HYBRID STACKED MLP–KNN–RANDOM FOREST MODEL FOR CYBER ATTACK DETECTION ACROSS SECURITY DATASETS

SK. Himam Basha [1], A. Chenchu Mahesh [2]
Assistant Professor [1], PG Scholar [2]
Department of Master of Computer Applications
QIS College of Engineering & Technology (Autonomous), Ongole
Prakasam Dist., AP

Abstract: Cyber-attacks have become one of the most significant threats to modern digital infrastructures, leading to data breaches, unauthorized access, service disruptions, and financial losses. Traditional intrusion detection systems often struggle to identify sophisticated and evolving attack patterns, creating the need for intelligent, accurate, and automated cyber-attack detection mechanisms. This project proposes a Hybrid Stacked Machine Learning Based Real-Time Cyber Attack Detection System that combines Multilayer Perceptron (MLP), K-Nearest Neighbor (KNN), and Random Forest (RF) classifiers using a stacking ensemble approach to improve detection performance and reliability.

The proposed system performs data preprocessing, feature extraction, feature scaling, and attack prediction using the CICIDS2017 dataset. In addition to dataset-based prediction, the system supports real-time network traffic monitoring through packet capture and analysis using Scapy. Network traffic is classified as either normal or malicious, and the prediction results are further processed through risk assessment and alert generation modules. A Flask-based web application is developed to provide an interactive dashboard for monitoring, visualization, and report generation.

To enhance transparency and trustworthiness, the system integrates Explainable Artificial Intelligence (XAI) techniques to identify important features contributing to attack predictions. Experimental evaluation demonstrates that the proposed hybrid stacked model achieves high detection accuracy and outperforms individual machine learning classifiers. The developed framework provides an accurate, scalable, interpretable, and user-friendly solution for real-time cyber-attack detection and contributes to improving cybersecurity resilience and proactive threat management.

Keywords: Cyber-Attack Detection, Machine Learning, Stacking Ensemble, Multilayer Perceptron (MLP), K-Nearest Neighbor (KNN), Random Forest (RF), Explainable Artificial Intelligence (XAI), Intrusion Detection System, Network Security.

1. INTRODUCTION

The rapid growth of computer networks, cloud computing, Internet of Things (IoT) devices, and online services has significantly increased the risk of cyber-attacks. Organizations and individuals face numerous threats, including malware, phishing, denial-of-service attacks, botnets, and unauthorized network intrusions. These attacks can lead to financial losses, data breaches, and disruption of critical services.Traditional intrusion detection systems primarily rely on predefined rules and attack signatures, making them less effective against new and sophisticated threats. Machine learning techniques have emerged as powerful solutions for cyber-attack detection because they can learn patterns from network traffic and automatically identify malicious activities. However, individual machine learning algorithms often exhibit limitations when dealing with diverse cybersecurity datasets and evolving attack behaviors.

To address these challenges, this work proposes a Hybrid Stacked MLP–KNN–Random Forest Model that combines multiple classifiers through a stacking ensemble approach. The framework supports both dataset-based analysis and real-time network monitoring using packet capture techniques. Additional modules such as risk assessment, alert generation, threat intelligence, and Explainable Artificial Intelligence (XAI) enhance system reliability and transparency. The proposed system is implemented using Python and Flask, providing an interactive web-based platform for cyber-attack detection, analytics, and prediction. The objective is to develop an accurate, scalable, and intelligent cybersecurity solution capable of strengthening network defense against modern cyber threats.

2. LITERATURE SURVEY

a) AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions

This study presents a comprehensive overview of Artificial Intelligence (AI) applications in cybersecurity. The authors

discuss how AI-driven techniques improve threat detection, intrusion identification, malware analysis, and network security monitoring. The research highlights the ability of machine learning algorithms to learn complex attack patterns from large-scale security data. It also identifies challenges such as adversarial attacks, data quality issues, and model interpretability. The study concludes that AI-based cybersecurity systems provide more adaptive and intelligent defense mechanisms compared to traditional rule-based security approaches.

b) Artificial Intelligence Predictions in Cyber Security: Analysis and Early Detection of Cyber Attacks

This research focuses on the use of artificial intelligence for predicting and detecting cyber-attacks at an early stage. Various machine learning algorithms were evaluated for their ability to classify malicious network activities. The study demonstrates that intelligent prediction models can significantly reduce response time and improve attack detection accuracy. The authors emphasize the importance of real-time monitoring and automated threat analysis in modern cybersecurity environments. The results indicate that AI-based solutions can effectively identify suspicious behavior before major damage occurs.

c) A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions

This survey examines the effectiveness of Artificial Intelligence and Machine Learning techniques in cybersecurity applications. The authors compare different classification algorithms including Random Forest, Support Vector Machine, Neural Networks, and K-Nearest Neighbor. The study evaluates their performance in intrusion detection, malware classification, and anomaly detection tasks. Experimental findings reveal that ensemble learning approaches generally outperform individual classifiers in terms of accuracy and robustness. The survey highlights the growing importance of machine learning in addressing evolving cyber threats.

d) Applying AI and Machine Learning to Enhance Automated Cybersecurity and Network Threat Identification

This paper investigates the application of AI and machine learning techniques for automated network threat identification. The

authors propose intelligent security models capable of analyzing large volumes of network traffic and identifying malicious activities. The study demonstrates how automated detection systems reduce human intervention and improve threat response capabilities. Various feature engineering and classification techniques were evaluated to enhance prediction performance. The results show that AI-based security frameworks can significantly improve cyber defense operations.

e) Machine Learning-Based Cyber Threat Detection: An Approach to Malware Detection and Security with Explainable AI Insights

This research explores the integration of machine learning and Explainable Artificial Intelligence (XAI) for cyber threat detection. The proposed framework focuses on malware detection while providing transparency regarding model decisions. Feature importance analysis is used to explain how specific network characteristics contribute to attack predictions. The study demonstrates that XAI improves trust, interpretability, and decision-making in cybersecurity systems. The findings highlight the importance of combining accurate detection models with explainable mechanisms for practical deployment.

3. METHODOLOGY

i) Proposed Work

The proposed work introduces a **Hybrid Stacked MLP–KNN–Random Forest Based Real-Time Cyber Attack Detection System** designed to accurately identify malicious network activities using machine learning and real-time traffic monitoring. The system utilizes the **CICIDS2017 dataset** for model training and evaluation, where network traffic records are processed to distinguish between normal and attack behaviors. Data preprocessing techniques such as missing value handling, feature selection, label encoding, normalization, and feature scaling are applied to improve data quality and prediction performance.

The framework employs three machine learning algorithms: Multilayer Perceptron (MLP), K-Nearest Neighbor (KNN), and Random Forest (RF). These models are trained independently and combined using a stacking ensemble technique. The stacking classifier integrates the outputs of the individual models and generates a final prediction, resulting in higher accuracy and

improved robustness compared to standalone classifiers.

In addition to dataset-based prediction, the system supports real-time packet capture using Scapy. Captured network packets are processed through feature extraction and preprocessing modules before being analyzed by the trained hybrid model. The system classifies traffic as either normal or malicious and generates risk scores, alerts, and security notifications accordingly.

To improve transparency and trustworthiness, the system integrates Explainable Artificial Intelligence (XAI) for feature importance analysis and prediction explanation. A Flask-based web application provides user authentication, dashboard analytics, dataset upload prediction, report generation, and REST API support. The proposed framework delivers an intelligent, scalable, and user-friendly cybersecurity solution capable of performing both offline and real-time cyber-attack detection.

ii) System Architecture

The proposed system follows a multi-layer architecture consisting of data acquisition, preprocessing, prediction, risk assessment, explainability, and visualization components. The system accepts input either from uploaded datasets or from real-time network traffic captured through packet sniffing.

Initially, network packets are collected using Scapy or uploaded through the dataset prediction module. The collected data undergoes preprocessing, including cleaning, normalization, encoding, and feature extraction. Important network traffic attributes are generated and transformed into a machine-learning-compatible format.

The processed features are supplied to the Hybrid Stacked Prediction Engine, which combines MLP, KNN, and Random Forest classifiers. Each model independently predicts the network behavior, and a stacking mechanism combines their outputs to generate the final classification result.

The prediction results are forwarded to the Risk Assessment Module, which calculates risk scores and categorizes attack severity. The Alert Generation Module produces notifications whenever malicious traffic is detected. Simultaneously, the Threat Intelligence Module enriches security information and the XAI Module explains prediction decisions through feature importance analysis.

The entire framework is deployed through a Flask-based web application, providing dashboard analytics, report generation, secure authentication, dataset upload prediction, and REST API integration. All logs, predictions, alerts, and user records are maintained in an SQLite database.

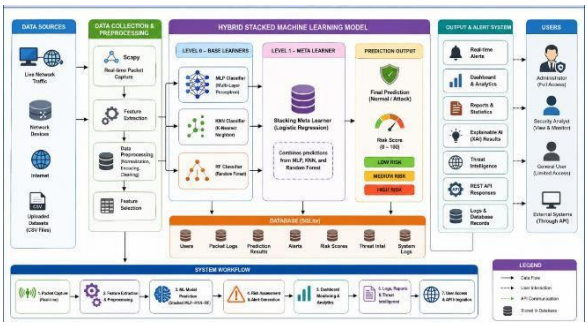

Fig 1: System Architecture

iii) Modules

1. User Authentication Module

This module manages user registration, login, session management, and role-based access control to ensure secure access to system resources.

2. Real-Time Packet Capture Module

This module captures live network packets using Scapy and continuously monitors network traffic for analysis.

3. Feature Extraction Module

This module extracts important network traffic features such as packet count, byte count, protocol information, flow duration, and port numbers.

4. Data Preprocessing Module

This module performs data cleaning, feature normalization, scaling, encoding, and transformation before prediction.

5. Hybrid Machine Learning Prediction Module

This module uses the stacked combination of MLP, KNN, and Random Forest classifiers to classify network traffic as normal or malicious.

6. Risk Assessment Module

This module calculates risk scores and determines attack severity levels for detected threats.

7. Alert Generation Module

This module generates real-time alerts and records security events whenever malicious activity is detected.

8. Threat Intelligence Module

This module enriches attack information using threat intelligence data and security indicators.

9. Explainable AI (XAI) Module

This module explains prediction decisions and identifies important features contributing to attack detection.

10. Dashboard and Analytics Module

This module provides visualization of predictions, attack statistics, security analytics, and system performance.

11. Dataset Upload Prediction Module

This module allows users to upload CSV datasets and obtain cyber-attack predictions through the web interface.

12. REST API Module

This module enables communication between the system and external applications through API services.

13. Database Management Module

This module stores user information, packet logs, alerts, prediction results, reports, and system records.

iv) Algorithms

1. Multilayer Perceptron (MLP)

MLP is a feedforward artificial neural network consisting of multiple hidden layers. It learns complex non-linear relationships within network traffic data and identifies sophisticated cyber-attack patterns.

2. K-Nearest Neighbor (KNN)

KNN is a supervised learning algorithm that classifies data based on the majority class of its nearest neighbors. It helps identify malicious traffic by comparing new observations with historical network behavior.

3. Random Forest (RF)

Random Forest is an ensemble learning algorithm that combines multiple decision trees to improve classification accuracy and reduce overfitting. It effectively handles complex cybersecurity datasets.

4. Hybrid Stacked MLP–KNN–Random Forest Model

The Hybrid Stacked Model combines the strengths of MLP, KNN, and Random Forest through a stacking ensemble technique. Individual predictions from all three models are aggregated by a meta-learning mechanism to generate the final classification result. This approach improves detection accuracy, reduces false alarms, increases robustness, and provides reliable

cyber-attack prediction in both offline and real-time environments.

4. EXPERIMENTAL RESULTS

The proposed Hybrid Stacked MLP–KNN–Random Forest Based Real-Time Cyber Attack Detection System was evaluated using the CICIDS2017 dataset and real-time network traffic captured through Scapy. Before model training, the dataset underwent preprocessing operations including missing value handling, feature selection, label encoding, normalization, and feature scaling. These preprocessing techniques improved data quality and ensured efficient machine learning performance.

Three machine learning algorithms, namely Multilayer Perceptron (MLP), K-Nearest Neighbor (KNN), and Random Forest (RF), were trained independently and later combined using a stacking ensemble approach. The Hybrid Stacked Model demonstrated superior performance compared to the individual classifiers by leveraging the strengths of all three algorithms. Experimental results showed that the proposed framework achieved high detection accuracy while maintaining robustness across different attack categories.

The developed system also supports real-time packet monitoring through Scapy. Captured packets are converted into machine-learning-compatible features and supplied to the trained model for attack prediction. The system successfully classifies network traffic as either normal or malicious and generates corresponding alerts, risk scores, and security notifications. Explainable Artificial Intelligence (XAI) techniques were used to identify the most influential features contributing to prediction decisions, improving transparency and trust in the model.

The Flask-based web application provides secure user authentication, dashboard analytics, dataset upload prediction, report generation, and real-time attack monitoring. The integration of machine learning, explainable AI, risk assessment, and web-based deployment demonstrates the effectiveness of the proposed framework for practical cybersecurity applications.

Accuracy: Accuracy measures the ability of the model to correctly classify network traffic as normal or malicious. It represents the ratio of correctly predicted observations to the total number of observations.

$$\text{Accuracy} = \text{TP} + \text{TN} /(\text{TP} + \text{TN} + \text{FP} + \text{FN})$$

$$Accuracy = \frac{(TN + TP)}{T}$$

Precision: Precision measures how many of the predicted attack instances are actually attacks. High precision indicates a low false positive rate.

$$\Pr e\,cision = \frac{TP}{(TP + FP)}$$

Recall: Recall measures the ability of the model to identify all actual attack instances. High recall indicates effective attack detection capability.

$$Recall = \frac{TP}{(FN + TP)}$$

F1-Score: The F1-Score combines precision and recall into a single metric. It provides a balanced measure of model performance.

$$F1 = 2 \cdot \frac{(Recall \cdot \Pr e\,cision)}{(Recall + \Pr e\,cision)}$$

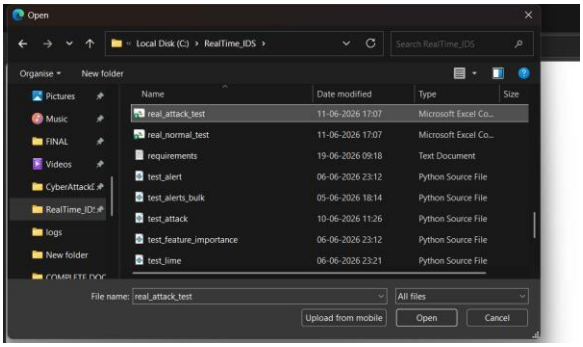

Fig 2 uploading test data file

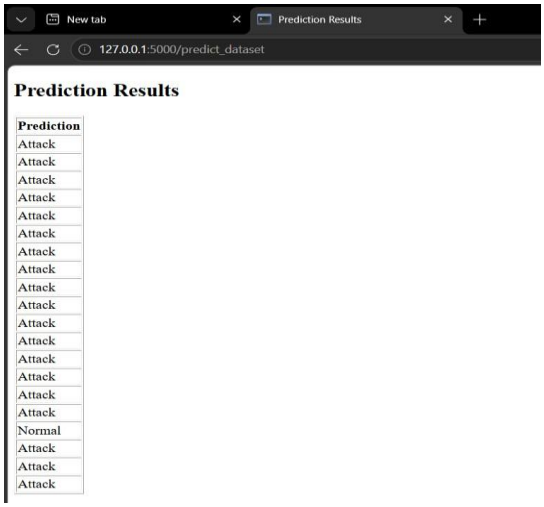

Fig 3 results

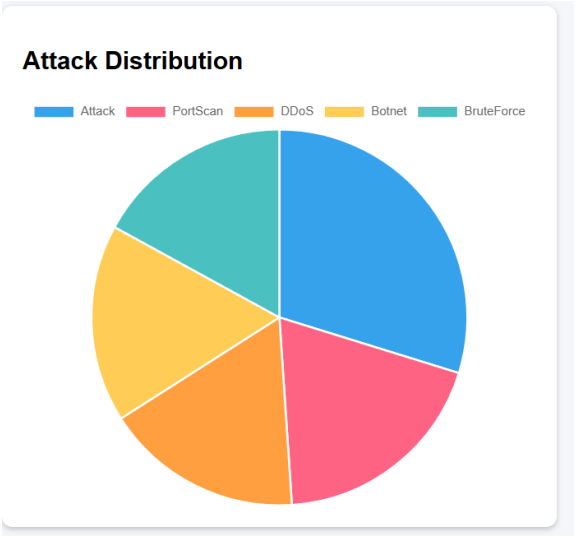

Fig 4 Accuracy graph

5. CONCLUSION

Cyber-attacks continue to pose serious threats to modern digital infrastructures due to their increasing frequency, complexity, and evolving attack patterns. Traditional security mechanisms often struggle to detect sophisticated and previously unseen attacks, creating a need for intelligent and automated detection systems. In this work, a Hybrid Stacked MLP–KNN–Random Forest Based Real-Time Cyber Attack Detection System was developed to improve the accuracy and reliability of cyber threat identification. The proposed framework combines the strengths of Multilayer Perceptron (MLP), K-Nearest Neighbor (KNN), and Random Forest (RF) classifiers using a stacking ensemble approach to achieve superior detection performance.

The system was trained and evaluated using benchmark cybersecurity datasets and integrated with real-time packet monitoring capabilities through Scapy. Experimental results demonstrated that the hybrid stacked model outperformed individual machine learning algorithms by providing highly accurate attack classification while reducing false detections. Additional components such as risk assessment, alert generation, threat intelligence integration, dashboard analytics, and dataset upload prediction enhanced the practical usability of the framework. The incorporation of Explainable Artificial Intelligence (XAI) further improved transparency by identifying important features that influence prediction outcomes.

A Flask-based web application was successfully implemented to provide secure user authentication, real-time monitoring, prediction services, analytics visualization, and report generation through a user-friendly interface. The integration of ensemble machine learning, real-time traffic analysis, explainable AI, and web deployment makes the proposed system a comprehensive cybersecurity solution. Overall, the developed framework demonstrates strong potential for protecting network environments against modern cyber threats and contributes toward building more intelligent, scalable, and reliable cyber-attack detection systems.

6. FUTURE SCOPE

The proposed Hybrid Stacked MLP–KNN–Random Forest Based Cyber Attack Detection System can be further enhanced by incorporating real-time large-scale network monitoring and advanced traffic analysis techniques. Future versions of the

system may support high-speed enterprise networks and cloud-based infrastructures, enabling continuous monitoring of massive volumes of network traffic. The integration of advanced stream processing technologies can improve detection speed and allow faster identification of emerging cyber threats.

The framework can also be extended by incorporating advanced Artificial Intelligence technologies such as Generative AI and Deep Learning models. Generative AI can be used to simulate new attack patterns, generate synthetic cybersecurity datasets, and improve model training against previously unseen threats. Additionally, automated model retraining mechanisms can be introduced to ensure that the detection engine continuously adapts to evolving cyber-attack techniques and changing network environments.

REFERENCES

[1] Shilpa Ankalaki, Aparna Rajesh Atmakuri, M. Pallavi, et al., "Cyber Attack Prediction: From Traditional Machine Learning to Generative Artificial Intelligence," IEEE Access, vol. 13, pp. 1–25, 2025.

[2] M. K. Rahman, H. M. Dalim, and M. S. Hossain, "AI-Powered Solutions for Enhancing National Cybersecurity: Predictive Analytics and Threat Mitigation," International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence, vol. 14, no. 1, pp. 1036–1069, 2023.

[3] Q. Chen, D. Li, and L. Wang, "The Role of Artificial Intelligence in Predicting and Preventing Cyber Attacks," Journal of Industrial Engineering and Applied Science, vol. 2, no. 4, pp. 29–35, 2024.

[4] M. A. Khalaf and A. Steiti, "Artificial Intelligence Predictions in Cyber Security: Analysis and Early Detection of Cyber Attacks," Babylonian Journal of Machine Learning, pp. 63–68, 2024.

[5] M. Paramesha, N. Rane, and J. Rane, "Artificial Intelligence, Machine Learning, and Deep Learning for Cybersecurity Solutions: A Review of Emerging Technologies and Applications," 2024.

[6] M. El-Ghoul, M. H. Al-Qadi, B. S. Abu-Nasser, and S. S. Abu-Naser, "Artificial Intelligence as a Frontline Defense: Preventing Cyberattacks in a Connected World," 2025.

[7] S. Sankar, R. Dutta, and S. Karmakar, "Cyber Threat Prediction and Assessment

with Machine Learning Approaches," IEEE INDICON, 2024.

[8] M. B. Karaja et al., "AI-Driven Cybersecurity: Transforming the Prevention of Cyberattacks," 2024.

[9] I. H. Sarker, M. H. Furhad, and R. Nowrozy, "AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions," SN Computer Science, 2021.

[10] R. Ejjami, "Enhancing Cybersecurity through Artificial Intelligence: Techniques, Applications, and Future Perspectives," 2024.

[11] M. Lourens et al., "Integration of AI with Cybersecurity: A Detailed Systematic Review with Practical Issues and Challenges," IEEE IC3I, 2022.

[12] A. Raji et al., "Integrating Artificial Intelligence, Machine Learning, and Data Analytics in Cybersecurity," World Journal of Advanced Research and Reviews, 2023.

[13] A. Sharma, S. Rani, and M. Shabaz, "A Comprehensive Review of Explainable AI in Cybersecurity: Decoding the Black Box," ICT Express, 2025.

[14] R. Gupta and P. Srivastava, "Artificial Intelligence and Machine Learning in Cyber Security Applications," Elsevier, 2025.

[15] M. Sankaram et al., "A Comprehensive Review of Artificial Intelligence Applications in Enhancing Cybersecurity Threat Detection and Response Mechanisms," 2024.

Author Profiles

Mr. Himam Basha Shaik is an Assistant Professor in the Department of Master of Computer Applications at QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He earned his Master of Computer Applications (MCA) from Anna University, Chennai. With a strong research background, He has authored and co-authored research papers published in reputed peer-reviewed journals. His research interests include Machine Learning, Artificial Intelligence, Cloud Computing, and Programming Languages. He is committed to advancing research and fostering innovation while mentoring students to excel in both academic and professional pursuits.

Mr. A CHENCHU MAHESH is an MCA Student in the Department of Computer Application at QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He completed his bachelor's degree in MPCS (Mathematics, Physics, Computer Science) from Sri Harshini Degree College, Ongole, Prakasam district.