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

Research Paper

AN OPTIMIZED CYBER THREAT CLASSIFICATION MODEL USING CHI-SQUARE FEATURE SELECTION AND RANDOM FOREST-BASED HYBRID VOTING

Phaneendra Nath Jakkula,Technology Lead, Dept: CORP IT,HGI HUB CITY TECHNOLOGIES PVT LTD,HYDERABAD,TELANGANA

Email: phaneendra.jakkula@gmail.com

Abstract— The increasing number of cyber threats and sophisticated attack techniques has created a significant demand for intelligent and automated cybersecurity solutions. Traditional threat detection approaches often face challenges in identifying evolving attack patterns and processing large volumes of cybersecurity data. To address these challenges, this paper proposes a hybrid ensemble-based cyber threat detection framework that integrates Chi-Square feature selection, Natural Language Processing (NLP)-driven feature extraction, and machine learning classification techniques. Chi-Square feature selection is employed to identify relevant features and reduce unnecessary attributes, while NLP techniques support the extraction of meaningful information from unstructured cyber threat intelligence data. The selected features are processed using a hybrid ensemble of Decision Tree, Random Forest, and Extra Trees classifiers. An ensemble voting mechanism combines the predictions of individual classifiers to perform binary and multiclass cyber threat classification. Furthermore, Explainable Artificial Intelligence techniques, including SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-agnostic Explanations), are integrated to provide transparency and interpretability by explaining the contribution of individual features to prediction outcomes. The proposed framework achieved 93.75% accuracy for binary classification and 98.96% accuracy for multiclass classification, outperforming individual machine learning models while maintaining transparency in prediction decisions. Finally, a Flask-based web application is developed to provide an interactive interface for dataset uploading and automated threat prediction. The framework aims to improve cyber threat classification through effective feature selection, hybrid ensemble learning, and explainable prediction mechanisms.

Keywords: Cyber Threat Detection, Chi-Square Feature Selection, Natural Language Processing, Hybrid Ensemble Learning, Decision Tree, Random Forest, Extra Trees, Explainable Artificial Intelligence, SHAP, LIME, Flask.

I. INTRODUCTION

The rapid growth of digital technologies, internet connectivity, cloud computing, and interconnected information systems has significantly increased the importance of cybersecurity in modern digital environments. Organizations across various sectors increasingly depend on digital infrastructure to store, process, and exchange sensitive information. However, this growing dependence has also expanded the attack surface, exposing systems to various cyber threats, including Distributed Denial-of-Service (DDoS) attacks, ransomware, malware, phishing, and other sophisticated security attacks. Cybercriminals continuously develop new techniques to exploit system vulnerabilities, making traditional security mechanisms insufficient for identifying and preventing evolving cyber threats. Therefore, intelligent, automated, and real-time cyber threat detection mechanisms are essential for strengthening information security and protecting digital infrastructures.

Traditional cyber threat detection approaches generally depend on predefined rules, static datasets, manual investigation, and conventional machine learning techniques. Although these approaches can identify previously known attack patterns, they often face difficulties in detecting emerging and previously unseen threats. Furthermore, analyzing large volumes of unstructured cybersecurity information manually is time-consuming and may result in delayed threat identification. To overcome these limitations, Artificial Intelligence (AI), Machine Learning (ML), and Natural Language Processing (NLP) techniques have become important approaches for automated cyber threat intelligence analysis. These technologies enable systems to process large amounts of threat-related information, identify hidden patterns, and classify suspicious activities more efficiently.

The existing framework, Real-Time Automated Cyber Threat Classification and Emerging Threat Detection Framework, focuses on collecting and analyzing cyber threat intelligence from different online sources, including surface web platforms, deep web sources, dark web forums, and cybersecurity discussion platforms. NLP techniques are applied to preprocess textual information by performing text cleaning, tokenization, and other preprocessing operations. The processed text is transformed into numerical representations using Bag-of-Words, TF-IDF, and Word2Vec techniques. Furthermore, Latent Dirichlet Allocation (LDA) and Non-negative Matrix Factorization (NMF) are incorporated to identify emerging cyber threat topics and analyze evolving attack patterns. Different machine learning and deep learning algorithms, including

Support Vector Machine (SVM), Random Forest, XGBoost, Naïve Bayes, Convolutional Neural Networks (CNN), and Long Short-Term Memory (LSTM), are utilized for binary and multiclass cyber threat classification.

Although the existing framework provides multiple classification techniques for identifying cyber threats, there is scope for further improvement in feature optimization, prediction reliability, and practical deployment. Processing a large number of features can increase computational complexity and may introduce irrelevant or less informative attributes into the classification process. Similarly, depending on individual classifiers may limit prediction robustness across different attack categories. Therefore, an enhanced feature selection and hybrid ensemble learning approach is introduced to improve the efficiency and reliability of cyber threat classification.

The proposed extension incorporates the Chi-Squared (CHI-Squared) feature selection algorithm to identify the most relevant features from the dataset. This statistical feature selection technique evaluates the relationship between individual features and target classes, helping to eliminate less informative attributes and reduce the dimensionality of the feature space. By selecting important features, the proposed framework aims to reduce unnecessary computational overhead, minimize irrelevant information, and improve the efficiency of the classification process.

Furthermore, a hybrid ensemble classification model is developed by integrating three machine learning algorithms: Decision Tree, Extra Trees, and Random Forest. Each classifier contributes its individual learning capabilities to identify different cyber threat patterns. A voting mechanism is employed to combine the predictions generated by these classifiers and determine the final classification output. This ensemble approach aims to improve prediction consistency, reduce the limitations of individual models, and provide more reliable classification results for both binary classification (normal and attack) and multiclass classification involving DDoS, ransomware, malware, and other cyber threat categories.

In addition to improving the classification methodology, the enhanced framework is deployed through a Flask-based web application to provide an interactive and accessible threat detection environment. Users can upload test datasets through the web interface, allowing the trained hybrid ensemble model to process the input data and generate automated cyber threat predictions. The web application simplifies the prediction process and enables users to access classification results without directly interacting with the underlying machine learning implementation.

Overall, the proposed extension combines NLP-based data preprocessing, CHI-Squared feature selection, hybrid ensemble classification, voting-based prediction, and Flask-based deployment to develop an efficient and intelligent cyber threat detection framework. By integrating these techniques, the system aims to improve feature selection efficiency, enhance classification robustness, reduce computational complexity, and support real-time cyber threat monitoring. The framework provides a practical approach for identifying known cyberattacks and analyzing emerging threat patterns, thereby supporting proactive cybersecurity management and informed security decision-making.

II. LITERATURE SURVEY

[1] Khalaf et al. (2025) presented a study on the development of real-time threat detection systems using artificial intelligence for protecting critical infrastructure. The work focuses on applying AI-driven cybersecurity techniques to identify potential security threats and support continuous monitoring. It highlights the importance of intelligent detection mechanisms in environments where security incidents may affect essential services. The study provides a foundation for developing automated threat detection systems that can respond to changing cyberattack patterns.

[2] Jain and Mitra (2025) investigated the application of machine learning algorithms for real-time threat detection and anomaly identification in cybersecurity. Their work discusses the use of machine learning models, including Random Forest, Support Vector Machine, and Long Short-Term Memory networks, with datasets such as CICIDS2017 and UNSW-NB15. The study emphasizes the importance of identifying abnormal network activities as they occur. It also highlights practical concerns such as processing latency and computational requirements when deploying machine learning models for real-time security applications.

[3] Balasubramanian et al. (2025) proposed a cognitive platform for collecting cyber threat intelligence and performing real-time detection using cloud computing. Their platform focuses on automating the collection and processing of threat information from online sources. The proposed approach uses containerized microservices, focused web crawlers, and automated extraction techniques to identify Indicators of Compromise (IOCs). It also incorporates cloud technologies and data-processing components to support scalable threat intelligence collection and analysis. This research demonstrates the role of cloud-based architectures in building automated CTI systems.

[4] Lahare and Wakchaure (2025) discussed proactive defense through automated cyber threat detection and intelligence, with particular attention to recent developments and implementation challenges. Their work examines the importance of identifying threats before they cause significant damage and the role of automation in improving cybersecurity operations. The study provides an overview of emerging trends in threat detection and intelligence gathering. It also indicates the need to address challenges associated with automated security systems, including the changing nature of attacks and the effective processing of threat information.

[5] Sundaramurthy et al. (2025) explored AI-driven threat detection by applying machine learning approaches to real-time cybersecurity in cloud environments. The study explains how the adoption of cloud computing increases the complexity of security management and expands the potential attack surface. It discusses the application of AI and machine learning for detecting known and emerging threats in cloud infrastructures. The authors also identify important implementation concerns, including data quality, processing overhead, and the need for continuous learning. Their work supports the development of adaptable threat detection solutions for cloud-based systems.

[6] Gautam, Gahlot, and Kamat (2020) presented research on hacker forum exploit identification and classification for proactive cyber threat intelligence. The study focuses on using information available in hacker forums to identify exploit-related content and support early threat awareness. Hacker forums can contain discussions about vulnerabilities, malicious activities, and exploitation techniques that may provide useful information for security analysts. Automated classification of such information can reduce the effort involved in manually examining large volumes of forum content. This work is relevant to systems that collect and classify threat information from online sources.

[7] Admass, Munaye, and Diro (2024) presented a review of the current state of cybersecurity, its major challenges, and possible future research directions. The study discusses the growing importance of cybersecurity as digital technologies become increasingly integrated into personal, organizational, and industrial environments. It explains that continuously changing cyber threats require security mechanisms capable of adapting to new attack methods. The review provides a broad understanding of cybersecurity research and highlights the need for improved approaches to threat prevention, detection, and system protection.

[8] Manjramkar and Jondhale (2023) discussed the application of machine learning techniques in cybersecurity. Their work explains how machine learning can identify patterns in previously observed data and use those patterns to recognize potentially malicious activities. The study considers cybersecurity applications such as intrusion detection, malware identification, and spam detection. Machine learning provides an opportunity to automate the analysis of security-related data and reduce dependence on manually defined detection rules. This research supports the use of classification algorithms for identifying different categories of cyber threats.

[9] Goel, Mansi, and Sethi (2022) presented a survey of progressive techniques and challenges in cyber threat intelligence. The study explains how CTI helps organizations collect and analyze information about cyberattacks, threat actors, Indicators of Compromise, and their Tactics, Techniques, and Procedures. It emphasizes that threat intelligence can support early warning and help security teams understand potential attack activities. The survey also discusses the challenges associated with collecting, analyzing, and using threat information effectively. This work establishes the importance of integrating threat intelligence with automated detection mechanisms.

[10] Silvestri et al. (2023) proposed a machine learning approach for NLP-based analysis of cyber threats and vulnerabilities in the healthcare ecosystem. The research addresses security concerns arising from the increased use of electronic health records, connected medical devices, and healthcare information systems. It highlights the importance of extracting useful information from security-related text to understand vulnerabilities and potential threats affecting healthcare infrastructure. The study demonstrates the relevance of natural language processing and machine learning for analyzing unstructured cybersecurity information in a specific application domain.

[11] Blei, Ng, and Jordan (2003) introduced Latent Dirichlet Allocation (LDA), a probabilistic topic modelling technique used to identify hidden topics within collections of documents. LDA represents each document as a mixture of topics, while each topic is represented through a probability distribution over words. This approach enables the discovery of meaningful themes from large collections of text without requiring every document to be manually categorized. In cybersecurity applications, LDA can be used to group threat-related documents and discover recurring subjects such as malware, vulnerabilities, exploits, and attack techniques. It provides a theoretical foundation for topic discovery in unstructured cyber threat intelligence.

[12] Deliu, Leichter, and Franke (2018) proposed a two-stage hybrid process for collecting cyber threat intelligence from hacker forums using Support Vector Machines and Latent Dirichlet Allocation. Their approach focuses on identifying relevant information from large collections of forum discussions and organizing the extracted content into meaningful topics. The SVM-based classification stage helps distinguish security-related content from irrelevant discussions, while LDA supports the discovery of underlying topics. The research demonstrates how supervised classification and unsupervised topic modelling can be combined to automate the analysis of hacker forum data. This approach is particularly relevant to collecting threat intelligence from unstructured online sources.

[13] Wang et al. (2023) investigated the use of topic modelling techniques to identify and understand cyber threats discussed on Twitter, using the Log4Shell vulnerability as a case study. The study presents a data-driven approach for collecting and analyzing cybersecurity-related social media discussions. It explores topic modelling methods to identify important threat-related themes and examines how these topics change over time. The research demonstrates that social media can provide useful information about emerging vulnerabilities and cybersecurity

incidents. It also shows the value of monitoring topic trends to support early identification of developing threats.

[14] Irshad and Siddiqui (2023) proposed a cyber threat attribution approach using unstructured reports available in cyber threat intelligence sources. Their research focuses on extracting meaningful information from security reports that may be published in different text and document formats. Natural language processing techniques are used to identify important threat-related features, including tactics, techniques, tools, malware, and targeted organizations. The authors introduced Attack2vec, a domain-specific embedding approach, and evaluated machine learning classifiers such as Decision Tree, Random Forest, and Support Vector Machine for cyber threat actor classification. The study demonstrates how NLP-based feature extraction and machine learning can support automated analysis of unstructured threat intelligence reports.

[15] Yang and Lam (2020) developed an automated cyber threat intelligence report classification approach to support early warning of cyberattacks in next-generation Security Operations Centers. Their work addresses the difficulty of manually analyzing the increasing volume of CTI reports generated from different sources. The proposed framework combines document embedding techniques with machine learning classifiers to categorize similar threat reports according to threat types and attack behaviors. The study uses a collection of 25,092 CTI reports from open sources and demonstrates the potential of automated classification for improving the efficiency of threat intelligence analysis. This research is closely related to automated cyber threat classification and early warning systems.

A) Proposed System

To increase classification accuracy, robustness, and efficiency, the proposed study proposes an updated real-time cyber threat detection system that incorporates feature selection and a hybrid ensemble learning approach. Text cleaning, tokenization, stop-word removal, and vectorization are some of the natural language processing procedures used to preprocess cyber threat intelligence data that is gathered from surface, deep, and dark web sources. Then, in order to reduce dimensionality and remove redundant or noisy information that could harm the model's performance, the most relevant textual characteristics are identified using chi-squared feature selection.

A hybrid ensemble model is created using the features that were chosen. This model incorporates Decision Tree, Extra Tree, and Random Forest classifiers. In order to choose the best accurate prediction for binary (normal vs. attack) and multiclass (DDoS, ransomware, malware, etc.) cyber threat categorization, these models are trained concurrently and a voting-based process is used. By integrating the characteristics of various classifiers, this ensemble technique improves prediction stability and identifies both existing and new threats more effectively.

With the suggested system's Flask-based web interface, users can upload test data and get instantaneous threat classification results, enabling real-time applicability. The suggested approach is effective for real-time cyber threat intelligence and emerging attack detection in dynamic cybersecurity contexts because the automated pipeline enables continuous analysis, scalable performance, and adaptive threat monitoring.

B) System Architecture

The proposed system architecture begins with the collection of cyber threat intelligence data from the Cresci dataset, which contains structured and unstructured textual information related to online activities. The collected data undergoes a preprocessing stage that includes noise removal, tokenization, normalization, and stop-word elimination to ensure clean and consistent input. Feature engineering is then performed to extract meaningful representations from the text, followed by feature selection to identify the most relevant attributes. This step reduces dimensionality and enhances learning efficiency by retaining only critical information required for accurate cyber threat classification.

After feature extraction, multiple feature types such as textual features, user-based features, and sentiment features are generated and combined into a unified feature vector. The dataset is then divided into training, validation, and testing subsets to ensure reliable performance evaluation. A fine-tuned classifier is trained using the selected features, enabling effective classification of cyber activities into normal or malicious categories. The system further integrates explainability modules such as SHAP and LIME to provide transparent and interpretable predictions, enhancing trust in the model's decisions. This end-to-end architecture supports scalable, real-time cyber threat detection with robust performance and adaptability to emerging attack patterns.

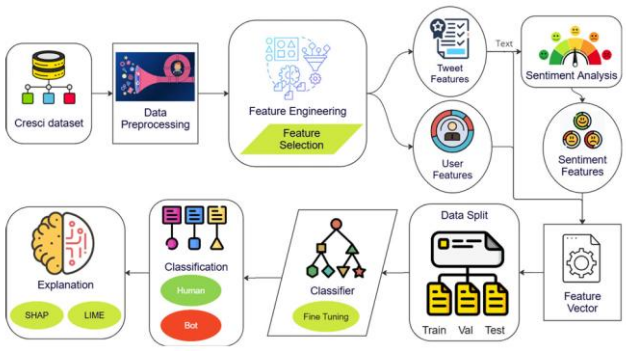

Fig.1. Proposed Architecture

C) MODULES

1. Data Collection Module

This module collects cyber threat intelligence data from datasets such as Cresci, representing information from online platforms relevant to cyber activities and threats.

2. Data Preprocessing Module

Raw textual data is cleaned using NLP techniques such as tokenization, stop-word removal, normalization, and noise filtering to make the data suitable for analysis.

3. Feature Engineering Module

Relevant features are extracted from preprocessed text, including textual features, user-based features, and sentiment-related attributes to capture meaningful threat information.

4. Feature Selection Module

Chi-Squared feature selection is applied to identify the most informative features, reducing dimensionality, eliminating redundancy, and improving classification efficiency.

5. Feature Vector Construction Module

Selected features from different sources are combined into a unified numerical feature vector that represents each data instance effectively.

6. Data Splitting Module

The feature vectors are divided into training, validation, and testing datasets to ensure proper model training and unbiased performance evaluation.

7. Classification Module

A hybrid ensemble classifier combining Decision Tree, Extra Tree, and Random Forest models is trained to perform binary and multiclass cyber threat classification.

8. Fine-Tuning Module

Hyperparameters of the classifiers are optimized to enhance prediction accuracy and robustness across different cyber threat categories.

9. Explainability Module

SHAP and LIME techniques are used to explain model predictions, providing transparency and interpretability for cybersecurity analysts.

10. Deployment Module

The trained model is deployed using a Flask-based web interface, enabling real-time cyber threat detection through user-uploaded input data.

D) ALGORITHMS

1. Chi-Square Feature Selection

Chi-Square feature selection is a statistical method used to identify the most relevant features from a cybersecurity dataset. It examines the relationship between input features and target classes to determine which attributes are more useful for classification. In the proposed system, Chi-Square is applied during the feature selection stage to remove less relevant attributes and retain important information related to cyber threats. This process helps reduce the dimensionality of the dataset, minimizes unnecessary information, and improves the efficiency of subsequent machine learning algorithms.

2. Decision Tree Classifier

Decision Tree is a supervised machine learning algorithm used to classify cybersecurity data based on learned decision rules. It creates a tree-like structure in which different input features are used to make decisions and divide the dataset into smaller groups. Each internal node represents a feature-based decision, while the leaf nodes represent the final classification results. In the proposed system, the Decision Tree classifier analyzes the selected features and identifies whether an input record belongs to normal traffic or a particular cyberattack category. It supports both binary and multiclass threat classification and provides an understandable approach for identifying patterns in cybersecurity data.

3. Extra Trees Classifier

Extra Trees, also known as Extremely Randomized Trees, is an ensemble machine learning algorithm that builds multiple decision trees using randomized feature and splitting strategies. Each tree learns different patterns from the training dataset and independently produces a classification result. The predictions from all trees are combined using majority voting to generate the final output. In the proposed extension, Extra Trees is used to analyze the selected cybersecurity features and identify different types of malicious activities. Its randomized tree construction helps capture diverse patterns in the dataset and reduces dependence on a single decision tree.

4. Random Forest Classifier

Random Forest is an ensemble learning algorithm that combines multiple decision trees to perform classification. Each tree is trained using a different sample of the training data and considers selected features while making decisions. During prediction, all trees generate their individual outputs, and the class receiving the highest number of votes is selected as the final prediction. In the proposed system, Random Forest is used to classify cybersecurity records into normal and attack categories, including different types of cyber threats. It helps identify complex relationships among selected features and provides a reliable classification component within the hybrid ensemble framework.

5. Hybrid Ensemble Voting Classifier

The proposed extension combines Decision Tree, Extra Trees, and Random Forest classifiers through a hybrid ensemble voting mechanism. After Chi-Square feature selection, the selected features are provided to all three machine learning algorithms for independent classification. Each classifier generates its own prediction based on the patterns learned during training. The ensemble voting mechanism combines these individual predictions and selects the class receiving the majority of votes as the final output. This approach reduces dependence on a single classification algorithm and utilizes the different learning capabilities of the three models. The hybrid classifier is designed to support both binary classification of normal and malicious activities

and multiclass identification of different cyber threat categories.

6. Flask-Based Web Application

Flask is used to deploy the trained cyber threat classification framework through a web-based application. It provides an interface through which users can upload cybersecurity datasets and obtain prediction results. Once a dataset is uploaded, the application performs the required preprocessing and applies the trained Chi-Square feature selector to identify the relevant attributes. The selected features are then passed to the trained Decision Tree, Extra Trees, and Random Forest models. Their predictions are combined through the ensemble voting mechanism to determine the final classification. The results are displayed through the web interface, allowing users to examine whether the uploaded records represent normal activity or different categories of cyber threats.

III. EXPERIMENTAL RESULTS

The experimental evaluation was conducted on both binary and multiclass cyber threat datasets to assess the effectiveness of the proposed framework. Multiple machine learning and deep learning algorithms, including Naïve Bayes, Random Forest, XGBoost, CNN, LSTM, and Support Vector Machine (SVM), were implemented and compared using standard performance metrics such as accuracy, precision, recall, and F1-score. The results on the binary dataset demonstrate that SVM achieves strong classification performance among individual classifiers, while the proposed extension hybrid ensemble model outperforms all baseline methods. The hybrid model achieves an accuracy of 93.75% with a high F1-score, indicating improved robustness and reduced misclassification through feature selection and ensemble voting.

For the multiclass dataset, the performance improvement of the proposed approach is even more significant. While traditional models such as Random Forest, XGBoost, and CNN show competitive results, the proposed hybrid ensemble model achieves the highest accuracy of 98.96%, along with superior precision, recall, and F1-score across all threat categories. These results confirm that the integration of Chi-Squared feature selection and hybrid ensemble learning effectively enhances classification accuracy and scalability. Overall, the experimental findings validate the proposed framework's ability to accurately detect and classify both known and emerging cyber threats in real-time environments.

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)

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

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.

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

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

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

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..

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

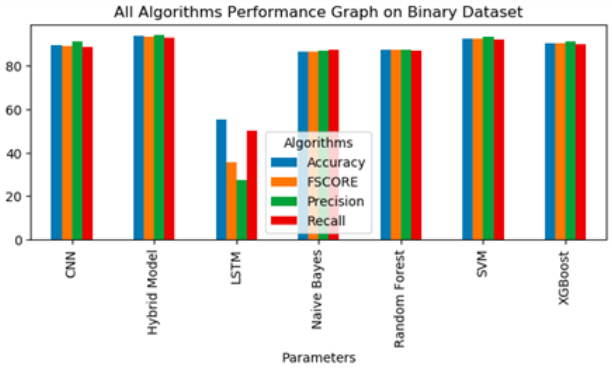

Fig 4 Binary data comparison graph

Dataset	Algorithm Name	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Binary	Random Forest	87.5	87.54	87.14	87.3

Binary	SVM	92.71	93.51	92.08	92.53
Binary	Naïve Bayes	86.46	87.15	87.3	86.46
Binary	XGBoost	90.63	91.33	89.97	90.39
Binary	CNN	89.58	91.19	88.59	89.2
Binary	LSTM	55.21	27.6	50	35.57
Binary	**Proposed Extension Hybrid Model**	**93.75**	**94.33**	**93.24**	**93.61**

Table1: Performance Comparison of Algorithms on Binary Dataset

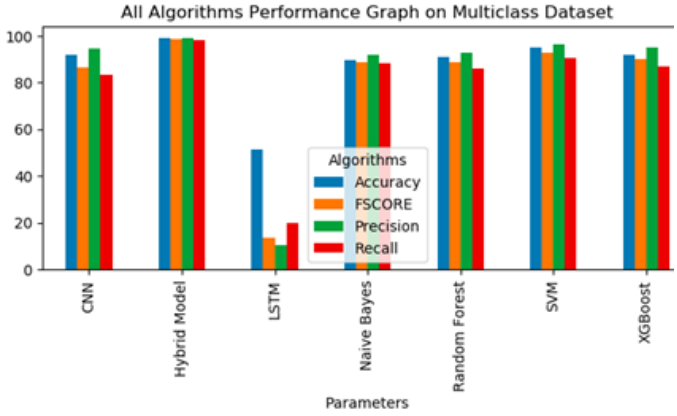

Fig 5 visualizing comparison graph

Dataset	Algorithm Name	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Multiclass	Random Forest	90.63	92.74	85.74	88.55
Multiclass	SVM	94.79	96.24	90.24	92.53
Multiclass	Naïve Bayes	89.58	91.65	88.2	88.75
Multiclass	XGBoost	91.67	95.02	86.7	89.9
Multiclass	CNN	91.67	94.28	83.19	86.2
Multiclass	LSTM	51.04	10.21	20	13.52
Multiclass	**Proposed Extension Hybrid Model**	**98.96**	**98.75**	**98.18**	**98.4**

Table2: Performance Comparison of Algorithms on Multiclass Dataset

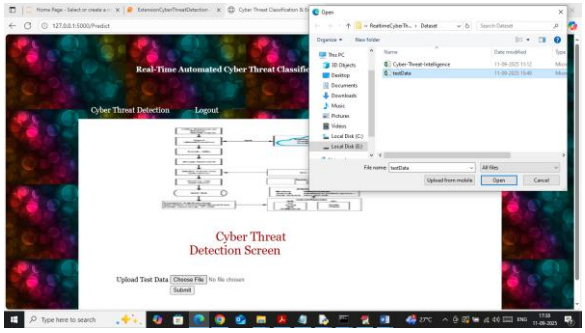

Fig 6 Upload Input Dataset

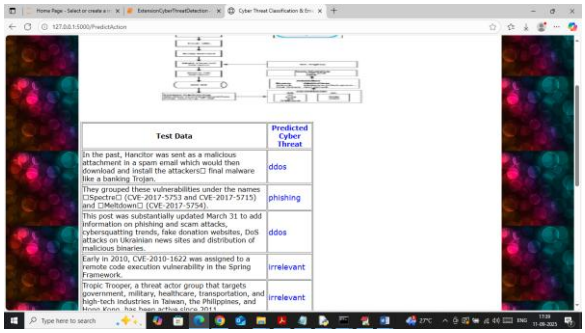

Fig 7 Final Outcome

IV. CONCLUSION

This paper presents a unified hybrid ensemble-based cyber threat detection framework that integrates Chi-Square feature selection, NLP-driven feature extraction, ensemble learning, and Explainable Artificial Intelligence for automated cyber threat classification. The proposed approach utilizes Chi-Square feature selection to identify relevant attributes and eliminate unnecessary features, improving the effectiveness of the classification process. The selected features are processed using Decision Tree, Random Forest, and Extra Trees classifiers, whose predictions are combined through a hybrid voting mechanism to generate the final classification results. The major contribution of this work is the design of an integrated cyber threat detection framework that combines feature optimization, hybrid ensemble learning, explainable artificial intelligence, and web-based deployment capabilities. Experimental results demonstrate that the proposed hybrid voting model achieves 93.75% accuracy for binary classification and 98.96% accuracy for multiclass classification, outperforming the evaluated conventional machine learning and deep learning approaches. Furthermore, SHAP and LIME techniques provide explanations for model predictions by identifying the contribution of individual features, thereby improving the transparency and interpretability of the classification process. The Flask-based web application enables users to upload cybersecurity datasets and obtain automated threat classification results through an interactive interface. Overall, the proposed framework provides an integrated

solution for accurate, interpretable, and efficient cyber threat detection and classification.

v. FUTURE SCOPE

The proposed framework can be further enhanced by incorporating advanced deep learning algorithms to identify complex and previously unseen cyber threat patterns. Additional machine learning models can be integrated into the ensemble architecture to explore improvements in classification performance and generalization. The feature selection process can also be extended by combining Chi-Square with other feature selection techniques to identify more informative cybersecurity attributes. In the future, the framework can be connected to live network traffic sources to support continuous monitoring and real-time threat classification instead of depending only on uploaded datasets. Additional threat categories, such as ransomware, phishing, botnet, malware, and Distributed Denial-of-Service attacks, can be incorporated to expand multiclass classification capabilities. The Flask application can also be improved with interactive dashboards, graphical reports, prediction history, and alert notifications to help users understand detected threats. Furthermore, cloud deployment and integration with Security Information and Event Management systems can be explored to make the framework more scalable and suitable for practical cybersecurity environments.

.

REFERENCES

[1] Khalaf, N. Z., Al Barazanchi, I. I., Radhi, A. D., Parihar, S., Shah, P., & Sekhar, R. (2025). Development of real-time threat detection systems with AI-driven cybersecurity in critical infrastructure. Mesopotamian Journal of CyberSecurity, 5(2), 501-513.

[2] Jain, V., & Mitra, A. (2025). Real-time threat detection in cybersecurity: leveraging machine learning algorithms for enhanced anomaly detection. In Machine Intelligence Applications in Cyber-Risk Management (pp. 315-344). IGI Global Scientific Publishing.

[3] Balasubramanian, P., Nazari, S., Kholgh, D. K., Mahmoodi, A., Seby, J., & Kostakos, P. (2025). A cognitive platform for collecting cyber threat intelligence and real-time detection using cloud computing. Decision Analytics Journal, 14, 100545.

[4] Lahare, P. A., & Wakchaure, M. A. (2025, July). Proactive defense through automated cyber threat detection and intelligence: Latest trends and challenges. In AIP Conference Proceedings (Vol. 3327, No. 1, p. 020023). AIP Publishing LLC.

[5] Sundaramurthy, S. K., Ravichandran, N., Inaganti, A. C., & Muppalaneni, R. (2025). AI-Driven Threat Detection: Leveraging Machine Learning for Real-Time Cybersecurity in Cloud Environments. Artificial Intelligence and Machine Learning Review, 6(1), 23-43.

[6] A. S. Gautam, Y. Gahlot, and P. Kamat, "Hacker forum exploit and classification for proactive cyber threat intelligence," in Proc. Inventive Computation Technol., vol. 98, S. Smys, R. Bestak, and Á. Rocha Eds. Cham, Switzerland : Springer, 2020, pp. 279–285, doi: 10.1007/978-3-030-33846-6_32.

[7] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," Cyber Secur. Appl., vol. 2, 2024, Art. no. 100031, doi: 10.1016/j.csa.2023.100031.

[8] M. A. Manjramkar and K. C. Jondhale, "Cyber security using machine learning techniques," in Proc. Int. Conf. Appl. Mach. Intell. Data Analytics, Dordrecht, The Netherlands, 2023, pp. 680–701, doi: 10.2991/978-94-6463-136-4_59.

[9] N. Goel, A. Mansi, and N. Sethi, "Cyber threat intelligence: A survey on progressive techniques and challenges," in Proc. Int. Conf. Big Data IoT Cyber Sect. Inf. Technol., Pune, India, 2022, pp. 37–41.

[10] S. Silvestri, S. Islam, S. Papastergiou, C. Tzagkarakis, and M. Ciampi, "A machine learning approach for the NLP-based analysis of cyber threats and vulnerabilities of the healthcare ecosystem," Sensors, vol. 23, no. 2, Jan. 2023, Art. no. 651, doi: 10.3390/s23020651.

[11] D. M. Blei, A. Y. Ng, and M. I. Jordan, "Latent Dirichlet allocation," J. Mach. Learn., vol. 3, pp. 993–1022, Jan. 2003.

[12] I. Deliu, C. Leichter, and K. Franke, "Collecting cyber threat intelligence from hacker forums via a two-stage, hybrid process using support vector machines and latent dirichlet allocation," in Proc. 2018 IEEE Big Data, Seattle, WA, USA, 2018, pp. 5008–5013, doi: 10.1109/BigData.2018.8622469.

[13] Y. Wang, M. A. Bashar, M. Chandramohan, and R. Nayak, "Exploring topic models to discern cyber threats on Twitter: A case study on Log4Shell," Intell. Syst. Appl., vol. 20, Nov. 2023, Art. no. 200280, doi: 10.1016/j.iswa.2023.200280.

[14] E. Irshad and A. Basit Siddiqui, "Cyber threat attribution using unstructured reports in cyber threat intelligence," Egyptian Inform. J., vol. 24, no. 1, pp. 43–59, Mar. 2023, doi: 10.1016/j.eij.2022.11.001.

[15] W. Yang and K.-Y. Lam, "Automated cyber threat intelligence reports classification for early warning of cyber attacks in next generation SOC," in Proc. Inf. Commun. Secur., J. Zhou, X. Luo, Q. Shen, and Z. Xu, Eds. Cham, Switzerland : Springer, 2020, vol. 11999, pp. 145–164, doi: 10.1007/978-3-030-41579-2_9..