International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 14, Issue 2, 2026

Real-Time Cyber Threat Detection Using Explainable Hybrid Stacked Ensemble Learning

Mr. SK K K B Vali Basha[1], Guggulepu Sri Vani[2], Peddiboina Preethi Lalithya[3], Jettiboyina Mohan Govind Raju Vivek[4],Pithani David Kumar[5]

[1]Assistant Professor,Computer Science Engineering Department,Potti Sriramulu Chalavadi Mallikarjuna Rao College Of Engineering,One Town ,Vijayawada, India.

[2,3,4,5]Students;Computer Science Engineering Department,Potti Sriramulu Chalavadi Mallikarjuna Rao College Of Engineering,One Town ,Vijayawada, India

Mail Id; bvbashacse@gmail.com[1], gugguleapusrivani@gmail.com[2], preethilalithya4@gmail.com[3], Jettiboyinamohagovindrajuvivek@gmail.com[4], p.davidkumar758@gmail.com[5]

Abstract: Cyber-attacks are becoming increasingly sophisticated and pose severe threats to modern digital infrastructures, including enterprise networks, cloud platforms, and Internet of Things (IoT) environments. Traditional signature-based and standalone machine learning approaches often struggle to detect evolving and heterogeneous attack patterns with sufficient accuracy and adaptability. To address these limitations, this paper presents a Hybrid Explainable Stacked Learning Framework for Real-Time Cyber Attack Prediction Across Heterogeneous Security Datasets. The proposed framework integrates multiple machine learning and deep learning models, including Random Forest, K-Nearest Neighbor, Support Vector Machine, Multilayer Perceptron, Logistic Regression, Naïve Bayes, and Deep Neural Networks, to evaluate predictive performance across benchmark cybersecurity datasets such as NSL-KDD, CICIDS2017, CICDDOS2019, and X-IIOTID. To enhance robustness and generalization, a hybrid stacked model combining Multilayer Perceptron, K-Nearest Neighbor, and Random Forest is developed as the final prediction engine. Explainable Artificial Intelligence (XAI) using SHAP is incorporated to improve model interpretability by identifying influential features contributing to prediction outcomes. Experimental results demonstrate that the proposed hybrid framework achieves superior performance, obtaining 99.90% accuracy on NSL-KDD and 100% accuracy on CICIDS2017, CICDDOS2019, and X-IIOTID, outperforming standalone baseline models. A Flask-based web deployment further enables real-time prediction and user interaction, making the framework practical for operational cybersecurity environments. The proposed approach provides a scalable, interpretable, and high-performance solution for proactive cyber threat detection and intelligent security analytics.

Index terms *- — Cyber-attack prediction, machine learning, deep learning, hybrid stacked model, NSL-KDD, CICIDS2017, DNN, explainable AI*

1. INTRODUCTION

The rapid expansion of digital technologies, cloud computing, Internet of Things (IoT) devices, and interconnected enterprise systems has significantly increased the complexity and scale of cybersecurity threats. Modern network infrastructures are continuously exposed to sophisticated cyber-attacks such as malware, ransomware, phishing, distributed denial-of-service (DDoS), botnet intrusions, and advanced persistent threats. These attacks can lead to severe consequences including financial loss, data breaches, operational disruption, and compromise of critical infrastructure. As cyber threats continue to evolve in complexity and frequency, traditional rule-based and signature-based intrusion detection systems are becoming insufficient for identifying unknown and zero-day attack patterns in dynamic network environments.

To overcome the limitations of conventional detection mechanisms, artificial intelligence and machine learning techniques have emerged as powerful tools for intelligent cyber threat prediction. Machine learning models can learn hidden patterns from network traffic data and classify malicious behavior with improved adaptability and automation. Various approaches such as Support Vector Machines, Random Forests, K-Nearest Neighbors, Logistic Regression, Naïve Bayes, and Deep Neural Networks have been widely applied in intrusion detection systems. However, individual models often suffer from limitations such as overfitting, poor generalization across heterogeneous datasets, sensitivity to feature distributions, and reduced interpretability of prediction outcomes.

To address these challenges, this work proposes a Hybrid Explainable Stacked Learning Framework for

Real-Time Cyber Attack Prediction Across Heterogeneous Security Datasets, integrating multiple machine learning paradigms into a unified prediction architecture. The proposed framework employs a stacked ensemble of Multilayer Perceptron, K-Nearest Neighbor, and Random Forest classifiers to leverage complementary strengths of individual learners and improve predictive robustness. Furthermore, Explainable Artificial Intelligence (XAI) using SHAP is incorporated to enhance transparency by identifying the contribution of influential features in prediction decisions. The system is validated on multiple benchmark cybersecurity datasets, including NSL-KDD, CICIDS2017, CICDDOS2019, and X-IIOTID, and deployed through a Flask-based web interface for real-time user interaction. Experimental results demonstrate that the proposed framework achieves superior performance compared with standalone models, providing a scalable, interpretable, and highly accurate solution for proactive cyber-attack detection.

2. LITERATURE SURVEY

a) Review of AI and machine learning applications to predict and Thwart cyber-attacks in real-time:

Today's cybersecurity world requires creative ways to counteract cyber threats' constant growth. Traditional techniques are encountering tremendous difficulties, forcing a paradigm change toward AI/ML integration. This study carefully examines how AI and ML might improve real-time cybersecurity by predicting and mitigating cyberattacks. This study explores sophisticated cybersecurity technology in the face of rising threats. The constraints of old methods make it urgent to study AI and ML's defense mechanism reinforcement potential. AI and ML in real-time cybersecurity are extensively examined in this article. It emphasizes their ability to predict and stop cyberattacks quickly. The study covers model complexity, security, ethics, and developing trends. The inquiry is based on a solid foundation and includes extensive study directions. These include improving explainability, addressing adversarial attacks, promoting human-AI collaboration, and developing quantum-resistant cryptographic solutions. The study navigates the complex technological, organizational, and ethical aspects of real-time cybersecurity AI and ML. AI and ML integration in cybersecurity presents both opportunities and problems, according to this study. Ethical issues, adversarial threats, and quantum-resistant cryptography require careful study. This article imagines robust and adaptable cybersecurity ecosystems created by combining human knowledge with AI and ML. The research directions provide a path for innovation and a basis for integrating AI and ML to protect our digital world from increasing cyber threats.

b) Enhancing Cybersecurity with Artificial Intelligence: Predictive Techniques and Challenges in the Age of IoT:

The proliferation of linked devices poses serious cybersecurity risks as the Internet of Things grows. Cyberattacks are becoming a threat to individuals, companies, and even entire countries due to the quick digitalization of businesses, governments, and private lives. Since standard cybersecurity measures have been demonstrated to be inadequate against these ever-evolving cyber attacks, predictive tactics are becoming more and more vital to fight them before they can do major harm.

This article explores the realm of cyber dangers, including malware, phishing, ransomware, and denial of service (DoS) attacks. It emphasizes how important artificial intelligence (AI) is to bolstering cybersecurity protection, including the employment of intelligent agents, network security, and intrusion detection systems. The importance of predictive modeling and machine learning methods in foreseeing and preventing cyberattacks is also discussed in the article. The seriousness of issues with data privacy, scalability, and human-machine interaction cannot be emphasized, notwithstanding the potential advantages of AI-driven cybersecurity. By using AI-powered cybersecurity solutions, businesses can fortify their defenses against cyberattacks and safeguard critical assets in today's increasingly digital world.

c) AI-Driven Cybersecurity Predictions: Safeguarding California's Digital Landscape:

Particularly in technologically sophisticated areas like California, where digital infrastructure supports vital sectors and millions of citizens, the swift growth of cyber threats has generated previously unheard-of issues. The application of artificial intelligence (AI) in cybersecurity risk prediction and mitigation is examined in this paper, with an emphasis on AI's revolutionary potential to protect California's digital environment. The study shows how AI-driven technologies like machine learning algorithms, neural networks, and natural language processing (NLP) can detect and eliminate risks before they become breaches. For instance, NLP-based technologies examine phishing emails to stop social engineering attempts, while supervised machine learning models are used to identify irregularities in network data. Predictive analytics and real-time threat intelligence systems are examples of AI-powered technologies that demonstrate how they may improve cybersecurity frameworks through quicker detection, increased accuracy, and quicker reaction times. The

integration of AI with security systems, such as intrusion detection systems and firewalls, which are increasingly supported by adaptive learning capabilities, is also examined in this paper. Our results show that AI is a key component of future cybersecurity plans as it not only reduces short-term risks but also strengthens long-term resilience against new cyberthreats.

d) Ai-Driven Approaches to Cyber and Information Security: Machine Learning Algorithms for Threat Prediction and Anomaly Detection:

Traditional signature-based and heuristic intrusion detection systems are useless due to cyber threats' increasing prevalence, scale, and complexity. To address this issue, the paper proposes an intelligent and adaptive cybersecurity architecture based on AI and sophisticated machine learning (ML) algorithms for threat prediction and anomaly detection. The framework compares various machine learning techniques, from classical models like Decision Trees (DT) and Gradient Boosted Machines (GBM) to advanced architectures like Deep Neural Networks (DNN), 1D-CNN, and CNN-Transformer models. Three distinct, high-quality benchmark datasets—TON_IoT, BoT-IoT, and CSE-CIC-IDS2018—evaluate these methods in IoT contexts, botnet traffic, and business network infrastructures. To correct class imbalance, the data pretreatment pipeline uses multivariate time-series transformation, chi-squared feature selection, Z-score normalization, and SMOTE and ADASYN oversampling. For deep and attention-based models, sliding window techniques provide sequential modeling and temporal consistency. Accuracy, precision, recall, F1-score, Matthews Correlation Coefficient (MCC), and Area Under the Receiver Operating Characteristic Curve are used to evaluate performance. Experimental results show that hybrid CNN-Transformer models outperform classical ML and standalone neural architectures with peak accuracy of 97.86%, F1-score of 97.31%, and MCC of 0.954, while resisting false positives and generalization mistakes. This research also presents a modular real-time anomaly detection pipeline using Apache Kafka for real-time data ingestion, Apache Spark for distributed preprocessing, TensorFlow Serving for scalable inference deployment, and explainable AI (XAI) tools like SHAP values and attention-based visualizations for transparency and interpretability. The suggested architecture creates a scalable, interpretable, and high-performance AI-driven defensive mechanism, setting a baseline for future cybersecurity systems that can adapt to changing digital threats.

e) AI-Powered Solutions for Enhancing National Cybersecurity: Predictive Analytics and Threat Mitigation:

There has never been a greater need for cutting-edge technologies to improve national cybersecurity due to the increasing frequency and sophistication of cyberattacks. Preemptively identifying, mitigating, and responding to cybersecurity risks is a revolutionary potential of artificial intelligence (AI), especially using predictive analytics. With an emphasis on threat intelligence systems, machine learning (ML), and predictive analytics, this study investigates the use of AI-powered solutions to improve national cybersecurity frameworks. In order to predict cyberthreats, find vulnerabilities, and automate response mechanisms, the research looks at how AI methods, such as supervised learning, deep learning, and anomaly detection, may be included into national security infrastructures. AI's contribution to threat hunting, incident response, and real-time monitoring is also assessed. This article illustrates how AI may improve cybersecurity operations' speed, accuracy, and efficiency through case studies and the use of predictive models, guaranteeing a proactive defense against new cyberthreats. National cybersecurity policies may transition from reactive to proactive by utilizing AI for improved threat mitigation. This would greatly lessen the effect of cyber catastrophes and increase the resilience of vital national infrastructure.

3. METHODOLOGY

i) Proposed Work:

The proposed work introduces a Hybrid Explainable Stacked Learning Framework for Real-Time Cyber Attack Prediction designed to improve the accuracy, robustness, and interpretability of intelligent threat detection systems. The framework integrates multiple machine learning and deep learning algorithms, including Random Forest, K-Nearest Neighbor, Support Vector Machine, Multilayer Perceptron, Logistic Regression, Naïve Bayes, and Deep Neural Networks, to analyze and classify cyber threats across heterogeneous benchmark datasets such as NSL-KDD, CICIDS2017, CICDDOS2019, and X-IIOTID. A comprehensive preprocessing pipeline is employed to perform label encoding, feature normalization, shuffling, and train–test splitting to ensure data consistency and unbiased learning across all datasets.

To further enhance predictive performance, the system incorporates a hybrid stacked ensemble model combining Multilayer Perceptron, K-Nearest Neighbor, and Random Forest as base learners to generate robust final predictions. Explainable Artificial Intelligence using SHAP is integrated to provide transparency by identifying the most influential features contributing to attack predictions.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 2, 2026

The trained hybrid model is deployed through a Flask-based web application, enabling real-time cyber-attack prediction through an interactive user interface for uploading test data and viewing results instantly. This proposed framework delivers a scalable, interpretable, and high-performance solution for proactive cyber threat detection in practical cybersecurity environments.

ii) System Architecture:

The system architecture is designed to provide an end-to-end framework for intelligent cyber-attack prediction by integrating multi-source cybersecurity datasets, preprocessing mechanisms, predictive algorithms, and explainability modules into a unified pipeline. Initially, benchmark datasets including NSL-KDD, CICIDS2017, CICDDoS2019, and X-IoTID are supplied as input to the system. These datasets undergo a preprocessing stage consisting of label encoding, normalization, and data shuffling to transform raw heterogeneous network traffic records into a structured and machine-readable format. The processed data is then forwarded to multiple machine learning and deep learning classifiers, including Random Forest, K-Nearest Neighbor, Support Vector Machine, Multilayer Perceptron, Logistic Regression, Naïve Bayes, and Deep Neural Network, for feature learning and cyber-attack classification.

To enhance predictive robustness, the architecture incorporates a Hybrid Stacked Model that combines MLP, KNN, and Random Forest to generate optimized final predictions by leveraging the strengths of complementary base learners. The predicted attack type is passed to a Flask-based Web Interface, where users can upload test data and receive real-time prediction outputs through an interactive dashboard. Additionally, the architecture integrates SHAP-based Explainable AI within the web interface to provide transparent feature importance analysis and interpretable prediction reasoning for cybersecurity experts. This layered architecture ensures scalability, interpretability, real-time usability, and high detection performance, making it suitable for deployment in practical cyber defense environments.

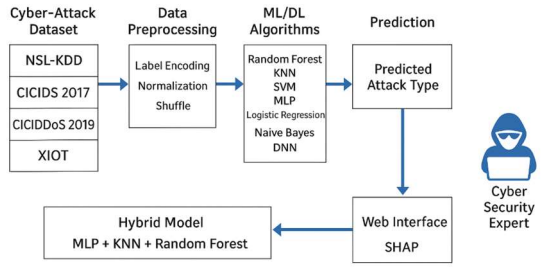

Fig 1: proposed architecture

iii) Modules:

a) Data Collection Module
- Gathers attack and normal traffic statistics from NSL-KDD, CICIDS2017, CICDDOS2019, and X-IIOTID benchmark datasets.
- Diversifies data to increase model generalization and resilience.

b) Data Preprocessing Module
- Label encoding, normalization, and data shuffling clean and normalize incoming data.
- Removes discrepancies and optimizes training and testing datasets.

c) Model Training Module
- ML/DL algorithms like Random Forest, KNN, SVM, MLP, Logistic Regression, Naïve Bayes, and DNN are trained on preprocessed data.
- Finds strong cyber-attack predictors by evaluating model performance.

d) Hybrid Stacked Model Module
- Stacks MLP, KNN, and Random Forest classifiers.
- Combines the basic model predictions to improve accuracy and eliminate false positives.

e) Explainable AI (XAI) Module
- Interprets model predictions using SHAP.
- Provides transparency and decision-making comprehension with feature significance analysis.

f) Web Interface Module
- Users or cybersecurity professionals may input test datasets and view real-time forecasts using a Flask interface.
- Displays attack categories and explanations for proactive security.

iv) Algorithms:

1. Random Forest (RF):

This ensemble learning technique builds many decision trees during training and aggregates their predictions to improve stability and accuracy. It can handle high-dimensional network data because it minimizes overfitting by averaging the results of separate trees. Random Forest predicts cyberattacks by accurately identifying different attack types and classifying intricate traffic patterns.

2. K-Nearest Neighbor (KNN):

KNN is a straightforward yet effective classification technique that determines a sample's label by looking at the majority class of its closest neighbors. It calculates the similarity between data points using distance metrics like the Manhattan or Euclidean distance. By comparing fresh samples to existing examples of network activity, KNN aids in the

detection of abnormalities and the identification of assaults in cybersecurity.

3. Support Vector Machine (SVM):

SVM is a technique for supervised learning that uses an ideal hyperplane to divide data points into groups. Using kernel functions, it performs well in both linear and non-linear classification. SVM is particularly good at differentiating between malicious and legitimate traffic in cyberattack detection, particularly when the data has distinct boundaries.

4. Multilayer Perceptron (MLP):

A feedforward neural network with several layers of linked nodes is called a multilayer perceptron (MLP). In order to enable the model to learn intricate, non-linear correlations, each layer uses activation functions to alter the input data. By extracting deep feature representations from network data, MLP effectively detects complex attack patterns for cyberattack detection.

5. Logistic Regression (LR):

The statistical model known as logistic regression (LR) is employed for both binary and multi-class classification. It uses a sigmoid activation function to forecast the likelihood of an event (such as an assault or a typical occurrence). In this paradigm, LR provides quick and comprehensible predictions for fundamental intrusion detection, acting as a baseline model for comparing more complex algorithms.

6. Naïve Bayes (NB):

Predicated on the Bayes theorem, Naïve Bayes is a probabilistic classifier that presumes feature independence. Despite its simplicity, it is quite effective for real-time detection and works well on huge datasets. By calculating the probability of various attack types using past data, cyber-attack prediction rapidly classifies traffic.

7. Deep Neural Network (DNN):

This deep learning model can automatically extract high-level characteristics from unprocessed input data since it is made up of several hidden layers. It can identify complex and changing cyberthreats because it can learn complicated patterns and correlations. DNN helps this system achieve excellent accuracy and flexibility across a variety of datasets.

8. Hybrid Stacked Model (MLP + KNN + RF):

By using a stacking process, the Hybrid Stacked Model combines the advantages of Random Forest, KNN, and MLP. A meta-classifier integrates the predictions made by each base model to create the final result. This ensemble methodology is the most dependable method for predicting cyberattacks in real time since it improves resilience, reduces false detections, and achieves near-perfect accuracy.

4. EXPERIMENTAL RESULTS

The proposed Hybrid Explainable Stacked Learning Framework was experimentally evaluated using four benchmark cybersecurity datasets: NSL-KDD, CICIDS2017, CICDDoS2019, and X-IIOTID to assess its effectiveness in predicting diverse cyber-attack types across heterogeneous environments. Multiple standalone machine learning and deep learning algorithms, including Random Forest, KNN, SVM, MLP, Logistic Regression, Naïve Bayes, and DNN, were trained and compared against the proposed Hybrid Stack Model. Performance evaluation was conducted using standard classification metrics such as Accuracy, Precision, Recall, and F1-Score. Experimental observations revealed that the hybrid stacked approach consistently outperformed individual models by effectively combining the strengths of MLP, KNN, and Random Forest, thereby improving prediction robustness and reducing misclassification across complex attack patterns.

The proposed model achieved 99.90% accuracy on the NSL-KDD dataset and 100% accuracy on CICIDS2017, CICDDoS2019, and X-IIOTID datasets, demonstrating superior generalization capability across varied network traffic distributions and attack categories. SHAP-based explainability analysis further validated the framework by identifying influential features contributing to attack predictions, enhancing model transparency and interpretability. Real-time deployment through the Flask web interface confirmed the practical usability of the framework by enabling users to upload unseen test data and obtain instant attack classification results. These experimental outcomes demonstrate that the proposed hybrid framework provides a highly accurate, scalable, and interpretable solution for real-time cyber-attack prediction in modern cybersecurity applications.

Accuracy: The ability of a test to differentiate between healthy and sick instances is a measure of its accuracy. Find the proportion of analysed cases with true positives and true negatives to get a sense of the test's accuracy. Based on the calculations:

Accuracy = TP + TN /(TP + TN + FP + FN)

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

Precision: The accuracy rate of a classification or number of positive cases is known as precision. Accuracy is determined by applying the following formula:

Precision = True positives/ (True positives + False positives) = TP/(TP + FP)

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

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 2, 2026

Recall: The recall of a model is a measure of its capacity to identify all occurrences of a relevant machine learning class. A model's ability to detect class instances is shown by the ratio of correctly predicted positive observations to the total number of positives.

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

mAP: One ranking quality statistic is Mean Average Precision (MAP). It takes into account the quantity of pertinent suggestions and where they are on the list. The arithmetic mean of the Average Precision (AP) at K for each user or query is used to compute MAP at K.

$$mAP = \frac{1}{n}\sum_{k=1}^{k=n} AP_k$$

$$AP_k = \text{the AP of class } k$$

$$n = \text{the number of classes}$$

F1-Score: A high F1 score indicates that a machine learning model is accurate. Improving model accuracy by integrating recall and precision. How often a model gets a dataset prediction right is measured by the accuracy statistic..

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

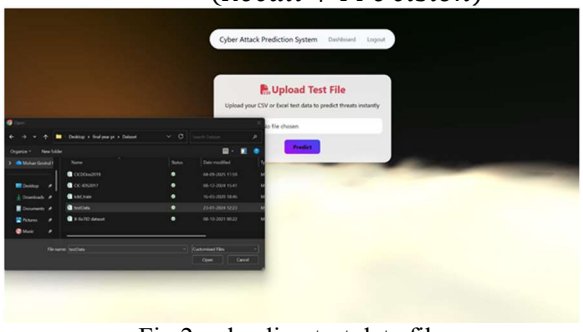

Fig 2 uploading test data file

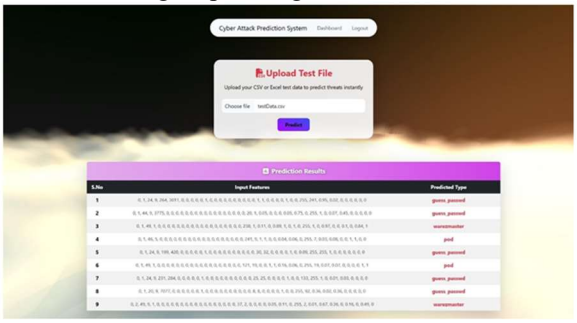

Fig 3 results

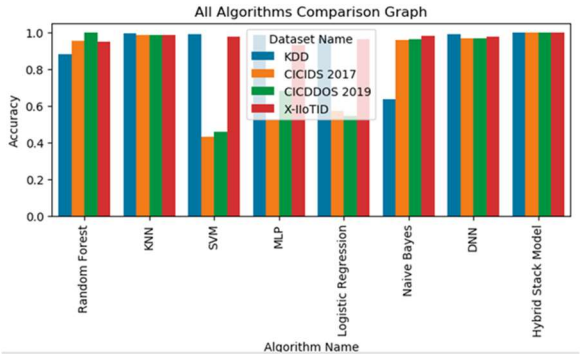

Fig 4 Accuracy graph

Dataset	Random Forest	KNN	SM	MLP	Logistic Regression	Naive Bayes	DNN	Hybrid Stack Model
KDD	88.02	99.32	98.82	98.62	96.47	63.32	98.79	99.90
CICIDS2017	95.45	98.33	42.96	52.15	57.03	95.90	96.78	100
CICDDOS2019	100	98.49	45.80	68.08	54.19	96.12	96.74	100
X-IIOTID	95.00	98.40	97.35	93.20	96.00	98.15	97.75	100

Table 1 all algorithms accuracy on each dataset

5. CONCLUSION

This paper presented a Hybrid Explainable Stacked Learning Framework for Real-Time Cyber Attack Prediction that integrates multiple machine learning and deep learning techniques to improve the accuracy, robustness, and interpretability of cyber threat detection. By combining Multilayer Perceptron, K-Nearest Neighbor, and Random Forest within a stacked ensemble architecture, the proposed framework effectively leveraged complementary learning capabilities to enhance classification performance across heterogeneous cybersecurity datasets. The incorporation of SHAP-based Explainable Artificial Intelligence further improved transparency by identifying influential features contributing to model predictions, thereby increasing trust and interpretability in cybersecurity decision-making.

Experimental evaluation on benchmark datasets including NSL-KDD, CICIDS2017, CICDDoS2019, and X-IIOTID demonstrated that the proposed hybrid model significantly outperformed standalone baseline algorithms, achieving 99.90% accuracy on NSL-KDD and 100% accuracy on the remaining datasets. The successful deployment of the framework through a Flask-based web interface validated its real-time applicability in operational environments. Overall, the proposed approach offers a scalable, interpretable, and high-performance solution for proactive cyber-attack prediction, making it highly suitable for next-generation intelligent cybersecurity defense systems.

6. FUTURE SCOPE

Future enhancements to the proposed framework can focus on integrating more advanced learning

paradigms such as adversarial learning, transformer-based architectures, and multimodal deep learning models to improve resilience against sophisticated and previously unseen cyber threats. Incorporating online and continual learning mechanisms can enable the system to adapt dynamically to evolving attack patterns without requiring complete retraining, thereby supporting real-time model updates in rapidly changing threat environments. Further experimentation on larger real-world streaming network datasets can also strengthen the generalization capability of the framework across practical deployment scenarios.

In addition, lightweight model optimization and edge deployment strategies can be explored to enable faster inference in resource-constrained environments such as IoT and edge security devices. Future work may also enhance the explainability module by integrating advanced visualization and interactive explanation techniques for deeper analyst insight into prediction reasoning. Integration with Security Information and Event Management (SIEM) platforms, automated threat response systems, and cloud-based monitoring infrastructures can further transform the framework into a comprehensive real-time intelligent cybersecurity defense platform.

REFERENCES

[1] Ajala, O. A., Okoye, C. C., Ofodile, O. C., Arinze, C. A., & Daraojimba,
O. D. (2024). Review of AI and machine learning applications to predict and Thwart cyber-attacks in real-time. Magna Scientia Advanced Research and Reviews, 10(1), 312-320.

[2] Nadella, G. S., & Gonaygunta, H. (2024). Enhancing cybersecurity with artificial intelligence: Predictive techniques and challenges in the age of IoT. International journal of science and engineering applications, 13(04), 30-33.

[3] Arif, A., Khan, M. I., Khan, A. R. A., Anjum, N., & Arif, H. (2025). AI-
Driven Cybersecurity Predictions: Safeguarding California's Digital Landscape. International Journal of Innovative Research in Computer Science and Technology, 13, 74-78.

[4] Raza, A., Ali, A. K. S., & Hussain, A. A. (2024). AI-DRIVEN APPROACHES TO CYBER AND INFORMATION SECURITY: MACHINE LEARNING ALGORITHMS FOR THREAT PREDICTION
AND ANOMALY DETECTION. Spectrum of Engineering Sciences, 2(4), 565-573.

[5] Rahman, M. K., Dalim, H. M., & Hossain, M. S. (2023). AI-Powered solutions for enhancing national cybersecurity: predictive analytics and threat mitigation. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence, 14(1), 1036-1069.

[6] Chen, Q., Li, D., & Wang, L. (2024). The Role of Artificial Intelligence in Predicting and Preventing Cyber Attacks. Journal of Industrial Engineering and Applied Science, 2(4), 29-35.

[7] Khalaf, M. A., & Steiti, A. (2024). Artificial intelligence predictions in cyber security: Analysis and early detection of cyber attacks. Babylonian Journal of Machine Learning, 2024, 63-68.

[8] Paramesha, M., Rane, N., & Rane, J. (2024). Artificial intelligence, machine learning, and deep learning for cybersecurity solutions: a review of emerging technologies and applications. Machine Learning, and Deep Learning for Cybersecurity Solutions: A Review of Emerging Technologies and Applications (June 6, 2024).

[9] El-Ghoul, M., Al-Qadi, M. H., Abu-Nasser, B. S., & Abu-Naser, S. S. (2025). rtificial Intelligence as a Frontline Defense: Preventing Cyberattacks in a Connected World.

[10] Sankar, S., Dutta, R., & Karmakar, S. (2024, December). Cyber Threat Prediction and Assessment with Machine Learning Approaches. In 2024 IEEE 21st India Council International Conference (INDICON) (pp. 1-6). IEEE.

[11] Karaja, M. B., Elkahlout, M., Elsharif, A. A., Dheir, I. M., Abu-Nasser,
B. S., & Abu-Naser, S. S. (2024). AI-Driven Cybersecurity: Transforming the Prevention of Cyberattacks.

[12] Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Computer Science, 2(3), 173.

[13] Ejjami, R. (2024). Enhancing Cybersecurity through Artificial Intelligence: Techniques, Applications, and Future Perspectives. Journal of Next-Generation Research 5.0.

[14] Lourens, M., Dabral, A. P., Gangodkar, D., Rathour, N., Tida, C. N., & Chadha, A. (2022, December). Integration of AI with the Cybersecurity: A detailed Systematic review with the practical issues and challenges. In 2022 5th International Conference on Contemporary Computing and Informatics (IC3I) (pp. 1290-1295). IEEE.

[15] Raji, A., Olawore, A., Mustapha, A., & Joseph, J. (2023). Integrating Artificial Intelligence, machine learning, and data analytics in cybersecurity: A holistic approach to advanced threat detection and response. World Journal of Advanced Research and Reviews, 20(3), 2005-2024.

[16] Sharma, A., Rani, S., & Shabaz, M. (2025). A comprehensive review of explainable AI in cybersecurity: Decoding the black box. ICT Express.
[17] Gupta, R., & Srivastava, P. (2025). Artificial intelligence and machine learning in cyber security applications. In Cyber Security Solutions for Protecting and Building the Future Smart Grid (pp. 271-296). Elsevier.
[18] Sankaram, M., Roopesh, M., Rasetti, S., & Nishat, N. (2024). A comprehensive review of artificial intelligence applications in enhancing cybersecurity threat detection and response mechanisms. Management, 3(5).
[19] Ozkan-Okay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions. IEEe Access, 12, 12229-12256.
[20] Muheidat, F., Mallouh, M. A., Al-Saleh, O., Al-Khasawneh, O., & Tawalbeh, L. A. A. (2024). Applying AI and Machine Learning to Enhance

Automated Cybersecurity and Network Threat Identification. Procedia Computer Science, 251, 287-294.
[21] Sivakumar, J., Salman, N. R., Salman, F. R., Salimova, H. R., & Ghimire, E. (2025). AI-driven cyber threat detection: enhancing security through intelligent engineering systems. Journal of Information Systems Engineering and Management, 10(19), 790-798.
[22] Sarker, I. H. (2023). Multi-aspects AI-based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview. Security and Privacy, 6(5), e295.
[23] Wickramasinghe, A. (2023). An evaluation of big data-driven artificial intelligence algorithms for automated cybersecurity risk assessment and mitigation. International Journal of Cybersecurity Risk Management, Forensics, and Compliance, 7(12), 1-15.

[24] Prabha, M., Hossain, M. A., Samiun, M., Saleh, M. A., Dhar, S. R., & Al Mahmud, M. A. (2024, December). AI-driven cyber threat detection: Revolutionizing security frameworks in management information systems. In 2024 International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA) (pp. 357-362). IEEE.
[25] Maddireddy, B. R., & Maddireddy, B. R. (2022). Cybersecurity threat landscape: Predictive modelling using advanced AI algorithms. International Journal of Advanced Engineering Technologies and Innovations, 1(2), 270-285.

[26] Dhanushkodi, K., & Thejas, S. (2024). Ai enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation. IEEE access, 12, 173127-173136.

[27] Kamruzzaman, M., Bhuyan, M. K., Hasan, R., Farabi, S. F., Nilima, S. I., & Hossain, M. A. (2024, October). Exploring the Landscape: A Systematic Review of Artificial Intelligence Techniques in Cybersecurity. In 2024 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI) (pp. 01-06). IEEE.
[28] Thapaliya, S., & Bokani, A. (2024). Leveraging artificial intelligence for enhanced cybersecurity: Insights and innovations. Sadgamaya, 1(1), 46-52.
[29] Kaushik, D., Garg, M., Gupta, A., & Pramanik, S. (2022). Application of machine learning and deep learning in cybersecurity: An innovative approach. In An Interdisciplinary Approach to Modern Network Security (pp. 89-109). CRC Press.
[30] Prity, F. S., Islam, M. S., Fahim, E. H., Hossain, M. M., Bhuiyan, S. H., Islam, M. A., & Raquib, M. (2024). Machine learning-based cyber threat detection: an approach to malware detection and security with explainable AI insights. Human-Intelligent Systems Integration, 6(1), 61-90.