AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 3(2026)

AI-Driven Predictive Cyber Defense Framework Integrating Hybrid Learning Models for Real-Time Intrusion Analysis

M.Sujana Priya Darshini,
Assistant professor, Department of AI,
PYDAH college of engineering, Patavala.
msujana135@gmail.com

V. Raj Kumar
Department of Computer Science and Engineering,
Pydah College of Engineering,
Patavala
rajkumar.vari013@gmail.com

***Abstract*— As cyber assaults are rising in complexity and number, there is a need for sophisticated proactive security measures that can effectively identify and predict the network attacks. The paper suggests the advanced AI based cyber attack prediction system built with CICIDS2017 dataset and based on ML, DL, Generative AI and Explainable AI. The entries are cleaned for missing values and duplicated ones and then labelled and normalized, and Principal Component Analysis is applied to the data to reduce its dimensionality for efficient learning. Different classifiers that rely on ML are applied like Decision Tree, Random Forest, Extra Trees Classifier, Logistic Regression, Gaussian Naive Bayes and a hybrid Voting Classifier (Random Forest, LightGBM and XGBoost). Furthermore, DL models are also employed including deep neural network (DNN), convolutional neural network (CNN), long-short term memory (LSTM), CNN-LSTM and CNN-LSTM-GRU. We employ generative models to generate attack patterns (Variational Autoencoder, Generative Adversarial Network, DistilGPT2) and enhance anomaly representation. Experimental testing indicates that the Voting Classifier achieves 99.6% accuracy, whereas the LSTM model achieves 99.3% accuracy, a good detection rate in all attack categories, such as DoS, DDoS, PortScan, Bot and Infiltration. LIME and SHAP are used to guaranty the model interpretability. It has been implemented in Flask that enables authentication, processing of input, visualization and categorization of network traffic as benign or dangerous.**

"Keywords— Cyber attack prediction, ML, DL, Generative AI, Explainable AI, LSTM, Ensemble Learning, Intrusion Detection."

I. INTRODUCTION

Effective security measures are now more important than ever due to the rapid growth and integration of digital technology and the growing interdependence between various sectors. The magnitude of cyber attacks has grown exponentially and the threat has become more prevalent as businesses, governments and individuals rely more and more on online platforms for critical functions. Ransomware attacks, phishing, DDoS (Distributed Denial of Service) attacks, and data breaches cause critical services to be disrupted, economic losses, and exposure of sensitive data [1]. The prevalent traditional defense mechanisms are mostly reactive and have been shown to be inadequate in the current scenario of an escalating cyber threat, thus highlighting the need for smart, proactive and adaptive security solutions [2].

AI, including its subsets, Machine Learning, Deep Learning, NLP, and Generative AI (GenAI) are transformative technologies that can help strengthen cybersecurity [3,4]. They enable predictive threat intelligence, real-time anomaly detection and automated mitigation techniques, shifting cybersecurity from reacting to protection and taking a data-driven approach. For instance, conventional ML models can analyze the network traffic to detect very slight variations that could signify an intrusion, and NLP-based algorithms can identify and classify phishing attempts, malicious correspondence, and so on [3]. Complex attack patterns in various cybersecurity applications have been successfully identified using some sophisticated DL models, such as CNNs, LSTM networks, and hybrid CNN-LSTM or CNN-Transformer architectures [4]. Additionally, Generative AI models can emulate specific threat scenarios, helping security systems to anticipate and prepare for new attack vectors and making them more resilient against adaptive threats [5].

However, issues in the areas of data quality, scalability, model interpretability and interface with current infrastructure [6,7] still exist. The use of XAI techniques such as SHAP and LIME have been more prevalent to promote transparency and build trust in AI-driven cybersecurity systems, allowing analysts to comprehend the reasoning behind automated predictions [8,9]. These AI techniques are important for the development of an end-to-end cybersecurity solution that can run in real-time and high-volume network environments [10].

The main goal of this project is to develop and demonstrate a holistic AI-based cybersecurity solution using ML, DL, NLP and GenAI models for predictive threat identification and mitigation. The system's ability to process data in advance, reduce its dimensionality and make instant inferences boost detection accuracy, alongside decision making and thus fortifying the digital resilience of numerous infrastructures, anticipating new cyber attacks.

II. RELATED WORK

As digital infrastructures become increasingly vital, cybersecurity is also a primary research focus, and AI has come into the spotlight to create predictive and adaptive protection systems. Other research has emphasized the importance of implementing information security management and risk reduction frameworks grounded in the internationally accepted information security standards, such as ISO/IEC 27000, 27001 and 27002, which provide a structured path for information security management [11]. The standards highlight the need for methodical ways to safeguarding digital resources, together with AI-powered solutions for threat detection and prevention.

Several ML and DL techniques have been researched that can enhance threat detection, anomaly detection, and

predictive analytics [12]. It has been found that conventional cybersecurity methods like signature-based and heuristic techniques are not able to catch up with the escalating sophistication of attacks. With this background, the supervised and unsupervised ML models have demonstrated promising potential in analyzing network data, detecting malicious patterns and identifying zero day attacks [13]. These models are boosted by the use of large-scale datasets, which leads to increased accuracy and lower false positive rates, which in turn enables more proactive protection measures.

In the core of cybersecurity, AI has emerged as an integral part of anomaly detection and predictive analysis, making it a vital component. Using ML techniques such as DT, RF and SVMs, the normal and abnormal network activity can be classified and thus early detection of threats can be achieved [14]. These strategies are the basis of predictive cybersecurity where future risks are predicted on the basis of past patterns. Furthermore, the use of hybrid approaches, combining ML with DL, such as CNN and LSTM networks can enhance the detection of complex threat signatures, particularly in large-scale IoT and business networks [16,17].

Explainable AI (XAI) has been established as a crucial part of AI-enabled cybersecurity to cope with the transparency and interpretability issues of black-box models. SHAP and LIME are methods that can be used to understand the decisions made by a model, highlight the importance of certain features, and create trust in automated threat predictions [15]. On the other hand, research has also shown that XAI techniques are vulnerable to adversarial black-box attacks that alter the explanations given by the model, and thus undermine security measures [20]. Through our results, we show that XAI can enhance usability and trust, but additional protection is needed to safeguard against malicious interference.

Recently, DL-based anomaly detection in network has gained considerable interest due to its ability to learn complicated patterns and temporal correlations from network traffic data [18]. The models like CNN, LSTM, and hybrid CNN-LSTM models have performed better than the classical ML models in detecting advanced persistent threats (APT) and botnets in terms of accuracy and scalability. These models are particularly effective when used alongside real-time data processing pipelines, to identify and respond to new cyber threats as they arise.

These cloud adoption-related characteristics are also observed to introduce attack surfaces and privacy concerns for clouds, thus the cybersecurity challenges have been extensively studied. The use of AI for monitoring and predictive analytics in cloud infrastructures has shown the ability to identify anomalies, policy violations, and unauthorized access, thereby enhancing the security of cloud services. With the continuous learning capabilities of AI models, security systems can evolve and stay up to date with new and ever-changing attack methods without sacrificing efficiency and latency.

III. MATERIALS AND METHODS

The suggested system utilizes an ensemble of ML (DT, RF, LR, Naive Bayes, Voting Classifier), DL (DNN, CNN, LSTM, CNN+LSTM, CNN+LSTM+GRU) and Generative AI (VAE, GAN, DistilGPT2) models for improving cybersecurity thru predictive intelligence. The implementation is done on the CICIDS2017 data set. Data preparation, normalization and PCA-based dimensionality reduction are used to improve the computational efficiency and feature relevance. Use explainable AI techniques like LIME and SHAP to boost transparency and interpretability, allowing users to understand the significance of features and the logic behind the model's decisions. DL-based systems, particularly CNN and LSTM-based systems, help detect subtle and evolving attack patterns, while Generative AI models simulate specific attack scenarios to predict attacks proactively [21,22,25]. The system is deployed through a web interface developed with Flask where data is entered in real-time, and models are inferred and visualized. This all-in-one platform delivers a scalable, adaptive and interpretable cybersecurity solution to effectively manage complex and evolving cyber threats.

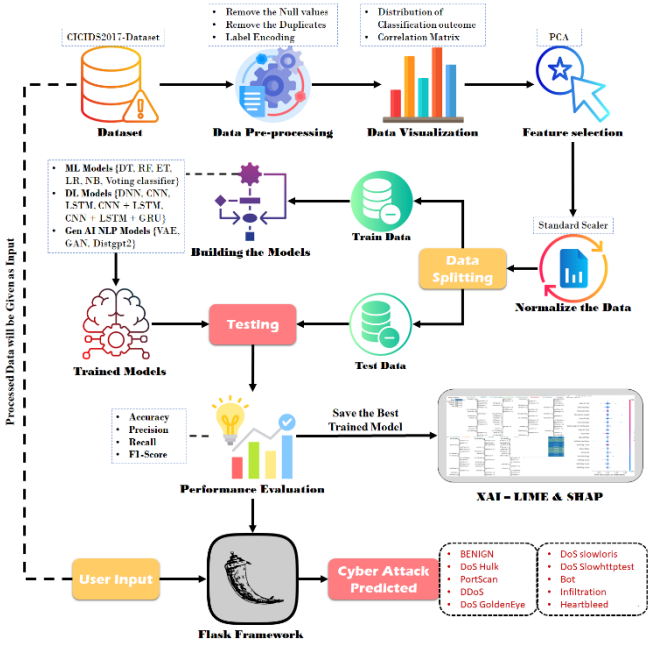


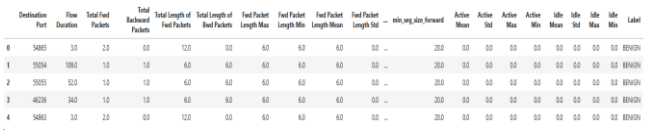
Fig. 1. System Architecture

The framework for prediction of the cyberattack is shown in Figure 1 which starts with the CICIDS2017 data, then the data is preprocessed, visualized and feature selection based on PCA is performed. Once after the data has been standardized and split into training and testing sets, using the help of Flask framework, ML and DL models are trained, tested and deployed to predict for users.

A) Dataset Collection:

In this study, the data set employed is CICIDS2017 dataset, which encompasses huge network traffic captures for various cyber-attack scenarios such as DoS, DDoS, PortScan, Botnet, Infiltration and Heartbleed, as well as benign traffic. It contains 2,214,469 instances and 79 features such as flow statistics, packet lengths, inter-arrival durations and flag counts, which allow for a thorough examination of network behavior. The diversity, quality of labelling and presence of both simple and advanced attacks make the dataset suitable to assess predictive cybersecurity models. However, with the highly skewed distribution of data, particularly in the case of benign and unusual attack types, comprehensive pre-processing and feature engineering are essential for efficient

model training. CICIDS2017 is a standard in research for anomaly detection and intrusion detection using artificial intelligence [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 processing is one of the critical steps in the data preparation pipeline, which is required for AI-powered cybersecurity research, when dealing with raw network traffic data. It handles missing data, removes duplicates, and maps categorical labels to numbers to ensure data quality, consistency, and reliability. Proper preprocessing increases the accuracy of the model, reduces computational load and allows for the identification of sophisticated and dynamic cyber threat patterns.

i) Data Preprocessing: The first step in the data processing workflow is to exclude missing data from the dataset because incomplete or inconsistent data can adversely affect the performance of the model. Redundancy and bias of data was avoided by the duplication of items. Label encoding is used to convert the categorical attack categories into numbers in order to be compatible with ML and techniques used in DL. The following normalization and scaling were applied to the features to normalize their amplitude. This facilitates convergence and stability of training. The preprocessing pipeline refers to a series of systematic processes used to clean and transform the data to ensure high-quality, structured inputs for AI models, enabling accurate and quick identification and categorization of cyber risks.

ii) Data Visualization: Visualization provides a means of understanding the patterns of network traffic and the propagation of a variety of forms of cyber-attacks. The class imbalance is reflected in the visualization of the classification result, which shows that most of the samples are benign traffic while the attack classes (Infiltration and Heartbleed) are minor. To identify dependency and interactions between features, correlation matrix is built that helps identify multicollinearity and duplicate qualities. Histograms, box plots, and heatmaps are graphical ways to help visualize the distributions of features and outliers. These visual insights help feature engineering, feature selection and building models, which ensures that predictive algorithms are directed toward the most relevant features to help identify threats accurately and effectively.

iii) Feature Selection: To enable the reduce the dimensionality of the feature space, to boost the computational efficiency and to boost the interpretability of the model, feature selection is applied on the original high dimensional feature space, and PCA is used to transform the original high dimensional feature space into a low dimensional set of principle components that capture the maximum variance in the data. PCA eliminates redundancy and noise by selecting the components which have maximum variance and preserve the important information to detect attacks. This dimensionality reduction will speed up the training, reduce overfitting and enhance generalization to new data. By selecting the most relevant attributes, feature selection can help AI models to be more powerful, scalable, and accurate in making cybersecurity predictions.

iv) Normalization: Normalisation is an important pre-processing phase, which scales the numerical features into a similar range, giving all numbers the same influence when training a model. In this work, each feature is scaled to have mean 0 and standard deviation 1 using the Standard Scaler. This is particularly important when the algorithm used is sensitive to the magnitudes of the features, for instance, a distance-based classification algorithm where the largest features might be used to determine the class label and a neural network; features with large values may dominate the learning process. Normalization also helps during training by stabilizing the updates of the gradients, enabling faster convergence. This also minimises the risk of exploding or disappearing gradients. Normalization uniformly scales the data set to increase model performance , resilient learning , and accuracy and stability of cyber-attack detection systems based on AI .

C) Train & Test:

Data splitting is an essential component of predictive modeling in cybersecurity, as it ensures privacy and security while preserving the information's integrity. The source for CICIDS2017 is divided into training and testing sets with typically 80% training and 20% testing. This way, algorithms can uncover patterns and remove the records they haven't seen yet to make objective judgments. Well-separated training data minimizes overfitting which occurs when the behavior learned performs well at the time of training, but performs poorly on new data. When benign traffic is predominant and infrequently encountered attack categories in practice, stratified splitting can be used to keep the proportions of the classes the same in the subsets.

D) Algorithms:

Decision Trees represent the decisions as a tree, splitting the data at each node according to a feature value, till a prediction is reached. It forecasts cyber attacks based on identifying whether traffic is normal or malicious and offers interpretability and insights into the most critical factors that fuel cyber attacks.

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

Random Forest generates a lot of DT models on random selections of features and averages the output to get a more robust forecast. In the field of cybersecurity, it works with high dimensional data, enhances accuracy, deals with overfitting and finds important aspects to detect intrusions reliably.

The equation below is the Gini Equation:

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

The splitting strategy of Extra Trees is more random and they are good at classification of harmful patterns, noise or

imbalance data, rapid and accurate prediction and capturing of complex relationships among features.

The LR uses sigmoid function to forecast likelihood of classes. It is used in the detection of cyber attacks to identify suspicious network activity, and offers interpretability, simplicity, probabilistic outputs, and a baseline for performance benchmarks for cyber attack detection.

The equation estimates the class probabilities by logistic sigmoid function.

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

Naïve Bayes is a data classification technique that uses Bayes' Theorem with the assumption that features are independent. For cyber attack prediction is has a very fast, cheap and effective classification of the traffic, performs well on large datasets and allows for real time intrusion detection.

Bayes' Theorem is given by:

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

Voting Classifier is the aggregation of multiple classifiers to improve the accuracy and avoid bias. In terms of cyber security, it will come with a compromise between precision and recall, but uses the power of tree-based learning to effectively identify regular and harmful network events in a consistent and strong way.

Many layers are used to learn complex non-linear models from data in DNNs. They are able to take higher level information from network data and predict cyber attacks, thereby boosting accuracy, and can identify more advanced attacks than can be found with older algorithms.

CNNs utilize convolution and pooling layers to extract the spatial characteristics. For cyber attack detection they are able to identify local correlations in network data without the need for manual feature engineering, and efficiently identify hidden patterns and anomalies in high-dimensional cybersecurity datasets.

The CNN's main operation is the following equation.

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

The LSTM has memory cells and gates that can store the long-term dependencies of sequences. They model the time series trend in network traffic for cyber attack prediction in order to make it more accurate and detect new attacks.

The update of the hidden state in LSTM is given by the following equation .

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

This is a hybrid model that extracts spatial features with CNN and models the temporal features with LSTM. It gives better accuracy and contextual awareness to detect more advanced cyber attacks, by capturing local patterns and sequential dependencies.

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

This CNN-LSTM-GRU hybrid has the capacity to efficiently capture the spatial and temporal patterns. GRU minimizes complexity and preserves performance to enable accurate adaptive detection of complex, changing cyber dangers in network data.

VAE learns distributions via encoding to latent space and reconstruction. In the cyber security area, it aids in identifying anomalies and generates new attack patterns, making systems more resilient and adapting models to threats that have not previously been encountered.

GANs consist of two adversarially trained components: a generator, and a discriminator. In the cyber attack prediction, they create realistic scenarios for training, improving ability to detect unusual or zero-day attacks, enhancing adaptive threat intelligence.

DistilGPT2 is a small transformer based model for text and sequential data. In the field of cybersecurity it examines log files, warnings and reports to find infiltration patterns, providing quick, scalable, context-aware threat intelligence for real-time anomaly identification.

E) Integration of XAI & Flask:

The proposed cybersecurity system is enhanced by incorporating XAI techniques, such as LIME and SHAP, which help increase the transparency and interpretability of model predictions. LIME provides local explanations of the behaviour of complex models, highlighting the importance of features in specific predictions. SHAP measures the effect of each feature globally throughout the dataset. This allows security analysts to understand the reasons behind a certain network flow being labeled malicious or benign, thus increasing confidence and responsibility for AI-based intrusion detection systems.

Building a web interface to communicate with the AI models with Flask.Creating a web interface for communicating with the AI models using Flask. Users can input live network data, run the model and view results including explanations provided by XAI. With its lightweight and modular design, deployments are simple, so is rapid prototyping and implementation of preprocessing, predictive analytics, and interpretability capabilities into an end-to-end cybersecurity platform.

IV. EXPERIMENTAL RESULTS

Accuracy: The accuracy of a test is its ability to correctly identify a patient and healthy cases. To calculate the accuracy of the test, we should calculate the percentages of true positive and true negative for all cases that we tested. Mathematically:

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

Precision: Precision is the ratio of the correctly classified positive samples or instances to all the positive samples or instances classified. Thus the formula to compute the precision is given by:

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

Recall: Recall is a ML measure to evaluate a model's capacity to retrieve all the relevant examples of a particular class. It is the percentage of correct predictions that are positive and gives us an intuitive sense of how comprehensive a model is in capturing the examples of a particular class.

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

F1-Score: In ML, a score statistic that reflects the accuracy of a model is called F1 score. It is a mixture of the precision and recall of a model. The accuracy measure is the percentage of the correct predictions the model made for 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

The results of several ML and DL models (accuracy, precision, recall, and F1-score) are depicted in Table 1.

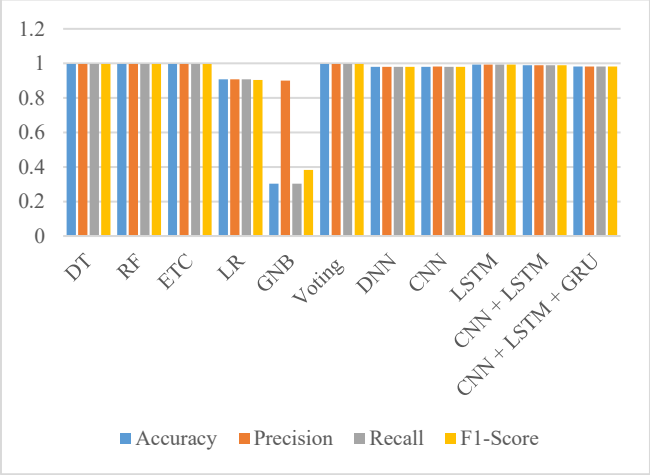


Fig.3 Comparison Graph

Figure 3 shows the comparison of Accuracy (blue), Precision (orange), Recall (grey) and F1-Score (yellow) of the different categorization models using a bar chart.

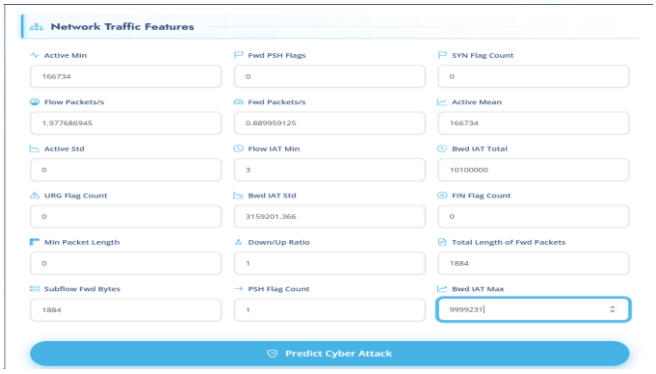


Fig.4 Upload Input Data

The input page for network traffic feature values to be used for the final cyber-attack prediction analysis is shown in Figure 4.

Fig.5 Predict Result

The final output result is "BENIGN" (SAFE) with the confidence score being 100.0 %. This means continuous flow of network traffic. This is a Figure 5 of the invention.

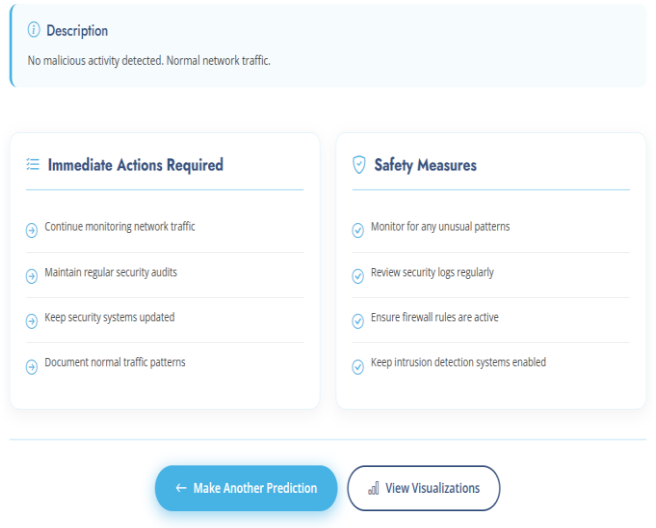


Fig.6 Immediate Actions & Safety Measures

The Immediate Actions Required (such as monitoring, audits) and Safety Measures (such as firewall rules, intrusion detection) are displayed for the network status that is expected.

V. CONCLUSION

The proposed AI cyber security framework is able to seamlessly incorporate the most advanced algorithmic intelligence and practical cyber threat identification and prediction. Systematic data preparation, PCA optimization of features, and assessment of the models within the paradigm of ML, DL and Generative AI, yielded a high detection rate accuracy and interpretability. The ensemble Voting Classifier (RF, LightGBM and XGBoost) achieved the highest accuracy of 99.6%, highest precision of 99.6% and highest recall of 99.6% among the standard ML models, indicating good generalization and robustness to detect different categories of attacks. The LSTM model performed best in the DL domain with an accuracy of 99.3% by capturing temporal correlations and complicated intrusion patterns. Generative AI models such as VAE, GAN and DistilGPT2 significantly boosted the capability to create synthetic attack scenarios for adaptive cybersecurity intelligence. Explainable AI approaches using LIME and SHAP enable transparency by showing the contribution of features and model reasoning to ensure trustable and interpretable predictions. The combined outcome confirms that the fusion of ensemble-based ML models and sequential DL architectures with interpretability frameworks is a valid way to create an accurate, explainable, and scalable approach for automation of modern cyber attacks prediction and defense.

It will eventually turn the system into cybersecurity adaptive, autonomous systems which can respond to dynamic cyber threats in real-time. A mix of on-line and reinforcement learning gives dynamic self-updating and robustness. New transformer models such as BERT and GPT enhance the understanding of threats in context. The more data sources over the domains, the more generalisation can be obtained. Cloud and edge deployment, scalability and less latency, log management and federated learning based on blockchain further enhance the privacy, integrity and collaborative defense of international networks and across distributed cyber infrastructures.

REFERENCES

[1] Ajala, O. A., Okoye, C. C., Ofodile, O. C., et al. (2024). Review of AI and ML 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: ML 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 ML 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 ML 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 ML 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 ML techniques for malware analysis. Comput. Secur., 81, 123–147.

[18] Kwon, D., Kim, H., Kim, J., et al. (2019). A survey of DL-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). DL 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 DL in Biometric Security: Trends Potential and Challenges. Boca Raton, FL, USA: CRCPress.

[24] Rudin, C. (2018). Stop explaining black box ML 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 DL approach for password guessing. arXiv:1709.00440.