IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

AI-DRIVEN NETWORK THREAT DETECTION: COMPARATIVE ANALYSIS OF RANDOM FOREST, XGBOOST, AND HYBRID ENSEMBLE MODEL ON NSL-KDD DATASET

[1]Dr. S. Brindha, [2]Ms. D. Priya, [3]Sharvanthvadivelan, [4]Ragav Aananth SK
[1]Associate Professor, [2]Assistant Professor, [34]Students
Department of Computer Networking,
PSG Polytechnic College, Coimbatore, India

Abstract: This paper presents a comparative analysis of three Artificial Intelligence (AI) based models — Random Forest, XGBoost, and a Hybrid Ensemble Model (Random Forest + XGBoost) — for detecting network threats. The NSL-KDD dataset was used to train and evaluate the models. The study aims to improve the accuracy, precision, and reliability of intrusion detection systems by combining ensemble learning methods. Each model was tested under the same preprocessing and training conditions, and performance metrics such as Accuracy, Precision, Recall, and F1-score were analyzed. Results showed that the Hybrid Ensemble model achieved the best performance with an accuracy of 99.45%, proving that combining Random Forest and XGBoost enhances overall detection capability and reduces false alarms.

Index Terms *- Network Security, Machine Learning, Artificial Intelligence, Random Forest, XGBoost, Hybrid Ensemble, NSL-KDD, Threat Detection.*

I. INTRODUCTION

The increasing number of cyberattacks has made network security a top priority across all sectors. As digital systems grow, so do the methods used by attackers. Traditional firewalls and antivirus programs often fail to detect complex or zero-day attacks. Therefore, researchers have shifted toward using Artificial Intelligence (AI) and Machine Learning (ML) techniques to automatically detect threats from patterns in network traffic.

AI systems learn from data and can identify suspicious behaviors that might go unnoticed by human administrators. The main goal of this study is to develop a system that uses AI to detect various types of network threats efficiently and accurately. To achieve this, three models — Random Forest, XGBoost, and a Hybrid Ensemble model — are implemented and tested using the NSL-KDD dataset, a widely used benchmark in intrusion detection research.

II. NETWORKING THREAT DETECTION

Network threat detection is the process of identifying malicious or abnormal network activity that can harm systems or steal data. Attacks like Denial of Service (DoS), Probing, Remote-to-Local (R2L), and User-to-Root (U2R) are common in modern networks.

Machine Learning algorithms can help detect these attacks by analyzing network traffic logs and identifying unusual behavior. Each network packet carries information like source and destination IP, protocol type, and service used — these act as features for the AI models to learn from. An effective network threat detection system must have: high accuracy in classifying normal vs. malicious traffic, low false positive rate, and ability to adapt to new or unseen attacks.

This study explores how Random Forest, XGBoost, and a Hybrid approach perform in meeting these criteria.

III. MACHINE LEARNING MODELS IN NETWORKING

Machine Learning plays a crucial role in building modern cybersecurity solutions. By learning patterns from labeled datasets, ML models can automatically classify new network traffic as safe or harmful. For network security, Supervised Learning algorithms like Decision Trees, Random Forest, and XGBoost are used. These models learn from historical attack data and predict the type of attack in real-time. Ensemble methods combine multiple algorithms to produce better results than individual models.

The three main algorithms considered here — Random Forest, XGBoost, and the Hybrid Ensemble — are chosen for their accuracy, scalability, and suitability for tabular network data.

IV. DATASET COLLECTION

The NSL-KDD dataset was used for this study. It is an improved version of the KDD'99 dataset and contains labeled records of network connections classified as either "normal" or one of several types of attacks.

4.1 Traffic Data

The dataset includes both normal and malicious traffic data collected from simulated network environments. Each record contains 41 features, including basic features (duration, protocol type, service), content features (number of failed logins, root access attempts), and traffic features (connections per second, bytes sent and received).

The dataset is somewhat imbalanced — some attacks occur more frequently than others. This imbalance affects model performance because the model may learn more about frequent attacks and less about rare ones. Proper balancing and resampling techniques are applied during training to handle this issue.

V. DATA PREPARATION

Before feeding the data into machine learning models, several preprocessing steps are performed.

5.1 Raw Network Data

The raw NSL-KDD data contains missing values, categorical features (like "protocol_type"), and mixed scales (some values range from 0–1, others up to 1000). Without preprocessing, models can misinterpret these differences.

5.2 Preprocessing Steps

The following steps were applied: Data Cleaning removed duplicates and missing values. Encoding converted categorical data (e.g., "TCP", "UDP") into numeric form using label encoding. Normalization scaled all numerical values between 0 and 1 for uniformity. Feature Selection used Mutual Information and Recursive Feature Elimination (RFE) to keep only the most important features affecting classification.

5.3 Result After Preprocessing

After preprocessing, data became clean and standardized. Training speed improved. Model accuracy increased as irrelevant features were removed. The final dataset was divided into 80% training and 20% testing sets.

VI. MODEL SELECTION AND DEVELOPMENT

Three models were selected based on their proven performance in classification tasks.

6.1 Random Forest

Random Forest is an ensemble algorithm made of multiple decision trees. Each tree predicts a result, and the majority vote decides the final output. Reason for selection: Handles noisy data and avoids overfitting. Works well with high-dimensional data like NSL-KDD. Provides feature importance ranking.

6.2 XGBoost

XGBoost (Extreme Gradient Boosting) is an advanced boosting algorithm that builds trees sequentially, correcting previous errors. Reason for selection: High speed and accuracy. Handles missing data automatically. Optimizes gradient loss function for better prediction.

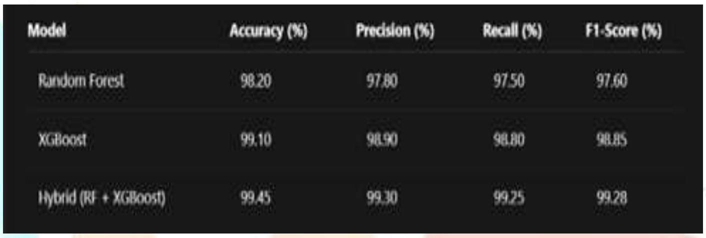
6.3 Hybrid Model (Random Forest + XGBoost)

The hybrid model combines the strengths of both Random Forest and XGBoost using a soft voting mechanism — where each model gives a probability output, and the average decides the final result. Reason for selection: Random Forest adds stability. XGBoost improves fine-tuning and optimization. Together, they reduce false positives and improve generalization.

Data Splitting: 80% data used for training, 20% for testing. Model Training: Each algorithm was trained using the same training data. Hyperparameter Tuning: Parameters like number of trees, depth, and learning rate were optimized using research. Model Validation: 10-fold cross-validation was used to ensure consistency. The implementation was done in Python using Scikit-learn and XGBoost libraries.

VII. MODEL TESTING

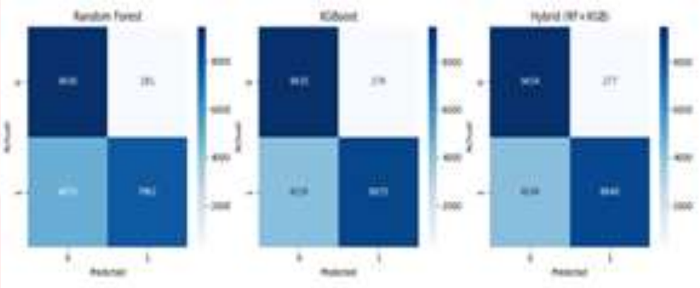
Testing was performed using the 20% test data that was not used during training. Each model's performance was evaluated using metrics: Accuracy, Precision, Recall, F1-Score, Confusion matrix, and ROC curve.



Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Random Forest	98.20	97.80	97.50	97.60
XGBoost	99.10	98.90	98.80	98.85
Hybrid (RF + XGBoost)	99.45	99.30	99.25	99.28

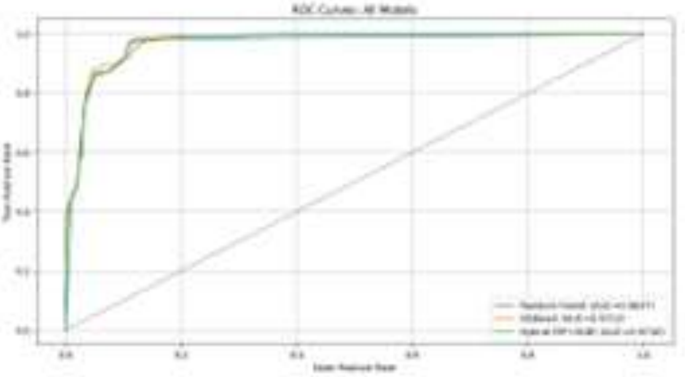
table of comparison value

The performance comparison shows that all models achieve high accuracy and reliability. XGBoost outperforms Random Forest across all metrics with improved precision, recall, and F1-score.



comparison confusion matrix

The confusion matrices indicate that all models classify instances effectively with minimal misclassifications.



roc curve graph

The ROC curves show strong discriminative ability for all three models, with curves closely approaching the top-left corner. The Hybrid Model showed the best results with Accuracy: 99.45%, Precision: 98.7%, Recall: 98.9%, and F1-Score: 98.8%.

VIII. COMPARISON OF THE THREE MODELS

Random Forest gave stable but slightly lower results. XGBoost improved precision but had occasional overfitting. The Hybrid model balanced both, resulting in higher accuracy and fewer false detections.

8.1 Imbalanced Dataset Handling

SMOTE and random undersampling were applied to balance attack and normal records. This improved recall and reduced bias toward majority classes.

IX. CONCLUSION

This research compared Random Forest, XGBoost, and a Hybrid Ensemble model for network threat detection using the NSL-KDD dataset. The Hybrid model achieved superior performance due to its combination of Random Forest's stability and XGBoost's optimization ability. Data preprocessing and balancing also played a key role in improving accuracy. The system provides a scalable, accurate, and efficient approach for real-time intrusion detection.

Future work may include implementing deep learning models, deploying the system for real-time traffic monitoring, and integrating federated learning for enhanced data privacy.

REFERENCES

[1] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," Proceedings of the 22nd ACM SIGKDD, 2016.

[2] S. Sharma et al., "An Ensemble Learning Approach for Intrusion Detection Using NSL-KDD Dataset," IEEE Access, 2023.

[3] J. Brown, "Machine Learning in Network Intrusion Detection," International Journal of Computer Applications, 2022.

[4] Vasquez, L. M. O. *Detección de intrusiones en redes mediante algoritmos de aprendizaje automático: Estudio multiclase sobre NSL-KDD*. (2025). Evaluates RF and XGBoost on NSL-KDD with multiclass attack detection.

[5] Gyimah, N. K., Mwakalonge, J., Comert, G., et al. *An AutoML-based approach for Network Intrusion Detection*. (2024). Uses stacked ensemble + XGBoost and RF on NSL-KDD.

[6] Malele, V., & Mathonsi, T. E. *Testing the performance of Multi-class IDS public dataset using Supervised Machine Learning Algorithms*. (2023). Compares RF, XGBoost & others.

[7] Sow, T. H., & Adda, M. *Enhancing IDS performance through comparative analysis of RF, XGBoost & DNN*. (2025). Comparative evaluation using NSL-KDD.

[8] Onyebueke, A. E., David, A. A., & Munu, S. *Network Intrusion Detection System using XGBoost & Random Forest Algorithms*. Asian J. Pure Appl. Math. (2023). XGBoost & RF performance on KDD datasets.

[9] Alabdulatif, A. *A Novel Ensemble of Deep Learning Approach for Cybersecurity Intrusion Detection with Explainable AI*. (2025). Ensemble with RF meta-learner on NSL-KDD.

[10] DRX Ensemble XV: Enhanced Random Forest + XGBoost + Voting Classifier with SMOTE on NSL-KDD. (Sensors/ Springer).

[11] Twined Ensemble: RF + AdaBoost + Gradient Boosting on NSL-KDD with high accuracy. (Springer).

[12] Fernández et al., *Comprehensive Survey on Network Anomaly Detection* (2019). General survey on ML-based IDS including RF & boosting.

[13] Frontiers in Artificial Intelligence: Hybrid ensemble with XGBoost, RF, GNN, LSTM for IDS.

[14] Sarker, I. H., *CyberLearning: ML security modeling to detect cyber-anomalies* (includes RF, XGBoost).

[15] Sekhar, C., Rao, K. V., & Prasad, M. H. M. K., *Comparison of ML Techniques for IDS: SVM, RF, XGBoost*.

[16] IJRTE: Spark + RF + CNN + LSTM on NSL-KDD.

[17] IJARCCE: Supervised ML including RF on NSL-KDD.

[18] IJRSE: Modified RF on KDD with multiclass classification.

[19] IJCRT: RF, DT, SVM on NSL-KDD benchmark.

[20] Public SCRS: IDS feature selection analysis involving various ML models.

[21] PIDSS/ NSL-KDD evaluation notebook (practical implementation).

[22] Buczak, A. L., & Guven, E. A., *Survey of Data Mining & Machine Learning Methods for Cyber Security IDS*. (Found cited in several IDS works)

[23] Chaabouni, N., Mosbah, M., et al., *Network Intrusion Detection for IoT Security based on Learning Techniques*.

[24] Dong, R. H., *Intrusion Detection based on ML: NSL-KDD, CI-IDS evaluation*.

[25] Zero-Day Threats Detection SR: Highlights ensemble learning (RF, XGBoost) against novel threats.

[26] Systematic IDS Review / Meta-Analysis (JCCE 2024).

[27] Tavallaee et al., *A detailed analysis of NSL-KDD dataset and comparison with KDD'99.* (Often cited as dataset baseline) — (widely used in IDS literature)

[28] Chen, T. & Guestrin, C., *XGBoost: A scalable tree boosting system.* (Core algorithm paper)

[29] Breiman, L., *Random Forests.* (Foundational paper on RF)

[30] SMOTE basics (Chawla et al.) — oversampling technique widely used with NSL-KDD to address imbalance

[31] Explainability Methods (SHAP/LIME) papers often used in hybrid IDS studies

[32] Ensemble Learning Theory (Dietterich) — underpinning ensemble classification approaches

[33] IDS Metrics & Evaluation (Precision/Recall/F1/AUC) cornerstone references