International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

Cyber Attack Prediction From Traditional Machine Learning to Generative Artificial Intelligence

Komari Dinesh Kumar
PG Scholar, Department of Computer Science and Engineering, Sree Dattha Institute of Engineering and Science, Sheriguda, Ibrahimpatnam, Hyderabad, Telangana, India – 501510.
Email: komaridineshkumar1@gmail.com

C. Jyothi Sree
Assistant Professor, Department of Computer Science and Engineering, Sree Dattha Institute of Engineering and Science, Sheriguda, Ibrahimpatnam, Hyderabad, Telangana, India – 501510.
Email: jyothikjr@gmail.com

Abstract*— The increasing complexity and frequency of cyber threats necessitate intelligent and proactive security mechanisms capable of accurately detecting and predicting network attacks. This study introduces an advanced AI-driven cyber attack prediction framework developed using the CICIDS2017 dataset, integrating Machine Learning, Deep Learning, Generative AI, and Explainable AI techniques. Comprehensive preprocessing is performed, including removal of missing and duplicate records, label encoding, data normalization, and dimensionality reduction through Principal Component Analysis to improve learning efficiency. Multiple machine learning classifiers, namely Decision Tree, Random Forest, Extra Trees Classifier, Logistic Regression, Gaussian Naïve Bayes, and a hybrid Voting Classifier combining Random Forest, LightGBM, and XGBoost, are evaluated alongside deep learning models such as DNN, CNN, LSTM, CNN–LSTM, and CNN–LSTM–GRU. Generative models, including Variational Autoencoder, Generative Adversarial Network, and DistilGPT2, are employed to generate synthetic attack patterns and strengthen anomaly representation. Experimental evaluation demonstrates that the Voting Classifier achieves the highest performance with 99.6% accuracy, while the LSTM model attains 99.3% accuracy, indicating robust detection across attack categories such as DoS, DDoS, PortScan, Bot, and Infiltration. Model interpretability is ensured using LIME and SHAP. The framework is deployed using Flask, enabling authentication, input processing, visualization, and classification of network traffic as benign or malicious.

Keywords*— Cyber attack prediction, Machine Learning, Deep Learning, Generative AI, Explainable AI, LSTM, Ensemble Learning, Intrusion Detection.

I. INTRODUCTION

The rapid proliferation of digital technologies and the widespread interconnectivity across various sectors have significantly heightened the importance of robust cybersecurity mechanisms. As organizations, governments, and individuals increasingly rely on online platforms for critical operations, the risk and sophistication of cyber threats have grown exponentially. Cyberattacks such as ransomware, phishing, distributed denial-of-service (DDoS) attacks, and data breaches not only disrupt essential services but also result in substantial economic losses and compromise sensitive information [1]. Traditional defense mechanisms, largely reactive in nature, have proven inadequate against the evolving landscape of cyber threats, highlighting the urgent need for intelligent, proactive, and adaptive security solutions [2].

Artificial Intelligence (AI) and its associated domains, including Machine Learning (ML), Deep Learning (DL), Natural Language Processing (NLP), and Generative AI (GenAI), have emerged as transformative tools for enhancing cybersecurity [3,4]. These technologies enable predictive threat intelligence, real-time anomaly detection, and automated mitigation strategies, effectively shifting cybersecurity from reactive defenses to proactive, data-driven protection. Machine learning models can analyze network traffic patterns to detect subtle deviations indicative of intrusions, while NLP-based algorithms are capable of identifying and classifying phishing attempts and malicious communications [3]. Advanced deep learning architectures, such as Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, and hybrid models combining CNNs with LSTM or Transformer mechanisms, have demonstrated high accuracy in detecting complex attack patterns across diverse cybersecurity domains [4]. Moreover, Generative AI models can simulate novel threat scenarios, allowing security systems to anticipate and prepare for previously unseen attack vectors, enhancing resilience against adaptive adversaries [5].

Despite these advancements, challenges remain in the areas of data quality, scalability, model interpretability, and integration with existing infrastructure [6,7]. Explainable AI (XAI) techniques, such as SHAP and LIME, have been increasingly applied to improve transparency and facilitate trust in AI-driven cybersecurity systems, enabling analysts to understand the rationale behind automated predictions [8,9]. Integrating these AI techniques into a practical, real-time framework is essential for developing an end-to-end cybersecurity solution capable of operating in dynamic and high-volume network environments [10].

The primary objective of this project is to design and implement a comprehensive AI-driven cybersecurity system that integrates ML, DL, NLP, and GenAI models for predictive threat detection and mitigation. The system leverages preprocessing, dimensionality reduction, and real-time inference to enhance detection accuracy, optimize

decision-making, and strengthen digital resilience across diverse infrastructures, ensuring proactive protection against evolving cyber threats.

II. Related Work

The increasing reliance on digital infrastructures has made cybersecurity a critical area of research, where artificial intelligence (AI) has emerged as a powerful enabler of predictive and adaptive defense mechanisms. Several studies have emphasized the importance of aligning cybersecurity frameworks with international standards such as ISO/IEC 27000, 27001, and 27002, which provide structured guidelines for information security management and risk mitigation [11]. These standards underscore the need for systematic approaches to protect digital assets, complementing AI-driven solutions for threat detection and prevention.

The integration of AI with cybersecurity has been explored through a variety of machine learning (ML) and deep learning (DL) methodologies aimed at enhancing threat detection, anomaly identification, and predictive analytics [12]. Research highlights that conventional cybersecurity approaches, including signature-based and heuristic methods, struggle to keep pace with the growing sophistication of cyberattacks. Supervised and unsupervised ML models have shown significant potential in analyzing network traffic, identifying malicious patterns, and detecting zero-day exploits [13]. These models benefit from large-scale datasets, which facilitate improved accuracy and reduced false positive rates, thereby enabling more proactive defense mechanisms.

Anomaly detection and predictive analysis have become key areas where AI can contribute to cybersecurity. The use of ML algorithms, such as Decision Trees, Random Forests, and Support Vector Machines, allows for the classification of normal versus abnormal network behavior, aiding in early threat identification [14]. These techniques provide the foundation for predictive cybersecurity, where future threats can be anticipated based on historical patterns. Furthermore, hybrid approaches combining ML with DL architectures, such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, enhance the detection of complex attack signatures, particularly in large-scale IoT and enterprise networks [16,17].

Explainable AI (XAI) has emerged as an essential component in AI-driven cybersecurity to address the transparency and interpretability challenges of black-box models. Techniques such as SHAP and LIME enable analysts to understand model decisions, highlight feature importance, and facilitate trust in automated threat predictions [15]. However, research has also shown that XAI methods are susceptible to adversarial black-box attacks, which can manipulate model explanations and compromise cybersecurity defenses [20]. These findings indicate that while XAI enhances usability and trust, additional safeguards are required to maintain robustness against malicious interference.

Deep learning-based network anomaly detection has received particular attention in recent studies, as it allows for capturing temporal dependencies and intricate patterns within network traffic data [18]. Models such as CNNs, LSTMs, and hybrid CNN-LSTM architectures have demonstrated superior performance in identifying advanced persistent threats (APTs) and botnet activities, outperforming traditional ML approaches in both accuracy and scalability. These models are particularly effective when coupled with real-time data processing pipelines, enabling immediate detection and response to evolving cyber threats.

Cybersecurity threats in cloud environments have also been extensively investigated, as cloud adoption introduces additional attack surfaces and data privacy concerns [19]. AI-driven monitoring and predictive analytics in cloud infrastructures have been shown to detect anomalies, policy violations, and unauthorized access events, thereby improving the resilience of cloud services. Integrating AI models with continuous learning mechanisms ensures that defense systems can adapt to new and evolving attack strategies while maintaining high efficiency and minimal latency.

III. Materials And Methods

The proposed system leverages a combination of Machine Learning (DT, RF, LR, Naive Bayes, Voting Classifier), Deep Learning (DNN, CNN, LSTM, CNN+LSTM, CNN+LSTM+GRU), and Generative AI models (VAE, GAN, DistilGPT2) to enhance cybersecurity through predictive intelligence. Using the CICIDS2017 dataset, the system incorporates data preprocessing, normalization, and PCA-based dimensionality reduction to improve computational efficiency and feature relevance. Explainable AI tools, including LIME and SHAP, are integrated to enhance transparency and interpretability, allowing users to understand feature importance and model reasoning [22,25]. Deep learning architectures, particularly CNN and LSTM hybrids, facilitate detection of subtle and evolving attack patterns, while Generative AI models simulate novel threat scenarios for proactive intrusion prediction [21]. The system is deployed via a Flask-based web interface, enabling real-time data input, model inference, and visualization. This end-to-end framework offers a scalable, adaptive, and interpretable cybersecurity solution capable of mitigating complex and emerging cyber threats effectively.

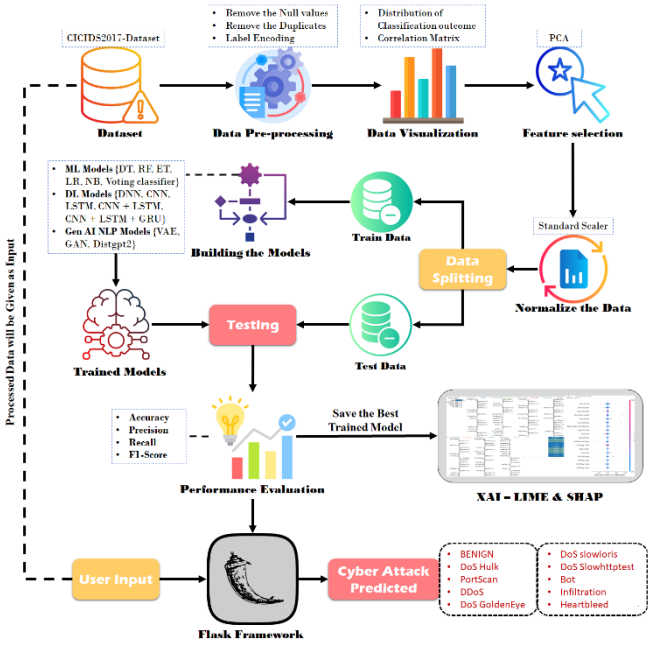


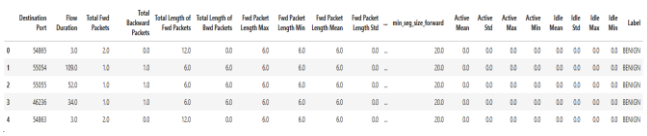
Fig. 1. System Architecture

Figure 1 presents a cyberattack prediction framework, starting with CICIDS2017 data, followed by preprocessing,

visualization, and PCA-based feature selection. After normalization and data splitting, ML and DL models are trained, evaluated, and deployed through a Flask framework for user-based prediction purposes.

A) Dataset Collection:

The dataset used in this study is the CICIDS2017 dataset, which provides comprehensive network traffic captures for various cyber-attack scenarios, including DoS, DDoS, PortScan, Botnet, Infiltration, and Heartbleed, alongside benign traffic. It contains 2,214,469 instances across 79 features, encompassing flow statistics, packet lengths, inter-arrival times, and flag counts, allowing detailed analysis of network behavior. The dataset is well-suited for evaluating predictive cybersecurity models due to its diversity, high-quality labeling, and representation of both common and sophisticated attacks. The substantial class imbalance, particularly between benign and rare attack types, necessitates careful preprocessing and feature engineering for effective model training. CICIDS2017 serves as a benchmark for AI-driven intrusion detection and anomaly detection research [23].



	Destination Port	Flow Duration	Total Fwd Packets	Total Backward Packets	Total Length of Fwd Packets	Total Length of Bwd Packets	Fwd Packet Length Max	Fwd Packet Length Min	Fwd Packet Length Mean	Fwd Packet Length Std	...	min_seg_size_forward	Active Mean	Active Std	Active Max	Active Min	Idle Mean	Idle Std	Idle Max	Idle Min	Label
0	54865	3.0	2.0	0.0	12.0	0.0	6.0	6.0	6.0	0.0	...	20.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	BENIGN
1	55054	109.0	1.0	1.0	6.0	6.0	6.0	6.0	6.0	0.0	...	20.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	BENIGN
2	55055	52.0	1.0	1.0	6.0	6.0	6.0	6.0	6.0	0.0	...	20.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	BENIGN
3	46236	34.0	1.0	1.0	6.0	6.0	6.0	6.0	6.0	0.0	...	20.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	BENIGN
4	54863	3.0	2.0	0.0	12.0	0.0	6.0	6.0	6.0	0.0	...	20.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	BENIGN

Fig.2 Dataset Collection

B) Pre-processing:

Data preprocessing is a critical step in preparing raw network traffic data for AI-driven cybersecurity analysis. It ensures data quality, consistency, and reliability by handling missing values, eliminating duplicate entries, and converting categorical labels into numerical format. Effective preprocessing enhances model accuracy, reduces computational overhead, and enables robust detection of subtle and evolving cyber-attack patterns.

i) Data Preprocessing: The data processing workflow begins by removing null values to prevent incomplete or inconsistent records from affecting model performance. Duplicate entries are eliminated to avoid bias and redundancy in the dataset. Label encoding is applied to convert categorical attack types into numerical values, facilitating compatibility with machine learning and deep learning algorithms. Additional normalization and scaling steps ensure that feature magnitudes are standardized, improving convergence and stability during training. By systematically cleaning and transforming the dataset, the preprocessing pipeline ensures high-quality, structured input suitable for AI models, enabling accurate and efficient detection and classification of cyber threats.

ii) Data Visualization: Data visualization provides insights into network traffic patterns and the distribution of different cyber-attack types. Visualization of the classification outcomes highlights class imbalances, revealing the dominance of benign traffic relative to rare attack categories such as Infiltration or Heartbleed. Correlation matrices are generated to identify dependencies and relationships between features, helping to detect multicollinearity and redundant attributes. Graphical representations, such as histograms, box plots, and heatmaps, facilitate intuitive understanding of feature distributions and outliers. These visual insights guide feature engineering, selection, and model design, ensuring that predictive algorithms focus on the most relevant attributes for accurate and efficient threat detection.

iii) Feature Selection: Feature selection is employed to reduce dimensionality, enhance computational efficiency, and improve model interpretability. Principal Component Analysis (PCA) is applied to transform the original high-dimensional feature space into a set of uncorrelated principal components that capture the majority of variance in the data. By selecting components that explain the most significant variance, PCA mitigates redundancy and noise while retaining critical information for attack detection. This dimensionality reduction accelerates training, reduces overfitting, and improves generalization across unseen data. Feature selection ensures that AI models focus on the most informative attributes, leading to more robust, scalable, and accurate cybersecurity predictions.

iv) Normalization: Normalization is an essential preprocessing step to standardize the scale of numerical features, ensuring that all input variables contribute equally to model training. In this study, Standard Scaler normalization is applied to transform each feature such that it has a mean of zero and a standard deviation of one. This process is particularly important for algorithms sensitive to feature magnitudes, including neural networks and distance-based classifiers, as it prevents larger-valued features from dominating the learning process. Normalization also accelerates convergence during training by stabilizing gradient updates, reducing the likelihood of exploding or vanishing gradients. By scaling the dataset consistently, normalization enhances model performance, ensures robust learning, and improves the accuracy and stability of AI-driven cyber-attack detection systems.

C) Train & Test:

Splitting data is a fundamental step in building and evaluating predictive cybersecurity models. The CICIDS2017 source is divided into training and testing subsets, commonly using an 80/20 ratio, where most samples support model learning and the remainder enables independent evaluation. This strategy allows algorithms to capture underlying patterns while preserving unseen records for objective assessment. Proper separation reduces overfitting, a condition where learned behavior performs well during learning but degrades on new inputs. Stratified splitting can be applied to preserve class proportions across subsets, which is critical when benign traffic dominates and rare attack categories occur infrequently in practice consistently.

D) Algorithms:

A **Decision Tree** splits data based on feature values to make predictions, representing decisions in a tree structure. In cyber attack prediction, it classifies network traffic as normal or malicious, offering interpretability and insight into key attributes influencing attacks.

$$I\,(i) = 1 - \sum_{i=1}^{k} p_i^2 \qquad (1)$$

Random Forest builds multiple decision trees on random feature subsets, aggregating outputs for robust predictions. In cybersecurity, it handles high-dimensional data, improves accuracy, mitigates overfitting, and identifies key features for reliable intrusion detection.

The Gini Equation given below:

$$Gini = 1 - \sum_{i=1}^{C} (Pi)^2 \qquad (2)$$

Extra Trees introduce additional randomness in tree splits for ensemble learning. In cyber threat detection, they efficiently classify malicious patterns, handle noisy or imbalanced data, and provide fast, accurate predictions while capturing complex feature interactions.

Logistic Regression predicts the probability of classes using a sigmoid function. In cyber attack detection, it identifies malicious network activity, offering interpretability, simplicity, probabilistic outputs, and a baseline for performance benchmarking in cybersecurity analytics.

The equation predicts class probabilities using a logistic sigmoid function.

$$\hat{y}_i = \sigma(w^T x + b) = \frac{1}{1 + e^{-(w^T x + b)}} \qquad (3)$$

Naïve Bayes uses Bayes' theorem assuming feature independence to classify data. In cyber attack prediction, it provides fast, low-cost, and effective traffic classification, performing well with large datasets and supporting real-time intrusion detection.

The formula for Bayes' Theorem is:

$$P(A|B) = \frac{P(B|A).P(A)}{P(B)} \qquad (4)$$

Voting Classifier aggregates predictions from multiple models to improve accuracy and reduce bias. In cybersecurity, it balances precision and recall, leveraging strengths of tree-based learners for stable, robust detection of normal and malicious network activities.

DNNs use multiple layers to learn complex, non-linear patterns in data. In cyber attack prediction, they extract high-level features from network traffic, improving accuracy and detecting sophisticated attacks that traditional models may miss.

CNNs extract spatial features using convolution and pooling layers. In cyber attack detection, they capture local correlations in network data, reduce manual feature engineering, and efficiently identify hidden patterns and anomalies in high-dimensional cybersecurity datasets.

The following equation represents the core operation in CNNs.

$$S(i,j) = \sum_m \sum_n I(i+m, j+n) \cdot K(m,n) \qquad (5)$$

LSTMs model long-term dependencies in sequential data via memory cells and gates. In cyber attack prediction, they capture temporal patterns in network traffic, improving accuracy and detecting evolving threats in time-series behaviors.

The equation below represents the hidden state update in LSTM.

$$h_t = \sigma(w_o \cdot [h_{t-1}, x_t] + b_o) \cdot \tanh(C_t) \qquad (6)$$

This **hybrid** combines CNN spatial feature extraction with LSTM temporal modeling. It enhances detection of sophisticated cyber attacks by learning both local patterns and sequential dependencies, offering improved accuracy and contextual understanding.

$$y = Softmax\left(W_o.LSTM\left(MaxPool\left(f(W_c.X_{i:i+k-1} + b_c)\right)\right) + b_o\right) \qquad (7)$$

Combining **CNN, LSTM, and GRU**, this hybrid captures spatial and temporal patterns efficiently. GRU reduces complexity while maintaining performance, enabling precise, adaptive detection of complex, evolving cyber threats in network data.

VAE encodes data into a latent space and reconstructs it, learning distributions. In cybersecurity, it supports anomaly detection and simulates novel attack patterns, enhancing resilience and adapting models to unseen threats.

GANs consist of a generator and discriminator trained adversarially. In cyber attack prediction, they generate realistic attack scenarios for training, improving detection of rare or zero-day attacks and strengthening adaptive threat intelligence.

DistilGPT2 is a compact transformer model for text and sequential data. In cybersecurity, it analyzes logs, alerts, and reports to detect intrusion patterns, offering fast, scalable, and context-aware threat intelligence for real-time anomaly detection.

E) Integration of XAI & Flask:

Explainable AI (XAI) is integrated into the proposed cybersecurity system using LIME and SHAP to enhance transparency and interpretability of model predictions. LIME (Local Interpretable Model-Agnostic Explanations) provides local approximations of complex model behavior, highlighting feature contributions for individual predictions, while SHAP (SHapley Additive exPlanations) quantifies the impact of each feature globally across the dataset. This combination enables security analysts to understand why a specific network flow is classified as malicious or benign, ensuring trust and accountability in AI-driven intrusion detection systems.

The Flask framework is employed to develop a web-based interface for real-time interaction with the AI models. It allows users to input live network data, trigger model inference, and visualize results, including XAI-generated explanations. The lightweight and modular architecture of Flask ensures seamless deployment, rapid prototyping, and easy integration of preprocessing, predictive analytics, and

interpretability features into an end-to-end cybersecurity platform.

IV. Experimental Results

Accuracy: The accuracy of a test is its ability to differentiate the patient and healthy cases correctly. To estimate the accuracy of a test, we should calculate the proportion of true positive and true negative in all evaluated cases. Mathematically, this can be stated as:

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \quad (8)$$

Precision: Precision evaluates the fraction of correctly classified instances or samples among the ones classified as positives. Thus, the formula to calculate the precision is given by:

$$Precision = \frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}} \quad (9)$$

Recall: Recall is a metric in machine learning that measures the ability of a model to identify all relevant instances of a particular class. It is the ratio of correctly predicted positive observations to the total actual positives, providing insights into a model's completeness in capturing instances of a given class.

$$Recall = \frac{TP}{TP + FN} \quad (10)$$

F1-Score: F1 score is a machine learning evaluation metric that measures a model's accuracy. It combines the precision and recall scores of a model. The accuracy metric computes how many times a model made a correct prediction across the entire dataset.

$$F1\ Score = 2 * \frac{Recall\ X\ Precision}{Recall + Precision} * 100 \quad (11)$$

Table.1 Performance Evaluation

ML Model	Accuracy	Precision	Recall	F1-Score
DT	0.996	0.996	0.996	0.996
RF	0.996	0.996	0.996	0.996
ETC	0.996	0.996	0.996	0.996
LR	0.907	0.908	0.907	0.904
GNB	0.304	0.900	0.304	0.382
Voting (RF + LGBM + XGB)	0.996	0.996	0.996	0.996
DNN	0.980	0.980	0.980	0.980
CNN	0.980	0.981	0.980	0.980
LSTM	0.993	0.993	0.993	0.993
CNN + LSTM	0.990	0.990	0.990	0.990
CNN + LSTM + GRU	0.981	0.982	0.981	0.981

Table 1 presents the performance metrics of various ML and DL models, showing accuracy, precision, recall, and F1-score.

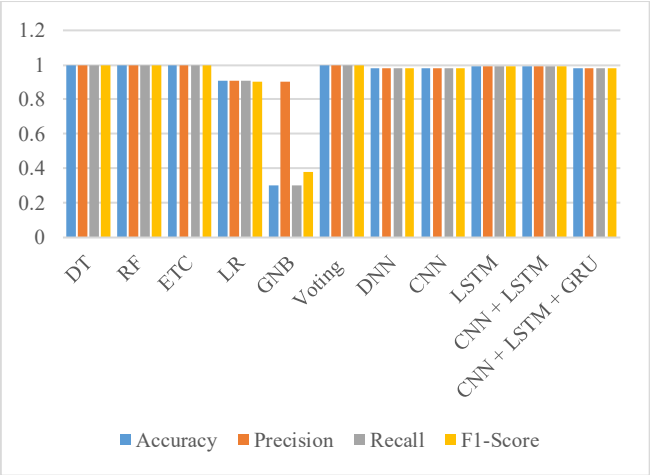


Fig.3 Comparison Graph

This Figure 3 bar chart compares the Accuracy (blue), Precision (orange), Recall (grey), and F1-Score (yellow) for various classification models.

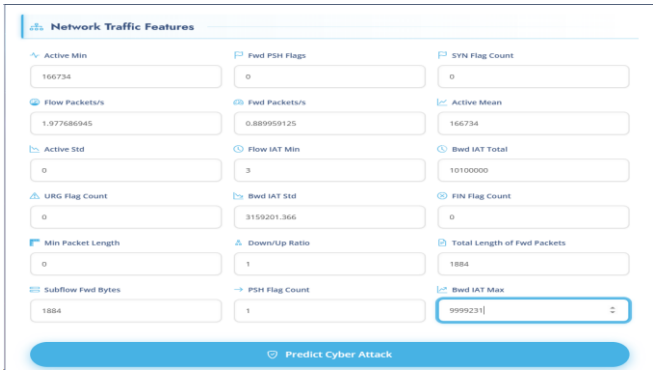


Fig.4 Upload Input Data

This Figure 4 shows the input screen used to enter network traffic feature values for final cyber-attack prediction analysis.



Fig.5 Predict Result

This Figure 5 shows the final output result is "BENIGN" (SAFE), with a 100.0% confidence score, indicating normal network traffic.

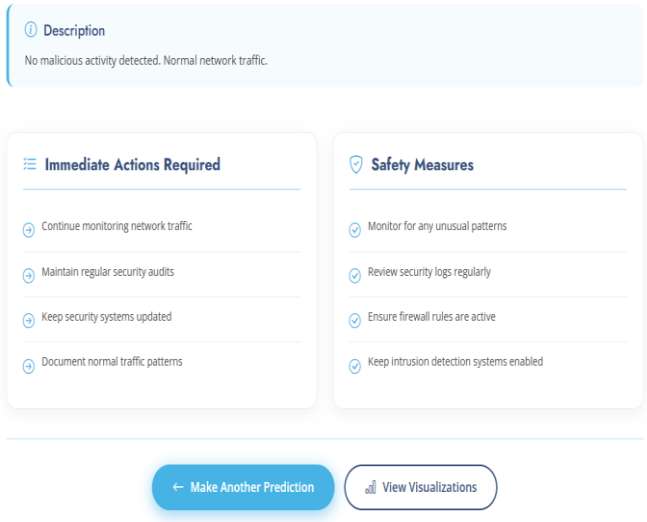


Fig.6 Immediate Actions & Safety Measures

This Figure 6 displays the Immediate Actions Required (e.g., monitoring, audits) and Safety Measures (e.g., firewall rules, intrusion detection) for the predicted network status.

V. Conclusion

The developed AI-driven cybersecurity framework effectively bridges advanced algorithmic intelligence with practical cyber threat detection and prediction. Through systematic preprocessing, feature optimization using PCA, and model evaluation across Machine Learning, Deep Learning, and Generative AI paradigms, the system achieved exceptional detection accuracy and interpretability. Among the Machine Learning models, the ensemble Voting Classifier combining Random Forest, LightGBM, and XGBoost demonstrated the highest performance with an accuracy of 99.6%, precision of 99.6%, and recall of 99.6%, reflecting superior generalization and robustness in detecting diverse attack categories. Within the Deep Learning domain, the Long Short-Term Memory (LSTM) model achieved the best performance, with an accuracy of 99.3%, effectively capturing temporal dependencies and complex intrusion patterns. The integration of Generative AI models such as VAE, GAN, and DistilGPT2 further enhanced the capability to simulate synthetic attack scenarios, supporting adaptive cybersecurity intelligence. Explainable AI techniques using LIME and SHAP provided transparency by visualizing feature contributions and model reasoning, ensuring trustworthy and interpretable predictions. The overall outcome validates that combining ensemble-based ML models with sequential DL architectures and interpretability frameworks delivers a highly accurate, explainable, and scalable approach for modern cyber attack prediction and defense automation.

Future advancements aim to evolve the system into adaptive, autonomous cybersecurity frameworks capable of responding to dynamic threats in real time. Integrating online learning and reinforcement learning enables continuous self-updating and resilience. Incorporating transformer architectures such as BERT and GPT enhances contextual threat understanding. Expanding data sources across domains improves generalization. Cloud and edge deployment ensures scalability and low latency. Blockchain-based log management and federated learning further strengthen privacy, integrity, and collaborative defense across distributed cyber infrastructures worldwide networks ecosystems.

References

[1] Ajala, O. A., Okoye, C. C., Ofodile, O. C., et al. (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., et al. (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] Kao, D.-Y., Hsiao, S.-C., & Tso, R. (2019). Analyzing WannaCry ransomware considering the weapons and exploits. In Proc. 21st Int. Conf. Adv. Commun. Technol. (ICACT), pp. 1098–1107.

[7] Bresniker, K., Gavrilovska, A., Holt, J., et al. (2019). Grand challenge: Applying artificial intelligence and machine learning to cybersecurity. Computer, 52(12), 45–52.

[8] Husák, M., Komárková, J., Bou-Harb, E., & Celeda, P. (2019). Survey of attack projection, prediction, and forecasting in cyber security. IEEE Commun. Surveys Tuts., 21(1), 640–660.

[9] Mohamed, N. (2023). Current trends in AI and ML for cybersecurity: A state of-the-art survey. Cogent Eng., 10(2), 1–11.

[10] Chan, L., Morgan, I., Simon, H., et al. (2019). Survey of AI in cybersecurity for information technology management. In Proc. IEEE Technol. Eng. Manage. Conf. (TEMSCON), pp. 1–8.

[11] Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. J. Inf. Secur., 4(2), 92–100.

[12] Li, J. H. (2018). Cyber security meets artificial intelligence: A survey. Frontiers Inf. Technol. Electron. Eng., 19(12), 1462–1474.

[13] Sarker, I. H., Kayes, A. S. M., Badsha, S., et al. (2020). Cybersecurity data science: An overview from machine learning perspective. J. Big Data., 7, 1–29.

[14] Aggarwal, D., Sharma, D., & Saxena, A. B. (2023). Role of AI in cybersecurity through anomaly detection and predictive analysis. J. Informat. Educ. Res., 3(2), 1–12.

[15] Srivastava, G., Jhaveri, R. H., Bhattacharya, S., et al. (2022). XAI for cybersecurity: State of the art, challenges, open issues and future directions. arXiv:2206.03585.

[16] Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-driven cybersecurity: An overview, security intelligence modeling and research directions. Social Netw. Comput. Sci., 2(3), 1–18.

[17] Ucci, D., Aniello, L., & Baldoni, R. (2019). Survey of machine learning techniques for malware analysis. Comput. Secur., 81, 123–147.

[18] Kwon, D., Kim, H., Kim, J., et al. (2019). A survey of deep learning-based network anomaly detection. Cluster Comput., 22(S1), 949–961.

[19] Nafea, R. A., & Almaiah, M. A. (2021). Cyber security threats in cloud: Literature review. In Proc. Int. Conf. Inf. Technol. (ICIT), pp. 779–786.

[20] Kuppa, A., & Le-Khac, N.-A. (2020). Blackbox attacks on explainable artificial intelligence(XAI) methods in cyber security. In Proc. Int. Joint Conf. Neural Netw. (IJCNN), pp. 1–8.

[21] Ahmed, K. D., & Askar, S. (2021). Deep learning models for cyber security in IoT networks: A review. Int. J. Sci. Bus., 5(3), 61–70.

[22] Gerlings, J., Shollo, A., & Constantiou, I. (2020). Reviewing the need for explainable artificial intelligence (xAI). arXiv:2012.01007.

[23] Jaswal, G., Kanhangad, V., & Ramachandra, R. (2021). AI and Deep Learning in Biometric Security: Trends Potential and Challenges. Boca Raton, FL, USA: CRCPress.

[24] Rudin, C. (2018). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. arXiv:1811.10154.

[25] Zhang, Z., Hamadi, H. A., Damiani, E., et al. (2022). Explainable artificial intelligence applications in cyber security: State of-the-Art in research. IEEE Access, 10, 93104–93139.

[26] Bandi, A., Adapa, P. V. S. R., & Kuchi, Y. E. V. P. K. (2023). The power of generative AI: A review of requirements, models, input–output formats, evaluation metrics, and challenges. Future Internet, 15(8).

[27] Babcock, J., & Bali, R. (2021). Generative AI With Python and Tensorflow 2: Create Images, Text, and Music With VAEs, GANs, LSTMs, Transformer Models. Birmingham, U.K.: Packt.

[28] ChatGPT. Accessed: Jun. 22, 2023. [Online]. Available: https://chat.openai.com/

[29] Dall·e. Accessed: Jun. 22, 2023. [Online]. Available: https://openai.com/blog/dall-e-now-available-without-waitlist

[30] Hitaj, B., Gasti, P., Ateniese, G., & Perez-Cruz, F. (2017). PassGAN: A deep learning approach for password guessing. arXiv:1709.00440.