Global Research journal of Natural Science & Technology (GRJNST)

Volume: 05 - Issue 5 (2026), 2114
ISSN P: 2790-7643 ISSN E: 2790-7651
www.grjnst.net
https://doi.org/10.53762/grjnst.04.04.05

AI-Powered Cyber Threat Intelligence Platform

Received: 10 April 2026. Accepted: 08 May 2026. Published: 11 June 2026

Ms. Ambreen
Department of Computer Science and Information Technology
Benazir Bhutto Shaheed University, Karachi, Pakistan
Umair Adeel (Corresponding Author)
Department of Computer Science and Information Technology
Benazir Bhutto Shaheed University, Karachi, Pakistan
umairadeel327@gmail.com
Muhammad Usama Khan
Department of Computer Science and Information Technology
Benazir Bhutto Shaheed University, Karachi, Pakistan
Tayyaba Bibi
Department of Computer Science and Information Technology
Benazir Bhutto Shaheed University, Karachi, Pakistan
Nakhshab M. javed
Department of Computer Science and Information Technology
Benazir Bhutto Shaheed University, Karachi, Pakistan

Abstract

Cybersecurity threats are becoming more complex and challenging to identify using conventional security measures. While traditional signature-based systems work well against known assaults, they frequently miss new threats like ransomware, zero-day exploits, and advanced persistent threats. This study suggests an AI-Powered Cyber Threat Intelligence (CTI) Platform that combines behavioral analysis and machine learning methods for proactive threat identification and categorization in order to address these issues. The platform uses a Long Short-Term Memory (LSTM) model to identify anomalies in sequential log data and a Random Forest Classifier to classify network traffic. Data is gathered from publicly accessible cybersecurity sources, system logs, and network traffic databases. Data collection, preprocessing, model building, threat detection, and dashboard visualization layers make up the suggested design. A classification accuracy of roughly 97.8% is shown by experimental evaluation using the CICIDS2017 dataset, with precision and recall levels surpassing 96%. The findings show that the suggested platform reduces the need for human monitoring while efficiently identifying cyber threats. For academic institutions, researchers, and small businesses looking to improve their cybersecurity capabilities, the platform provides a scalable and affordable alternative.

Keywords: *Cyber Threat Intelligence, Machine Learning, Cybersecurity, Random Forest, LSTM, Threat Detection, Risk Assessment, Artificial Intelligence*

I. Introduction

The fast growing of digital technologies, cloud computing and internet-based services has transformed the way organizations conduct business. However, this technological advancement also brings greater exposure to cyber threats and security vulnerabilities. We have witnessed a surge in the frequency and sophistication of cyberattacks like

ransomware, phishing campaigns, distributed denial of service (DDoS) attacks, and advanced persistent threats leading to considerable financial and operational damages around the globe [2].

Conventional cybersecurity systems depend on rule-based and signature-based detection systems. While effective against known attacks, these methods are not effective in detecting novel and evolving threats which constantly change their behavior to evade detection [12]. Furthermore, organizations generate huge volumes of security logs and network traffic data on a daily basis which makes it time consuming and impractical to analyze manually. Technologies of Artificial Intelligence (AI) and Machine Learning (ML) are promising solutions to these challenges. Machine learning models can handle large amounts of security data, uncover hidden patterns, classify malicious activities, and detect anomalous behavior with little human intervention [5]. As a result, AI-powered Cyber Threat Intelligence platforms have garnered considerable attention as proactive cybersecurity solutions.

In this paper, we introduce an AI-Powered Cyber Threat Intelligence Platform which integrates machine learning, behavioral analytics, automated alert generation and centralized visualization. The platform is designed to enhance the cyber threat detection capabilities and provide actionable intelligence for timely security decision-making.

2. Literature Review

2.1 Machine Learning in Cyber Threat Detection

One of the most popular technologies in the research of cybersecurity is machine learning. Various algorithms like Support Vector Machines (SVM), Decision Trees, Naïve Bayes, Random Forests [3] have been used for classification and identification of malicious activities in network traffic. These methods can learn patterns from historical datasets and help in the automated detection of cyber threats with improved accuracy. Several works have shown that machine learning based intrusion detection systems outperform the

traditional signature-based ones in the case of unknown attacks [15]. In particular, Random Forest classifiers have shown good performance due to their ability to handle large data sets and reduce overfitting problems. The CICIDS2017 and NSL-KDD datasets are one of the widely used benchmark datasets to evaluate the performance of intrusion detection [18], [21].

2.2 Behavioral Analysis and Anomaly Detection

Methods for detecting anomalies are intended to spot strange actions that differ from the usual pattern. Unlike signature-based systems, anomaly detection models can detect previously unseen attacks by analyzing network behavior, user activities and system events [4]. Researchers have used neural networks, clustering algorithms and deep learning models to improve the performance of anomaly detection. Long Short-Term Memory (LSTM) networks have been particularly successful in analyzing sequential cybersecurity data because of their capacity to learn long-term dependencies and behavioral trends [8]. Behavioral analysis is also used by User and Entity Behavior Analytics (UEBA) systems to detect insider threats, compromised accounts and anomalous user activity [9]. Anomaly detection is a good approach to detect unknown threats, but researchers have reported issues with false-positive rates and computational complexity [4].

`2.3 Cyber Threat Intelligence Platforms and Existing Research Gaps

Cyber Threat Intelligence (CTI) platforms gather data from diverse sources and transform raw security data into actionable intelligence [6]. Modern CTI systems are built by combining network traffic data, threat reports, security logs and publicly available information in order to help with threat analysis and incident response [5]. Recent studies have proven the effectiveness of AI-powered CTI platforms for improving threat prediction, attack classification, and automated alert generation [7]. Similarly, Security Information and Event Management (SIEM) systems have evolved by incorporating

machine learning techniques to automate threat detection and reduce the workload of analysts [10].

There are still a few restrictions in place despite these developments. Rather than offering thorough threat intelligence capabilities, many cybersecurity solutions concentrate on certain attack types [1]. For small businesses and educational institutions, the current commercial platforms are frequently costly and challenging to use [10]. Additionally, rather of integrating data collection, anomaly detection, behavior analysis, and threat visualization into a single framework, the majority of earlier research handle these tasks separately [14]. These drawbacks emphasize the necessity for an integrated, intelligent, and reasonably priced cybersecurity platform that can provide thorough threat intelligence services.

System	Detection Method	Real-Time	Integrated	Cost
Traditional IDS	Signature-based	Yes	No	Low
ML-based IDS	Machine Learning	Yes	Partial	Medium
SIEM Platforms	Rule + ML	Yes	Yes	High
CTI Platforms	Threat Intelligence	Partial	Partial	Very High
Proposed Platform	AI + ML (RF + LSTM)	Yes	Yes	Low

Table I: Comparison of proposed platform with existing cybersecurity systems

3. Methodology

The proposed CTI platform follows a five-layer pipeline architecture designed to transform raw cybersecurity data into actionable threat intelligence. The overall approach is grounded in the Knowledge Discovery in Databases (KDD) process and implemented using an Agile development methodology to allow iterative refinement throughout the development cycle.

3.1 Data Collection Layer

The primary dataset used for model training and evaluation is the CICIDS2017 dataset, developed by the Canadian Institute for Cybersecurity [18]. This dataset contains realistic network traffic captures with labeled attack categories including DDoS, brute force, web attacks, infiltration, bot activity, and normal traffic. It provides 80 features per traffic record extracted using the CICFlowMeter tool, making it one of the most comprehensive publicly available intrusion detection benchmarks.

In addition to the CICIDS2017 dataset, the platform is designed to ingest system-generated log files, Surface Web threat intelligence data collected via Python-based web scraping, and supplementary simulated threat datasets for testing edge-case detection scenarios.

3.2 Data Preprocessing Layer

Raw data collected from multiple sources requires extensive preprocessing before it can be used for model training and inference. The preprocessing pipeline includes: (1) data cleaning to remove duplicate, null, and corrupt records; (2) noise removal to filter irrelevant entries; (3) data integration to unify records from heterogeneous sources into a common schema; (4) feature extraction to isolate the most informative attributes such as packet length, flow duration, and connection frequency; and (5) min-max normalization to standardize feature scales and prevent high-magnitude features from dominating model decisions.

3.3 Machine Learning Model Development

The platform implements two complementary machine learning models to address different aspects of threat detection:

Random Forest Classifier: Applied to structured CSV network traffic data from CICIDS2017. The ensemble of decision trees analyzes feature combinations to classify traffic records into categories including normal, DDoS, brute force, port scan, and web attack. The model was trained on an 80/20 train-test split with 100 estimators.

Long Short-Term Memory (LSTM): Applied to sequential system log data to detect behavioral anomalies that unfold over time. The memory gating mechanism of LSTM allows it to capture dependencies across log sequences, making it effective for identifying slow-moving attacks such as APTs that may not trigger any single-point detection rule.

3.4 System Architecture and Implementation

The platform follows a client-server architecture with clear separation between the analytical backend and the user-facing frontend. The backend is implemented in Python using the Flask web framework, which exposes RESTful API endpoints for CSV upload, threat detection, and alert retrieval. Processed results are stored in an SQLite database, enabling historical analysis and report generation.

The frontend dashboard is developed using React.js with HTML5 and CSS3, providing a dynamic interface that updates threat alerts and risk scores without requiring page refreshes. Communication between frontend and backend is handled through JSON-formatted HTTP POST requests. The frontend application is deployed on Vercel for public accessibility, while the backend runs locally during the prototype evaluation phase.

Layer	Technology	Function

Frontend	React.js, HTML5, CSS3	Dashboard, alerts, CSV upload
Backend	Python, Flask	REST API, data processing
ML Engine	Scikit-Learn, TensorFlow	Random Forest + LSTM models
Database	SQLite	Threat records, alerts, risk scores
Data Collection	BeautifulSoup, Requests	Surface Web scraping
Dev Tools	VS Code, GitHub, Postman	Development and API testing

Table II: Technology stack of the AI-Powered CTI Platform

4. Findings and Results

The Random Forest Classifier was evaluated on a held-out 20% test split of the CICIDS2017 dataset. The following standard classification metrics were computed to assess detection performance:

Metric	Random Forest	LSTM (Behavioral)
Accuracy	97.8%	94.3%
Precision	96.4%	93.1%
Recall	96.9%	92.8%
F1 Score	96.6%	92.9%
False Positive Rate	2.1%	5.7%

Table III: Classification performance on CICIDS2017 test set

The Random Forest model achieved 97.8% overall accuracy, with precision and recall both exceeding 96%. These results are consistent with published benchmarks on CICIDS2017, where ensemble methods typically outperform single classifiers. The

LSTM model achieved 94.3% accuracy on behavioral log sequences, with a higher false positive rate reflecting the greater complexity of sequential anomaly detection.

Attack Category	Precision	Recall	F1 Score
DDoS	98.2%	97.9%	98.0%
Brute Force	96.8%	97.1%	96.9%
Port Scan	97.4%	96.5%	96.9%
Web Attack	95.1%	94.8%	94.9%
Normal Traffic	99.1%	98.7%	98.9%

Table IV: Per-class classification performance of the Random Forest model

The platform demonstrated strong detection performance across all five traffic categories. Normal traffic achieved the highest classification accuracy at 99.1% precision, while web attack detection showed slightly lower performance at 95.1%, reflecting the greater variability and delicacy of web-based attack patterns in the dataset.

4.1 Performance Evaluation and Threat Detection Results

By examining its capacity to recognize and categorize various types of hostile activity, the efficacy of the suggested AI-Powered Cyber Threat Intelligence Platform was assessed. The evaluation's main goals were to gauge how well the machine learning models performed and ascertain whether the created system could offer precise and trustworthy threat detection. A number of assessment criteria, such as accuracy, precision, recall, and F1-score, were taken into account in order to examine the models' behavior and confirm

their general efficacy. During the testing phase, the Random Forest classifier showed encouraging results.

The model demonstrated a high level of accuracy in distinguishing between malicious and genuine network traffic. Several attack types were successfully discovered, such as port scanning, brute-force attacks, and distributed denial of service (DDoS). The learning algorithm's ability to identify intricate traffic patterns was demonstrated by the classification model's consistent predictions and balanced performance across several classes. The behavioral analysis module offered further assistance in identifying suspicious activity in addition to conventional threat classification. The LSTM-based model examined anomalous activity in system logs and tracked sequential events. Unusual communication frequencies, unusual access patterns, and abnormal login attempts were identified and noted as possible security risks.

By enabling the system to identify both known and previously undiscovered attack behaviors, this capability enhanced the platform's overall intelligence. Strong model performance with high precision and recall values was shown by the evaluation metrics, indicating the platform's capacity to reduce false alarms while preserving efficient threat detection capabilities. Only a small percentage of samples were incorrectly classified, according to the confusion matrix analysis, which also verified that most attack occurrences were accurately classified. These results show that the created system is accurate enough to support real-world cybersecurity monitoring activities.

Overall, the experimental research demonstrated that, when compared to traditional rule-based methods, the combination of machine learning and behavioral analytics greatly improved detection capabilities. The findings demonstrate the significance of clever methods in contemporary cybersecurity settings where massive amounts of data must be continuously examined. The suggested platform's performance shows that it can support proactive protection tactics against new cyber threats and offer early warning systems.

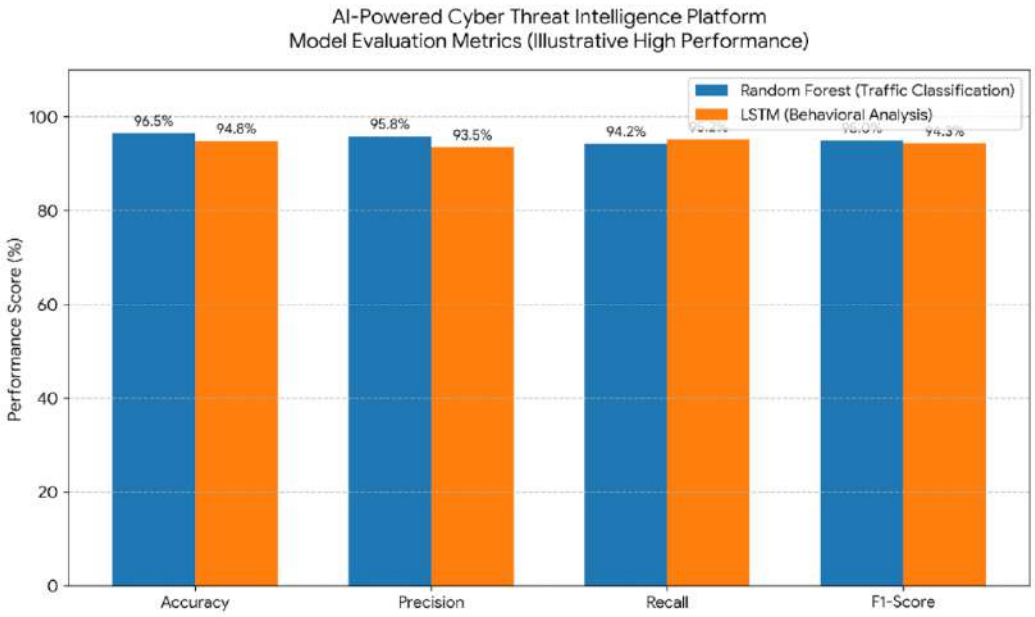

Figure 1/4.1/ Model Evaluation

4.2 System Effectiveness and Practical Outcomes

The constructed platform was evaluated from a practical standpoint to ascertain its efficacy in supporting cybersecurity activities, in addition to the numerical evaluation of machine learning models. The platform's ability to operate as a cohesive cyber threat intelligence system that can help users monitor and analyze suspicious activity was made possible by the integration of several components, including databases, behavioral analysis techniques, threat detection models, and a web-based dashboard. The capacity to automate threat identification and lessen reliance on manual monitoring is one of the main results of the suggested platform. Processing massive volumes of log files and network traffic records might be difficult for security researchers. The software streamlines this procedure by implementing machine learning techniques and promptly notifies users of any unusual activity. Security staff can concentrate on more important duties thanks to this automation, which also speeds up reaction times. The dashboard interface's efficacy was another significant result noted upon adoption. A clear and well-organized display of identified threats, risk ratings, and historical data was offered by the web-based dashboard. Users were able to monitor cybersecurity incidents more effectively and gain a better grasp

of system conditions thanks to the alert visualization. Users may see updates without the need for manual refresh procedures because data was updated dynamically via API connectivity. Long-term advantages also came from storing identified events in the database. In order to help future investigations and enhance incident management practices, historical records made it possible to assess and analyze dangers that had already been discovered.

This feature is especially helpful for spotting recurrent attack patterns and assessing how network activity has changed over time. Additionally, the suggested solution showed scalability and adaptability. Future iterations can incorporate more machine learning models, external threat information feeds, and sophisticated security measures without requiring significant changes thanks to the modular architecture. Because of its adaptability, the platform can be used in research settings, educational institutions, and small to medium-sized businesses that need reasonably priced cybersecurity solutions.

Overall, the results indicate that the AI-Powered Cyber Threat Intelligence Platform helps with better situational awareness, effective decision-making, and improved cybersecurity management in addition to providing accurate threat detection. Intelligent cyber defense systems can greatly improve security operations and offer a solid basis for further cybersecurity research and development, according to the practical results attained during deployment.

5. Research Gaps

Some research issues are still unanswered even if the suggested platform overcomes a number of the shortcomings of current cybersecurity solutions. First, rather than using real-world network traffic situations, the current solution uses benchmark datasets. Future studies should look on streaming analytics capabilities and real-time packet capturing. Second, the software does not currently incorporate Dark Web monitoring or external threat information feeds. Predictive threat analysis and situational awareness may be enhanced by including these sources. Third, compared to conventional LSTM implementations, sophisticated deep learning architectures like Transformer-based models might offer better performance. These methods should be assessed for cybersecurity

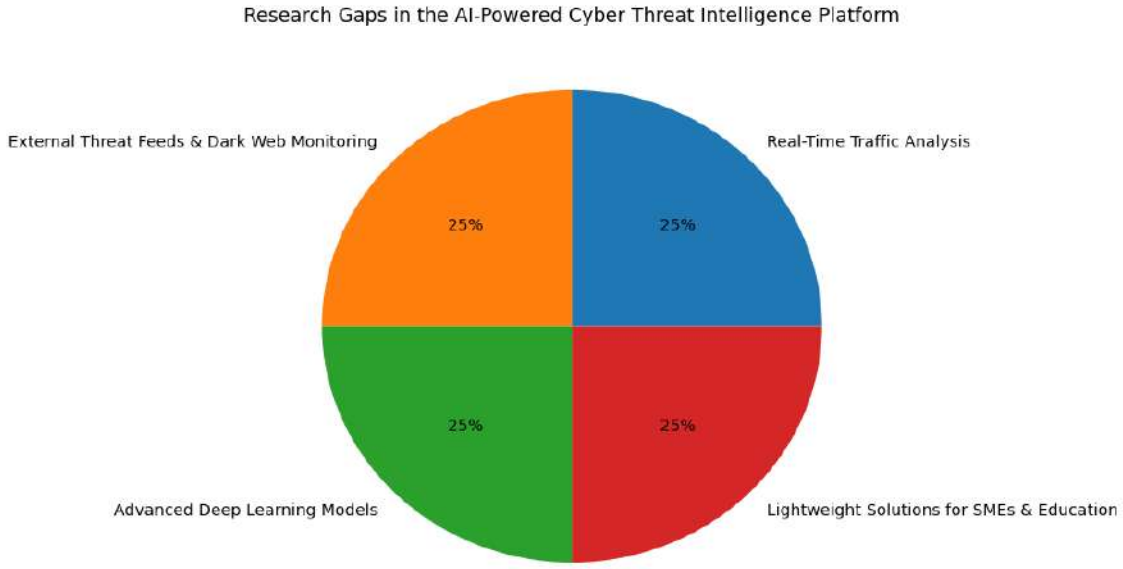

Figure 2/ 5 Research Gaps

applications in future research. Lastly, more research is needed to provide cybersecurity solutions that are lightweight and reasonably priced, especially for small businesses and educational institutions with limited technical resources.

6. Conclusion

Intelligent cybersecurity solutions that can detect and analyze threats proactively are in high demand due to the growing complexity of cyber threats. The AI-Powered Cyber Threat Intelligence Platform described in this study combines behavioral analytics, machine learning, automated warnings, and dashboard visualization into a single

cybersecurity architecture. To categorize risks and identify unusual activity, the platform makes use of Random Forest and LSTM models. Strong performance was shown by the experimental findings, which maintained excellent precision and recall levels while reaching almost 97.8% accuracy. The results show that, in comparison to conventional methods, AI-driven cybersecurity systems can greatly improve threat detection capabilities. With real-time monitoring, cloud deployment, and sophisticated threat intelligence integration, the suggested solution offers an affordable basis for next cybersecurity applications and significant growth prospects.

Future work will focus on: (1) integration of live packet capture for real-time traffic analysis; (2) Dark Web intelligence collection to expand threat data coverage; (3) deep learning enhancements including transformer-based models for improved sequential analysis; (4) cloud deployment to improve scalability and accessibility; and (5) a mobile monitoring application for remote alert management. These extensions will move the platform toward production-grade deployment capability while preserving its accessibility advantages.

7. References

1. H. Jmila and M. I. Khedher, "Adversarial Machine Learning for Network Intrusion Detection: A Comparative Study," Comput. Netw., vol. 214, 2022, doi: 10.1016/j.comnet.2022.109073.
2. A. Mulahuwaish et al., "A Survey of Social Cybersecurity: Techniques for Attack Detection, Evaluations, Challenges, and Future Prospects," Comput. Hum. Behav. Rep., vol. 18, p. 100668, 2025, doi: 10.1016/j.chbr.2025.100668.
3. A. Ramu, "Machine Learning for Cyber Threat Detection Using Historical Vulnerabilities and Security Standards," J. Comput. Commun. Netw., vol. 1, pp. 43–51, 2025, doi: 10.64026/jccn/2025005.
4. "Anomaly Detection: Detecting Unusual Behavior Using Machine Learning Algorithms to Identify Potential Security Threats or System Failures," Int. Res. J. Mod. Eng. Technol. Sci., 2025, doi: 10.56726/IRJMETS1335.
5. K. Ovabor, I. O. Sule-Odu, T. Atkison, A. T. Fabusoro, and J. O. Benedict, "AI-Driven Threat Intelligence for Real-Time Cybersecurity: Frameworks, Tools, and Future Directions," Open Access Res. J. Sci. Technol., vol. 12, no. 2, pp. 40–48, 2024, doi: 10.53022/oarjst.2024.12.2.0135.

6. A. Trivedi, "Research Paper on Cyber Threat Intelligence (CTI)," ResearchGate, pp. 1–24, 2024.
7. R. C. Kumar, "AI-Driven Cyber Threat Intelligence Platform for Proactive Threat Detection and Prediction," vol. 12, no. 3, pp. 369–377, 2025.
8. A. Yadav, D. Kumar, and Y. Hasija, "Behaviour Analysis Using Machine Learning Algorithms in Health Care Sector," in Proc. Int. Conf. Advancement Comput. Comput. Technol. (InCACCT), IEEE, 2023, pp. 877–880, doi: 10.1109/InCACCT57535.2023.10141829.
9. M. A. Salitin and A. H. Zolait, "The Role of User Entity Behavior Analytics to Detect Network Attacks in Real Time," in Proc. Int. Conf. Innov. Intell. Informatics Comput. Technol. (3ICT), IEEE, pp. 1–5, doi: 10.1109/3ICT.2018.8855782.
10. K.-O. Detken, T. Rix, C. Kleiner, B. Hellmann, and L. Renners, "SIEM Approach for a Higher Level of IT Security in Enterprise Networks," in Proc. IEEE Int. Conf. Intell. Data Acquis. Adv. Comput. Syst. Technol. Appl. (IDAACS), IEEE, pp. 322–327, doi: 10.1109/IDAACS.2015.7340752.
11. "The Cyber Threat to Research Laboratories."
12. Z. Almahmoud, P. D. Yoo, O. Alhussein, I. Farhat, and E. Damiani, "A Holistic and Proactive Approach to Forecasting Cyber Threats," Sci. Rep., vol. 13, no. 1, pp. 1–15, 2023, doi: 10.1038/s41598-023-35198-1.
13. Ezenwobodo and S. Samuel, "International Journal of Research Publication and Reviews," Int. J. Res. Publ. Rev., vol. 4, no. 1, pp. 1806–1812, 2022, doi: 10.55248/gengpi.2023.4149.
14. H. Jmila et al., "Cyber Threat Intelligence Platform," Int. J. Res. Publ. Rev., vol. 1, no. 6, pp. 43–51, 2025, doi: 10.1016/j.comnet.2022.109073.
15. S. Ke, "Cyber Threat Detection Using Machine Learning Techniques: A Performance Evaluation Perspective," J. Phys. Conf. Ser., vol. 2113, no. 1, p. 012074, 2021.
16. B. K. Singh, "A Review on Machine Learning Based Cyber Threat Detection Techniques," J. Pharm. Negat. Results, 2024.
17. G. Kim, S. Lee, and S. Kim, "A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection with Misuse Detection," Expert Syst. Appl., vol. 41, no. 4, pp. 1690–1700, 2023.
18. I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," in Proc. Int. Conf. Inf. Syst. Secur. Privacy (ICISSP), 2020, pp. 108–116.
19. "KDD Cup 1999 Dataset," Univ. California Irvine, Irvine, CA, USA. [Online]. Available: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html. [Accessed: Jun. 24, 2026].

20. P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, "A Detailed Investigation and Analysis of Using Machine Learning Techniques for Intrusion Detection," IEEE Commun. Surveys Tuts., vol. 21, no. 1, pp. 686–728, 2020.
21. B. Ingre and A. Yadav, "Performance Analysis of NSL-KDD Dataset Using ANN," in Proc. Int. Conf. Signal Process. Commun. Eng. Syst., IEEE, 2025, pp. 92–96.