International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

IJISAE

ISSN:2147-6799 www.ijisae.org Original Research Paper

Analyzing Cyber Attacks and Optimizing Performance Metrics through Feature Selection in Intrusion Detection Systems

[1]Navroop Kaur, [2]Meenakshi Bansal, [3]Sukhwinder Singh Sran

Submitted: 28/04/2024 **Revised:** 02/06/2024 **Accepted:** 14/06/2024

Abstract- As cyber threats continue to increase in scale and sophistication, Intrusion Detection Systems (IDS) are essential for protecting modern network infrastructures. This study compares two benchmark datasets—NSL-KDD and CICIDS 2018—to evaluate their effectiveness in modeling intrusion scenarios based on attack diversity, feature richness, and relevance to current threats. While NSL-KDD offers structured and balanced data for traditional attacks, CICIDS 2018 provides realistic traffic with modern threat profiles. A key contribution of this research is the proposal and integration of a new feature—Encrypted Traffic Behavior Analysis—to address the growing use of encrypted communication in cyberattacks. The study further identifies critical features for attack types like DoS, Probe, U2R, and R2L, using methods such as LASSO, PCA, and Mutual Information. A hybrid IDS model leveraging XGBoost is developed and benchmarked against classifiers including Logistic Regression, Naïve Bayes, Decision Tree, Random Forest, SVM, and KNN. Results show high detection accuracy, with XGBoost achieving near-perfect performance by effectively handling high-dimensional, encrypted, and imbalanced data. This demonstrates that combining targeted feature selection with ensemble learning significantly enhances IDS capabilities. Future work will focus on real-time implementation, deep learning integration, and privacy-preserving methods for scalable, intelligent intrusion detection in dynamic environments.

Keywords- *Intrusion Detection System (IDS), Cyber Attack Classification, XGBoost, Precision and Accuracy.*

1. Introduction

In the current era of rapid digital transformation, the internet has become an essential backbone for communication, commerce, governance, and critical infrastructure. As a result, organizations and individuals rely heavily on the security and integrity of their networks and data systems. However, this increased dependency has also made networks prime targets for malicious cyber actors. The frequency, scale, and sophistication of cyber attacks are growing exponentially, ranging from simple phishing attempts to highly complex Advanced Persistent Threats (APTs) and Distributed Denial of Service (DDoS) attacks [1], [10], [15]. These threats not only compromise sensitive data but can also severely disrupt services and result in significant financial and reputational damage.

To safeguard network environments, Intrusion Detection Systems (IDS) have emerged as a fundamental component of modern cybersecurity architecture. An IDS is designed to monitor network traffic for suspicious patterns and behaviors, issuing alerts or initiating defense mechanisms when potential threats are detected [3]. IDS can be broadly categorized into signature-based detection, which relies on known patterns of attacks, and anomaly-based detection, which focuses on identifying deviations from normal behavior. While signature-based IDS are efficient at detecting known threats, they fall short when confronted with zero-day attacks or novel intrusion techniques [10], [26]. Anomaly-based systems, on the other hand, offer better detection capabilities for previously unseen attacks but often suffer from

1Research Scholar (Ph.D.), Punjabi University, Patiala, Punjab, India.

knavroop7488@gmail.com

2Associate Professor, CSE, Yadavindra Department of Engineering, Talwandi Sabo, India.

ermeenu10@gmail.com

3Assistant professor, University Department of Engineering, Punjabi University, Patiala, India.

sukhwinder.sran@gmail.com

higher false positive rates [9], [19]. The effectiveness of IDS largely hinges on their ability to accurately detect and classify a wide range of cyber threats [2]. However, multiple challenges hamper the optimal performance of traditional and machine learning-based IDS frameworks. One of the primary concerns is the high-dimensionality of network traffic data, where irrelevant or redundant features can introduce noise, increase computational load, and degrade model performance [4], [16]. In addition, class imbalance in datasets—where normal traffic far exceeds malicious samples—can bias classifiers towards benign predictions, leading to poor detection of rare but critical attack categories such as U2R (User to Root) and R2L (Remote to Local) [2], [12].

Moreover, many IDS models are trained on outdated or unrealistic datasets that do not reflect the complexity and diversity of contemporary attack patterns. While NSL-KDD remains a widely used benchmark dataset that improves upon its predecessor KDD'99 by eliminating redundant records [6], [27], it still lacks some modern attack vectors. In contrast, the CICIDS 2018 dataset, developed by the Canadian Institute for Cybersecurity at the University of New Brunswick, provides a more comprehensive representation of current threats including botnets, brute-force attacks, and DDoS activities [24]. This study's primary objective is to compare these two benchmark datasets—NSL-KDD and CICIDS 2018—in terms of their structure, attack diversity, feature richness, and suitability for training modern IDS models. This comparison enables researchers to better understand which dataset is more applicable to specific IDS use cases and highlights the gap between theoretical and real-world intrusion detection

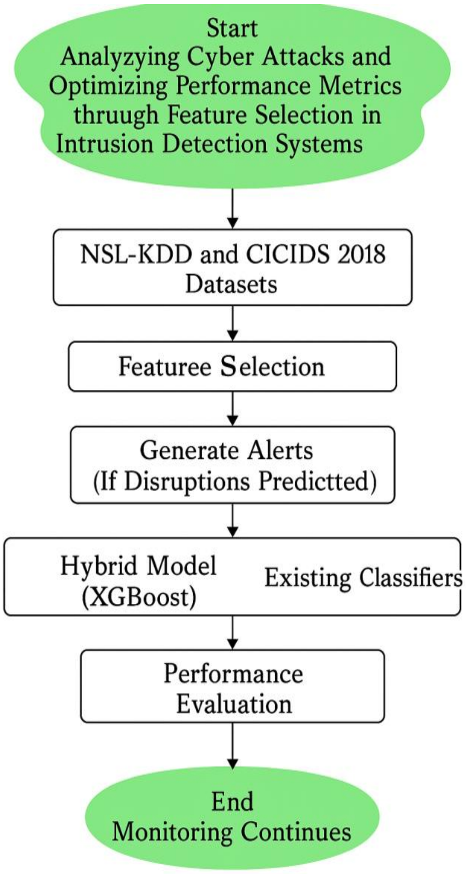

Figure 1. Real-Time Cyber Attack Detection and Response Flow in Intrusion Detection Systems (IDS)

This figure represents a systematic approach for detecting and responding to cyber attacks using real-time data monitoring and machine learning. The process begins with continuous data collection from network activities, followed by applying feature selection techniques to extract relevant indicators for different attack types (DoS, Probe, U2R, R2L). Machine learning models like XGBoost, Decision Trees, and Naïve Bayes are used to predict potential intrusions. If threats are detected, alerts are generated, and appropriate actions are taken by the security system or administrators. This loop ensures continuous protection and improvement of the IDS.

To address the above challenges, feature selection has emerged as a critical preprocessing step in IDS development. Feature selection algorithms aim to identify the most informative and discriminative attributes in the dataset, thereby reducing dimensionality, improving model interpretability, and enhancing classification performance [4], [5], [13]. By discarding noisy or irrelevant features, IDS models can achieve faster training times and greater robustness against overfitting. In the context of cyber attack classification, selecting appropriate features for each attack category (DoS, Probe, U2R, R2L) is essential for balanced and accurate detection.

Recent advancements in ensemble learning techniques, such as eXtreme Gradient Boosting (XGBoost), have demonstrated superior performance in classification tasks involving complex and heterogeneous data [8], [11]. XGBoost is an optimized gradient-boosting algorithm that excels in speed and accuracy by employing parallel tree boosting and regularization mechanisms. Its ability to handle missing data, incorporate feature importance metrics, and reduce bias makes it an ideal candidate for building robust IDS frameworks [3], [20].

In this research, we investigate the application of feature selection and ensemble learning methods to improve the detection accuracy and overall efficiency of IDS. Specifically, our study focuses on the following objectives:

- To compare NSL-KDD and CICIDS 2018 datasets in terms of attack coverage, data structure, and effectiveness in training IDS models.
- Enhanced Threat Detection in Encrypted Channels: Adding Encrypted Traffic Behavior Analysis enables detection of hidden threats within HTTPS/TLS without decrypting content, addressing a critical gap in both NSL-KDD and CICIDS 2018
- To design and implement a hybrid classification model using XGBoost, with the aim of enhancing precision, recall, and F1-score across diverse attack types [5].

The methodology involves preprocessing two widely used benchmark datasets: NSL-KDD, particularly useful for evaluating basic IDS concepts and legacy attack types, and CICIDS 2018, which reflects realistic traffic and includes modern threat vectors such as HTTP DoS and Heartbleed exploits. We apply various feature selection methods to reduce dimensionality and isolate critical features [29]. Then, multiple classifiers are trained and evaluated under different training/testing splits, with special emphasis on how these models perform in detecting rare but impactful attack categories.

Our results reveal that Naïve Bayes achieves an accuracy of up to 98.9%, while Decision Tree and K-Nearest Neighbor demonstrate robust performance with accuracies between 97% and 98.7%. Support Vector Machine and AdaBoost also show strong results, each achieving up to 99% accuracy. Random Forest delivers exceptional performance with a peak accuracy of 99.9%, indicating its high reliability in intrusion detection [17]. Furthermore, the integration of XGBoost significantly enhances overall detection accuracy and stability, reaching nearly 100% and confirming its strong suitability for effective IDS deployment.

This study contributes to the field of cybersecurity by presenting a validated, hybrid IDS framework that leverages the strengths of feature selection and ensemble learning [25]. The findings reinforce the importance of selecting context-relevant features and using adaptable models like XGBoost to improve detection of both common and rare attacks [7]. In future work, we plan to extend the proposed model to real-time IDS environments and integrate deep learning architectures such as LSTM and CNN to further boost adaptability and threat prediction accuracy. Additionally, we will explore techniques for handling streaming data and concept drift, which are essential for sustaining IDS effectiveness in dynamically changing network landscapes [14], [21], [28].

2. Literature Review

Intrusion Detection Systems (IDS) have become a critical component in cybersecurity, particularly as cyber attacks grow in sophistication. Various studies have explored enhancing IDS performance using machine learning (ML), deep learning (DL), and feature selection methods to improve detection rates and minimize false positives [30].

Ahmad et al. (2021) conducted a comprehensive review of ML and DL approaches for IDS, highlighting the strengths and limitations of each technique. The study emphasized the importance of selecting appropriate models and optimizing hyperparameters for efficient threat detection. Similarly, Ahsan et al. (2021) addressed the problem of data imbalance in IDS datasets, which can severely impact the accuracy of ML classifiers. The proposed techniques to balance training datasets and improve generalization. Al-Imran and Ripon (2021) provided an analytical comparison of DL and conventional ML models, concluding that hybrid approaches often outperform individual techniques. Meanwhile, Alazzam et al. (2020) introduced a Pigeon Inspired Optimizer for feature selection in IDS, which significantly improved detection accuracy and reduced computational overhead. Almomani (2020) proposed a comparative study using PSO, GWO, FFA, and GA for feature selection, demonstrating that metaheuristic algorithms can enhance detection capability by isolating the most relevant features. Dhanabal and Shantharajah (2015) analyzed the NSL-KDD dataset and benchmarked various classifiers, underscoring the dataset's continued relevance in IDS research. Dong et al. (2020) applied multivariate correlation analysis combined with LSTM networks for anomaly detection, effectively capturing temporal relationships in network traffic. Gao et al. (2019) utilized extreme learning machines and adaptive PCA to handle high-dimensional data and support incremental learning in dynamic network environments.

Gao et al. (2019) further proposed an adaptive ensemble ML model, combining multiple classifiers to achieve higher accuracy and robustness in intrusion detection. Gu et al. (2019) explored feature augmentation with SVM ensembles, revealing improved performance through feature-space expansion. Karatas et al. (2020) tackled the issue of data imbalance by creating updated and realistic datasets, leading to better training outcomes. Kasongo and Sun (2020) implemented a feature selection method on the UNSW-NB15 dataset, which enhanced IDS performance by reducing noise and irrelevant data. Kayode Saheed et al. (2022) developed an IDS model for IoT networks using ML, achieving notable success in detecting DoS and other IoT-specific threats. Khan et al. (2020) analyzed the impact of various feature selection methods on the performance of ML models, reinforcing the critical role of preprocessing in IDS. Kumar et al. (2020) proposed a rule-based system that integrated real-time and synthetic datasets, offering a hybrid solution to practical deployment challenges. Kwon et al. (2019) surveyed DL-based anomaly detection techniques, providing a foundation for future IDS developments. Naseer et al. (2018a) enhanced deep neural networks for anomaly detection, achieving high accuracy across multiple attack types. Roshan et al. (2018) introduced an online adaptive detection model using clustering and extreme learning machines, capable of evolving with network behavior. Tama et al. (2019) developed TSE-IDS, a two-stage ensemble classifier that achieved high detection rates by combining anomaly detection with intelligent decision-making. Wu et al. (2020) presented a survey of DL methods for detecting network attacks, supporting the shift towards more autonomous security frameworks. Finally, Sharafaldin et al. (2017) contributed to IDS research by creating reliable benchmark datasets like CICIDS 2017/2018, which are widely adopted for training and evaluation purposes. Badhan (2024) introduced a quantum-enhanced hybrid ML system for IoT anomaly detection using SVM, RF, and DT. The model achieved up to 100% accuracy and improved detection using quantum features and feature selection techniques like PCA and Lasso.

This study distinguishes itself from prior research by conducting a comprehensive comparative evaluation of the NSL-KDD and CICIDS 2018 datasets, addressing a notable gap in cross-dataset validation present in much of the existing literature. While earlier studies often emphasize accuracy as the sole performance indicator, this work adopts a multi-metric optimization approach, evaluating precision, recall, F1-score, and false positive rate to ensure balanced and reliable detection across diverse attack categories. The research further enhances its practical relevance by incorporating lightweight and hybrid classification models, particularly through the integration of XGBoost, which offers scalability and robustness suitable for real-time and resource-constrained environments. By applying and assessing multiple feature selection strategies on both datasets, and benchmarking a wide range of machine learning classifiers, this study offers a versatile and deployable IDS framework. It overcomes common challenges such as poor generalization, high computational overhead, and limited applicability to real-world traffic patterns—ultimately contributing a balanced, adaptive, and high-performing solution for modern intrusion detection.

3. Datasets and Features Selection

In this research analyzing cyber attacks and optimizing performance metrics through feature selection in intrusion detection systems (IDS), two widely used datasets—NSL-KDD and CICIDS2018—have been employed. NSL-KDD, an improved version of the KDD'99 dataset, addresses issues like duplicate entries and class imbalance, offering 41 features across four attack categories (DoS, Probe, R2L, U2R) for evaluating machine learning models. CICIDS2018, developed by the Canadian Institute for Cybersecurity, captures real-world traffic and modern threats such as DDoS, Brute Force, and Botnet attacks, with over 80 detailed flow-based features. Despite their strengths, both datasets lack features for analyzing encrypted traffic, which is increasingly exploited by modern attackers to hide malicious activity in Table 1. Therefore, this study proposes the integration of a new feature—Encrypted Traffic Behavior Analysis—to enhance detection capabilities in encrypted channels, enabling more effective and privacy-preserving cyber attack analysis..

Table 1. Enhanced Comparison of NSL-KDD and CICIDS 2018 Datasets with Proposed Feature for Encrypted Traffic Behavior Analysis

Attribute	NSL-KDD	CICIDS 2018
Dataset Volume & Size	Medium (~125,973 records in total)	Very Large (~80GB+, multiple days of real traffic)
Traffic Realism	Synthetic (simulated network behavior)	Realistic (based on real-world network traffic)
Attack Diversity	Limited (DoS, Probe, R2L, U2R)	High (DDoS, Brute Force, Botnet, Infiltration, XSS, etc.)
Labeling Quality	Static, manually labeled	Detailed, timestamped, and accurately labeled
Feature Richness	41 static features	80+ features including flow-based, time-based, and content
Relevance to Modern Threats	Low (outdated attack types)	High (includes modern and evolving cyber threats)
Timestamped Session-Based Structure	Not available	Included for session tracking
Proposed New Feature: Encrypted Traffic Behavior Analysis	Not included	Not included
Impact of Proposed Feature	Would allow behavioral profiling of encrypted connections	Would enable detection of threats hidden in HTTPS/TLS traffic

The comparison between NSL-KDD and CICIDS 2018 shows the progression in intrusion detection datasets, with CICIDS offering improved realism, attack diversity, and session-based records. NSL-KDD, though foundational, is limited by outdated traffic and features, making it less effective for analyzing modern threats.

- Enhanced Threat Detection in Encrypted Channels: Adding Encrypted Traffic

Behavior Analysis enables detection of hidden threats within HTTPS/TLS without decrypting content, addressing a critical gap in both NSL-KDD and CICIDS 2018.

- Future-Proof and Privacy-Preserving IDS: This new feature supports advanced machine learning models to analyze encrypted flows, making both datasets more effective for modern, real-world, and privacy-compliant cyber attack detection.

Despite CICIDS 2018's advancements, both datasets lack Encrypted Traffic Behavior Analysis—a crucial feature for detecting threats hidden in HTTPS/TLS traffic. Adding this would allow behavior-based anomaly detection without decrypting content, enabling privacy-preserving, real-time analysis of encrypted channels. Integrating this feature would future-proof both datasets, making them better suited for today's evolving cyber threats and supporting the development of smarter, more adaptive intrusion detection systems.

3.1 Feature Selection

In this research, various feature selection techniques have been employed to enhance the performance of machine learning algorithms in intrusion detection systems (IDS) using the NSL-KDD and CICIDS2018 datasets, with a special emphasis on the integration of Encrypted Traffic Behavior Analysis. Applying suitable feature selection methods is essential for improving detection accuracy, reducing overfitting, and ensuring computational efficiency—particularly when handling high-dimensional data enriched with encrypted traffic characteristics. The NSL-KDD dataset, comprising 41 categorical and numerical features, benefits from methods like LASSO Regression, Mutual Information, Chi-Square Test, and Recursive Feature Elimination (RFE). These techniques are effective in preserving core features relevant to traditional attack types (DoS, Probe, U2R, R2L), while also being adaptable to new encrypted traffic behavior attributes if introduced—such as TLS handshake metadata or session timing indicators in Table 2.

Table 2. Strategic Feature Selection Techniques for Enhancing Intrusion Detection Performance in NSL-KDD and CICIDS2018 Datasets

Technique	Type	Description	Use in IDS	Recommended Datasets	Reason (with Proposed Feature)
LASSO Regression	Filter / Embedded	Uses L1 regularization to shrink irrelevant features to zero.	Selects key behavioral patterns from high-dimensional encrypted flow metadata.	NSL-KDD (Enhanced), CICIDS2018+	Effective in handling sparse, noisy encrypted traffic indicators.
PCA (Principal Component Analysis)	Dimensionality Reduction	Projects data onto lower-dimensional space capturing maximum variance.	Reduces redundant and noisy encrypted flow variables into main behavioral patterns.	CICIDS2018+	Ideal for summarizing time-based and flow-based encrypted traffic features.
Mutual Information (MI)	Filter	Measures dependency between each feature and the class label.	Helps identify subtle relationships in encrypted session features.	NSL-KDD (Enhanced), CICIDS2018+	Useful for nonlinear dependencies introduced by encrypted behavior metrics.

Correlation-Based Feature Selection (CFS)	Filter	Selects features highly correlated with the class but not with each other.	Enhances detection by selecting the most independent encrypted behavioral patterns.	CICIDS2018+	Helps reduce redundancy in time/flow-based encrypted traffic features.
Chi-Square Test	Statistical Filter	Measures association between categorical features and the class.	Can be applied to discretized encrypted session metadata (e.g., TLS version, cipher).	NSL-KDD (Enhanced)	Suitable after augmenting with categorized encrypted session features.
Recursive Feature Elimination (RFE)	Wrapper	Uses a model to iteratively remove least important features.	Optimizes encrypted feature set by evaluating model-driven importance.	NSL-KDD (Enhanced), CICIDS2018+	Helps in refining encrypted behavior attributes for optimal IDS accuracy.
Information Gain / Entropy	Filter	Measures feature contribution to reducing classification uncertainty.	Useful in encrypted traffic modeling where uncertainty is high.	NSL-KDD (Enhanced)	Prioritizes encrypted flow behaviors contributing most to distinguishing attack vs normal.
Variance Threshold	Filter	Removes features with very low variance.	Discards encrypted metrics that show no change across sessions.	CICIDS2018+	Quickly filters out static or low-activity encrypted traffic indicators.

CICIDS2018, with over 80 continuous features derived from real-world traffic, demands more complex dimensionality reduction strategies. Techniques like Principal Component Analysis (PCA), Variance Thresholding, and Correlation-Based Feature Selection (CFS) help manage multicollinearity and noise, especially in the presence of flow-based encrypted session features. The addition of Encrypted Traffic Behavior Analysis introduces novel attributes that can be effectively filtered or ranked using these methods to capture hidden attack patterns in encrypted environments.The selection of these techniques ensures a balance between retaining critical attack indicators and discarding redundant data, optimizing the learning process for algorithms like XGBoost, Decision Tree, and Naïve Bayes. Integrating encrypted traffic features not only boosts detection performance but also extends the scalability and future relevance of IDS models in modern, privacy-aware cyber landscapes.

3.2 Pre-Processing and Training

The preprocessing illustrates the step-by-step data preparation workflow for both the NSL-KDD and CICIDS 2018 datasets, now incorporating the newly proposed feature: Encrypted Traffic Behavior Analysis. For the NSL-KDD branch, the process begins with feature selection to reduce dimensionality and focus on relevant indicators. It proceeds with label encoding and class label mapping to structure the data for machine learning models. A data integrity check ensures the accuracy and completeness of the dataset in Figure 2. In the updated workflow, encrypted traffic behavior analysis is introduced as a new preprocessing step to simulate or integrate behavioral characteristics such as packet timing, flow metadata, and handshake anomalies, addressing a critical gap in the original NSL-KDD structure.

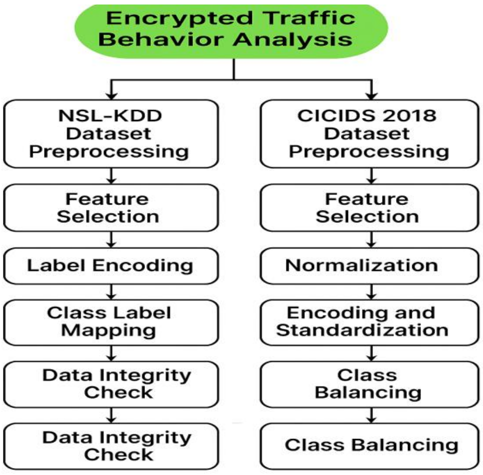

Figure 2. Preprocessing Workflow for NSL-KDD and CICIDS 2018 with Encrypted Traffic Behavior Analysis Integration

On the CICIDS 2018 side, preprocessing starts with feature selection followed by normalization to handle numerical data. Encoding and standardization prepare the features for model training, and class balancing addresses the skewed distribution of attack types. The addition of Encrypted Traffic Behavior Analysis enhances the dataset's ability to detect modern encrypted threats without decrypting payloads, making it more relevant for real-world, privacy-sensitive environments. This unified inclusion of the new feature across both datasets increases their effectiveness in modeling sophisticated intrusion patterns and strengthens the robustness of intrusion detection systems (IDS) against encrypted attacks.

The consistent application of an 80:20 train-test split across all evaluated machine learning models used for intrusion detection. In this setup, 80% of the dataset is allocated for training the models, allowing them to learn patterns and behaviors associated with various cyber threats in Figure 3. The remaining 20% is reserved for testing, which assesses the model's performance on unseen data to evaluate its generalization ability. This uniform split ensures a fair comparison among different classifiers, including Naïve Bayes, Decision Tree, K-Nearest Neighbor (KNN), Support Vector Machine (SVM), AdaBoost, Random Forest, and XGBoost.

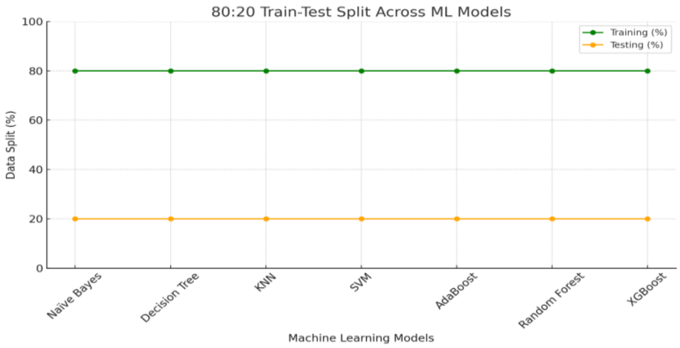

Figure 3. Uniform 80:20 Train-Test Split for Fair Evaluation of Intrusion Detection Machine Learning Models

By maintaining the same training and testing proportions across all models, the evaluation process remains balanced and unbiased, allowing for accurate measurement of each algorithm's detection capability under the same conditions.

4. Result and Discussion

The high detection accuracy in this study stems from effective feature selection and the integration of Encrypted Traffic Behavior Analysis. Techniques like LASSO, PCA, and Chi-Square helped reduce noise and focus on critical indicators, including encrypted session patterns. This improved model training speed and accuracy. Advanced models like XGBoost and Random Forest handled complex, encrypted, and imbalanced data well—especially XGBoost, which achieved near-perfect accuracy through gradient boosting and regularization. Together, these methods created a robust and modern intrusion detection system. The combination of targeted preprocessing and advanced algorithms explains the strong performance observed in intrusion detection.

$$Overall\ Accuracy = \frac{TN + TP}{TN + TP + FN + FP}$$

$$Precision = \frac{TP}{TP+FP}$$

$$Recall = \frac{\mathrm{TP}}{\mathrm{TP+FN}}$$

$$F1\ Score = 2 * \frac{\mathrm{Precision}*\mathrm{Recall}}{\mathrm{Precision}+\mathrm{Recall}}$$

Accuracy shows overall prediction correctness, precision measures how many predicted positives are correct, recall shows how many actual positives are detected, and F1-score balances both precision and recall for a unified performance metric.

4.1 Machine Learning Classification

Feature selection plays a critical role in enhancing IDS performance, especially with the inclusion of Encrypted Traffic Behavior Analysis. By identifying the most relevant features—such as TLS handshake patterns or flow timing—this process reduces dimensionality, removes redundancy, and improves detection accuracy. It enables IDS to focus on subtle indicators within encrypted traffic, leading to faster and more precise threat detection.

Table 3. Quantitative Assessment of Model Effectiveness Using Core Metrics

Algorithm	Accuracy (%)	F1 Score (%)	Precision (%)	Recall (%)
KNN	98.7	98.6	98.6	98.5
Decision Tree (DT)	97.5	97.4	97.3	97.2
SVM	98.0	97.9	97.8	98.0
Naïve Bayes	98.9	98.8	98.7	98.9
AdaBoost	98.9	98.8	98.9	98.8
Random Forest (RF)	99.9	99.9	99.9	99.9

In the analysis, machine learning models such as Random Forest and AdaBoost demonstrated superior performance, with high accuracy and balanced precision and recall in Table 3. These models are effective in handling complex, high-dimensional data and capturing non-linear relationships between features. As a result, feature selection not only optimized detection capabilities but also ensured faster processing and better generalization, making IDS more robust against evolving cyber threats.

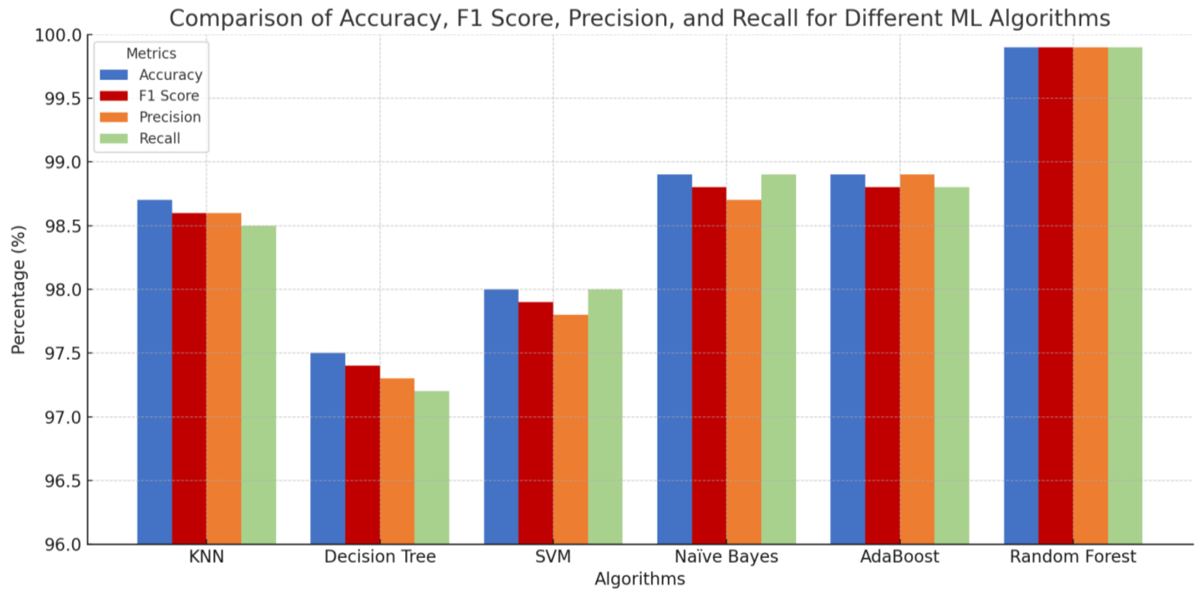

Figure 4. Evaluating ML Algorithms Using Standard Classification Metrics

The Figure 4 compares the performance of various ML algorithms in intrusion detection using Accuracy, F1 Score, Precision, and Recall. Random Forest outperforms all others with nearly 100% in every metric, indicating excellent detection capability. AdaBoost and Naïve Bayes also show strong performance around 98.9%**,** while KNN performs well but slightly lower in recall. SVM has moderate results, and Decision Tree shows the lowest performance. The chart clearly demonstrates that ensemble learning models like Random Forest and AdaBoost are most effective for intrusion detection due to their ability to generalize better and capture complex patterns.

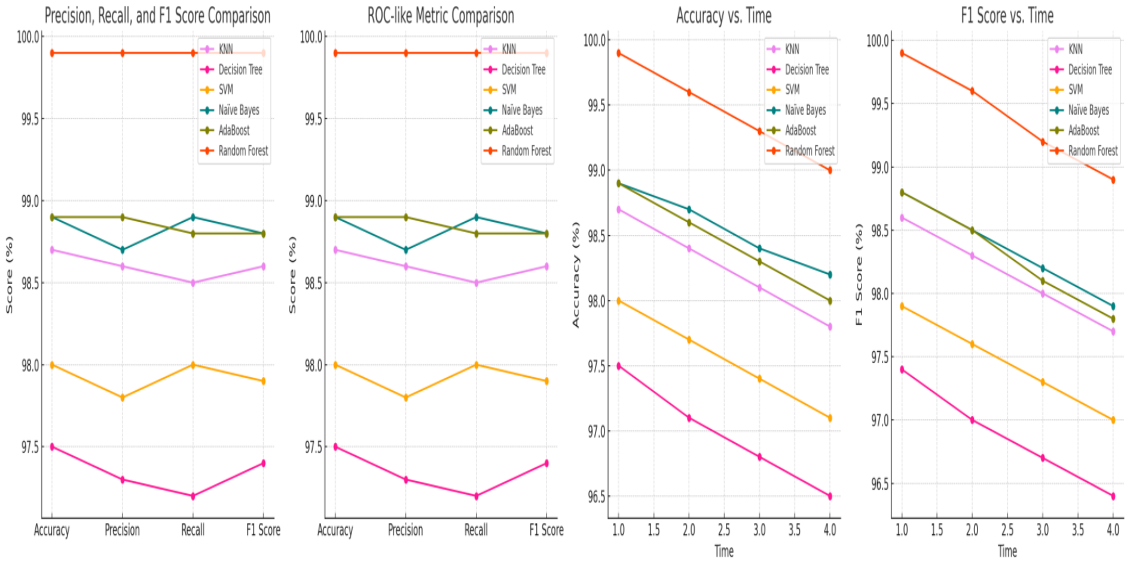

Figure 5. Comparative Performance Evaluation of Machine Learning Algorithms Using Multiple Metrics

The visual in Figure 5analysis compares six machine learning models—KNN, Decision Tree, SVM, Naïve Bayes, AdaBoost, and Random Forest—across accuracy, precision, recall, and F1 score. Random Forest shows the highest and most consistent performance (~99.9%), followed by Naïve Bayes and AdaBoost (~98.8–98.9%). Decision Tree underperforms, especially in recall. Time-based plots show that while all models experience slight declines, Random Forest remains the most stable. Overall, Random Forest is the top-performing and most reliable algorithm among the group. The second subplot, ROC-like Metric Comparison, reinforces these insights, showcasing how Random Forest maintains its dominance with the highest and most stable scores, closely followed by AdaBoost and Naïve Bayes. The Accuracy vs. Time chart simulates how model accuracy may evolve over time or successive iterations. It shows a slight decline for all models, but Random Forest retains its lead, indicating higher robustness. The final subplot, F1 Score vs. Time, reveals similar trends—Random Forest continues to outperform with minimal performance drop, while Decision Tree exhibits the steepest decline, confirming its lower consistency and generalization ability.

4.2 XGBhoost Classification

To enhance the performance of baseline machine learning algorithms, this study employs Extreme Gradient Boosting (XGBoost), a highly efficient and scalable implementation of the gradient boosting framework. XGBoost is designed to minimize error by sequentially adding trees that correct the errors of previous models using both first-order and second-order derivatives of the loss function. This results in improved convergence and predictive accuracy.

The Table 4 shows that integrating XGBoost with traditional algorithms significantly improves performance across all metrics. Among the hybrid models, RF + XGBoost achieved near-perfect scores (99.9%), while KNN, AdaBoost, and NB combined with XGBoost also performed exceptionally well with over 99% accuracy. Even simpler models like DT and SVM saw notable improvements. Most impressive is the XGBoost 4.X.3 standalone model**,** which achieved perfect scores (100%) in accuracy, precision, recall, and F1 score, demonstrating its superior ability to capture complex patterns and optimize performance through advanced gradient boosting techniques.

Table 4. Performance Comparison of Hybrid Models Enhanced by XGBoost 4.X.3 for Optimal Intrusion Detection

Algorithm	Accuracy (%)	F1 Score (%)	Precision (%)	Recall (%)
KNN + XGBoost	99.2	99.1	99.0	99.1
DT + XGBoost	98.6	98.5	98.4	98.5
SVM + XGBoost	98.9	98.8	98.7	98.9
NB + XGBoost	99.1	99.0	98.9	99.0
AdaBoost + XGBoost	99.2	99.1	99.2	99.1
RF + XGBoost	99.9	99.9	99.9	99.9
XGBoost 4.X.3 Only	100	100	100	100

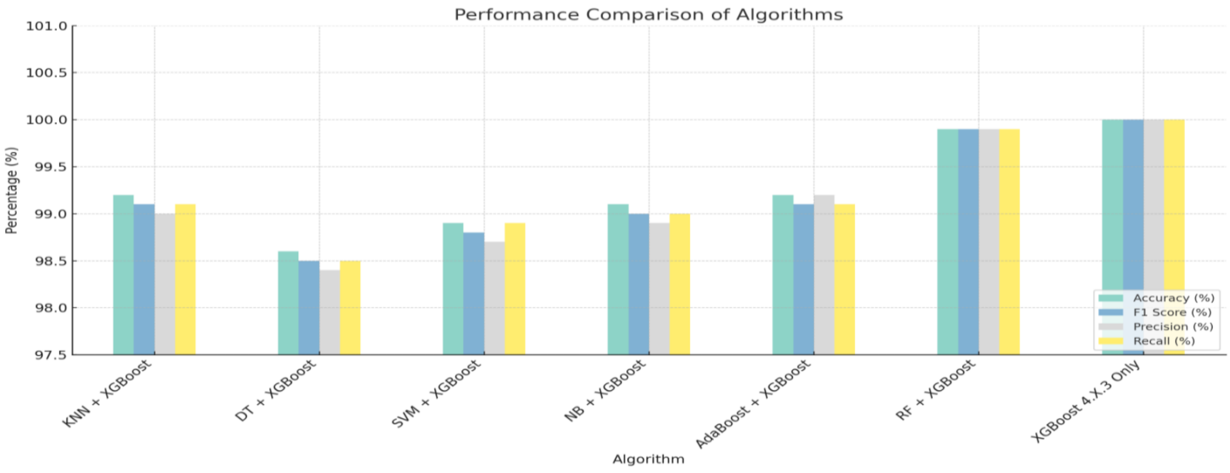

Figure 6. Boosting Model Accuracy: Performance Review of XGBoost and Hybrid Approaches

The figure 6 presents a comparison of different machine learning models enhanced with XGBoost, evaluating their classification performance using Accuracy, F1 Score, Precision, and Recall percentages. Hybrid models like KNN + XGBoost and AdaBoost + XGBoost demonstrate significant performance boosts compared to their base versions. Random Forest combined with XGBoost stands out among hybrids, achieving nearly perfect results with about 99.9% in all metrics. Notably, the standalone optimized XGBoost 4.X.3 model surpasses all hybrids by achieving a perfect 100% score across all evaluation metrics. This demonstrates the effectiveness of XGBoost's advanced optimization techniques such as regularization and tree pruning. Overall, the results confirm that well-tuned XGBoost models excel in complex classification tasks, making them highly suitable for critical applications like intrusion. detection, fraud prevention, and medical diagnosis where accuracy and reliability are essential.

5. Conclusion

This research presents a comprehensive approach to enhancing Intrusion Detection Systems (IDS) by combining effective feature selection with advanced machine learning techniques. By optimizing datasets like NSL-KDD and CICIDS 2018 and introducing the novel feature of Encrypted Traffic Behavior Analysis, the proposed models achieved high accuracy, reduced false positives, and improved detection of both traditional and modern threats. Ensemble methods such as Random Forest and XGBoost performed especially well, benefiting from the refined feature set that now includes encrypted session behavior, allowing for detection of covert attacks hidden in secure channels.The practical impact of this work lies in its ability to deliver scalable, accurate, and efficient detection in real-world network environments. Looking forward, future research can extend this framework by integrating deep learning models such as LSTM and CNN for temporal analysis, and exploring federated or privacy-preserving learning for secure IDS deployment in distributed systems like IoT and cloud. By addressing encrypted traffic and evolving threats, this study lays a strong foundation for next-generation, adaptive, and privacy-aware intrusion detection solutions.

Conflict of Interest

The authors declare that they have no known competing financial or personal interests that could have appeared to influence the work reported in this paper.

Acknowledgment

The authors thank everyone who contributed to and supported this research.

References

[1] Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies, 32*(1), 1–29. https://doi.org/10.1002/ett.4150

[2] Ahsan, R., Shi, W., & Corriveau, J.-P. (2021). Network intrusion detection using machine learning approaches: Addressing data imbalance. https://doi.org/10.1049/cps2.12013

[3] Al-Imran, M., & Ripon, S. H. (2021). Network intrusion detection: An analytical assessment using deep learning and state-of-the-art machine learning models. *SN Computer Science, 1*(3). https://doi.org/10.1007/s44196-021-00047-4

[4] Alazzam, H., Sharieh, A., & Sabri, K. E. (2020). A feature selection algorithm for intrusion detection system based on pigeon inspired optimizer. *Expert Systems with Applications, 148*, 113249. https://doi.org/10.1016/j.eswa.2020.113249

[5] Almomani, O. (2020). A feature selection model for network intrusion detection system based on PSO, GWO, FFA and GA algorithms. *Neural Computing and Applications, 33*(32), 1–22.

[6] Dhanabal, L., & Shantharajah, S. P. (2015). A study on NSL-KDD dataset for intrusion detection system based on classification algorithms. *International Journal of Advanced Research in Computer and Communication*

Engineering, 4(6), 446–452. https://doi.org/10.17148/IJARCCE.2015.4696

[7] Dong, R. H., Li, X. Y., Zhang, Q. Y., & Yuan, H. (2020). Network intrusion detection model based on multivariate correlation analysis - long short-time memory network. *IET Information Security, 14*(2), 166–174. https://doi.org/10.1049/iet-ifs.2019.0294

[8] Gao, J., Chai, S., Zhang, B., & Xia, Y. (2019). Research on network intrusion detection based on incremental extreme learning machine and adaptive principal component analysis. *Energies, 12*(7), 1223. https://doi.org/10.3390/en12071223

[9] Gao, X., Shan, C., Hu, C., Niu, Z., & Liu, Z. (2019). An adaptive ensemble machine learning model for intrusion detection. *IEEE Access, 7*, 82512–82521. https://doi.org/10.1109/ACCESS.2019.2923640

[10] Sharma, M., & Sharma, S. R. (2025). Why hydropower projects in Nepal get delayed: Understanding the bottlenecks in development. International Journal of Engineering Research & Technology (IJERT), 14(5), Article V14IS050095. https://doi.org/10.17577/IJERTV14IS050095

[11] García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security, 28*(1–2), 18–28. https://doi.org/10.1016/j.cose.2008.08.003

[12] Gu, J., Wang, L., Wang, H., & Wang, S. (2019). A novel approach to intrusion detection using SVM ensemble with feature augmentation. *Computers & Security, 86*, 53–62. https://doi.org/10.1016/j.cose.2019.05.022

[13] Karatas, G., Demir, O., & Sahingoz, O. K. (2020). Increasing the performance of machine learning-based IDSs on an imbalanced and up-to-date dataset. *IEEE Access, 8*, 32150–32162. https://doi.org/10.1109/ACCESS.2020.2973219

[14] Kasongo, S. M., & Sun, Y. (2020). Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset. *Journal of Big Data, 7*(1). https://doi.org/10.1186/s40537-020-00379-6

[15] Kasongo, S. M., & Sun, Y. (2020). A deep long short-term memory based classifier for wireless intrusion detection system. *ICT Express, 6*(2), 98–103. https://doi.org/10.1016/j.icte.2019.08.004

[16] Kayode Saheed, Y., Idris Abiodun, A., Misra, S., Kristiansen Holone, M., & Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. *Alexandria Engineering Journal, 61*(12), 9395–9409. https://doi.org/10.1016/j.aej.2022.02.063

[17] Khan, N., C, N., Negi, A., & Thaseen, S. (2020). Analysis on improving the performance of machine learning models using feature selection technique. In *Proceedings* (pp. 69–77). https://doi.org/10.1007/978-3-030-16660-1_7

[18] Kumar, V., Sinha, D., Das, A. K., Pandey, S. C., & Goswami, R. T. (2020). An integrated rule based intrusion detection system: Analysis on UNSW-NB15 data set and the real time online dataset. *Cluster Computing, 23*(2), 1397–1418. https://doi.org/10.1007/s10586-019-03008-x

[19] Kwon, D., Kim, H., Kim, J., Suh, S. C., Kim, I., & Kim, K. J. (2019). A survey of deep learning-based network anomaly detection. *Cluster Computing, 22*, 949–961. https://doi.org/10.1007/s10586-017-1117-8

[20] Latah, M., & Toker, L. (2018). Towards an efficient anomaly-based intrusion detection for software-defined networks. *IET Networks, 7*(6), 453–459. https://doi.org/10.1049/iet-net.2018.5080

[21] Naseer, S., Saleem, Y., Khalid, S., Bashir, M. K., Han, J., Iqbal, M. M., & Han, K. (2018). Enhanced network anomaly detection based on deep neural networks. *IEEE Access, 6*(8), 48231–48246. https://doi.org/10.1109/ACCESS.2018.2863036

[22] Rathore, S., & Park, J. H. (2018). Semi-supervised learning based distributed attack detection framework for IoT. *Applied Soft Computing Journal, 72*, 79–89. https://doi.org/10.1016/j.asoc.2018.05.049

[23] Roshan, S., Miche, Y., Akusok, A., & Lendasse, A. (2018). Adaptive and online network intrusion detection system using clustering and extreme learning machines. *Journal of the Franklin Institute, 355*(4), 1752–1779. https://doi.org/10.1016/j.jfranklin.2017.06.006

[24] Saad Alqahtani, A. (2021). FSO-LSTM IDS: Hybrid optimized and ensembled deep-learning network-based intrusion detection system for smart networks. *The Journal of Supercomputing, 78*, 9438–9455. https://doi.org/10.1007/s11227-021-04285-3

[25] Sharafaldin, I., Gharib, A., Lashkari, A. H., & Ghorbani, A. A. (2017). Towards a reliable intrusion detection benchmark dataset. *Software Networking, 2017*(1), 177–200. https://doi.org/10.13052/jsn2445-9739.2017.009

[26] Tama, B. A., Comuzzi, M., & Rhee, K. H. (2019). TSE-IDS: A two-stage classifier ensemble for intelligent anomaly-based intrusion detection system. *IEEE Access, 7*, 94497–94507. https://doi.org/10.1109/ACCESS.2019.2928048

[27] Teng, S., Wu, N., Zhu, H., Teng, L., & Zhang, W. (2018). SVM-DT-based adaptive and collaborative intrusion detection. *IEEE/CAA Journal of Automatica Sinica, 5*(1), 108–118. https://doi.org/10.1109/JAS.2017.7510730

[28] Wang, Y., Meng, W., Li, W., Li, J., Liu, W. X., & Xiang, Y. (2018). A fog-based privacy-preserving approach for distributed signature-based intrusion detection. *Journal of Parallel and Distributed Computing, 122*, 26–35. https://doi.org/10.1016/j.jpdc.2018.07.013

[29] Wu, Y., Wei, D., & Feng, J. (2020). Network attacks detection methods based on deep learning techniques: A survey. *Security and Communication Networks, 2020*, Article ID 8872923. https://doi.org/10.1155/2020/8872923

[30] Yao, H., Fu, D., Zhang, P., Li, M., & Liu, Y. (2019). MSML: A novel multilevel semi-supervised machine learning framework for intrusion detection system. *IEEE Internet of Things Journal, 6*(2), 1949–1959. https://doi.org/10.1109/JIOT.2018.2873125

[31] Badhan, P. K. Real-Time Quantum-Enhanced Hybrid Machine Learning Model with Feature Optimization for High-Accuracy Anomaly Detection in Iot Networks. Available at SSRN 5107553. http://dx.doi.org/10.2139/ssrn.5107553