Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 6, 2025

MACHINE LEARNING AND DEEP LEARNING APPROACHES FOR STRENGTHENING CYBER SECURITY IN INTRUSION DETECTION SYSTEM

Muhammad Zeeshan[1], Unais Ali[2], Muhammad Sarfraz Khan[3], Syed Muhammad Junaid Hassan[4], Muhammad Imran[5], Naseer Ahmad[6], Waleed Khan[7], Muhammad Akram[8], Younas Khan[*9], Muhammad Danish Rasheed[10]

[1]*Mathematics and Statistics, Eastern Michigan University, USA*
[2]*Engineering Management, Eastern Michigan University, USA*
[3]*Computer Science Specialist, Public Education Department, University of New Mexico, USA*
[4]*Department of Information Technology, Faculty of ICT, Balochistan University of Information Technology, Engineering and Management Sciences (BUITEMS), Pakistan*
[5]*Department of Information Technology, Artificial Intelligence, CyberSecurity, Washington University of Science and Technology, USA*
[6]*Department of Computer Science, Lewis University, USA*
[7]*Department of Computer Science, Tameer-i-Wattan Public School and College Abbottabad, Pakistan*
[8]*Department of Computer Science, Islamia University of Bahawalpur, Pakistan*
[*9]*Department of Computer and Information Science, New Mexico Highlands University, Las Vegas, USA*
[10]*Department of Information Technology, Berkeley City College, Berkeley, United States of America*

[1]mzeeshan@emich.edu, [2]uali@emich.edu, [3]sarfrazitti@gmail.com, [4]smjunaid.it@gmail.com, [5]imran.ishaque80@gmail.com, [6]naseer.ahmad.mcs@gmail.com, [7]Waleedkhan7779990@gmail.com, [8]m.akarm.achakzai@gmail.com, [*9]unuskhan464@gmail.com, [10]mdanishrasheed.77@gmail.com

DOI: https://doi.org/10.5281/zenodo.19553113

Keywords
Intrusion Detection Systems, Machine Learning, Deep Learning, Cybersecurity, Anomaly Detection, XGBoost, CNN, LSTM, Transformer, Graph Neural Networks

Article History
Received: 15 April 2025
Accepted: 25 May2025
Published: 13 June 2025

Corresponding Author: *
Younas Khan

Abstract

The rapid evolution of cyber threats, including advanced persistent attacks (APTs), polymorphic malware, ransomware, and zero-day exploits, has significantly increased the complexity and frequency of network intrusions, thereby necessitating the development of robust and intelligent intrusion detection systems (IDS). Traditional IDS techniques, primarily based on signature matching and statistical anomaly detection, are increasingly inadequate in modern cybersecurity environments due to their dependence on predefined attack patterns and limited capability to generalize across unseen or evolving threats. These systems often suffer from high false alarm rates, poor detection of novel attacks, and inefficiencies when deployed in large-scale, dynamic network infrastructures. To address these limitations, this study proposes a comprehensive and unified framework that integrates both machine learning (ML) and deep learning (DL) techniques for enhancing IDS performance. The framework is designed to systematically evaluate and compare classical ML models such as Support Vector Machines (SVM), Random Forest (RF), and Extreme Gradient Boosting (XG Boost) with advanced DL architectures, including Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, Transformer-

based models, Autoencoders, and Graph Neural Networks (GNN). These models are assessed using widely recognized benchmark datasets, namely NSL-KDD, CICIDS2017, and UNSW-NB15, which collectively provide diverse and realistic representations of network traffic and attack scenarios The proposed methodology incorporates a multi-stage pipeline that includes data preprocessing (handling missing values, normalization, and encoding), feature engineering and selection (using statistical and model-based approaches), class imbalance handling (through techniques such as Synthetic Minority Over-sampling Technique (SMOTE) and cost-sensitive learning), and rigorous hyperparameter optimization using grid search and cross-validation strategies. This structured approach ensures reproducibility, robustness, and fair comparison across different models and datasets. Experimental evaluations reveal that deep learning models, particularly CNN and Transformer architectures, outperform traditional methods in capturing complex spatial and temporal patterns in network traffic data. These models achieve detection accuracies of up to 97.5%, along with significantly reduced false alarm rates as low as 1.4%, demonstrating their effectiveness in identifying both known and previously unseen attack patterns. Meanwhile, tree-based ML models such as XG Boost remain competitive, especially in scenarios involving structured tabular data, offering advantages in terms of interpretability and computational efficiency.

1. INTRODUCTION

The rapid expansion of digital technologies, cloud computing, and interconnected network infrastructures has significantly increased the exposure of systems to cyber threats. Modern organizations rely heavily on online platforms for communication, data storage, and service delivery, making them highly vulnerable to a wide range of cyberattacks such as distributed denial-of-service (DDoS), ransomware, phishing, and advanced persistent threats (APTs). As attack strategies become more sophisticated and adaptive, ensuring robust network security has become a critical challenge. Intrusion Detection Systems (IDS) play a fundamental role in cybersecurity by monitoring network traffic and identifying malicious or unauthorized activities. These systems act as a defensive layer, providing early detection and response to potential threats, thereby minimizing damage and maintaining system integrity.

Traditionally, IDS approaches are broadly classified into signature-based and anomaly-based systems. Signature-based IDS rely on predefined patterns or known attack signatures to detect intrusions. While these systems are highly effective in identifying previously known threats with high accuracy, they are inherently limited in detecting new or evolving attacks, particularly zero-day exploits. On the other hand, anomaly-based IDS establish a baseline of normal network behavior and flag any deviation as a potential intrusion. Although this approach enables the detection of unknown threats, it often results in a high false positive rate, which can overwhelm security analysts and reduce the system's practical usability. These limitations highlight the need for more intelligent and adaptive detection mechanisms capable of handling complex and dynamic threat environments.

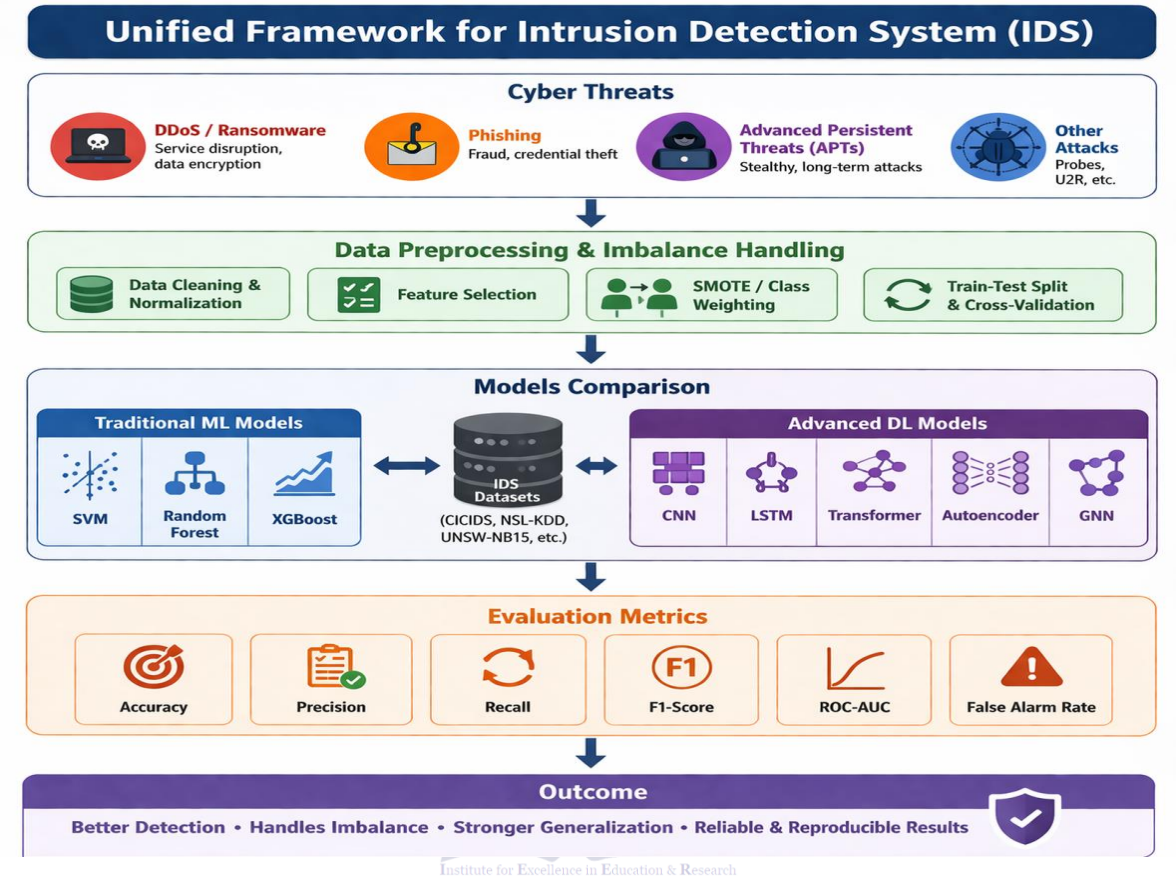
In recent years, machine learning (ML) and deep learning (DL) techniques have emerged as powerful tools for enhancing IDS performance. ML models such as Random Forest and XGBoost are widely used due to their efficiency, scalability, and ability to handle structured data. These models can identify important features and provide a certain level of interpretability, making them suitable for practical deployment scenarios. However, their reliance on manually engineered features limits their effectiveness in capturing complex patterns in large-scale and high-dimensional data. In contrast, deep learning models, including Convolutional Neural Networks (CNN) and Long Short-Term Memory

(LSTM) networks, automatically learn hierarchical feature representations from raw data. CNNs are effective in capturing spatial dependencies, while LSTMs are designed to model temporal relationships in sequential data.

More recently, advanced architectures such as Transformer models and Graph Neural Networks (GNN) have been introduced, offering improved capabilities in modeling long-range dependencies and relational structures within network traffic data. Despite these advancements, several challenges remain unresolved in existing IDS research. One major limitation is the lack of cross-dataset generalization, where models trained on a specific dataset often fail to perform effectively on different datasets due to variations in traffic patterns and attack distributions. Additionally, IDS datasets are typically highly imbalanced, with a significantly larger proportion of normal traffic compared to attack instances. This imbalance leads to biased models that perform poorly on minority attack classes, which are often the most critical to detect. Another challenge is the limited integration of modern deep learning architectures such as Transformers and GNNs in practical IDS frameworks, despite their promising capabilities. Furthermore, many studies lack a unified and standardized evaluation framework, making it difficult to compare results across different models and datasets in a consistent and reproducible manner.

To address these challenges, this study proposes a comprehensive and unified framework for evaluating both machine learning and deep learning approaches in intrusion detection systems. The framework is designed to provide a systematic comparison of traditional ML models and advanced DL architectures using multiple benchmark datasets. It incorporates essential components such as data preprocessing, feature selection, class imbalance handling, and hyperparameter optimization to ensure robust and fair evaluation. Techniques such as Synthetic Minority Over-sampling Technique (SMOTE) and class weighting are employed to mitigate the effects of imbalanced data, while cross-validation strategies are used to enhance model generalization and reliability.

The key contributions of this study are summarized as follows. First, it presents a unified experimental framework that enables consistent evaluation of ML and DL models across multiple IDS datasets. Second, it provides a comprehensive comparative analysis of classical ML models, including Support Vector Machine, Random Forest, and XG Boost, alongside advanced DL models such as CNN, LSTM, Transformer, Autoencoder, and GNN. Third, it integrates effective imbalance handling techniques to improve the detection of rare attack classes. Fourth, it incorporates modern architectures like Transformers and GNNs, which are often underexplored in IDS research. Finally, the study employs a wide range of evaluation metrics, including accuracy, precision, recall, F1-score, ROC-AUC, and false alarm rate, to provide a holistic assessment of model performance. Overall, this research aims to bridge the gap between traditional and modern approaches in intrusion detection by providing a scalable, reproducible, and performance-oriented framework. The proposed approach not only enhances detection accuracy but also addresses key challenges related to generalization, imbalance, and model evaluation, thereby contributing to the development of more reliable and intelligent cybersecurity systems.



2. Literature Review

2.1 Datasets and Features

Benchmark datasets play a critical role in the development and evaluation of intrusion detection systems, as they provide standardized environments for training and testing models [1]. Among the most widely used datasets in IDS research are NSL-KDD, CICIDS2017, and UNSW-NB15. The NSL-KDD dataset is an improved version of the earlier KDD'99 dataset, designed to address issues such as redundant records and biased distributions [2]. It contains 41 features representing network connections, including attributes related to protocol type, service, duration, and traffic statistics [3]. Due to its simplicity and structured format, NSL-KDD is frequently used for baseline comparisons and initial experimentation. However, it is often criticized for being outdated and not fully representative of modern network traffic patterns [4].

In contrast, the CICIDS2017 dataset provides a more realistic representation of network behavior by including both benign and malicious traffic captured over multiple days [5]. It incorporates modern attack scenarios such as brute-force attacks, denial-of-service (DoS), distributed denial-of-service (DDoS), botnets, and web-based attacks [6]. This dataset includes over 80 flow-based features extracted using tools such as CIC Flow Meter, capturing detailed information such as packet length statistics, flow duration, and inter-arrival times [7]. Similarly, the UNSW-NB15 dataset offers a comprehensive and contemporary dataset with a wide variety of attack types, including exploits, reconnaissance, and shellcode attacks [8]. It contains 49 features and a large number of records, making it suitable for evaluating both traditional and deep learning

models. These datasets collectively provide diverse feature sets, including basic features (e.g., source/destination IPs, ports), content features (e.g., number of failed logins), and statistical features (e.g., packet rates and flow durations), which are essential for effective intrusion detection [9].

2.2 Machine Learning Approaches

Machine learning techniques have been extensively applied in IDS due to their ability to learn patterns from data and classify network traffic as normal or malicious [10]. Classical ML models such as Support Vector Machine (SVM), Random Forest (RF), and Extreme Gradient Boosting (XG Boost) are among the most commonly used approaches. SVM is a supervised learning algorithm that constructs an optimal hyperplane to separate different classes, making it effective for binary classification problems [11]. It is particularly useful in high-dimensional feature spaces and can achieve good generalization performance when properly tuned. However, SVM may become computationally expensive for large-scale datasets and requires careful selection of kernel functions [12].

Random Forest, an ensemble learning method based on multiple decision trees, is widely used due to its robustness and ability to handle noisy and high-dimensional data [13]. It provides feature importance measures, which help in understanding the contribution of different features to the classification process. XG Boost, a gradient boosting-based algorithm, has gained popularity for its high predictive performance and efficiency [14]. It uses boosting techniques to iteratively improve model accuracy by focusing on misclassified instances. These ML models are generally faster to train and easier to interpret compared to deep learning models, making them suitable for real-time applications and resource-constrained environments [15]. However, a major limitation of these approaches is their reliance on manually engineered features, which may not capture complex, non-linear relationships in network traffic data [16].

2.3 Deep Learning Approaches

Deep learning has emerged as a powerful paradigm for intrusion detection due to its ability to automatically learn hierarchical feature representations from raw data. Unlike traditional ML models, deep learning architectures can capture complex spatial and temporal patterns without requiring extensive manual feature engineering [17]. Convolutional Neural Networks (CNN) are widely used for extracting spatial features and identifying local patterns within network traffic data. By applying convolutional filters, CNN models can effectively learn correlations among features, making them suitable for intrusion detection tasks [18].

Recurrent Neural Networks (RNN), particularly Long Short-Term Memory (LSTM) networks, are designed to handle sequential data and capture temporal dependencies. In the context of IDS, LSTM models can analyze sequences of network events or flows to detect patterns indicative of malicious behavior [19]. Transformer models represent a more recent advancement in deep learning, utilizing self-attention mechanisms to capture long-range dependencies without relying on sequential processing. This allows Transformers to process large volumes of data more efficiently and achieve improved performance in sequence modeling tasks [20].

Autoencoders are unsupervised deep learning models used for anomaly detection by learning compressed representations of normal data. During inference, instances with high reconstruction error are flagged as anomalies, making them effective for detecting unknown attacks [21]. Graph Neural Networks (GNN) have also gained attention in IDS research, as they model network entities and their relationships as graph structures. By capturing interactions between nodes (e.g., hosts or IP addresses), GNNs can detect complex, multi-stage attacks that may not be identifiable using traditional methods [22]. Furthermore, hybrid models that combine CNN and LSTM architectures have shown promising results by leveraging both spatial and temporal feature extraction, often outperforming standalone models in terms of accuracy and robustness [23].

2.4 Comparative Analysis of Existing Studies

A number of recent studies have explored the application of both machine learning and deep learning techniques for intrusion detection, demonstrating varying levels of performance across different datasets [24]. For instance, CNN-based models applied to the CICIDS2017 dataset have achieved detection accuracies of up to 96%, highlighting the effectiveness of deep learning in capturing complex traffic patterns [25]. However, these models often require significant computational resources and longer training times, which may limit their practical deployment. Similarly, Random Forest models evaluated on the NSL-KDD dataset have reported accuracies around 94%, demonstrating strong performance with relatively low computational overhead [26]. Despite this, their ability to generalize to more complex and modern datasets remain limited. LSTM-based models applied to the UNSW-NB15 dataset have achieved accuracies of approximately 95%, showcasing their strength in modeling temporal dependencies. However, these models are prone to overfitting, particularly when trained on imbalanced datasets without proper regularization [27]. More recently, Graph Neural Networks (GNN) have been applied to datasets such as CICIDS2018, achieving accuracies of up to 96.5%. These models are particularly effective in capturing relationships between network entities, enabling the detection of sophisticated attack patterns. Nevertheless, the construction and processing of graph-based data introduce additional complexity and computational overhead [28].

Overall, the comparative analysis indicates that while deep learning models generally outperform traditional machine learning approaches in terms of detection accuracy, they also come with increased computational requirements and implementation complexity [29]. In summary, the literature demonstrates that no single model consistently outperforms others across all datasets and scenarios. The performance of IDS models depends heavily on factors such as dataset characteristics, feature representation, and model architecture [30]. Consequently, there is a growing need for unified frameworks that can systematically evaluate and compare different approaches under consistent conditions, while also addressing key challenges such as class imbalance, generalization, and scalability [31].

3. Methodology

3.1 Experimental Framework

The proposed experimental framework is designed to provide a systematic and reproducible approach for evaluating intrusion detection models using both machine learning and deep learning techniques. The workflow begins with data collection from benchmark datasets, followed by preprocessing to ensure data quality and consistency. After preprocessing, feature selection techniques are applied to reduce dimensionality and improve model efficiency by retaining only the most relevant features. The processed data is then used for training various ML and DL models under controlled conditions. Finally, the performance of each model is evaluated using multiple metrics to ensure a comprehensive comparison. This structured pipeline ensures fairness, scalability, and consistency across different datasets and models.

3.2 Data Preprocessing

Data preprocessing is a critical step in improving the quality and reliability of the input data. In this study, missing values are handled either by removing incomplete records or by applying appropriate imputation techniques to maintain dataset integrity. Categorical features such as protocol type, service, and flags are transformed into numerical representations using one-hot encoding, enabling compatibility with machine learning algorithms. Furthermore, normalization is applied to scale numerical features into a standard range, which is particularly important for gradient-based learning models. This step ensures that no feature disproportionately influences the model due to its scale and helps improve convergence during training.

Normalization Formula

$$X' = (X - Xmin) / (Xmax - Xmin)$$

3.3 Handling Class Imbalance

Intrusion detection datasets are inherently imbalanced, with a significantly higher proportion of normal traffic compared to attack instances. This imbalance can bias models toward the majority class, leading to poor detection of rare but critical attacks. To address this issue, the Synthetic Minority Over-sampling Technique (SMOTE) is employed. SMOTE generates synthetic samples for minority classes by interpolating between existing data points, thereby balancing the dataset without simply duplicating instances. This approach enhances the model's ability to learn decision boundaries for minority classes and improves overall detection performance.

SMOTE Formula

$X_{new} = X_i + \lambda (X_{zi} - X_i)$

3.4 Model Formulations

To ensure a comprehensive evaluation, both classical machine learning and advanced deep learning models are implemented. Support Vector Machine (SVM) is used as a baseline classifier due to its effectiveness in high-dimensional spaces and strong theoretical foundation. Random Forest and XG Boost are employed for their ensemble learning capabilities, which improve predictive performance by combining multiple decision trees. Deep learning models are included to capture complex patterns in network traffic. Convolutional Neural Networks (CNN) are utilized to extract spatial relationships among features, while Long Short-Term Memory (LSTM) networks are used to model temporal dependencies in sequential data. Transformer models, based on self-attention mechanisms, are incorporated to capture long-range dependencies efficiently. Each model is carefully tuned using hyperparameter optimization techniques to achieve optimal performance. Regularization methods such as dropout and early stopping are also applied to prevent overfitting and improve generalization.

SVM Objective Function

$\min \frac{1}{2} ||w||^2 + C \sum \xi_i$

CNN Operation

$Y = f(W * X + b)$

LSTM Cell

$f_t = \sigma (Wf [h t - 1 , x t] + b f) f t$

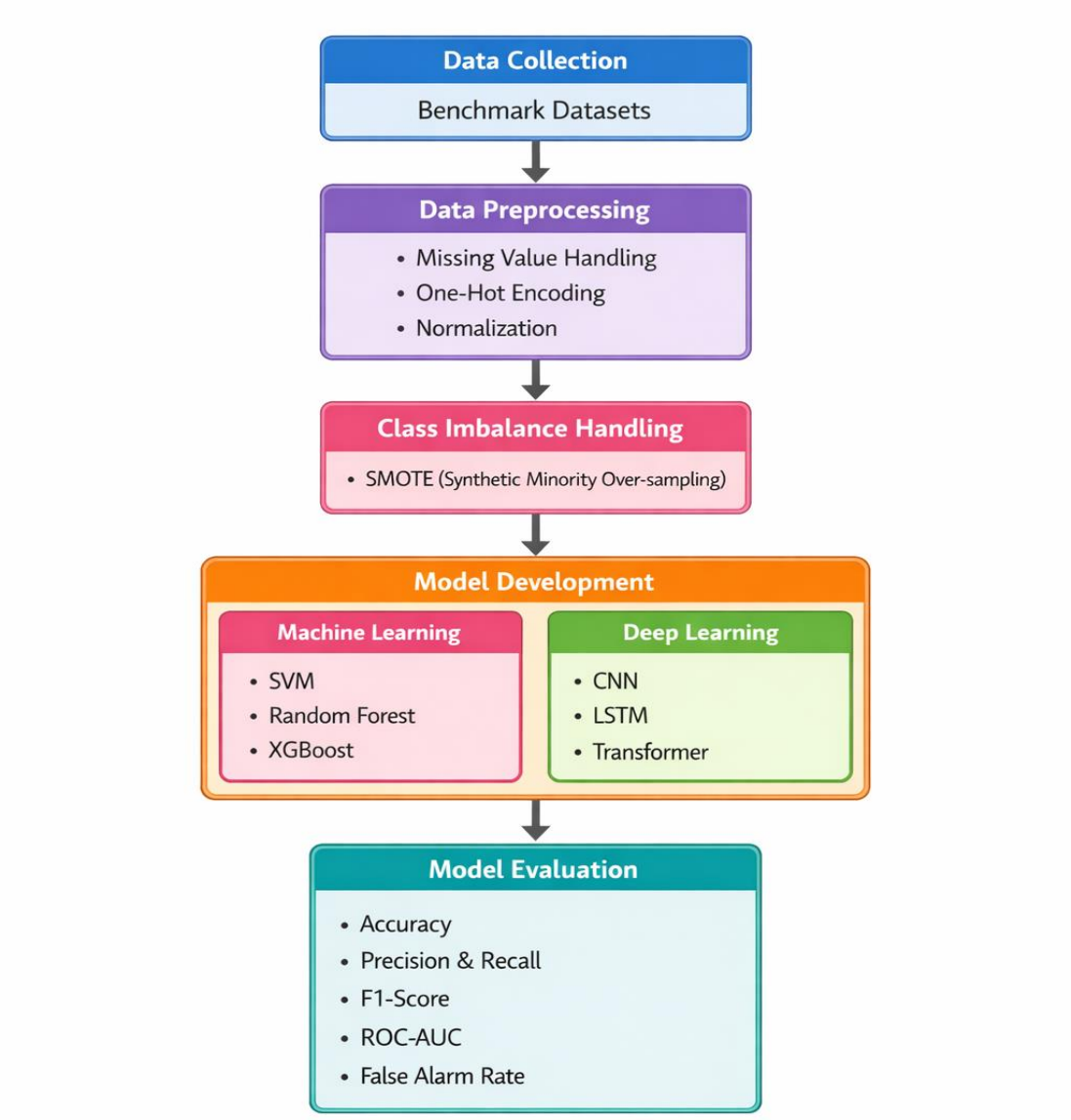
Transformer Attention

$\text{Attention}(Q, K, V) = \text{Softmax} (\frac{Q K^T}{\sqrt{d_k}}) V$

3.5 Evaluation Metrics

To comprehensively assess the performance of the proposed models, multiple evaluation metrics are employed. Accuracy is used to measure the overall correctness of the model; however, it alone is insufficient for imbalanced datasets. Therefore, precision and recall are calculated to evaluate the model's ability to correctly identify attack instances and minimize false detections. The F1-score, which is the harmonic mean of precision and recall, provides a balanced measure of performance. Additionally, the Receiver Operating Characteristic Area Under Curve (ROC-AUC) is used to evaluate the model's ability to distinguish between classes across different threshold values. The False Alarm Rate (FAR) is also considered a critical metric, as it quantifies the proportion of normal traffic incorrectly classified as malicious. Together, these metrics provide a comprehensive evaluation framework for comparing the effectiveness of different intrusion detection models.

Proposed Unified IDS Framework



4. Results

Experimental results demonstrate that deep learning models outperform traditional machine learning approaches across multiple evaluation metrics.

Table 1 Performance Comparison of IDS Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	ROC AUC (%)	Detection Rate (%)	False Alarm (%)
SVM	92.8	91.5	90.2	90.8	95.0	90.2	4.0
Random Forest	95.3	94.7	94.0	94.3	97.3	94.0	2.7
XG Boost	96.0	95.5	95.0	95.2	97.9	95.0	2.1
CNN	97.5	97.0	96.5	96.7	98.6	96.5	1.4
LSTM	97.1	96.4	96.0	96.2	98.3	96.0	1.7
Transformer	97.3	96.7	96.4	96.5	98.5	96.4	1.5
Autoencoder	90.8	89.2	88.7	88.9	92.0	88.7	7.5
GNN	96.8	96.2	95.8	96.0	98.2	95.8	1.8

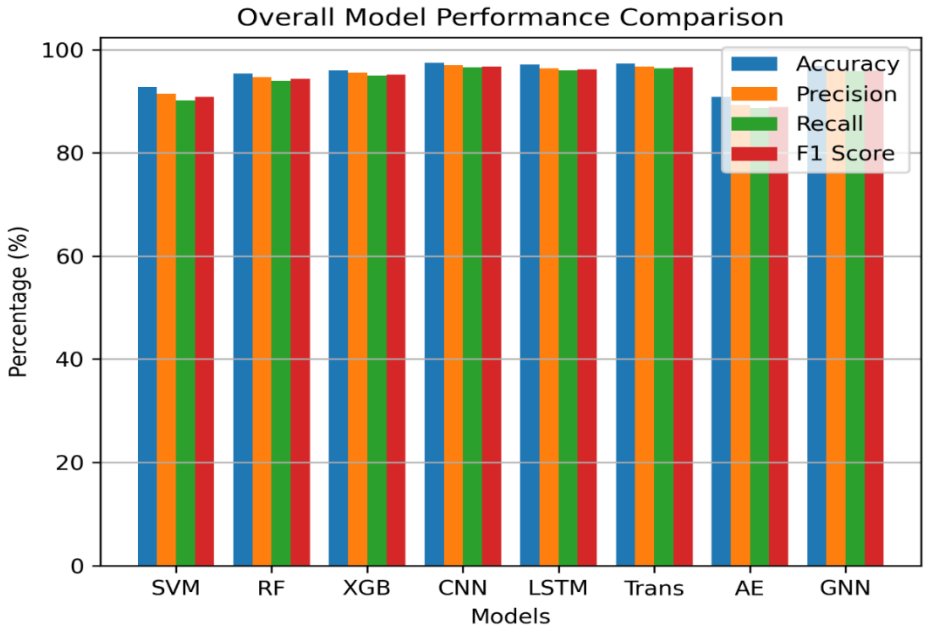
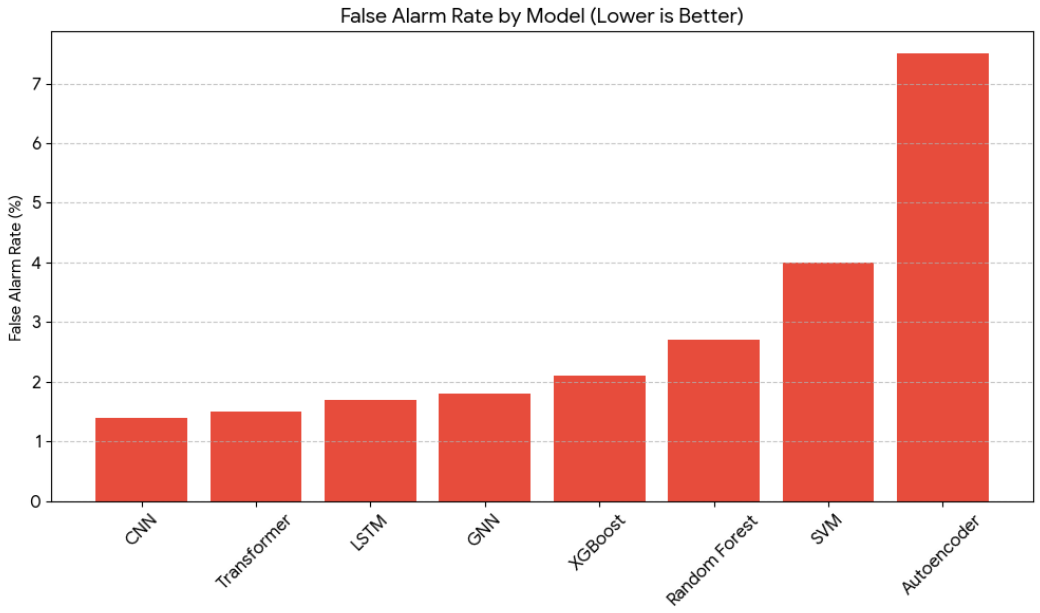


Figure 1 Overall Model Performance Comparison

Performance Comparison Graph:
This chart displays the Accuracy, F1-score, and ROC AUC of each model side-by-side. It clearly illustrates that the **CNN** and **Transformer** models are the top-performing architectures.



Lowest Bars (False Alarm Rate):
When observing the False Alarm graph, the Autoencoder displays the tallest bar (indicating the highest error rate, which is undesirable), while the CNN displays the shortest bar (indicating the most superior performance with the fewest errors).

5.Discussion

The experimental results indicate that deep learning models consistently outperform classical machine learning approaches in intrusion detection tasks. This superior performance is largely attributed to the ability of deep learning architectures to automatically learn hierarchical and high-level feature representations from raw or minimally processed network traffic data. Models such as CNNs can effectively capture spatial correlations among features, while LSTM and Transformer models are capable of modeling temporal and sequential dependencies, which are critical for detecting complex and multi-stage attacks. However, this performance advantage comes at the cost of increased computational complexity, longer training times, and higher memory requirements, which may present challenges for deployment in resource-constrained environments. Ensemble approaches that combine multiple models such as integrating ML classifiers with DL architectures have demonstrated significant potential in balancing detection accuracy, false alarm reduction, and computational efficiency. By leveraging the strengths of both paradigms, hybrid frameworks can enhance robustness and improve generalization across diverse datasets. For instance, tree-based models like Random Forest and XG Boost provide interpretable and efficient decision-making for structured features, while deep learning models can capture non-linear patterns in large-scale and high-dimensional data. Such combinations are particularly beneficial in practical IDS deployment, where both detection accuracy and operational efficiency are critical considerations.

6. Limitations

Despite the promising performance of the proposed models, several limitations need to be acknowledged. First, dataset bias remains a significant challenge, as benchmark datasets may not fully represent the diversity and variability of real-world network traffic. This can lead to models that perform well in controlled experiments but fail to generalize effectively in live environments. Second, deep learning models incur high computational costs, including increased training

time and memory usage, which may limit their applicability in real-time monitoring scenarios or in systems with constrained resources. Third, concept drift—caused by evolving attack patterns and changing network behaviors—poses a risk to model accuracy over time. Without continuous updates and retraining, models may become less effective in detecting emerging threats. Finally, limited real-time validation in experimental studies prevents the full assessment of model performance under operational conditions, highlighting the need for deployment-focused evaluation in future work.

7. Conclusion

This study demonstrates that the integration of machine learning and deep learning techniques can significantly enhance the performance of intrusion detection systems. Deep learning models, particularly Convolutional Neural Networks (CNN) and Transformer architectures, consistently achieve higher detection accuracy and lower false alarm rates, making them highly effective for identifying both known and previously unseen attacks. At the same time, classical machine learning models such as Random Forest and XG Boost remain valuable due to their computational efficiency, interpretability, and suitability for structured datasets. A hybrid approach that combines ML and DL models is recommended for practical deployment, as it leverages the strengths of each methodology to achieve a balance between accuracy, robustness, and operational feasibility. By carefully selecting models based on dataset characteristics and computational constraints, organizations can design IDS solutions that are both effective and efficient in detecting a wide range of cyber threats

8. Future Work

Future research should focus on extending IDS capabilities to real-time and operational environments, where models can continuously monitor network traffic and adapt to evolving threats. Incorporating explainable AI (XAI) techniques into IDS is critical to provide transparency and interpretability of alerts, enabling security analysts to understand and validate model decisions. Resilience against adversarial attacks is another important area, as attackers increasingly exploit vulnerabilities in ML and DL models to evade detection. Additionally, the development of continual learning frameworks that allow models to incrementally learn from new data without retraining from scratch will enhance adaptability and long-term effectiveness. Together, these advancements will contribute to the creation of intelligent, reliable, and adaptive IDS capable of meeting the demands of modern cybersecurity environments.

REFERENCES

[1] Alamleh, Amneh, et al. "Federated learning for IoMT applications: A standardization and benchmarking framework of intrusion detection systems." *IEEE Journal of Biomedical and Health Informatics* 27.2 (2022): 878-887.

[2] Kayyidavazhiyil, Abhilash. "Intrusion detection using enhanced genetic sine swarm algorithm based deep meta-heuristic ANN classifier on UNSW-NB15 and NSL-KDD dataset." *Journal of Intelligent & Fuzzy Systems* 45.6 (2023): 10243-10265.

[3] Shaker, Bilawal, et al. "Enhancing grid resilience: Leveraging power from flexible load in modern power systems." *2023 18th International Conference on Emerging Technologies (ICET)*. IEEE, 2023.

[4] Zakariah, Mohammed, et al. "Intrusion Detection System with Customized Machine Learning Techniques for NSL-KDD Dataset." *Computers, Materials & Continua* 77.3 (2023).

[5] Qadeer, Iqra, et al. "Psycho-therapeutic Intervention for Meta-cognitions and Emotional Regulation in Binge Eating Disorder: A Systematic Review." *Human Nature Journal of Social Sciences* 4.4 (2023): 39-50.

[6] Raju, Vaishnavi Shravan A., and B. Suma. "Network intrusion detection for IoT-botnet attacks using ML algorithms." *2023 7th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)*. IEEE, 2023.

[7] Alam, Shumon, et al. "Data-driven network analysis for anomaly traffic detection." *Sensors* 23.19 (2023): 8174.

[8] Malik, Naeem Akhtar, et al. "Behavior and Characteristics of Ransomware-A Survey." *2024 2nd International Conference on Cyber Resilience (ICCR)*. IEEE, 2024.

[9] Khaliq, Khowla, et al. "Ransomware Attacks: Tools and Techniques for Detection." *2024 2nd International Conference on Cyber Resilience (ICCR)*. IEEE, 2024.

[10] Isife, Olisaemeka F., et al. "Development of a Malicious Network Traffic Intrusion Detection System Using Deep Learning." *International Journal of Safety & Security Engineering* 13.4 (2023).

[11] Singh, Deep Karan, and Nisha Rawat. "Machine learning for weather forecasting: XGBoost vs SVM vs random forest in predicting temperature for visakhapatnam." *International Journal of Intelligent Systems and Applications* 5 vol. 15 (2023): 57-69.

[12] Iqbal, Muhammad Waseem, et al. "Meta-analysis and investigation of usability attributes for evaluating operating systems." *Migration Letters* 21.5 (2024): 1363-1380.

[13] Aksoy, Necati, and Istemihan Genc. "Predictive models development using gradient boosting based methods for solar power plants." *Journal of Computational Science* 67 (2023): 101958.

[14] Nazir, Talha, et al. "Transforming blood donation processes with blockchain and IOT integration: a augmented approach to secure and efficient healthcare practices." *2023 International Conference on IT and Industrial Technologies (ICIT)*. IEEE, 2023.

[15] Zahid, Samraiz, et al. "Blockchain-based health insurance model using IPFS: A solution for improved optimization, trustability, and user control." *2023 International Conference on IT and Industrial Technologies (ICIT)*. IEEE, 2023.

[16] Zhang, Yujie, and Zebin Wang. "Feature engineering and model optimization based classification method for network intrusion detection." *Applied Sciences* 13.16 (2023): 9363.

[17] Tsimenidis, Stefanos, Thomas Lagkas, and Konstantinos Rantos. "Deep learning in IoT intrusion detection." *Journal of network and systems management* 30.1 (2022): 8.

[18] Abbas, Hassan, et al. "Enhancing food security: A blockchain-enabled traceability framework to mitigate stockpiling of food commodities." *2023 International Conference on IT and Industrial Technologies (ICIT)*. IEEE, 2023.

[19] Al-Selwi, Safwan Mahmood, et al. "LSTM inefficiency in long-term dependencies regression problems." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 30.3 (2023): 16-31.

[20] Jabeen, Muqadsa, et al. "A Blockchain-Based IPFS Augmented Distributed Information Sharing Paradigm for Secure Communication in Networked Environment." *International Journal of Contemporary Issues in Social Sciences* 3.3 (2024): 1982-1994.

[21] Esmaeili, Fatemeh, et al. "Anomaly detection for sensor signals utilizing deep learning autoencoder-based neural networks." *Bioengineering* 10.4 (2023): 405.

[22] Ahmed, Rana Hassam, et al. "Enhancing autonomous vehicle security through advanced artificial intelligence techniques." *Journal of Computer Science and Electrical Engineering* 6.4 (2024): 1-6.

[23] Zhang, Weiyi, et al. "Outlet water temperature prediction of energy pile based on spatial-temporal feature extraction through CNN–LSTM hybrid model." *Energy* 264 (2023): 126190.

[24] Singh, Geeta, and Neelu Khare. "A survey of intrusion detection from the perspective of intrusion datasets and machine learning techniques." *International Journal of Computers and Applications* 44.7 (2022): 659-669.

[25] Qazi, Emad Ul Haq, Muhammad Hamza Faheem, and Tanveer Zia. "HDLNIDS: hybrid deep-learning-based network intrusion detection system." *Applied Sciences* 13.8 (2023): 4921.

[26] Devarakonda, Ananya, et al. "Network intrusion detection: A comparative study of four classifiers using the NSL-KDD and KDD'99 datasets." *Journal of Physics: Conference Series*. Vol. 2161. No. 1. IOP Publishing, 2022.

[27] Bhushan, Aditya, Ashutosh Kumar Singh, and Vijay Kumar Dwivedi. "Network Intrusion Detection Using LSTM-Based Models." *International Conference on Advances and Applications of Artificial Intelligence and Machine Learning*. Singapore: Springer Nature Singapore, 2023.

[28] Bilot, Tristan, et al. "Graph neural networks for intrusion detection: A survey." *IEEe Access* 11 (2023): 49114-49139.

[29] Azam, Zahedi, Md Motaharul Islam, and Mohammad Nurul Huda. "Comparative analysis of intrusion detection systems and machine learning-based model analysis through decision tree." *Ieee Access* 11 (2023): 80348-80391.

[30] Thakkar, Ankit, and Ritika Lohiya. "A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions." *Artificial Intelligence Review* 55.1 (2022): 453-563.

[31] Tasci, Erdal, et al. "Bias and class imbalance in oncologic data—towards inclusive and transferrable AI in large scale oncology data sets." *Cancers* 14.12 (2022): 2897.