Proceedings of the 7th International Conference on Innovative Data Communication Technologies and Application (ICIDCA-2025)
IEEE Xplore Part Number: CFP25CR5-ART; ISBN: 979-8-3315-1414-3

# Advancing Network Security with Artificial Intelligence: A Study on Anomaly Detection in Traffic Data

Anjitha K
Research Scholar
*Department of Computer Science And Engineering*
Vels Institute of Science, Technology And Advanced Studies
Chennai, India
Anjithakmcchet@gmail.com

Dr. A.Saritha
Associate Professor
*Department of Computer Science And Engineering*
Vels Institute of Science, Technology And Advanced Studies
Chennai, India
saritha.se@vistas.ac.in

***Abstract*—Anomaly detection in network traffic data plays a critical role in advancing modern digital networks from more sophisticated and subtle cyber assaults. As network environments continue to expand and increase in complexity, detecting deviations from normal traffic behaviors has become essential for maintaining security, reliability, and operational continuity. Conventional approaches such as rule-based systems, statistical models, and threshold analysis struggle with adaptability, accuracy, and real-time application, particularly in dynamic network environments. The study explores the significance of anomaly detection in network security, highlighting its necessity in detecting evolving attack patterns. This study provides a comprehensive review of recent research on the artificial intelligence (AI) techniques in network traffic anomaly detection. This approach evaluates the effectiveness of AI-based methods in addressing challenges of traditional techniques, including sensitivity to high-dimensional data, reliance on manual feature selection, and limited detection capabilities in real-time scenarios. The study analyses various AI techniques, highlighting key performance outcomes and challenges identified in prior studies. The study identifies the common research challenges, such as dataset limitations, high computational costs, and insufficient scalability. By analyzing recent trends and research gaps in existing literature, this study advances the research fields of AI-driven anomaly detection and supports the development of more robust, scalable, and intelligent systems for enhancing network security.**

***Keywords*—Anomaly Detection, Network Traffic Data, Network Security, Artificial Intelligence, Network Monitoring, Automated Intrusion Detection***

## I. INTRODUCTION

In today's interconnected digital environments, networks serve as the backbone of communication, business, governance, and everyday life. With the increasing reliance on internet-based services and the rapid expansion of connected devices, the intensity of network traffic data has increased significantly [1]. Along with this expansion, the complexity and frequency of cyber-attacks have increased, rendering network security a top priority across industries. Anomaly detection in network traffic data has emerged as a significant resource for detecting potential threats and vulnerabilities. Anomaly detection systems identify unusual activities that indicate cyber-attacks, intrusions, or network failure by analyzing deviations from normal traffic patterns [2].

Anomaly detection has become much more important because data is now flowing through modern networks more often and at a faster pace; its role in analyzing network traffic. The overall process of anomaly detection in network traffic data is illustrated in Fig. 1, which highlights the deviations between normal and abnormal traffic flow Traditional defense mechanisms, which rely on recognizing threats, are often unable to identify new or subtle attacks. This provides a valuable tool for early warning and prevention of harmful incidents. As organizations confront increasing demands to protect sensitive information and maintain uninterrupted digital services, the ability to detect anomalies in real-time has become an essential element of network security.


Fig. 1. Significance of network traffic analysis

Traditional approaches for anomaly detection in network traffic data employ rule-based systems, threshold monitoring, and statistical techniques. These approaches often involve manual configurations and rely on predefined concepts of normal behavior. While effective in some cases, they tend to lack the adaptability required in complex and continuously changing network environments. These methods are also prone to high false positive rates and fail to detect sophisticated attacks that do not follow predicted patterns [3]. As network data becomes more complex and diverse, traditional approaches struggle to maintain accuracy and relevance.

In response to the challenges in traditional approaches, AI techniques have emerged as a promising solution for enhancing anomaly detection in network traffic data. AI-based approaches are capable of learning from diverse historical data and identifying subtle or hidden patterns without relying on

predefined rules. These systems are intended to adapt to changing conditions and to provide more accurate and context-aware detection. By reducing the reliance on static setups and enabling automated analysis, AI techniques highlight the potential for more responsive and intelligent anomaly detection. Unlike prior surveys that focus exclusively on either ML, DL, or hybrid methods, this work provides an integrated comparative study across all three categories. The unique contribution of this study lies in synthesizing existing limitations into a well-defined research gap and outlining the essential requirements for next-generation AI-driven anomaly detection frameworks. The application of AI in this field also promotes enhanced scalability and faster detection, which are essential in modern high-speed network scenarios. The main contribution of the study is given below:

- To explore the advancements of AI contributions in detecting anomalies within network traffic data.
- To evaluate the effectiveness of AI-based methods in identifying unusual network behaviour and enhancing detection accuracy.
- To highlight the current emerging trends in AI-based anomaly detection in network traffic and identify existing challenges in the field.

## II. LITERATURE REVIEW

### *A. Anomaly Detection in Network Traffic Data Using Machine Learning Techniques*

Machine Learning (ML) techniques play a significant role in detecting anomalies in network traffic data by learning from patterns and distinguishing irregular behaviours. These approaches enhance automated detection of suspicious activities without relying solely on predefined rules. It provides better accuracy, adaptability, and scalability in processing huge quantities of data, rendering them useful for enhancing network security and detecting potential threats in real-time.

Ness et al. (2025) [4] investigated the ML models for network anomaly detection in network traffic data. The study employed Isolation Forest, Naïve Bayes (NB), XGBoost, LightGBM, Support Vector Machine (SVM), Random Forest (RF), and Logistic Regression (LR) and evaluated their performance using the NSL-KDD dataset. Recursive Feature Elimination (RFE) was applied for feature selection. LightGBM achieved the highest training accuracy and a test accuracy of 0.85, while XGBoost attained 0.83. NB indicated a test accuracy of 0.81, whereas Isolation Forest demonstrated poor generalization with a test accuracy of 0.4. The results highlighted the significance of model selection in optimizing detection performance and minimizing false positives in network security applications. However, the study faced several limitations, as XGBoost and LightGBM required substantial computational resources, rendering them ineffective in resource-constrained environments. Naïve Bayes relied on an unrealistic assumption of feature independence, reducing its reliability on complex datasets. Isolation Forest showed weak performance on high-dimensional data. Scalability and latency challenges further hindered the practical use of these models in real-world settings.

Fosic et al. (2023) [5] investigated anomaly detection in network traffic using ML classifiers. The study employed Stochastic Gradient Descent (SGD), SVM, K-Nearest Neighbor (K-NN), Gaussian Naive Bayes (GNB), DT, RF, and AdaBoost on the UNSW-NB15 dataset. Different encoding methods and data split ratios were tested to optimize the classifier's performance. The RF classifier achieved the highest performance with an F2 score of 97.68% and an area under curve (AUC) score of 98.47%. Feature reduction improved computational efficiency by eliminating non-essential attributes. Label encoding outperformed one-hot encoding in terms of execution time without compromising accuracy. The study demonstrated that optimizing feature encoding, data split ratios, and classifier selection improved anomaly detection accuracy in network traffic analysis. The study had limitations, including the lack of full optimization of the RF classifier, which resulted in undetected anomalies. Additionally, the model was not tested in a real-network environment, rendering its real-time effectiveness uncertain.

Sakhnevych et al. (2023) [6] suggested anomaly detection in tyre–road interaction using ML techniques. The study addressed the challenges of tyre data variability influenced by vertical force, wear, and road roughness. After preprocessing to remove duplicates and ensure temporal continuity, the authors applied clustering methods (K-Means, K-Medoids, Gaussian Mixture, and Hierarchical) to group tyre conditions, followed by four anomaly detection algorithms: One-Class SVM, Isolation Forest, Local Outlier Factor, and Elliptic Envelope. Experimental datasets were used for tyre model calibration. Results showed that K-Means clustering efficiently differentiated operating conditions, while the Elliptic Envelope minimized deviations in grip coefficient. For stiffness evaluation, One-Class SVM attained the lowest deviations, achieving 0.01% (lateral) and 1.09% (longitudinal) compared to the target values. The analysis was limited by the difficulty of defining normal behavior, the need for large datasets to set thresholds, and the impact of sensor measurement uncertainty on effectiveness.

Mohammed et al. (2025) [7] implemented anomaly detection of Distributed Denial of Service (DDoS) attacks in IoT networks using machine learning. The study utilized a publicly available IoT DDoS dataset (Lange & Kettani, 2019), which was preprocessed by removing null values, balancing, and scaling the data. Relevant features were extracted, and the dataset was split into 70% training and 30% testing subsets. Multiple machine learning models were evaluated, and the K-Nearest Neighbors (KNN) algorithm achieved the best performance. Device metadata, sensor data, and server logs were analyzed to detect abnormal patterns, and the approach was shown to outperform existing methods in detecting DDoS attacks in IoT networks. Apart from dataset constraints, the study faced limitations in computational efficiency and scalability in large IoT networks. It also focused only on DDoS attacks, potentially overlooking other cyber threats, and variations in device behavior could lead to false positives or negatives.

Baldoni and Battisti (2024) [8] implemented a network traffic representation method combined with a Principal Component Analysis (PCA)-based anomaly detection approach. The study analyzed multiple datasets, including UNSW-NB15, UGR'16, CCDIS17, SWAT, and IOTD2020, which contained both normal and attack traffic. Network traffic was summarized into compact vectors using one-second time windows to enable prompt anomaly detection. The PCA-based detector operated in an unsupervised manner,

requiring no prior knowledge of attack features, and reduced computational complexity compared to DL methods. Experimental results demonstrated that the approach effectively highlighted attack presence and achieved comparable performance to state-of-the-art methods while being faster and less complex. The method handled DoS attacks well, though detection of scan attacks was less effective due to shorter observation windows. The study was limited in detecting scan attacks due to short time windows and relied on traffic volume features, which may not capture subtle or complex anomalies. The summary of the recent works on anomaly detection in network traffic data using ML is given in Table I.

TABLE I. SUMMARY OF RECENT WORKS ON ANOMALY DETECTION IN NETWORK TRAFFIC DATA USING ML

| Author [Ref] | Methodology | Advantages | Disadvantages / Limitations |
|---|---|---|---|
| Ness et al. (2025) [4] | ML classifiers: Isolation Forest, Naïve Bayes, XGBoost, LightGBM, SVM, Random Forest, Logistic Regression | ▪ Explored multiple ML models for comparison.<br>▪ Highlighted importance of model selection for detection performance. | ▪ XGBoost and LightGBM required high computational resources.<br>▪ Naïve Bayes relied on feature independence.<br>▪ Isolation Forest performed poorly on high-dimensional data.<br>▪ Scalability and latency issues. |
| Fosic et al. (2023) [5] | ML classifiers: SGD, SVM, K-NN, GNB, Decision Tree, RF, AdaBoost; Feature encoding optimization; Data split ratio optimization | ▪ RF achieved high F2 score and AUC.<br>▪ Feature reduction improved efficiency.<br>▪ Label encoding reduced execution time. | ▪ RF not fully optimized, some anomalies undetected.<br>▪ Model not tested in real-network environment. |
| Sakhnevych et al. (2023) [6] | ML clustering (K-Means, K-Medoids, Gaussian Mixture, Hierarchical) + anomaly detection (One-Class SVM, Isolation Forest, LOF, Elliptic Envelope) | ▪ K-Means efficiently differentiated tyre conditions.<br>▪ One-Class SVM minimized deviations. | ▪ Defining normal behavior was difficult.<br>▪ Large datasets required for thresholds.<br>▪ Sensor measurement uncertainty affected effectiveness. |
| Mohammed et al. (2025) [7] | ML models for IoT DDoS detection; KNN performed best; Dataset preprocessing and feature extraction | ▪ KNN outperformed existing methods.<br>▪ Effective detection of DDoS attacks. | ▪ Limited computational efficiency and scalability.<br>▪ Focused only on DDoS attacks.<br>▪ Variations in device behavior could cause false positives/negatives. |
| Baldoni & Battisti (2024) [8] | PCA-based anomaly detection; Unsupervised; Network traffic summarized in one-second time windows | ▪ Reduced computational complexity.<br>▪ Prompt anomaly detection.<br>▪ Comparable performance to state-of-the-art methods. | ▪ Less effective in detecting scan attacks due to short time windows.<br>▪ Relied on traffic volume, missing subtle anomalies. |

### *B. Anomaly Detection in Network Traffic Data Using Deep Learning Techniques*

Deep learning (DL) techniques enable advanced anomaly detection in network traffic data by automatically developing hierarchical representations from raw inputs. These techniques capture complex and non-linear patterns, rendering them effective in detecting subtle and diverse anomalies. The DL models analyse high-dimensional data and adapt to dynamic environments, allowing for considerable enhancements to the accuracy and reliability of network anomaly detection systems.

Altaf et al. (2024) [9] designed a sequential gated graph convolutional neural network (GGCN) for anomaly detection in Internet of Things (IoT) networks. By modelling network traffic as time-stamped multi-edge graphs, the system captured temporal patterns critical to recognizing botnet anomalies. The GGCN framework, enhanced with gated message-passing and aggregation functions, effectively managed time-series traffic complexities. Using the Botnet of Things-Internet of Things (BoT-IoT) and Mirai datasets, the model achieved significant performance gains, improving detection accuracy by 0.01% on BoT-IoT and up to 25% on Mirai. The results demonstrated better anomaly detection capabilities, particularly in binary classification scenarios with imbalanced data, outperforming graph neural network (GNN) models across various evaluation metrics. The study was limited by its focus on binary classification tasks, which constrained its performance in handling multiclass scenarios. Additionally, the model's adaptability to varying network complexities and evolving IoT security threats was not fully addressed.

Sattar et al. (2025) [10] introduced ET SSL, a self-supervised contrastive learning framework for anomaly detection in encrypted network traffic. The model extracted flow level statistical features such as packet length, inter arrival time, flow duration, and protocol metadata without payload inspection. Three publicly available datasets, CIC Darknet2020, ISCX VPN nonVPN, and UNSW NB15, were used after preprocessing through feature scaling and removal of corrupted records. ET SSL achieved 96.8%accuracy, 92.7% true positive rate, 1.2 percent false positive rate, and a 94.9% F1 score, surpassing supervised random forest which achieved 88.3% accuracy and unsupervised K Means. It also demonstrated real time detection with 15 to 25 milliseconds latency and 10 Gbps throughput, while ensuring full privacy preservation. The system detected 120 anomalies during live traffic tests and consumed only 0.5 Joules per detection. The study was limited by simulated traffic, reliance on adaptive retraining, and high computational complexity.

Wang and Song (2024) [11] investigated network traffic classification and anomaly detection using DL. The study collected large-scale network traffic data from the CIC-IDS2017 and ISCX VPN NOVPN datasets, which included normal and abnormal traffic patterns. A convolutional neural

network (CNN) model was constructed to classify and identify network traffic effectively. The model was trained and tested on these datasets, and its performance was evaluated in terms of recall, F1 score, and error rate. The experimental results demonstrated significant improvements over traditional methods, effectively reducing error rates and false alarms. Further optimization of the network structures and parameters enhanced the model's robustness and adaptability, showing strong performance across multiple real network environments. The study faced limitations due to high data and computational requirements, which constrained its use in resource-limited scenarios. The models also lacked interpretability, and their effectiveness decreased when data was insufficient or unrepresentative.

Morshedi and Matinkhah (2025) [12] developed anomaly detection in IoT traffic using DL under the presence of Gaussian noise. The study utilized the CIC-IDS2017 dataset, which included diverse IoT traffic patterns and attack types such as DoS, DDoS, and advanced threats. A simple and optimized Long Short-Term Memory (LSTM) model with 128 memory units was trained on the dataset and deployed on edge servers for evaluation. The research also examined the integration of the Hurst parameter with the LSTM model to enhance noise resilience. The findings demonstrated that the proposed approach effectively detected anomalies and improved robustness against Gaussian noise, emphasizing the importance of advanced statistical features and noise-resistant models in IoT network security.

Zhang et al. (2025) [13] investigated real-time data quality assessment and anomaly detection in large-scale distributed data streams using a deep neural network (DNN) with adaptive online learning. The study collected three large-scale datasets, including industrial IoT sensors (2.5TB), network traffic (1.8TB), and financial transactions (3.2TB). The DNN integrated quality-aware feature extraction with online learning to enable real-time monitoring and detection. The system employed a distributed architecture with parallel processing for scalable, low-latency operations and incorporated temporal-spatial correlations for comprehensive quality evaluation. Experimental results demonstrated high performance, achieving detection accuracies above 96%, precision around 95%, and processing latency below 10ms, with throughput exceeding 1.2 million events per second, maintaining robust performance across different datasets and operational conditions. The study faced limitations in computational resource requirements, as processing large-scale distributed data streams demanded substantial CPU and memory usage. It also had reduced interpretability, making it difficult to explain specific anomaly detections within the deep neural network model. The summary of the recent works on anomaly detection in network traffic data using DL is given in Table II.

TABLE II. SUMMARY OF RECENT WORKS ON ANOMALY DETECTION IN NETWORK TRAFFIC DATA USING DL

| Author [Ref] | Methodology | Advantages | Disadvantages / Limitations |
|---|---|---|---|
| Altaf et al. (2024) [9] | Sequential Gated Graph Convolutional Network (GGCN) for IoT traffic; time-stamped multi-edge graphs with gated message passing | ▪ Captured temporal patterns in IoT traffic.<br>▪ Outperformed standard GNN models.<br>▪ Effective in binary classification with imbalanced data. | ▪ Focused only on binary classification.<br>▪ Limited evaluation on multiclass scenarios.<br>▪ Adaptability to evolving network threats not fully addressed. |
| Sattar et al. (2025) [10] | Self-supervised contrastive learning (ET SSL) for encrypted traffic; flow-level statistical features | ▪ Real-time detection with low latency and energy consumption.<br>▪ Preserved privacy.<br>▪ High detection accuracy and F1 score. | ▪ Simulated traffic used- Relied on adaptive retraining.<br>▪ High computational complexity. |
| Wang & Song (2024) [11] | CNN-based deep learning for network traffic classification and anomaly detection | ▪ Reduced error rates and false alarms.<br>▪ Robust performance across multiple real network environments. | ▪ High data and computational requirements.<br>▪ Reduced interpretability.<br>▪ Effectiveness decreased with insufficient. or unrepresentative data. |
| Morshedi & Matinkhah (2025) [12] | LSTM-based deep learning for IoT traffic under Gaussian noise; integrated Hurst parameter | ▪ Effectively detected anomalies.<br>▪ Improved robustness against noise.<br>▪ Suitable for edge deployment. | ▪ Required sufficient data for training.<br>▪ Limited interpretability of LSTM outputs. |
| Zhang et al. (2025) [13] | Deep neural network (DNN) with adaptive online learning for real-time quality assessment and anomaly detection in distributed streams | ▪ Real-time monitoring and detection.<br>▪ High detection performance and throughput.<br>▪ Scalable distributed architecture. | ▪ High computational resource requirements.<br>▪ Reduced interpretability of anomaly detections. |

### *C. Anomaly Detection in Network Traffic Data Using Hybrid Approaches*

Hybrid approaches for anomaly detection in network traffic data combine the best attributes of several techniques, including ML, DL, and statistical models, to enhance detection accuracy and robustness. These methods combine various feature extraction, learning, and classification methodologies to address the limitation of individual models. By exploring complementary capabilities, hybrid approaches enhance adaptability to diverse network environments, identify complex anomalies more effectively, and offer better performance in real-time environments.

Marfo et al. (2024) [14] developed a GNN-based anomaly detection framework for securing IoT networks. The model integrated GraphSAGE and Graph Attention Networks (GAT) to capture both local and significant node interactions. GraphSAGE was used to learn embeddings from neighborhood data, while GAT focused on essential communication patterns. The authors modelled host and flow nodes to construct a heterogeneous graph that accurately reflected network behaviour. The methodology was evaluated

using the UNSW-NB15 dataset, where the hybrid model achieved high accuracy, outperforming individual GraphSAGE and GAT models. The study demonstrated the effectiveness of combining multiple GNN architectures for enhanced detection of anomalies in IoT networks, with reduced false positives and false negatives. The study was constrained by limited dataset diversity, lack of real-time testing, and unverified scalability on distributed systems, which affected the evaluation of adaptability and performance in dynamic environments.

Kamal and Mashaly (2023) [15] designed enhanced hybrid DL models for anomaly detection in intrusion detection systems. Their work introduced two architectures, Autoencoder with Convolutional Neural Network (Autoencoder CNN) and Transformer with Deep Neural Network (Transformer DNN). The Autoencoder was applied to reshape traffic data and manage class imbalance, while the CNN carried out precise classification. The Transformer component extracted contextual features, and the DNN performed final classification. To further handle imbalance, the study incorporated enhanced adaptive synthetic sampling with synthetic minority oversampling and edited nearest neighbors. The models were trained and evaluated on publicly available datasets, including CICIDS2017 and NF BoT IoT v2, and demonstrated high performance compared with traditional approaches to intrusion detection. The study was limited by uncertain generalization, as the models were tested only on specific datasets and not across diverse traffic or attack types. It was also constrained by reliance on extensive data preprocessing and by the trial-and-error process required for model adaptation.

.Lebaku et al. (2025) [16] implemented anomaly detection in connected autonomous vehicles (CAVs) using ML and DL techniques. The study generated a dataset simulating vehicle behavior, including time-series data of position, speed, and acceleration under normal and atypical conditions. A stacked LSTM model was applied to capture temporal dependencies and sequence-based anomalies, while a Random Forest model provided ensemble-based predictions. The stacked LSTM model achieved an $R^2$ of 0.9998, a Mean Absolute Error (MAE) of 82.425, and a 95th percentile anomaly threshold of 265.63, whereas the Random Forest model attained an $R^2$ of 0.9830, MAE of 5.746, and a 95th percentile threshold of 14.18. Both models effectively detected anomalies, with LSTM excelling in temporal patterns and Random Forest providing precise predictions. The study faced limitations in the precision of the stacked LSTM model, as its MAE indicated reduced accuracy for small distance predictions. Additionally, the 95th percentile threshold used for anomaly detection caused smaller disruptions to be overlooked, limiting the detection of subtle anomalies.

Onsu et al. (2024) [17] investigated anomaly detection in vehicles using hybrid DL. Real-time data were collected on experimental roads from multiple vehicles equipped with AI-enabled edge units, capturing signals related to harsh cornering, harsh braking, and rapid acceleration. The raw data were preprocessed to remove redundant and noisy features, and an autoencoder-based labeling process identified and labeled anomalous behaviors. A hybrid DL model combining CNN, LSTM, attention mechanisms, and Fully Connected Neural Networks (FCDNN) was trained and tested on the labeled dataset. The approach effectively detected anomalous driving events and outperformed state-of-the-art methods, demonstrating the capability of hybrid DL for accurate and robust vehicle anomaly detection. The study faced limitations in computational complexity, as the hybrid DL model required substantial processing power for training and real-time detection. It also had reduced interpretability, making it difficult to explain specific anomaly detections.

Rezakhani et al. (2023) [18] developed a transfer learning framework for anomaly detection in multivariate IoT traffic data. The study addressed the challenge of limited labeled datasets by proposing a Contrastive Target-Adaptive LSTM-VAE (CTAL-VAE) that required no labeled data from either source or target domains. The framework combined contrastive learning with an LSTM-VAE architecture and domain-specific adaptors. Experiments were conducted on the WUSTL-IIOT-2021 and ACI-IoT-2023 datasets. Results showed that CTAL-VAE achieved 90% accuracy, outperforming VAE and AE models, which attained 82% and 79%, respectively. Moreover, CTAL-VAE recorded the highest Matthews Correlation Coefficient (MCC) and sensitivity, confirming its robustness in detecting anomalies and handling imbalanced data more effectively than baseline models. The study was constrained by evaluation metrics under class imbalance and by the computational complexity of the architecture, which reduced interpretability. The summary of the recent works on anomaly detection in network traffic data using hybrid models is given in Table III.

TABLE III. SUMMARY OF RECENT WORKS ON ANOMALY DETECTION IN NETWORK TRAFFIC DATA USING HYBRID MODELS

| Author [Ref] | Methodology | Advantages | Disadvantages / Limitations |
|---|---|---|---|
| Marfo et al. (2024) [14] | Hybrid GNN combining GraphSAGE and Graph Attention Network (GAT) for IoT anomaly detection | ▪ Captured local and significant node interactions.<br>▪ Reduced false positives and negatives.<br>▪ Outperformed individual GNN models. | ▪ Limited dataset diversity.<br>▪ No real-time testing.<br>▪ Unverified scalability in distributed systems. |
| Kamal & Mashaly (2023) [15] | Hybrid deep learning: Autoencoder-CNN and Transformer-DNN; enhanced adaptive synthetic sampling for class imbalance | ▪ Managed class imbalance effectively.<br>▪ Extracted contextual features and precise classification.<br>▪ High performance compared to traditional IDS. | ▪ Tested only on specific datasets.<br>▪ Extensive preprocessing required.<br>▪ Trial-and-error adaptation needed. |

| | | | |
|---|---|---|---|
| Lebaku et al. (2025) [16] | ML and deep learning: Stacked LSTM + Random Forest for anomaly detection in connected autonomous vehicles | ▪ LSTM captured temporal dependencies.<br>▪ Random Forest provided precise predictions.<br>▪ Effective anomaly detection | ▪ LSTM precision limited for small distances.<br>▪ 95th percentile threshold unnoticed subtle anomalies. |
| Onsu et al. (2024) [17] | Hybrid deep learning: CNN + LSTM + Attention + FCDNN; autoencoder-based labeling for vehicle anomaly detection | ▪ Detected anomalous driving events accurately.<br>▪ Outperformed state-of-the-art methods.<br>▪ | ▪ High computational complexity.<br>▪ Reduced interpretability of detections. |
| Rezakhani et al. (2023) [18] | Transfer learning: Contrastive Target-Adaptive LSTM-VAE (CTAL-VAE) for multivariate IoT traffic | ▪ Handled limited labeled data effectively.<br>▪ Outperformed VAE and AE models.<br>▪ Robust against class imbalance. | ▪ Evaluation affected by class imbalance.<br>▪ High computational complexity.<br>▪ Reduced interpretability. |

## III. Research Gap

Despite the widespread application of AI techniques for anomaly detection in network traffic data, several models present limitations that hinder broader applicability. Some models, such as XGBoost and LightGBM, require high computational resources, making them unsuitable for resource-constrained or latency-sensitive networks. Other classifiers, like Naïve Bayes, depend on unrealistic feature independence assumptions, while Isolation Forest shows weak performance on high-dimensional data, further reducing their applicability [4]. In addition, random forest models have not been fully optimized and were not validated in real-network environments, which questions their generalizability. The difficulty in defining normal behavior, dependence on large datasets for threshold calibration, and sensitivity to sensor measurement uncertainties further limit the effectiveness of certain approaches [6]. Some studies restrict their focus to specific attacks such as DDoS, which reduces their ability to detect a broader range of anomalies, while also facing computational efficiency and scalability challenges in large-scale IoT networks. Methods relying on short time windows and traffic volume features demonstrate reduced effectiveness in detecting subtle or scan-based anomalies [8]. DL approaches, though powerful, are often limited to binary classification tasks, restricting their ability to address multiclass traffic scenarios. Others depend on simulated traffic and require frequent retraining, while also introducing high computational overheads [10].

High data and computational requirements constrain scalability, and interpretability challenges reduce trust and adoption in operational settings. Similarly, LSTM-based models demand sufficient training data but still face reduced interpretability of results. Moreover, deep neural networks for large-scale streaming environments incur significant computational resource requirements and limited interpretability. Hybrid techniques attempt to overcome these gaps, yet many suffer from limited dataset diversity, lack of real-time testing, and unverified scalability in distributed networks [14]. Some rely heavily on preprocessing and trial-and-error adaptation, affecting efficiency. Thresholding mechanisms risk overlooking subtle anomalies [16], while hybrid deep learning frameworks often demand substantial computational power and remain difficult to interpret. Additionally, the problem of class imbalance continues to hinder fair evaluation and robust anomaly detection [18]. Existing studies on anomaly detection demonstrate valuable contributions but also exhibit notable shortcomings. ML-based methods often face scalability issues, over-reliance on feature independence assumptions, and poor performance on high-dimensional data. DL-based techniques achieve higher accuracy but require heavy computational resources, lack interpretability, and are constrained by binary-class setups. Hybrid approaches attempt to mitigate these gaps but remain challenged by limited dataset diversity, high preprocessing demands, and restricted real-time validation. These limitations collectively frame the research gap: the absence of lightweight, interpretable, and scalable AI-based anomaly detection models that can operate effectively across diverse traffic scenarios with real-time adaptability.

## IV. Conclusion

Anomaly detection in network traffic data remains a crucial aspect of modern cybersecurity strategies, enabling the identification of irregular patterns that signal malicious activity, system faults, or policy violations. As networks grow more dynamic and diverse, the need for timely and accurate detection has become vital for safeguarding data integrity, maintaining operational stability, and preventing large-scale disruptions. Traditional detection methods, such as rule-based systems and statistical models, have historically supported network monitoring, but they often struggle with evolving attack vectors, suffer from high false alarm rates, and lack adaptability in complex environments. Their reliance on predefined rules and assumptions limits their effectiveness, particularly when applied to real-time or large-scale settings. Despite the progress of ML, DL, and hybrid approaches, AI-driven anomaly detection still faces significant constraints such as high computational cost, limited interpretability, and dependency on large annotated datasets. In addition, challenges remain in managing rapidly evolving attack patterns, addressing class imbalance, and ensuring scalability for real-time deployments across heterogeneous and resource-constrained environments. Another critical limitation is the lack of transparency in many advanced models, which reduces user trust and complicates adoption in sensitive domains. Future opportunities lie in multiple directions. The development of lightweight yet accurate models will be essential for deployment on edge devices and in latency-sensitive applications. Incorporating explainable and interpretable AI techniques can enhance user trust and provide actionable insights for network administrators. Privacy-

preserving anomaly detection frameworks will also become increasingly important in safeguarding user data while enabling large-scale monitoring. Furthermore, the integration of domain knowledge, the use of federated and collaborative learning frameworks, and the evaluation of models across diverse real-world and multi-institutional datasets can address scalability and generalization issues. By bridging these shortages and challenges, AI-driven anomaly detection systems can evolve into resilient, adaptive, and sustainable frameworks that provide robust protection against emerging cyber threats.

## REFERENCES

[1] Wei, Z., Wang, J., Zhao, Z., & Shi, K. (2025). Toward data efficient anomaly detection in heterogeneous edge–cloud environments using clustered federated learning. Future Generation Computer Systems, 164, 107559.

[2] Marfo, W., Tosh, D. K., & Moore, S. V. (2025). Adaptive client selection in federated learning: A network anomaly detection use case. arXiv preprint arXiv:2501.15038.

[3] Park, D., Choi, S. S., Lim, D., & Kang, Y. S. (2025). Graph Multi-Resolution Transformer for Road Traffic Anomaly Detection. IEEE Access.

[4] Ness, S., Eswarakrishnan, V., Sridharan, H., Shinde, V., Janapareddy, N. V. P., & Dhanawat, V. (2025). Anomaly Detection in Network Traffic using Advanced Machine Learning Techniques. IEEE Access.

[5] Fosić, I., Žagar, D., Grgić, K., & Križanović, V. (2023). Anomaly detection in NetFlow network traffic using supervised machine learning algorithms. Journal of industrial information integration, 33, 100466.

[6] Sakhnevych, A., Pasquino, N., & Sperlì, G. (2025). Design of a machine learning approach to anomaly detection in tyre-road interaction. IEEE Access.

[7] Mohammed, B. H., Sallehudin, H., Satar, N. S. M., Murhg, H. D., Mohamed, S. A., Alaba, F. A., ... & Bianchi, I. (2025). Anomaly detection of distributed denial of service (DDoS) in IoT network using machine learning. In Digital Technologies and Transformation in Business, Industry and Organizations: Volume 3 (pp. 41-64). Cham: Springer Nature Switzerland.

[8] Baldoni, S., & Battisti, F. (2025). Histogram-based network traffic representation for anomaly detection through PCA. Computer Networks, 111276.

[9] Altaf, T., Wang, X., Ni, W., Yu, G., Liu, R. P., & Braun, R. (2024). GNN-Based Network Traffic Analysis for the Detection of Sequential Attacks in IoT. Electronics, 13(12), 2274.

[10] Sattar, S., Khan, S., Khan, M. I., Akhmediyarova, A., Mamyrbayev, O., Kassymova, D., ... & Alimkulova, J. (2025). Anomaly detection in encrypted network traffic using self-supervised learning. Scientific Reports, 15(1), 26585.

[11] Wang, Y., & Song, L. (2025). Application and optimization of convolutional neural networks based on deep learning in network traffic classification and anomaly detection. Informatica, 49(14).

[12] Morshedi, R., & Matinkhah, S. M. (2025). Anomaly Detection in IoT Traffic in the Presence of Gaussian Noise Using Deep Neural Networks. Journal of AI and Data Mining.

[13] Zhang, H., Jia, X., & Chen, C. (2025). Deep Learning-Based Real-Time Data Quality Assessment and Anomaly Detection for Large-Scale Distributed Data Streams. *International Journal of Medical and All Body Health Research*, *6*(1), 1-01.

[14] Marfo, W., Tosh, D. K., & Moore, S. V. (2024, June). Enhancing network anomaly detection using graph neural networks. In 2024 22nd Mediterranean Communication and Computer Networking Conference (MedComNet) (pp. 1-10). IEEE.

[15] Kamal, H., & Mashaly, M. (2025). Enhanced Hybrid Deep Learning Models-Based Anomaly Detection Method for Two-Stage Binary and Multi-Class Classification of Attacks in Intrusion Detection Systems. Algorithms, 18(2), 69.

[16] Lebaku, P. K. R., Gao, L., Zhang, Y., Li, Z., Liu, Y., & Arafin, T. (2025). Cybersecurity-focused anomaly detection in connected autonomous vehicles using machine learning. In International Conference on Transportation and Development 2025 (pp. 566-580)

[17] Onsu, M. A., Simsek, M., Fobert, M., & Kantarci, B. (2025). Intelligent multi-sensor fusion and anomaly detection in vehicles via deep learning. Internet of Things, 31, 101561.

[18] Rezakhani, M., Seyfi, T., & Afghah, F. (2025). A transfer learning framework for anomaly detection in multivariate iot traffic data. arXiv preprint arXiv:2501.15365.