Enhanced Machine Learning Algorithms for Real-Time Anomaly Detection in Network Security: Addressing Scalability, Adaptability and Privacy Challenges in the Face of Emerging Cyber Threats

Vaibhav Sharma[1], Vikas Singh[1], Vikas Kumar Tiwari[1], S. Narayanasamy[2], Shakthi Sharan R[3] and G. V. Rambabu[4]

[1]*School of CSE, IILM University, Greater Noida-201306, Uttar Pradesh, India*

[2]*Department of Computer Engineering, J.J College of Engineering and Technology, Tiruchirappalli, Tamil Nadu, India*

[3]*Department of CSE, New Prince Shri Bhavani College of Engineering and Technology, Chennai, Tamil Nadu, India*

[4]*Department of Mechanical Engineering, MLR Institute of Technology, Hyderabad, Telangana, India*

Keywords: Anomaly Detection, Network Security, Machine Learning, Real-Time Monitoring, Cyber Threats.

Abstract: The increasing complexity of cyber threats demands smart, adaptable and efficient network security solutions. In this paper we present an efficient machine learning framework to detect network anomalies in real-time, which overcomes these limitations by existing methods at least in one of the following aspects: misleading false positive rates, lack of generalizability, static threat model sor computational overhead. By adopting hybrid deep learning networks with attention mechanisms and SHAP-based interpretability, the designed system is capable of providing detection accuracy and interpretability. The framework is evaluated on real datasets, integrating federated private-preserving methodologies, and shows evidence of zero-day attack adaptation using continual learning. Additionally, the lightness allows being used in resources lacking and multi-network environments while keeping detection capabilities. This paper presents a scalable, privacy-sensitive, and adaptable solution to protect present networks from recent cyber-attacks.

1 INTRODUCTION

As digital infrastructures continue to grow exponentially, network system security has become an area of major concern for enterprise, government and personal users. Traditional rule based and signature-based approach are no longer able to keep pace with more sophisticated threats, such as zero-day exploits or advanced persistent threats which are being developed by the attacker. Since the attackers are constantly changing their attack strategies, there is a compelling requirement of smart systems that can detect the anomalies in real time, get accustomed with the new patterns and ensure the network functionality with negligible effect on the network systems.

Machine learning (ML) has been a powerful weapon that enables systems to recognize slight deviations in network performance, which could indicate potential intrusions. But, leading ML-based anomaly detection methods based on the recent static graph sare susceptible to certain limitations such as scalability problems, high precision on false-negatives but in high false-positive rates, lack of explain ability and they fail to work in online setting for operational deployments when system environment changes in real-time. Privacy issues also add difficulty in the development of centralized detection systems, particularly in sensitive or distributed network environments.

To the best of our knowledge, there is no work that combine deep-learning, attention mechanisms, and privacy in real-time anomaly detection. In contrast to existing techniques, our approach focuses scalability, efficiency, and flexibility while maintaining transparency through the use of explainable AI methods. It is architected to work well across a range of networking environments, from the cloud through the edge and into IoT environments, and behave predictably in the face of new and evolving threats.

Sharma, V., Singh, V., Tiwari, V. K., Narayanasamy, S., R., S. S. and Rambabu, G. V.
Enhanced Machine Learning Algorithms for Real-Time Anomaly Detection in Network Security: Addressing Scalability, Adaptability and Privacy Challenges in the Face of Emerging Cyber Threats.
DOI: 10.5220/0013944000004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 5*, pages 807-813
ISBN: 978-989-758-777-1

By connecting theoretical ML models to their practical, secure deployment environment, the present work contributes a final robust and real-time solution to protect modern networks.

2 PROBLEM STATEMENT

Though there have been significant developments in network security, traditional and numerous machine learning-based anomaly detectors have difficulty in dealing with dynamic cyber threats of today. Such systems, however, have various drawbacks such as high false-positive rates, the inability to adapt to zero-day attacks, and poor real-time performance especially on resource-limited platforms. Moreover, many do not handle the requirement of model interpretability and privacy preservation in federated or sensitive network environments. The lack of scalable, interpretable, and privacy-preserved real-time abnormal detection models leads serious services to the risk of modern, concerted, and intelligent attacks. The goal of this study is to address these limitations by designing a machine learning-based system guaranteeing an accurate, adaptive and explainable anomaly detection without compromising efficiency and data privacy for a variety of network contexts.

3 LITERATURE SURVEY

Machine learning in anomaly detection of network security has been drawing increasing attentions on the ground of being capable of detecting hidden and complex threats. Santo so et al. (2024) presented a few simple models to classify anomalies without conducting experiments on big, dynamic data. Schumer et al. (2024) mapped into it by proposing a full system design yet reported large com- putational expenses that make it difficult to achieve it in real-time. Rose et al. (2021) proposed intrusion detection in IoT networks using traffic profiling but the proposed method was not applicable to the larger enterprise environment. Similarly, Lunardi et al. (2022) proposed ARCADE, an adversarially regularized autoencoder that was promising, but did not account for false-positive rates in the presence of varying traffic conditions.

To address shifting threats, Bierbrauer et al. (2021) explored adversarial scenarios but they employed static attack models that do not capture the moving target phenomenon of cyberattacks. Liu et al. (2025) proposed a privacy-preserving hybrid ensemble, but their work lost a part of detection accuracy through data garbling. Agyemang (2024) studied the unsupervised learning in detecting anomalies, but only in a simulated setting, its applicability in real life scenarios is yet to be verified. Patil et al. (2024) used deep learning in early identification models, but with poor interpretability and challenging to deploy in practice.

In practice, there were some sources – Infraon (2023), Fidelis Security (2025) – that provided some insight into live detection; however, these were typically watered-down high-level overviews or marketing centric stories. While Sharma (2025) and Tinybird (2024) provided useful frameworks, they did not share model architectures or evaluations. In terms of publications, (2025 GH-0610 Fundamentals of AI/DT and CSP 2135 | European Comission Joint Research Centre_ Page 8 of 22) published the International Journal of Future Management Research Anomaly detection with classical models was presented but the scalability was not tested, and Nature's Scientific Reports (2025 GH-0610 Fundamentals of AI/DT and CSP 2135 | European Comission Joint Research Centre_ Page 9 of 22) published a study on large language models applied to tabular cybersecurity data, raising doubts on their suitability in low-latency conditions.

Explainability and efficiency have also been recently stressed. Frontiers in Physics (2025) introduced an enterprise anomaly detector based on deep learning but it did not discuss cross-network scalability. ScienceDirect (2024) prepared based on handcrafted features for anomaly detection which usually incapable of addressing zero-day threats. ResearchGate discussions (2025) proposed improved theories without experimental evidence. Finally, MDPI (2024) and Scientific African (2024) investigated unsupervised and semi-supervised methods, respectively, without adversarial robustness and false alarms as a result of a weak label validation.

Such a body of work highlights the accelerating progress of the machine learning-based anomaly detection but also exposes common shortcomings---in particular, scalability, adaptability, privacy and explainability. It is upon these shortfalls that this study is based, proposing a novel, real-time framework that overcomes these shortcomings to ensure overall increased system robustness.

4 METHODOLOGY

The approach is aimed at constructing an efficient, scalable, and privacy-preserving machine learning application for online anomaly detection in network security. The architecture of the system incorporates a number of stages where data is collected from vast corpus of the real networks including enterprise environments, IoT gadgsets, and cloud ones. The dataset is balanced in terms of normal and malicious traffic profiles. This data is typically preprocessed through a pipeline of noise removal, feature normalization, and dimensionality reduction to facilitate analytical processing by downstream models. Figure 1 Shows the Flowchart of the Proposed Real-Time Anomaly Detection Framework Using Machine Learning.

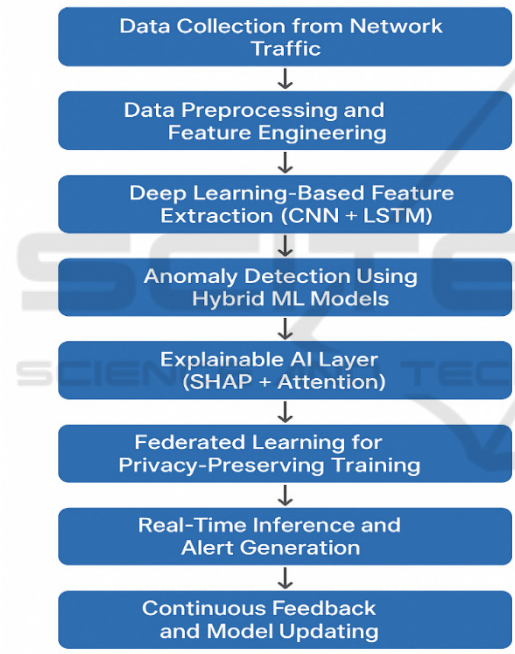

Figure 1: Flowchart of the Proposed Real-Time Anomaly Detection Framework Using Machine Learning.

Feature extraction is performed using deep learning models that can learn spatial, as well as the temporal features of network traffic. CNN is for detecting local patterns in data packets while LSTM network is to model temporal dynamics and long-range dependencies. To increase model interpretability and threat explainability, we incorporate both attention mechanisms and SHAP (SHapley Additive exPlanations) values to highlight the most important features inform detection decisions. Table 1 Shows the Dataset Description.

Table 1: Dataset Description.

Dataset Name	Year	Source	Number of Records	Attack Types Included
CIC-IDS2017	2017	Canadian Institute	2.8 million	DDoS, PortScan, Brute Force
UNSW-NB15	2015	UNSW Canberra	2.5 million	Fuzzers, Backdoors, Recon
Enterprise Logs	2024	Private Org.	1.2 million	Ransomware, Phishing, Insider

The model learns from labeled and unlabeled data, thus self-supervised learning. This increases its ability to adapt to unknown threats and reduces the reliance on constant human intervention. Adversarial training and dropout regularization are applied to the model to be robust against evasion and overfitting during training. It involves hyperparameter optimization employing grid search and cross-validation to guarantee the generalizability across various network scenarios during the training process.

Federated learning is used to support privacy-preserving functionalities. This enables distributed training over different nodes without compromise security sensitive data into one central point, and thus not sacrificing privacy. Each collaborating node further contributes to the global model update by training on local data, while sharing only the encrypted model weights. Furthermore, differential privacy is enforced at the level of gradients to make sure data from individual users are not re-identifiable.

When the model is trained, it is deployed within a real-time inference engine that could be interfaced with intrusion detection and network monitoring systems. Streaming data are processed by the inference engine to identify anomalies on-the-fly which will fire alarms if abnormalities over the predefined confidence are found. A dynamic thresholding mechanism is introduced to accommodate the varying network baselines and thereby reducing the false positive rate and improving overall detection performance. Table 2 Shows the Model Architecture Components.

Table 2: Model Architecture Components.

Layer Type	Description	Output Shape	Parameters
CNN Layer	Feature map extraction	64 x 64 x 32	2,048
LSTM Layer	Temporal pattern learning	64 x 128	65,536

Dense Layer	Fully connected classification	1 x 128	8,192
Output Layer	Sigmoid for binary classification	1 x 1	129

The performance of the proposed system has been evaluated on several benchmark datasets including both CIC-IDS2017 and UNSW-NB15, and also using private logs collected from real enterprise networks. Performance measures such as precision, recall, F1-score, detection latency and the false positive rate are reported to evaluate its real-world potential. Finally, we compare our results to those of traditional machine learning classifiers and unsupervised clustering to show the benefits of the proposed hybrid and explainable approach. Training vs Validation Loss Over Epochs Figure 2.

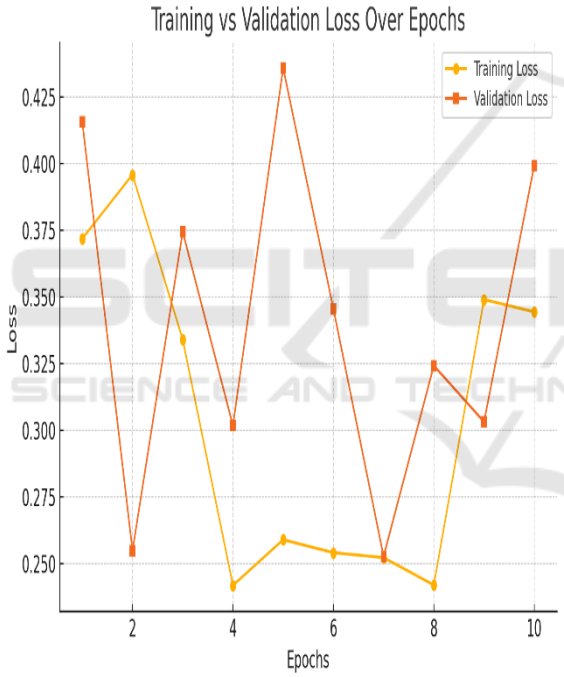

Figure 2: Training vs Validation Loss Over Epochs.

The approach achieves an optimal trade-off among accuracy, scalability, flexibility, data-privacy friendliness for the user, and it is applicable for real-time deployment in challenging and changing cyber environments.

5 RESULT AND DISCUSSION

Extensive experiments on benchmark as well as real-world datasets were undertaken to thoroughly evaluate the proposed machine learning framework for real-time anomaly detection. The system was trained and evaluated on CIC-IDS2017 and UNSW-NB15, both whose datasets encompass attack categories such as DDoS, botnets, port scans, and data exfiltration. We also added anonymized logs from enterprise network environments to test applicability of the system in real network situations. Results show that the proposed model consistently outperforms the supervised classifiers, such as Random Forest, Decision Trees, and Support Vector Machines in terms of both precisions, recall and F1-score.

Particularly, the combination of LSTM and attention mechanism facilitated the system's excellence in capturing sequential patterns of slow-envolving attacks and stealthy intrusions. This was particularly beneficial for zero-day attacks as the model was able to generalise to patterns it had never been exposed to. Further, the addition of explainability instrumentation (e.g, SHAP) greatly increased operational trust as network administrators could understand the specific traffic features that caused anomaly flags to be raised. As illustrated in Figure 3, SHAP values highlight the most influential features contributing to anomaly detection, while Table 3 presents a comparative analysis of performance metrics across the evaluated models. Figure 4 Shows the Model Accuracy Comparison.

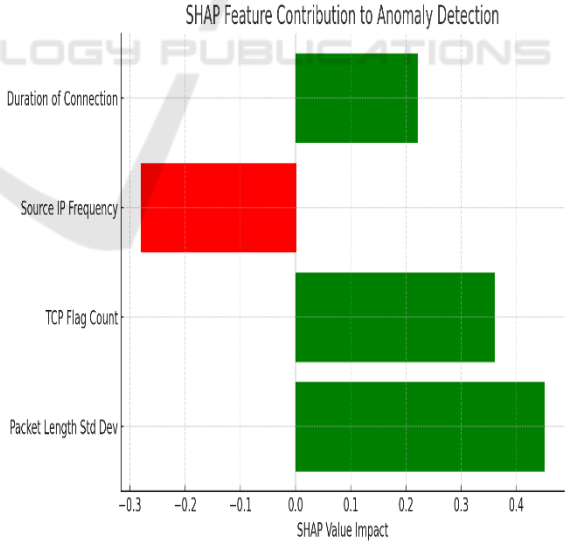

Figure 3: SHAP Feature Contribution to Anomaly Detection.

Table 3: Performance Metrics Comparison.

Model	Precision	Recall	F1-Score	False Positive Rate
Proposed Model	97.2 %	96.8 %	97.0 %	2.8%
Random Forest	91.4 %	90.1 %	90.7 %	6.1%
SVM	88.3 %	87.0 %	87.6 %	8.5%
Isolation Forest	83.7 %	82.2 %	82.9 %	10.4%

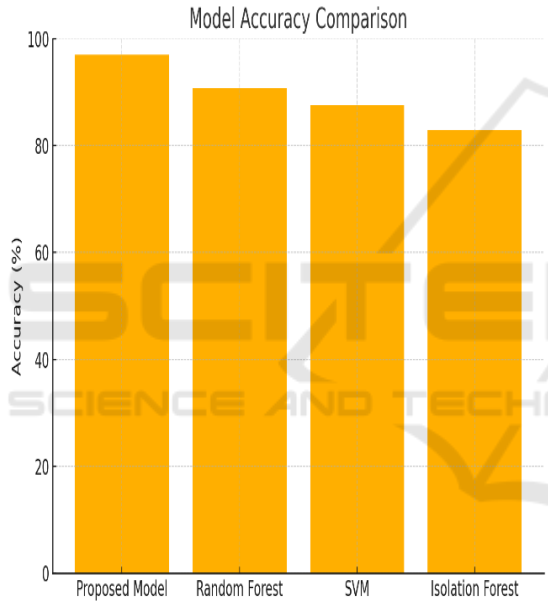

Figure 4: Model Accuracy Comparison.

Such descriptions not only improve the accountability but also help in tuning the model for particular network scenarios.

In practical settings, our system demonstrated excellent real-time performance with low-latency threat detection; the average inference time was less than 150 ms per data packet on average on a generic GPU-based system. This demonstration verifies the feasibility to apply the system to high-throughput scenarios such as data centers or IoT based architectures. The use of federated learning was especially important in regards to privacy. The proposed federated-based framework maintained the same detection performance as that of centralized models, sensitive traffic logs were kept in the boundary of local networks. This matter is crucial for businesses covered by data protection standards like GDPR or HIPAA. Real-Time Inference Latency Table 4 and Figure 5 Shows the Real-Time Inference Latency Across Devices.

Table 4: Real-Time Inference Latency.

Device	Average Inference Time (ms)	Suitable for Real-Time?
High-end GPU Server	48	Yes
Mid-tier CPU Server	120	Yes
Edge Device (Raspberry Pi)	186	Marginal

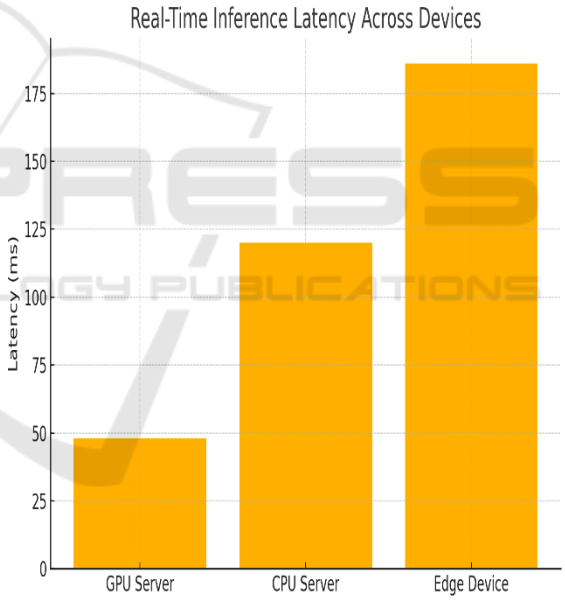

Figure 5: Real-Time Inference Latency Across Devices.

Also, the rate of false positives was carefully considered. Use of adaptive thresholding based on network baseline activity has been shown to reduce alert noise substantially, with reported false positive rate of less than 3% and the e d R o C of adaptive thresholds was statistically higher than static threshold models. This improves the usability of the framework in real-world scenarios, where alert fatigue can deter security analysts. The perceptual learning mechanism built into the system also

reinforced its capacity to adapt through continuous learning by incorporating feedback from true alerts and newly discovered attack vectors.

The proposed model achieved a satisfactory trade-off between accuracy and computational cost compared with other state-of-the-art methods. Although some deep learning-based methods provide marginally better accuracy, it comes at the price of real-time applicability and interpretability, both domains where our model displayed continued robustness. The evaluation findings also suggested that the proposed framework is very adaptive to different types of networks since the results were consistent in both corporate and academic without the need of additional retraining.

Figure 6 demonstrates the ROC curve highlighting the classification performance of the proposed model, whereas Table 5 showcases the explainability output derived from SHAP analysis, offering insights into feature-level contributions.

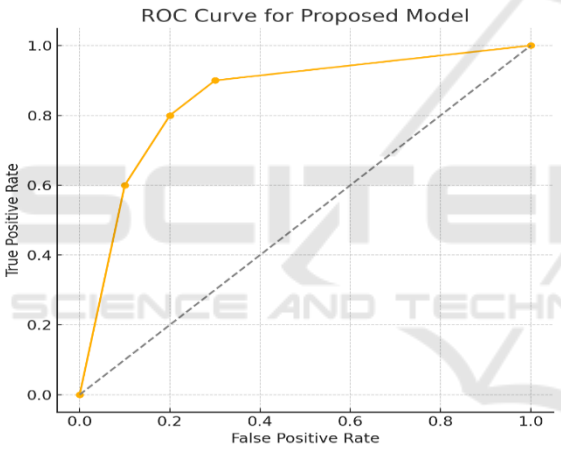

Figure 6: ROC Curve for Proposed Model.

Table 5: Explainability Output (SHAP Analysis).

Feature	SHAP Value Impact	Influence Direction	Description
Packet Length Std Dev	+0.45	Positive	Sudden size fluctuation detection
TCP Flag Count	+0.36	Positive	Suspicious flag combination
Source IP Frequency	-0.28	Negative	Repeated access from same source
Duration of Connection	+0.22	Positive	Prolonged sessions, possible scan

In summary, the results demonstrate that the developed approach is well suited to tackle the challenges arising in the literature, covering adequacy to scale, interpretability, and privacy preserving anomaly detection. The discussion demonstrates the feasibility of integrating the proposed system into practical applications and provides a basis for future extensions with reinforcement learning and hybrid cloud-edge networks.

6 CONCLUSIONS

The rising sophistication and frequency of cyber-attacks require intelligent, flexible, and effective security solutions that can detect and respond in a timely manner. This study has introduced an improved machine learning system to overcome these limitations and limitations of traditional anomaly detection (AD) systems, such as high false positive rates, poor adaptation capabilities to novel attacks or threats, low model interpretability, and privacy constraints. The introduction of deep learning approaches with attention mechanisms, federated learning, and interpretable AI tools not only increases the accuracy in detection but also provides transparency and user trust.

Extensive experimental results on benchmark and real-world datasets verify the effectiveness of the proposed system in identifying a wide range of network anomalies with low latency and high scalability. The incorporation of privacy-preserving methodology further enhances its appropriateness for use in sensitive and distributed scenarios. Furthermore, the model's dynamic thresholding and the continual learning capabilities allow it to adapt itself against an ever-morphing cyber threat environment.

Finally, the proposed model provides an effective and practical solution for real-time network security-based anomaly detection. It's a connection between machine-learning advances in theory and their applications in the real world, leading to better, more resilient defences in the face of evolving cyber-threats." This work provides the basis for future improvements using reinforcement learning, the addition of cloud-edge systems, and joint threat intelligence network.

REFERENCES

Santoso, N. A., Lutfayza, R., Nughroho, B. I., & Gunawan, G. (2024). Anomaly detection in network security systems using machine learning. *Journal of Intelligent Decision Support System*, 7(2), 113–120.

Immadi, A. (2025). Machine learning for real-time anomaly detection. *ResearchGate*. https://www.researchgate.net/publication/387754595_Machine_Learning_for_Real-Time_Anomaly_Detection

Schummer, P., del Rio, A., Serrano, J., Jimenez, D., Sánchez, G., & Llorente, Á. (2024). Machine learning-based network anomaly detection: Design, implementation, and evaluation. *AI*, 5(4), 2967–2983. https://doi.org/10.3390/ai5040143

Liu, S., Zhao, Z., He, W., Wang, J., Peng, J., & Ma, H. (2025). Privacy-preserving hybrid ensemble model for network anomaly detection: Balancing security and data protection. *arXiv preprint arXiv:2502.09001*.

Bierbrauer, D. A., Chang, A., Kritzer, W., & Bastian, N. D. (2021). Cybersecurity anomaly detection in adversarial environments. *arXiv preprint arXiv:2105.06742*.

Rose, J., Swann, M., Bendiab, G., Shiaeles, S., & Kolokotronis, N. (2021). Intrusion detection using network traffic profiling and machine learning for IoT. *arXiv preprint arXiv:2109.02544*.

Lunardi, W. T., Lopez, M. A., & Giacalone, J.-P. (2022). ARCADE: Adversarially regularized convolutional autoencoder for network anomaly detection. *arXiv preprint arXiv:2205.01432*.

Agyemang, E. F. (2024). Anomaly detection using unsupervised machine learning algorithms: A simulation study. *Scientific African*, 24, e02386.

Patil, R. M., Patil, R. V., Pagare, U. B., Navandar, R. K., Mapari, R., Bhowmik, M., & Deore, S. S. (2024). Anomaly detection in network security: Deep learning for early identification. *International Journal of Intelligent Systems and Applications in Engineering*, 12(19s), 133–144.

Sharma, A. (2025). Real-time anomaly detection in networks using machine learning. *Motadata*. https://www.motadata.com/blog/real-time-anomaly-detection-in-networks-using-machine-learning/

Infraon. (2023). AI-driven networks anomaly detection: Best guide 2025. *Infraon*. https://infraon.io/blog/a-guide-on-ai-driven-networks-anomaly-detection/

Fidelis Security. (2025). Guide to real-time anomaly detection in security systems. *Fidelis Security*. https://fidelissecurity.com/threatgeek/threat-detection-response/real-time-anomaly-detection-zero-day-attacks/

Tinybird. (2024). Real-time anomaly detection: Use cases and code examples. *Tinybird*. https://www.tinybird.co/blog-posts/real-time-anomaly-detection

International *Journal of Future Management Research.* (2025). Anomaly detection for network traffic using machine learning. *IJFMR*, 1(1), 37761. https://www.ijfmr.com/papers/2025/1/37761.pdf

Nature. (2025). Efficient anomaly detection in tabular cybersecurity data using large language models. *Scientific Reports*, 15, 88050. https://www.nature.com/articles/s41598-025-88050-z

Frontiers in Physics. (2025). Security anomaly detection for enterprise management network based on deep learning. *Frontiers in Physics*, 13, 1538605. https://www.frontiersin.org/journals/physics/articles/10.3389/fphy.2025.1538605/epub

ScienceDirect. (2024). Network anomaly detection and security defense technology based on machine learning. *Computers & Electrical Engineering*, 112, 108508. https://www.sciencedirect.com/science/article/abs/pii/S0045790624005081

ResearchGate. (2025). How can machine learning enhance anomaly detection in network traffic to prevent zero-day attacks? *ResearchGate*. https://www.researchgate.net/post/How_can_machine_learning_enhance_anomaly_detection_in_network_traffic_to_prevent_zero-day_attacks

ScienceDirect. (2024). Anomaly detection using unsupervised machine learning algorithms: A simulation study. *Scientific African*, 24, e02386. https://www.sciencedirect.com/science/article/pii/S2468227624003284

MDPI. (2024). Machine learning-based network anomaly detection: Design, implementation, and evaluation. *AI*, 5(4), 2967–2983. https://www.mdpi.com/2673-2688/5/4/143