Journal of Global Research in Electronics and Communication
Volume 2, No. 2, February 2026
Available Online at: www.jgrec.info
REVIEW PAPER

AI For Cybersecurity: Real-Time Anomaly Detection in Network Traffic Using AI

Suraj Panthi
Scholar
Department of Computer Science and Engineering
Sri Aurobindo Institute of Technology
Indore, India
surajpanthi02@gmail.com

***Abstract*—The large-scale, high-speed characteristics of network traffic in the modern digital world and the constantly changing threat environment requires real-time detection of anomalies in cybersecurity infrastructure. The paper is a synthesis and review of recent studies (2015-2024) at the crossroads of artificial intelligence (AI) and network traffic anomaly detection, with a specific focus on real-time or near real-time detection. The review features classical statistical techniques, ML-based techniques, DL, and hybrid/edge paradigm that allow rapid detection. Then identify key limitations in current frameworks (such as latency, false-alarm rates, model drift, adversarial robustness, and feature-engineering overhead) and propose a conceptual architecture that extends prior work by integrating lightweight unsupervised online learning, edge computing, and adversarial regularization for real-time responsiveness and scalability. The analysis wraps up with unresolved issues and research directions in the future of AI-based anomaly detection of network traffic.**

Keywords—anomaly detection, network traffic, real-time monitoring, machine learning, deep learning, edge computing, cybersecurity, artificial intelligence.

I. INTRODUCTION

In the modern globalized world, information and communications networks host large volumes of traffic and underpin essential infrastructures, which are prime targets in cyber threats [1][2]. Traditional signature-based intrusion detection systems (IDSs) find it difficult to remain ahead of zero-day attacks and polymorphic malware in addition to insider threats and exfiltration through normal-looking flows [3][4]. The use of AI [5], ML and DL algorithms has become a promising paradigm of anomaly detection in network traffic that can indicate undesirable or unpredicted behaviour [6][7][8].

The process of real-time (or near-real-time) anomaly detection is particularly tricky: it is necessary to process streaming traffic with a low latency, deal with changing network behaviors, high accuracy and low false positive rates, and the system must be scalable and adaptive. Since 2015 the progress in using AI in detecting anomalies in the network has been significant, but there are still many gaps.

The paper is addressed to academic researchers who are interested in AI in cybersecurity and network traffic analysis [9][10]. The survey key work and trends presented in the 2015-2024 period, summarizes the findings and suggests how a next generation framework can be enhanced in comparison with current systems. The rest of the paper is organized as follows: Section II evaluates relevant work. Section III describes approaches and common architectures. Section IV summarizes the outcomes and findings of the literature. Section V discusses limits, Section VI proposes further work, and Section VII concludes.

II. RELATED WORK

A. Traditional and Statistical Methods

Early work on network anomaly detection relied heavily on statistical modelling or signature-based heuristics. For example, incremental anomaly detection approaches surveyed by Bhuyan et al. (2012) highlighted the use of baseline traffic modelling and thresholding, though they emphasized issues of online-processing and scalability [11]. These techniques are fragile when network behaviors change and often have significant false-alarm rates.

B. Machine-Learning Approaches

In the past decade, supervised and unsupervised ML techniques began to dominate the domain. Schummer et al. (2024) developed a ML-based system for network anomaly detection combining unsupervised and supervised methods (e.g., clustering, classification) along with SHAP values for interpretability [12][13][14]. Their findings showed Random Forest achieved ≈94.3 % accuracy in point- anomaly detection tasks on network traffic data.

Similarly, D. Ramotsoela et al. (2018) proposed a CNN-based online anomaly-detection system tied to software-defined networks (SDN) for real-time monitoring in edge-clustered networks. Their system exhibited improved accuracy and mitigation speed when compared to shallow classification models [15].

C. Deep Learning and Hybrid Models

The arrival of deep learning enabled richer representations of network traffic flows and temporal dependencies. Singh & Jang-Jaccard (2022) proposed MSCNN-LSTM-AE, a multi-scale convolutional- recurrent autoencoder for unsupervised intrusion detection on NSL-KDD, UNSW-NB15, and CICDDoS2019 datasets, showing superior performance to prior unsupervised methods [16]. Lunardi et al. (2022) introduced ARCADE: an adversarially regularized convolutional autoencoder for unsupervised network anomaly detection, training exclusively on normal traffic and therefore enabling detection of unknown attacks; they achieved faster detection with fewer parameters than baselines [17][18].

D. Surveys and Real-Time Considerations

Recent survey articles underscore the shift toward real-time and streaming settings. M. Kohli and I. Chhabra (2025) provide an overview of anomaly detection in cyber-physical systems (CPS), with a focus on edge computing, adversarial machine learning, real-time detection, and the need of human-in-loop systems [19]. A. D'Alconzo et al. (2019) deliver a comprehensive survey on network-packet anomaly detection techniques, demographics, and performance evolution—highlighting the move from rule-based methods to DL paradigms [20].

E. Key Takeaways

From these works extract several trends: (1) unsupervised / semi-supervised learning is increasingly used to detect unknown anomalies; (2) feature engineering is being replaced or supplemented by automatic feature extraction (CNN, LSTM, graph-networks); (3) edge computing and SDN frameworks enable lower latency and distributed detection; (4) adversarial training and explainability (XAI) are emerging to strengthen model robustness and transparency [21]. Nevertheless, latency, real-time streaming, model drift, life-cycle administration and adversarial evasion are still unresolved problems.

III. Methodology (Typical AI + Network-Traffic Anomaly-Detection Framework)

A. Data Sources and Pre-processing

A network traffic data consists of packet-level captures (PCAPs) and flow records (NetFlow/IPFIX), logs, and metadata. Some of the most common public datasets in research are NSL-KDD, UNSW-NB15, CICDDoS2019, and others [22][23]. The process of pre-processing usually includes: feature extraction (packet counts, bytes, flow durations, protocols), transformations (normalization, one-hot encoding) and streaming detection by windowing/time-series fragmentation.

B. Feature Engineering vs Automatic Feature Learning

Conventional ML is based on engineered features (e.g., destination/source ports, size and time of packets), and the DL methods do not require much manual feature engineering. For instance, Liu et al. (2023) used CNNs directly on raw flow features in an SDN-based real-time environment. Hybrid methods may combine both.

C. Model Architectures for Real-Time Detection

- **Supervised classifiers** (e.g., SVM, RF) trained on labelled normal/anomalous data [24].
- **Unsupervised models** (e.g., Isolation Forest, LOF, One-Class SVM) for anomaly detection without labelled attacks.
- **Deep models:** Autoencoders, CNN-LSTM combinations, graph neural networks for temporal/spatial modelling [25].
- **Adversarial regularization:** ARCADE uses an adversarial method to regularize a convolutional autoencoder and improve detection of unseen anomalies.

Online/streaming & edge deployment: Real-time detection requires models that update or adapt online, often deployed at network edge/SDN switches for low latency [26].

D. Performance Metrics and Real-Time Constraints

The most important evaluation measures are accuracy, recall, precision, F1-score, false-alarm rate, processing latency (milliseconds scale) and throughput (flows/s) [27]. Streaming flows need to be processed by real-time systems in a minimal time; Lunardi et al. measured processing time per flow less than 0.033 ms in one instance.

E. Conceptual Proposed Extension

Based on the gaps identified, propose a conceptual architecture:

- Deploy lightweight unsupervised online-learning model (e.g., One-Class SVM or isolation-forest variant) at edge nodes;
- Complement with an adversarial-regularized autoencoder for analyzing deeper temporal/spatial correlations centrally;
- Leverage SDN-based flow-monitoring for dynamic feature capture;
- Incorporate concept drift adaptation and model-update pipeline;
- Integrate explainable AI (XAI) for transparency and operator trust;
- Seamlessly escalate suspected anomaly flows to central system for deeper analysis and signature extraction.

IV. Results and Discussion

A. Comparative Review of Approaches

ML techniques that are supervised (e.g., Random Forest) tend to report very high classification (when in controlled settings): which reported a reported accuracy of around 94 percent in detection of point-anomalies. Nonetheless, these models are based on labeled attack information, and have difficulty in unknown threats and streaming contexts [28].

Anomaly detection of unsupervised ML (One-Class SVM, Isolation Forest) is not labeled, although it tends to have a higher false-positive error. As an example, real-time network anomaly detection with Isolation Forest and SHAP-based explainability were demonstrated to be feasible but had computational and scalability limitations.

Deep-learning techniques are promising in the ability to model temporal and spatial dependencies. Singh & Jang-Jaccard's MSCNN-LSTM-AE achieved superior performance across multiple datasets [29]. The ARCADE model achieved faster detection and fewer parameters than prior work—thus improving responsiveness.

Edge/SDN deployment delivered real-time packet/extraction and detection, highlighting the value of co-design of network infrastructure and anomaly detection model [30].

B. Real-Time Considerations

Real-time anomaly detection demands sub-second (or sub-millisecond) processing, high flow- throughput support, and adaptation to traffic drift [31]. Lunardi et al. reported per-flow processing time < 0.033 ms. Liu et al. used SDN and CNN for online packet extraction and detection. These show that real-time operation is feasible—but often at cost of dataset realism, limited attack types, or offline training.

C. *Identified Gaps and Improvement Opportunities*

- **Model drift and adaptivity:** Many models assume fixed distributions; few handle network behaviour change over time.
- **Edge deployment and resource constraints:** Lightweight models are needed for deployment at switches or IoT/edge devices; most research still uses server-class hardware.
- **Adversarial robustness:** Attackers increasingly target AI systems (adversarial examples, evasion). Few anomaly detection works address such threats explicitly (except ARCADE).
- **Explainability and trust:** Operators require transparent decision-making (e.g., via SHAP).
- **Labelled data scarcity and novel anomaly detection:** Supervised models falter on unknown attack types. Unsupervised/one-class methods are promising but less mature.
- **Scalability and streaming throughput:** Techniques must scale to millions of flows/second and maintain low latency.
- **Integration with network infrastructure:** SDN, flow-monitoring, edge computing and AI must be co-designed for maximum effectiveness.

The proposed architecture (Section III-E) addresses several of these gaps by combining online unsupervised learning at the edge, adversarial regularization centrally, adaptive model updates, and deployment in SDN/edge environments.

V. Limitations

This survey has several limitations:

- **Scope restriction:** The limitations of the review to literature published between 2015 and 2024 and focused on AI-based network traffic anomaly detection; broadband descriptive coverage of signature-based IDS or non-AI methods is omitted [32].
- **Data source limitations:** While referencing publicly available literature, access to full dataset details and implementation specifics was limited in some cases.
- **Lack of empirical replication:** The proposed architecture is conceptual do not provide experimental results or real-world deployment validation.
- **Rapidly evolving field:** The field of AI-driven cybersecurity evolves rapidly; new works beyond 2024 may mitigate some identified gaps [33][34].

VI. Future Work

Future research directions include:

- **Online, incremental, drift-aware learning:** Develop methods that adapt continuously to network behaviour changes and concept drift without full retraining.
- **Resource-aware edge deployment:** Create ultra-lightweight models (e.g., compressed autoencoders, quantized models) for deployment on edge/IoT devices and within SDN switches.
- **Adversarial & robust models:** Integrate adversarial learning, detection of evasion attacks, and resilience to poisoning or mimicry attacks.
- **Explainable and operationally usable systems:** Incorporate XAI frameworks to deliver actionable insights to SOC analysts, reducing alert fatigue and building operator trust.
- **Streaming anomaly detection at scale:** Investigate architectures capable of sustaining millions of flows per second with sub-millisecond latency and low false-positive rates.
- **Benchmarking and real-world datasets:** Open, realistic streaming network traffic datasets with labelled anomalies (and drift) would support realistic evaluation and deployment readiness.
- **Co-design with network infrastructure:** Work with SDN, network telemetry, and programmable data planes to embed anomaly detection directly in network fabrics.

VII. Conclusion

The current paper examines the current state of the art in AI-driven anomaly detection for network traffic in real-time or near-real-time contexts, with a particular emphasis on the years 2015–2024. They observed the evolution from statistical and rule-based methods towards ML, DL, and hybrid edge/streaming systems. While significant progress has been made—especially in unsupervised learning, edge-based deployment, and adversarially regularized models—several important challenges remain, including model adaptivity, scalability, adversarial robustness, explainability, and deployment readiness. They proposed a conceptual architecture to advance the field and provided directions for future research. With the complexity of the networks expanding and the threat actors becoming more advanced, the implementation of AI into real-time anomaly detection will play a significant role in building resilient cybersecurity.

References

[1] S. Singamsetty, "CyNet: Amalgam Deep Learning Model for Multi-Vector Cyber Intrusion Detection System (IDS)," in *2025 3rd International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI)*, IEEE, Sep. 2025, pp. 914–918. doi: 10.1109/ICoICI65217.2025.11253990.

[2] G. Modalavalasa, "Strengthening Threat Detection and Mitigation Strategies in Cybersecurity with Artificial Intelligence," in *2025 5th International Conference on Intelligent Technologies (CONIT)*, IEEE, Jun. 2025, pp. 1–6. doi: 10.1109/CONIT65521.2025.11166691.

[3] S. Kumara, "AI-Driven Threat Identification and Response: Implications for Secure and Scalable Telecom Infrastructure," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 4, p. 559, Dec. 2025, doi: 10.48175/IJARSCT-30567.

[4] S. Narang and A. Gogineni, "Zero-Trust Security in Intrusion Detection Networks: An AI-Powered Threat Detection in Cloud Environment," *Int. J. Sci. Res. Mod. Technol.*, vol. 4, no. 5, pp. 60–70, Jun. 2025, doi: 10.38124/ijsrmt.v4i5.542.

[5] S. P. Kalava, "Building Trust in AI: Ethical Principles for Transparent Autonomous Systems," *J. Artif. Intell. Mach. Learn. Sata Sci.*, vol. 2, no. 2, 2024.

[6] Y. Mehmet and L. Charlotte, "AI Driven Anomaly Detection for Real Time Network Traffic Monitoring," 2025.

[7] A. Katangoori, "The Role of Big Data in Advancing Artificial Intelligence: Methods and Case Studies," *Int. J. Artif. Intell. Mach. Learn.*, vol. 6, no. 1, pp. 37–54, 2026, doi: 10.51483/IJAIML.6.1.2026.37-54.

[8] P. Chandrashekar and M. Kari, "Design Machine Learning-Based Zero-Trust Intrusion Identification Models for Securing Cloud Computing System," *Int. J. Res. Anal. Rev.*, vol. 11, no. 4, pp. 901–907, 2024.

[9] S. Singamsetty, "Data Engineering for Dynamic and Secure Blockchain Networks in AI Applications," *Int. J. Inf. Electron. Eng.*, vol. 13, no. 4, pp. 52–61, 2023, doi: 10.48047/ijiee.2025.13.4.7.

[10] R. V. S. S. B. R, Y. M. M. John, M. B. B. G, B. Karim, and G. Saritha,

"Multi-Domain Cyber Threat Classification Using Enhanced Genetic Algorithm and Deep Neural Networks," in *2025 Third International Conference on Networks, Multimedia and Information Technology (NMITCON)*, IEEE, Aug. 2025, pp. 1–6. doi: 10.1109/NMITCON65824.2025.11187556.

[11] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Survey on Incremental Approaches for Network Anomaly Detection," *Int. J. Commun. Networks Inf. Secur.*, vol. 3, no. 3, 2012.

[12] H. Liu and H. Wang, "Real-Time Anomaly Detection of Network Traffic Based on CNN," *Symmetry (Basel).*, vol. 15, no. 6, p. 1205, Jun. 2023, doi: 10.3390/sym15061205.

[13] T. A. Khan *et al.*, "Multi-Source Cyber Intrusion Detection Using Ensemble Machine Learning," *J. Comput. Sci.*, vol. 21, no. 1, pp. 111–123, Jan. 2025, doi: 10.3844/jcssp.2025.111.123.

[14] D. Bhattacharjee, "Design and Evaluation of Deep Generative AI Model for Intrusion Detection in Cyber Threat Monitoring," in *2025 7th International Symposium on Advanced Electrical and Communication Technologies (ISAECT)*, 2025, pp. 1–6. doi: 10.1109/ISAECT68904.2025.11318752.

[15] D. Ramotsoela, A. Abu-Mahfouz, and G. Hancke, "A Survey of Anomaly Detection in Industrial Wireless Sensor Networks with Critical Water System Infrastructure as a Case Study," *Sensors*, vol. 18, no. 8, 2018, doi: 10.3390/s18082491.

[16] A. Singh and J. Jang-Jaccard, "Autoencoder-based Unsupervised Intrusion Detection using Multi-Scale Convolutional Recurrent Networks." 2022.

[17] W. T. Lunardi, M. Andreoni, and J.-P. Giacalone, "ARCADE: Adversarially Regularized Convolutional Autoencoder for Network Anomaly Detection." 2022. doi: 10.48550/arXiv.2205.01432.

[18] A. Nerella, N. Kolli, and J. W. Sajja, "Building Secure AI Agents for Autonomous Data Access in Compliance/Regulatory-Critical Environments," *SSRN Electron. J.*, p. 11, 2025, doi: 10.2139/ssrn.5528763.

[19] M. Kohli and I. Chhabra, "A comprehensive survey on techniques, challenges, evaluation metrics and applications of deep learning models for anomaly detection," *Discov. Appl. Sci.*, vol. 7, no. 7, p. 784, Jul. 2025, doi: 10.1007/s42452-025-07312-7.

[20] A. D'Alconzo, I. Drago, A. Morichetta, M. Mellia, and P. Casas, "A Survey on Big Data for Network Traffic Monitoring and Analysis," *IEEE Trans. Netw. Serv. Manag.*, vol. 16, no. 3, pp. 800–813, 2019, doi: 10.1109/TNSM.2019.2933358.

[21] A. Alabdulatif, "A Novel Ensemble of Deep Learning Approach for Cybersecurity Intrusion Detection with Explainable Artificial Intelligence," *Appl. Sci.*, vol. 15, no. 14, p. 7984, Jul. 2025, doi: 10.3390/app15147984.

[22] P. Nutalapati, J. R. Vummadi, S. Dodda, and N. Kamuni, "Advancing Network Intrusion Detection: A Comparative Study of Clustering and Classification on NSL-KDD Data," in *2025 International Conference on Data Science and Its Applications (ICoDSA)*, IEEE, Jul. 2025, pp. 880–885. doi: 10.1109/ICoDSA67155.2025.11157595.

[23] N. K. Prajapati, "Federated Learning for Privacy-Preserving Cybersecurity: A Review on Secure Threat Detection," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 4, pp. 520–528, Apr. 2025, doi: 10.48175/IJARSCT-25168.

[24] A. Syed, *AI-Powered Threat Detection and Mitigation*. 2024.

[25] G. Sarraf and V. Pal, "Adaptive Deep Learning for Identification of Real-Time Anomaly in Zero-Trust Cloud Networks," *ESP J. Eng. Technol. Adv.*, vol. 4, no. 3, 2024, doi: 10.56472/25832646/JETA-V4I3P122.

[26] D. Patel, "Leveraging Blockchain and AI Framework for Enhancing Intrusion Prevention and Detection in Cybersecurity," *Tech. Int. J. Eng. Res.*, vol. 10, no. 6, 2023, doi: 10.56975/tijer.v10i6.158517.

[27] K. M. R. Seetharaman and P. Yadav, "A Machine Learning Framework for Detecting and Mitigation of Cyber Threats in IoT Environments," in *2025 3rd International Conference on Inventive Computing and Informatics (ICICI)*, IEEE, Jun. 2025, pp. 1112–1119. doi: 10.1109/ICICI65870.2025.11069697.

[28] S. K. Chintagunta, "Enhancing Cloud Database Security Through Intelligent Threat Detection and Risk Mitigation," *TIJER – Int. Res. J.*, vol. 9, no. 10, pp. 49–55, 2022.

[29] S. Amrale, "Anomaly Identification in Real-Time for Predictive Analytics in IoT Sensor Networks using Deep," *Int. J. Curr. Eng. Technol.*, vol. 14, no. 6, pp. 526–532, 2024.

[30] S. Thangavel, "AI Enhanced Image Processing System For Cyber Security Threat Analysis," 202411074557, 2024

[31] V. Shah, "Traffic Intelligence in IoT and Cloud Networks: Tools for Monitoring, Security, and Optimization," *Int. J. Recent Technol. Sci. Manag.*, vol. 9, no. 5, 2024, doi: 10.10206/IJRTSM.2025894735.

[32] A. R. Bilipelli, "AI-Driven Intrusion Detection Systems for Large-Scale Cybersecurity Networks Data Analysis : A Comparative Study," *TIJER – Int. Res. J.*, vol. 11, no. 12, pp. 922–928, 2024.

[33] A. Gupta, "A Strategic approach - Enterprise-Wide Cyber Security Quantification via Standardized Questionnaires and Risk Modeling impacting financial sectors globally," *Int. J. AI, BigData, Comput. Manag. Stud.*, vol. 3, no. 1, pp. 89–98, 2022, doi: 10.63282/3050-9416.IJAIBDCMS-V3I1P110.

[34] H. Cyril and S. Kumara, "Cybersecurity Architecture For Autonomous Telecommunication Networks," *Int. J. Adv. SIGNAL IMAGE Sci.*, vol. 1, no. 1, pp. 618–639, 2026, doi: 10.29284/9admy374.

