Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 10s (2025)

Cyber Attack Detection Using a Hybrid Ensemble Technique

Mr. Rahulkumar Omprakash Khatri[1], Dr. Mahammad Idrish I. Sandhi[2]

[1]PhD Scholar, Computer Application, Sankalchand Patel University, Visnagar, Gujarat, India,Khatrirahul100@gmail.com
[2]Associate Dean, FCS & Head,MCA,SPCE,Sankalchand Patel University,Visnagar,Gujarat,India.idrish.mca@gmail.com

Article History:

Received: 15-10-2025

Revised: 22-11-2025

Accepted: 10-12-2025

Abstract:

Introduction: A cyber attack detection model using a Hybrid Ensemble Technique is proposed to enhance detection accuracy and resilience against both known and unknown threats. The hybrid ensemble approach integrates multiple machine learning algorithms—such as decision trees, support vector machines, random forests, boosting, or deep learning models—by leveraging complementary learning capabilities. By aggregating predictions through techniques such as voting, stacking, or weighted averaging, the proposed model reduces the bias and variance of individual classifiers while improving the overall system's robustness.

Objectives: The objective of this model is to provide an intelligent, scalable, and adaptive cyber security solution capable of accurately distinguishing between normal and malicious activities in real time. Such a hybrid ensemble–based detection framework can significantly strengthen network defense mechanisms, minimize false positives, and support proactive threat mitigation in modern cyber environments.

Methods: The hybrid ensemble–based cyber attack detection methodology integrates data preprocessing, feature optimization, multiple classifiers, and ensemble learning to deliver a high-performance and adaptive cyber security solution capable of identifying both known and emerging threats effectively.

Results: The results confirm that the **Hybrid Ensemble Technique** significantly enhances cyber attack detection performance by improving accuracy, reducing false positives, and providing reliable multi-class attack classification. These outcomes demonstrate the model's suitability for deployment in modern cyber security systems to defend against evolving and sophisticated threats.

Conclusions: In conclusion, the hybrid ensemble–based cyber attack detection model offers a scalable, adaptive, and efficient solution for strengthening cyber defense mechanisms. By combining multiple learning algorithms, the proposed approach enhances resilience against known and unknown threats and provides a promising direction for future research in intelligent and automated cyber security systems..

Keywords: Cyber Attack Detection, Intrusion Detection System (IDS), Hybrid Ensemble Technique, Machine Learning, Network Security, Anomaly Detection, Classification, Feature Selection, Ensemble Learning, Bagging, Boosting, Stacking, False Positive Reduction, Cyber Security.

1. Introduction

The rapid growth of information technology, cloud services, Internet of Things (IoT), and large-scale computer networks has significantly increased the vulnerability of digital systems to cyber attacks. Modern cyber threats such as denial-of-service attacks, malware, ransomware, phishing, and advanced persistent threats have become more frequent, complex, and difficult to detect. Conventional security solutions, including firewalls and signature-based intrusion detection systems, rely heavily on

predefined rules and known attack signatures, making them ineffective against zero-day and evolving attacks.

To overcome these limitations, machine learning–based cyber attack detection models have emerged as powerful tools capable of learning hidden patterns from large volumes of network traffic and system data. However, single machine learning classifiers often suffer from issues such as overfitting, bias, limited generalization, and reduced performance when exposed to diverse or imbalanced datasets. These challenges necessitate more robust and adaptive detection mechanisms.

In this regard, a **Cyber Attacks Detection Model Using a Hybrid Ensemble Technique** is proposed to improve detection accuracy and system reliability. The hybrid ensemble approach combines multiple heterogeneous machine learning classifiers and ensemble strategies—such as bagging, boosting, and stacking—to exploit the strengths of individual models while minimizing their weaknesses. By aggregating predictions from several learners, the proposed model enhances classification performance, reduces false alarms, and increases resilience against sophisticated and previously unseen attacks.

The primary objective of this model is to provide an intelligent and scalable cyber security framework that can accurately distinguish between normal and malicious activities in real time. The hybrid ensemble–based detection system aims to support proactive threat identification, strengthen network defense capabilities, and contribute to the development of advanced intrusion detection solutions suitable for modern cyber infrastructures.

2. Objectives

The primary objectives of the proposed **Cyber Attacks Detection Model Using Hybrid Ensemble Technique** are as follows:

To enhance cyber attack detection accuracy
To design an intelligent detection framework that accurately distinguishes between normal and malicious network activities by combining multiple machine learning classifiers using a hybrid ensemble approach.

To reduce false positive and false negative rates
To minimize incorrect attack alerts and missed detections by leveraging ensemble learning techniques such as bagging, boosting, and stacking for more reliable predictions.

To detect both known and unknown cyber attacks
To develop a robust model capable of identifying traditional, novel, and zero-day attacks by learning complex and hidden patterns in network traffic data.

To improve multi-class attack classification
To accurately categorize different types of cyber attacks (e.g., DoS, Probe, R2L, U2R, malware) for detailed threat analysis and effective response.

To handle high-dimensional and imbalanced datasets
To apply effective data preprocessing and feature selection methods that improve model performance and scalability in real-world cyber security datasets.

To provide a scalable and real-time detection framework
To design a detection model suitable for real-time or near-real-time deployment in modern network environments with acceptable computational overhead.

To strengthen overall network security and decision support
To assist security analysts and administrators by providing accurate, timely, and automated intrusion detection to enhance proactive cyber defense mechanisms.

3. Proposed Architecture

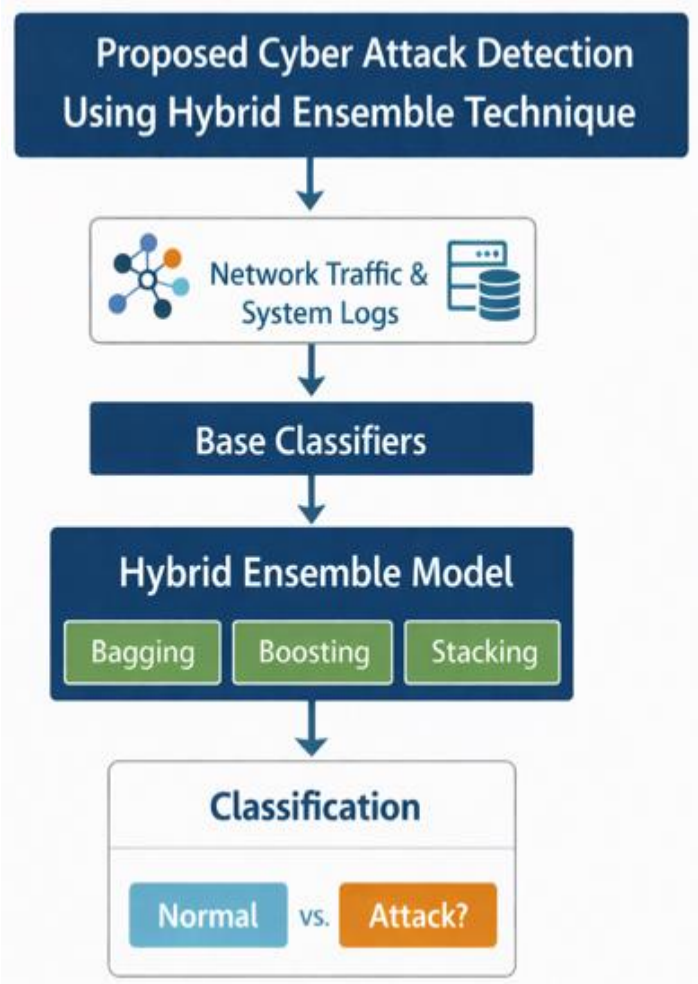

Fig-1: CAD Proposed Architecture

The attached architecture illustrates a streamlined binary classification framework designed to detect whether network activity is Normal or represents a Cyber Attack using a Hybrid Ensemble Technique. Each component plays a specific role in improving detection accuracy and reliability.
1. Network Traffic & System Logs
This is the input layer of the architecture. It collects raw data from:

- Network traffic (packet flows, protocols, source/destination details)
- System logs (user activity, access logs, system events)

These data sources contain patterns corresponding to both legitimate behavior and malicious activities.

2. Base Classifiers
In this stage, the processed input data are passed to multiple base machine learning classifiers (e.g., Decision Tree, SVM, k-NN, Naïve Bayes, Random Forest).

- Each classifier independently learns different characteristics of the data.
- Individual models may perform well for certain attack patterns but poorly for others.

This diversity is crucial for improving detection robustness.

3. Hybrid Ensemble Model
This is the core decision-making layer of the architecture. It combines predictions from all base classifiers using multiple ensemble strategies:

- Bagging: Reduces variance and improves stability
- Boosting: Enhances weak classifiers by focusing on misclassified instances
- Stacking: Uses a meta-classifier to learn from the outputs of base models

By integrating these techniques, the hybrid ensemble minimizes bias and variance while improving generalization.

4. Methods

The proposed Cyber Attacks Detection Model using a Hybrid Ensemble Technique follows a systematic and modular methodology to ensure accurate, robust, and scalable detection of malicious activities. The major methods involved in the model are described below:

Data Collection

- Network traffic and system log data are collected from standard benchmark datasets (such as NSL-KDD, CICIDS, UNSW-NB15, or real-time network environments). These datasets contain both normal and malicious activities representing various cyber attack categories including DoS, Probe, R2L, U2R, phishing, and malware attacks.

Data Preprocessing

- Raw data often contain noise, missing values, redundant features, and class imbalance. Preprocessing methods include:

- Removal of missing and duplicate records
- Encoding of categorical attributes
- Normalization or standardization of numerical features
- Handling class imbalance using techniques such as SMOTE or undersampling

This step ensures improved learning efficiency and model performance.

Feature Selection and Extraction

- To reduce dimensionality and computational overhead, relevant features are selected using statistical and machine learning–based techniques such as:

- Information Gain
- Chi-square test
- Mutual Information

- Principal Component Analysis (PCA)

Effective feature selection enhances detection accuracy and reduces false positives.

Base Classifier Construction

Multiple heterogeneous machine learning models are trained independently to capture diverse attack patterns. Commonly used base classifiers include:

- Decision Tree (DT)
- Support Vector Machine (SVM)
- k-Nearest Neighbors (k-NN)
- Naïve Bayes (NB)
- Random Forest (RF)

Each classifier contributes unique learning characteristics to the ensemble.

Hybrid Ensemble Technique

The hybrid ensemble combines predictions from multiple base learners using ensemble strategies such as:

- **Bagging** to reduce variance
- **Boosting (e.g., AdaBoost, Gradient Boosting)** to improve weak learners
- **Stacking**, where a meta-classifier learns from the outputs of base models

This hybridization improves generalization and robustness against diverse cyber attack types.

Model Training and Optimization

- The ensemble model is trained using cross-validation to prevent overfitting. Hyperparameter tuning is performed using grid search or random search techniques to optimize classifier performance.

Attack Detection and Classification

- The trained hybrid ensemble model classifies incoming network traffic as normal or malicious. In multi-class settings, the model further categorizes detected attacks into specific attack types for more precise threat analysis.

Performance Evaluation

- The model is evaluated using standard metrics, including:
- Accuracy
- Precision
- Recall
- F1-score
- False Positive Rate (FPR)
- ROC-AUC

These metrics help assess the effectiveness and reliability of the proposed detection framework.

Deployment and Real-Time Monitoring

- The final model can be deployed in a real-time intrusion detection environment where it continuously monitors network traffic and raises alerts upon detecting suspicious activities.

5. Results

	precision	recall	f1-score	support
0	1.00	0.99	0.99	379
1	0.99	1.00	1.00	528
accuracy			1.00	907
macro avg	1.00	1.00	1.00	907
weighted avg	1.00	1.00	1.00	907

Fig-2: CAD Hybrid Model Classification Report

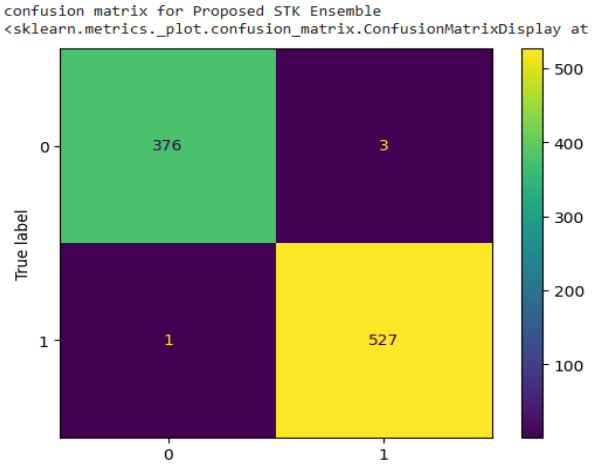

Fig-3: CAD Hybrid Model Confusion Matrix

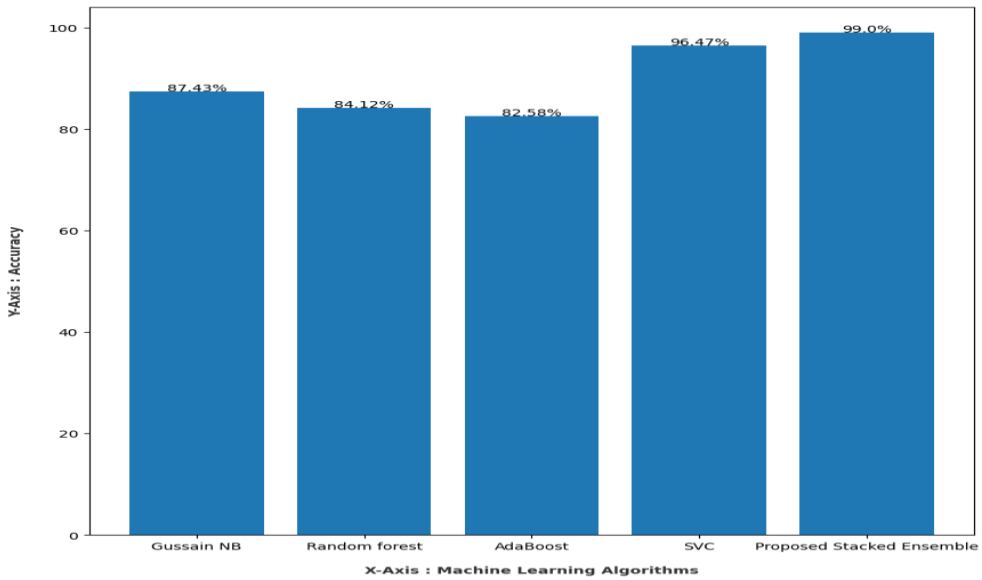

Fig-4: CAD Comparison Chart

6. Discussion

Performance of Individual Classifiers

- **Gaussian Naïve Bayes (87.43%)**

Gaussian NB shows moderate performance due to its strong assumption of feature independence, which is often violated in complex network traffic data. While computationally efficient, it struggles to capture non-linear relationships among features.

- **Random Forest (84.12%)**

Although Random Forest is generally robust, its performance in this case is relatively lower. This may be due to suboptimal hyperparameter tuning or high feature correlation, which can limit its generalization ability on imbalanced cyber security datasets.

- **AdaBoost (82.58%)**

AdaBoost records the lowest accuracy among the compared models. Boosting methods are sensitive to noise and misclassified instances, which can degrade performance when cyber attack datasets contain overlapping or noisy patterns.

- **Support Vector Classifier (SVC – 96.47%)**

SVC demonstrates strong performance, indicating its ability to model complex decision boundaries effectively. However, its performance is still limited by kernel selection and parameter sensitivity.

Superiority of the Proposed Stacked Ensemble

- **Proposed Stacked Ensemble (99.0%)**

The proposed hybrid stacked ensemble model achieves the highest accuracy, significantly outperforming all individual classifiers. This improvement is attributed to:

- The integration of multiple diverse learners
- Reduction of individual model bias and variance
- Effective learning of complementary patterns through a meta-classifier

By combining predictions from different base models, the stacked ensemble provides a more stable and generalized detection mechanism.

Conclusion

The chart clearly validates that the **Hybrid Stacked Ensemble technique** offers superior detection capability compared to traditional machine learning models, making it a reliable and efficient solution for accurate **Normal vs. Attack classification** in cyber security applications.

Refrences

[1] Verma, A. & Rathore, M., *Intelligent Cyber Threat Detection in IoT and Network Environments Using Hybrid Ensemble Learning*, Journal of Information Systems Engineering and Management (2025).

[2] Alqaraleh, S., *An Efficient Ensemble Network Anomaly Detection System for Cyber-Attacks*, Engineering, Technology & Applied Science Research (2025).
[3] Jumaah, N. S. & Ashkafaki, A. T., *Hybrid Ensemble Deep Learning Framework for Efficient DDoS Attack Detection in SDN*, Journal of Electrical Systems (2024).
[4] Boori, K. C., Bhatt, P. K., & Kumar, S., *Detection of Cyber Attacks in Networks Using Hybrid Decision Tree Technique*, Journal of Information Systems Engineering and Management (2025).
[5] Sharma, V. & Shah, D. J., *Ensemble Learning Classifiers and Hybrid Feature Selection for Enhancing IDS Performance*, Journal of Information Systems Engineering and Management (2025).
[6] *Explainable AI-based Innovative Hybrid Ensemble Model for Intrusion Detection*, Journal of Cloud Computing (2024).
[7] *Machine Learning-based Hybrid Technique to Enhance Cyber-Attack Perspective*, Journal of Cloud Computing (2025).
[8] *New Intrusion Detection Method Using Ensemble Classification and Feature Selection*, Scientific Reports (2025).
[9] *Ensemble Deep Learning-based Cyber Attack Detection Using Optimization Strategy*, Knowledge-Based Systems (2024).
[10] *Cyberattack Detection in Wireless Sensor Networks Using Hybrid Feature Reduction*, Journal of Big Data (2024).
[11] *A Hybrid Machine Learning Method for Increasing the Performance of Network IDS*, Journal of Big Data (2021).
[12] *Deploying Hybrid Ensemble Machine Learning Techniques for XSS Attack Detection*, Computers, Materials & Continua (2024).
[13] Ahmed, W., *Hybrid Ensemble Method for Detecting Cyber-Attacks in Water Distribution Systems*, arXiv (2025).
[14] Chatterjee, S. & Hanawal, M. K., *Federated Learning for Intrusion Detection Using a Hybrid Ensemble Approach*, arXiv (2021).
[15] Alharbi, S. & Khan, A., *Ensemble Defense System: A Hybrid IDS Approach for Effective Cyber Threat Detection*, arXiv (2024).