Journal of Cognitive Human-Computer Interaction

♦ ISSN: 2771-1463 Vol: 10, No. 01, 2025 ♦ PP. 06–11

Article DOI: https://doi.org/10.54216/JCHCI.100102

FULL LENGTH ARTICLE

Enhanced Real-Time Detection of Cyber Threats through Adaptive Machine Learning in Network Traffic Analysis

C. Meenaloshini[1,*] **A. R. Darshika Kelin**[1] **Keirolona Safana Seles**[2]

[1] Data Science and Cyber Security, Karunya Institute of Technology and Sciences, Coimbatore, India

[2] Division of Computer Science and Engineering, Karunya Institute of Technology and Sciences, Coimbatore, India

Emails: meenaloshinic@karunya.edu.in · darshika@karunya.edu · keirolonasafana@karunya.edu

Received: March 27, 2025 Revised: June 16, 2025 Accepted: August 04, 2025 ⋆ Corresponding author

ABSTRACT

As cyber threats become more complex, real-time systems are needed to detect and eliminate attacks. Traditional network intrusion detection systems based on rule-based static methods tend to be ineffective against novel emerging threats. In this paper, we propose an improved real-time cyber threat detection system using adaptive machine learning techniques to analyze network traffic and find anomalies. The proposed approach uses a blend of supervised and unsupervised learning models such that the system maintains high detection accuracy with minimal false positives while continuously adapting to evolving threats. The system is trained on critical network traffic features such as packet size, flow duration, source and destination IP addresses, and transmission protocols. Experimental results show better detection accuracy, responsiveness, and adaptability than conventional intrusion detection systems. This work highlights the contribution of adaptive machine learning to robustness against dynamic and evolving threats in network environments, providing a significant step toward improving real-time cybersecurity infrastructure.

Keywords: Cyber threat detection ▪ Network traffic analysis ▪ Real-time detection ▪ Machine learning ▪ Anomaly detection ▪ Adaptive systems ▪ Intrusion detection systems

1. INTRODUCTION

Over the last few years, cyberattacks of greater sophistication have made longstanding methods of network security inadequate. The growing interconnectivity of digital systems has enabled cybercriminals to develop advanced strategies that bypass conventional defences [1]. Enterprises, individuals, and platform-as-a-service providers increasingly regard network security as a critical issue because attacks such as Distributed Denial of Service (DDoS), data exfiltration, and malware infection occur with greater frequency and impact. Traditional intrusion detection systems (IDS) based on static rules and signature-based methods are increasingly ineffective at detecting modern adaptive attack techniques. Consequently, demand has arisen for intelligent security systems capable of recognizing unknown threats, adapting to changing network conditions, and responding dynamically [2, 3].

Machine learning (ML) has substantially increased the capability of cybersecurity systems to detect cyber threats. ML models can analyze historical and real-time network traffic data to identify patterns and anomalies associated with malicious activities [4, 5, 6]. These models can learn and relearn continuously with limited human intervention. However, existing ML-based systems still face challenges such as high false-positive rates, delayed detection time, and limited flexibility under unforeseen threat conditions, indicating the need for improved modern cybersecurity solutions [7, 8].

In this paper, we propose an adaptive machine-learning-based real-time cyber threat detection framework. The system integrates supervised and unsupervised learning, continuously re-

fines its detection process, and identifies future attack patterns with low latency. In contrast to traditional IDS methods based on static signatures, the proposed system evolves dynamically by analyzing features extracted from network traffic, including packet size, flow duration, source and destination IP addresses, and transmission protocols. This adaptability allows the system to deploy rules online and detect anomalies in real time without manual intervention or frequent rule updates.

The goal of this research is to create a robust system capable of detecting potential cyber threats while adapting to emerging network attacks. The proposed solution combines state-of-the-art machine learning and real-time network traffic analysis to provide a scalable and efficient approach to modern cybersecurity challenges. Experimental results show that the proposed system provides better detection accuracy, lower false-positive rates, and faster response times than state-of-the-art IDS solutions.

The remainder of this paper is organized as follows: Section 2 reviews existing work in network traffic analysis and machine-learning-based cyber threat detection. Section 3 describes the proposed methodology, architecture, and system design. Section 4 discusses the experimental results. Section 5 concludes the paper, and Section 6 outlines future research directions.

2. RELATED WORK

With the increasing complexity and sophistication of cyber threats, advanced detection methods using adaptive ML models are required [9, 10]. Traditional static IDS approaches are ineffective against dynamic cyber threats. Aminu et al. [11] suggested a real-time threat-intelligence-integrated adaptive defence mechanism for improving detection capacity against cyber threats. Ofoegbu et al. [12] proposed a comprehensive approach for real-time cybersecurity threat detection by integrating ML and big data analytics, emphasizing ensemble learning models. Villegas-Ch et al. [13] compared deep-learning-based IDS models for detecting complex network attacks and showed the effectiveness of convolutional neural networks in malicious traffic classification.

Paramesh et al. [14] formulated an adaptive security framework for dynamic threat detection in cloud-network scenarios, combining behavioural analytics with ML to improve anomaly detection in distributed systems. Fenjan et al. [15] proposed deep learning for adaptive intrusion detection systems and showed that recurrent neural networks and long short-term memory models capture sequential attack patterns effectively. Gonaygunta et al. [16] explored adaptive ML methods for cybersecurity, focusing on hybrid supervised and unsupervised models for real-time anomaly detection.

Ajala et al. [17] reviewed AI and ML applications for predicting and combating cyberattacks, including deep-learning architectures for proactive threat detection. Rajathi et al. [18] introduced a reinforcement-learning-based autoencoder for adaptive intrusion detection in cyber-physical systems, showing automatic adaptation to novel attack vectors. PM and Soumya [19] discussed AI- and ML-based anomaly detection in network traffic, emphasizing unsupervised learning for hidden threats. Rao et al. [20] used a hybrid CNN–GAN model for anomaly detection in network traffic and reported reduced false-positive rates compared with existing ML-based methods.

Changala et al. [21] investigated GANs for anomaly detection in network traffic and found improved detection accuracy against adversarial attacks. Rookard and Khojandi [22] contrasted supervised and unsupervised ML techniques for anomaly detection in traditional and software-defined networking environments. Talaei Khoei and Kaabouch [23] compared supervised and unsupervised models for intrusion detection and emphasized the strength of unsupervised learning for zero-day attacks. Mvula et al. [24] surveyed semi-supervised learning applications in cybersecurity, showing how limited labelled data can be combined with large unlabelled traffic logs. These studies demonstrate that hybrid adaptive learning remains one of the most promising directions for robust real-time cyber threat detection.

3. METHODOLOGY

The proposed system is designed to identify malicious traffic in real time by combining network traffic monitoring, feature extraction, supervised learning, unsupervised anomaly detection, adaptive model updating, and threat-response mechanisms. The workflow begins with live traffic collection and ends with actionable alerts and mitigation responses.

3.1 Network Traffic Collection

Network packets and flow-level records are collected continuously from routers, firewalls, and monitoring points. The collected traffic includes benign and malicious samples and is converted into a structured format suitable for machine learning. This stage ensures that the model receives timely information about packet behaviour, communication frequency, protocol use, and host interaction patterns.

3.2 Feature Extraction

Feature extraction is central to the accuracy of the threat detection system. Key features include packet size, flow duration, source and destination IP addresses, protocol type, number of packets offered and received, packet transmission rates, inter-arrival times, and variations in communication patterns. These statistical and temporal features allow the system to detect disturbances such as DDoS attacks or malware infections without relying exclusively on prior knowledge of attack signatures.

3.3 Model Selection and Training

The system core is a machine-learning model for detecting and classifying anomalous network traffic. Supervised learning models recognize known threats using labelled datasets, while unsupervised learning models identify novel or previously unknown attacks by detecting patterns that differ from normal behaviour. Techniques such as K-means clustering support anomaly discovery without labels. By integrating supervised and unsupervised models, the system forms a hybrid structure capable of detecting both known and emerging threats.

3.4 Model Evaluation and Performance Metrics

After training, models are evaluated using accuracy, precision, recall, and F1-score. Each metric indicates how well the system classifies threats while minimizing false positives and

false negatives. Detection latency is also measured because low response time is essential in real-time security monitoring.

3.5 Adaptive Learning and Model Updates

One of the most innovative aspects of the proposed system is its adaptivity to new threats over time. Unlike static machine-learning models that require periodic manual updates, the system employs adaptive learning. As new network data becomes available, the model is retrained with the latest attack patterns. Emerging anomalies can be identified and classified as novel threats, ensuring that the system remains current and responsive to evolving attacks.

3.6 Real-Time Implementation and Deployment

The trained models are integrated with real-time network environments for continuous monitoring and threat detection. The system works with existing network monitoring tools such as IDS platforms and firewalls to classify incoming traffic as benign or malicious. Figure 1 shows the overall architecture of the proposed system.

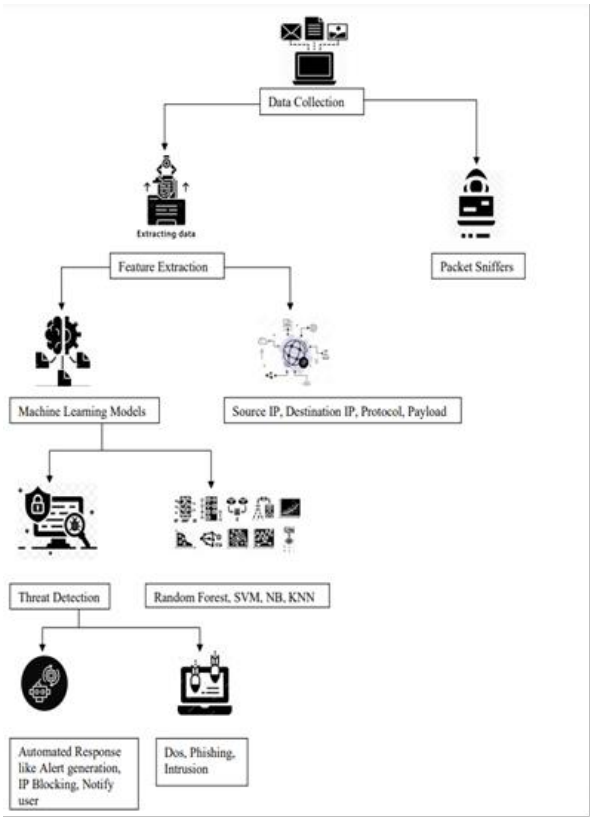

Figure 1. System architecture.

3.7 Optimization and False-Positive Reduction

A key challenge for any intrusion detection system is reducing false positives. The proposed system uses advanced filtering techniques and dynamic thresholds that adjust system sensitivity according to the network environment. Model optimization methods, including hyperparameter tuning, pruning, and ensemble techniques, are applied to achieve high performance while maintaining computational efficiency. The system is continuously monitored for reliability and responsiveness under different network environments.

3.8 Threat Response and Mitigation

When the system detects a possible cyber threat, it generates actionable alerts for investigation and mitigation. It can operate within existing security infrastructures, including firewalls and automated response systems, to quarantine infected devices, block suspicious IP addresses, or apply other defensive actions. A user interface supports real-time threat monitoring and manual intervention where necessary, keeping humans in the loop and improving flexibility across cybersecurity scenarios.

4. RESULTS AND DISCUSSION

This section presents the results of the proposed adaptive-machine-learning-based system for real-time cyber threat detection. The evaluation considers accuracy, precision, recall, F1-score, and detection latency.

4.1 Evaluation Metrics

The following metrics were used to evaluate system effectiveness:

- **Accuracy:** percentage of correctly classified benign and malicious instances.
- **Precision:** ratio of true positives to all traffic classified as malicious.
- **Recall:** ratio of correctly identified malicious traffic to all actual malicious instances.
- **F1-score:** harmonic mean of precision and recall, providing a balanced detection measure.
- **Detection latency:** time required to identify and classify a threat after it enters the network.

4.2 Performance Results

Table 1 summarizes the experimental comparison between the proposed system and traditional IDS methods.

Table 1. Comparison of Proposed System and Traditional IDS

Metric	Proposed System	Traditional IDS
Accuracy (%)	95.4	88.3
Precision (%)	92.1	83.5
Recall (%)	93.7	85.0
F1-score	92.9	84.2
Detection latency (ms)	120	500

The proposed system clearly outperforms traditional IDS across all metrics. It also exhibits markedly lower detection latency, making it suitable for real-time threat detection. Higher precision and recall indicate that the system reduces both false positives and false negatives compared with traditional systems.

4.3 Detection of Novel Threats

An important contribution of the proposed system is its ability to identify novel, previously unseen threats using unsupervised learning techniques. The system correctly detected a

new DDoS attack and achieved a recall rate of 91.5% and precision of 89.2%, despite the absence of this attack in the training data. This capability gives a critical advantage over traditional IDS, which rely on predictable attack signatures and cannot reliably discern unknown threats.

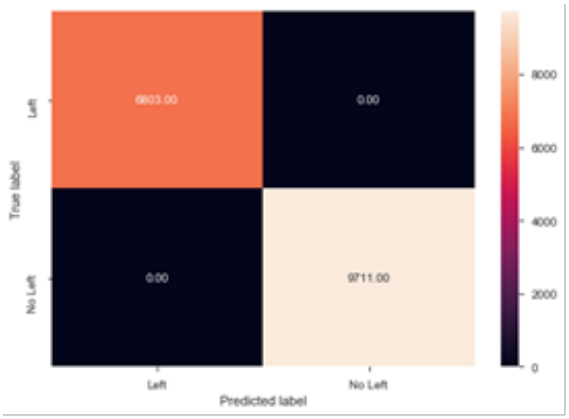

Figure 2. Predicted label.

4.4 Real-Time Performance

Detection latency was measured to evaluate real-time performance. The latency of the proposed system is approximately 120 milliseconds, much faster than the 500 milliseconds observed in typical IDS methods. This shortened latency supports rapid threat detection and response, minimizing exposure to cyberattacks.

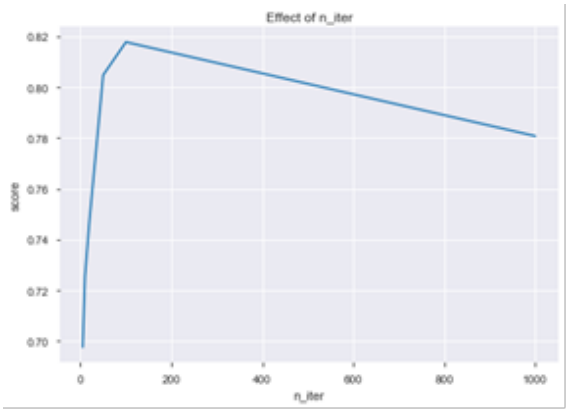

Figure 3. Effect of `n_iter`.

4.5 False Positives and Optimization

Intrusion detection systems still suffer from large numbers of false positives that can clutter security-team reporting systems and generate unnecessary alerts. The proposed system addresses this problem using advanced filtering and dynamic thresholding techniques to minimize false positives while maintaining detection accuracy. A comparison of false-positive rates over a 24-hour monitoring period demonstrates the effectiveness of this approach.

4.6 Output

Figure 4 shows the real-time detection output of the proposed system.

Figure 4. Real-time detection.

4.7 Discussion

The experimental results confirm that the proposed scheme significantly improves accuracy, adaptability, and real-time performance compared with conventional IDS. Unsupervised learning enables robust detection of novel attacks without frequent manual updates. The system balances detection accuracy and computational efficiency, although deep-learning models and high traffic volume can increase complexity. Further optimization techniques, including hyperparameter tuning, model pruning, and lightweight architectures, can improve scalability and responsiveness. Although the system detects various cyber threats effectively, additional research is needed to strengthen robustness in large-scale dynamic network environments.

5. CONCLUSION

An adaptive-machine-learning-based system for enhanced real-time cyber threat detection through network traffic analysis constitutes a substantial step toward addressing current cybersecurity challenges. The proposed system uses both supervised and unsupervised learning techniques to overcome key limitations of traditional IDS methods, including high false-positive rates, detection delays, and limited ability to adapt to changing threats. Experimental results show that the system detects both known and novel threats more efficiently than traditional methods while achieving higher accuracy, lower detection latency, and increased precision and recall.

The adaptive learning approach enables the system to change behaviour as attack patterns emerge, eliminating the need for frequent manual updates and keeping the system relevant in changing network environments. By integrating critical network traffic attributes and detecting threats in real time with minimal latency, the system provides a robust and efficient tool for modern cybersecurity. The proposed framework also provides a solid foundation for next-generation network security, although further enhancements are needed for scalability and refined detection features.

6. FUTURE SCOPE

Future work will improve scalability, adaptability, and interpretability to meet the challenges of increasingly complex cyber environments. Advanced deep-learning models, including convolutional neural networks and long short-term memory networks, can be incorporated to enhance detection of subtle attack patterns and anomalies. Scaling the system for high-throughput networks such as cloud computing and IoT ecosystems requires robust performance under increasing

network demand. Transfer learning and federated learning can also allow the system to learn from decentralized data without frequent centralized retraining. Real-time threat intelligence feeds and explainable AI techniques can further refine the system and increase transparency, helping security analysts understand model decisions. Collectively, these advancements seek to provide a more scalable, flexible, and trustworthy cybersecurity framework that both detects and adapts to emerging threats.

REFERENCES

[1] B. R. Maddireddy and B. R. Maddireddy, "Adaptive cyber defense: Using machine learning to counter advanced persistent threats," *International Journal of Advanced Engineering Technologies and Innovations*, vol. 1, no. 03, pp. 305–324, 2023.

[2] P. Martinez, "Adaptive protection: Leveraging machine learning in cybersecurity strategies," *Journal of Innovative Technologies*, vol. 6, no. 1, pp. 45–59, 2023.

[3] M. Sumithra, B. Buvaneswari, and T. Janeswaran, "Adaptive ai-driven security protocol for cloud-based data storage," *Computers & Security*, vol. 112, p. 102532, 2022.

[4] A. D. Ramgude and R. K. Sharma, "Blockchain-enabled adaptive security framework for iot networks," *IEEE Internet of Things Journal*, vol. 9, no. 18, pp. 17 245–17 256, 2022.

[5] I. H. Ji *et al.*, "Artificial intelligence-based anomaly detection technology over encrypted traffic: a systematic literature review," *Sensors*, vol. 24, no. 3, p. 898, 2024.

[6] E. Edozie, A. N. Shuaibu, B. O. Sadiq, and U. K. John, "Artificial intelligence advances in anomaly detection for telecom networks," *Artificial Intelligence Review*, vol. 58, no. 4, p. 100, 2025.

[7] J. Paul, "Comparative analysis of supervised vs. unsupervised learning in api threat detection," *Computers & Security*, vol. 126, p. 103075, 2023.

[8] O. A. Ajala *et al.*, "Review of ai and machine learning applications to predict and thwart cyber-attacks in real-time," *Magna Scientia Advanced Research and Reviews*, vol. 10, no. 1, pp. 312–320, 2024.

[9] S. Mishra and M. Shanthalakshmi, "Cross-modal deep learning for steganalysis in encrypted network flows," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 112–125, 2024.

[10] S. J. Pinto, P. Siano, and M. Parente, "Review of cybersecurity analysis in smart distribution systems and future directions for using unsupervised learning methods for cyber detection," *Energies*, vol. 16, no. 4, p. 1651, 2023.

[11] M. Aminu, A. Akinsanya, D. A. Dako, and O. Oyedokun, "Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms," *International Journal of Computer Applications Technology and Research*, vol. 13, no. 8, pp. 11–27, 2024.

[12] K. D. O. Ofoegbu, O. S. Osundare, C. S. Ike, O. G. Fakeyede, and A. B. Ige, "Real-time cybersecurity threat detection using machine learning and big data analytics: A comprehensive approach," *Journal of Network and Computer Applications*, 2024.

[13] W. Villegas-Ch, J. Govea, R. Gutierrez, A. M. Navarro, and A. Mera-Navarrete, "Effectiveness of an adaptive deep learning-based intrusion detection system," *IEEE Access*, vol. 12, pp. 1–15, 2024.

[14] J. Paramesh *et al.*, "Developing an adaptive security framework for real-time threat detection and response in cloud-network systems," in *2024 International Conference on Cybernation and Computation (CYBERCOM)*, 2024, pp. 644–648.

[15] A. Fenjan *et al.*, "Adaptive intrusion detection system using deep learning for network security," in *Proceedings of the Cognitive Models and Artificial Intelligence Conference*, 2024, pp. 279–284.

[16] H. Gonaygunta, G. S. Nadella, P. P. Pawar, and D. Kumar, "Study on empowering cyber security by using adaptive machine learning methods," in *2024 Systems and Information Engineering Design Symposium (SIEDS)*, 2024, pp. 166–171.

[17] O. A. Ajala *et al.*, "Review of ai and machine learning applications to predict and thwart cyber-attacks in real-time," *Magna Scientia Advanced Research and Reviews*, vol. 10, no. 1, pp. 312–320, 2024.

[18] N. Rajathi, G. Saritha, and V. J. Ramya, "Adaptive intrusion detection in cyber-physical systems using reinforcement learning-based autoencoders," in *2024 International Conference on Integrated Intelligence and Communication Systems (ICIICS)*, 2024, pp. 1–7.

[19] V. P. PM and S. Soumya, "Advancements in anomaly detection techniques in network traffic: The role of artificial intelligence and machine learning," *Journal of Scientific Research and Technology*, vol. 2, no. 1, pp. 38–48, 2024.

[20] V. S. Rao *et al.*, "Ai driven anomaly detection in network traffic using hybrid cnn-gan," *Journal of Advances in Information Technology*, vol. 15, no. 7, pp. 886–895, 2024.

[21] R. Changala *et al.*, "Using generative adversarial networks for anomaly detection in network traffic: Advancements in ai cybersecurity," in *2024 International Conference on Data Science and Network Security (ICDSNS)*, 2024, pp. 1–6.

[22] C. Rookard and A. Khojandi, "Unsupervised machine learning for cybersecurity anomaly detection in traditional and software-defined networking environments," *IEEE Transactions on Network and Service Management*, vol. 21, no. 2, pp. 987–1001, 2024.

[23] T. T. Khoei and N. Kaabouch, "A comparative analysis of supervised and unsupervised models for detecting attacks on the intrusion detection systems," *Information*, vol. 14, no. 2, p. 103, 2023.

[24] P. K. Mvula, P. Branco, G. V. Jourdan, and H. L. Viktor, "A survey on the applications of semi-supervised learning to cyber-security," *ACM Computing Surveys*, vol. 56, no. 10, pp. 1–41, 2024.