International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 14, Issue 2, 2026

An Efficient Hybrid Ensemble Model With Feature Selection For Emerging Cyber Threat Detection

Mr. Kudupudi Chakra Hari Duba Raju[1], **Mr. Lakshmi Prasad Amjuri**

[1]M. Tech PG Scholar, Department Of CSE BVC Engineering College, Odalarevu Andhra Pradesh, India.
chakraharik93@gmail.com

[2]Associate Professor , Department Of CSE BVC Engineering College, Odalarevu Andhra Pradesh, India.
lakshmiprasad.anjuri2k14@gmail.com

Abstract: *This work presents an enhanced real-time cyber threat detection framework by integrating feature selection and a hybrid ensemble learning strategy to improve classification accuracy and computational efficiency. Chi-Squared feature selection is applied to identify the most informative textual features from cyber threat intelligence data, effectively reducing dimensionality and noise. The selected features are then used to train a hybrid ensemble model combining Decision Tree, Extra Tree, and Random Forest classifiers, where a voting mechanism ensures robust and reliable prediction for both binary and multiclass cyber threat classification. To support real-time applicability, the proposed system is deployed through a Flask-based web interface, enabling interactive and automated cyber threat analysis on user-provided data. Experimental results demonstrate that the proposed extension significantly enhances detection performance and adaptability, making it effective for identifying both known and emerging cyber threats in dynamic environments.*

Index Terms—Cyber threat detection, feature selection, hybrid ensemble model, voting classifier, real-time monitoring, emerging threats

1. INTRODUCTION

Cyber attacks are more complicated and frequent due to the rapid rise of digital technology and online services, threatening organizational infrastructures and sensitive data. Modern cybercriminals exploit network, application, and online platform vulnerabilities with evolving attack tactics. Thus, traditional security measures and manual threat analysis cannot address the magnitude, speed, and diversity of modern cyber threats. Cyber threat intelligence (CTI) is vital to current cybersecurity, allowing the collecting and analysis of threat-related data from many internet sources.

Unstructured cyber threat intelligence comes from surface online platforms, deep and dark web forums, blogs, and cybersecurity discussion communities. These sources typically reveal new attack methods, malware variants, and zero-day vulnerabilities. Real-time analysis of such textual data is difficult due to its volume and noise. Traditional machine learning methods use static datasets and predetermined features, making them less adaptable to changing threats and less successful in dynamic contexts.

Recent study uses natural language processing and machine learning to automate cyber threat identification. Existing models show promise for known attack types, but they frequently have high-dimensional feature spaces, redundant information, and low real-time robustness. Single-model classifiers may also fail to perform consistently across threat categories, stressing the need for better feature optimization and ensemble-based solutions.

We propose an improved real-time cyber threat detection system that uses Chi-Squared feature selection and hybrid ensemble learning to increase classification accuracy and computing efficiency. By choosing the most informative textual elements, the algorithm eliminates noise and learns crucial threat signs. For binary and multiclass cyber threat classification, the hybrid ensemble model including Decision Tree, Extra Tree, and Random Forest classifiers plus a voting mechanism makes accurate predictions. The framework's Flask-based web interface allows interactive, real-time threat analysis. This comprehensive method helps respond to new cyber threats and make fast, automated cybersecurity decisions.

2. LITERATURE SURVEY

2.1 Towards Continuous Enrichment of Cyber Threat Intelligence: A Study on a Honeypot Dataset

https://m4d.iti.gr/wp-content/uploads/2022/12/Towards-Continuous-Enrichment-of-Cyber-Threat-Intelligence-A-Study-on-a-Honeypot-Dataset_accepted_v02.pdf

Organizations can benefit from Cyber Threat Intelligence because it provides ongoing knowledge on the cyber threat landscape, which helps with decision-making and defense strategy. Honeypots are a popular method of collecting information about potential dangers in this setting. On the other hand, honeypots don't tell you anything about the background, strength, and influence of danger groups. Consequently, we present a method that uses four

ensemble machine learning algorithms applied to security incidents detected using a rule-based method on a deployed honeypot to categorize threats as highly abusive or less abusive according to their behavioral traits. All four models—Adaptive Boosting Classifier (AdaBoost), Random Forest Classifier (RFC), Light Gradient Boosting Machine (LGBM), and Extreme Gradient Boosting (XGBoost)—perform well after parameter prepossessing and hyper-tuning. RFC and LGBM show the best recall (84% and 83%, respectively), while LGBM and XGB have the best area under the curve (91% and 90%, respectively).

2.2 Cyber security: State of the art, challenges and future directions:

https://www.sciencedirect.com/science/article/pii/S2772918423000188

Researchers, academics, and businesses must now devote their whole focus to the urgent matter of cyber security in order to guarantee the confidentiality, integrity, and availability of information systems. Every person and business is vulnerable to ever-evolving cyber threats as a result of the growing need for digitalization. Current circumstances, worldwide trends, and the current state of cyber security are all covered in this article. Our goal in performing this systematic review was to keep up with the ever-changing landscape of cyber security by identifying the most recent trends, issues, and state-of-the-art solutions. In addition, we discuss where cyber security is headed in the future, outlining potential tactics and approaches to deal with the ever-growing cyber security threat landscapes, new trends, and innovations like ML and AI to automate responses to cyber threats. This essay also stresses the significance of stakeholders in the cyber ecosystem working together and continuously adopting new technologies.

2.3 Cyber Security Using Machine Learning Techniques:

https://www.researchgate.net/publication/370424775_Cyber_Security_Using_Machine_Learning_Techniques

A branch of artificial intelligence called machine learning (ML) allows systems to learn from historical data, spot trends, and come to logical conclusions on their own without the need for human assistance. Attacks are detected and countered using modern cybersecurity techniques. Older security techniques are insufficient since thieves can get around common security measures. Cybersecurity protects data, networks, mobile devices, computers, and servers from malicious attacks. The key elements of combining ML and cyber security are enabling and using machine learning to cyber security. With the least amount of human intervention, this union can strengthen cyber security protocols, increase ML model security, and facilitate the efficient detection of zero-day assaults. In this work, we employ ML and cyber security to solve two issues. An overview of ML techniques in cyberspace security is given in this article.

2.4 Cyber Threat Intelligence: A Survey On Progressive Techniques And Challenges:

https://www.researchgate.net/publication/361276941_CYBER_THREAT_INTELLIGENCE_A_SURVEY_ON_PROGRESSIVE_TECHNIQUES_AND_CHALLENGES

Organizations and even individuals are subject to massive cyberattacks in the current digital era by persistent threat actors that attempt to circumvent network and device security and alter sensitive data. In order to mitigate and further lessen the impact of cyberattacks, cyber businesses can obtain information on the attack, its evidence, threat actors, and their tactics, techniques, and procedures (TTP) and indicators of compromise (IOC) by using Cyber Threat Intelligence (CTI). Bridging the security gap involves more than just data protection in the current environment of cyber threats. Furthermore, a person's fundamental right is to have secure access to online content. In order to maintain adequate early warning and threat detection systems, this paper summarizes the state of the art of CTI and the numerous issues that need to be resolved.

2.5 A Machine Learning Approach for the NLP-Based Analysis of Cyber Threats and Vulnerabilities of the Healthcare Ecosystem:

https://pubmed.ncbi.nlm.nih.gov/36679446/

Healthcare systems are becoming more digitally advanced due to the widespread use of electronic health records, linked medical equipment, software, and systems that facilitate effective management and delivery of healthcare services. However, there are now far more cyberthreats in the healthcare industry as a result of the utilization of these technologies. One of the main reasons for the threats and associated risks is vulnerabilities in the legacy and current systems. Ensuring security throughout the entire healthcare ecosystem requires an understanding of and response to the dangers posed by linked medical devices and other components of the ICT health infrastructure. Analyzing threats and vulnerabilities offers a practical means of reducing the impact of hazards associated with current weaknesses. However, this is a difficult process because of the abundance of data that makes it hard to find possible security risk patterns. By using machine learning models, such as the BERT neural language model and XGBoost, to extract updated information from natural language documents that are widely available online and assess the degree of threats and vulnerabilities that have been identified that could

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

affect the healthcare system, this paper helps to effectively analyze threats and vulnerabilities. It also provides the necessary information for the best risk management. The Common Vulnerabilities and Exposures (CVE) vulnerability reports and CS news taken from the Hacker News website served as the basis for the experiments. The outcomes show how well the suggested method works, offering a practical way to evaluate the risks and weaknesses in natural language texts, enabling its implementation in actual healthcare environments.

3. METHODOLOGY

a) Proposed Work:

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:

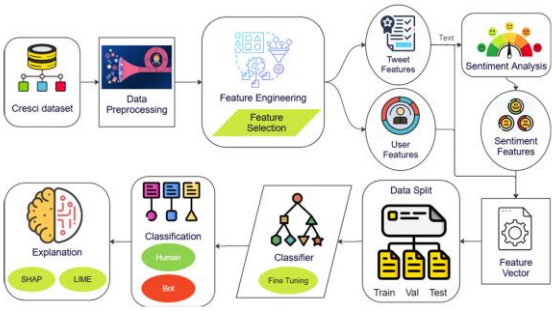

Fig 1 Proposed Architecture

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.

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. Support Vector Machine (SVM)
Support Vector Machine consistently demonstrates high performance across both binary and multiclass datasets, as reflected in the accuracy, precision, recall, and F1-score bars in the graphs. Its ability to construct an optimal separating hyperplane allows it to handle high-dimensional feature spaces efficiently. The strong margin maximization capability makes SVM highly effective for distinguishing complex cyber threat patterns, especially when combined with well-selected textual features.
2. Proposed Extension Hybrid Ensemble Model
The proposed extension hybrid model achieves the highest performance among all evaluated algorithms in both binary and multiclass classification tasks. By integrating Decision Tree, Extra Tree, and Random Forest classifiers through a voting-based ensemble strategy, the model reduces individual classifier bias and variance. The performance graphs clearly show superior accuracy and F1-score, validating the impact of Chi-Squared feature selection and ensemble learning in improving robustness and detection of emerging cyber threats.
3. XGBoost
XGBoost exhibits strong predictive capability, particularly in terms of accuracy and precision, as seen in both datasets. Its gradient boosting mechanism effectively captures complex feature interactions and improves learning efficiency. However, the graphs indicate that while XGBoost performs competitively, it is slightly outperformed by SVM and the proposed hybrid ensemble in overall classification consistency.
4. Random Forest
Random Forest delivers stable and reliable performance across all evaluation metrics, benefiting from the aggregation of multiple decision trees. The graphs show balanced accuracy and recall, making it suitable for handling diverse cyber threat classes. Nevertheless, its performance remains marginally lower than the proposed hybrid ensemble due to limited feature optimization and lack of advanced voting refinement.

5. Convolutional Neural Network (CNN)
CNN achieves reasonable accuracy and precision in both binary and multiclass datasets, indicating its capability to learn abstract feature representations. However, the performance graphs reveal that CNN does not significantly outperform tree-based ensemble models. This suggests that deep learning models may require larger datasets and more complex tuning to achieve optimal performance in textual cyber threat classification.
6. Naïve Bayes
Naïve Bayes provides moderate performance with low computational complexity, making it suitable for baseline comparisons. The graphs indicate acceptable accuracy but reduced precision and recall compared to advanced classifiers. Its strong independence assumptions limit its ability to model complex feature dependencies present in cyber threat data.
7. Long Short-Term Memory (LSTM)
LSTM shows the lowest performance across all evaluation metrics in both datasets, as observed in the graphs. This suggests that sequential modeling is less effective for the given feature representation and dataset size. The results highlight the importance of feature selection and model suitability when applying

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

deep learning techniques to cyber threat intelligence data.

4. 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 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 = TP + TN TP + TN + FP + FN.

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

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.

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

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

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

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.

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

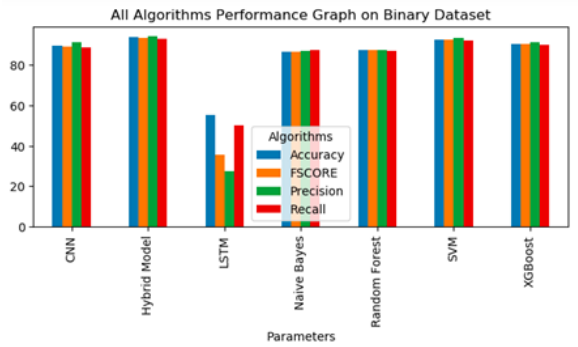

Fig 4 Binary data comparison graph

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

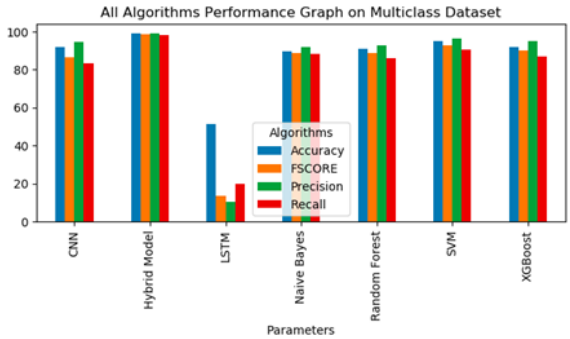

Fig 5 visualizing comparison graph

Dataset	Algorithm Name	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Multiclass	Random Forest	90.63	92.74	85.74	88.55

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

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

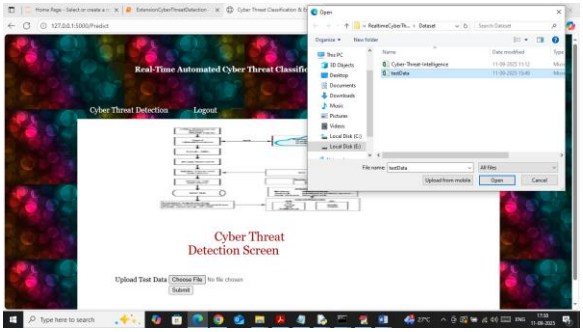

Fig 6 Upload Input Dataset

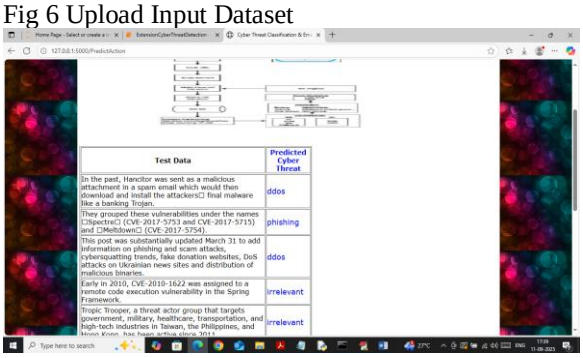

Fig 7 Final Outcome

5. CONCLUSION

This study introduced a framework for automated cyber threat identification and classification in real time, which was improved using a hybrid ensemble learning approach and Chi-Squared feature selection. Classification efficiency and robustness are both enhanced by the suggested addition, which uses a voting mechanism to integrate Random Forest, Decision Tree, and Extra Tree classifiers. The suggested hybrid model achieves a 93.75 percent success rate for binary classification and a 98.96 percent success rate for multiclass classification, according to experimental results on both the binary and multiclass datasets. This surpasses the performance of separate deep learning and machine learning methods.

Deploying the framework using a web interface based on Flask further confirms its practical use for monitoring and analyzing cyber threats in real-time. Enhancing cybersecurity preparedness in dynamic and growing digital settings, the suggested system offers a scalable, accurate, and dependable approach for identifying both known and emerging cyber threats.

6. FUTURE SCOPE

If researchers want to go further into the semantic linkages in cyber threat intelligence data, they can add advanced deep learning architectures like Transformers and attention-based models to the suggested cyber threat detection framework. Further improvement in adaptability can be achieved by integrating online learning methods with real-time streaming platforms. This would allow for continuous model modifications in response to new threat data. Improving detection coverage is another benefit of extending the system to accommodate multilingual threat intelligence analysis from worldwide cyber forums. Deploying the system in cloud or edge environments can further improve response times and support large-scale, distributed cyber threat monitoring.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

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

[5] 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.

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

[7] 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.

[8] Y. Wang, M. A. Bashar, M. Chandramohan, and R. Nayak, "Exploringtopic 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.
[9] 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.
[10] 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.
[11] V. Behzadan, C. Aguirre, A. Bose, and W. Hsu, "Corpus and deep learning classifier for collection of cyber threat indicators in Twitter stream," in Proc. IEEE Big Data, Seattle, WA, USA, 2018, pp. 5002–5007, doi: 10.1109/BigData.2018.8622506.
[12] J. Liu et al., "TriCTI: An actionable cyber threat intelligence discoverysystem via trigger-enhanced neural network," Cybersecurity, vol. 5, no. 1, Dec. 2022, Art. no. 8, doi: 10.1186/s42400-022-00110-3.
[13] N. Dionisio, F. Alves, P. M. Ferreira, and A. Bessani, "Cyberthreat detection from Twitter using deep neural networks," in Proc. 2019 Int. Joint Conf. Neural Netw., Jul. 2019, pp. 1–8, doi: 10.1109/ijcnn.2019.8852475.
[14] R. Basheer and B. Alkhatib, "Threats from the dark: A review over dark web investigation research for cyber threat intelligence," J. Comput. Netw. Commun., vol. 2021, Dec. 2021, Art. no. e1302999, doi: 10.1155/2021/1302999.

Author Profiles:

Mr. KUDUPUDI CHAKRA HARI DUBA RAJU is currently an M.Tech student at Bonam Venkata Chalamayya Engineering College, pursuing a Master's degree in Computer Science and Engineering, He is passionate About Machine Learning, Deep Learning, Robotics, Artificial Intelligence and Cyber security. He is proficient in Java, SELENIUM, and Python.

Mr. Lakshmi Prasad Amjuri is currently serving as an Assistant Professor and Training & Placement Coordinator in the Department of Computer Science and Engineering (C.S.E) and the Training and Placement Department at Bonam Venkata Chalamayya Engineering College, Odalarevu, Amalapuram.

He completed his B.Tech in Computer Science & Engineering from Narasaraopet Engineering college and his M.Tech in Computer Science & Engineering from Prasiddha College of Engineering and Technology.

Mr. Lakshmi Prasad has 17 years of rich teaching experience in Diploma and Engineering education. His research interests include Software Engineering, Software Testing Methodologies, and Quantum Computing.

He has actively attended Faculty Development Programs (FDPs), Seminars and has successfully guided numerous B.Tech and M.Tech student projects.

Email:
lakshmiprasad.anjuri2k14@gmail.com