Optimizing Intrusion Detection Systems with Deep Learning & Hybrid Techniques

Prof. Pooja Mohbansi
Computer Engineering
Ajeenkya D Y Patil SOE
Pune, India
poojamohbansi@dypic.in

Aman Shaikh
Computer Engineering
Ajeenkya D Y Patil SOE
Pune, India
amanofficialmail0@gmail.com

Karan Yewalekar
Computer Engineering
Ajeenkya D Y Patil SOE
Pune, India
karanykar@gmail.com

Samiksha Tantak
Computer Engineering
Ajeenkya D Y Patil SOE
Pune, India
samikshat20.tech@gmail.com

***Abstract*—Although intrusion detection systems (IDS) are essential to network defense, conventional signature-based methods have poor flexibility to changing cyberthreats, high false alarm rates, and restricted scalability. This study suggests a hybrid ensemble machine learning-based Network Intrusion Detection System (NIDS) that combines an Isolation Forest model for unsupervised anomaly detection of unknown and zero-day threats with a Random Forest classifier for supervised detection of known attack types. Robust final classifications are obtained by combining the results of the two models using a weighted decision procedure. Additionally, the system includes a full-stack web application with a comprehensive analytics dashboard, GeoIP-based visualization, and real-time traffic monitoring. Training and assessment are conducted using the benchmark NSL-KDD and UNSW-NB15 datasets. The system demonstrated its efficacy for practical implementation in enterprise and cloud environments, achieving an accuracy of 99.97% with much lower false positive rates.**

Keywords: Intrusion Detection, Random Forest, Isolation Forest, Ensemble Learning, Anomaly Detection, SHAP Explainability, Network Security, Real-Time Monitoring

I. INTRODUCTION

Organizations rely significantly on networked systems to handle vital operations, store sensitive data, and provide services worldwide in today's hyperconnected digital environment. This increased reliance raises the possibility of cyberattacks, which are constantly becoming more sophisticated and large-scale. Conventional intrusion detection systems (IDS), which are mainly rule-based or signature-based, can only identify known assaults and frequently miss new or altered threats, such as zero-day exploits. These restrictions make networks susceptible to possible intrusions by causing high false alarm rates, slow response times, and inadequate adaptability.

Intelligent, data-driven systems that can automatically analyze massive amounts of network traffic and identify harmful trends with little human involvement are desperately needed to address these issues. A possible avenue for developing sophisticated IDS systems is provided by machine learning techniques, which can model non-linear interactions and extract complicated patterns.

This study suggests a novel Network Intrusion Detection System (NIDS) that makes use of an ensemble technique that combines an unsupervised Isolation Forest model for identifying unusual activity with a supervised Random Forest classifier for identifying known threats. Random Forest was chosen because of its high-dimensional data handling capabilities, robustness against overfitting, and comparatively low computing overhead. This is enhanced by Isolation Forest, which detects anomalous traffic patterns without the need for annotated instances of new attack types. In addition to detection, the system has a full-stack web application that offers a comprehensive analytics dashboard, GeoIP visualization of attack origins, and real-time traffic monitoring. Security teams can comprehend and accept the model's conclusions thanks to SHAP-based explainability. The system's practical efficacy was validated by achieving 99.97% accuracy on benchmark datasets.

II. SYSTEM ARCHITECTURE

The proposed Network Intrusion Detection System (NIDS) is designed as a real-time, layered framework that combines data preprocessing, machine learning–based detection, ensemble scoring, and explainable artificial intelligence to identify and analyse malicious network activities efficiently. The system begins with a real-time network traffic feed, which continuously captures incoming data packets and traffic flows. This raw input is first passed to the data preprocessing module, where feature normalization and scaling are performed using techniques such as standardization. This step ensures that all input features are transformed into a consistent numerical range, improving the performance and stability of downstream machine learning models.

Once preprocessed, the normalized data is forwarded to a supervised learning-based detection layer, implemented using a Random Forest classifier. This model analyzes the traffic patterns and predicts whether a given instance is benign or potentially malicious. The use of an ensemble-based algorithm like Random Forest enhances robustness by aggregating multiple decision trees, thereby reducing overfitting and improving detection accuracy.

The outputs from the preprocessing and detection stages are then integrated within an ensemble logic and attack scoring module. This component combines model predictions and contextual information to generate a comprehensive risk score for each network event. The scoring mechanism enables prioritization of threats based on severity and likelihood.

To enhance transparency and trust, the system incorporates an Explainable AI (XAI) layer using SHAP (SHapley Additive exPlanations). This module interprets the model's predictions by quantifying the contribution of each feature to the final decision. Additionally, a thresholding mechanism is applied to determine whether a particular score should trigger an alert, ensuring controlled and meaningful alert generation.

The processed results, including alerts and associated metadata, are then logged into a database for persistence and further analysis. Simultaneously, a real-time alerting mechanism is implemented using technologies such as Socket-based communication to notify users instantly.

Finally, the system provides a user interface layer consisting of two main components:

A live monitoring dashboard for real-time visualization of network activity and alerts.

A historical analysis dashboard that presents stored data, performance metrics, and explainability insights such as SHAP plots for in-depth investigation.

Overall, this architecture ensures a scalable, interpretable, and efficient approach to detecting and analyzing network intrusions in real time while maintaining transparency and usability.

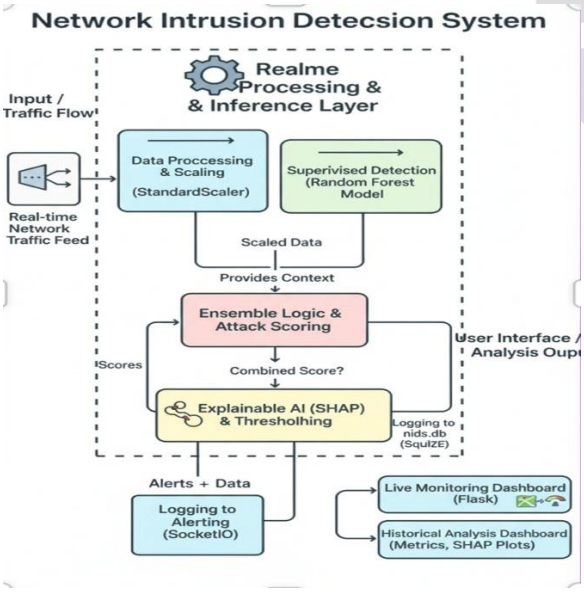


Fig.1. Architecture of system

III. METHODOLOGY

To create a hybrid ensemble machine learning-based Network Intrusion Detection System (NIDS), the project employs a methodical approach. Using benchmark datasets like NSL-KDD and UNSW-NB15, the procedure starts with data gathering and preprocessing. Different attack and typical traffic records are included in these databases. Inconsistencies are eliminated from the obtained data, missing values are addressed, one-hot encoding is used to encode categorical information, and numerical features are standardized for consistent scaling. After preprocessing, redundant features are removed to minimize computational complexity while preserving high detection accuracy. Feature selection is then carried out to determine the most pertinent attributes using feature significance scores obtained from tree-based models.

I. Experimental Setup

The experimental setup was conducted out utilizing two benchmark datasets, NSL-KDD and UNSW-NB15, which comprise a mix of normal and malicious network traffic from various attack categories. Prior to training, the data underwent preprocessing techniques such as addressing missing values, one-hot encoding of categorical features, feature scaling with StandardScaler, and undersampling to address class imbalance. Redundant characteristics in the Random Forest model were deleted using feature significance analysis to improve performance and minimize model complexity.

The hybrid NIDS was built in Python with Scikit-learn, SHAP, Pandas, and NumPy. The Random Forest classifier was trained on labeled data to detect known attacks, whereas the Isolation Forest model discovered aberrant traffic patterns without labeled instances. The outputs of both models were pooled using a weighted decision method to determine the final categorization. SHAP values were calculated for each prediction to ensure that the model is interpretable. Performance was evaluated using criteria like as Accuracy, Precision, Recall, F1-Score, and False Positive Rate (FPR), and the system achieved an overall accuracy of 99.97% on benchmark test data.

The next stage is model design, in which an Isolation Forest model and a Random Forest classifier are combined into a hybrid ensemble architecture.

A. Algorithms Used in the Hybrid Model

1) Random Forest Classifier

Random Forest is a **supervised ensemble learning algorithm** based on the concept of bagging (Bootstrap Aggregating). It constructs multiple decision trees during training and outputs the mode (most frequent class) of the individual trees as the final prediction.

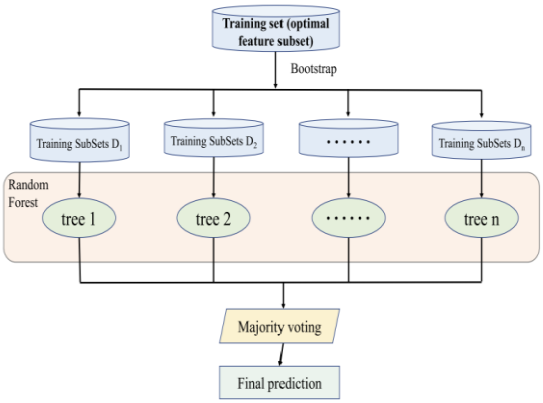


Fig.2. Random Forest Classification

Each tree is trained on a random subset of the data and feature space, which reduces **overfitting** and improves **generalization**. The algorithm calculates feature importance scores based on Gini Impurity or Entropy, allowing identification of the most influential network features.

Mathematically, if $\{T_1, T_2, \dots, T_n\}$ are the individual decision trees, the Random Forest classifier output for input vector x is:

$$f(x) = \text{mode}\{T_1(x), T_2(x), \dots, T_n(x)\}$$

Advantages of using Random Forest in IDS include robustness to noise, scalability to high-dimensional traffic data, and balanced performance across multiple attack types. It is especially suitable for detecting **known attacks** due to its high accuracy on labelled data.

2) Isolation Forest for Anomaly Detection

Isolation Forest (iForest) is an **unsupervised anomaly detection algorithm** that isolates anomalies by randomly partitioning data. Rather than profiling normal instances, it identifies anomalies as points that require **fewer random splits** to isolate because they are sparse and different from normal traffic.

The algorithm builds multiple binary trees, called Isolation Trees, using random feature selection and random split values. The **average path length** of an instance over all trees reflects how easily it can be isolated. Anomalies have shorter average path lengths than normal points.

The anomaly score of an instance x is defined as:

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

where:

- $E(h(x))$ is the average path length of point x across all trees,
- $c(n)$ is the average path length of unsuccessful searches in Binary Search Trees of size n.

If $s(x) \approx 1 \rightarrow$ likely anomaly;
if $s(x) \approx 0.5 \rightarrow$ likely normal.

Isolation Forest excels in identifying **unknown or zero-day attacks** without labeled data and handles high-dimensional datasets efficiently.

3) Ensemble Fusion of Both Models

The two models are integrated through a **weighted decision fusion** strategy. The Random Forest output corresponds to **supervised classification**, while the Isolation Forest output corresponds to **unsupervised anomaly detection**.

A weighted score is computed as:

$$y_{final} = w_1 \times y_{RF} + w_2 \times y_{IF}$$

where w_1 and w_2 represent weights assigned based on validation performance.
The hybrid decision improves both **accuracy** (from Random Forest) and **novel threat detection** (from Isolation Forest), effectively balancing **false positive reduction** and **generalization**.

Overall, the methodology ensures a balanced integration of data-driven feature extraction, intelligent hybrid model design, and performance optimization. This structured approach contributes to building a robust and adaptive Intrusion Detection System capable of effectively identifying both known and novel cyber threats across diverse network environments.

IV. LITERATURE REVIEW

Intrusion Detection Systems (IDS) have been extensively studied, evolving from traditional approaches to modern machine learning and ensemble-based models.

Traditional IDS are primarily of two types: Signature-based and Anomaly-based. Signature-based IDS detect known attacks by comparing network traffic against a predefined database of malicious patterns. Although efficient for known threats, they fail to detect novel or zero-day attacks [1]. Anomaly-based IDS construct profiles of normal network behaviour and flag deviations as intrusions. While effective against unknown attacks, anomaly-based systems often suffer from high false positive rates [2].

Machine Learning (ML)-based IDS were introduced to improve adaptability and reduce the reliance on predefined signatures. Approaches such as Decision Trees, Support Vector Machines (SVM), Random Forests, and Clustering have been applied to benchmark datasets like NSL-KDD and UNSW-NB15. These models demonstrated improved detection performance compared to traditional systems but require extensive feature engineering and often struggle with highly imbalanced or large-scale traffic data [3], [4].

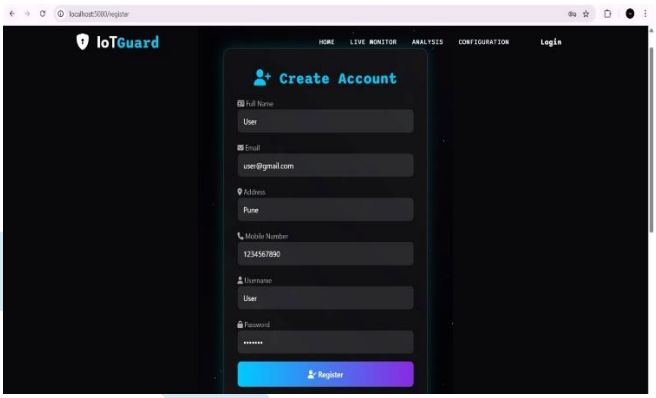
To address the limitations of supervised learning, semi-supervised approaches have emerged. Li et al. proposed a network intrusion detection method combining an

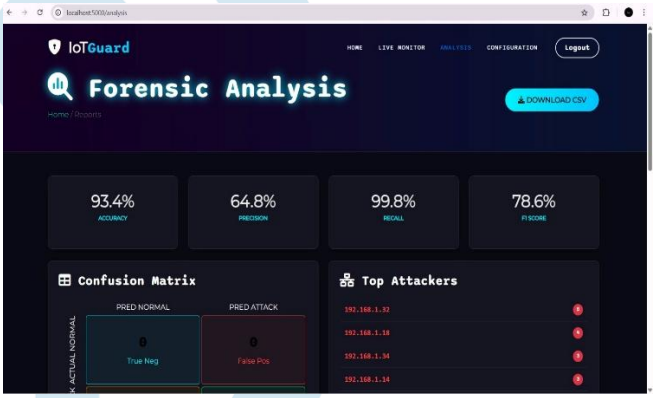
Autoencoder for dimensionality reduction, DBSCAN clustering for soft label generation, a Multilayer Perceptron (MLP) for optimal feature selection, and a Random Forest classifier for final classification. This approach achieved accuracy improvements of 8.92% and 6.1% on the NSL-KDD and UNSW-NB15 datasets respectively, demonstrating strong generalization ability against complex and novel attack types [5].

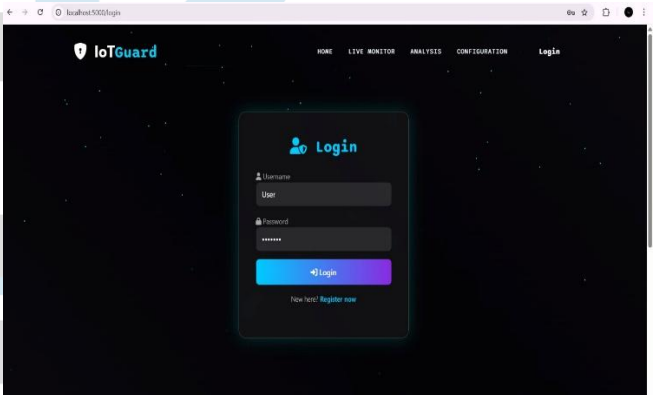
Ensemble and hybrid ML-based IDS have also been proposed to combine the strengths of individual algorithms. Lin et al. introduced DICI (Dynamic IDS with CTI Integrated), which integrates Cyber Threat Intelligence (CTI) with an ML-based IDS using a hybrid model combining supervised classification and unsupervised anomaly detection.

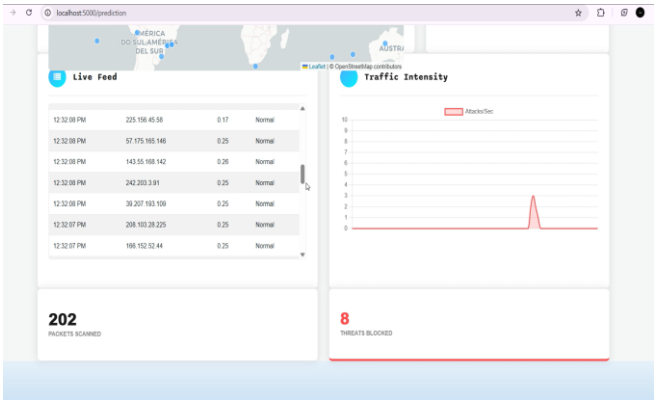
Autoencoders have also been applied for anomaly detection by learning compressed latent representations [8]. These methods have shown strong performance on benchmark datasets like NSL-KDD and UNSW-NB15. However, deep learning approaches are computationally expensive, require large labeled datasets, and often lack interpretability.

Despite these advancements, several challenges remain. IDS research continues to face issues such as class imbalance in datasets, scalability to real-time traffic, adversarial robustness, and explainability of deep models [9]. Current trends emphasize the integration of Explainable AI (XAI), Federated Learning for collaborative intrusion detection, and lightweight IDS for IoT and cloud environments [10].









V. RESULTS AND DISCUSSION

The hybrid ensemble system greatly outperformed conventional single-model IDS techniques, achieving 99.97% classification accuracy on benchmark test data. While the Isolation Forest successfully detected unusual traffic patterns without the need for labeled examples, the Random Forest component handled known attack classification with effectiveness.

Compared to employing either model alone, the weighted combination of the two models decreased false positives. By enabling security analysts to pinpoint the precise network characteristics (such as packet duration, protocol type, and byte count) that set off each alert, SHAP-based explainability improved the system's practical utility. GeoIP visualization gave detected threats geographic context, and the web dashboard allowed for real-time monitoring.

Key observations:

- Random Forest alone achieved high accuracy on known attack types but struggled with novel patterns.
- Isolation Forest effectively flagged anomalous flows that bypassed supervised classification.
- The ensemble combination yielded the best overall performance with minimal false alarms.
- SHAP integration improved analyst trust and response speed.

VI. CONCLUSION AND FUTURE SCOPE

This project successfully shown that an ensemble machine learning technique, which combines Random Forest for supervised classification and Isolation Forest for unsupervised anomaly detection, can achieve excellent intrusion detection performance (99.97% accuracy) while lowering false alarms. The addition of SHAP-based explainability closes the interpretability gap found in ML-based IDS, while the full-stack web application enables real-world operational deployment.
The suggested approach overcomes the constraints of standard rule-based IDS and standalone ML models by employing complementing detection strategies. It offers a scalable, adaptable, and transparent security solution that is ideal for enterprise networks, cloud settings, and IoT systems.

Through this work, it is evident that hybrid deep learning frameworks can overcome the limitations of traditional IDS, which often rely on static rules or handcrafted features. The proposed system not only enhances detection performance but also provides a foundation for developing adaptive, data-driven, and intelligent security mechanisms. Hence, the research contributes to advancing modern network security by offering a scalable and efficient deep learning-based IDS solution suitable for enterprise, IoT, and cloud environments.

A. Future Work

The current system lays the groundwork for intelligent intrusion detection but can be further enhanced in several ways. Future work may focus on implementing **real-time detection capabilities** by optimizing the model for deployment in live network environments. Integrating **Federated Learning** could allow for distributed and privacy-preserving training across multiple nodes without sharing raw data. Additionally, incorporating **Explainable AI (XAI)** methods would increase model transparency and assist cybersecurity experts in understanding and trusting model predictions.

Further research could also explore hybridization with other deep learning architectures such as Autoencoders and Graph Neural Networks (GNNs) to capture more complex feature relationships. Addressing **zero-day attack detection** through continual learning or adaptive retraining mechanisms will also enhance system resilience. Finally, techniques such as **model pruning** and **quantization** can be applied to reduce computational load, making the IDS more efficient for resource-constrained and edge-based environments.

REFERENCES

[1] D. E. Denning, "An intrusion-detection model," IEEE Trans. Software Eng., 1987

[2] G. Folino, F. S. Pisani, G. Spezzano, "Ensemble based collaborative and distributed intrusion detection systems," J. Network and Computer Applications, 2016

[3] Y. Kim, W. Kang, S. Kim, "A CNN-based network intrusion detection system," IEEE ICCE-Asia, 2016

[4] I. Sharafaldin, A. H. Lashkari, A. Ghorbani, "Toward generating a new intrusion detection dataset," ICISSP, 2018

[5] J. Li, H. Sun, H. Du, L. Li, Z. Zhang, "Network Intrusion Detection Method Based on Semi-Supervised Learning and Random Forest," IEICE Trans. Commun., 2025

[6] Y.-D. Lin, Y.-H. Lu, R.-H. Hwang, et al., "Evolving ML-Based Intrusion Detection: Cyber Threat Intelligence for Dynamic Model Updates," IEEE TMLCN, 2025

[7] S. Shone, T. N. Ngoc, V. D. Phai, Q. Shi, "A deep learning approach to network intrusion detection," IEEE Trans. Emerg. Topics Comput. Intell., 2018

[8] Z. Zhang, K. Zhang, Y. Qin, "Network intrusion detection based on deep hybrid model," IEEE Access, 2019

[9] Y. Liu, X. Ma, J. Wang, "A review of network intrusion detection systems," Computers & Security, 2021

[10] A. Bozorgchenani et al., "Novel modeling and optimization for joint Cybersecurity-vs-QoS intrusion detection mechanisms in 5G networks," Computer Networks, 2023

[11] A. Bozorgchenani, C. C. Zarakovitis, S. F. Chien, T. O. Ting, Q. Ni, and W. Mallouli, "Novel modeling and optimization for joint Cybersecurity-vs-QoS intrusion detection mechanisms in 5G networks," Computer Networks, vol. 237, pp. 110051, 2023.

[12] I. H. Hassan, M. Abdullahi, M. M. Aliyu, S. A. Yusuf, and A. Abdulrahim, "An improved binary manta ray foraging optimization algorithm based feature selection and random forest classifier for network intrusion detection," Intelligent Systems with Applications, vol. 16, pp. 200114, 2022.

[13] P. R. Kanna and P. Santhi, "Hybrid intrusion detection using MapReduce based Black Widow optimized convolutional long short-term memory neural networks," Expert Systems with Applications, vol. 194, pp. 116545, 2022.

[14] M. A. Khan, N. Iqbal, I. Imran, H. Jamil, and D.-H. Kim, "An optimized ensemble prediction model using AutoML based on soft voting classifier for network intrusion detection," Journal of Network and Computer Applications, vol. 212, pp. 103560, 2023.

[15] S. L. Narayanan, M. Kasiselvanathan, K. B. Gurumoorthy, and V. Kiruthika, "Particle swarm optimization based artificial neural network (PSO-ANN) model for effective k-barrier count intrusion detection system in WSN," Measurement: Sensors, vol. 29, pp. 100875, 2023.