

Application of Machine Learning for Anomaly Detection in Network Traffic to Enhance Cybersecurity

Fajar Maulana Putra^{a,1*}, Kevin Jonathan^{b,2}, Ahmad Fauzan Ramadhan^{c,3}

^a Program of Computer Science, Universitas Indonesia, Depok, Indonesia
^b Department of Computer Science, National University of Singapore, Singapore, Singapore
^c Program of Information Technology, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia
¹ fajar.maulana.putra@email.com ^{*}; ² kevin.jonathan@gmail.com; ³ ahmad.fauzan.ramadhan.academic@gmail.com
^{*} Corresponding author

ARTICLE INFO	ABSTRACT
Article history Received: 25 August 2026 Revised: 23 September 2026 Accepted: 24 September 2026 Published: 26 September 2026 Keywords machine learning network traffic anomaly detection cybersecurity network security  License by CC-BY-SA Copyright © 2025, The Author(s).	The increasing volume and complexity of network traffic have created significant challenges for cybersecurity, particularly in identifying abnormal activities that may indicate security threats. Machine learning has emerged as an important approach for network anomaly detection because it can identify complex traffic patterns and support automated threat detection. This study aims to examine the application of machine learning for anomaly detection in network traffic and analyze its contribution to cybersecurity. The study employed a structured literature review and comparative qualitative synthesis based on 27 scientific publications published between 2024 and 2026. The analysis focused on conventional machine learning, deep learning, ensemble learning, hybrid approaches, real-time detection, adaptive detection, and scalable network anomaly detection. The empirical evidence shows that algorithm performance varies according to the dataset and evaluation context. Pai et al. (2025) reported accuracies of 98.28% for K-nearest neighbors, 97.00% for random forest, 96.62% for gradient boosting, 87.95% for support vector machine, and 85.59% for logistic regression on the CICIDS2017 dataset. Their hybrid ensemble stacking approach achieved 98.79% accuracy. Ness et al. (2025) reported 1.00 training accuracy and 0.85 test accuracy for LightGBM, demonstrating the importance of evaluating model generalization. The study concludes that machine learning can strengthen network anomaly detection, but model selection must consider data characteristics, feature complexity, class imbalance, scalability, and real-time processing requirements.

How to cite: Putra, F. M., Jonathan, K., & Ramadhan, A. F. (2026). Application of Machine Learning for Anomaly Detection in Network Traffic to Enhance Cybersecurity. *Journal of Computer Science and Information Technology*, 2 (3), 131-141. doi: <https://doi.org/10.70716/jocsit.v2i3.841>

INTRODUCTION

The rapid expansion of digital networks has increased the volume and complexity of network traffic generated by users, applications, cloud services, connected devices, and distributed information systems. This development has also increased the potential exposure of network infrastructures to unauthorized access, malicious activities, abnormal communication patterns, and other cybersecurity threats. Network traffic anomaly detection has therefore become an important component of cybersecurity because it enables security systems to identify deviations from expected network behavior. Machine learning has received increasing attention in this context because it can analyze traffic characteristics and identify patterns associated with anomalous behavior. Alang and Bindewari (2025) demonstrate the relevance of machine learning for anomaly detection and prediction in network data, while Alwan (2024) emphasizes its application to cybersecurity through automated anomaly identification. These developments indicate that machine learning can provide a more adaptive analytical capability than security mechanisms that depend exclusively on predefined detection rules.

Traditional network security mechanisms commonly rely on predefined signatures, rules, or known attack characteristics. Such mechanisms remain useful for detecting previously identified threats, but their effectiveness can decline when network behavior changes or when attacks exhibit characteristics that differ from previously defined patterns. Chen et al. (2024) explain that artificial intelligence and machine learning can strengthen threat detection by enabling systems to analyze complex data patterns. El Hajj Hassan and Duong-Trung (2024) similarly identify machine learning as an important approach for network traffic detection and classification. Mahmood et al. (2025) further report that machine learning-based network

anomaly detection can support the identification of abnormal traffic while reducing dependence on manually defined detection rules. The growing use of machine learning is therefore associated with the need to develop security mechanisms that can process large-scale network data and respond to changing traffic characteristics.

The application of machine learning to network anomaly detection involves several algorithmic approaches with different characteristics and operational requirements. Comparative research is important because no single algorithm necessarily provides the most appropriate solution for every network environment. Aswathy and Rajkumar (2024) examine real-time network traffic anomaly detection through a comparative analysis of machine learning algorithms, demonstrating the importance of evaluating algorithmic performance in relation to network traffic conditions. Bakhare and Mohod (2024) also emphasize the performance and challenges associated with machine learning models for network anomaly detection. Kareliya et al. (2024) investigate machine learning-based network anomaly detection, while Zhao et al. (2024) examine the use of the K-nearest neighbors method for detecting anomalies in network security traffic. These studies show that algorithm selection remains a central issue because differences in model characteristics can influence the ability to distinguish normal and abnormal network behavior.

Recent research has expanded beyond individual machine learning classifiers toward deep learning, ensemble learning, and hybrid approaches. Sharma and Grover (2024) evaluate isolation forests and autoencoders for anomaly detection, while Simon et al. (2024) investigate autoencoders as a deep learning approach for enhanced network anomaly detection. These approaches are relevant because network traffic can contain complex relationships that may not be adequately represented by simple classification mechanisms. Banerjee et al. (2025) extend this direction through a hybrid machine learning and deep learning approach for real-time network traffic anomaly detection. Kumari et al. (2025) examine machine learning classifiers for cybersecurity anomaly detection, while Gudnavar et al. (2025) investigate a dual-layered approach for cyber threat detection and analysis. The development of these approaches indicates a shift from evaluating individual algorithms toward combining complementary models to improve the detection of complex network anomalies.

Ensemble learning represents another important development in this research area because it combines the outputs or learning capabilities of multiple algorithms. Pai et al. (2025) evaluate several machine learning algorithms, including K-nearest neighbors, gradient boosting, support vector machines, random forests, and logistic regression, and further examine voting and stacking techniques. Their study demonstrates the potential of a hybrid multi-layered stacking model for network anomaly detection. The approach was evaluated using the CICIDS 2017 dataset and incorporated feature importance and dimensionality reduction to improve model efficiency. The study reported that the hybrid ensemble stacking model achieved an accuracy of 98.79% within its experimental setting (Pai et al., 2025). This finding should be interpreted as evidence from the respective study rather than as a general performance guarantee because the effectiveness of a model depends on the dataset, preprocessing procedures, features, attack categories, and evaluation conditions. Nevertheless, the result supports the relevance of ensemble strategies in addressing the limitations of individual classifiers.

The increasing requirement for real-time cybersecurity also creates additional challenges for machine learning-based anomaly detection. Network traffic is generated continuously, and security systems must process large amounts of information while maintaining adequate detection performance. Jakkani (2024) examines real-time network traffic analysis and anomaly detection using machine learning approaches, highlighting the relationship between anomaly detection, network security, and performance. Sharma (2025) also focuses on anomaly detection in network traffic, reinforcing the relevance of continuous traffic analysis. Narang (2025) addresses scalable artificial intelligence techniques for detecting anomalies in extensive computer networks, indicating that scalability is an important consideration when applying intelligent detection mechanisms to large network environments. Shoyab and Ahmed (2025) further examine network anomaly detection using machine learning and streaming-oriented approaches. These studies indicate that network anomaly detection should be considered not only from the perspective of classification performance but also from the perspective of processing requirements and operational deployment.

Network data characteristics present another significant challenge. Network traffic can contain numerous features, varying traffic distributions, and unequal representations of normal and anomalous events. Such characteristics can affect the performance and generalization of machine learning models. Ness et al. (2025) specifically examine advanced machine learning techniques for network traffic anomaly detection while addressing class imbalance and feature complexity. Their work demonstrates that model

evaluation should consider the characteristics of the input data rather than relying exclusively on a single performance measure. Mahmood et al. (2025) likewise identify computational complexity and dataset quality as important challenges in machine learning-based network anomaly detection. Kikbayev et al. (2025) contribute a comparative perspective by examining machine learning methods for detecting anomalies in network traffic. These findings establish that effective anomaly detection requires an appropriate relationship between the characteristics of network data, feature representation, algorithm selection, and evaluation procedures.

The cybersecurity orientation of anomaly detection has also become broader. Detection systems are increasingly expected to support threat identification and prevention rather than merely classify network observations as normal or abnormal. Saritha (2025) examines artificial intelligence for network security with an emphasis on anomaly detection in traffic data, while Pushkar (2025) connects machine learning-based network traffic anomaly detection with cyber threat prevention. Chen et al. (2024) similarly position artificial intelligence-driven detection as a mechanism for strengthening cybersecurity. Usoro and Etuk (2025a, 2025b) extend the discussion by examining automated identification and forensic analysis of network traffic anomalies through ensemble learning. This direction is important because cybersecurity operations require detection results that can contribute to subsequent investigation and response activities. Gouda et al. (2026) also examine anomaly-based network intrusion detection using machine learning, further demonstrating the continuing development of machine learning applications for intrusion and anomaly detection.

Despite the increasing number of studies, a research gap remains in the integration and comparison of recent findings across different machine learning approaches. Existing studies frequently emphasize particular algorithms, datasets, detection objectives, or experimental configurations. As a result, reported performance cannot always be directly compared across studies. A model that performs effectively on one dataset may produce different results under another traffic distribution or attack configuration. This issue is particularly relevant when studies report accuracy without simultaneously considering precision, recall, F1 score, false positives, false negatives, feature complexity, computational requirements, and adaptability. Ness et al. (2025) and Pai et al. (2025) demonstrate the importance of considering these factors in evaluating network anomaly detection systems. Therefore, the assessment of machine learning for cybersecurity should extend beyond identifying which algorithm produces the highest reported accuracy and should instead consider the broader relationship between detection performance and practical network requirements.

Another gap concerns the transition from isolated model evaluation toward adaptive and integrated cybersecurity systems. Research has increasingly examined hybrid machine learning and deep learning models, ensemble methods, real-time detection, scalable architectures, and forensic applications. However, these developments also introduce methodological diversity that makes it difficult to establish a unified understanding of the strengths and limitations of current approaches. Banerjee et al. (2025) emphasize hybrid machine learning and deep learning for real-time detection, Gudnavar et al. (2025) investigate a dual-layered detection architecture, and Usoro and Etuk (2025a, 2025b) focus on ensemble-based identification and forensic analysis. These developments indicate that the field is moving toward more integrated detection mechanisms, but the effectiveness of such mechanisms remains dependent on data quality, feature representation, algorithm configuration, computational resources, and evaluation criteria.

Based on these conditions, the present study focuses on the application of machine learning for anomaly detection in network traffic to enhance cybersecurity. The study examines recent research concerning conventional machine learning, deep learning, ensemble learning, hybrid approaches, real-time detection, and scalable network anomaly detection. The analysis is directed toward identifying methodological tendencies, the role of machine learning in recognizing anomalous network behavior, and the principal challenges that affect cybersecurity implementation. The study does not treat the performance reported by individual source studies as newly generated experimental results. Instead, the findings are interpreted in accordance with the evidence reported in the reviewed literature. This approach is important for maintaining analytical accuracy because differences in datasets, algorithms, preprocessing procedures, and evaluation protocols can affect reported results.

The contribution of this study is to provide a structured synthesis of recent evidence on machine learning-based network traffic anomaly detection and its relevance to cybersecurity. The analysis connects algorithmic approaches with practical considerations such as real-time detection, scalability, feature complexity, class imbalance, false-positive and false-negative reduction, and integration with broader cybersecurity processes. The study therefore provides an analytical basis for understanding why machine learning has become an important approach to network anomaly detection while also identifying the

limitations that must be considered before deployment. The main objective is to examine how recent machine learning approaches are applied to network traffic anomaly detection and to determine the methodological and operational factors that influence their contribution to cybersecurity. The resulting synthesis is expected to support more systematic evaluation of machine learning approaches and provide a basis for future research that uses consistent datasets, transparent evaluation procedures, and clearly defined operational requirements.

METHODS

Research Design

This study employed a structured literature review with comparative qualitative synthesis to examine the application of machine learning for network traffic anomaly detection and its contribution to cybersecurity. The study adopted a secondary research design because the analysis was based exclusively on previously published scientific literature. The review focused on conventional machine learning, deep learning, ensemble learning, hybrid approaches, real-time detection, adaptive detection, and scalable network anomaly detection.

The review process consisted of five stages: literature identification, screening, eligibility assessment, data extraction, and comparative qualitative synthesis. This procedure was used to ensure that the selected publications were relevant to the research objectives and that findings from different studies could be compared systematically while preserving their original research contexts.

Literature Scope and Selection

The literature population consisted of scientific publications addressing machine learning, artificial intelligence, network anomaly detection, network traffic analysis, intrusion detection, or cybersecurity threat detection. The analytical sample comprised 27 publications published between 2024 and 2026. The selected publications included journal articles, conference proceedings, and a research work available through Zenodo.

The selection of publications was based on their relevance to the research focus. Publications were considered eligible when they addressed the identification, classification, prediction, analysis, or prevention of abnormal network traffic using machine learning or related artificial intelligence techniques. Studies addressing real-time detection, deep learning, ensemble learning, hybrid approaches, scalability, or cybersecurity applications were also considered because these dimensions were directly related to the objectives of the review.

The final sample of 27 publications was determined based on the literature available and considered relevant to the analytical scope of the study. Because the original research records did not document the number of records identified before screening, duplicate removal, or exclusion at each screening stage, this study does not report unsupported numerical values for those stages. The 27 publications represent the final literature set analyzed in this review.

Inclusion and Exclusion Criteria

The inclusion criteria were established according to the research objectives. A publication was included when it met the following conditions: (1) it was published between 2024 and 2026; (2) it addressed machine learning or a related artificial intelligence approach; (3) it concerned network traffic anomaly detection, network security, intrusion detection, or cybersecurity threat detection; and (4) it provided information relevant to at least one of the analytical dimensions examined in this study.

Publications that did not address network-related anomaly detection, did not involve machine learning or a closely related artificial intelligence approach, or did not provide information relevant to the research focus were excluded from the analytical synthesis. Publications that were outside the defined publication period were also excluded.

Data Collection and Extraction

Data were collected through document analysis of the 27 selected scientific publications. A structured extraction framework was used to organize information from each publication. The extracted information included publication year, research focus, dataset or network traffic context, machine learning approach, algorithmic category, detection objective, reported performance metrics, and cybersecurity implications.

The extracted information was organized into a study-characteristics matrix to facilitate comparison across publications. The matrix included author, publication year, dataset or evaluation context, algorithm or methodological approach, research objective, reported evaluation metrics, and principal findings. When a particular characteristic was not explicitly reported in the source publication, it was recorded as not reported rather than inferred.

The reviewed studies were subsequently grouped according to their dominant methodological characteristics. Conventional machine learning approaches included studies examining standard classification and anomaly detection algorithms. Deep learning and autoencoder-based approaches were represented by studies examining autoencoders and related architectures. Hybrid and ensemble approaches included studies combining multiple machine learning or machine learning and deep learning techniques. Other studies were grouped according to their emphasis on real-time detection, scalability, adaptive detection, streaming analysis, or broader cybersecurity applications.

Quality Appraisal

This study did not perform a formal standardized risk-of-bias or methodological quality assessment of the 27 publications. The analysis instead emphasized the relevance of each publication to the research objectives and the evidence explicitly reported by the respective source.

To minimize overinterpretation, reported numerical results were retained only when they were explicitly available in the source studies. The interpretation also considered differences in datasets, algorithms, preprocessing procedures, experimental configurations, and evaluation protocols. Consequently, findings from individual publications were not treated as directly equivalent and were not combined into a pooled quantitative estimate.

The absence of a formal quality appraisal represents a limitation of the review. Therefore, the findings should be interpreted as a structured qualitative synthesis of the available literature rather than as an assessment of the relative methodological quality of the reviewed studies.

Data Analysis and Coding

The extracted data were analyzed using comparative qualitative synthesis. The analysis was conducted through three sequential stages: coding, categorization, and cross-study synthesis.

First, each publication was coded according to its dominant methodological approach and research objective. The methodological codes included conventional machine learning, deep learning, ensemble learning, hybrid approaches, real-time detection, adaptive detection, scalable detection, and cybersecurity-oriented applications. The objective-related codes included anomaly identification, classification, prediction, threat detection, prevention, intrusion detection, and forensic analysis.

Second, the coded studies were categorized according to recurring analytical dimensions. These dimensions included algorithm selection, dataset characteristics, detection objectives, reported performance, feature complexity, class imbalance, model generalization, computational efficiency, scalability, real-time processing, and cybersecurity implications.

Third, findings within and across categories were compared to identify recurring patterns, differences, methodological limitations, and research directions. Findings were considered recurring when similar methodological or operational characteristics were identified across multiple publications. Findings specific to an individual dataset, algorithm, or experimental configuration were retained within the context of the corresponding source study.

The synthesis mechanism therefore connected the methodological characteristics of the reviewed studies with their reported findings and operational implications. The analysis did not assign numerical scores or rankings to algorithms because the reviewed publications used different datasets, experimental configurations, and evaluation procedures. Instead, the synthesis emphasized contextual interpretation and the identification of consistent patterns across the literature.

Comparative Performance Analysis

The comparative analysis considered performance-related dimensions reported in the reviewed literature, including accuracy, precision, recall, F1 score, false positives, false negatives, feature complexity, class imbalance, scalability, computational efficiency, and real-time detection. These dimensions were selected because they were relevant to evaluating machine learning-based network anomaly detection and were discussed across the reviewed studies.

Numerical performance values were retained only as findings of the respective source publications. They were not recalculated or presented as original experimental results of this study. For example, the accuracy values reported by Pai et al. (2025) were interpreted within the experimental context of that study and were not generalized to other network environments. This procedure prevented differences between datasets and experimental configurations from being treated as directly equivalent.

Synthesis Validity and Limitations

The final synthesis connected the methodological characteristics of machine learning approaches with their potential contribution to cybersecurity. Particular attention was given to algorithm selection, network traffic characteristics, class imbalance, feature complexity, false-positive and false-negative considerations, scalability, adaptability, and real-time processing.

Because the reviewed publications used different datasets, algorithms, experimental configurations, and evaluation protocols, this study did not perform statistical meta-analysis or calculate a pooled performance estimate. The validity of the synthesis was maintained by preserving the original context of each reported finding and distinguishing source-reported evidence from the analytical conclusions of the present review.

The resulting synthesis should therefore be understood as a comparative qualitative interpretation of 27 recent publications rather than as a new experimental evaluation of machine learning algorithms. This approach allows the study to identify methodological tendencies, recurring challenges, and practical considerations while avoiding unsupported generalization of performance results across different network environments.

RESULTS AND DISCUSSION

3.1 Empirical Evidence from the Reviewed Studies

The literature synthesis demonstrates that machine learning has been applied through diverse approaches for network traffic anomaly detection. The reviewed studies include conventional machine learning, deep learning, ensemble learning, hybrid architectures, real-time detection, and scalable detection frameworks. However, the reported empirical metrics are not directly comparable across all studies because the publications use different datasets, experimental configurations, algorithms, and evaluation procedures. Therefore, this study presents only numerical findings that are explicitly reported in the reviewed literature and retains their original experimental context.

The most detailed empirical comparison was reported by Pai et al. (2025). Their study evaluated K-nearest neighbors, random forest, gradient boosting, support vector machine, and logistic regression using CICIDS2017 and NFS-2023-TE. The study subsequently developed voting and stacking ensemble approaches. The reported results show that K-nearest neighbors achieved 98.28% and 91.00% accuracy on the two datasets, respectively. Random forest achieved 97.00% and 96.00%, while gradient boosting achieved 96.62% and 92.00%. Support vector machine achieved 87.95%, and logistic regression achieved 85.59% in the reported comparison. The hybrid ensemble stacking model subsequently achieved an accuracy of 98.79%.

Table 1. Reported Accuracy of Base Machine Learning Models in Pai et al. (2025)

Model	CICIDS2017 Accuracy (%)	NFS-2023-TE Accuracy (%)
K-nearest neighbors	98.28	91.00
Random forest	97.00	96.00
Gradient boosting	96.62	92.00
Support vector machine	87.95	Not reported in the cited result
Logistic regression	85.59	Not reported in the cited result
Hybrid ensemble stacking	98.79	Not reported as a separate value

Note. Values are reproduced from the empirical results reported by Pai et al. (2025). "Not reported" indicates that a corresponding value was not available in the source result used for this synthesis. The values are not results generated by the present study.

The results in Table 1 indicate that the performance of individual algorithms varies across network datasets. On CICIDS2017, K-nearest neighbors produced the highest accuracy among the reported base

models at 98.28%, followed by random forest at 97.00% and gradient boosting at 96.62%. Support vector machine and logistic regression produced lower reported accuracy values of 87.95% and 85.59%, respectively. On NFS-2023-TE, random forest produced 96.00%, followed by gradient boosting at 92.00% and K-nearest neighbors at 91.00%. The difference between the results across datasets demonstrates that algorithm performance depends on the characteristics of the evaluated network traffic rather than remaining constant across environments. This finding supports the argument that model selection should consider dataset characteristics and operational requirements.

The empirical comparison also provides evidence supporting the use of ensemble learning. The hybrid stacking model reported by Pai et al. (2025) achieved 98.79% accuracy, which was higher than the reported accuracy of each individual base model on CICIDS2017. The difference is relatively small compared with the strongest base model, K-nearest neighbors, but the result demonstrates that combining multiple classifiers can produce a competitive detection model. The study also incorporated feature importance and dimensionality reduction and explicitly considered false positives and false negatives for practical deployment. This finding is consistent with the broader direction identified in Banerjee et al. (2025) and Gudnavar et al. (2025), which examine hybrid and layered approaches for network threat and anomaly detection. The evidence therefore suggests that ensemble and hybrid approaches should be evaluated not only on their final accuracy but also on their ability to maintain reliable detection across different traffic conditions.

A second source providing explicit numerical evidence is Ness et al. (2025). The study evaluates Isolation Forest, Naive Bayes, XGBoost, LightGBM, and support vector machine for network traffic anomaly detection. The authors report that LightGBM achieved a training accuracy of 1.00 and a test accuracy of 0.85. The study also reports that Isolation Forest showed substantially lower accuracy than the stronger supervised models. The difference between the LightGBM training and test results is important because it demonstrates why evaluation should not rely exclusively on training performance. A high training result does not necessarily indicate equivalent performance on unseen test data. Ness et al. (2025) therefore provide empirical support for evaluating anomaly detection models using independent test data and multiple performance criteria.

Table 2. Explicit Numerical Findings Available from the Reviewed Literature

Study	Dataset or evaluation context	Model/approach	Reported empirical result
Pai et al. (2025)	CICIDS2017	K-nearest neighbors	98.28% accuracy
Pai et al. (2025)	CICIDS2017	Random forest	97.00% accuracy
Pai et al. (2025)	CICIDS2017	Gradient boosting	96.62% accuracy
Pai et al. (2025)	CICIDS2017	Support vector machine	87.95% accuracy
Pai et al. (2025)	CICIDS2017	Logistic regression	85.59% accuracy
Pai et al. (2025)	CICIDS2017	Hybrid ensemble stacking	98.79% accuracy
Pai et al. (2025)	NFS-2023-TE	K-nearest neighbors	91.00% accuracy
Pai et al. (2025)	NFS-2023-TE	Random forest	96.00% accuracy
Pai et al. (2025)	NFS-2023-TE	Gradient boosting	92.00% accuracy
Ness et al. (2025)	Network anomaly detection evaluation	LightGBM	1.00 training accuracy; 0.85 test accuracy

Note. The table includes only numerical values explicitly available from the reviewed source studies. No missing values were estimated or calculated.

3.2 Comparison with Recent Machine Learning Approaches

The empirical evidence is supported by the broader methodological findings in the reviewed literature. Aswathy and Rajkumar (2024) compare machine learning algorithms for real-time network traffic anomaly detection, while Bakhare and Mohod (2024) emphasize the performance and challenges associated with machine learning models. Alang and Bindewari (2025) examine machine learning for anomaly detection and prediction in network data, and Kareliya et al. (2024) investigate machine learning-based network anomaly detection. These studies reinforce the importance of comparing alternative algorithms rather than assuming that one classifier will perform optimally across all network environments.

Deep learning provides another methodological direction. Sharma and Grover (2024) evaluate isolation forests and autoencoders, while Simon et al. (2024) investigate autoencoders for proactive network anomaly detection. These approaches are relevant when network traffic contains complex patterns that require more advanced representation mechanisms. However, the numerical findings available in the present literature set do not provide sufficiently consistent performance metrics across these studies to support a direct quantitative ranking. Consequently, their contribution is interpreted at the methodological level rather than converted into unsupported numerical comparisons.

Hybrid and ensemble approaches have become increasingly prominent in recent research. Banerjee et al. (2025) investigate a hybrid machine learning and deep learning approach for real-time anomaly detection, while Gudnavar et al. (2025) examine a dual-layered approach for cyber threat detection and analysis. Pai et al. (2025) provide the clearest numerical evidence in this group because their study reports both individual classifier performance and hybrid stacking performance. The evidence indicates that combining classifiers can achieve competitive performance, but the result should remain associated with the dataset and experimental configuration used in the source study. It should not be interpreted as evidence that stacking will always outperform individual classifiers.

3.3 Network Data Complexity and Generalization

Network traffic anomaly detection involves methodological challenges that extend beyond algorithm selection. Ness et al. (2025) explicitly examine class imbalance and feature complexity and compare supervised and unsupervised approaches. Their reported LightGBM results demonstrate the importance of distinguishing training performance from test performance. The training accuracy of 1.00 compared with the test accuracy of 0.85 indicates that strong performance on training data does not automatically translate into equivalent performance on unseen data. This issue is particularly relevant for cybersecurity applications because detection models must process traffic patterns that can differ from the observations used during model development.

Mahmood et al. (2025) identify machine learning as an important approach for network anomaly detection while emphasizing the broader methodological challenges associated with the field. Kikbayev et al. (2025) provide a comparative analysis of machine learning methods for network traffic anomalies, while Zhao et al. (2024) demonstrate the application of K-nearest neighbors to network security traffic anomalies. Together, these studies reinforce the importance of evaluating models according to their data characteristics and intended detection context. The empirical evidence available in the reviewed literature therefore supports a cautious interpretation of model performance and discourages the use of a single metric as the sole basis for selecting a cybersecurity detection model.

3.4 Real-Time Detection, Scalability, and Cybersecurity Implications

The practical deployment of network anomaly detection requires more than high classification accuracy. Network security systems must process traffic continuously and respond to anomalous activity within operational constraints. Jakkani (2024) examines real-time network traffic analysis and anomaly detection, while Sharma (2025) focuses on anomaly detection in network traffic. Shoyab and Ahmed (2025) also examine machine learning-based network anomaly detection in a streaming context. These studies indicate that real-time processing is an important consideration when translating machine learning research into operational cybersecurity systems.

Scalability is similarly important because network environments can generate large volumes of traffic. Narang (2025) investigates scalable artificial intelligence techniques for anomaly detection in extensive

computer networks, while Vinisha and Gopala Krishna (2025) examine network traffic anomaly detection through a comprehensive machine learning approach. Saritha (2025) considers artificial intelligence for network security and traffic anomaly detection, and Pushkar (2025) links machine learning-based anomaly detection with cyber threat prevention. The collective evidence indicates that machine learning can contribute to cybersecurity through automated identification of anomalous traffic, but practical effectiveness depends on the ability to operate under the specific computational and traffic conditions of the target environment.

The reviewed literature also extends anomaly detection toward broader cybersecurity functions. Kumari et al. (2025) examine machine learning classifiers for cybersecurity anomaly detection, while Usoro and Etuk (2025a, 2025b) address automated identification and forensic analysis through ensemble learning. Gouda et al. (2026) investigate anomaly-based network intrusion detection using machine learning. These studies support the interpretation that anomaly detection can function as part of a broader cybersecurity process involving identification, analysis, prevention, and subsequent investigation. However, because the studies employ different experimental settings, their results should be interpreted individually rather than combined into a single quantitative performance estimate.

Overall, the empirical evidence confirms that machine learning provides a relevant basis for network traffic anomaly detection, while also demonstrating that performance varies according to the selected algorithm and evaluation environment. Pai et al. (2025) provide direct evidence that model performance varies across CICIDS2017 and NFS-2023-TE and that their hybrid stacking approach achieved 98.79% accuracy in the reported experimental setting. Ness et al. (2025) demonstrate that training and test performance can differ substantially, with LightGBM achieving 1.00 training accuracy and 0.85 test accuracy. These findings strengthen the argument that cybersecurity anomaly detection should be evaluated through independent test performance, multiple metrics, and consideration of the operational characteristics of network traffic.

The principal implication is that there is no sufficient empirical basis within the reviewed literature to declare one machine learning algorithm universally superior for network anomaly detection. Instead, the evidence supports a context-dependent selection process. Conventional models remain relevant, while ensemble, deep learning, hybrid, real-time, and scalable approaches provide additional directions for addressing increasingly complex network traffic. The appropriate approach should therefore be determined by the characteristics of the network data, detection objectives, computational requirements, and evaluation criteria. This interpretation is consistent with the overall findings of the reviewed studies and avoids extrapolating numerical performance beyond the experimental conditions under which those results were obtained.

CONCLUSION

This study examined recent applications of machine learning for anomaly detection in network traffic to support cybersecurity. The literature synthesis shows that machine learning provides an important approach for identifying abnormal network behavior and addressing the limitations of conventional detection mechanisms. The reviewed studies demonstrate the use of conventional machine learning, deep learning, ensemble learning, hybrid architectures, and approaches designed for real-time and scalable detection. The empirical evidence reported by Pai et al. (2025) shows that model performance varies across network datasets and algorithms. Their hybrid ensemble stacking approach achieved 98.79% accuracy in the reported experimental setting, while individual algorithms produced different results across CICIDS2017 and NFS-2023-TE. Ness et al. (2025) further demonstrate the importance of evaluating generalization because LightGBM achieved 1.00 training accuracy compared with 0.85 test accuracy. These findings confirm that high training or benchmark performance should not be interpreted independently of the evaluation context.

The study concludes that effective network anomaly detection requires consideration of algorithm selection, data characteristics, feature complexity, class imbalance, false positives, false negatives, scalability, and real-time processing requirements. Ensemble and hybrid approaches provide promising directions, but their effectiveness remains dependent on the dataset and experimental conditions. Future research should therefore emphasize consistent evaluation procedures, transparent reporting, independent testing, and practical deployment considerations. Such efforts can strengthen the reliability and applicability of machine learning-based anomaly detection for cybersecurity.

REFERENCES

- Alang, K. S., & Bindewari, S. (2025). Machine learning for anomaly detection and prediction in network data. *Journal of Quantum Science and Technology*, 2(2), 207–220. <https://doi.org/10.63345/jqst.v2i2.268>
- Alwan, S. J. (2024). Enhancing cybersecurity through machine learning: An exploration of anomaly detection. *International Journal of Computer Science and Mobile Computing*, 13(6). <https://doi.org/10.47760/ijcsmc.2024.v13i06.005>
- Aswathy, M. C., & Rajkumar, T. (2024). Real time anomaly detection in network traffic: A comparative analysis of machine learning algorithms. *International Research Journal of Advanced Engineering Hub*, 2(7), 1968–1977. <https://doi.org/10.47392/IRJAEH.2024.0269>
- Bakhare, S., & Mohod, S. W. (2024). Evaluating the performance and challenges of machine learning models in network anomaly detection. *International Journal of Scientific Research in Science, Engineering and Technology*. <https://doi.org/10.32628/IJSRSET5241134>
- Banerjee, S., Basak, B., Mandal, S., Manna, S., Chakraborty, S., Ghatak, S., & Das, A. (2025). Real-time anomaly detection in network traffic: A hybrid ML-DL approach. In *2025 International Conference on Engineering Innovations and Technologies (ICoEIT)* (pp. 536–539). IEEE. <https://doi.org/10.1109/ICoEIT63558.2025.11211805>
- Chen, H., Shen, Z., Wang, Y., Ke, H., & Xu, J. (2024). Threat detection driven by artificial intelligence: Enhancing cybersecurity with machine learning algorithms. *World Journal of Innovation and Modern Technology*, 7(6), 58–70. [https://doi.org/10.53469/wjimt.2024.07\(06\).09](https://doi.org/10.53469/wjimt.2024.07(06).09)
- El Hajj Hassan, S., & Duong-Trung, N. (2024). Machine learning in cybersecurity: Advanced detection and classification techniques for network traffic environments. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, 11(3). <https://doi.org/10.4108/eetinis.v11i3.5237>
- Gouda, M. B., Varshini, S., Pranati, B., Naik, V. R., et al. (2026). Anomaly based network intrusion detection system using ML. *International Journal of Research and Scientific Innovation*, 12(13), 202–219. <https://doi.org/10.51244/IJRSI.2025.1213CS0017>
- Gudnavar, A., Naregal, K., & Madagouda, B. (2025). Cyber threat detection and analysis using dual-layered approach. *Journal of Computer Information Systems*. <https://doi.org/10.1080/08874417.2025.2553156>
- Jakkani, A. K. (2024). Real-time network traffic analysis and anomaly detection to enhance network security and performance: Machine learning approaches. *Journal of Electronics, Computer Networking and Applied Mathematics*, 4(4), 32–44. <https://doi.org/10.55529/jecnam.44.32.44>
- Kareliya, R., Mokal, N., Shah, P., Solanki, H., & Shingare, S. (2024). ML-based network anomaly detection. *International Journal of Research Publication and Reviews*, 5(4), 7959–7962. <https://doi.org/10.55248/gengpi.5.0424.10124>
- Kikbayev, N. E., Zhexebay, D., Xin, Y., et al. (2025). Comparative study of machine learning methods for detecting anomalies in network traffic. *Kazakhstan-British Technical University Bulletin*, 22(4), 79–96. <https://doi.org/10.55452/1998-6688-2025-22-4-79-96>
- Kumari, L. K., Balasubramanian, K., Krishnasamy, R., Mohan, B., et al. (2025). Anomaly detection in cybersecurity using machine learning classifiers. In *2025 6th International Conference on Recent Advances in Information Technology (RAIT)*. IEEE. <https://doi.org/10.1109/RAIT65068.2025.11089051>
- Mahmood, N. H., Hussein, D. H., Askar, S., & Ibrahim, M. A. (2025). Machine learning for network anomaly detection: A review. *The Indonesian Journal of Computer Science*, 14(1). <https://doi.org/10.33022/ijcs.v14i1.4703>
- Narang, S. (2025). Advanced scalable artificial intelligence techniques for detecting anomalies in extensive computer networks for improved cybersecurity. In *2025 International Conference on Smart & Sustainable Technology (INCSST)*. IEEE. <https://doi.org/10.1109/INCSST64791.2025.11210388>

- 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*, 13, 16133–16149. <https://doi.org/10.1109/ACCESS.2025.3526988>
- Pai, V., Pai, K., Manjunatha, S., Hirmeti, S., & Bhat, V. V. (2025). Adaptive network anomaly detection using machine learning approaches. *EURASIP Journal on Information Security*, 2025, Article 29. <https://doi.org/10.1186/s13635-025-00216-4>
- Pushkar, V. (2025). Anomaly detection in network traffic using machine learning for cyber threat prevention. *International Scientific Journal of Engineering and Management*. <https://doi.org/10.55041/isjem03144>
- Saritha, A. (2025). Advancing network security with artificial intelligence: A study on anomaly detection in traffic data. In *2025 International Conference on Intelligent Computing, Data Communication and Applications*. IEEE. <https://doi.org/10.1109/ICIDCA66325.2025.11280503>
- Sharma, R., & Grover, M. (2024). Enhancing cybersecurity with machine learning: Evaluating the efficacy of isolation forests and autoencoders in anomaly detection. In *2024 International Conference on Communication, Computing and Power Technologies*. IEEE. <https://doi.org/10.1109/ICCPCT61902.2024.10673338>
- Sharma, S. (2025). Anomaly detection in network traffic. In *2025 International Conference on Advances in Robotics, Computing and Systems Technologies*. IEEE. <https://doi.org/10.1109/ACROSET66531.2025.11280898>
- Shoyab, M. A., & Ahmed, M. (2025). Network anomaly detection using machine learning and stream it. *Indian Journal of Computer Science and Technology*. <https://doi.org/10.59256/indjct.20250403006>
- Simon, J., Kapileswar, N., Vani, R., Reddy, N. M., Moulali, D., & Narayana Reddy, A. R. (2024). Enhanced network anomaly detection using autoencoders: A deep learning approach for proactive cybersecurity. In *2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI)* (pp. 90–96). IEEE. <https://doi.org/10.1109/ICoICI62503.2024.10696845>
- Usoro, E. B., & Etuk, E. M. (2025a). *Automated identification and forensic analysis of network traffic anomalies through ensemble learning techniques: An advanced machine learning framework for cybersecurity threat intelligence*. Zenodo. <https://doi.org/10.5281/zenodo.18104051>
- Usoro, E. B., & Etuk, E. M. (2025b). *Automated identification and forensic analysis of network traffic anomalies through ensemble learning techniques: An advanced machine learning framework for cybersecurity threat intelligence*. Zenodo. <https://doi.org/10.5281/zenodo.18104052>
- Vinisha, N., & Gopala Krishna, S. (2025). Detecting network traffic anomalies with machine learning: A comprehensive approach. *International Journal for Research in Applied Science and Engineering Technology*, 13(10), 762–770. <https://doi.org/10.22214/ijraset.2025.74139>
- Zhao, F., Zhang, M., Zhou, S., & Lou, Q. (2024). Detection of network security traffic anomalies based on machine learning KNN method. *Journal of Artificial Intelligence General Science*, 1(1), 209–218. <https://doi.org/10.60087/jaigs.v1i1.213>