International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 13 Issue 02 February 2026

Study of various technique for Anomaly Detection in Network Security

Sunil kumar[1], Aman Prakash Janoriya[2]
Research Scholar[1], Assistant Professor[2]
Department Of Computer Science & Engineering, Radha Raman Engineering College, Bhopal (M.P.)[1, 2]
Sunilkancsejsr@gmail.com[1], amanprakashjanoriya@gmail.com[2]

Abstract: *Anomaly detection in network security plays a vital role in identifying malicious activities, intrusions and abnormal behaviors that deviate from normal network operations. With the increasing sophistication and volume of cyber attacks, traditional rule-based and signature-based intrusion detection systems are often inadequate for detecting novel or evolving threats. This survey presents a comprehensive review of various anomaly detection techniques applied in network security, encompassing statistical methods, machine learning algorithms and deep learning approaches. It examines their underlying principles, strengths, limitations and suitability for different network environments. The paper also explores hybrid and ensemble models that combine multiple detection strategies to enhance accuracy and reduce false alarms. Furthermore, recent advancements leveraging artificial intelligence and big data analytics for real-time anomaly detection are discussed. By comparing existing methodologies, this study aims to provide insights into current research trends, highlight open challenges and suggest potential directions for developing more adaptive and intelligent network anomaly detection systems.*

Keywords: *Machine Learning, Deep Learning, Cyber Attacks, Network Security, Support Vector Machines.*

1. INTRODUCTION

In the digital era, network security has become a cornerstone of modern information systems, playing a crucial role in ensuring data confidentiality, integrity and availability. The increasing reliance on the internet and networked systems across all sectors—ranging from banking, healthcare and education to defense and e-commerce—has led to an exponential growth in network traffic. This surge in connectivity, while beneficial, has simultaneously created new opportunities for cybercriminals to exploit vulnerabilities and launch sophisticated attacks. Consequently, detecting and mitigating such malicious activities before they can cause damage has become one of the foremost challenges in cybersecurity. Among the various methods developed to safeguard digital assets, anomaly detection has emerged as a key approach for identifying irregular patterns in network behavior that may indicate potential security threats.

Anomaly detection in network security refers to the process of identifying patterns or behaviors that deviate significantly from established norms. Such anomalies may indicate intrusions, malware infections, unauthorized access attempts, or other malicious actions. Unlike signature-based systems, which rely on known attack patterns and predefined rules, anomaly detection techniques can identify previously unseen or "zero-day" attacks by learning what constitutes normal behavior and flagging any deviations. This makes them highly effective in detecting novel threats in dynamic and complex network environments. However, developing robust anomaly detection models is challenging due to the constantly evolving nature of network traffic, the diversity of attack types and the vast volume of data generated by modern communication systems.

Traditionally, intrusion detection systems (IDS) were classified into two main categories: signature-based detection and anomaly-based detection. Signature-based IDSs, such as Snort and Bro (now Zeek), rely on predefined signatures or rules to identify known threats. While effective against

familiar attacks, they often fail to recognize new or modified attack variants. On the other hand, anomaly-based detection systems aim to overcome this limitation by constructing a model of normal network behavior and flagging any deviation as suspicious. This approach has garnered significant attention from researchers due to its ability to detect previously unknown intrusions. Over the past decade, advancements in machine learning (ML), deep learning (DL) and statistical modeling have revolutionized the field, enabling more accurate, scalable and adaptive anomaly detection solutions.

Early approaches to anomaly detection primarily relied on statistical methods, where network metrics such as packet size, flow duration, or traffic rate were analyzed to determine deviations from a normal distribution. Although simple to implement, these models often struggled with dynamic network conditions and high false-positive rates. The advent of machine learning techniques brought significant improvements. Algorithms such as k-means clustering, support vector machines (SVM), decision trees and random forests enabled the development of systems capable of learning complex patterns in network data. Machine learning-based systems can automatically adapt to changes in network behavior, offering better detection accuracy compared to rule-based systems.

More recently, deep learning techniques have gained prominence due to their ability to automatically extract hierarchical and abstract features from raw data. Models such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), long short-term memory (LSTM) networks and autoencoders have been applied to detect anomalies in large-scale network traffic with remarkable success. Deep learning approaches can capture temporal dependencies and nonlinear relationships, making them particularly suitable for analyzing dynamic network environments. Moreover, hybrid frameworks that combine traditional ML and DL methods have shown promise in achieving high accuracy while maintaining computational efficiency.

Despite these advancements, several challenges persist in the domain of network anomaly detection. One major issue is the imbalance of network datasets, where normal traffic vastly outnumbers anomalous instances, leading to biased model training and reduced detection accuracy. Another challenge is the high false-positive rate, where benign activities are misclassified as attacks, causing unnecessary alerts and administrative overhead. Furthermore, as network architectures evolve—incorporating technologies such as cloud computing, the Internet of Things (IoT) and 5G—the nature of traffic patterns becomes increasingly complex, demanding more scalable and adaptive detection mechanisms. The need for real-time processing also adds another layer of complexity, as anomaly detection systems must analyze massive streams of data at high speed without compromising accuracy.

Several benchmark datasets, such as KDD Cup 99, NSL-KDD, UNSW-NB15 and CICIDS2017, have been widely used in research to evaluate anomaly detection models. While these datasets provide valuable insights, many of them fail to fully capture the characteristics of modern network traffic, highlighting the need for continuous dataset updates and realistic simulations. Furthermore, issues related to model interpretability, transparency and explainability remain significant concerns. Many advanced models, especially deep learning-based ones, operate as "black boxes," making it difficult for security analysts to understand the reasoning behind specific detections or false alarms. Therefore, integrating explainable AI (XAI) techniques into anomaly detection systems is becoming an important research direction.

Given these challenges and developments, there is a growing need for a comprehensive study that systematically examines the evolution, methodologies and effectiveness of various anomaly detection techniques in network security. This survey aims to review and analyze existing approaches—ranging from classical statistical and machine learning methods to modern deep learning and hybrid models. The objective is to highlight their operational principles, advantages, limitations and applicability in different contexts. Additionally, the paper discusses recent trends such as federated learning, graph-based detection and AI-driven adaptive systems that are shaping the future of network anomaly detection.

2. LITERATURE REVIEW

Anomaly detection in network security has been extensively studied over the past two decades, evolving from statistical and rule-based systems to advanced machine learning and deep learning techniques. Numerous researchers have contributed significant insights into the design, implementation and evaluation of detection mechanisms to identify malicious or abnormal network behavior. This section reviews key studies that have shaped the development of anomaly detection systems, highlighting their methodologies, contributions and limitations.

M. Ahmed et al. [1] presented one of the most comprehensive early surveys on network anomaly detection techniques. Their study categorized detection approaches into statistical, knowledge-based and machine learning-based methods, providing a detailed comparison of each in terms of performance and adaptability. The authors emphasized that while statistical models are simple and effective for small datasets, they struggle with high-dimensional and dynamic network traffic. Knowledge-based systems, such as rule-based and fuzzy logic approaches, were shown to provide interpretability but lack generalization capabilities when faced with novel attacks. The study further highlighted that machine learning methods, particularly supervised algorithms like Support Vector Machines (SVM) and Decision Trees, offer better adaptability and accuracy in complex network environments. However, Ahmed et al. also pointed out the major challenges faced by ML-based systems, including dataset imbalance, high false-positive rates and the difficulty of feature selection in large-scale networks. Their work laid the foundation for subsequent research exploring more advanced and automated learning techniques.

In a significant advancement over traditional approaches, S. Naseer et al. [2] proposed an enhanced deep neural network (DNN) model for anomaly detection. Their research demonstrated that deep learning could outperform classical machine learning models by automatically extracting complex and hierarchical features from raw network data. Using benchmark datasets such as NSL-KDD and UNSW-NB15, the authors showed that their DNN-based approach achieved higher detection accuracy and lower false alarm rates. They also discussed the importance of parameter optimization and regularization techniques to prevent overfitting. The study concluded that deep learning, with its feature-learning capabilities, holds substantial promise for developing intelligent and adaptive intrusion detection systems. However, it also acknowledged limitations in computational cost and training time, especially for real-time network applications.

Kostas and Kahraman [3] explored the potential of machine learning for network anomaly detection through an empirical research proposal. They reviewed algorithms including K-means, Random Forest and SVM, focusing on their capacity to classify network traffic and detect anomalies efficiently. The authors emphasized the role of data preprocessing, feature normalization and dimensionality reduction in improving model performance. Their study also discussed the importance of combining supervised and unsupervised learning methods to balance detection accuracy with adaptability to unknown attacks. Although the research was primarily conceptual, it contributed to highlighting practical considerations and implementation challenges in deploying ML-based anomaly detection in real-world networks.

Radford et al. [4] introduced a recurrent neural network (RNN)-based approach for detecting network traffic anomalies. Their study leveraged the sequential modeling capabilities of RNNs to capture temporal dependencies in network data streams. Using large-scale datasets, the authors demonstrated that RNNs, particularly Long Short-Term Memory (LSTM) architectures, can effectively model time-series patterns of normal and anomalous traffic. The results showed that this approach could successfully identify subtle and temporally extended attacks that traditional classifiers often miss. The paper also noted that while RNNs provide superior detection accuracy, they require substantial computational resources and careful tuning of hyperparameters to achieve optimal performance.

Building upon this foundation, Kwon et al. [5] conducted a comprehensive survey of deep learning-based network anomaly detection methods. Their work systematically categorized deep learning models into supervised, unsupervised and hybrid approaches. The authors analyzed CNNs, RNNs, autoencoders and generative adversarial networks (GANs), evaluating their effectiveness in detecting complex and evolving threats. The survey highlighted that deep learning methods significantly improve detection rates and scalability but often suffer from interpretability issues. Kwon et al. also identified key research challenges, including data imbalance, model transparency and real-time deployment efficiency, which remain central concerns in modern network security research.

Following this, Malaiya et al. [6] provided an empirical evaluation of deep learning models for network anomaly detection using multiple benchmark datasets. Their comparative analysis of CNN, LSTM and hybrid models revealed that deep architectures outperform traditional ML algorithms in terms of detection accuracy and robustness against unseen attacks. The study also emphasized the role of hyperparameter tuning and feature representation in influencing model performance. However, the authors acknowledged that deep models demand high computational resources and may not be suitable for lightweight or embedded systems. Their empirical insights serve as a

practical guideline for selecting suitable DL architectures in anomaly detection applications.

Usama et al. [7] expanded the discussion by focusing on unsupervised machine learning for networking, highlighting its relevance for detecting unknown or zero-day attacks. Their survey examined clustering, self-organizing maps (SOM) and autoencoder-based methods, emphasizing their ability to uncover hidden structures in unlabeled data. The authors noted that unsupervised learning can significantly enhance anomaly detection when labeled data is scarce, a common limitation in network security datasets. They also addressed key research challenges, such as scalability, explainability and model convergence, proposing potential solutions through hybrid and semi-supervised learning frameworks.

Similarly, Fernandes et al. [8] conducted a comprehensive survey covering traditional and modern anomaly detection methods. They provided a detailed taxonomy of anomaly detection techniques, including statistical analysis, information theory-based methods and machine learning approaches. Their work also examined the performance metrics and evaluation methodologies used across various studies, highlighting inconsistencies in benchmarking practices. The authors emphasized the importance of developing standardized datasets and evaluation frameworks to ensure fair comparison and reproducibility in anomaly detection research. This study remains one of the most detailed surveys in the domain, offering both historical context and insights into emerging trends.

Ali et al. [9] contributed a review of current machine learning approaches for anomaly detection in network traffic. Their work analyzed both supervised and unsupervised algorithms, focusing on their comparative strengths and weaknesses. The authors noted that while supervised models generally achieve higher accuracy, they are heavily dependent on labeled datasets, which are often unavailable or incomplete in real-world scenarios. In contrast, unsupervised models offer better adaptability but may suffer from reduced precision. Their review also emphasized the growing role of ensemble and hybrid methods, which combine the strengths of multiple algorithms to achieve better generalization and robustness against diverse attack types.

Lastly, Lam and Abbas [10] investigated machine learning-based anomaly detection for 5G networks, an emerging area with unique security challenges. Their study addressed the need for scalable, low-latency detection mechanisms capable of handling the massive data throughput of 5G infrastructure. The authors proposed leveraging federated learning and edge-based anomaly detection to maintain data privacy while achieving real-time response. They concluded that integrating AI-driven anomaly detection within 5G systems could significantly enhance proactive threat management, though challenges related to resource allocation, model synchronization and communication overhead remain open research issues.

Wang et al. [11] presented a detailed survey on the role of machine learning in network anomaly detection, focusing on how data-driven methods can improve detection accuracy and adaptability in dynamic network environments. The study categorized ML-based techniques into supervised, unsupervised and reinforcement learning paradigms, analyzing their applicability in various network architectures such as traditional enterprise networks, IoT and cloud systems. The authors emphasized that while supervised learning algorithms such as SVM, Random Forest and Gradient Boosting offer high detection accuracy when trained on quality-labeled datasets, they are limited by their dependency on labeled data and vulnerability to evolving attack patterns. Conversely, unsupervised approaches, including clustering and autoencoders, were highlighted for their ability to detect zero-day attacks in unlabeled data environments. The paper also reviewed hybrid and ensemble learning approaches, concluding that combining multiple models can enhance robustness and reduce false positives. Wang et al. further identified open challenges, including explainability, computational scalability and the need for real-time adaptability in large-scale deployments.

Haji and Ameen [12] conducted a review focusing on attack and anomaly detection in Internet of Things (IoT) networks using machine learning techniques. The authors observed that IoT networks, due to their distributed and resource-constrained nature, introduce unique challenges in anomaly detection such as limited computational capacity, heterogeneous data sources and increased attack surfaces. Their review analyzed various ML algorithms, including Decision Trees, K-Nearest Neighbors (KNN) and Artificial Neural Networks (ANN), applied to IoT-based intrusion detection systems (IDS). The study highlighted that lightweight and adaptive ML algorithms are essential for efficient anomaly detection in IoT environments, as traditional deep models may not suit devices with limited processing capabilities. The authors also emphasized the importance of data preprocessing, feature selection and the use of federated learning techniques to maintain privacy and

reduce communication overhead. This work contributes valuable insights into balancing detection accuracy with computational efficiency in IoT anomaly detection systems.

Fotiadou et al. [13] proposed a deep learning-based framework for network traffic anomaly detection, employing a combination of convolutional and recurrent neural networks. Their approach focused on capturing both spatial and temporal features within network traffic data, thereby improving the detection of complex and evolving attacks. The study demonstrated that deep architectures, particularly CNN-LSTM hybrids, outperform traditional ML models in identifying subtle anomalies in network flows. Experimental evaluations using benchmark datasets confirmed that the proposed model achieved superior accuracy and lower false alarm rates. However, the authors acknowledged challenges related to computational complexity, large-scale data handling and real-time detection latency. They also emphasized that the explainability of deep learning decisions remains an open problem that must be addressed before practical deployment in mission-critical network environments.

Hajj et al. [14] presented a comprehensive review of anomaly-based intrusion detection systems (AIDS), examining their core requirements, methodologies and evaluation metrics. The study classified anomaly detection systems based on detection principles, such as statistical analysis, machine learning and deep learning and evaluated their performance using standard datasets like KDD Cup 99, NSL-KDD and CICIDS2017. The authors also reviewed various metrics including accuracy, precision, recall and F1-score, which are used to assess IDS performance. A key contribution of this work was the discussion of dataset quality and its significant influence on model performance. Hajj et al. noted that many datasets are outdated and lack representation of modern attack vectors, underscoring the need for new, realistic datasets that capture the characteristics of emerging threats such as IoT and 5G-based attacks. The study thus provides a foundational perspective on performance evaluation standards in anomaly detection research.

Chen et al. [15] introduced an improved Naïve Bayes classification algorithm for traffic risk management and anomaly detection. Their modified model incorporated weighted probability estimation and dynamic thresholding to enhance the classifier's sensitivity to rare events and imbalanced datasets. The study demonstrated that the improved Naïve Bayes algorithm achieved better detection accuracy and reduced false-positive rates compared to the traditional approach. The model was computationally lightweight, making it suitable for real-time network monitoring applications. Chen et al. also emphasized that although probabilistic models like Naïve Bayes are simple and interpretable, their performance heavily depends on the quality of input features and assumptions of data independence. Their contribution lies in improving a classic algorithm to make it more applicable for modern, large-scale traffic anomaly detection tasks.

Umer et al. [16] explored machine learning-based intrusion detection for Industrial Control Systems (ICS), which are vital components in critical infrastructure sectors such as power grids and manufacturing. The study reviewed ML applications in detecting anomalies within industrial networks, highlighting the distinct characteristics of ICS traffic, including deterministic communication patterns and stringent latency requirements. The authors discussed the applicability of supervised and unsupervised methods, including SVM, Random Forest and Autoencoders, for detecting cyber-physical anomalies. They also identified several challenges such as dataset scarcity, system heterogeneity and the difficulty of deploying ML solutions in real-time environments without disrupting industrial operations. Their recommendations emphasized developing domain-specific ML models and leveraging transfer learning to enhance detection in ICS networks.

Jebur et al. [17] presented a review on deep learning approaches for anomaly event detection in video surveillance systems. Although their focus extended beyond traditional network traffic, their analysis is relevant to network security as video data often transmits over IP networks. The authors reviewed CNN, RNN and autoencoder architectures used for detecting anomalous activities in video streams, highlighting their adaptability for real-time detection. They also discussed data augmentation techniques, feature extraction and transfer learning strategies that can improve generalization in limited data scenarios. The study concluded that while deep learning significantly advances anomaly event detection, its application in network-based contexts requires optimization for bandwidth efficiency and low-latency inference.

Kim et al. [18] proposed a machine learning framework for anomaly detection in blockchain-based networks, where traffic monitoring is essential for ensuring secure decentralized communication. The study integrated supervised ML algorithms such as Random Forest and SVM with blockchain analytics to identify irregular transaction

patterns indicative of network attacks. The authors demonstrated that ML can enhance blockchain security by detecting anomalies in peer-to-peer communication and consensus processes. Experimental results showed that their framework effectively detected malicious nodes and improved the reliability of blockchain transactions. Kim et al. highlighted the growing importance of combining network monitoring with blockchain analysis, paving the way for secure distributed network anomaly detection solutions.

Fosić et al. [19] focused on NetFlow-based network anomaly detection using supervised machine learning algorithms. Their study evaluated multiple classifiers, including Decision Trees, Random Forest and Gradient Boosting, on large-scale NetFlow datasets collected from real network environments. The results indicated that supervised learning models could achieve high detection rates when trained on diverse and well-labeled datasets. The authors also analyzed feature importance and selection techniques, showing that optimized feature sets significantly reduce computational cost while maintaining detection performance. However, they pointed out that supervised approaches struggle with detecting novel or evolving attacks due to overfitting on historical data. The paper thus highlighted the trade-off between model accuracy and adaptability in supervised ML-based anomaly detection.

Marappan and Marappan [20] introduced deep learning-based intelligent algorithms for anomaly identification and secure communication in vehicular networks. Their study developed an authentication and anomaly detection framework using hybrid deep learning models combining CNN and LSTM networks. The approach aimed to enhance the integrity of data transmission between connected vehicles by identifying abnormal communication behaviors in real time. Simulation results demonstrated improved detection accuracy and reliability under varying network loads. The authors also discussed the challenges of implementing deep learning in vehicular environments, such as computational constraints and rapid mobility. Their research provided valuable insights into the integration of intelligent anomaly detection for securing next-generation vehicular networks (V2X systems).

Kumar et al. [21] proposed a hybrid modified deep learning architecture for intrusion detection that integrates optimal feature selection to improve detection accuracy and computational efficiency. Their model combines convolutional neural networks (CNN) with advanced optimization algorithms to identify significant features from network traffic datasets. By applying hybrid learning strategies, the proposed system achieved high precision and recall, effectively distinguishing between normal and malicious patterns. The study demonstrated that optimal feature selection enhances model interpretability and reduces false positives, offering a robust framework for real-time intrusion detection systems.

Ola-Obaado et al. [22] explored an anomaly-based intrusion detection system leveraging transfer learning techniques. Their approach focused on reusing pretrained deep learning models to detect anomalies in network traffic with minimal training data. This method addressed the challenge of limited labeled datasets, which often hampers deep learning model performance. The transfer learning-based model achieved faster convergence and improved detection accuracy, particularly in identifying zero-day attacks. The research emphasized the efficiency of model reuse in dynamic network environments.

Lahesoo et al. [23] introduced SIURU, a framework for machine learning-based anomaly detection in IoT network traffic. The framework is designed to address the unique constraints of IoT systems, such as limited computational power and heterogeneous data sources. It employs lightweight machine learning models with efficient feature extraction mechanisms to detect anomalous communication patterns in real-time. The experimental results indicated superior adaptability and scalability, making SIURU a promising solution for securing large-scale IoT ecosystems.

Rele et al. [24] conducted a comparative analysis of intrusion detection techniques utilizing machine learning, deep learning and anomaly-based approaches. Their study provided a comprehensive evaluation of algorithms like Random Forest, Support Vector Machines (SVM) and Long Short-Term Memory (LSTM) networks across different benchmark datasets. The findings revealed that deep learning models generally outperform traditional ML techniques in detecting complex attack patterns but require higher computational resources. The study concluded that hybrid approaches could balance performance and efficiency.

Ahmad et al. [25] proposed an early anomaly detection method using deep learning for network security attacks. Their architecture emphasizes early-stage detection to minimize the impact of intrusions before they escalate. By employing temporal deep learning models capable of analyzing sequential network data, the study achieved significant improvements in response time and detection

accuracy. The research highlighted the importance of proactive detection mechanisms in modern cybersecurity infrastructures.

Akhiat et al. [26] presented IDS-EFS, an ensemble feature selection-based method for intrusion detection systems. The study introduced a multi-stage ensemble approach combining several feature selection techniques to identify the most relevant attributes from high-dimensional network traffic data. The proposed system demonstrated improved classification accuracy while maintaining computational efficiency. The authors concluded that ensemble feature selection enhances model robustness against noisy or redundant data features.

Jihado et al. [27] developed a hybrid deep learning-based intrusion detection model combining Convolutional Neural Networks (CNN) and Bidirectional Long Short-Term Memory (BiLSTM) networks. This hybrid design leveraged CNN for spatial feature extraction and BiLSTM for capturing temporal dependencies in network traffic. The results showed enhanced performance in identifying both known and unknown attack types. The study underscored the potential of hybrid architectures in improving detection rates and reducing false alarms.

Khalaf et al. [28] focused on deep learning-based anomaly detection in network traffic for cyber threat identification. The authors implemented advanced neural networks to analyze massive traffic flows and detect deviations from normal behavior. Their model successfully identified complex and evolving threats, demonstrating the scalability of deep learning approaches for high-volume network environments. The study reinforced the relevance of deep architectures in modern cyber defense systems.

Gunupusala [29] examined multi-class network anomaly detection using diverse machine learning techniques. Their work compared algorithms such as Decision Trees, Naïve Bayes and Gradient Boosting for classifying multiple types of network attacks. The study found that ensemble learning models outperform single algorithms, especially in multi-class classification scenarios. The research highlighted that choosing appropriate models for each attack category enhances overall detection accuracy.

Lu et al. [30] conducted a study on network anomaly traffic analysis focusing on statistical and behavior-based methods. The research explored metrics such as packet frequency, data entropy and temporal correlation to identify irregularities in network behavior. Lu emphasized that statistical anomaly detection remains fundamental for understanding baseline traffic characteristics, which aids in complementing machine learning models with domain-specific knowledge.

Alfardus et al. [31] investigated machine learning-based anomaly detection methods for securing in-vehicle networks (IVN). With the rise of connected vehicles, the study emphasized the importance of securing vehicular communications from cyber intrusions. The proposed ML-based framework effectively detected abnormal message exchanges within the Controller Area Network (CAN). Their findings suggest that supervised learning models can provide real-time protection against IVN-based cyber threats.

Takale et al. [32] proposed SecureNet, a network intrusion detection system utilizing a combination of machine learning and deep learning techniques. The hybrid design aimed to integrate the interpretability of ML models with the accuracy of DL architectures. Through experimental evaluation, SecureNet achieved high detection rates for various attack types, proving that multi-level hybridization enhances adaptability and resilience in dynamic network conditions.

Rafique et al. [33] conducted a comprehensive survey of machine learning and deep learning techniques for anomaly detection in IoT networks. Their review identified key challenges such as data heterogeneity, privacy issues and scalability constraints in IoT anomaly detection systems. The study provided insights into the latest research trends, emphasizing lightweight deep models and federated learning frameworks as promising solutions for decentralized IoT environments.

Mynuddin et al. [34] designed an automatic network intrusion detection system integrating both machine learning and deep learning components. Their system employed ensemble classification techniques to enhance reliability and accuracy across diverse datasets. The hybrid system outperformed traditional IDS methods in detecting modern cyber threats, highlighting the effectiveness of combining multiple learning paradigms.

Siddiqui et al. [35] applied machine learning for anomaly detection in IoT-enabled kitchen area networks. Their approach utilized clustering and classification algorithms to identify abnormal device communication patterns, ensuring safety and operational stability. The research demonstrated

that even small-scale IoT environments can benefit from intelligent anomaly detection for preventing potential system failures or cyber risks.

Zhang et al. [36] conducted a comprehensive survey on network security traffic analysis and anomaly detection techniques. Their review compared statistical, rule-based and AI-driven methods, identifying deep learning as the most promising approach for complex anomaly detection tasks. The study highlighted challenges such as high computational demands and model explainability issues, advocating for interpretable AI-based IDS solutions.

Vishnu Priya et al. [37] explored the advancements in anomaly detection techniques in network traffic, focusing on the role of artificial intelligence and machine learning. Their study discussed how AI-enabled models enhance the detection of sophisticated attacks through adaptive learning and continuous improvement. They also emphasized the integration of explainable AI to address the transparency concerns of black-box models.

Ness et al. [38] developed an advanced machine learning framework for network traffic anomaly detection. Their research utilized ensemble and deep reinforcement learning models to dynamically adjust detection thresholds based on network conditions. The results demonstrated improved adaptability and reduced false positives, making it a suitable approach for real-world deployment in large-scale networks.

Zhen et al. [39] proposed an anomaly detection model for network security situational awareness based on machine learning. Their work focused on identifying limitations in existing models, such as poor generalization and insufficient interpretability. They introduced techniques to enhance model transparency and discussed future trends in integrating graph learning and self-supervised techniques for enhanced situational awareness.

Dehkordi et al. [40] presented an overview of recent advances in network security and new anomaly detection techniques. Their review covered both signature-based and behavior-based detection mechanisms, emphasizing hybrid approaches that blend heuristic analysis with ML algorithms. The study suggested that future systems should prioritize adaptability to evolving attack patterns through online learning mechanisms.

Mahmood et al. [41] provided a comprehensive review of machine learning techniques for network anomaly detection. The study classified approaches into supervised, unsupervised and semi-supervised categories, analyzing their respective performance and applicability. The authors concluded that semi-supervised learning holds significant potential for addressing data scarcity and imbalance in real-world intrusion detection datasets.

Yuan et al. [42] explored anomaly detection and privacy protection in network security data using machine learning. The study emphasized the importance of balancing detection performance with user data confidentiality. By integrating privacy-preserving mechanisms such as differential privacy, the research proposed a secure framework that mitigates information leakage while maintaining high detection accuracy.

3. CONCLUSION

Anomaly detection in network security has emerged as one of the most critical and dynamic areas of research, driven by the increasing complexity and sophistication of cyber threats. The literature reviewed in this study highlights the rapid evolution of methodologies—from traditional statistical and rule-based systems to modern machine learning and deep learning approaches. Early systems primarily focused on fixed thresholds and signature matching, which, although effective for known attacks, failed to identify novel or evolving threats. In contrast, contemporary research demonstrates the growing adoption of intelligent and adaptive models that can learn and evolve from data, thereby enhancing detection accuracy and reducing false alarms.

The literature also reveals significant progress in domain-specific applications, such as anomaly detection in IoT networks, vehicular systems, and industrial environments. Lightweight ML models, federated learning, and privacy-preserving techniques have been developed to cater to resource-constrained and privacy-sensitive settings. These advancements demonstrate the versatility and adaptability of AI-driven anomaly detection systems across varied network infrastructures. However, challenges remain in ensuring scalability, explainability, and real-time performance. The black-box nature of deep learning models continues to pose interpretability issues, making it difficult for security analysts to trust automated decisions without transparent explanations.

Furthermore, as cyber threats evolve, traditional static models must give way to dynamic, self-learning frameworks capable of continuous adaptation. The integration of reinforcement learning, graph neural networks, and self-

supervised learning represents promising future directions for creating context-aware, autonomous intrusion detection systems. Additionally, the importance of balancing performance with ethical considerations, such as data privacy and fairness, has become increasingly evident in recent studies.

REFERENCES

[1] M. Ahmed, A. N. Mahmood and J. Hu, ‘‘A survey of network anomaly detection techniques,’’ J. Netw. Comput. Appl., vol. 60, pp. 19–31, Jan. 2016, doi: 10.1016/ j.jnca.2015.11.016.

[2] S. Naseer, Y. Saleem, S. Khalid, M. K. Bashir, J. Han, M. M. Iqbal and K. Han, ‘‘Enhanced network anomaly detection based on deep neural networks,’’ IEEE Access, vol. 6, pp. 48231–48246, 2018, doi: 10.1109/ACCESS.2018.2863036.

[3] Kostas, Kahraman. "Anomaly detection in networks using machine learning." Research Proposal 23 (2018): 343.

[4] Radford, Benjamin J., Leonardo M. Apolonio, Antonio J. Trias and Jim A. Simpson. "Network traffic anomaly detection using recurrent neural networks." arXiv preprint arXiv:1803.10769 (2018).

[5] Kwon, Donghwoon, Hyunjoo Kim, Jinoh Kim, Sang C. Suh, Ikkyun Kim and Kuinam J. Kim. "A survey of deep learning-based network anomaly detection." Cluster Computing 22, no. Suppl 1 (2019): 949-961.

[6] Malaiya, Ritesh K., Donghwoon Kwon, Sang C. Suh, Hyunjoo Kim, Ikkyun Kim and Jinoh Kim. "An empirical evaluation of deep learning for network anomaly detection." IEEE Access 7 (2019): 140806-140817.

[7] M. Usama, J. Qadir, A. Raza, H. Arif, K. A. Yau, Y. Elkhatib, A. Hussain and A. Al-Fuqaha, ‘‘Unsupervised machine learning for networking: Techniques, applications and research challenges,’’ IEEE Access, vol. 7, pp. 65579–65615, 2019, doi: 10.1109/ACCESS.2019.2916648.

[8] G. Fernandes, J. J. P. C. Rodrigues, L. F. Carvalho, J. F. Al-Muhtadi and M. L. Proença, ‘‘A comprehensive survey on network anomaly detection,’’ Telecommun. Syst., vol. 70, no. 3, pp. 447–489, Mar. 2019, doi: 10.1007/s11235-018-0475-8.

[9] Ali, Wasim A., K. N. Manasa, Malika Bendechache, Mohammed Fadhel Aljunaid and P. Sandhya. "A review of current machine learning approaches for anomaly detection in network traffic." Journal of Telecommunications and the Digital Economy 8, no. 4 (2020): 64-95.

[10] Lam, Jordan and Robert Abbas. "Machine learning based anomaly detection for 5g networks." arXiv preprint arXiv:2003.03474 (2020).

[11] Wang, Song, Juan Fernando Balarezo, Sithamparanathan Kandeepan, Akram Al-Hourani, Karina Gomez Chavez and Benjamin Rubinstein. "Machine learning in network anomaly detection: A survey." IEEe Access 9 (2021): 152379-152396.

[12] Haji, Saad Hikmat and Siddeeq Y. Ameen. "Attack and anomaly detection in iot networks using machine learning techniques: A review." Asian journal of research in computer science 9, no. 2 (2021): 30-46.

[13] K. Fotiadou, T.-H. Velivassaki, A. Voulkidis, D. Skias, S. Tsekeridou and T. Zahariadis, ‘‘Network traffic anomaly detection via deep learning,’’ Information, vol. 12, no. 5, p. 215, May 2021, doi: 10.3390/info12050215.

[14] S. Hajj, R. El Sibai, J. B. Abdo, J. Demerjian, A. Makhoul and C. Guyeux, ‘‘Anomaly-based intrusion detection systems: The requirements, methods, measurements and datasets,’’ Trans. Emerg. Telecommun. Technol., vol. 32, no. 4, p. e4240, Apr. 2021, doi: 10.1002/ett.4240.

[15] H. Chen, S. Hu, R. Hua and X. Zhao, ‘‘Improved naive Bayes classification algorithm for traffic risk management,’’ EURASIP J. Adv. Signal Process., vol. 2021, no. 1, p. 30, Dec. 2021, doi: 10.1186/s13634-021-00742-6.

[16] M. A. Umer, K. N. Junejo, M. T. Jilani and A. P. Mathur, ‘‘Machine learning for intrusion detection in industrial control systems: Applications, challenges and recommendations,’’ Int. J. Crit. Infrastruct. Protection, vol. 38, Sep. 2022, Art. no. 100516, doi: 10.1016/j.ijcip.2022.100516.

[17] S. A. Jebur, K. A. Hussein, H. K. Hoomod, L. Alzubaidi and J. Santamaría, ‘‘Review on deep learning approaches for anomaly event detection in video surveillance,’’ Electronics, vol. 12, no. 1, p. 29, Dec. 2022, doi: 10.3390/electronics12010029.

[18] Kim, Jinoh, Makiya Nakashima, Wenjun Fan, Simeon Wuthier, Xiaobo Zhou, Ikkyun Kim and Sang-Yoon Chang. "A machine learning approach to anomaly detection based on traffic monitoring for secure blockchain networking." IEEE Transactions on Network and Service Management 19, no. 3 (2022): 3619-3632.

[19] Fosić, Igor, Drago Žagar, Krešimir Grgić and Višnja Križanović. "Anomaly detection in NetFlow network traffic using supervised machine learning algorithms." Journal of industrial information integration 33 (2023): 100466.

[20] S. Marappan and H. Marappan, ‘‘Deep learning-based intelligent algorithms for effective transmission authentication and anomaly identification in vehicular networks,’’ in Proc. Int. Conf. Innov. Comput., Intell. Commun. Smart Electr. Syst. (ICSES), Dec. 2023, pp. 1–7, doi:10.1109/icses60034.2023.10465346.

[21] N. Kumar and S. Sharma, ‘‘A hybrid modified deep learning architecture for intrusion detection system with optimal feature selection,’’ Electronics, vol. 12, no. 19, p. 4050, Sep. 2023, doi: 10.3390/electronics12194050.

[22] S. Ola-Obaado and M. A. Suleiman, ‘‘Anomaly-based network intrusion detection using transfer learning,’’ in Proc. 2nd Int. Conf. Multidisciplinary Eng. Appl. Sci. (ICMEAS), Nov. 2023, pp. 1–5, doi: 10.1109/icmeas58693.2023.10379384.

[23] L. Lahesoo, U. Do, R. Carnier and K. Fukuda, ‘‘SIURU: A framework for machine learning based anomaly detection in IoT network traffic,’’ in Proc. 18th Asian Internet Eng. Conf., Dec. 2023, pp. 87–95, doi: 10.1145/3630590.3630601.

[24] M. Rele and D. Patil, ‘‘Intrusive detection techniques utilizing machine learning, deep learning and anomaly-based approaches,’’ in Proc. IEEE Int. Conf. Cryptography, Informat., Cybersecurity (ICoCICs), Aug. 2023, pp. 88–93, doi: 10.1109/icocics58778.2023.10276955.

[25] T. Ahmad and D. Truscan, ‘‘Efficient early anomaly detection of network security attacks using deep learning,’’ in Proc. IEEE Int. Conf. Cyber Secur. Resilience (CSR), Jul. 2023, pp. 154–159, doi: 10.1109/csr57506.2023.10224923.

[26] Y. Akhiat, K. Touchanti, A. Zinedine and M. Chahhou, ‘‘IDS-EFS: Ensemble feature selection-based method for intrusion detection system,’’ Multimedia Tools Appl., vol. 83, no. 5, pp. 12917–12937, Jul. 2023, doi: 10.1007/s11042-023-15977-8.

[27] A. A. Jihado and A. S. Girsang, ‘‘Hybrid deep learning network intrusion detection system based on convolutional neural network and bidirectional long short-term memory,’’ J. Adv. Inf. Technol., vol. 15, no. 2, pp. 219–232, 2024, doi: 10.12720/jait.15.2.219-232.

[28] L. I. Khalaf, B. Alhamadani, O. A. Ismael, A. A. Radhi, S. R. Ahmed and S. Algburi, ‘‘Deep learning-based anomaly detection in network traffic for cyber threat identification,’’ in Proc. Cognit. Models Artif. Intell. Conf., May 2024, pp. 303–309, doi: 10.1145/3660853.3660932.

[29] S. Gunupusala and S. C. Kaila, ‘‘Multi-class network anomaly detection using machine learning techniques,’’ Contemp. Math., vol. 5, no. 2, pp. 5–22, Jun. 2024, doi: 10.37256/cm.5220243723.

[30] K. Lu, ‘‘Network anomaly traffic analysis,’’ Academic J. Sci. Technol., vol. 10, no. 3, pp. 65–68, Apr. 2024, doi: 10.54097/8as0rg31.

[31] A. Alfardus and D. B. Rawat, ‘‘Machine learning-based anomaly detection for securing in-vehicle networks,’’ Electronics, vol. 13, no. 10, p. 1962, May 2024, doi: 10.3390/electronics13101962.

[32] V. Takale, A. Patil, A. Lonikar, A. Shinde and P. V. Rupnar, ‘‘SecureNet: Network intrusion detection using machine learning and deep learning techniques,’’ Int. J. Res. Appl. Sci. Eng. Technol., vol. 12, no. 3, pp. 439–443, Apr. 2024, doi: 10.22214/ijraset.2024.59791.

[33] S. H. Rafique, A. Abdallah, N. S. Musa and T. Murugan, ‘‘Machine learning and deep learning techniques for Internet of Things network anomaly detection—Current research trends,’’ Sensors, vol. 24, no. 6, p. 1968, Mar. 2024, doi: 10.3390/s24061968.

[34] M. Mynuddin, S. U. Khan, Z. U. Chowdhury, F. Islam, M. J. Islam, M. I. Hossain and D. M. A. Ahad, ‘‘Automatic network intrusion detection system using machine learning and deep learning,’’ in IEEE MTT-S Int. Microw. Symp. Dig., Feb. 2024, pp. 1–9, doi:10.1109/aims61812.2024.10512607.

[35] M. A. Siddiqui, M. Kalra and C. Rama Krishna, ‘‘Anomaly detection for IoT-enabled kitchen area network using machine learning,’’ in Proc. Int. Conf. MAchine Telligence Res. Innov., 2024, pp. 195–209, doi: 10.1007/978-981-99-8129-8_17.

[36] Zhang, Weibao and Joan P. Lazaro. "A survey on network security traffic analysis and anomaly detection techniques." International Journal of Emerging Technologies and Advanced Applications 1, no. 4 (2024): 8-16.

[37] PM, Vishnu Priya and S. Soumya. "Advancements in anomaly detection techniques in network traffic: The role of artificial intelligence and machine learning." Journal of Scientific Research and Technology (2024): 38-48.

[38] Ness, Stephanie, Vishwanath Eswarakrishnan, Harish Sridharan, Varun Shinde, Naga Venkata Prasad Janapareddy and Vineet Dhanawat. "Anomaly Detection in Network Traffic using Advanced Machine Learning Techniques." IEEE Access (2025).

[39] Zhen, Li, Nazhatul Hafizah Kamarudin, Ven Jyn Kok and Faizan Qamar. "Anomaly Detection Model in Network Security Situational Awareness based on Machine Learning: Limitation, Techniques, Future Trends." IEEE Access (2025).

[40] Dehkordi, Sajad Balali, Saeed Nasri and Sina Dami. "Advances in network security and new anomaly detection techniques." Majlesi Journal of Electrical Engineering 19, no. 2 (June 2025) (2025).

[41] Mahmood, Nawzad Hamad, Diana Hayder Hussein and Shavan Askar. "Machine Learning for Network Anomaly Detection A Review." The Indonesian Journal of Computer Science 14, no. 1 (2025).

[42] Yuan, Shuang. "Research on Anomaly Detection and Privacy Protection of Network Security Data Based on Machine Learning." Procedia Computer Science 261 (2025): 227-236.