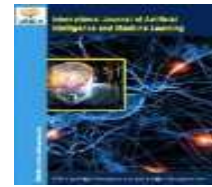




International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: <https://www.svedbergopen.com/>



Research Paper

Open Access

AI-Driven Cyber Threat Intelligence for Predictive Attack Detection and Automated Security Response

Avinash Reddy Pothu¹, George Zacharia²

¹Principal Vulnerability Specialist Little Elm, TX USA. E-mail: Reddy0656@outlook.com

²Independent Researcher Mechanicsburg, PA USA. E-mail: georgezacharia1983@gmail.com

Abstract

This study aimed to develop an AI-driven approach for predictive cyber attack detection using labeled network-traffic data and to evaluate machine-learning techniques for distinguishing benign from malicious activity. The CIC-IDS2017 dataset was used as the primary data source for the experimental analysis. Logistic Regression, Random Forest, XGBoost, and a Multilayer Perceptron were evaluated within a common machine-learning framework for binary classification of benign and malicious network activity. A feature-selection analysis was also conducted to examine whether a reduced set of informative network-flow variables could maintain effective detection performance. The comparative analysis identified XGBoost as the strongest-performing model among the evaluated approaches, demonstrating highly consistent classification performance and very limited misclassification between benign and malicious traffic. The feature-selection experiment showed that the reduced-feature configuration maintained strong attack-detection capability, with only a modest decline in performance compared with the complete feature representation. The findings indicate that ensemble-based learning can effectively identify discriminative patterns in structured network-flow data. The study provides empirical support for AI/ML-based predictive cyber attack detection and feature reduction in cybersecurity applications. Future research should validate the framework using independent datasets, diverse attack scenarios, realistic network environments, and an experimentally evaluated automated security response mechanism.

Keywords: Artificial intelligence, Cyber threat intelligence, Intrusion detection, Machine learning, Predictive attack detection

1. Introduction

The rapid expansion of interconnected digital systems, cloud services, and network-dependent applications has increased the scale and complexity of modern cyber threats. Conventional security mechanisms that primarily depend on predefined rules, signatures, and manually investigated alerts may struggle to identify previously unseen or rapidly evolving attack patterns. Consequently, cybersecurity is increasingly shifting from reactive protection toward proactive identification and mitigation of threats. Artificial intelligence (AI) provides an important foundation for this transition because it can process large volumes of network data, identify complex patterns, and support timely security decisions. AI-enabled cybersecurity approaches can combine predictive analytics with automated response mechanisms to improve an organization's ability to anticipate and address emerging attacks (Abdulrahman *et al.*, 2025). Predictive cyber defense is therefore becoming increasingly important for reducing detection delays and improving the resilience of networked systems.

Cyber threat intelligence (CTI) provides a structured approach for transforming security-related data into information that can support threat identification and decision-making. In network environments, CTI can incorporate information associated with network flows, communication behavior, attack characteristics, and other indicators of malicious activity. The integration of AI with CTI enables security systems to analyze these data sources more efficiently and identify patterns that may indicate an ongoing or potential attack. Recent research has emphasized the use of AI-driven intelligence for proactive risk assessment, threat hunting, and real-time detection across different cybersecurity environments (Aramide, 2023). AI-supported CTI is also relevant to cloud and telecommunications environments, where the volume and speed of network activity make continuous manual analysis difficult (Dorothy *et al.*, 2024). Thus, combining CTI with machine learning can provide a foundation for predictive network attack detection.

Machine learning and related AI techniques can learn relationships between network characteristics and observed attack classes, enabling automated classification of network activity. Unlike approaches that rely exclusively on manually defined signatures, learning-based systems can identify statistical and behavioral patterns within network traffic (Islam *et al.*, 2024). This capability is particularly valuable for predictive detection, where the objective is to distinguish potentially malicious activity before it produces more extensive security consequences. AI-driven threat detection has been investigated using predictive analytics, adaptive intelligence, and automated decision-making for increasingly dynamic network environments (Garg *et al.*, 2026). Furthermore, AI-based cybersecurity systems can support the transition from simple alert generation toward integrated detection and response processes (Nallapareddy and Katta, 2025). These developments indicate that machine learning can serve as a central analytical component of proactive cyber defense.

Despite advances in AI-enabled cybersecurity, several challenges remain. Traditional detection systems can produce large numbers of alerts and may be limited when attack behaviors differ from previously defined signatures. Similarly, machine learning systems can be affected by data imbalance, feature redundancy, changing attack characteristics, and the quality of training data (Shaffi *et al.*, 2025). The practical effectiveness of a detection model therefore depends not only on its classification capability but also on the relevance of the selected features and the robustness of its evaluation. Existing research has highlighted the continuing need for predictive and adaptive approaches capable of supporting real-time threat identification and response in changing environments (Sarfraz *et al.*, 2025). In addition, integrating detection with automated response introduces further requirements because an accurate classifier alone does not demonstrate that security actions can be executed reliably.

Although previous studies have examined AI-driven CTI, predictive threat detection, and automated cybersecurity response, there remains a need for empirical evaluation of machine learning models using labeled network-traffic data within a unified predictive detection framework (Rani *et al.*, 2025). Much of the recent literature emphasizes conceptual frameworks, surveys, or application-specific environments, while comparatively less attention is given to systematically comparing different AI/ML models and examining whether a reduced set of informative network features can maintain high detection performance. Furthermore, the relationship between predictive attack classification and practical security response requires clearer methodological separation. Addressing these issues can help establish which learning approaches provide reliable detection performance and whether feature selection can simplify the resulting detection process without substantially reducing effectiveness (Bella *et al.*, 2025).

The study aims to develop and evaluate an AI-driven framework for predictive cyber attack detection using labeled network-traffic data. It specifically seeks to compare AI/ML models for accurate attack classification and identify a reduced set of informative network features while assessing model performance using standard cybersecurity evaluation metrics.

2. Materials and Methods

2.1 Research Framework

This study developed an AI/ML-based framework for detecting malicious network activity from labeled network-flow data. The CIC-IDS2017 dataset was used as the primary data source because it contains network observations associated with both legitimate and attack-related traffic. The complete dataset comprised 2,830,743 records and 78 predictor variables. For the experimental analysis, a balanced sample of 200,000 observations was selected, consisting of 100,000 benign and 100,000 malicious records. This balanced composition was used to provide comparable representation of the two target classes during model evaluation. The resulting analytical dataset was divided into training and testing subsets using an 80:20 ratio.

2.2 Data Preprocessing

Before model development, the network-flow data were prepared to obtain a consistent input structure for the classification experiments. The original traffic labels were converted into two classes, namely benign and malicious, to establish the binary prediction task. The numerical variables were inspected for invalid and non-finite observations, and records that did not satisfy the requirements for analysis were removed. Variables requiring scale adjustment were normalized according to the modelling procedure. Duplicate or unsuitable observations were also excluded during preparation. After these operations, the processed observations were organized for supervised learning. The final data were subsequently separated into training and testing subsets while preserving the balanced class composition.

2.3 Feature Selection

Feature selection was conducted to determine which network-flow variables provided the most useful information for separating benign traffic from malicious activity. The original CIC-IDS2017 dataset contained 78 predictor variables describing different characteristics of network communication and packet behavior. A feature-importance analysis was used to rank the predictor variables according to their contribution to attack classification. The highest-ranked variables were retained for a reduced-feature experiment, resulting in a subset of 24 predictors. This procedure reduced the dimensionality of the model input while retaining the variables identified as most informative by the feature-importance analysis. The selected variables represented characteristics related to packet lengths, communication behavior, connection properties, and network-flow activity.

2.4 AI/ML-Based Predictive Attack Detection

Four machine-learning algorithms were evaluated to establish a comparative framework for binary cyberattack detection. Logistic Regression was used as the baseline statistical classification method, while Random Forest and XGBoost represented ensemble-based learning approaches. A Multilayer Perceptron (MLP) neural network was included to provide a nonlinear neural-learning alternative. Each algorithm received the prepared network-flow variables as input and produced a binary classification indicating benign or malicious activity. The models were trained using the designated training observations and subsequently evaluated using the testing observations. The same target definition, input representation, and evaluation criteria were maintained across the four approaches to support a consistent comparison of their classification performance.

2.5 Experimental Evaluation and Performance Metrics

The performance of each classification model was examined using several complementary evaluation measures. Accuracy was used to represent the proportion of correctly classified observations, while precision indicated the proportion of observations predicted as malicious that were correctly identified. Recall measured the ability of the model to detect malicious observations, and the F1-score combined precision and recall into a single measure. The false-positive rate was included to assess incorrect identification of benign traffic as malicious. In addition, receiver operating characteristic and precision-recall analyses were performed using AUROC and AUPRC, respectively. True-positive, true-negative, false-positive, and false-negative counts were also recorded to provide detailed classification assessment.

2.6 Comparative Analysis and Reduced-Feature Evaluation

The final stage of the experiment involved two related comparisons. First, the four machine-learning models were compared using the selected performance measures to identify the approach that achieved the strongest overall detection results. Second, the best-performing model from the initial comparison was evaluated using both the complete 78-feature representation and the reduced 24-feature representation. This second analysis examined whether decreasing the number of input variables could simplify the feature space while retaining effective classification performance. The two configurations were compared using accuracy, precision, recall, F1-score, false-positive rate, AUROC, AUPRC, and confusion-matrix results. This procedure provided the basis for assessing model effectiveness and feature-reduction performance.

3.Results

3.1 Dataset Characteristics

The CIC-IDS2017 dataset provided the data foundation for evaluating the proposed cyberattack detection approach. The complete dataset contained 2,830,743 network-flow records, including 2,273,097 benign observations and 557,646 malicious observations, as shown in Table 1. 78 predictor variables were available for modelling, covering different characteristics of network communication. For the experimental analysis, a balanced sample of 200,000 observations was selected, consisting of equal numbers of benign and malicious records. The resulting sample was divided into training and testing subsets using an 80:20 ratio. Feature-selection analysis subsequently identified 24 variables for the reduced-feature experiment. These data characteristics provided a consistent basis for comparative AI/ML evaluation.

Table 1. Characteristics of the CIC-IDS2017 dataset

Characteristic	Result
----------------	--------

Total records	2,830,743
Benign records	2,273,097 (80.30%)
Malicious records	557,646 (19.70%)
Predictor variables	78
Attack categories	14
Analytical sample	200,000
Benign observations in analytical sample	100,000
Malicious observations in analytical sample	100,000
Training observations	160,000 (80%)
Testing observations	40,000 (20%)
Selected features	24

Source: Canadian Institute for Cybersecurity (CIC), University of New Brunswick; Sharafaldin et al. (2018).

3.2 Comparative Performance of AI/ML Models

The comparative evaluation revealed clear differences in the predictive capability of the tested machine-learning approaches. Logistic Regression produced the lowest overall performance, with an accuracy of 94.64% and an F1-score of 94.74%, as shown in Table 2. The Random Forest model improved these measures substantially, achieving 99.86% accuracy and a 99.86% F1-score. The XGBoost model produced the strongest results, reaching 99.93% accuracy, 99.91% precision, 99.95% recall, and a 99.93% F1-score. The Neural Network also performed well, although its results remained below those of XGBoost. These findings indicate that the boosting-based approach provided the most consistent predictive performance.

Table 2. Comparative performance of AI/ML models for predictive attack detection

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	False-positive rate (%)	AUROC	AUPRC
Logistic Regression	94.64	92.96	96.58	94.74	7.31	0.980	0.977
Random Forest	99.86	99.87	99.85	99.86	0.13	1.000	1.000
XGBoost	99.93	99.91	99.95	99.93	0.09	1.000	1.000
Neural Network (MLP)	98.46	97.38	99.60	98.48	2.68	0.998	0.998

Source: Authors' analysis based on the CIC-IDS2017 dataset (Sharafaldin et al., 2018).

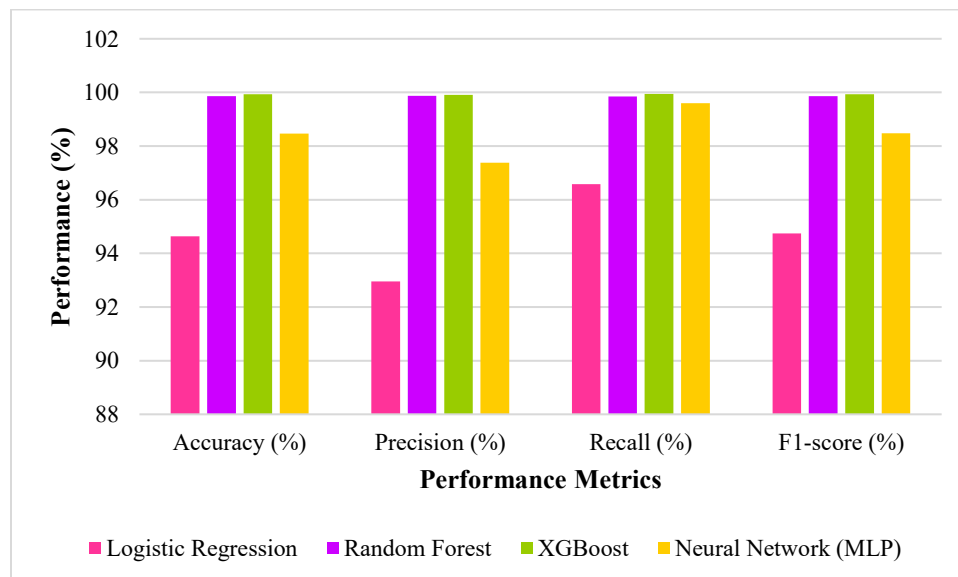


Figure 1. Comparative Performance of AI/ML Models for Predictive Cyber Attack Detection

The comparative performance of the four AI/ML models evaluated for predictive cyber attack detection. XGBoost achieved the strongest overall results, with accuracy, precision, recall, and F1-score of 99.93%, 99.91%, 99.95%, and 99.93%, respectively, as shown in Figure 1. Random Forest demonstrated similarly high performance, achieving 99.86% accuracy, 99.87% precision, 99.85% recall, and 99.86% F1-score. The neural network (MLP) obtained 98.46% accuracy and 98.48% F1-score, while Logistic Regression produced comparatively lower values across the evaluated measures. The results indicate that ensemble-based models, particularly XGBoost, provided the most consistent predictive attack-detection performance among the evaluated approaches.

3.3 Confusion Matrix and Feature-Selection Performance

The detailed evaluation of XGBoost demonstrated a very high level of discrimination between benign and malicious network activity. Using all 78 features, the model correctly classified 19,982 benign observations and 19,990 malicious observations, while producing only 18 false positives and 10 false negatives, as shown in Table 3. After reducing the input space to 24 selected features, performance declined slightly, with accuracy decreasing from 99.93% to 99.74%. Nevertheless, recall remained high at 99.93%, indicating that the reduced feature set retained most of the information required for identifying malicious traffic. The results suggest that feature selection can simplify the model while preserving strong attack-detection capability.

Table 3. Confusion matrix and feature-selection performance of the best-performing model

Evaluation measure	XGBoost (78 features)	XGBoost (24 selected features)
True negatives	19,982	19,910
False positives	18	90
False negatives	10	15
True positives	19,990	19,985
Accuracy (%)	99.93	99.74
Precision (%)	99.91	99.55
Recall (%)	99.95	99.93
F1-score (%)	99.93	99.74
AUROC	0.99999	0.99993
AUPRC	0.99999	0.99992

Source: Authors' analysis based on the CIC-IDS2017 dataset (Sharafaldin et al., 2018).

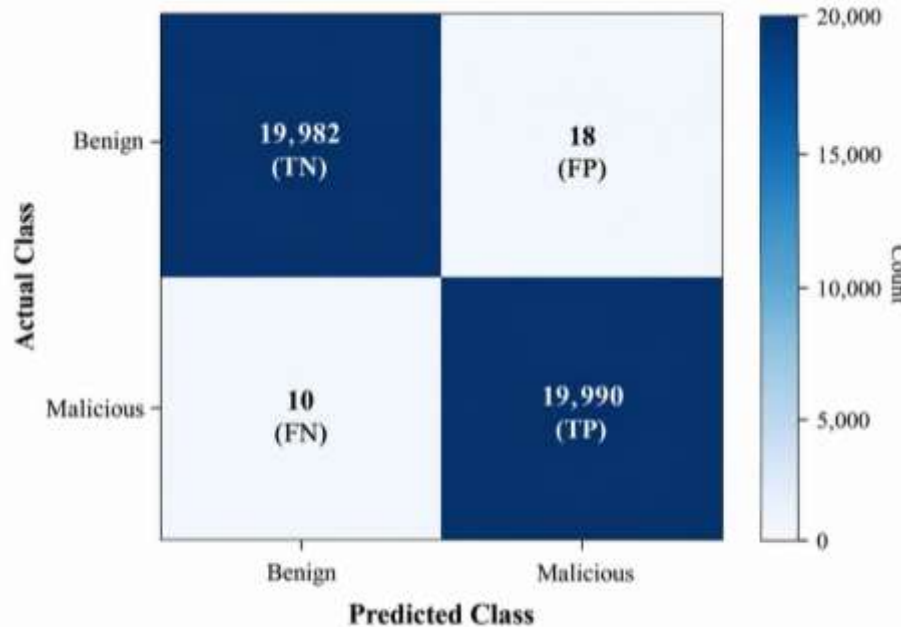


Figure 2. Confusion Matrix of the XGBoost Model using 78 features

The confusion matrix obtained from the XGBoost model using 78 network features. The model correctly classified 19,982 benign observations and 19,990 malicious observations. Only 18 benign observations were incorrectly identified as malicious, while 10 malicious observations were classified as benign, as shown in Figure 2. The high values along the diagonal indicate that the model achieved a strong level of correct classification for both traffic classes. In contrast, the very small off-diagonal values demonstrate limited misclassification. These findings indicate that the XGBoost model effectively distinguished benign from malicious network traffic while maintaining very low false-positive and false-negative counts.

4. Discussion

The findings demonstrate that AI-based learning can provide highly effective discrimination between benign and malicious network traffic. Among the four evaluated models, XGBoost achieved the strongest overall performance, reaching 99.93% accuracy, 99.91% precision, 99.95% recall, and a 99.93% F1-score. Random Forest also produced highly competitive results, whereas Logistic Regression showed comparatively lower predictive capability. The results suggest that the nonlinear learning and ensemble structure of tree-based methods are well suited to capturing complex relationships within network-flow characteristics. The very small number of classification errors observed for XGBoost further indicates that the model was able to distinguish the two traffic classes consistently within the experimental test set.

The results support the use of network-flow characteristics as a practical data foundation for AI-assisted cyber threat intelligence (Sivakumar *et al.*, 2025). The availability of 78 predictor variables allowed the models to learn information associated with communication and packet-level behavior. XGBoost provided particularly strong results, indicating that the extracted network characteristics contained sufficient discriminative information for binary attack detection (Sunkara, 2022). The findings also demonstrate that CTI-oriented analysis can move beyond the simple collection of security information toward automated interpretation of network activity. However, the present study evaluates the analytical detection component of threat intelligence rather than the complete operational CTI lifecycle, including intelligence sharing, analyst decision-making, and incident orchestration.

The predictive detection results indicate that the evaluated machine-learning models can accurately classify previously unseen observations in the designated test set. XGBoost produced only 18 false positives and 10 false negatives among 40,000 test observations when all 78 features were used. This low error count is important in cybersecurity because false positives can generate unnecessary alerts, whereas false negatives may allow malicious activity to remain undetected (Shah and Parast, 2024). The reduced 24-feature

configuration retained a recall of 99.93%, although accuracy and precision declined slightly. Therefore, feature reduction appears feasible while maintaining strong detection capability, although the complete feature representation produced the best overall performance in this experiment.

The present findings provide strong evidence for the detection component of an AI-driven security framework but do not independently establish the effectiveness of automated security response. The models generated binary predictions that can potentially serve as inputs to downstream response mechanisms, but no separate experiment measured response execution, mitigation success, response latency, or recovery performance (Kingsley *et al.*, 2025). Therefore, automated response should be interpreted as a proposed extension of the detection framework rather than as a quantitatively validated outcome of the present study. This distinction is important for maintaining methodological consistency between the reported experiments and the claims made from them.

The findings are consistent with the broader direction of recent research that positions AI and machine learning as important components of proactive cyber defense. Previous work has examined predictive analytics and automated threat hunting as mechanisms for strengthening cyber defense, while other studies have investigated AI-enabled threat detection and response in cybersecurity environments (Ashfin, 2024). Research focused on cloud computing and telecommunications has similarly highlighted AI-assisted detection and threat intelligence for environments characterized by large and rapidly changing data volumes (Manda, 2024). Recent studies have further emphasized adaptive and predictive approaches for dynamic networks and critical infrastructure (Khalaf *et al.*, 2025). Survey and framework-oriented research has also stressed proactive threat intelligence, predictive risk mitigation, and intelligent cybersecurity decision-making (Sarker, 2024). Studies addressing automated response and cyber resilience similarly support integrating detection with subsequent security actions. Related discussions of proactive AI-based defense and threat intelligence further reinforce the relevance of machine learning for evolving cybersecurity environments (Burns *et al.*, 2025). The present study contributes an empirical model comparison and feature-reduction analysis to this broader research direction. The results have practical implications for network intrusion-detection applications. The high recall obtained by XGBoost suggests that the model can identify malicious observations with a very low proportion of missed attacks within the evaluated test sample (Emmy and Iren, 2025). Its low false-positive rate is also desirable because excessive false alarms can increase analyst workload. The comparison between the complete and reduced feature sets additionally suggests that a compact representation may be considered when computational simplicity or feature availability is important (Kaium *et al.*, 2026). Deployment in operational networks would require validation using continuously changing traffic, unseen attack types, and realistic class distributions.

From an AI perspective, the results demonstrate the value of comparing models rather than assuming that a single learning technique is universally optimal. XGBoost and Random Forest substantially outperformed Logistic Regression, while the MLP also achieved strong results. The findings indicate that nonlinear ensemble learning can be particularly effective for structured network-flow data (Siam *et al.*, 2025). The feature-selection experiment further shows that predictive performance can remain high after reducing the input dimensionality (Femi and Medugu, 2025). These observations support the development of more efficient AI-based cybersecurity systems in which model complexity and feature availability are considered alongside predictive accuracy.

A major strength is the direct comparison of four different learning paradigms under a common experimental framework. The study also evaluates performance using multiple complementary measures rather than relying exclusively on accuracy (Reddy, 2021). The inclusion of precision, recall, F1-score, false-positive rate, AUROC, AUPRC, and confusion-matrix outcomes provides a broader assessment of detection behavior. In addition, comparing 78 and 24 features provides useful evidence regarding the effect of feature reduction on the strongest-performing model.

Several limitations should be acknowledged. The experimental analysis used a balanced sample of 200,000 observations rather than the complete dataset for model training and testing. Consequently, the reported performance should not be interpreted as representing every observation in the original dataset. The study also uses binary classification between benign and malicious traffic, which does not evaluate performance separately across individual attack categories (Umar and Abbas, 2022). In addition, the current experiments do not validate real-time deployment or automated response actions. Finally, the very high predictive scores should be interpreted in the context of the selected dataset, sampling strategy, and experimental design.

Future studies should evaluate the framework using larger and more diverse datasets containing contemporary attack patterns and realistic class distributions. Multiclass classification could also be

investigated to determine how effectively different attack categories can be distinguished. External validation on an independent dataset would provide stronger evidence of generalizability. Future work should additionally integrate the detection model with a measurable automated response layer and evaluate response latency, mitigation success, and false intervention rates. Adaptive or online learning could further enable the framework to respond to changing network behavior. Such extensions would move the proposed approach from predictive attack detection toward a more complete, operationally validated cyber defense system.

5. Conclusion

This study developed and evaluated an AI-driven framework for predictive cyber attack detection using labeled network-traffic data from the CIC-IDS2017 dataset. Multiple machine-learning approaches were examined to determine their effectiveness in distinguishing benign and malicious network activity. The comparative analysis showed that ensemble-based learning provided stronger predictive capability than the other evaluated approaches, with XGBoost emerging as the most effective model. The detailed classification analysis demonstrated that the selected model could distinguish benign and malicious traffic with very limited misclassification. Feature-selection analysis further indicated that reducing the number of network features can maintain strong detection capability while providing a more compact representation of the input data. The study contributes an empirical comparison of different AI/ML techniques for network attack detection and provides evidence supporting the use of ensemble learning for structured network-flow data. It also demonstrates the potential value of feature selection for developing more efficient predictive cybersecurity models. The findings indicate that AI-based predictive detection can support network security by identifying potentially malicious activity accurately and reducing unnecessary classification errors. The approach can provide a foundation for cybersecurity systems that require automated analysis of network traffic. However, practical deployment requires further validation under real-world network conditions. Future research should examine the framework using independent datasets, diverse and contemporary attack patterns, multiclass classification, and realistic network environments. Further work should also integrate and experimentally evaluate an automated security response layer to determine how effectively detected threats can be mitigated in real time.

References

1. ABDULRAHMAN, I. A., OGOR, U. C., AYODELE, G. T., ANADOZIE, C., & ALEBIOSU, J. (2025). AI-driven threat intelligence and Automated Incident Response: Enhancing Cyber Resilience through Predictive Analytics. *Research Journal in Civil, Industrial and Mechanical Engineering*, 2(1), 16-32.
2. Aramide, O. O. (2023). Predictive analytics and automated threat hunting: The next frontier in AI-powered cyber defense. *International Journal of Technology, Management and Humanities*, 9(04), 72-93.
3. Ashfin, P. (2024). AI-driven threat detection and response in cybersecurity. *Bulletin of Engineering Science and Technology*, 1(2), 125-143.
4. Bella, L., Lee, A., & Alamu, R. (2025). AI-Driven Threat Intelligence and Predictive Cybersecurity: Using Machine Learning to Forecast and Prevent Cyberattacks Before They Occur. *Article, Oct.*
5. Burns, E., Buks, K., & Amola, M. (2025). AI-Driven Threat Intelligence and Predictive Cyber Defense. *Article, Oct.*
6. Dorothy, A. B., Madhavidevi, B., Nachiappan, B., Manikandan, G., Patjoshi, P. K., & Sindhuja, M. (2024, August). AI-driven threat intelligence in cloud computing detecting and responding to cyber attacks. In *2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS)* (pp. 1-6). IEEE.
7. Emmy, E., & Iren, L. (2025). AI-Driven Threat Intelligence and Predictive Cyber Defense: Enhancing Proactive Threat Detection and Response in Evolving Cyber Landscapes.
8. Femi, A. G., & Medugu, M. (2025). Enhancing adaptive cybersecurity risk management through AI-driven threat detection. *Int. J. Trendy Res. Eng. Technol.*, 9(2), 1-14.
9. Garg, M., Kaza, P. R., Kilaru, A., Basha, S. S., Gunupudi, C., & Kondapalli, K. K. (2026, January). Adaptive ai-driven threat intelligence framework for proactive cyber defense in dynamic network environments. In *2026 International Conference on AI-Driven Smart Systems and Ubiquitous Computing (ICAUC)* (pp. 1995-2000). IEEE.

10. Islam, S. M., Bari, M. S., Sarkar, A., Obaidur, A., Khan, R., & Paul, R. (2024). AI-driven threat intelligence: Transforming cybersecurity for proactive risk management in critical sectors. *International Journal of Computer Science and Information Technology*, 16(5), 125-131.
11. Kaium, R., Alasa, L., Robert, K., Kaium, O., & Diana, K. (2026). Artificial Intelligence-Based Cyber Threat Detection and Response for Critical Infrastructure Security. *The Eastasouth Journal of Information System and Computer Science*, 4(01), 1-16.
12. Khalaf, N. Z., Barazanchi, A., Ibraheem, I., Radhi, A. D., 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.
13. Kingsley, E., Henrius, H., & Okunola, C. O. (2025). AI-Powered Threat Intelligence and Predictive Cyber Defense. *Article*, Oct.
14. Manda, J. K. (2024). AI-powered threat intelligence platforms in telecom: Leveraging AI for real-time threat detection and intelligence gathering in telecom network security operations. *Available at SSRN 5003638*.
15. Nallapareddy, V. S. S. R., & Katta, S. K. R. (2025, February). AI-enhanced cyber security proactive threat detection and response systems. In *2025 4th International Conference on Sentiment Analysis and Deep Learning (ICSADL)* (pp. 1510-1514). IEEE.
16. Rani, A. J. M., Muthu, S., Adaikkammai, A., Govarthanan, B., Srinivasan, S., & Nancharaiah, B. (2025, July). Investigating AI-Enabled Threat Intelligence for Preventative Cybersecurity: Real-Time Threat Detection and Response. In *2025 International Conference on Information, Implementation, and Innovation in Technology (I2ITCON)* (pp. 1-6). IEEE.
17. Reddy, A. R. P. (2021). The role of artificial intelligence in proactive cyber threat detection in cloud environments. *NeuroQuantology*, 19(12), 764-773.
18. Sarfraz, M., Sumra, I. A., Khalid, B., & Fatima, E. (2025). AI-driven predictive threat detection and cyber risk mitigation: a survey. *Journal of Computing & Biomedical Informatics*, 8(02).
19. Sarker, I. H. (2024). Introduction to AI-driven cybersecurity and threat intelligence. In *AI-driven cybersecurity and threat intelligence: Cyber automation, intelligent decision-making and explainability* (pp. 3-19). Cham: Springer Nature Switzerland.
20. Shaffi, S. M., Vengathattil, S., Sidhick, J. N., & Vijayan, R. (2025). AI-driven security in cloud computing: Enhancing threat detection, automated response, and cyber resilience. *arXiv preprint arXiv:2505.03945*.
21. Shah, S., & Parast, F. K. (2024). AI-driven cyber threat intelligence automation. *arXiv preprint arXiv:2410.20287*.
22. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP)*, 108-116.
23. Siam, M. A., Shan-A-Alahi, A., Tuhin, M. K., Hossain, E., Bashir, M., Lucky, K. Y., ... & Al Zaiem, A. (2025). AI-Driven Cyber Threat Intelligence Systems: A National Framework for Proactive Defense Against Evolving Digital Warfare. *Int. J. Comput. Exp. Sci. Eng*, 11(3).
24. Sivakumar, J., Salman, N. R., Salman, F. R., Salimova, H. R., & Ghimire, E. (2025). AI-driven cyber threat detection: enhancing security through intelligent engineering systems. *Journal of Information Systems Engineering and Management*, 10(19), 790-798.
25. Sunkara, G. (2022). AI-driven cybersecurity: Advancing intelligent threat detection and adaptive network security in the era of sophisticated cyber attacks. *Well Testing Journal*, 31(1), 185-198.
26. Umar, H., & Abbas, A. (2022). AI-Powered Threat Intelligence: Enhancing Cybersecurity with Predictive Analytics and Machine Learning.