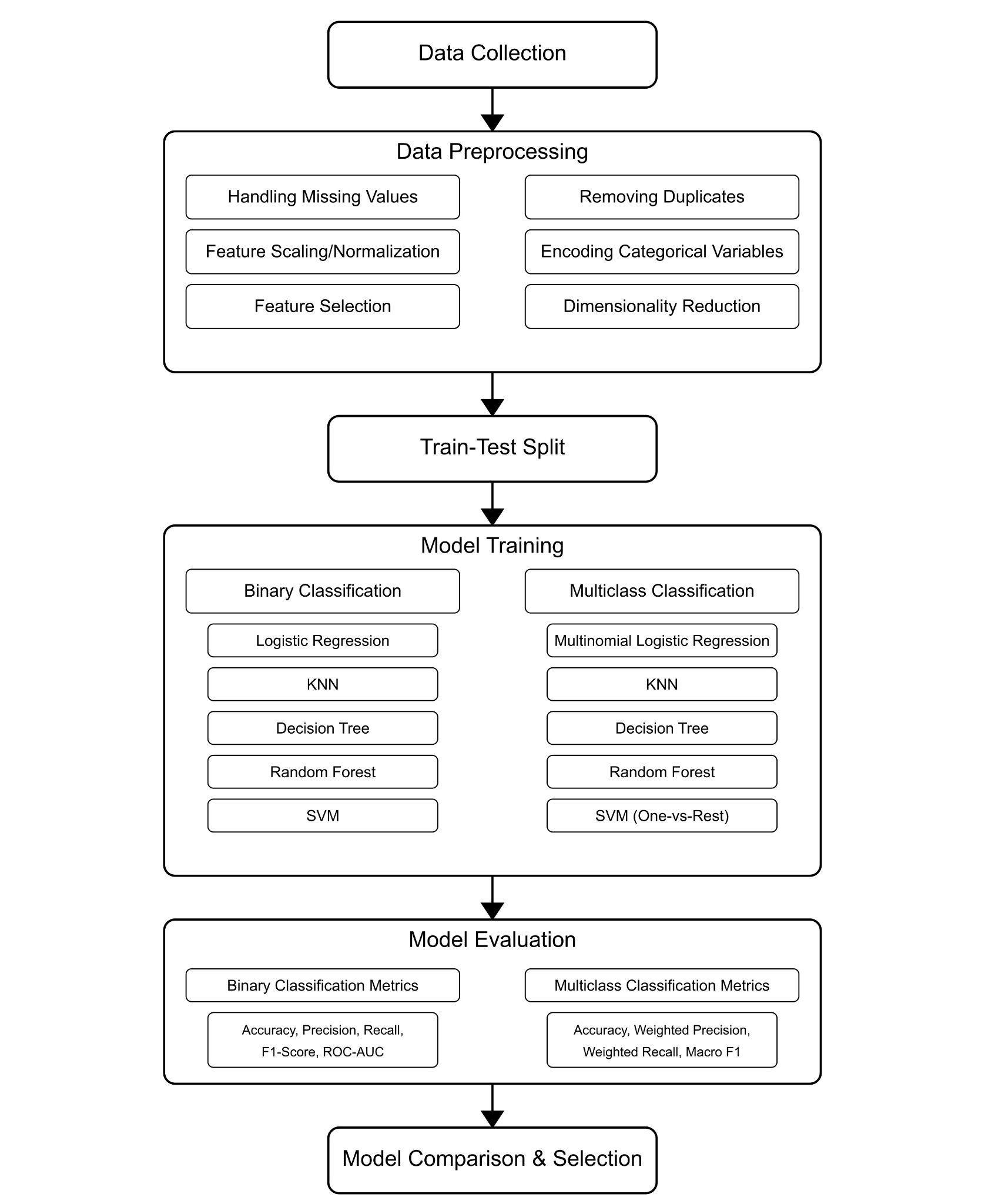
Convolutional Neural Networks (CNNs) now present themselves as a strong competitor to traditional methods of intrusion detection by approaching the data as structured input. Roy et al. (2020) designed a CNN-based classifier that obtained a 88.77% accuracy, marking it as being strong in the detection of spatial characteristics of the dataset but lacking when it came to temporal pattern extraction.

**3. Comparative Insights and Limitations**

Throughout the discussed literature, deep learning techniques in general provide better accuracy and identification of intricate patterns than conventional machine learning algorithms but consume more computation, take more time to train, and demand larger labeled training datasets for efficient operation. Meanwhile, machine learning models provide faster training and increased interpretability that can be a boon in real-time intrusion detection systems.

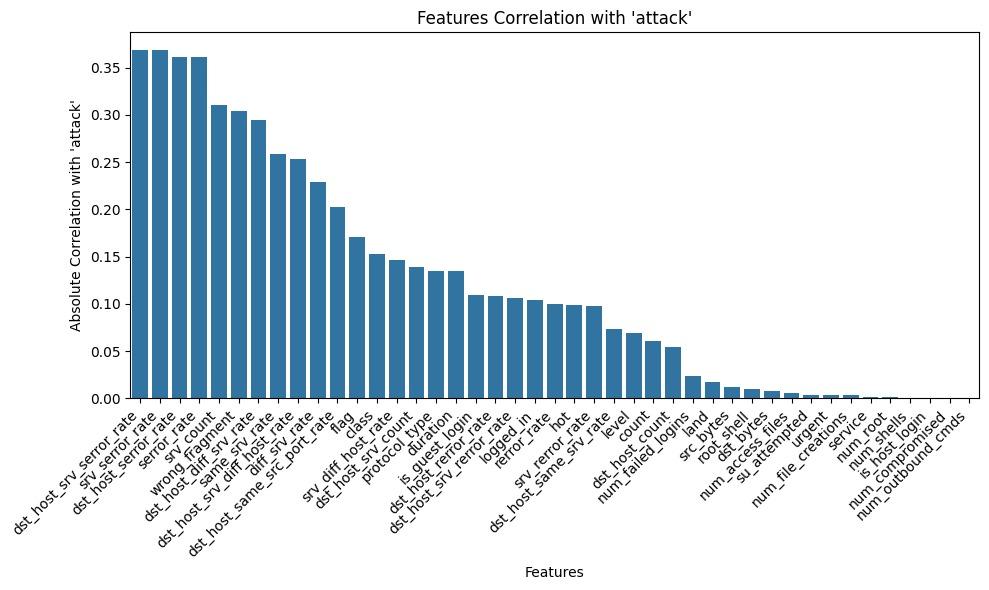
Although NSL-KDD is a handy benchmark, its artificiality and restricted simulation of contemporary network traffic pose problems. Numerous studies have recommended its use together with real data or new dataset creation to make IDS evaluations more relevant.

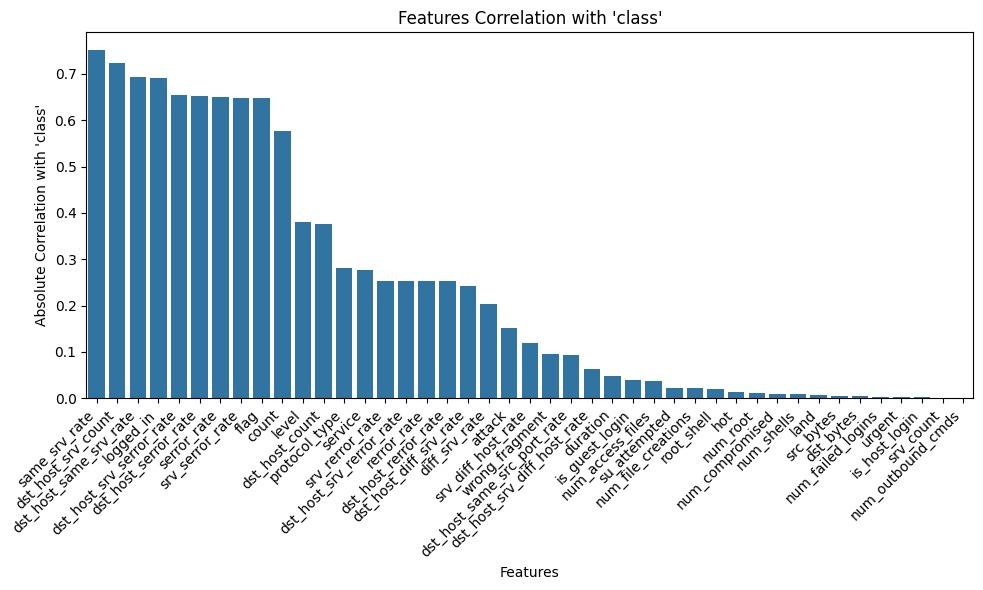
**Methodology**

****

**Data Preprocessing**

Data preprocessing is a crucial part of ML model without preprocessing, models can create problems such as overfitting, low accuracy scores, inaccurate predictions, and much more. In our NSL-KDD dataset we dealt with missing and duplicate values by replacing them with their mean or mode values and deleting the duplicate values. Many features were of object data type so we used label encoder to convert it into numerical data types. Initially our dataset was multiclass classification based, we have further added a new column ‘class’ for binary classification. As there are many features (more than 40) we need to use correlation matrix for both binary as well as multi class classification for important feature extraction for better accuracy. Standardization, also known as the z-score normalization method for feature scaling used as it significantly enhances the accuracy of our predictive model.





**ML Algorithms**

**Logistic regression**

It is a statistical model mainly used for binary classification ,where it predicts one of two possible results. Logistic Regression predicts the probability of features whereas linear regression predicts continuous values .It is widely used due to its simplicity and efficiency.

**KNN**

As the full form suggests that it selects the nearest neighbours in its decision making from the surrounding data points , here k is the hyperparameter which decides range of nearest neighbours which are taken in considerations while the the model is trained .this comes under lazy learner ,as it does not train during the model but just stores entire training datasets.

In our case we used k as 3 , and it gave us best case accuracy .

**Decision Tree**

Decision trees are particularly good at high volumes of network data ,separating normal and suspicious behaviours which helps cyber security professionals in real time.

They are composed of three types of nodes: the root node , internal node and leaves nodes.

Gini impurity and information gain are the two important metrics utilized in the process.

Decision trees efficiently handle large datasets excel in classification and prediction, adapt to evolving intrusion methods and contribute to robust network security with their simplicity and speed.

**SVC**

SVC is a type of support vector machine used for classification tasks , it works by finding the optimal hyperplane that separates different classes in the feature space .The kernel function used was linear , rbf , poly , sigmoid , depending upon datasets characteristics . standardization was applied prior to model fitting due to SVC’s sensitivity to feature scales.

**Random forest classifier**

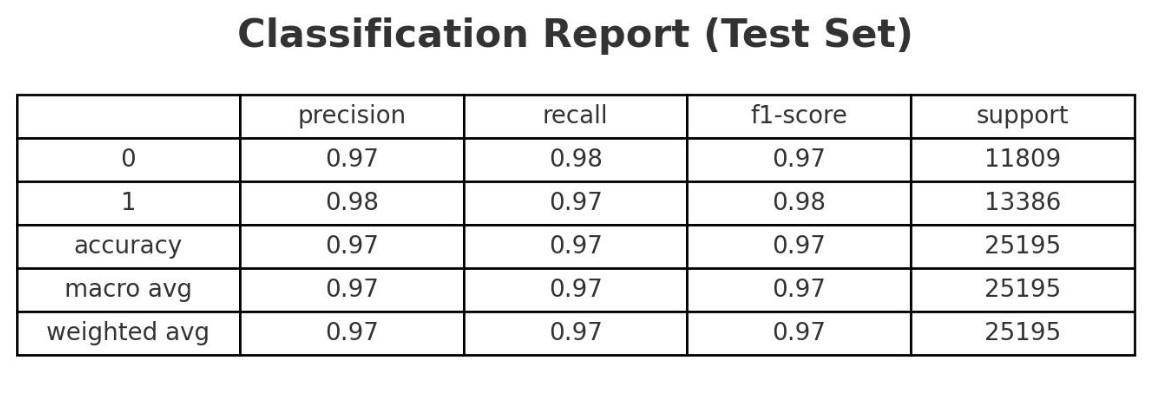
Random forest is an ensemble learning method that builds multiple decision trees and merges their output to improve classification accuracy and control overfitting.the model was trained on the same training data and evaluated on the test set . feature importance scores were also extracted to interpret the model’s decision making process.

**Result & Analysis**

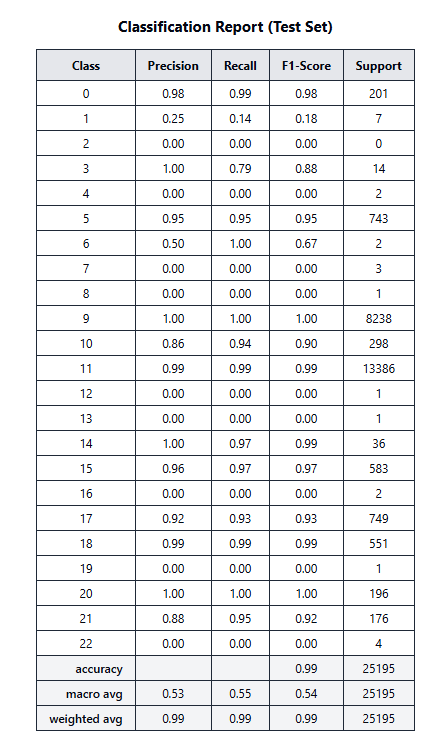
In our analysis of the results, we evaluated the performance of five ML models for Intrusion IDS such as DT, RF, SVC, Logistic regression and KNN. Our focus was on assessing key performance metrics by considering “Important features ” set in our evaluation.We evaluate each model’s effectiveness using metrics such as accuracy,recall, precision, and F1 score, supplemented by visual representations of confusion matrices to illustrate their classification capabilities.

**Logistic regression results:**

Binary :

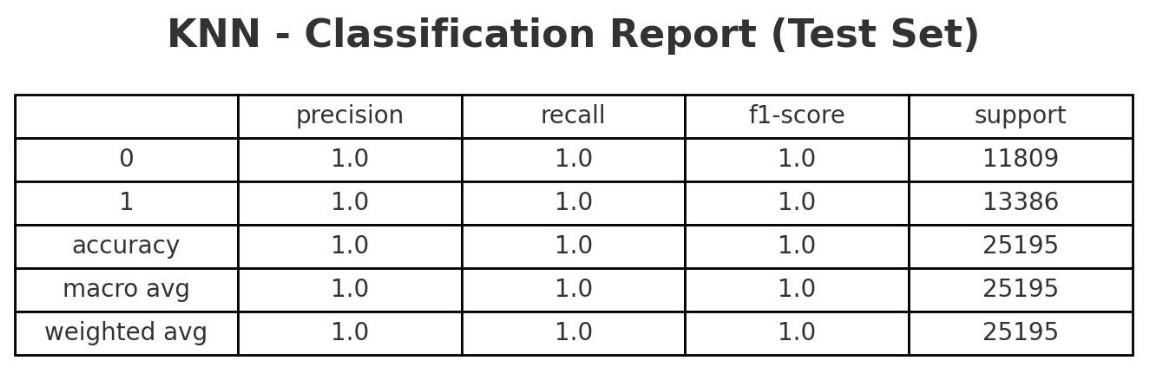


Multiclass:

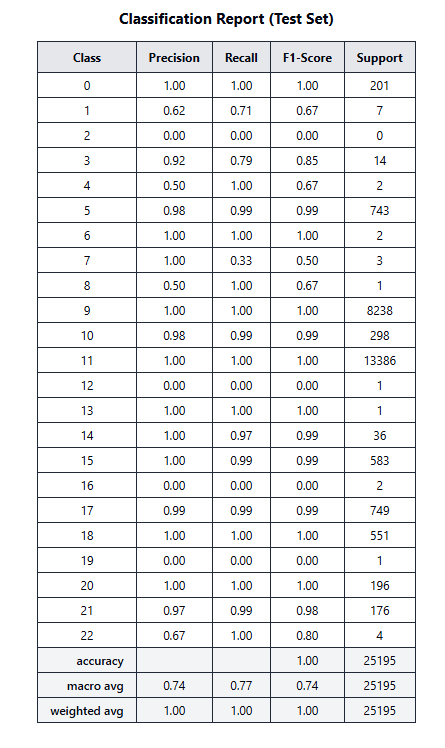


**KNN Results:**

Binary class:



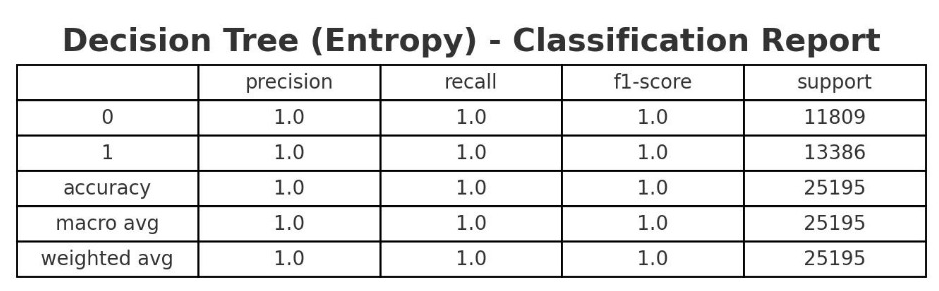
Multiclass:



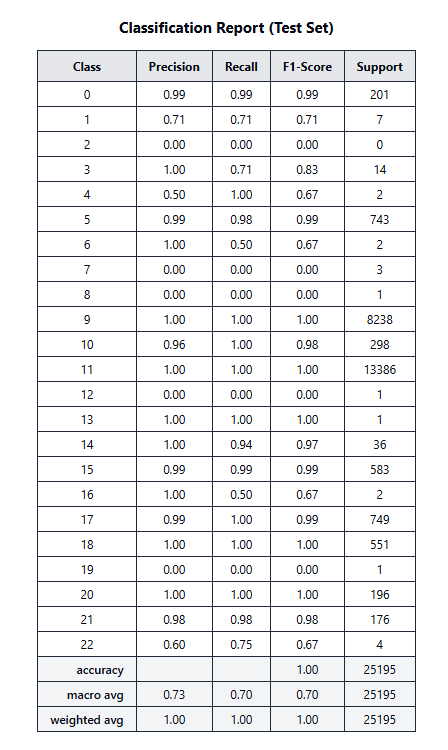
**Decision Tree Results**

Binary class:



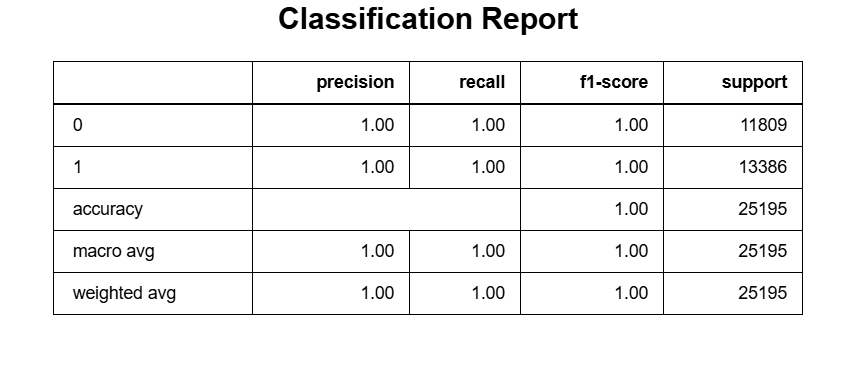


Multiclass:

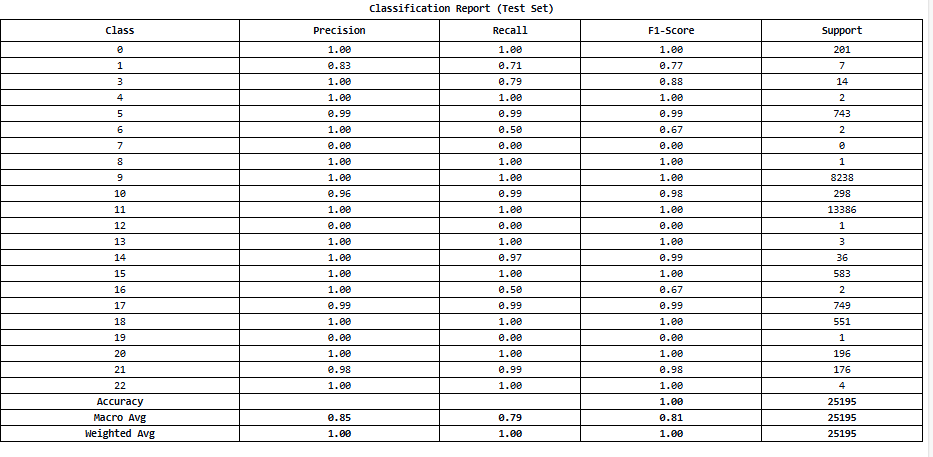


**Random Forest Results**

Binary class:

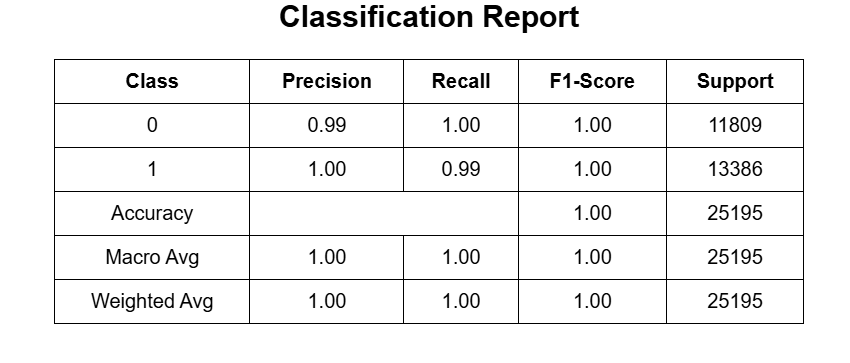


Multiclass:

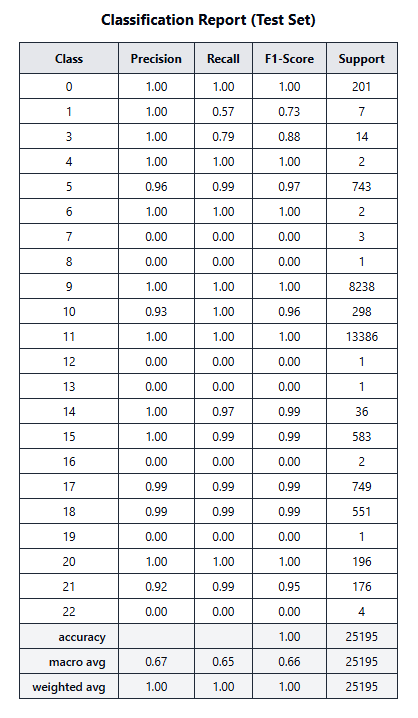


**SVC**

Binary:

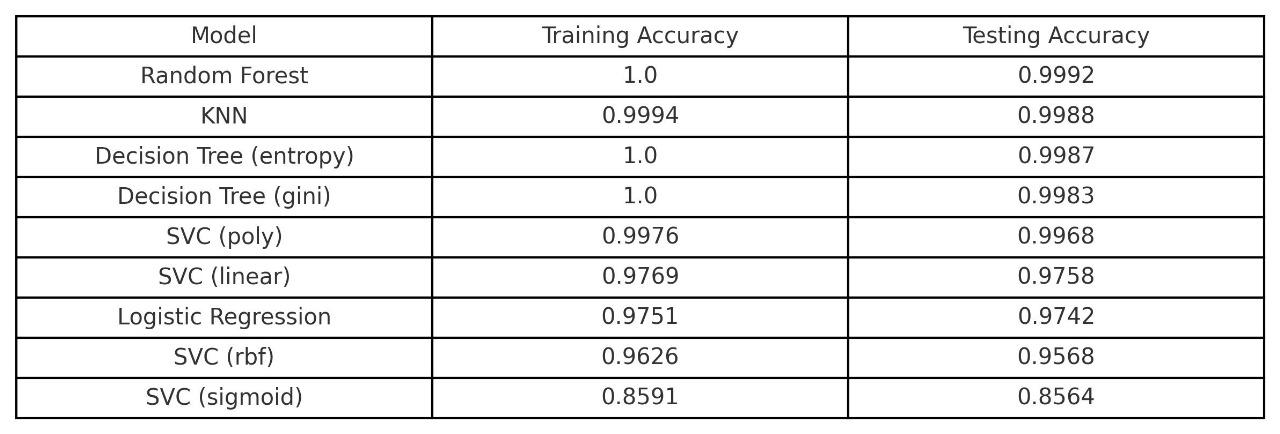


Multiclass:

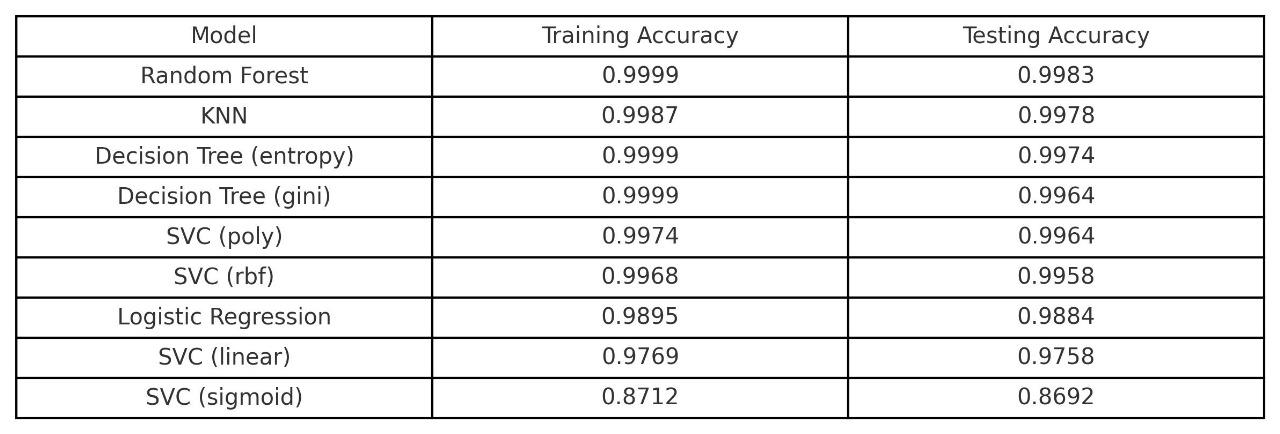


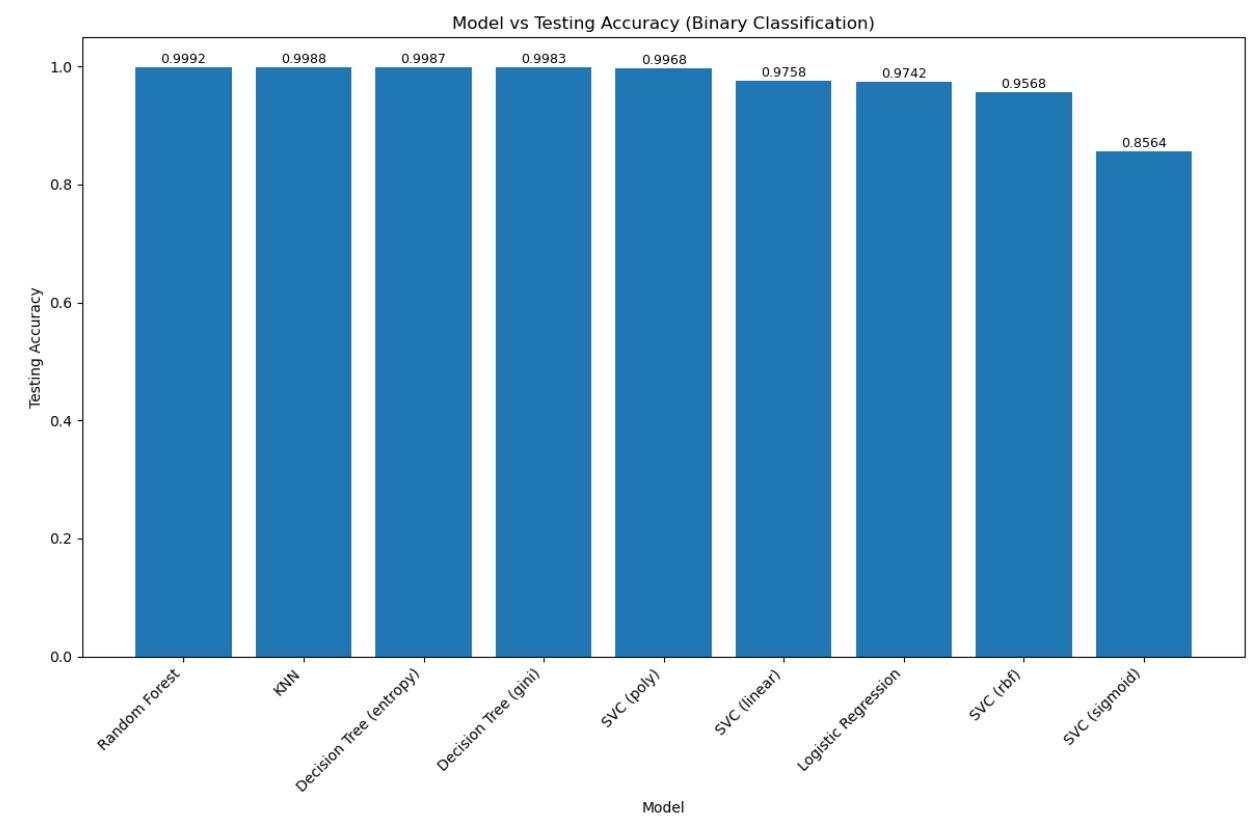
**All Model Comparison**

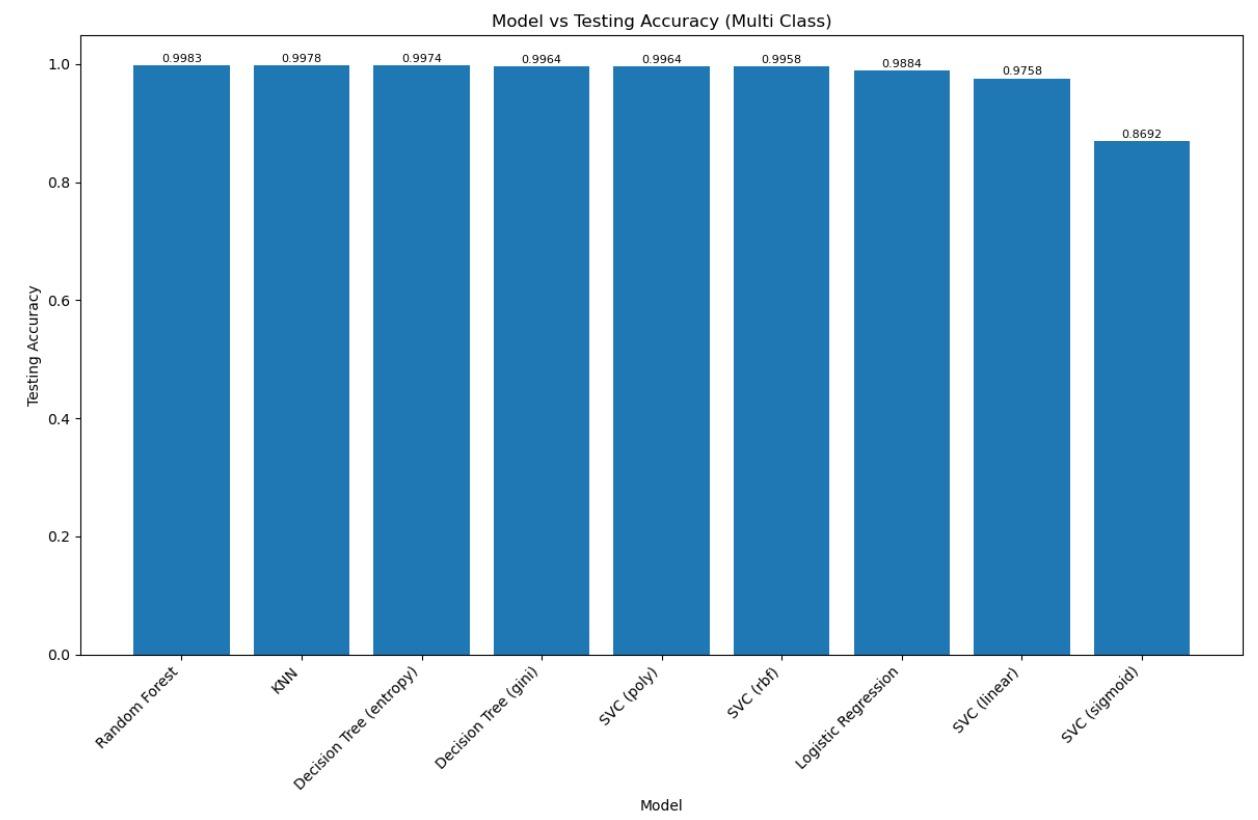
Binary class



Multiclass



****

****

**Conclusion**

The growing sophistication of cyber attacks requires sophisticated Intrusion Detection Systems (IDS) that can effectively detect and counter malicious behavior. This research investigated the performance of different machine learning algorithms—Logistic Regression, K-Nearest Neighbors (KNN), Decision Tree, Random Forest, and Support Vector Classifier (SVC)—on the NSL-KDD dataset for binary and multi-class intrusion detection. Amongst them, Random Forest and KNN classifiers exhibited exemplary performance, providing accuracies of 99.92% and 99.88%, respectively. These observations portray the effectiveness of ensemble and proximity-based algorithms for identifying intrusions with high accuracy and recall rate. Our results are consistent with previous work, affirming that machine learning algorithms, especially ensemble methods such as Random Forest, provide strong solutions for IDS by effectively managing feature correlations, scalability, and class imbalance. Although deep learning methods have been promising in other research, our paper highlights that classical ML models can provide similar—or even better—accuracy with less computational cost, making them viable for real-time implementation.

Yet, there are challenges, such as the necessity of ongoing model adjustment to changing attack patterns and the incorporation of real-world network traffic data for more realistic testing. Future work might investigate hybrid models that blend deep learning with ensemble methods to further improve detection while preserving interpretability.

In summary, this research highlights the promise of machine learning in constructing more intelligent, more dependable IDS, which can help make cybersecurity frameworks more robust in a more digital world. Through the use of high-performing models such as Random Forest and KNN, organizations can more effectively protect their networks from known threats as well as emerging threats.

**References**

1. Tahri, Rachid & Balouki, Youssef & Jarrar, Abdessamad & Abdellatif, Lasbahani. (2022). Intrusion Detection System Using machine learning Algorithms. ITM Web of Conferences. 46. 02003. 10.1051/itmconf/20224602003.
2. Talukder, M.A., Islam, M.M., Uddin, M.A. *et al.* Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction. *J Big Data* 11, 33 (2024).
3. Benmalek, Mourad & Haouam, Kamel-Dine. (2024). Advancing Network Intrusion Detection Systems with Machine Learning Techniques. Advances in Artificial Intelligence and Machine Learning. 4. 2575-2592. 10.54364/AAIML.2024.43150.
4. Thapa, N., Liu, Z., KC, D. B., Gokaraju, B., & Roy, K. (2020). Comparison of Machine Learning and Deep Learning Models for Network Intrusion Detection Systems. *Future Internet*, *12*(10)