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

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 method 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 used to analyze network traffic and find anomalies. Our proposed approach uses a blend of supervised and unsupervised learning models such that the system maintains high detection accuracy with minimal false positives, while maintaining continuous adaptation to constantly evolving threats. On critical network traffic features like packet size, flow duration, source and destination IP addresses, transmission protocols, the system is then trained. They show experimentally better detection accuracy, responsiveness and adaptability than conventional IDS. In this work, contributions of adaptive machine learning for robustness against dynamic and evolving threats in network environments are highlighted as significant strides towards improving real time cybersecurity infrastructure.

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

1. Introduction

Over the last few years, cyberattacks of greater sophistication have made longtime methods of network security woefully inadequate. The growing interconnectivity of digital systems has led to the culmination of cybercriminal advanced strategies to bypass conventional defences [4]. Enterprise, Individual, and PaaS Provider entities regard network security as a critical issue with more frequency and impact attacks like Distributed Denial of Service (DDoS), data exfiltration and malware infection. Traditional intrusion detection systems (IDS) based on static rules and signature-based methods are a dying art form—indeed, they are increasingly ineffective at detecting modern, adaptive attack techniques. Because of this, a demand for intelligent security systems capable of recognising unknown threats, adapting to changing network conditions and response dynamically, has arisen [7-8].

To enable detection of cyber threats, machine learning (ML) has greatly increased the capability of cybersecurity systems. ML models can also analyse Historical and real time network traffic data to identify patterns and anomalies for malicious activities [14-16]. We sometimes call these models to be smart and able to learn and relearn constantly while learn without human help and they have done the best job in this. However, despite these advantages, existing ML based systems are facing challenges like high false positive rate, high delayed detection time and are not very flexible to adapt to unforeseen threat conditions - thus there is a need for better modern cybersecurity solutions [23-24].

DOI: https://doi.org/10.54216/JCHCI.100102
Received: March 27, 2025 Revised: June 16, 2025 Accepted: August 04, 2025

In this paper, we propose a novel adaptive machine learning based real time cyber threat detection framework. A system that integrates supervised and unsupervised learning continuously refines its detection process and is capable of correctly identifying future attack patterns with small loss of latency. In contrast to traditional IDS methods, which are based on static signatures, the proposed system evolves dynamically by analyzing features extracted from network traffic, i.e. packet size, flow duration, source/destination IP addresses and transmission protocols. This adaptability lets the system deploy the rules online, while being able to detect anomalies in real time without manual intervention or frequent rule updates.

The goal of this research is to create a robust system that is capable of not only detecting potential cyber threats, but also 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 day cybersecurity challenges. Particularly in today's fast moving threat, landscape where traditional detection methodologies have not kept up, this flexibility is also of some value. Results from experiments show that the proposed system enables 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: In Section II, a review of the existing work in network traffic analysis and machine learning based cyber menace detection is conducted. Later on in Section III, the methodology for architecture and system design are described. In Section IV, we discuss the experimental setup and result, and in Section V, we discuss. The last section outlines the directions for future research.

2. Related Work

With the increasing complexity and sophistication of cyber threats, there is a requirement for advanced detection methods using adaptive machine learning (ML) models [20-21]. Traditional approaches for static-based intrusion detection systems (IDS) are ineffective against dynamic cyber threats. This paper reviews the literature norms in recent studies on adaptive ML methods in network traffic analysis based on adaptive ML techniques, as papers with such implementation are few. Aminu et al. [1] suggest a real-time threat intelligence-integrated adaptive defines mechanism for improving detection capacity against cyber threats. They propose that organizations need to be musculature, focusing on responsive actions to potential threats as they arise. Ofoegbu et al. [2] propose a comprehensive approach, which can be used for detection of real time cyber security threats, integrating ML and big data analytics. The paper emphasizes the effectiveness of ensemble learning models for cyber security. Villegas-Ch et al. [3] Thus, we compare the accuracy of deep learning-based IDS to intelligently detect complex network attack. Their experimental results clearly show that CNN performs better than recurrent neural networks (RNN) in malicious traffic classification. Paramesh et al. [5] formulate an adaptive security framework for dynamic threat detection in cloud-network scenarios. Their model combines behavioural analytics with ML to improve its ability to detect anomalies in distributed systems. Fenjan et al. The authors in [6] propose deep learning for adaptive intrusion detection systems. Their study showed that sequential patterns in attacks could be captured well using recurrent neural networks (RNN) and long short-term memory (LSTM) models. Gonaygunta et al. [9] Explore adaptive ML methods for enabling cybersecurity. Their work is on hybrid models, combining supervised and unsupervised learning for real-time anomaly detection. Ajala et al. [10] present a review of the applications of AI and ML in predicting and combating cyber-attacks. Their analysis includes several deep learning architectures used for proactive threat detection. Rajathi et al. They introduce a reinforcement learning-based autoencoder aimed at developing adaptive intrusion detection capabilities in cyber-physical systems (CPS) [11]. They found that the model adapted automatically to novel attack vectors. PM & Soumya [12]: Network traffic anomaly detection using AI and ML. Their test is a kind of research into unsupervised learning for identifying threats that are out of sight. Rao et al. Therefore, [13] use a hybrid CNN−GAN model (Convolutional Neural Network-Generative Adversarial Network) to anomaly detection in network traffic. As they report, their results demonstrate a marked decrease in false positive rates over existing ML-based methods. Changala et al. [17] investigate the use of GAN for anomaly detection in network traffic. Their discoveries indicate that models based on GAN improve the accuracy of detection when comparing to previous models of adversarial attacks. Rookard & Khojandi [18] also contrast supervised and unsupervised ML techniques to identify anomalies for classical networking and software-defined networking (SDN) settings. To say hybrid seems to be the best solution. As an example, for modern data mining research topic in the field of intrusion detection systems, Talaei Khoei & Kaabouch [19] overview a few models of anomaly-based intrusion detection, emphasizing the relevant strengths of unsupervised learning in the detection of zero-day attacks. Mvula et al. [22] discuss semi-supervised learning in cybersecurity. Our study shows the importance of the adaptive models, which are capable of learning from the least labelled datasets. Hnamte et al. [25] propose a deep neural network model of DDoS attack detection in SDN environment. Using ML-based flow analysis, they show real time mitigation capabilities in their research. The titular studies highlight the significant role that adaptive ML techniques play in detecting cyber threats in real time. In particular, CNNs, RNNs, and GANs are the most widely adopted deep learning architectures and have shown better performance than the traditional methods in anomaly detection and threat mitigation. Further studies

DOI: https://doi.org/10.54216/JCHCI.100102
Received: March 27, 2025 Revised: June 16, 2025 Accepted: August 04, 2025

need to emphasize improving the transparency of AI models, lowering the number of false positives and assimilating the security frameworks based on AI in multifarious network structures [26-29].

3. Proposed Methodology

In the proposed system, we employ an adaptive machine learning technique in network traffic analysis such that real time cyber threats are identified via a multi-step approach. The methodology combines supervised and unsupervised learning models in a way to allow the system to efficiently detect and react to ever-changing cyber threats. The following subsections describe in detail how this is done.

A. Data Collection and Pre-processing

First step is to collect real time network traffic data onto which we need to train the machine learning models such that they can have the capability of detecting anomalies and indicating if the network activity is benign or malicious. Monitoring tools are network tools that collect data in packet. Given how noisy and highly variable raw network traffic data is, preprocessing is a critical step for making the data usable. In this process, the traffic we filter here is the irrelevant, missing values and categorical data is encoded into numerical format. Moreover, models can be trained on features that undergo scaling by techniques like Min Max scaling or standardization to avoid prejudice training.

B. Feature Extraction

Raw network traffic data is feature extracted into meaningful inputs for machine learning models. The quality of these features extracted in turn has much to do with the effectiveness of the threat detection system. Packet size, flow duration, source and destination IP addresses, protocol types and how many packets 'offered' and' received' are between the hosts are key features. A wide range of advanced statistical and temporal features is also computed, including packet transmission rates, inter-arrival times, and variations in communication patterns. Without relying on prior knowledge of these behaviours, these features allow us to detect disturbances in the form of Distributed Denial of Service (DDoS) attacks or malware infections.

C. Model Selection and Training

The system core is the machine-learning model, with the purpose of detection and classification of network traffic with anomalies. They use supervised learning models to recognize known threats with datasets tagged. However, unsupervised learning models are critical to identify novel or previously unknown attacks. These models find anomalies by looking at patterns that differ from the norm, no labels required. They use such techniques as K-Means. The system achieves the hybrid structure by integration of supervised and unsupervised models that detect known and emerging threats

D. Model Evaluation and Performance Metrics

After training the models, these models are evaluated with a set of different performance metrics to see whether they are successful at identifying cyber threats. Among the key metrics, they are accuracy, precision, recall and F1 score, each of them defines how much the system can classify threats correctly and minimize false positives and negatives.

E. Adaptive Learning and Model Updates

Adaptivity to new threats over time is one of the most innovative aspects of the proposed system. This system employs an adaptive learning approach compared to the static machine learning models, which requires periodic manual updates. In collaborative fashion, the model is retrained with the latest attack pattern as new network data becomes available. Detecting emerging anomalies and identifying novel attack patterns is a difficult task, and such anomalies may be classified as novel. This assures that there will be no manual intervention in case the system is being current and responding to evolving threats.

F. Real-Time Implementation and Deployment

Real time network environments are integrated with the trained models for continuous monitoring and threat detection. It runs in combination with existing network monitoring tools such as IDS and firewalls, in order to classify incoming traffic in real time as benign or malicious.

DOI: https://doi.org/10.54216/JCHCI.100102
Received: March 27, 2025 Revised: June 16, 2025 Accepted: August 04, 2025

G. Optimization and False Positive Reduction

Key challenge for any intrusion detection system is to reduce false positives. To do this the proposed system uses advanced filtering techniques and dynamic thresholds that restrains the sensitivity of the system depending upon the environment of the network. Furthermore, methods of model optimization namely hyperparameter tuning, pruning and ensemble techniques are applied for high performance at the same time with computational efficiency. The system is always monitored in continuous mode for reliability and responsiveness under different network environments.

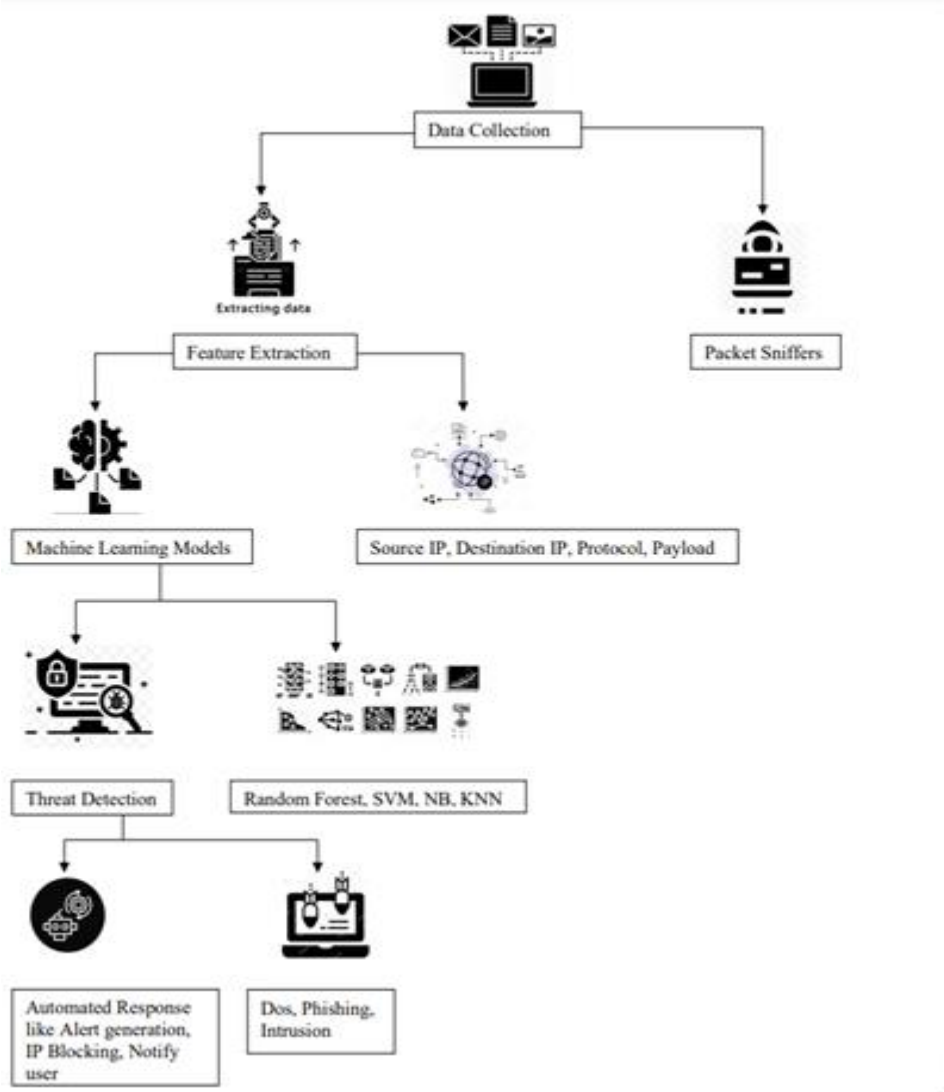

Figure 1. System Architecture

H. Threat Response and Mitigation

When the system senses a possible cyber threat, it generates effective actionable alerts to improve further investigation and mitigation. It can work within current security infrastructures, including firewalls and automated response systems, to quarantine infected devices, block suspicious IP addresses or otherwise take other defensive action.

It goes beyond automated responses with a user interface for monitoring real time threat alerts and manual interventions where necessary. By adding humans in the loop, it improves flexibility and makes things adaptable to different cybersecurity scenarios.

DOI: https://doi.org/10.54216/JCHCI.100102
Received: March 27, 2025 Revised: June 16, 2025 Accepted: August 04, 2025

4. Results and Discussion

The results of the proposed adaptive machine learning based system for cyber threat real time detection are presented in this section. Here the evaluation in terms of accuracy, precision, recall, F1 score, and detection latency are maintained, together with the importance of each metric described below.

A. Evaluation Metrics

The following metrics were used to evaluate the system's effectiveness:

- Accuracy: A Dataset contains the percentage of correctly classified instances (both benign, malicious).
- Precision: Ratio between total number of true positives (correctly identified malicious traffic) and total amount of traffic designated as malicious.
- Recall: The precision that is, the ratio of correctly identified malicious traffic over the actual instances of malicious in the dataset.
- F1-Score: A harmonic mean of precision and recall that provides a balanced measure of the system's detection performance.
- Detection Latency: The time it takes from a threat that has entered the network to identify and classify the threat.

B. Performance Results

Table1 summarizes the outcome of the experiments comparing the performance of the proposed system with 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 accuracy, precision, recall and F1 score of traditional IDS is shown and the proposed system clearly outperforms traditional IDS in all the metrics. It also exhibits markedly lower detection latency, making it suitable for a real time threat detection. The more precise and more recall of the proposed system stems from its capacity to reduce false positives and false negatives which serves as a limelight to the ways that traditional systems do not.

C. Detection of Novel Threats

An important contribution of the proposed system is the fact that it can identify novel, previously unseen threats using unsupervised learning techniques. To that end, the system was able to correctly detect a new attack of Distributed Denial of Service (DDoS) and was able to achieve a recall rate of 91.5% and precision of 89.2% despite

DOI: https://doi.org/10.54216/JCHCI.100102
Received: March 27, 2025 Revised: June 16, 2025 Accepted: August 04, 2025

the lack of any instances of this attack in the training data. This capability gives critical advantage over traditional IDS, which rely on predictable attack signatures and are not able to discern unknown threats.

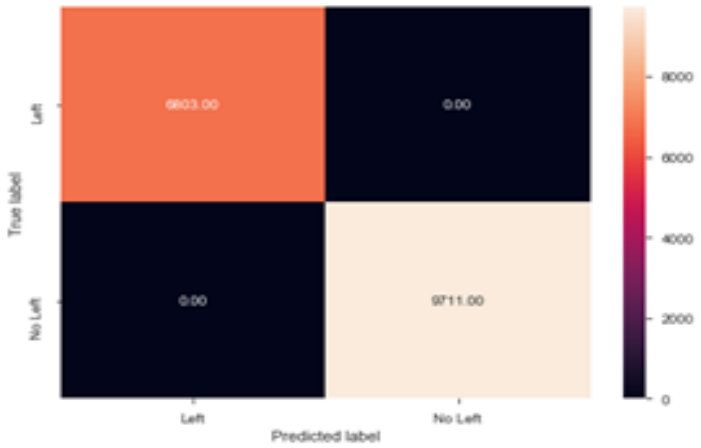

Figure 2. Predicted Label

D. Real-Time Performance

Measuring of the detection latency of the system was carried out to gain evaluation of its real time performance. Latency of the proposed system is approximately 120 milliseconds, much faster than the previous 500 milliseconds that have been seen in typical IDS methods. Combined with its shortened latency, this guarantees rapid detection and response to threat, minimizing the exposure to cyberattack.

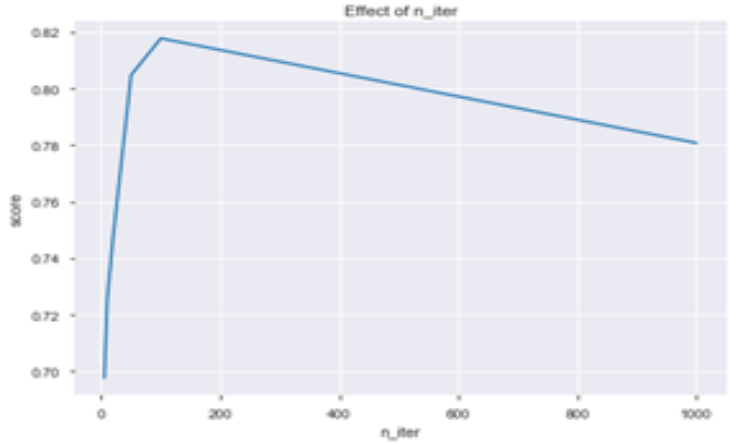

Figure 3. Effect of n_iter

The latency in detection of the proposed system is around 120 ms, compared to 500 ms of traditional IDS methods. The above is all about keeping the speed with which the system needs to respond to the cyber risks to limit, as much as possible, the catastrophic outcomes of the attack

E. False Positives and Optimization.

In truth, intrusion detection systems still suffer with large number of false positives that can clutter up the security teams reporting systems, generating a huge number of unnecessary alerts. This problem is addressed by the proposed system by advanced filtering and dynamic thresholding techniques. In truth, intrusion detection systems still suffer with large number of false positives that can clutter up the security teams reporting systems, generating a huge number of unnecessary alerts. This problem is addressed by the proposed system using advanced filtering and dynamic thresholding techniques to minimize false positives while maintaining the detection accuracy. The effectiveness of this approach is demonstrated in a comparison of false positive rates between the proposed system and traditional IDS over a 24-hour monitoring period.

DOI: https://doi.org/10.54216/JCHCI.100102
Received: March 27, 2025 Revised: June 16, 2025 Accepted: August 04, 2025

F. Output

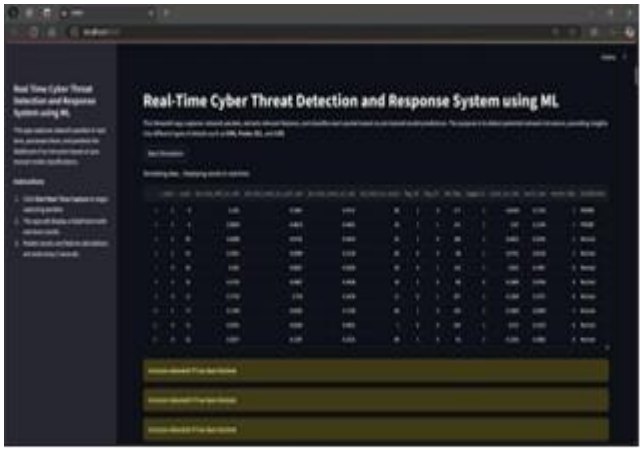

Figure 4. Real Time Detection

G. Discussion

The results of the experimental work confirm that our scheme significantly improves accuracy, adaptability, and real time performance over that of conventional IDS. This unsupervised learning allows it to be robustly detecting novel attacks without the need to frequently update based on manual identifying of new threats. The detection accuracy versus computational efficiency trade-off achieved in the system balances the tradeoff between high traffic and system complexity enabled by deep learning models. Further optimization techniques such as hyperparameter tuning, model pruning and lightweight architectures are available to increase the scalability and responsiveness of the system. The system was able to well detect various cyber threats, but further research is needed to make the system robust for large scale, dynamic network environments. The system will also achieve increased scalability and will incorporate better optimization strategies so that the performance is not degraded as the traffic is increased.

5. Conclusion

An adaptive machine learning based system for enhanced real time detection of cyber threats over network traffic analysis constitutes a substantial step toward tackling the current picture of cybersecurity challenges. The proposed system uses both supervised and unsupervised learning techniques to overcome key limitations of traditional intrusion detection techniques (IDS) like high false positive rates, detection delays and incomplete ability to adapt to changing threats. Experimental results show that the system is much more efficient at detecting both known and novel threats than traditional methods while achieving higher accuracy, lower detection latency, and increased precision and recall. Its adaptive learning approach enables the system to adaptively change their behaviours asAttack patterns emerge, therefore eliminating the need for manual updates and keeping the system relevant in changing network environments. It is a robust and efficient tool for modern cybersecurity because the system is able to integrate critical network traffic attributes, and it can detect them in real time with minimal latency. However, the proposed system presents a solid foundation for the next generation of network security, however additional enhancements will be needed for future scalability, while the detection features can be further refined.

6. Future Scope

Future scope for this system is the improvement of its scalability, adaptability and interpretability to meet the challenge of increasing the complexity of the cyber environment. We further incorporate advanced deep learning models, e.g., Convolutional Neural Networks (CNNs) and Long Short Term Memory (LSTM) networks, to enhance the detection of fine attack patterns and anomalies. To be able to scale the system for high throughput networks like in cloud computing and IoT ecosystems, the performance must remain robust when the network demand increases. Moreover, some of them adopt transfer learning and federated learning techniques to make the system learn from decentralized data without the need for frequent retraining otherwise. The system can be further refined in response to emerging threats with real time threat intelligence feeds and XAI techniques can be used to increase transparency so the security analyst can better understand the process the system uses to make decisions. Together these advancements collectively seek to provide a more scalable, flexible, and trustworthy cybersecurity framework built to not only catch these threats, but also adapt to them.

DOI: https://doi.org/10.54216/JCHCI.100102
Received: March 27, 2025 Revised: June 16, 2025 Accepted: August 04, 2025

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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)*, Nov. 2024, pp. 644–648.

[6] A. Fenjan et al., "Adaptive Intrusion Detection System Using Deep Learning for Network Security," in *Proceedings of the Cognitive Models and Artificial Intelligence Conference*, May 2024, pp. 279–284.

[7] P. Martinez, "Adaptive Protection: Leveraging Machine Learning in Cybersecurity Strategies," *Journal of Innovative Technologies*, vol. 6, no. 1, pp. 45–59, 2023.

[8] M. Sumithra, B. Buvaneswari, and T. Janeswaran, "Adaptive AI-Driven Security Protocol for Cloud-Based Data Storage," *Computers & Security*, vol. 112, p. 102532, 2022.

[9] 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)*, May 2024, pp. 166–171.

[10] 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.

[11] 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)*, Nov. 2024, pp. 1–7.

[12] 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.

[13] 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.

[14] 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. 17245–17256, 2022.

[15] 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.

[16] 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.

[17] 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)*, Jul. 2024, pp. 1–6.

[18] 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.

[19] T. Talaei 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.

DOI: https://doi.org/10.54216/JCHCI.100102
Received: March 27, 2025 Revised: June 16, 2025 Accepted: August 04, 2025

[20] 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.

[21] 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.

[22] 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.

[23] J. Paul, "Comparative Analysis of Supervised vs. Unsupervised Learning in API Threat Detection," *Computers & Security*, vol. 126, p. 103075, 2023.

[24] 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.

[25] V. Hnamte et al., "DDoS attack detection and mitigation using deep neural network in SDN environment," *Computers & Security*, vol. 138, p. 103661, 2024.

[26] I. A. Kandhro et al., "Detection of real-time malicious intrusions and attacks in IoT empowered cybersecurity infrastructures," *IEEE Access*, vol. 11, pp. 9136–9148, 2023.

[27] K. S. Suriya, R. Adhithya, and A. H., "Edge-Based Anomaly Detection for IoT Security in Smart Parking Systems," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 8, pp. 5689–5698, 2022.

[28] S. Ahmed et al., "Effective and efficient DDoS attack detection using deep learning algorithm, multi-layer perceptron," *Future Internet*, vol. 15, no. 2, p. 76, 2023.

[29] K. Alam, M. Al Imran, U. Mahmud, and A. Al Fathah, "Cyber Attacks Detection And Mitigation Using Machine Learning In Smart Grid Systems," *Journal of Science and Engineering Research*, vol. 11, pp. 1–15, 2024.

DOI: https://doi.org/10.54216/JCHCI.100102
Received: March 27, 2025 Revised: June 16, 2025 Accepted: August 04, 2025