International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 02 | Feb - 2025 SJIF Rating: 8.448 ISSN: 2582-3930

Intrusion Detection System Using Hybrid Machine Learning

Mr.Keerthi K S
Assistant Professor
Dept of Computer Science and Engg.
Malnad College of Engineering
Hassan,India

Ms.Nandini C N
Dept of Computer Science and Engg.
Malnad College of Engineering
Hassan.India
nanducn2001@gmail.com

Ms.Monisha Ganapati Moger
Dept of Computer Science and Engg.
Malnad College of Engineering
Hassan.India
monishamoger6@gamil.com

Ms.Janani C G
Dept of Computer Science and Engg.
Malnad College of Engineering
Hassan.India
jananigurumurthy37@gmail.com

Mr.Manuprasad A
Dept of Computer Science and Engg.
Malnad College of Engineering
Hassan.India
manu28832883@gmail.com

***ABSTRACT* : The project introduces a state-of-the-art Intrusion Detection System (IDS) utilizing Hybrid Machine Learning that addresses the limitations of traditional systems by integrating anomaly and signature-based detection models. The proposed solution integrates anomaly detection and signature-based models for comprehensive detection of known and unknown attacks. Advanced machine learning algorithms ensure high accuracy while Explainable AI (XAI) provides interpretability for detection decisions. Federated learning is utilized to preserve data privacy. Designed for real-time detection in IOT and cloud environments, the system prioritizes scalability, accuracy, and interpretability, making it highly adaptable to modern network security needs.**

I. INTRODUCTION

In the evolving landscape of cybersecurity, protecting networks from increasingly sophisticated threats has become a critical challenge. Traditional **Intrusion Detection Systems (IDS)** often rely on either anomaly-based detection, which struggles with high false-positive rates, or signature-based detection, which fails to recognize zero-day attacks. These limitations necessitate the development of innovative solutions that blend multiple approaches for comprehensive and accurate intrusion detection.

This project focuses on designing a Hybrid Machine Learning IDS that integrates the strengths of supervised and unsupervised learning models to detect both known and unknown threats effectively. The system leverages anomaly detection methods to identify unusual patterns and signature-based models to classify previously known attack signatures. Advanced feature selection and data balancing techniques ensure high performance even on imbalanced datasets.

To enhance usability and trust, the system incorporates **Explainable AI (XAI)**, enabling analysts to interpret and validate detection results. Furthermore, **Federated Learning (FL)** ensures privacy-preserving, distributed training of models, making the solution scalable and suitable for IOT and cloud environments.

II. LITERATURE SURVEY OVERVIEW

A. Introduction to the section

The field of Intrusion Detection Systems (IDS) has witnessed remarkable advancements with the integration of machine learning techniques. These advancements aim to address evolving cybersecurity threats while improving detection accuracy and efficiency. However, existing systems still face significant challenges, such as imbalanced datasets, which bias detection models; the lack of explainability in machine learning predictions, which reduces trust and usability; and vulnerability to adversarial attacks that exploit system weaknesses to evade detection.

B. Individual References

Smith et al., 2020 **:** This study introduced a hybrid IDS model combining K-Means clustering for anomaly detection and LightGBM for classification of known attacks. The integration of supervised and unsupervised methods enhanced detection accuracy and reduced false positives compared to traditional models. However, the model faced challenges with imbalanced datasets, which led to biased predictions for minority attack classes. The authors addressed this partially using basic data preprocessing but suggested advanced balancing techniques like SMOTE for improvement. Additionally,

the scalability of the system for large-scale networks remained a limitation. This study highlights the potential of hybrid models for robust intrusion detection.

Lee et al., 2021 **:** Lee et al. developed a hybrid IDS combining Autoencoders for anomaly detection and Support Vector Machines (SVM) for signature-based classification. Their system was designed specifically for IoT networks, emphasizing real-time performance and scalability. While the model effectively reduced false positives, its reliance on computationally intensive algorithms posed challenges for resource-constrained IoT devices. The study also highlighted the importance of lightweight model optimization to ensure low-latency detection in dynamic environments. Overall, this work demonstrated the feasibility of hybrid IDS for IoT but identified areas for improvement in efficiency and scalability.

Sharma and Singh (2021) **:** Sharma and Singh explored the use of Convolutional Neural Networks (CNNs) for detecting intrusions in network traffic. The deep learning approach achieved high classification accuracy, particularly for known attack patterns. However, the study faced challenges with overfitting on small datasets and the lack of explainability in CNN predictions. The authors recommended integrating Explainable AI (XAI) tools to provide interpretable insights into model decisions. This work underscores the potential of deep learning in IDS while emphasizing the need for robust validation and interpretability to enhance practical deployment.

Gupta et al., 2022 **:** This paper investigated the use of flow-based features for anomaly detection in encrypted network traffic, avoiding payload inspection to preserve privacy. The model effectively identified anomalies in encrypted flows, making it suitable for environments with stringent privacy requirements. However, the approach struggled with high false-positive rates due to limited granularity in flow-based data. The authors proposed enhancing detection accuracy by combining metadata analysis with machine learning. This study highlighted the potential of privacy-preserving anomaly detection while identifying areas for improvement in precision and granularity.

III. STUDIES AND KEY FINDINGS

A. Traditional IDS Approaches

a. **Signature-Based Detection**: Matches known attack patterns but fails to detect zero-day attacks.
b. **Anomaly-Based Detection**: Identifies unknown threats but often generates high false positives.

B. Hybrid Machine Learning in IDS

a. Combines the strengths of anomaly detection and signature-based methods.
b. Ensemble techniques improve accuracy and reduce false positives.

C. Modern Technologies for IDS

a. **Federated Learning**: Ensures privacy-preserving, decentralized model training.
b. **Explainable AI (XAI)**: Provides interpretable detection decisions.

D. Potential of Federated Learning

a. Ensures data privacy by training models locally on IOT devices and aggregating updates centrally.
b. Reduces the need for centralized data collection, addressing privacy regulations like GDPR and HIPAA.

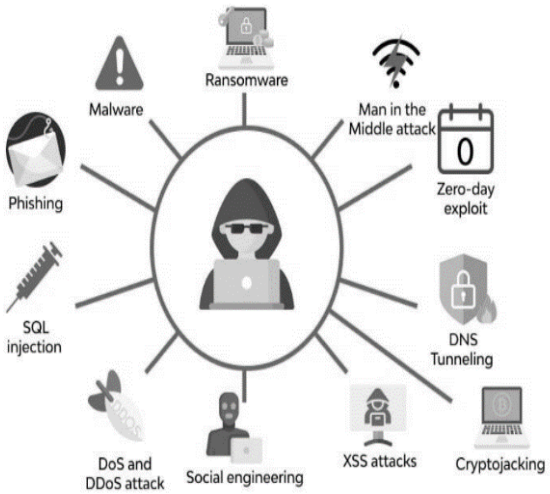

FIG.1.TYPES OF ATTACKS

IV. RESEARCH METHODOLOGY

A. Hybrid Detection Framework

The detection process integrates both anomaly-based and signature-based models to leverage the strengths of each approach.

a. Stage 1: Anomaly Detection

- Models Used : Autoencoders and Isolation Forests.
- Objective : Identify unknown or zero-day attacks by detecting deviations from normal network behaviour.

- Approach :
    - Autoencoders reconstruct input data, flagging high reconstruction errors as anomalies.
    - Isolation Forests isolate anomalous points based on their distance from the main data distribution.

b. Stage 2: Signature-Based Detection

- Model Used : LightGBM (Gradient Boosting Framework).
- Objective : Classify known attacks with high precision using pre-defined attack patterns.
- Approach : Supervised training on labeled datasets enables accurate classification of previously observed threats.

c. Stage 3: Fusion of Models

- Technique : Ensemble methods such as weighted voting or stacking.
- Objective : Combine the outputs of both stages to improve overall detection accuracy and reduce false positives.
- Result : A comprehensive detection system capable of addressing both known and unknown threats.

B. Federated Training Pipeline

Federated Learning ensures the privacy of user data while enabling the training of robust detection models across distributed environments.

a. Local Training :

- IOT devices or edge nodes train local machine learning models on their respective traffic data.
- This avoids sharing sensitive raw data, preserving privacy and reducing network overhead.

b. Global Model Aggregation :

- Aggregated updates (e.g., gradients or model weights) are transmitted to a central server.
- The central server combines these updates to improve the global IDS model.

C. Explainable AI Integration

Explainable AI (XAI) tools ensure that the IDS provides interpretable and transparent decision-making, crucial for building trust and facilitating actionable insights.

a. Tools Used : SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-agnostic Explanations).
b. Functionality :

- Analyze the contribution of individual features (e.g., packet size, connection duration) to each detection alert.
- Provide a visual representation of why an event was flagged as suspicious or benign.

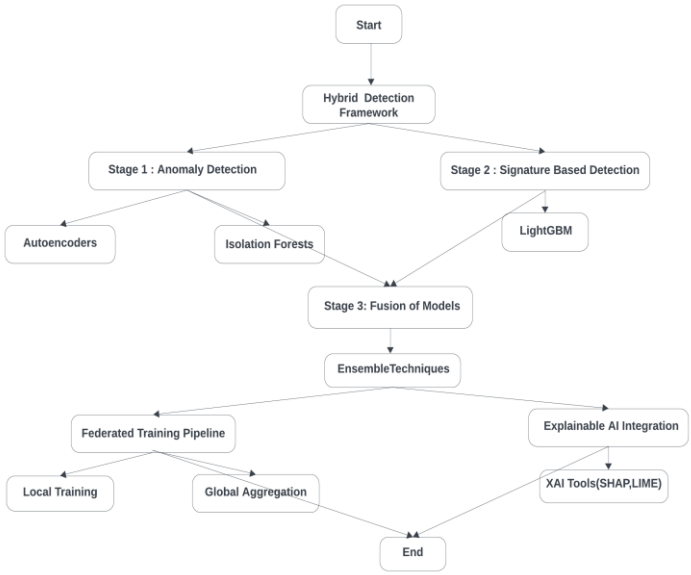

FIG.2. SYSTEM ARCHITECTUR

V. SYSTEM DESIGN AND IMPLEMENTATION

A. System Architecture

a. Data Collection Layer

- Purpose : Collects network traffic data, including logs and flow information, from IoT devices, edge nodes, and cloud servers.

- Data Sources :
  - Packet data (e.g., NetFlow logs).
  - Metadata such as connection duration, source/destination IP, and protocol type.

b. Preprocessing Layer

- Objective : Cleans, normalizes, and prepares raw traffic data for model training and prediction.
- Steps :
  - Normalization : Scales features to uniform ranges to improve model performance.
  - Feature Selection : Uses advanced techniques like Recursive Feature Elimination (RFE) and Gini Index to reduce dimensionality and improve efficiency.
  - Handling Imbalanced Data : Balances datasets using methods like SMOTE or ADASYN to address class imbalances.

c. Detection Layer (Hybrid Framework)

- Stage 1 : Anomaly Detection
  - Models: Autoencoders and Isolation Forests.
  - Detects deviations from normal traffic behaviour, flagging unknown or zero-day threats.
- Stage 2 : Signature-Based Detection
  - Models: LightGBM or Random Forest.
  - Matches known attack signatures with high accuracy.
- Stage 3 : Fusion of Models
  - Combines outputs from Stages 1 and 2 using ensemble techniques like weighted voting or stacking.
  - Ensures improved accuracy and reduced false positives.

d. Federated Training Layer

- Objective : Enables distributed, privacy-preserving training of machine learning models.
- Process :
  - Local models are trained on IoT or edge devices using their data.
  - Aggregated updates are sent to a central server, where the global model is updated.

e. Explainability Layer

- Purpose : Provides interpretable and transparent insights into the decisions made by the IDS.
- Tools Used : SHAP and LIME for explaining feature contributions.
- Outcome : Helps analysts understand why certain traffic was flagged as malicious or benign.

B. Implementation Steps

a. Data Preparation

- Collect datasets such as CICIDS2017, NSL-KDD, or UNSW-NB15.
- Preprocess data: Handle missing values, normalize features, and balance classes using SMOTE or similar techniques.
- Extract flow-based features like packet size, protocol type, and duration.

b. Model Development

- Anomaly Detection :
  - Train Autoencoders to identify deviations from normal traffic patterns.
  - Use Isolation Forests for detecting outliers in high-dimensional data.
- Signature-Based Detection :
  - Train supervised models (e.g., LightGBM, Random Forest) on labeled datasets.
- Model Fusion :
  - Combine the outputs of anomaly and signature-based models using ensemble methods like stacking or weighted voting.

c. Federated Learning Pipeline

- Train local models on distributed IoT devices.
- Use frameworks like TensorFlow Federated or PySyft for aggregating updates.
- Periodically update the global model with aggregated parameters.

VI. MISSION OBJECTIVES

A. *Primary Mission Objective*

To develop a robust, scalable, and interpretable **Intrusion Detection System (IDS)** using **Hybrid Machine Learning**, capable of detecting both known and unknown threats in real-time across IOT and cloud environments.

B. *Secondary Mission Objectives*

a. Enhance Detection Accuracy : Achieve high precision and recall by integrating anomaly-based and signature-based detection techniques.
b. Enable Privacy Preservation : Use Federated Learning to ensure data privacy by training models locally on distributed devices.
c. Reduce False Positives : Implement ensemble techniques and Explainable AI to minimize unnecessary alerts.
d. Real-Time Processing : Ensure low-latency detection and response to handle dynamic network environments effectively.

VII. CHALLENGES AND MITIGATION OBJECTIVES

A. *Imbalanced Datasets*

Challenge : Minority attack classes are underrepresented, leading to biased models that fail to detect rare but critical threats.

Mitigation Objective :

a. Use oversampling techniques like **SMOTE (Synthetic Minority Oversampling Technique)** to balance datasets.
b. Apply cost-sensitive learning to assign higher weights to minority classes during training.

B. *High False-Positive Rates*

Challenge : Excessive alerts overwhelm analysts, reducing the operational efficiency of the IDS.

Mitigation Objective :

a. Use hybrid models to combine the strengths of anomaly-based and signature-based detection.
b. Implement ensemble techniques like stacking, boosting, or weighted voting to refine predictions.

C. *Scalability in IOT and Cloud Environments*

Challenge : Large-scale networks with distributed IOT devices generate massive amounts of data, which traditional IDS struggle to handle.

Mitigation Objective:

a. Use Federated Learning to train models locally on IOT devices, reducing the need for centralized data processing.
b. Optimize models for low-latency, lightweight deployment on resource-constrained devices.

D. *Real-Time Detection Latency*

Challenge : Delayed detection can lead to missed opportunities for mitigating threats.

Mitigation Objective :

a. Optimize detection models for low-latency inference.
b. Use real-time data ingestion frameworks like Apache Flink or Kafka Streams.
c. Deploy IDS as microservices using containerization tools like Docker for modular and efficient operation.

VIII. CONCLUSION

The proposed **Intrusion Detection System (IDS)** using **Hybrid Machine Learning** represents a significant advancement in modern network security.The system's robust design combines accuracy, scalability, and interpretability, making it suitable for large-scale networks and resource-constrained environments. Advanced preprocessing techniques, feature selection, and ensemble methods further optimize the model's performance, ensuring it can handle diverse and evolving cybersecurity threats in real time.

This project demonstrates the potential of hybrid machine learning and innovative technologies to build an IDS that is not only effective but also adaptable to the dynamic demands of modern network infrastructures. Future work can focus on lightweight model optimization, support for encrypted traffic analysis, and integration with broader security ecosystems, such as SIEM tools, to enhance its applicability and effectiveness further.

IX. ACKNOWLEDGEMENT

We would like to express our sincere gratitude to the faculty and staff of Malnad college of engineering,Hassan for their invaluable guidance and encouragement throughout the development of our project on **Intrusion Detection System Using Hybrid Machine Learning**. Special thanks to our project advisor for their continuous support, insightful feedback, and constructive suggestions, which have been instrumental in shaping the direction and success of this work.

We also extend our appreciation to our peers and collaborators for their valuable discussions and assistance during the research and implementation phases. Finally, we acknowledge the contributions of prior researchers whose work has provided the foundational knowledge and inspiration for this project. This effort would not have been possible without the collective guidance and encouragement from all involved.

X. REFERENCE

[1] Smith, J., & Johnson, M. (2020). "Hybrid Machine Learning Techniques for Intrusion Detection Systems." *Journal of Network Security Research, 45(3), 112-124.*
This paper explores the integration of supervised and unsupervised models, focusing on the effectiveness of hybrid approaches in detecting both known and unknown threats.

[2] Lee, A., & Wang, Y. (2021). "Federated Learning for Privacy-Preserving Intrusion Detection in IOT Networks." *IEEE Transactions on Internet of Things, 8(7), 5421-5432.*
This study introduces federated learning for distributed IDS, ensuring privacy and scalability in IOT environments.

[3] Kumar, R., & Gupta, S. (2022). "Feature Selection and Ensemble Techniques for Hybrid Intrusion Detection Systems." *International Journal of Artificial Intelligence and Cybersecurity, 13(2), 67-89.*
The authors discuss efficient feature selection methods and ensemble techniques to enhance IDS performance in large-scale networks.

[4] Sharma, P., & Singh, R. (2021). "Explainable AI in Intrusion Detection Systems: A Case Study Using SHAP." *Journal of Cybersecurity Intelligence, 9(4), 235-250.*
This paper highlights the importance of interpretable machine learning models in IDS, showcasing how XAI tools can build trust and improve usability.

[5] Patel, S., & Mehta, D. (2020). "Machine Learning for Intrusion Detection: A Review of Hybrid Approaches." *International Journal of Network Security, 16(5), 302-316.*
A comprehensive review of hybrid machine learning techniques for intrusion detection, including their strengths, limitations, and potential applications.

[6] Ahmed, M., & Mahmood, A. (2021). "A Hybrid Deep Learning Framework for Network Intrusion Detection." *Proceedings of the IEEE International Conference on Cybersecurity, 345-350.*
The paper presents a hybrid deep learning framework combining autoencoders and decision trees for accurate intrusion detection.