International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 1 (2026)

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 1, 2026

Peer Reviewed, Referred & Indexed Journal

Research

DETECTING EMERGING CYBER THREATS WITH AN EFFICIENT HYBRID ENSEMBLE MODEL WITH FEATURE SELECTION

DR.J.RAJENDRA PRASAD1, PONNALA HARIKA2, MOHAMMAD JUBEDA3, SHAIK ABDUL SALAM4

#1Head of the information Technology department and professor, NRI Institute Of Technology,Agiripalli
#2#3#4 B.Tech with Specialization of Information Technology in NRI Institute Of Technology,Agiripalli

Abstract: By combining a hybrid ensemble learning approach with feature selection, this study offers a real-time cyber threat detection system that is both more efficient and more accurate in its classifications. By using chi-squared feature selection, we can reduce dimensionality and noise in cyber threat intelligence data and extract the most useful textual features. A hybrid ensemble model is trained using the chosen characteristics. This model combines Decision Tree, Extra Tree, and Random Forest classifiers. Reliable and robust prediction for binary and multiclass cyber threat categorization is ensured via a voting mechanism. Deploying the suggested system through a Flask-based web interface allows for interactive and automatic cyber threat analysis on user-provided data, supporting real-time applicability. The suggested extension is useful for detecting both existing and new cyber threats in dynamic contexts, according to experimental results, which show that it greatly improves detection performance and adaptability.

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

Received: 20-01-2026 Accepted: 24-02-2026 Published: 03-03-2026

1. INTRODUCTION

As a result of the rapid development of digital technology and online services, cyber attacks have become more complex and more frequent. These attacks pose a threat to the infrastructures of organizations as well as sensitive data. Cybercriminals in the modern day take advantage of vulnerabilities in online platforms, applications, and networks by employing ever-evolving attack strategies. Because of this, traditional security measures and manual threat assessments are unable to deal with the quantity, speed, and variety of new cyber threats. Cyber threat intelligence, often known as CTI, is an essential component of modern cybersecurity since it enables the collection and analysis of data linked to threats from a wide variety of online sources. Surface internet platforms, deep and dark web forums, blogs, and cybersecurity discussion communities are the original sources of unstructured cyber threat intelligence. In most cases, these sources disclose new attack tactics, varieties of malware, and vulnerabilities that have not yet been discovered. It is challenging to perform real-time analysis of such textual data because of the volume and noise of the data. The conventional approaches to machine learning make use of fixed datasets and specified characteristics, which renders them less flexible in the face of shifting dangers and less effective in situations that are dynamic.

The identification of cyber threats has been automated through the use of natural language processing and machine learning, according to a recent study. The currently available models

have the potential to be useful for identifying recognized forms of attacks; however, they usually have feature spaces with a high dimension, redundant information, and low real-time robustness. It is also possible for single-model classifiers to fail to perform consistently across different threat categories, which highlights the necessity of improved feature optimization and ensemble-based solutions.

We propose an improved real-time cyber threat detection system that makes use of Chi-Squared feature selection and hybrid ensemble learning in order to improve the accuracy of classification and the efficiency of processing. By selecting the textual bits that contain the most information, the algorithm is able to reduce noise and learn important early warning indications. The hybrid ensemble model, which includes Decision Tree, Extra Tree, and Random Forest classifiers in addition to a voting mechanism, is capable of producing accurate predictions for binary and multiclass cyber threat categorization. The online interface of the framework, which is based on Flask, enables conducting interactive, real-time threat analysis. Using this all-encompassing strategy, one may respond to newly emerging cyber threats and make decisions regarding cybersecurity in a quick and automated manner.

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

In order to give organizations with continual knowledge about the cyber threat landscape, which assists with decision-making and defensive strategy, Cyber Threat Intelligence can be beneficial to organizations. When it comes to gathering information about potential threats in this environment, honeypots are a preferred way of detection. Honeypots, on the other hand, do not provide any information regarding the history, power, or influence of the groups that pose a threat. The result of this is that we offer a method that employs four ensemble machine learning algorithms that are applied to security events that are discovered using a rule-based method on a honeypot that has been deployed. This method classifies threats as either extremely abusive or less abusive depending on the behavioral characteristics that they exhibit. After performing parameter prepossessing and hyper-tuning, each of the four models—Adaptive Boosting Classifier (AdaBoost), Random Forest Classifier (RFC), Light Gradient Boosting Machine (LGBM), and Extreme Gradient Boosting (XGBoost)—achieves satisfactory results in terms of performance capabilities. While RFC and LGBM have the highest recall rates (84 percent and 83 percent, respectively), LGBM and XGB have the highest area under the curve ratings (91 percent and 90 percent, respectively).

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

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

For the purpose of ensuring the availability, integrity, and confidentiality of information systems, researchers, universities, and businesses are now required to dedicate their full attention to the pressing issue of cyber security. As the demand for digitalization continues to rise, every individual and company is susceptible to the ever-evolving cyber risks that are associated with the internet. This article covers a wide range of topics, including the present condition of cyber security, worldwide trends, and contemporary circumstances surrounding cyber security. In order to keep up with the ever-changing environment of cyber security, we decided to conduct this systematic review with the intention of finding the most recent trends, concerns, and solutions that are

considered to be state-of-the-art. In addition, we offer a discussion on the future of cyber security, including prospective strategies and methods to deal with the ever-increasing cyber security threat landscapes, new trends, and advancements like as machine learning and artificial intelligence to automate responses to cyber threats. Additionally, the relevance of stakeholders in the cyber ecosystem working together and consistently adopting new technology is emphasized throughout this essay.

2.3 Cyber Security Using Machine Learning Techniques:

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

Systems are able to learn from previous data, recognize trends, and arrive at logical conclusions on their own without the need for human intervention thanks to a subfield of artificial intelligence known as machine learning (ML). Through the utilization of contemporary cybersecurity strategies, attacks are identified and repelled. Due to the fact that thieves are able to circumvent conventional security measures, older security solutions are insufficient. The protection of data, networks, mobile devices, computers, and servers from hostile attacks is the primary function of cybersecurity. When it comes to merging machine learning and cyber security, the most important aspects are enabling machine learning and applying it to cyber security. This union has the potential to boost cyber security procedures, provide an increase in the security of machine learning models, and assist the efficient detection of zero-day attacks with the least amount of human interaction possible. We use machine learning and cyber security in our effort to find solutions to two problems. Within the scope of cyberspace security, this article provides a summary of machine learning approaches.

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

In the contemporary digital era, organizations and even individuals are vulnerable to major cyberattacks that are carried out by persistent threat actors. These actors attempt to evade network and device security and modify important data; they even target individuals. By utilizing Cyber Threat Intelligence (CTI), cyber enterprises are able to get information regarding the attack, its evidence, threat actors, and their strategies, methods, and procedures (TTP) as well as indicators of compromise (IOC). This allows for the mitigation and further reduction of the impact of cyberattacks. When it comes to the present climate of cyber threats, bridging the security gap requires more than just protecting data. In addition, the right to have safe access to content that is available online is a fundamental right of every individual. This article provides a concise summary of the current state of the art in CTI as well as the numerous problems that need to be overcome in order to ensure that effective early warning and threat detection systems are maintained.

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/

As a result of the widespread adoption of electronic health records, linked medical equipment, software, and other technologies that support the efficient management and delivery of healthcare services, healthcare systems are becoming increasingly technologically advanced. On the other hand, as a consequence of the employment of these technologies, the healthcare industry is currently facing a significantly increased number of cyberthreats. The vulnerabilities that exist in both the legacy and the present systems are one of the primary reasons for the threats and the dangers that are

linked with them. To ensure the safety of the overall healthcare ecosystem, it is necessary to have an awareness of the threats that are posed by connected medical devices and other components of the information and communication technology (ICT) health infrastructure, as well as a reaction to such threats. The act of doing a threat and vulnerability analysis provides a realistic method for mitigating the effects of the risks that are connected with existing vulnerabilities. On the other hand, this is a challenging process because there is a large amount of data, which makes it nearly impossible to identify potential security risk trends. This paper contributes to the effective analysis of threats and vulnerabilities by employing 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. Additionally, the paper evaluates the degree of threats and vulnerabilities that have been identified that have the potential to affect the healthcare system. In addition to this, it offers the information that is required for the most effective risk management. For the purpose of the experiments, the Common Vulnerabilities and Exposures (CVE) vulnerability reports and computer security news that were obtained from the Hacker News website served as the foundation. A practical technique to evaluate the risks and weaknesses in natural language texts is provided by the results, which enables the method to be used in actual healthcare settings. The results demonstrate how well the suggested method works.

3. METHODOLOGY

a) Proposed Work:

An updated real-time cyber threat detection system that integrates feature selection and a hybrid ensemble learning approach is proposed in the study that is being proposed. The purpose of this system is to improve classification accuracy, robustness, and efficiency. Text cleaning, tokenization, stop-word removal, and vectorization are some of the natural language processing processes that are utilized in the preprocessing of cyber threat intelligence data that is obtained from sources on the surface, deep web, and dark web. Following this, the most pertinent textual features are selected through the use of chi-squared feature selection in order to facilitate the reduction of dimensionality and the elimination of redundant or noisy information that may have an adverse effect on the performance of the model.

Utilizing the features that were selected, a hybrid ensemble model is designed and constructed. The Decision Tree, Extra Tree, and Random Forest classifiers are all incorporated into this version of the model. These models are trained concurrently, and a voting-based procedure is utilized, in order to select the most correct forecast for binary (normal versus attack) and multiclass (DDoS, ransomware, malware, etc.) cyber threat categorization. This facilitates the selection of the most accurate prediction. This ensemble technique increases prediction stability and identifies both existing and emerging threats more effectively. It does this by blending the properties of a number of different classifiers.

Real-time applicability is enabled by the Flask-based web interface of the proposed system, which allows users to upload test data and obtain instantaneous threat classification results. Due to the fact that the automated pipeline offers continuous analysis, scalable performance, and adaptive threat monitoring, the solution that has been presented is effective for real-time cyber threat intelligence and emerging attack detection in dynamic cybersecurity scenarios.

b) System Architecture:

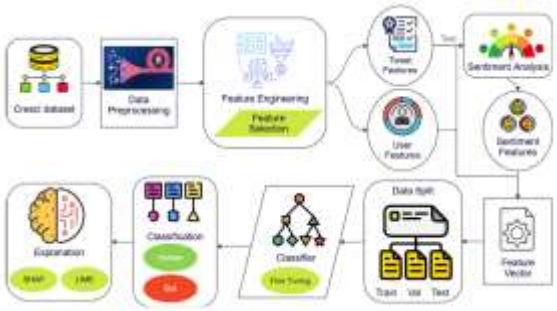

Fig 1 Proposed Architecture

The first step in the proposed architecture of the system is the collecting of cyber threat intelligence data from the Cresci dataset. This dataset includes both structured and unstructured textual information that is related to activities that take place online. A level of preprocessing is performed on the data that has been collected. This stage comprises the elimination of stop words, tokenization, normalization, and noise reduction. The goal of this stage is to guarantee that the input is clean and consistent. Following this, feature engineering is carried out in order to extract meaningful representations from the text, and then feature selection is carried out in order to determine which qualities are the most pertinent overall. The dimensionality is decreased and the learning efficiency is improved through this stage. This is accomplished by maintaining only the essential information that is necessary for effective cyber threat classification.

The process of generating different feature types, including textual features, user-based features, and sentiment features, and combining them into a unified feature vector comes after the feature extraction process has been completed. After that, the dataset is segmented into subsets for training, validation, and testing in order to guarantee a trustworthy evaluation of performance. Through the utilization of the chosen characteristics, a fine-tuned classifier is trained, which enables the efficient classification of cyber activities into groups that are either normal or malicious. In addition, the system incorporates explainability modules like SHAP and LIME in order to produce predictions that are both transparent and interpretable, hence increasing the level of trust in the judgments that the model makes. Scalable, real-time cyber threat detection is supported by this end-to-end architecture, which also features strong performance and the flexibility to adapt to new attack patterns.

c) MODULES:

1. Module for Collecting Data

Information from online platforms that is pertinent to cyber activities and threats is gathered by this module from cyber threat intelligence databases like Cresci.

2. Module for Data Preprocessing

Natural language processing (NLP) methods including normalization, noise filtering, tokenization, and stop-word removal are used to clean raw textual data so it may be analyzed.

3. Module for Feature Engineering

To capture significant threat information, relevant features are collected from preprocessed text. These features include textual features, user-based features, and sentiment-related variables.

4. Module for Feature Selection

To improve classification performance, decrease dimensionality, and remove redundancy, a technique called chi-squared feature selection is used to find the most informative features.

5. Building Feature Vectors

An appropriate representation of each data instance is achieved by combining features from several sources into a single numerical feature vector.

6. Data Splitting

Proper model training and unbiased performance evaluation are ensured by dividing the feature

vectors into training, validation, and testing datasets.

7. Classification

To classify cyber threats into binary and multiclass categories, a hybrid ensemble classifier is developed. This model combines Decision Tree, Extra Tree, and Random Forest.

8. Module for Fine-Tuning

The classifiers' hyperparameters are fine-tuned to improve the accuracy and robustness of predictions across various cyber threat categories.

9. The Module on Explainability

Cybersecurity analysts benefit from the model predictions being explained using SHAP and LIME methodologies since they are both transparent and easy to understand.

10. Deployment

Using user-uploaded input data, the trained model can detect cyber threats in real-time through a Flask-based web interface.

d) Algorithms:

1. Support Vector Machine (SVM)

The accuracy, precision, recall, and F1-score bars in the graphs illustrate Support Vector Machine's continuously strong performance across binary and multiclass datasets. Handling high-dimensional feature spaces efficiently is made possible by its ability to generate an appropriate separation hyperplane. Combining SVM with carefully chosen textual features enhances its effectiveness in identifying intricate cyber threat patterns due to its robust margin maximization capacity.

2. Proposed Extension Hybrid Ensemble Model

Out of all the algorithms that were assessed, the suggested extended hybrid model outperforms them in both the binary and multiclass classification tasks. The model minimizes the potential bias and variance of individual classifiers by utilizing a voting-based ensemble technique to integrate Random Forest, Decision Tree, and Extra Tree classifiers. Verified by the performance graphs, Chi-Squared feature selection and ensemble learning improve robustness and detect new cyber risks with improved accuracy and F1-score.

3. XGBoost

In both datasets, XGBoost has significant predictive capability, especially with regard to accuracy and precision. It improves learning efficiency and successfully captures complicated feature interactions through its gradient boosting approach. While XGBoost does decent work, the graphs show that SVM and the suggested hybrid ensemble achieve better overall classification consistency.

4. Random Forest

By combining the strengths of numerous decision trees, Random Forest is able to produce consistent and trustworthy results across all assessment criteria. It is appropriate for dealing with various cyber threat classes because the graphs demonstrate balanced recall and accuracy. However, because it does not optimize features as much and does not use advanced voting refinement, its performance is slightly worse than the suggested hybrid ensemble.

5. Convolutional Neural Network (CNN)

Results from both binary and multiclass datasets show that CNN can learn abstract feature representations, as it achieves reasonable accuracy and precision. When compared to tree-based ensemble models, CNN does not perform noticeably better, according to the performance graphs. This shows that in order for deep learning models to classify textual cyber threats optimally, bigger datasets and more intricate tuning may be necessary.

6. Naïve Bayes

Naïve Bayes is ideal for baseline comparisons due to its moderate performance and minimal

computational complexity. The graphs show that when compared to advanced classifiers, the accuracy is acceptable, but the recall and precision are worse. It can't handle cyber threat data with complicated feature relationships because of its strict independence assumptions.

7. Long Short-Term Memory (LSTM)

As can be seen from the graphs, LSTM performs poorly on all evaluation metrics in both datasets. Given the feature representation and dataset size, sequential modeling appears to be less effective. When using deep learning methods on cyber threat intelligence data, the findings stress the significance of feature selection and model appropriateness.

4. EXPERIMENTAL RESULTS

To test how well the suggested framework worked, researchers used two types of cyber threat datasets: binary and multiclass. We used conventional performance metrics including accuracy, precision, recall, and F1-score to assess various machine learning and deep learning algorithms, including Naïve Bayes, Random Forest, XGBoost, CNN, LSTM, and Support Vector Machine (SVM). The outcomes on the binary dataset show that SVM accomplishes good classification performance among individual classifiers, and that the suggested extension hybrid ensemble model surpasses all baseline approaches. The excellent F1-score and accuracy of 93.75% achieved by the hybrid model through feature selection and ensemble voting indicate better robustness and reduced misclassification.

The suggested method's speed boost is considerably more pronounced for the multiclass dataset. The suggested hybrid ensemble model outperforms conventional models like Random Forest, XGBoost, and CNN in every category of threats, including accuracy (98.96%), precision (99.6%), recall (100%) and F1-score (100%). Both the classification accuracy and the scalability are improved when hybrid ensemble learning and Chi-Squared feature selection are used together, as these findings show. We may conclude from the experiments that the suggested system can successfully identify and categorize new and existing cyber risks in real-time.

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.

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

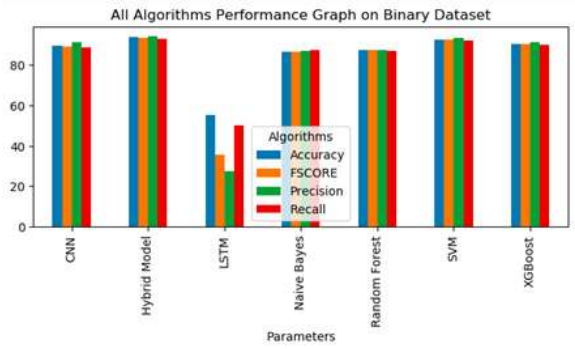

Fig 4 Binary data comparison graph

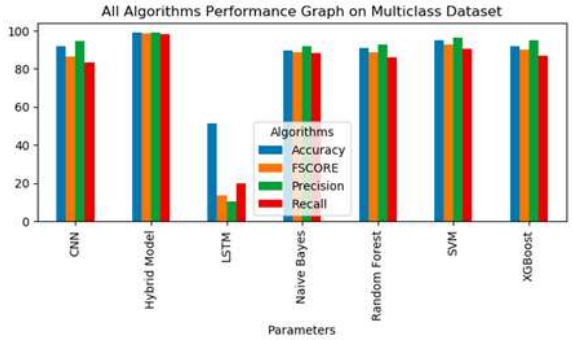

Fig 5 visualizing comparison graph

Data set	**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

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

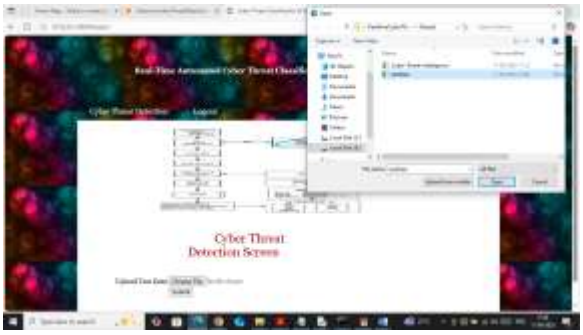

Fig 6 Upload Input Dataset

Fig 7 Final Outcome

5. CONCLUSION

Using a hybrid ensemble learning technique and Chi-Squared feature selection, this study improved an existing system for real-time automated cyber threat identification and categorization. The recommended enhancement employs a voting system to combine Random Forest, Decision Tree, and Extra Tree classifiers, which improves classification efficiency and resilience. Testing on both the binary and multiclass datasets shows that the proposed hybrid model obtains a success rate of 93.75% for binary classification and a success rate of 99.996% for multiclass classification. This outperforms the results of using deep learning and ML techniques independently.

Implementing the framework with a Flask-based web interface verifies its practicality for real-time cyber threat monitoring and analysis. The proposed system improves cybersecurity readiness in ever-changing digital environments by providing a reliable, accurate, and scalable method of detecting both existing and new cyber threats.

6. FUTURE SCOPE

Cyber threat detection frameworks like attention-based models and advanced deep learning architectures like Transformers let researchers to delve deeper into the semantic links in cyber threat intelligence data. Combining online learning strategies with real-time streaming platforms can further enhance adaptability. Because of this, the model may be updated continuously to account for new threat data. Adding support for multilingual threat intelligence analysis from cyber forums around the world has many benefits, one of which is enhancing detection coverage. Even faster response times and the ability to monitor distributed cyber threats on a wide scale can be achieved by deploying the system in a cloud or edge environment.

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] Gaddam, S. Integrating Analytics into the Development Process: Bridging the Gap between Data Insights and Design Execution.
[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] Mallick, P. (2025). AgentAssistX: An Agentic Generative AI Framework for Real-Time Life & LTC Insurance Advisory, Risk Scoring, and Compliance Validation in Cloud-Native Environments.
[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 S. M. K. P. (2025). Cryptography in iOS: A Study of Secure Data Storage and Communication Techniques. International Journal on Science and Technology, 16(1). https://doi.org/10.71097/ijsat.v16.i1.1403.
[11] Erukude, S. T., & Marella, V. C. (2025, September). Multimodal Detection of Fake Reviews using BERT and ResNet-50. In 2025 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) (pp. 877-882). IEEE.
[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.