International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 15, Issue 1, January 2026)

Network Intrusion Detection: A Comprehensive Review of Machine Learning-Driven Security Frameworks

[1]Himanshu Kumar Singh, [2]Vivek Richhariya, 3Vineet Richhariya
[1]M.Tech Scholar, Department of CSE, LNCT, Bhopal, MP, India
[2&3]Professor, Department of CSE, LNCT, Bhopal, MP, India
acadmyhimanshu@gmail.com, vivekr@lnct.ac.in, vineet@lnct.ac.in

***Abstract*— The exponential growth of internet-connected systems has amplified the need for robust cybersecurity mechanisms, particularly in detecting malicious activities within networks. Network Intrusion Detection Systems (NIDS) have emerged as a pivotal line of defense against both known and novel cyber threats. With traditional rule-based methods struggling to cope with the complexity and volume of modern network traffic, Machine Learning (ML) techniques have gained significant attention for their ability to learn patterns, adapt to new attack types, and reduce false alarm rates. This review comprehensively explores recent advancements in machine learning-based NIDS, categorizing techniques based on learning paradigms such as supervised, unsupervised, and deep learning. It also discusses key challenges including dataset limitations, feature selection, real-time detection, and the growing threat of adversarial attacks, while outlining future research directions aimed at developing intelligent, scalable, and adaptive intrusion detection systems.**

***Keywords*— NIDS, Machine Learning, Cybersecurity, Anomaly Detection, Supervised Learning, Deep Learning.**

I. INTRODUCTION

In the digital era, the exponential increase in internet usage, cloud computing, and connected devices has not only transformed communication and business operations but also significantly expanded the attack surface for cyber threats. Among these threats, network intrusions stand as one of the most pervasive and dangerous forms, often leading to data breaches, financial losses, and reputational damage [1]. As organizations strive to secure their network infrastructures, Network Intrusion Detection Systems (NIDS) have become essential components of modern cybersecurity frameworks. NIDS monitor network traffic to identify unauthorized access, malicious behavior, and potential security violations. However, conventional intrusion detection approaches—typically signature-based or rule-based—are increasingly insufficient in the face of sophisticated, evolving, and zero-day attacks [2].

To overcome these limitations, the integration of Machine Learning (ML) into NIDS has garnered significant interest from researchers and practitioners alike. Machine learning provides the capability to analyze vast volumes of data, learn from historical patterns, and generalize to detect previously unseen threats [3]. Unlike static rule-based systems, ML-based NIDS can adapt to dynamic network environments, thereby improving detection accuracy and reducing false positives. Various ML algorithms, including Support Vector Machines (SVM), Decision Trees, Random Forests, k-Nearest Neighbors (KNN), and more recently, deep learning architectures such as Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks, have shown remarkable success in classifying normal and anomalous network traffic [4].

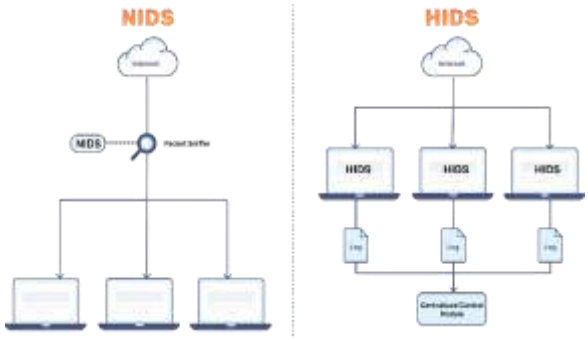

Figure 1: NIDS and HIDS

This review aims to present a consolidated understanding of machine learning applications in NIDS by evaluating recent scholarly contributions, techniques, and real-world implementations [5]. It categorizes ML approaches based on learning paradigms: supervised learning, where models are trained using labeled datasets; unsupervised learning, which identifies hidden patterns in unlabeled data; and reinforcement or semi-supervised methods, which offer hybrid approaches. Furthermore, it explores deep learning

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 15, Issue 1, January 2026)

techniques which have gained momentum due to their superior feature extraction and scalability capabilities [6].

A critical aspect of ML-based NIDS development lies in the availability of high-quality and realistic datasets. Datasets such as KDD Cup 99, NSL-KDD, CICIDS2017, and UNSW-NB15 have been widely used, yet they often suffer from outdated attack patterns, data imbalance, or lack of real-time traffic characteristics [7]. This poses challenges in developing generalized and deployable detection systems. Additionally, feature selection and dimensionality reduction play crucial roles in optimizing model performance, as irrelevant or redundant features can degrade accuracy and increase computation time.

Moreover, real-time intrusion detection remains a complex problem, especially in high-speed networks where timely response is critical. The deployment of ML models must consider latency, computational resources, and scalability [8]. With the rise of adversarial attacks—where attackers manipulate data to fool ML models—the security and robustness of NIDS themselves are now under scrutiny. Research into adversarial machine learning and explainable AI is gaining importance to ensure transparency and trust in the decision-making processes of ML-based systems[9].

While machine learning has revolutionized the landscape of intrusion detection by offering adaptive, intelligent, and data-driven solutions, numerous challenges remain before widespread, reliable deployment can be achieved[10]. This review paper sheds light on current progress, highlights open issues, and suggests future directions for researchers aiming to design effective and resilient network intrusion detection systems powered by machine learning.

Another important factor in the design and implementation of ML-based NIDS is the evaluation metrics used to measure system performance. Commonly adopted metrics such as accuracy, precision, recall, F1-score, and false positive rate (FPR) provide insights into how well the model detects attacks without misclassifying normal traffic. However, a high overall accuracy can sometimes be misleading if the model fails to detect low-frequency but critical attacks [11]. Therefore, confusion matrix analysis and class-wise performance evaluation are often necessary to better understand model behavior in detecting various types of intrusions such as Denial-of-Service (DoS), Remote-to-Local (R2L), User-to-Root (U2R), and Probe attacks. Moreover, cross-validation and testing on unseen datasets are crucial to ensure that the model generalizes well beyond the training data, especially in real-world environments where attack patterns are unpredictable and constantly evolving[12].

II. LITERATURE REVIEW

R. Fu et al., [1] presented a practical approach to designing a network intrusion detection system using machine learning, targeting modern cybersecurity challenges. The authors proposed a model that integrates machine learning algorithms to identify anomalies and malicious behaviors in network traffic. Their system was implemented and tested on recent intrusion datasets, demonstrating significant improvements in accuracy and detection speed. The paper also emphasized the need for adaptive learning to detect evolving threats. Additionally, the authors discussed the limitations of current datasets and recommended future efforts in dataset enrichment. This work serves as a practical contribution towards making ML-based NIDS more efficient and deployable.

Lin et al., [2] introduced E-GRACL, an IoT-based intrusion detection system that leverages the power of Graph Neural Networks (GNNs) for detecting cyber threats in complex network structures. The authors focused on addressing the limitations of conventional deep learning models, which often ignore the topological structure of network traffic. By representing the network as a graph, their proposed GNN model effectively captured relational dependencies among entities in IoT environments. The experimental validation showed high detection accuracy and robustness across different types of network attacks, especially on datasets simulating IoT environments. One key strength of their approach was its generalization capability across varied network topologies. The paper also analyzed performance in terms of computational efficiency, showing that the model scales well with large graphs. Lin et al. highlighted the potential of combining GNNs with other techniques like attention mechanisms for future improvements. Their research offers an innovative path toward smart and context-aware NIDS for IoT frameworks.

Abdulganiyu et al., [3] conducted a comprehensive systematic literature review of existing network intrusion detection systems and evaluated the evolution of methods from traditional approaches to advanced machine learning-based models. The paper categorizes intrusion detection techniques into misuse-based, anomaly-based, and hybrid models, with a focus on their strengths and shortcomings. Their analysis highlighted that supervised learning methods dominate the field, but also identified increasing interest in unsupervised and semi-supervised models to handle

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 15, Issue 1, January 2026)

unlabeled data. The study stressed the critical role of dataset quality, noting common issues like outdated attacks and unbalanced classes in KDD99 and NSL-KDD datasets. It also addressed evaluation metrics and challenges in real-time implementation. The authors emphasized the need for benchmark datasets that reflect modern attack scenarios, including encrypted traffic and adversarial inputs. Moreover, they explored the integration of ML models into cloud and edge computing for scalable solutions. Their review provides a broad foundation for understanding the state-of-the-art in ML-based NIDS.

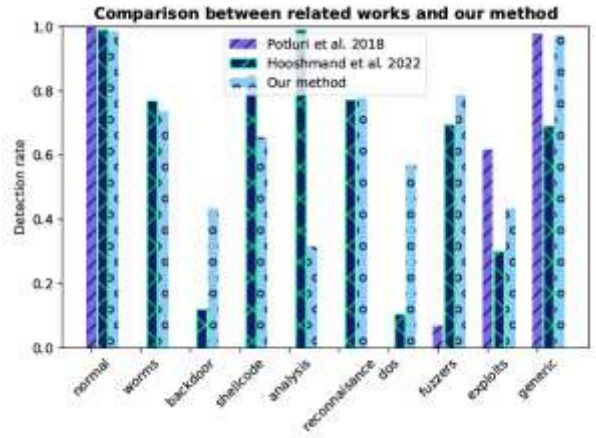

Figure 2: Multi-classification performed [6]

Yogesh and Goyal [4] offered an in-depth review focused specifically on deep learning models in the context of network intrusion detection. They outlined how architectures such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Autoencoders have been utilized for identifying complex attack patterns. The paper discussed key parameters that influence model performance, including input feature extraction, activation functions, training data diversity, and optimization strategies. However, the authors also acknowledged challenges such as high training cost, requirement for large labeled datasets, and vulnerability to adversarial examples. They proposed hybrid frameworks combining CNN and LSTM for capturing both spatial and temporal features of network traffic. This review contributes by mapping the technological landscape and recommending deep learning as a promising path, albeit with clear challenges to address in future research.

Bhutta et al., [5] explored the use of LightGBM, a gradient boosting framework, for real-time WiFi-based intrusion detection systems. The paper aimed to create a lightweight yet highly accurate model suitable for resource-constrained environments like mobile and IoT devices. Through comprehensive experimentation, the authors demonstrated that LightGBM significantly outperforms traditional methods in both detection rate and speed. One of the strengths of their approach was its ability to handle imbalanced data using built-in boosting mechanisms. The proposed system also incorporated data preprocessing techniques to enhance model generalization. Notably, the authors validated their model using publicly available datasets and compared results against SVM and Random Forest classifiers. Their findings support the viability of deploying fast and efficient ML-based NIDS in real-time applications. Bhutta et al. concluded by emphasizing the importance of updating models periodically to maintain detection effectiveness against evolving threats.

Cui et al., [6] proposed a multi-class intrusion detection framework for Software Defined Networks (SDN) using a hybrid model combining Bidirectional Long Short-Term Memory (BiLSTM) networks with traditional classifiers. The authors argued that SDN environments require adaptive and scalable detection solutions due to dynamic traffic patterns and virtualized infrastructures. Their hybrid model captures temporal dependencies in traffic data using BiLSTM, while a final decision layer refines predictions using Softmax or ensemble techniques. The evaluation, performed on benchmark SDN traffic datasets, showed improved precision, recall, and reduced false positives. One key highlight was the use of attention mechanisms to enhance focus on important traffic features, improving classification performance across various attack types. The model was also assessed for scalability and latency, demonstrating that it can operate within real-time constraints. The paper closes by discussing deployment challenges in SDN controllers and the potential integration with other security functions like firewalls and access control systems.

Rajabi et al., [7] proposed an advanced intrusion detection framework that combines Artificial Neural Networks (ANN) with the Firefly Algorithm (FA) to optimize detection accuracy. This hybrid model addresses key limitations in traditional IDS, such as slow convergence and low generalization. The proposed system was evaluated on standard benchmark datasets and demonstrated high detection accuracy, especially in identifying complex and multi-class attacks. The authors reported that the inclusion of the firefly algorithm significantly improved the training process and reduced false positives. They also emphasized the importance of balancing model complexity and

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 15, Issue 1, January 2026)

computational cost for real-time deployment. Overall, this study contributes to the growing body of work on nature-inspired optimization techniques for enhancing ML-based IDS systems, especially in dynamic and heterogeneous network environments.

Li et al., [8] introduced a novel network intrusion detection approach using a Tri-Broad Learning System (Tri-BLS) that integrates spatial-temporal granularity in traffic data analysis. The paper argues that traditional learning models fail to capture both spatial and temporal dependencies in network traffic effectively. The proposed Tri-BLS framework consists of three parallel broad learning models, each designed to extract different types of features — spatial, temporal, and contextual — from network traffic flows. This design enables the model to effectively recognize a wide range of attack patterns, including low-frequency and stealthy intrusions. Evaluation using public datasets demonstrated superior performance in terms of accuracy, recall, and robustness when compared with standard deep learning models. The authors also highlighted the model's fast training and inference times, making it suitable for high-throughput networks. This work underscores the importance of multi-dimensional feature extraction in the development of next-generation IDS solutions.

Xiao et al., [9] presented a robust anomaly-based intrusion detection system tailored for in-vehicle networks, utilizing a Graph Neural Network (GNN) framework. With the increasing complexity of modern automotive systems, securing in-vehicle communication has become a pressing concern. The proposed system models communication data as graphs to preserve structural relationships between different vehicle components. The GNN architecture then learns these relationships to identify anomalous behavior caused by cyber intrusions. The system was tested on real-world automotive datasets and showed remarkable detection capability with low false positive rates. Notably, the model could generalize well to unseen attack types due to its high-level feature abstraction. Additionally, the authors incorporated temporal attention mechanisms to improve detection accuracy in dynamic driving scenarios. This paper is significant as it extends the application of GNNs to the automotive cybersecurity domain, highlighting their potential in embedded and real-time environments.

Aswani et al., [10] focused on fault diagnosis through sound and vibration signal analysis using statistical features combined with machine learning algorithms. Though not a traditional intrusion detection study, the methodologies applied are relevant to network anomaly detection in terms of feature extraction and classification. The researchers collected acoustic and vibrational signals from industrial machines and applied various preprocessing techniques to extract statistical descriptors. These descriptors were then fed into classification models like Decision Trees and Support Vector Machines for fault identification. The study demonstrated that careful feature engineering can significantly improve model accuracy, even in noisy environments. This research contributes valuable insights into the use of non-traditional input sources and signal analysis techniques for anomaly detection, which can be translated into the cybersecurity domain — particularly for detecting physical-layer attacks in cyber-physical systems and IoT networks.

Table 1: Classification of NIDS [5]

Reference	ML model	dataset	classification	online
Yang et al. (2016)	DBN	KDD-KDDCUP99	binary	✗
Li et al. (2017)	CNN	KDD-KDD	binary	✗
Vinayakumar et al. (2017)	CNN/DNN	KDDCUP99	binary/multi	✗
Potluri and Diedrich (2017)	DNN	KDD-KDD	multi	✗
Kroon et al. (2018)	CNN	KDD/Kyoto-Honeypot/UNSWLab	binary	✗
Zheng et al. (2019)	GNN	N/A	binary	✗
Hooshmand and Hosahalli, (2022)	CNN	UNSW-NB15	multi	✗
Narasimha Prasad et al. (2022)	GNN	N/A	binary	✗
Wang and Zhu (2022)	GNN	Kyoto-Honeypot/KDD99SET	binary	✓
Lo et al. (2022)	GNN	Edge-IIoTset-IoT	binary/multi	✓
Our work	GNN	UNSW-NB15	binary/multi	✓

Zhu et al., [11] explored the application of data mining techniques for detecting network intrusions and maintaining system security. Their work primarily utilized clustering and classification methods to analyze large-scale network traffic data. Algorithms such as K-means clustering, Naïve Bayes, and Decision Trees were employed to distinguish normal behavior from suspicious activities. The study also incorporated feature reduction techniques to minimize noise and improve classifier performance. One of the key contributions of the paper was its focus on adaptive learning, enabling the model to evolve as new patterns emerge. Results demonstrated strong performance on legacy datasets, particularly in terms of precision and computational efficiency. The authors concluded that data mining, when appropriately integrated with machine learning, offers a powerful toolkit for developing intelligent and responsive NIDS. However, they also noted the limitations of static models in adapting to sophisticated and dynamic attack vectors.

Varzaneh and Rafsanjani [12] proposed a fuzzy rule-based classification system enhanced with a Genetic Algorithm (GA) for intrusion detection. Their hybrid approach seeks to

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 15, Issue 1, January 2026)

capture the ambiguity and uncertainty inherent in network traffic patterns using fuzzy logic, while the genetic algorithm optimizes rule generation and feature selection. This model offers high interpretability, making it suitable for environments where transparency is essential, such as critical infrastructure and healthcare networks. The authors validated their system using standard datasets and reported a marked improvement in both detection rate and processing time. They also discussed the trade-off between model complexity and computational overhead. The inclusion of genetic optimization allowed the system to maintain a compact rule set without sacrificing accuracy. This study provides a compelling case for the integration of soft computing techniques in IDS, particularly in scenarios requiring high adaptability and explainability.

III. CHALLENGES

The challenges are as follows-

1. Lack of High-Quality and Up-to-Date Datasets

One of the primary challenges in building efficient ML-based NIDS is the absence of comprehensive, real-time, and up-to-date datasets. Most widely used datasets like KDD Cup 99, NSL-KDD, CICIDS2017, and UNSW-NB15 either suffer from outdated attack signatures, class imbalance, or lack of modern threats like polymorphic malware, encrypted traffic, and adversarial inputs. Without representative and realistic datasets, machine learning models often fail to generalize well in real-world scenarios, resulting in high false positives and missed detections. The dynamic nature of cyberattacks demands that datasets evolve continuously to reflect the latest threat landscape.

2. High False Positive Rate

Machine learning-based NIDS often face the issue of high false positive rates (FPR), where benign traffic is mistakenly flagged as malicious. This not only increases the burden on security analysts but can also cause alarm fatigue and lead to genuine threats being ignored. Achieving a balance between detection sensitivity and specificity is critical. An over-sensitive model may generate many false alerts, while an under-sensitive one might miss actual attacks. Proper feature engineering, ensemble methods, and adaptive learning mechanisms are necessary to minimize FPR.

3. Real-Time Processing Constraints

Real-time intrusion detection requires models that are not only accurate but also fast and computationally efficient. Many advanced deep learning models, especially those using recurrent architectures like LSTM or BiLSTM, are resource-intensive and have high latency. Deploying such models in real-time environments, especially on resource-constrained devices (e.g., IoT gateways or edge nodes), is challenging. Optimization techniques such as model pruning, quantization, and hardware acceleration are often necessary but add further complexity to implementation.

4. Adversarial Attacks on ML Models

A significant and growing concern is the vulnerability of ML models to adversarial attacks. Attackers can manipulate input data in subtle ways to evade detection or mislead the model. For example, adding small perturbations to a network packet's features might fool an ML-based NIDS into classifying it as benign. This undermines the reliability and trustworthiness of the intrusion detection system. Developing adversarially robust models and employing explainable AI (XAI) techniques to understand model decisions are crucial areas of ongoing research.

5. Feature Selection and Dimensionality Reduction

Selecting the most relevant features from high-dimensional network traffic data is another critical challenge. Redundant or irrelevant features can degrade model performance, increase computational costs, and lead to overfitting. On the other hand, removing essential features may cause underfitting and missed intrusions. Techniques such as Principal Component Analysis (PCA), Information Gain, or recursive feature elimination are commonly used but may not always yield optimal results. Automating this process while preserving model interpretability remains difficult.

6. Integration with Existing Security Infrastructure

Integrating ML-based NIDS into existing security frameworks, such as firewalls, intrusion prevention systems (IPS), and security information and event management (SIEM) systems, poses technical and operational challenges. Compatibility, scalability, and the ability to provide actionable alerts in a standardized format are essential for practical deployment. Moreover, the system must support continuous updates, real-time communication, and interoperability with other components in a cyber defense architecture.

IV. PROPOSED STRATEGY

To overcome the current limitations and improve the effectiveness of Machine Learning-based Network Intrusion Detection Systems (ML-NIDS), a hybrid and adaptive

multi-stage strategy is proposed. This strategy begins with the use of real-time traffic monitoring tools integrated with data pre-processing modules to handle noisy, incomplete, and imbalanced data. Advanced feature selection techniques, such as Recursive Feature Elimination (RFE) combined with domain knowledge, can help retain only the most relevant attributes, reducing computational complexity while enhancing model performance. At the core, a hybrid ML model combining shallow classifiers (e.g., Random Forest, LightGBM) with deep learning architectures (e.g., BiLSTM, CNN) is recommended to capture both linear and non-linear patterns in temporal and spatial data.

To further enhance resilience, adversarial training techniques should be applied to harden the system against evasion attacks. Moreover, leveraging Graph Neural Networks (GNNs) and attention mechanisms can provide improved detection for complex relational data, especially in IoT and in-vehicle networks. For scalability, the model should be deployed in a distributed or edge computing architecture, ensuring low-latency response in high-speed environments. Additionally, integrating the proposed system with Security Information and Event Management (SIEM) tools and implementing feedback-based model updating will ensure continuous learning and threat adaptability. This multi-layered strategy aims to build an intelligent, efficient, and robust intrusion detection framework suited for dynamic cybersecurity landscapes.

V. CONCLUSION

The integration of machine learning techniques into network intrusion detection systems presents a promising direction for enhancing cybersecurity defenses. This review has highlighted various approaches, ranging from classical machine learning algorithms to advanced deep and graph-based learning models, each offering unique strengths in detecting and classifying network threats. Despite notable progress, challenges such as high false positive rates, dataset limitations, and adversarial vulnerabilities persist. The proposed hybrid strategy, which combines intelligent feature selection, deep learning, and real-time adaptability, aims to address these gaps effectively. With continuous advancements in data availability, computational power, and algorithmic innovations, ML-based NIDS can evolve into highly reliable systems that proactively defend networks against ever-evolving cyber threats.

REFERENCES

1. R. Fu, "Design and Implementation of Network Intrusion Detection System based on Machine Learning," 2025 International Conference on Intelligent Systems and Computational Networks (ICISCN), Bidar, India, 2025, pp. 1-6, doi: 10.1109/ICISCN64258.2025.10934502.
2. Lin, L., Zhong, Q., Qiu, J., & Liang, Z. (2025). E-gracl: an IoT intrusion detection system based on graph neural networks. The Journal of Supercomputing, 81(1), 1-31.
3. Abdulganiyu, O. H., Tchakoucht, T. A., & Saheed, Y. K. (2024). Towards an efficient model for network intrusion detection system (IDS): systematic literature review. Wireless Networks, 30(1), 453-482.
4. Yogesh, & Goyal, L. M. (2024). Deep learning based network intrusion detection system: a systematic literature review and future scopes. International Journal of Information Security, 23(6), 3433-3463.
5. Bhutta, A. A., Nisa, M. U., & Mian, A. N. (2024). Lightweight realtime WiFi-based intrusion detection system using LightGBM. Wireless Networks, 30(2), 749-761.
6. Cui, M., Chen, J., Qiu, X., Lv, W., Qin, H., & Zhang, X. (2024). Multi-class intrusion detection system in SDN based on hybrid BiLSTM model. Cluster Computing, 27(7), 9937-9956.
7. Rajabi, S., Asgari, S., Jamali, S., & Fotohi, R. (2024). An intrusion detection system using the artificial neural network-based approach and firefly algorithm. Wireless Personal Communications, 137(4), 2409-2440.
8. Li, J., Zhang, H., Liu, Z., & Liu, Y. (2023). Network intrusion detection via tri-broad learning system based on spatial-temporal granularity. The Journal of Supercomputing, 79(8), 9180-9205.
9. Xiao, J., Yang, L., Zhong, F., Chen, H., & Li, X. (2023). Robust anomaly-based intrusion detection system for in-vehicle network by graph neural network framework. Applied Intelligence, 53(3), 3183-3206.
10. Aswani, I., Kar, N.K., Ganguly, T., Ramesh, G.P. and Tejaswini, N.P. (2023, February). A Fault Diagnosis of Sound and Vibration Signals Using Statistical Features and Machine Learning

Algorithm. In 2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS) (pp. 1-7). IEEE.

11. Zhu, Y., Gaba, G. S., Almansour, F. M., Alroobaea, R., & Masud, M. (2021). Application of data mining technology in detecting network intrusion and security maintenance. Journal of Intelligent Systems, 30(1), 664-676.
12. Varzaneh, Z. A., & Rafsanjani, M. K. (2021). Intrusion detection system using a new fuzzy rule-based classification system based on genetic algorithm. Intelligent Decision Technologies, 15(2), 231-237.