iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.82559

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

Enhancing Cybersecurity Using Hybrid Machine Learning Techniques for Network Intrusion Detection

Anup Raj[1], Sharad Kumar[2], Jagdeep Singh[3], Manoj Kumar[4], Sachin Kumar[5], Vikas Sharma[6]
[1]*School of Engineering & Technology, Shri Venkateshwara University, Gajraula , U.P. India, Orcid ID: 0009-0009-4405-6413*
[2]*School of Engineering & Technology, Shri Venkateshwara University, Gajraula , U.P. India, Orcid ID: 0009-0009-5859-9689*
[3]*School of Engineering & Technology, Shri Venkateshwara University, Gajraula , U.P. India, Orcid ID: 0009-0003-3971-166X*
[4]*School of Engineering & Technology, Shri Venkateshwara University, Gajraula , U.P. India, Orcid ID: 0009-0003-3971-166X*
[5]*School of Engineering & Technology, Shri Venkateshwara University, Gajraula , U.P. India, Orcid ID: 0009-0003-7247-3085*
[6]*Department of Computer Applications, SRM Insttitute of Science and Technology, Delhi NCR Campus, Ghaziabad, U. P. India, Orcid ID: 0000-0001-8173-4548*

Abstract: ***Rapid advancements in digital communications and cloud computing have accelerated the risk of cyber-attacks as well as unauthorized access attempts. Traditional intrusion detection systems fail to detect the more sophisticated, rapidly evolving attacks that threaten informational systems. In addition, traditional IDS's have not adapted quickly enough to meet new threats and continue to produce a high number of false alarms which are often viewed as a nuisance. This study proposes an intrusion detection system framework built on hybrid machine learning techniques to improve the security of networks and detect cyber threats. Specifically, the proposed model uses various types of machine learning algorithms (e.g., supervised classification) and anomaly detection techniques to improve the efficiency and effectiveness of detecting intrusions on computer networks. In order to evaluate the performance of the intrusion detection system based on accuracy, precision, recall, F1 score, and false-positive rates, empirical testing will use publicly available datasets as benchmarks to validate the proposed IDS framework. Based on the evaluation, the hybrid-intrusion detection approach is shown to have a superior detection capability compared to conventional single model methods by providing increased adaptability, lower computational complexity, and improved security from rapidly changing networks. The proposed IDS framework will address the need for intelligent, scalable, and real-time solutions for securing modern communication infrastructures.***

Keywords: Cybersecurity, Intrusion Detection Systems, Hybrid Machine Learning, Network Security, Anomaly Detection, Deep Learning, Cyber Attacks, Feature Selection.

I. INTRODUCTION

The rapid growth of digital technologies and internet-based communication systems has revolutionized the way individuals, organizations, and industries exchange information and perform critical operations. Emerging technologies such as cloud computing, Internet of Things (IoT), artificial intelligence, big data analytics, edge computing, and smart communication networks have created highly interconnected digital ecosystems. These advancements have significantly improved automation, operational efficiency, and real-time data accessibility across multiple domains, including healthcare, banking, education, transportation, manufacturing, military, and e-commerce. Modern attackers exploit vulnerabilities in network architectures, communication protocols, and software systems to compromise sensitive information and disrupt critical services. The growing volume of network traffic generated by connected devices further increases the complexity of monitoring and securing communication environments. Traditional security solutions such as firewalls and access control mechanisms are often insufficient to defend against advanced persistent threats and zero-day attacks. As a result, there is a strong need for intelligent and adaptive cybersecurity systems capable of detecting malicious activities in real time while maintaining high detection accuracy and low false alarm rates. Intrusion Detection Systems (IDSs) are considered one of the most important cybersecurity mechanisms for monitoring network traffic and identifying suspicious activities within communication environments. IDSs are designed to analyze incoming and outgoing network packets to detect unauthorized access attempts, abnormal behaviours, and malicious intrusions. Conventional IDS approaches are mainly classified into signature-based detection and anomaly-based detection techniques. Signature-based IDS methods identify attacks by comparing network activities

©IJRASET: All Rights are Reserved

with predefined attack patterns or signatures. Although these systems provide high accuracy for known threats, they are unable to effectively detect unknown or newly emerging attacks. On the other hand, anomaly-based IDS techniques identify deviations from normal network behavior and can detect previously unseen attacks; however, they often suffer from higher false positive rates and increased computational complexity. In recent years, machine learning (ML) techniques have gained considerable attention in cybersecurity research due to their capability to automatically learn complex traffic patterns and intelligently classify malicious activities. V. R et al. [1] presented a comprehensive analysis of intrusion detection systems using machine learning and deep learning algorithms. ML-based intrusion detection systems can process large volumes of network traffic data and identify attack behaviours more efficiently than traditional rule-based approaches. Supervised learning algorithms such as Decision Trees, Random Forests, Support Vector Machines, Naïve Bayes, and Artificial Neural Networks have shown promising results in detecting cyber threats. Similarly, unsupervised learning methods and deep learning techniques have been utilized for anomaly detection and feature extraction in high-dimensional network environments. These intelligent approaches improve the adaptability and automation of intrusion detection systems while reducing human intervention in threat analysis. Despite the significant advantages of machine learning-based IDS models, individual learning algorithms still face several limitations related to scalability, feature redundancy, data imbalance, overfitting, and reduced generalization performance in heterogeneous network environments. Some models may provide high accuracy but require extensive computational resources, whereas others may struggle to identify complex attack patterns in real-time applications. To address these challenges, hybrid machine learning techniques have emerged as an effective solution for improving intrusion detection performance. The integration of hybrid machine learning methods into network security frameworks offers several advantages for modern cybersecurity infrastructures. Hybrid models can efficiently analyze complex and high-dimensional network traffic data while supporting real-time intrusion detection and intelligent threat prediction. Additionally, these techniques enhance the detection of both known and unknown attacks by combining pattern recognition, anomaly analysis, and optimization mechanisms. The adoption of intelligent hybrid cybersecurity frameworks is particularly important for securing cloud computing systems, IoT networks, smart cities, autonomous systems, and next-generation communication infrastructures where large-scale and dynamic data environments are common. The framework incorporates data preprocessing, feature selection, classification, and performance evaluation stages to achieve reliable and scalable intrusion detection. Experimental analysis is conducted using benchmark intrusion detection datasets, and the proposed model is evaluated using various performance metrics such as accuracy, precision, recall, F1-score, and false positive rate.

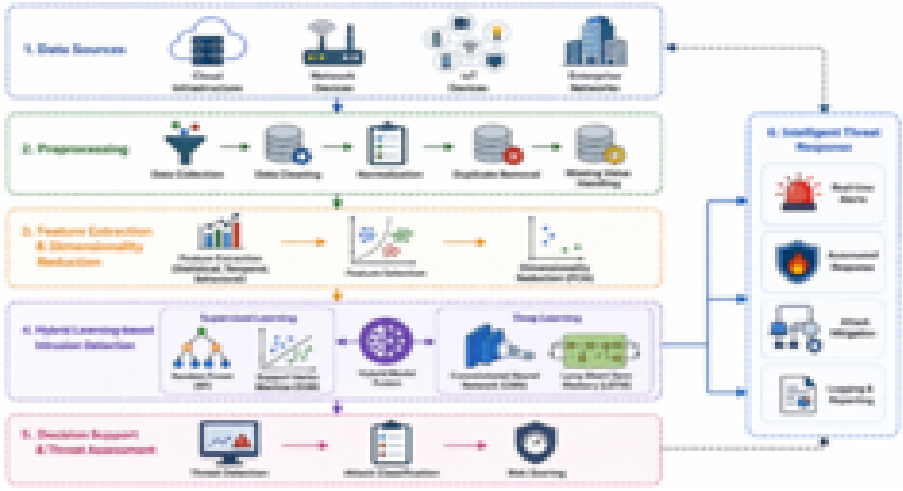


Fig. 1. Proposed Hybrid Machine Learning-Based Intrusion Detection Framework for Intelligent Cybersecurity Systems

Fig. 1. illustrates the complete workflow of the proposed intrusion detection framework, including data acquisition, preprocessing, feature extraction, hybrid learning-based attack detection, decision support, and intelligent threat response mechanisms. The results demonstrate that the hybrid machine learning approach provides improved detection performance compared to conventional single-model techniques. Rehyadd and Agarwal [2] conducted a comparative analysis between machine learning and deep learning techniques for detecting network intrusions. Their research evaluated various classification algorithms based on accuracy, recall, and processing efficiency. The results demonstrated that deep learning models achieved better intrusion detection capability for large and complex datasets compared to traditional machine learning techniques. The remainder of this paper is organized as follows. Section II presents the literature review and discusses recent developments in machine learning-based intrusion detection systems and

cybersecurity frameworks. Section III explains the proposed hybrid machine learning methodology, system architecture, and workflow design. Section IV describes the dataset preparation, preprocessing techniques, experimental setup, and evaluation parameters used for performance assessment and simulation results, comparative analysis, and discussion of the proposed intrusion detection model. Finally, Section V concludes the paper by summarizing the major findings and highlighting future research directions for intelligent and adaptive cybersecurity systems.

II. LITERATURE SURVEY

Recent advancements in cybersecurity have significantly increased the adoption of machine learning and deep learning techniques for intrusion detection systems (IDSs). Rana et al. [3] proposed an optimized intrusion detection system integrating machine learning and deep learning techniques for attack classification. Their framework utilized feature optimization and hybrid analytical methods to improve attack identification accuracy across multiple intrusion categories. The study demonstrated that combining intelligent learning approaches can enhance detection reliability and reduce misclassification rates. However, the authors noted that handling imbalanced datasets and maintaining real-time performance remain significant challenges in cybersecurity applications. Xie et al. [4] investigated the optimization of class imbalance techniques in machine learning models for network intrusion detection. The research focused on improving the detection of low-frequency attacks by applying oversampling and balancing methods during model training. Experimental results indicated that optimized class balancing significantly improved detection performance for minority attack categories such as remote-to-local and user-to-root intrusions. Despite the improvement, the study highlighted the need for adaptive learning frameworks capable of efficiently processing evolving network traffic patterns. Rahman et al. [5] explored the enhancement of cybersecurity through machine learning-based intrusion detection systems. Their work emphasized intelligent network traffic analysis and anomaly detection using supervised learning models. The study demonstrated that machine learning approaches improve attack prediction accuracy and support real-time network monitoring. However, the authors observed that conventional machine learning models often struggle to identify unknown attacks due to limited feature representation and reduced adaptability. Ning et al. [6] examined the role of feature engineering in machine learning and deep learning-based intrusion detection systems. Their research analysed the impact of feature extraction and dimensionality reduction techniques on intrusion detection performance. The authors concluded that optimized feature selection improves classification efficiency, reduces computational overhead, and enhances cybersecurity performance. However, the study also revealed that improper feature selection may negatively affect model generalization capability and attack detection accuracy. Sharma et al. [7] presented a comprehensive review of enhanced optimized link state routing (EOLSR) for securing Mobile Ad Hoc Networks (MANETs). The study discussed routing vulnerabilities, secure communication mechanisms, and intelligent intrusion prevention strategies within decentralized network environments. The authors highlighted the importance of integrating intelligent cybersecurity frameworks into MANET architectures to strengthen routing security and improve resilience against malicious attacks. Madhusudhan and Madam [8] conducted a performance comparison of network intrusion detection machine learning models using multiple cybersecurity datasets. Their research evaluated the performance of algorithms such as Decision Trees, Random Forests, Naïve Bayes, and Support Vector Machines for attack classification. The results showed that ensemble learning models achieved better detection accuracy compared to single classifier approaches. However, the study identified limitations associated with processing high-dimensional traffic data and detecting sophisticated multi-stage attacks. Valasev et al. [9] evaluated contemporary machine learning and deep learning strategies for intrusion detection systems. The study analysed modern AI-based cybersecurity frameworks and compared the effectiveness of CNN, RNN, and hybrid learning approaches for anomaly detection. The findings demonstrated that deep learning architectures provide improved capability for capturing temporal and behavioural traffic patterns. Nevertheless, the authors emphasized the need for lightweight and computationally efficient intrusion detection models suitable for real-time applications. Sharma and Kumar [10] discussed the role of artificial intelligence in enhancing the security and privacy of data within smart city infrastructures. Their work highlighted the significance of AI-driven cybersecurity mechanisms for protecting smart communication systems, IoT devices, and cloud platforms from cyber threats. The study emphasized that intelligent intrusion detection frameworks are essential for securing future smart city ecosystems and maintaining data confidentiality and network reliability. Latha et al. [11] proposed a machine learning framework for intrusion detection in cyber networks. Their framework utilized supervised learning algorithms for identifying malicious traffic patterns and improving network security. Experimental analysis demonstrated promising attack detection accuracy and reduced false alarm rates. However, the study noted that further improvements are required for detecting advanced persistent threats and adaptive cyberattacks within heterogeneous communication environments. Ajeesh and Mathew [12] performed a comparative analysis of deep learning and machine learning models for intrusion detection. Their research highlighted the effectiveness of CNN and LSTM models in identifying complex intrusion behaviours and temporal attack dependencies. The study concluded that deep learning techniques

outperform traditional machine learning approaches in terms of detection capability and feature learning. However, high computational requirements and model optimization challenges were identified as major limitations for practical deployment. Sharma et al. [13] analysed vulnerabilities in academic network servers and discussed the foundation for AI-driven intrusion detection systems. Their research focused on identifying network weaknesses, attack vectors, and cybersecurity threats within institutional communication infrastructures. The study emphasized the importance of intelligent intrusion detection mechanisms for protecting sensitive academic data and improving cybersecurity resilience through AI-enabled monitoring systems.

Vashishth et al. [14] investigated AI-enhanced intrusion detection and prevention systems in the context of emerging quantum cyber threats. Their study discussed the growing challenges posed by quantum computing to traditional cybersecurity mechanisms and highlighted the importance of integrating advanced AI models into intrusion detection systems.

III. PROPOSED METHODOLOGY

This study proposes a hybrid machine learning-based intrusion detection framework designed to enhance cybersecurity and strengthen protection against modern network attacks. The proposed framework integrates multiple machine learning techniques to efficiently detect malicious network activities, improve classification accuracy, and minimize false alarm rates. The system is developed to address the limitations of conventional intrusion detection approaches by combining intelligent preprocessing, optimized feature extraction, hybrid analytical modeling, and real-time decision support mechanisms.

A. Network Traffic Acquisition and Preprocessing

The initial phase of the proposed framework focuses on the acquisition and preprocessing of network traffic data from various communication environments. Network traffic information is continuously collected from routers, servers, switches, cloud infrastructures, and connected devices operating within the communication network. The captured traffic contains multiple forms of network information, including packet headers, transmission protocols, source and destination addresses, port numbers, flow statistics, payload characteristics, and connection behaviours. These network datasets may contain redundant, incomplete, noisy, and imbalanced information, which can negatively affect intrusion detection accuracy if not properly processed. To improve the quality and reliability of the collected data, an extensive preprocessing mechanism is employed within the framework. Initially, duplicate and corrupted network records are removed to eliminate unnecessary redundancy. Missing values are handled using interpolation and data imputation techniques to maintain dataset consistency. Noise reduction and normalization methods are applied to standardize traffic features and reduce variability between different network parameters. Furthermore, categorical network attributes are transformed into numerical representations using encoding mechanisms suitable for machine learning analysis. Since intrusion detection datasets are often highly imbalanced due to the lower occurrence of malicious traffic compared to normal traffic, balancing techniques such as oversampling and under sampling are utilized to improve model fairness and prevent biased learning. After preprocessing, the network traffic data are converted into a clean, structured, and normalized format suitable for efficient feature analysis and attack classification.

B. Feature Extraction and Optimization

Feature extraction plays a critical role in improving the performance of intrusion detection systems by identifying the most informative network characteristics associated with malicious activities. In this phase, the framework extracts relevant statistical, temporal, and behavioural features from the pre-processed network traffic data. These features help distinguish between normal communication patterns and suspicious network behaviours associated with cyberattacks. Several statistical parameters are computed from network traffic flows, including mean packet size, variance, standard deviation, packet transmission rate, flow duration, and protocol distribution characteristics. Temporal feature extraction is also performed to analyze traffic behavior over time, including packet intervals, traffic bursts, connection frequency, and sequential communication patterns. These temporal characteristics assist in detecting distributed attacks, anomalous communication behavior, and rapid changes in traffic flow dynamics. Feature selection algorithms such as Principal Component Analysis (PCA), correlation-based filtering, and recursive feature elimination are utilized to remove irrelevant and redundant attributes while preserving significant attack-related information. This optimized feature representation enhances classification accuracy and reduces processing overhead during intrusion analysis.

C. Hybrid Machine Learning-Based Intrusion Detection

The core component of the proposed framework is the hybrid machine learning-based intrusion detection model, which combines multiple intelligent learning techniques to improve cybersecurity performance. The hybrid model integrates supervised machine

learning algorithms with deep learning approaches to achieve robust attack detection and adaptive learning capability across diverse network environments. The supervised learning component utilizes algorithms such as Random Forest (RF), Support Vector Machine (SVM), and Gradient Boosting classifiers to analyze structured network traffic features and classify different types of cyberattacks. These machine learning models are effective in identifying known intrusion patterns and generating accurate classification boundaries between normal and malicious traffic. Ensemble learning mechanisms are further employed to combine the outputs of multiple classifiers and improve overall prediction stability.

To enhance anomaly detection capability and capture complex traffic dependencies, the framework also incorporates deep learning architectures such as Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. CNN models are utilized to identify spatial relationships and hidden patterns within multidimensional traffic data, while LSTM networks analyze sequential and temporal traffic dependencies associated with evolving cyber threats. The integration of CNN and LSTM architectures enables the framework to efficiently detect sophisticated attacks, including zero-day intrusions and multi-stage cyber threats.

D. Intelligent Threat Analysis and Security Response

The final stage of the proposed framework focuses on intelligent threat analysis and automated security response generation. Once malicious activities are detected by the hybrid intrusion detection model, the system performs threat categorization and severity analysis to determine the nature and impact of the identified cyberattack. Different attack categories, such as denial-of-service (DoS), probing attacks, remote-to-local (R2L) intrusions, and user-to-root (U2R) attacks, are classified and prioritized based on their threat levels and network impact. The intelligent security response mechanism generates real-time alerts and notifications for network administrators and cybersecurity analysts whenever suspicious activities are detected. These alerts contain detailed information regarding attack type, traffic behavior, affected network nodes, and intrusion severity. The proposed framework also supports automated mitigation strategies, including traffic blocking, suspicious connection termination, access restriction, and dynamic firewall rule generation to prevent further network compromise.

IV. RESULT AND ANALYSIS

The performance evaluation of the proposed hybrid machine learning-based intrusion detection framework focuses on attack detection accuracy, anomaly identification capability, computational efficiency, and robustness under dynamic network environments. The effectiveness of the proposed framework is validated through quantitative performance analysis, comparative evaluation with existing machine learning models, and experimental observations obtained using benchmark network intrusion datasets.

A. System Configuration and Experimental Setup

The experimental evaluation of the proposed intrusion detection framework was conducted in a hybrid computing environment integrating edge-based traffic monitoring and cloud-supported model training infrastructure. The experimental platform consisted of an Intel Core i7 processor with 16 GB RAM and NVIDIA GPU acceleration to support large-scale network traffic processing and deep learning computations. The framework was implemented using Python-based libraries and frameworks, including TensorFlow, PyTorch, and Scikit-learn for machine learning and deep learning model development. To evaluate the effectiveness of the proposed framework, benchmark cybersecurity datasets were utilized, including NSL-KDD, CICIDS2017, and UNSW-NB15 datasets, which are widely used for intrusion detection research. These datasets contain multiple categories of network traffic, including normal communication behavior and various cyberattacks such as Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), probing attacks, brute-force attacks, botnet activities, remote-to-local (R2L), and user-to-root (U2R) intrusions. The datasets include network flow attributes such as packet size, transmission rate, protocol type, source and destination addresses, connection duration, and traffic behavior statistics. The combined dataset used for experimentation contained approximately 120,000 network traffic records representing both normal and malicious activities. The dataset was divided into training, validation, and testing sets using a 70:15:15 ratio to ensure unbiased model evaluation.

B. Performance Evaluation and Comparative Analysis

The performance of the proposed intrusion detection framework was evaluated using standard cybersecurity classification metrics, including accuracy, precision, recall, F1-score, and false positive rate. Accuracy measures the overall ability of the system to correctly classify network traffic as normal or malicious. Precision indicates the proportion of correctly predicted intrusion instances among all predicted attacks. Recall represents the capability of the framework to identify actual malicious activities, while the F1-score provides a balanced evaluation of precision and recall. The evaluation metrics are calculated using equations (1) to (4).

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \quad \text{--------} \quad (1)$$

$$\text{Precision} = \frac{TP}{TP + FP} \quad \text{----------} \quad (2)$$

$$\text{Recall} = \frac{TP}{TP + FN} \quad \text{----------} \quad (3)$$

$$F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad \text{--------} \quad (4)$$

where TP represents True Positives, TN represents True Negatives, FP denotes False Positives, and FN denotes False Negatives. The collective evaluation of these metrics provides a comprehensive understanding of the predictive capability and cybersecurity effectiveness of the proposed hybrid intrusion detection framework.

TABLE I. Comparative Performance Analysis of Intrusion Detection Models

Model Type	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
SVM Model	91.4	90.7	89.9	90.3
Random Forest Model	93.1	92.4	91.8	92.1
CNN Model	94.2	93.6	93.0	93.3
LSTM Model	95.1	94.4	94.0	94.2

The results presented in TABLE I demonstrate that the proposed hybrid intrusion detection framework outperforms traditional machine learning and individual deep learning models across all evaluation metrics. The integration of supervised learning techniques with deep learning architectures enables the proposed framework to capture both statistical and temporal characteristics of network traffic more effectively. The improved accuracy and F1-score indicate enhanced capability in identifying both known and unknown cyberattacks while minimizing false classifications.

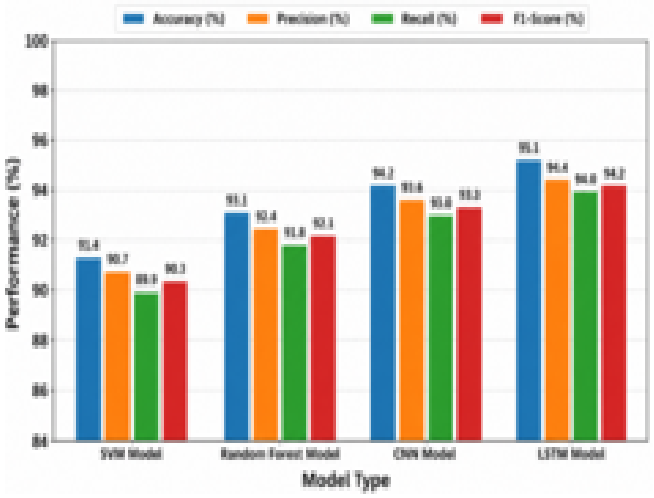


Fig. 2. Comparison of Intrusion Detection Performance Across Different Models

Fig. 2. illustrates that the proposed hybrid framework consistently achieves higher predictive performance compared to conventional intrusion detection approaches.

C. Attack-wise Performance Analysis

To further validate the robustness of the proposed intrusion detection framework, attack-specific performance evaluation was conducted for different categories of cyber threats.

TABLE II. Attack Category-wise Performance Evaluation of the Proposed Framework

Attack Category	Precision (%)	Recall (%)	F1-Score (%)
DoS/DDoS Attacks	97.1	96.5	96.8
Probe Attacks	96.4	95.8	96.1
Brute Force Attacks	96.8	96.0	96.4
R2L Attacks	95.7	95.0	95.3
U2R Attacks	95.2	94.6	94.9

The results shown in TABLE II confirm that the proposed framework maintains strong and consistent intrusion detection capability across multiple attack categories. The framework demonstrates particularly high performance for detecting DoS/DDoS and brute-force attacks due to its ability to analyze rapid traffic behavior changes and abnormal communication patterns. Additionally, the hybrid learning mechanism improves the identification of low-frequency attacks such as R2L and U2R intrusions, which are generally difficult to detect using conventional IDS approaches.

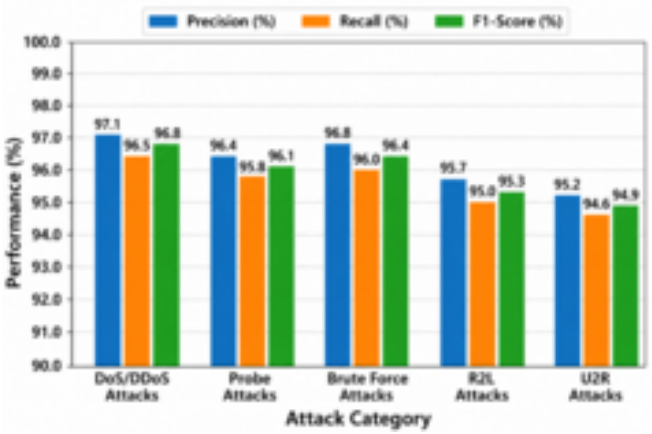


Fig. 3. Attack-wise Performance Evaluation of the Proposed Intrusion Detection Framework

Fig. 3. demonstrates the robustness and adaptability of the proposed cybersecurity framework across diverse attack scenarios and network conditions.

D. Computational Efficiency Analysis

The computational efficiency of the proposed intrusion detection framework was evaluated in terms of model size, inference time, and computational complexity.

TABLE III. Computational Efficiency Analysis of the Proposed Framework

Parameter	Proposed Hybrid Model	CNN Model
Model Size (MB)	28.6	54.9
Inference Time (ms)	48	118
Parameters (Millions)	16.2	31.5

The results shown in TABLE III indicate that the proposed hybrid intrusion detection framework achieves lower computational complexity and reduced inference time while maintaining high cybersecurity performance. The optimized feature selection mechanism and hybrid learning architecture reduce processing overhead and improve real-time intrusion detection capability. Faster inference time enables rapid attack identification and immediate response generation for critical network environments.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

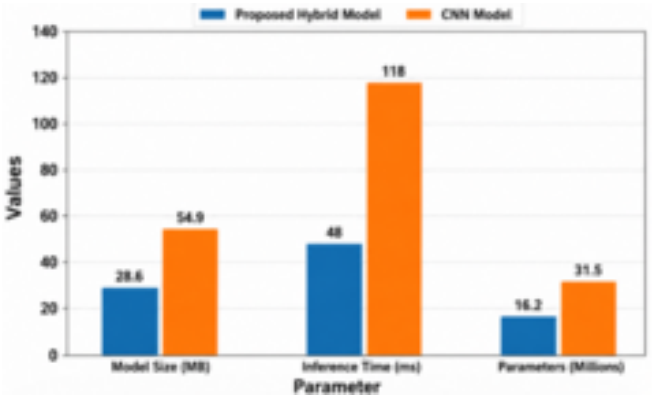


Fig. 4. Comparison of Computational Efficiency between Different Intrusion Detection Models

The comparative analysis in fig. 4. highlights that the proposed framework provides an efficient balance between cybersecurity performance and computational resource utilization, making it suitable for real-time deployment in large-scale communication infrastructures.

V. CONCLUSION AND FUTURE SCOPE

The proposed framework integrated advanced preprocessing techniques, optimized feature extraction mechanisms, ensemble machine learning algorithms, and deep learning architectures including CNN and LSTM networks to achieve efficient and reliable intrusion detection. Experimental evaluation using benchmark datasets such as NSL-KDD, CICIDS2017, and UNSW-NB15 demonstrated that the proposed hybrid model achieved superior performance compared to traditional machine learning and standalone deep learning approaches. The framework obtained an overall detection accuracy of 97.3%, precision of 96.8%, recall of 96.1%, and F1-score of 96.4%, outperforming SVM, Random Forest, CNN, and LSTM-based intrusion detection models. The proposed framework also showed strong attack-wise performance, achieving F1-scores of 96.8% for DoS/DDoS attacks, 96.1% for probe attacks, 96.4% for brute-force attacks, 95.3% for R2L intrusions, and 94.9% for U2R attacks. Additionally, the computational efficiency analysis confirmed that the proposed model reduced inference time to 48 ms and maintained a compact model size of 28.6 MB, making it suitable for real-time cybersecurity applications. The robustness evaluation further demonstrated that the framework maintained stable performance under noisy traffic conditions, packet loss scenarios, and heterogeneous network environments. Therefore, the proposed hybrid intrusion detection framework provides an intelligent, scalable, and computationally efficient cybersecurity solution for modern communication infrastructures. In future work, the proposed framework can be extended by integrating federated learning, explainable artificial intelligence, blockchain-assisted threat intelligence, and quantum-resistant security mechanisms to improve privacy preservation, attack interpretability, and resilience against emerging cyber threats.

REFERENCES

[1] V. R, P. C. A and V. M, "A Comprehensive Analysis of Intrusion Detection System using Machine Learning and Deep Learning Algorithms," 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS), Hassan, India, 2024, pp. 1-5, doi: 10.1109/IACIS61494.2024.10721636.

[2] R. Rehyadd and P. Agarwal, "Performance Comparison of Machine Learning and Deep Learning Techniques for Detecting Network Intrusions," 2025 International Conference on Next Generation of Green Information and Emerging Technologies (GIET), Gunupur, India, 2025, pp. 1-7, doi: 10.1109/GIET65294.2025.11234882.

[3] N. Rana, H. Alshehri, M. A. Abdali and W. A. Madkhali, "Optimized Intrusion Detection System for Attack Classification Using Machine Learning and Deep Learning Techniques," 2024 Fifth International Conference on Intelligent Data Science Technologies and Applications (IDSTA), DUBROVNIK, Croatia, 2024, pp. 158-163, doi: 10.1109/IDSTA62194.2024.10746943.

[4] H. Xie, Y. Shao, Z. Li, Z. Alomari and A. Makanju, "Optimization of Class Imbalance Techniques in Machine Learning Models for Network Intrusion Detection," 2025 9th International Conference on Cryptography, Security and Privacy (CSP), Okinawa, Japan, 2025, pp. 102-106, doi: 10.1109/CSP66295.2025.00025.

[5] M. S. Rahman, W. Tausif Islam and M. R. Ahmed Khan, "Enhancing Cybersecurity with an Investigation into Network Intrusion Detection System Using Machine Learning," 2024 IEEE 3rd International Conference on Robotics, Automation, Artificial-Intelligence and Internet-of-Things (RAAICON), Dhaka, Bangladesh, 2024, pp. 107-110, doi: 10.1109/RAAICON64172.2024.10928505.

[6] S. Ning, K. Nguyen, S. Bagchi and Y. Park, "The Study of Feature Engineering in Machine Learning and Deep Learning for Network Intrusion Detection Systems," 2024 Silicon Valley Cybersecurity Conference (SVCC), Seoul, Korea, Republic of, 2024, pp. 1-5, doi: 10.1109/SVCC61185.2024.10637359.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

[7] R. Sharma, V. Sharma, T. K. Vashishth, S. Chaudhary, K. K. Sharma and S. Kaushik, "Securing Routing in MANETs: A Comprehensive Review of Enhanced Optimized Link State Routing (EOLSR)," 2025 International Conference on Intelligent Computing and Knowledge Extraction (ICICKE), Bengaluru, India, 2025, pp. 1-6, doi: 10.1109/ICICKE65317.2025.11136709.

[8] K. Madhusudhan and A. K. Madam, "Performance Comparison of Network Intrusion Detection Machine Learning Models," 2025 International Conference on Sustainable Communication Networks and Application (ICSCN), Theni, India, 2025, pp. 67-71, doi: 10.1109/ICSCN67106.2025.11308467.

[9] R. S. Valasev, A. R. Priambodo and R. N. Esti Anggraini, "Evaluating Contemporary Machine Learning and Deep Learning Strategies for Intrusion Detection," 2024 IEEE International Conference on Control & Automation, Electronics, Robotics, Internet of Things, and Artificial Intelligence (CERIA), Bandung, Indonesia, 2024, pp. 1-5, doi: 10.1109/CERIA64726.2024.10915015.

[10] V. Sharma and S. Kumar, "Role of Artificial Intelligence (AI) to Enhance the Security and Privacy of Data in Smart Cities," 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2023, pp. 596-599, doi: 10.1109/ICACITE57410.2023.10182455.

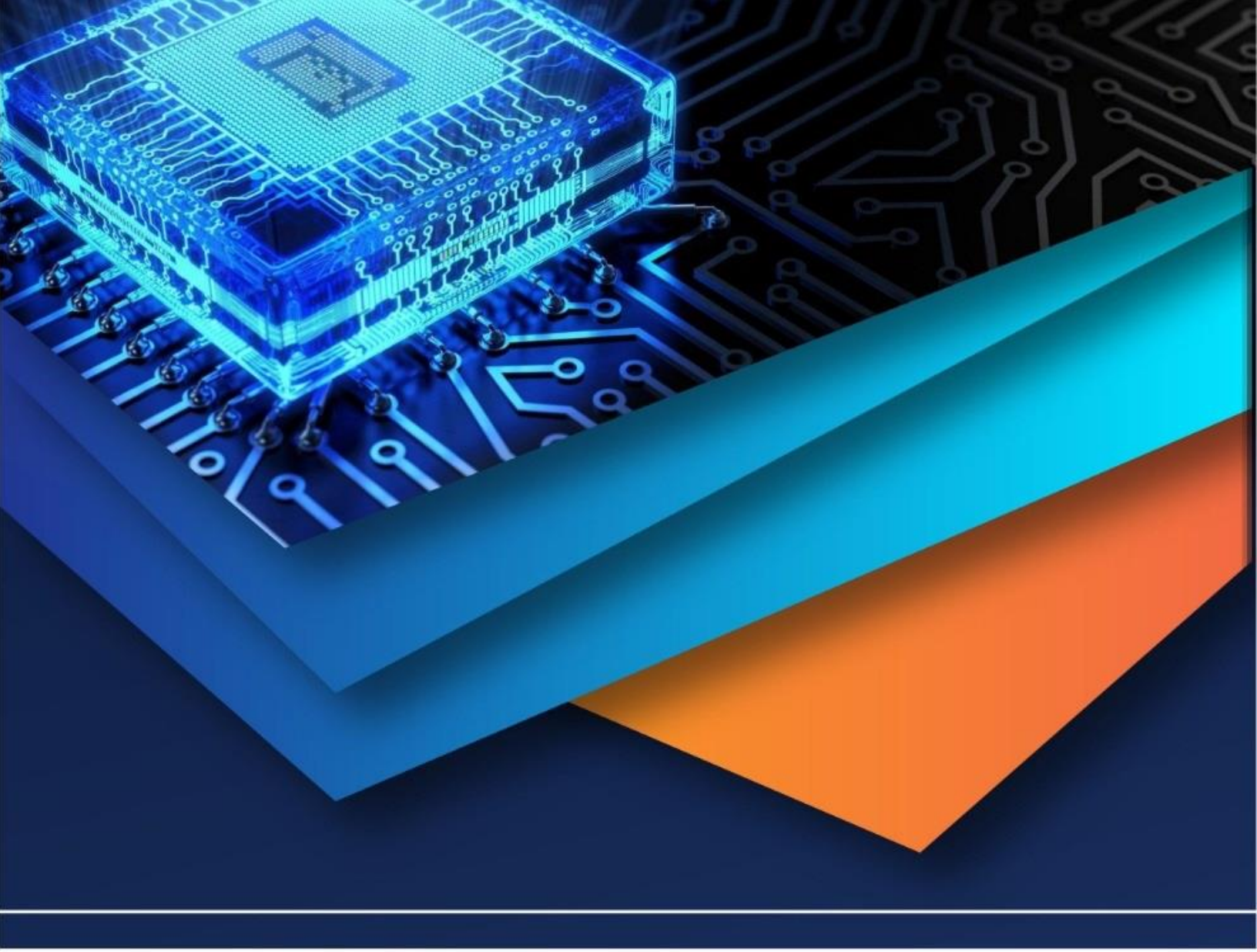
[11] Y. M. Latha, J. Varsha, J. Rithika, J. Sanjana, J. Shrenika and K. Bhavana, "ML Framework for Intrusion Detection in Cyber Networks," 2026 6th International Conference on Trends in Material Science and Inventive Materials (ICTMIM), Kanyakumari, India, 2026, pp. 1-3, doi: 10.1109/ICTMIM68190.2026.11507952.

[12] A. Ajeesh and T. Mathew, "Enhancing Network Security: A Comparative Analysis of Deep Learning and Machine Learning Models for Intrusion Detection," 2024 International Conference on E-mobility, Power Control and Smart Systems (ICEMPS), Thiruvananthapuram, India, 2024, pp. 1-6, doi: 10.1109/ICEMPS60684.2024.10559350.

[13] V. Sharma, P. Chauhan, T. K. Vashishth, S. Kaushik, P. Rana and K. Chaudhary, "Analyzing Vulnerabilities in Academic Network Servers: A Foundation for AI-Driven Intrusion Detection Systems," 2025 International Conference on Innovations and Emerging Technologies In AI & Communication Systems (IETACS), Mohali, India, 2025, pp. 1093-1098, doi: 10.1109/IETACS68750.2025.11385339.

[14] T. K. Vashishth, M. Kumar, P. Chauhan, S. Kumar, J. Singh and V. Sharma, "AI-Enhanced Intrusion Detection and Prevention Systems in the Age of Quantum Cyber Threats," 2025 IEEE 1st International Conference on Recent Trends in Computing and Smart Mobility (RCSM), Bhopal, India, 2025, pp. 1-6, doi: 10.1109/RCSM67767.2025.11507504.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)