iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** X **Month of publication:** October 2026

DOI: https://doi.org/10.22214/ijraset.2026.85265

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 X Oct 2026- Available at www.ijraset.com

Hybrid Machine Learning and XAI Approach for Real-Time Intrusion Detection

Abhishek Kumar[1], Dilip Kumar[2]
[1]*Research Scholar, Department of Computer Science and Engineering, Vishveshwarya Group of Institutions, Dr. A. P. J. Abdul Kalam Technical University, Lucknow, U.P, India*
abhishek7464054801@gmail.com
Orcid Id: 009-0005-8468-3826
[2]*Associate Professor, Department of Computer Science and Engineering, Vishveshwarya Group of Institutions, Dr. A. P. J. Abdul Kalam Technical University, Lucknow, U.P, India*
kumardilip1@gmail.com
Orcid Id: 0009-0001-1756-9397

Abstract: ***The growth of communication technologies and advancement in cloud computing have led to an increase in the possibility of cybercrime and attacks. Traditional IDSs (Intrusion Detection Systems) are ineffective in detecting sophisticated attacks that evolve rapidly and target information systems and therefore do not provide sufficient protection. Moreover, traditional systems are slow to adapt to the appearance of new threats and produce a high number of false alarms which are often considered a nuisance. The proposed study offers an intrusion detection system framework that incorporates the hybrid techniques of machine learning to enhance the security of networks and detect cyber threats. The key aspects of the system are the following: the model uses various machine learning algorithms as well as anomaly detection methods in order to detect intrusions effectively. The effectiveness of the framework in terms of its accuracy, precision, recall, F1 score, and false positive index calculation is measured through conducting empirical testing applying public datasets as references for verification of the effectiveness of the proposed model. The results of the study show that the hybrid intrusion detection system manages to achieve better performance in comparison with conventional solitary models due to its adaptability, low computational complexity and ability to provide security in the context of rapidly evolving networks. The developed intrusion detection system aims to meet the rising demand for intelligent solutions which provide security for modern communication systems.***
Keywords: Intrusion detection systems, Cybersecurity, Hybrid machine learning, Cyber-attacks, Network security, Anomaly detection, Deep learning, Feature selection.

I. INTRODUCTION

Recent years have witnessed an unprecedented rise in the development of digital technologies and new internet-based communication methods that have changed the way people, organizations, and companies communicate with one another and carry out their business activities. The emergence of technologies such as cloud computing, IoT, AI, big data analysis, edge computing, and smart communication networks has resulted in the emergence of interconnected digital ecosystems. Modern threats make use of the vulnerabilities in the design of network systems, protocols of communication, and software to steal confidential data and prevent some operations from taking place. The increase in the volume of traffic produced by the connected devices complicates the monitoring and security of communication systems. Existing technologies such as firewalls and access control sometimes fail to protect from modern cyber threats and zero-day attacks. Accordingly, the need for the development of intelligent and adaptive cybersecurity technologies that will enable to track criminal actions in real time and provide high accuracy and low amounts of false alarms becomes apparent. Intrusion Detection Systems (IDSs) appear to be among the most important cybersecurity technologies that monitor network traffic and identify suspicious actions in communication systems. IDSs gain access to incoming and outgoing packets to identify the attempts to gain access without permission and malicious intrusions. The majority of traditional IDS technologies can be grouped into signature-based and anomaly-based detection methods. While such systems may succeed in identifying known attacks, they fail to recognize new or unknown kinds of attacks quickly. On the other hand, anomaly-based IDS techniques create a model of baseline normal behavior and then look for anything outside that norm, and while they have great potential to detect never seen attacks before, they tend to yield many false positives and involve great processing power.

©IJRASET: All Rights are Reserved

In recent times, ML techniques are being heavily researched in the context of cybersecurity because they offer the possibility of automatic learning of complex traffic patterns and being able to identify malicious activities automatically. As discussed by V. R et al. [1], machine learning approaches in IDS are known for their potential to perform automatic operations in the intrusion detection process. Using various techniques of supervised learning, such as Decision Trees, Random Forests, Support Vector Machines, Naïve Bayes, and Artificial Neural Networks, the IDS can achieve remarkable results in the detection of cyber-attacks. They also show the effectiveness of employing unsupervised learning and deep learning techniques in anomaly detection and feature extraction in high-dimensional traffic environments. The methods allow to significantly enhance the efficiency of IDS in monitoring activities on the network and help to automate the whole threat detection process. To tackle these issues, hybrid machine learning techniques have been developed to enhance the efficiency of intrusion detection systems. The use of hybrid techniques in the area of network security provides multiple benefits for modern-day cyber security setups. The key advantage of hybrid systems is their ability to analyze highly complex and non-linear traffic data while real-time intrusion detection systems work in conjunction for intelligence threat predictions as well. Moreover, hybrid technology methods increase the chances of discovering both known and unknown intrusion attempts through complex combinations of such methods/processes as pattern recognition, anomaly detection, optimization methods, etc. In the world where data environments are always large and dynamic the importance of implementing hybrid intelligent cyber security technologies increases significantly in order to secure not only cloud computing, IoT technologies, and smart cities but also autonomous systems and new-generation telecommunication technologies. The model which is provided in this research consists of the following stages of data preprocessing, data selection, classification, and model's evaluation in order to achieve effective and scalable intrusion detection. The experimental analysis is carried out using benchmark databases, and different performance measures such as accuracy, precision, recall, F1-score, and false positive rate are employed in order to assess the model.

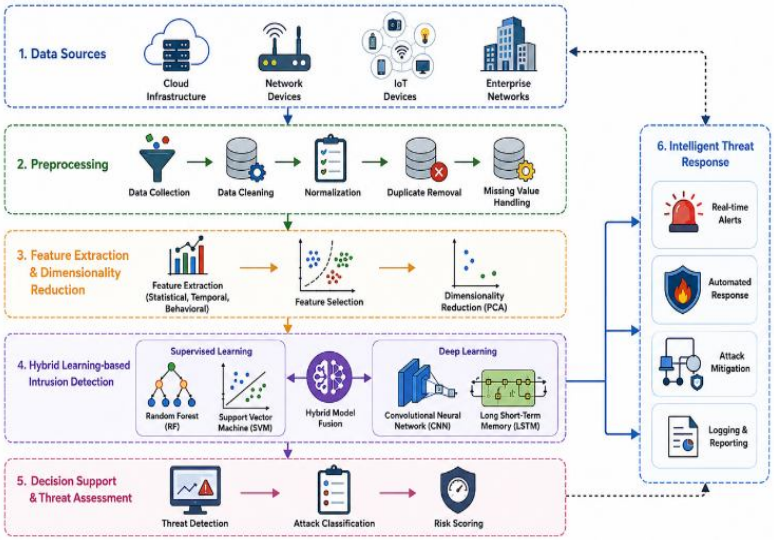


Fig. 1. Proposed Hybrid Machine Learning-Based Intrusion Detection Framework for Intelligent Cybersecurity Systems

Fig. 1. illustrates the complete process of the suggested intrusion detection system including the process of acquisition of the data, the preprocessing of the data, the extraction of features, the use of hybrid learning methods for detecting attacks and the use of decision-making systems and intelligent defense methods. The results showed that the hybrid approaches of the machine learning give better results than the single-model approaches. Rehyadd and Agarwal [2] compared machine learning and deep learning for the detection of network intrusions and measured the effectiveness of different algorithms based on their correctness, recall and efficiency. The results showed that deep learning is a better solution in terms of detecting attacks based on large and complicated data compared to the existing machine learning technologies. The structure of the paper is the following. In section II the literature review is presented with the recent innovations in intrusion detection systems based on machine learning or cybersecurity methods. Section III contains the description of the proposed method including the system architecture and process design. Section IV consists of the preparation of the data sets, the description of the methods of data processing and the section performance assessment based on simulation results, comparison of the results and evaluation of the performance of the developed model and the work finishes with the statement of conclusion and the suggestions for future studies on intelligent and adaptive cybersecurity systems.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue X Oct 2026- Available at www.ijraset.com

II. LITERATURE SURVEY

New developments in the cybersecurity sphere have resulted in extensive utilization of machine learning and deep learning techniques in intrusion detection systems (IDSs). For instance, the study by Rana et al. [3] presented an ICS which combines machine learning and deep learning approaches for attack categorization. The authors developed a framework for solving purpose, which employs feature optimization and hybrid analytical techniques to increase the effectiveness of the attack detection process. The experiment conducted within the study proved that if intelligent learning techniques are combined, this may considerably increase detection accuracy. However, it has also been identified that dealing with unbalanced datasets and assuring real-time performance in cybersecurity is still a crucial problem. In turn, Xie et al. [4] studied optimization of class imbalance methods implementation in machine learning models for IDSs. The study was aimed at finding effective ways to recognize low-frequency attacks through the employment of class balancing and oversampling approach in model training for the purpose of achieving higher detection efficiency. Thus, the experimental results showed significant effectiveness of class balancing when detecting the minority class types of attacks such as remote-to-local and user-to-root cyber-attacks. However, the research was focused on the establishment of adaptive learning models that would cope with the problem of achieving utilization of efficient class balancing methods. Finally, another research conducted by Rahman et al. [5] focused on the possibility to enhance cybersecurity through the implementation of intrusion detection models based on machine learning techniques. The main attention was paid to intelligent analysis of network traffic and anomaly detection using supervised learning approaches in the course of the research. The results of the study showed that machine learning techniques can be a solution for improving attack detection accuracy and providing real-time monitoring of the network. However, the authors also mentioned that traditional machine learning models have serious limitations when it comes to detection of unknown attacks. Ning et al. [6] studied the importance of feature engineering in machine learning and deep learning-based intrusion detection systems. The research was dedicated to the study of the influence of feature extraction and dimensionality reduction methods on intrusion detection. The authors concluded that effective feature selection leads to the better classification efficiency and less computational overhead. Nevertheless, it was also mentioned in the research that poor feature selection may have adverse effects on model generalization capability and attack detection accuracy. Sharma et al. [7] offered an overview of the enhanced optimized link state routing (EOLSR) in order to secure Mobile Ad Hoc Networks (MANETs). The article discussed routing weaknesses, mechanisms for secure communication, and methods for preventing intrusion in decentralized networks. The authors pointed out the importance of putting into practice the intelligent cybersecurity techniques within MANET networks to ensure the safety of routing and security against attacks. The research conducted by Madhusudhan and Madam [8] took a look at different network intrusion detection machine learning systems from the view of performance evaluation using different cybersecurity datasets. Specifically, the authors presented the findings of such algorithms as Decision Trees, Random Forests, Naïve Bayes, and Support Vector Machines in the field of attack classification. The results revealed the fact that the algorithm of ensemble learning provides better detection accuracy than the algorithm of single classifier. There were also noted the challenges faced when dealing with the high-dimensional traffic data to detect sophisticated attacks. Valasev et al. [9] analyzed modern machine learning and deep learning solutions for intrusion detection systems. Sharma and Kumar [10] have explored the role of artificial intelligence in improving the security and privacy of data in smart city networks. Their research demonstrated the importance of cybersecurity technologies based on artificial intelligence for safeguarding the smart communication systems, Internet of Things devices, and cloud computing platforms from cyber assaults. The article states that proper intelligent intrusion detection systems are required to prevent all the attacks in upcoming smart cities and to keep the transferred data safe from any unauthorized access. Latha et al. [11] have devised a scheme of intrusion detection for cyber networks using machine learning. The algorithm they implemented utilized supervised algorithms in order to detect malicious patterns in data traffic. Ajeesh and Mathew [12] carried out a comparative study of deep learning and machine learning techniques utilized for intrusion detection. Their research emphasized the success of keeping track of intricate intrusion patterns and timing of conflictual strikes that emerged from the use of convolutional neural networks and long short-term memory. The latter method was recognized as more efficient as far as features learning and detection capabilities are concerned. At the same time, high dependence on computing resources and difficulty of model development were identified as significant disadvantages. Sharma et al. [13] uncovered the weaknesses of academia-connected systems and made an examination on grounds for artificial intelligence-based intrusion detection systems. Their research demonstrated the ability of intruders to identify weaknesses in networks, paths of attacks, and means of cyber security in institutional networks communications. Vashishth et al. [14] have studied the issues of intrusion detection and prevention systems improved through artificial intelligence in terms of the appearance of quantum threats.

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

III. PROPOSED METHODOLOGY

This research paper proposes a machine learning-based intrusion detection framework that serves to strengthen cybersecurity and enhance mitigation of modern network attacks. This framework combines several methods from the machine learning field for effective identification of malicious activities on networks, high classification accuracy, and decreased false alarm rate. The system is designed to overcome the limitations of traditional intrusion detection systems, as it utilizes intelligent preprocessing, feature extraction, hybrid analytical modeling, and real-time decision-making.

A. Network Traffic Acquisition and Preprocessing

The preliminary step of the recommended framework centers around gathering and processing network traffic data from multiple communication contexts. Network traffic attributes are perpetually collected from servers, routers, switches, cloud systems, and devices connected to the communication network. The traffic contains a number of forms of network traits such as the header of the packet, protocols of transmission, addresses of source and destination, numbers of ports, statistics of flow, characteristics of the payload, and activities of connection. Network traffic datasets may possess redundant, incomplete, noisy, and unbalanced data that may compromise the effectiveness of intrusion detection if not processed effectively. To establish the accuracy and reliability of the processed data, a thorough preprocessing technique will be applied in the framework. The first thing that is done is the exclusion of duplicate and corrupted data of the network from the record to eliminate the unnecessary redundancy. Missing values are dealt with by employing data imputation methods and interpolation procedures to ensure the consistency of datasets. Techniques of reduction of noise and normalization of data are utilized for ensuring the standardization of traffic parameters and reduction of variety of parameters of network. Moreover, categorical traits of networks are turned into the numerical format by using appropriate encoding methods for analysis in terms of machine learning. Considering that the datasets connected to intrusion detection are always characterized by high imbalance due to limited quantity of the crimes, methods of balancing, i.e. oversampling and under sampling will be implemented for suitable correction of bias of the model.

B. Feature Extraction and Optimization

Feature extraction is an important step in improving the overall performance of the intrusion detection systems by identifying the significant network characteristics related to malicious activities. This phase takes relevant statistical, temporal, and behavioural characteristics from the non-processed network traffic data for this model. These features serve to differentiate between normal communication patterns and suspicious network behaviours revealing an opportunity for a cyber-attack. Several statistical parameters are computed from the network traffic flows, such as mean packet size, variance, standard deviation, packet transmission rate, flow duration, and protocol distribution characteristics. Temporal feature extraction considers events or tendencies that exist over a time period concerning actual packet intervals, bursts of traffic, connection frequency, and sequence of communications. These features allow one to identify distributed attacks, anomalous communication behaviours, and sharp variation in the dynamics of traffic flow. Feature selection is carried out by principal component analysis, a correlation-based filter method, and recursive feature elimination just to eliminate the irrelevant and redundant attributes and retain any significant information related to attacks. This optimal representation-of-features typically improves the classification accuracy and minimizes the analysis overhead.

C. Hybrid Machine Learning-Based Intrusion Detection

The central aspect of the introduced methodology is the hybrid intrusion detection framework built on machine learning technology, which merges a range of intelligent learning method in order to enhance cybersecurity functioning. The hybrid method comprises supervised machine learning methods and deep learning technologies in order to achieve effective attacks detection and ability to adapt learning in various network environments. Within the supervised element machine learning techniques like Random Forest (RF), Support Vector Machine (SVM) and Gradient Boosting classifiers are applied to analyze well-structured network traffic characteristics and classify types of cyber-attacks. Such machine learning technologies can contribute to the realization of particular types of cyber intrusions and construction of precise classification boundaries between normal and abnormal traffic. Besides that, methods of ensemble learning can be combined with machine learning techniques output in order to receive more stable prediction. In addition to that, the framework is supplemented with various deep learning technologies including Convolutional Neural Networks (CNN) and Long Short-Time Memory (LSTM) networks for the sake of enhancement of its anomaly detection potential as well as involvement of complex dependencies of network traffic. CNN are applied to detect hidden features and explore dependency between different traffic indicators in three-dimensional traffic information while LSTM networks are used for the analysis of the temporal dependencies of the developed cyber-attacks.

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

D. Intelligent Threat Analysis and Security Response

The last stage of the proposed framework deals with advanced threat analysis and automatic generation of security responses. After intrusion detection performed by the hybrid intrusion detection system, the system categorizes threats and estimates their severity. Intrusions are classified as denial of service, probing, R2L, and U2R attacks and assigned the respective threat categories according to their risk and impact on the network. Through the intelligent security response system, alerts and notifications are generated in real time whenever suspicious activity is detected on the network. Alerts indicate the type of attack, traffic pattern, affected nodes, and the level of intrusions. The framework operates with different mitigation techniques including blocking of traffic, terminating suspicious sessions, limiting access rights, and generating dynamic firewall rules.

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 proposed intrusion detection framework was evaluated experimentally in a hybrid computing environment utilizing edge-based traffic monitoring and cloud assisted model training infrastructure. The experimental platform consisted of an Intel Core i7 processor, 16 GB RAM, accompanied by NVIDIA GPU for support in large-scale processing tasks of network traffic and deep learning computations. The whole framework was developed using Python libraries and frameworks including TensorFlow, PyTorch, and Scikit-learn for machine-learning and deep-learning model development. As benchmarks, widely used datasets in intrusion detection research, including NSL-KDD, CICIDS2017, and UNSW-NB15 were utilized to evaluate the effectiveness of the proposed framework. The datasets present a variety of types of network traffic inclusive of natural communication behaviours and distinct types of cyber-attacks; including denial-of-service (DoS), distributed denial-of-service (DDoS), probe and brute-force attacks, botnet activities, remote-to-local (R2L), and user-to-user (U2R) intrusions. The datasets include network-flow attributes such as packet-size, transmission-rate, protocol-type, source and destination address. duration of connection, and traffics-behavior statistics. The dataset to be used during the experimentation consisted in an aggregated manner of around 120,000 network traffic records representing normal activities and malicious ones. The dataset was segmented into training, validation, and testing using a 70:15:15 ratio for 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).

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

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

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

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

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.

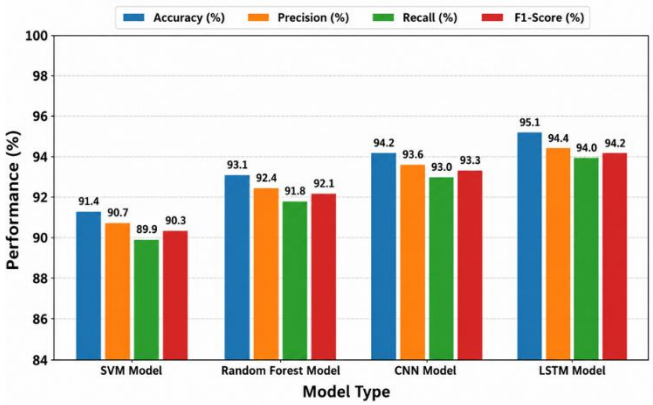


Fig. 2. Comparison of Intrusion Detection Performance Across Different Models

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.

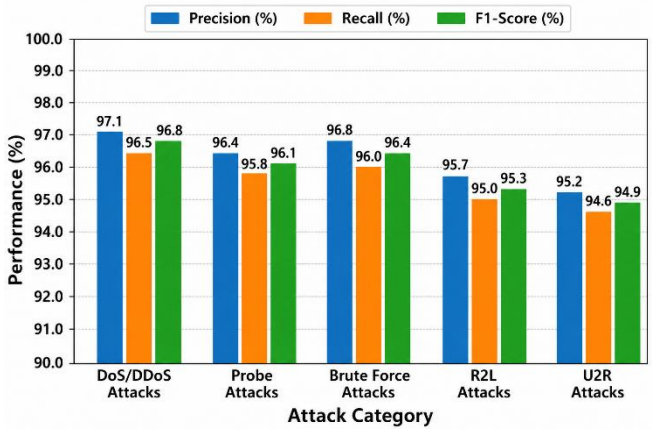


Fig. 3. Attack-wise Performance Evaluation of the Proposed Intrusion Detection Framework

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.

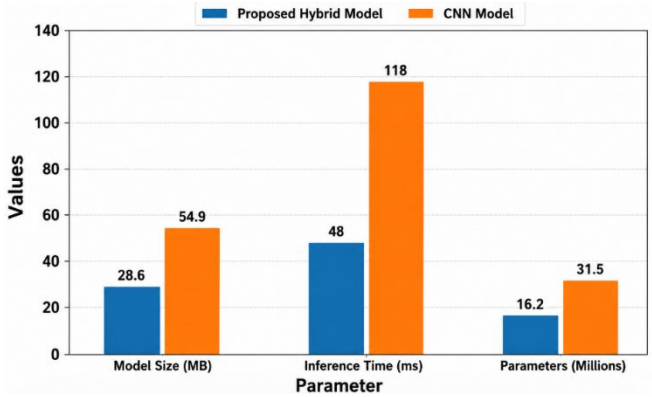


Fig. 4. Comparison of Computational Efficiency between Different Intrusion Detection Models

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 outlined system is characterized by the combination of advanced preprocessing techniques, the most efficient methods for extracting meaningful features, ensemble machine learning algorithms, and deep learning approaches like CNN and LSTM platforms to establish effective and reliable detection of breaches. As per the experiment evaluation conducted on the benchmark datasets taking NSL-KDD, CICIDS2017, and UNSW-NB15 as references, it was discovered that the hybrid approach operates much better than conventional machines as well as independent deep learning techniques. The detection rate achieved by the hybrid system is noted to be equal to 97.30%, precision of 96.80%, and recall rate of 96.10%. Moreover, the proposed framework demonstrates the significant achievement in the attack-wise performance with the F1 scores achieving 96.80% for DoS/DDoS attacks, 96.10% for probing attacks, 96.40% for brute force attacks, 95.30% for R2L infringements, and 94.90% for U2R attacks. Besides, it was noted during the computation efficiency analysis that the new model has reduced the time of inference to 48 milliseconds as well as kept the model's size compact (28.6 MB). The presented information regarding the stability showed the ability of the hybrid system to remain stable in noisy traffic, packet loss, and heterogeneous environments. Thus, the hybrid framework offers a realistic, scalable, and computing-efficient solution for cybersecurity in terms of modern communication systems. In the future, the framework may be enhanced by the introduction of elements of federated learning, explanatory AI, and blockchain-oriented threat intelligence.

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 Confrence 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.

[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.

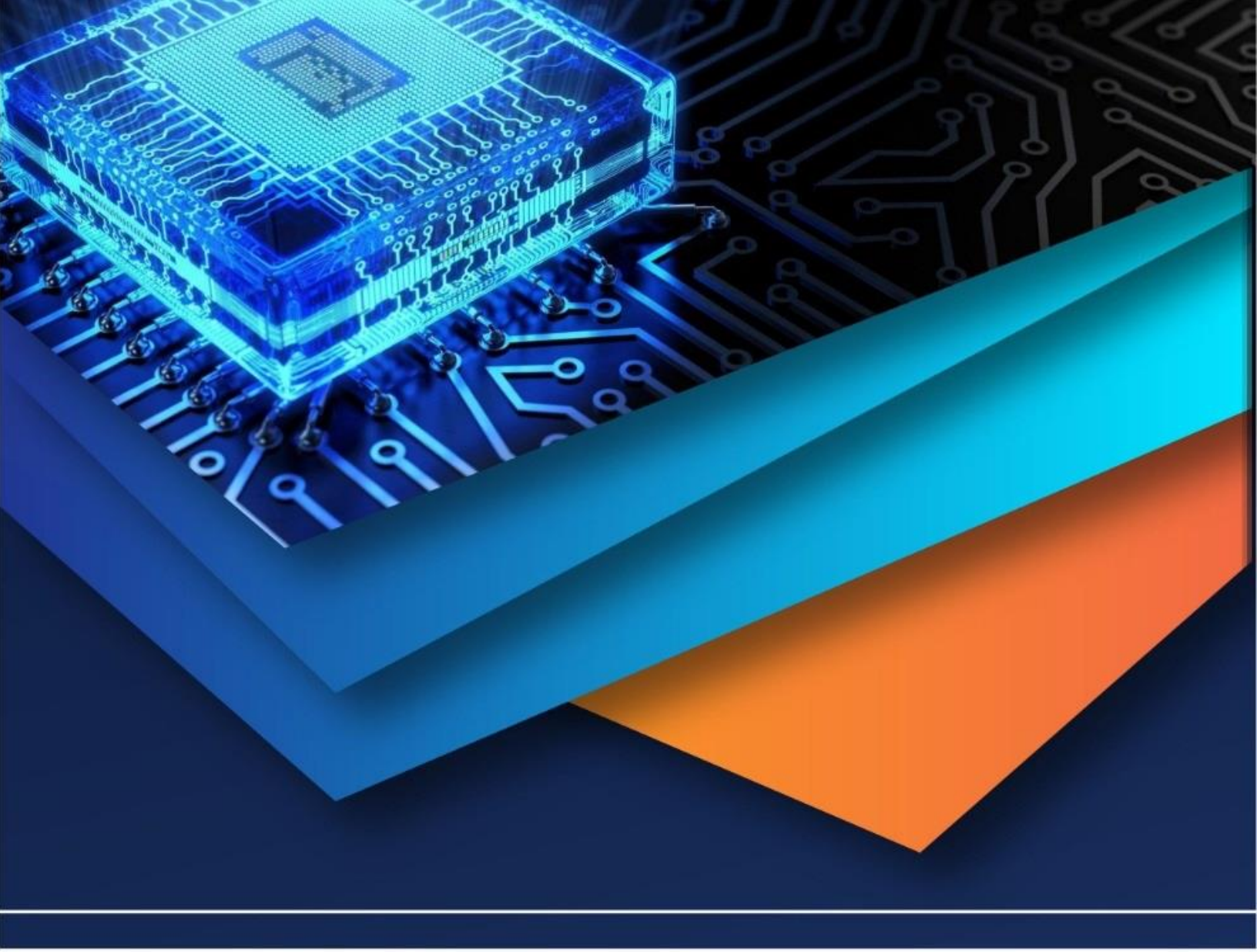
[10] V. Sharma and S. Kumar, "Role of Artificial Intelligence (AI) to Enhance the Security and Privacy of Data in Smart Cities," 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2023, pp. 596-599, doi: 10.1109/ICACITE57410.2023.10182455.

[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.



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)