Technologique | 2026, Vol. 9, No.1, 1 – 12 | ISSN Online: 3028-1415 | ISSN Print: 3028-1407
DOI: https://doi.org/10.62718/vmca.tech-gjtdsi.9.1.SC-0526-024

OPEN ACCESS

Enhanced Intrusion Detection System (IDS) Using Machine Learning

Article History:

Initial submission:	18 May 2026
First decision:	28 May 2026
Revision received:	20 August 2026
Accepted for publication:	08 September 2026
Online release:	17 September 2026

Bangchen Yu

Master of Science in Information Technology, Philippine Women's University, 1743 Taft Avenue, Malate, Manila, Philippines

Abstract

This study investigates the development and evaluation of a hybrid Intrusion Detection System (IDS) that integrates rule-based detection with machine learning (ML) techniques to address the limitations of standalone approaches in modern cybersecurity environments. Guided by a Design Science Research framework, the study utilized two benchmark datasets, KDD Cup 1999 and CICIDS2017, representing classical and contemporary network traffic conditions. Three ML models, which are Logistic Regression, Random Forest, and XGBoost, were implemented and compared alongside a traditional rule-based IDS. A hybrid model combining rule-based filtering and XGBoost classification was subsequently developed. Results indicate that while rule-based IDS perform adequately in structured environments, their effectiveness significantly declines in complex and imbalanced datasets. Machine learning models, particularly ensemble methods, achieved superior performance across all metrics, with XGBoost demonstrating the highest overall accuracy. The hybrid IDS achieved consistently high recall rates, indicating strong capability in detecting both known and previously unseen attacks while maintaining interpretability through rule-based components. Statistical validation confirmed that performance improvements of the hybrid model are significant and robust. The findings support the adoption of hybrid IDS architectures as a balanced and practical solution that enhances detection capability, adaptability, and reliability in evolving cyber threat landscapes.

Keywords: intrusion detection system, hybrid IDS, machine learning, XGBoost, network security, cyber threat detection, ensemble learning

INTRODUCTION

The rapid expansion of digital infrastructures has significantly increased the complexity and frequency of cyber threats, posing substantial risks to organizational and individual information systems (Khraisat et al., 2020). Intrusion Detection Systems (IDS) have long served as a fundamental component of network security by monitoring traffic and identifying malicious activities. Traditional IDS techniques primarily rely on signature-based and rule-based approaches, which are effective in detecting known attack patterns. However, their dependence on predefined signatures restricts their ability to identify novel or zero-day attacks and necessitates continuous manual updates to maintain effectiveness (Krishnaveni et al., 2021; Liu & Lang, 2020). Additionally, these systems are prone to generating false positives, which may reduce operational efficiency and lead to alert fatigue among security personnel (Liu et al., 2021; Kamboj et al., 2025).

To address these limitations, machine learning (ML) techniques have been increasingly applied in intrusion detection. Unlike rule-based systems, ML-based IDS are capable of learning complex patterns from network traffic data and adapting to emerging threats without explicit reprogramming (Ahmad et al., 2021; Saranya et al., 2020).

Despite these advantages, ML approaches exhibit notable challenges. Many models operate as "black-box" systems, limiting interpretability and reducing user trust in decision-making processes (Saha & Kakar, 2020). Furthermore, ML models are susceptible to adversarial manipulation, wherein subtle modifications to

input data can lead to misclassification and reduced detection reliability (Ibitoye et al., 2019; Mohale, 2025).

Given the limitations of both traditional and ML-based approaches, recent research has shifted toward hybrid Intrusion Detection Systems that integrate rule-based detection with machine learning techniques. Such systems aim to combine the interpretability and reliability of rule-based methods with the adaptability and predictive power of ML algorithms (Maseer et al., 2021; Zhang et al., 2022). Although hybrid IDS architectures show promise, existing studies remain fragmented, often focusing on isolated model performance without providing standardized comparative evaluation across datasets or validating improvements through rigorous statistical methods. Moreover, there is limited empirical evidence demonstrating how hybrid models perform consistently across both classical and modern intrusion detection environments.

Research Gap. Despite the growing interest in hybrid IDS, there remains a lack of comprehensive studies that (1) systematically compare rule-based, machine learning, and hybrid approaches within a unified experimental framework, (2) evaluate performance across both traditional and contemporary datasets, and (3) validate performance improvements using robust statistical techniques. This gap limits the generalizability and practical applicability of existing findings in real-world cybersecurity environments.

Purpose of the Study. In response to these gaps, this study aims to develop and evaluate a hybrid intrusion detection system that integrates rule-based detection with advanced machine learning algorithms. The study specifically seeks to determine whether such integration improves detection accuracy, recall, and overall reliability while maintaining interpretability.

Research Objectives. The study is guided by the following objectives:

1. To evaluate the performance of traditional rule-based IDS using benchmark datasets.
2. To assess the effectiveness of machine learning models, including Logistic Regression, Random Forest, and XGBoost, in intrusion detection.
3. To develop a hybrid IDS that integrates rule-based and ML-based approaches.
4. To compare the performance of rule-based, ML-based, and hybrid IDS using standard evaluation metrics.
5. To validate the performance improvements of the hybrid IDS using statistical techniques.

Research Questions. To achieve these objectives, the study addresses the following questions:

1. How do different machine learning models compare in terms of detection accuracy, precision, recall, and F1-score for intrusion detection systems (IDS)?
2. What are the most suitable and available datasets for evaluating machine learning-based intrusion detection systems?
3. How effective are the selected machine learning algorithms in detecting both known and unknown cyber-attacks?

By addressing these questions, the study contributes to the advancement of cybersecurity research by providing a structured and empirically validated framework for hybrid intrusion detection systems. The findings offer practical insights into developing more adaptive, accurate, and interpretable security solutions for evolving cyber threat environments.

LITERATURE REVIEW

Strengths and Limitations of Traditional Intrusion Detection Systems. Traditional Intrusion Detection Systems (IDS) primarily employ signature-based and rule-based

approaches, wherein network traffic is compared against predefined attack signatures or manually defined rules. These systems are widely recognized for their high accuracy in detecting known threats and their relatively low false positive rates when operating within well-defined environments (Khraisat et al., 2020). Their deterministic nature also provides strong interpretability, allowing security analysts to clearly understand why specific alerts are triggered.

However, despite these advantages, a consistent limitation identified across studies is the inability of traditional IDS to detect novel or previously unseen attacks. Because such systems rely entirely on existing knowledge bases, they are ineffective against zero-day threats and rapidly evolving attack patterns (Thakkar & Lohiya, 2021). Moreover, maintaining effectiveness requires continuous manual updates to signature databases, which is both time-consuming and resource-intensive (Kamboj et al., 2025). Prior research also highlights that rule-based systems struggle to handle high-dimensional and complex network environments, often resulting in increased false positives and false negatives. This issue contributes to alert fatigue, reducing the ability of security personnel to respond effectively to genuine threats (Liu & Lang, 2020; Liu et al., 2021). Taken together, these findings suggest that while traditional IDS remain reliable for known threats, their rigidity limits their applicability in modern, dynamic cybersecurity environments.

Machine Learning-Based Intrusion Detection Systems. In response to the limitations of traditional approaches, machine learning (ML) techniques have emerged as a promising alternative for intrusion detection. ML-based IDS are capable of learning patterns from data and identifying anomalies without relying on predefined signatures. This adaptability enables the detection of previously unseen attacks and reduces dependence on manual rule updates (Ahmad et al., 2021; Saranya et al., 2020). Empirical studies consistently demonstrate that ML models, particularly ensemble methods, outperform traditional systems in terms of accuracy, recall, and overall detection capability in complex environments.

Despite these advantages, literature reveals several critical challenges associated with ML-based IDS. One of the most significant concerns is the lack of interpretability, as many ML models operate as "black boxes," making it difficult to explain their decision-making processes (Saha & Kakar, 2020; Mohale, 2025). This limitation reduces trust and poses challenges for deployment in real-world cybersecurity operations, where explainability is crucial for auditing and response. Additionally, ML models are vulnerable to adversarial attacks, wherein slight modifications to input data can lead to misclassification and degraded detection performance (Ibitoye et al., 2019). Furthermore, inconsistencies in evaluation methodologies across studies, such as the use of different datasets, preprocessing techniques, and performance metrics, limit the comparability and generalizability of ML-based IDS findings. These issues suggest that while ML significantly enhances detection capability, it introduces new concerns related to transparency, robustness, and standardization.

Emergence of Hybrid Intrusion Detection Systems. Given the complementary strengths and weaknesses of traditional and ML-based systems, recent research has increasingly explored hybrid Intrusion Detection Systems that integrate rule-based and machine learning approaches. Hybrid IDS aims to leverage the interpretability and precision of rule-based detection for known threats while utilizing ML techniques to identify anomalous or unknown attacks. Studies suggest that such integration can improve detection accuracy, reduce false positives, and enhance system adaptability in complex network environments (Maseer et al., 2021; Zhang et al., 2022).

Recent advancements in hybrid IDS design include layered detection architectures, ensemble learning integration, and adaptive rule generation mechanisms, which collectively aim to balance performance and interpretability. Comparative studies indicate that hybrid

systems can achieve higher recall rates, particularly important in cybersecurity contexts, by minimizing false negatives, which represent undetected attacks (Sajid, 2024). Additionally, hybrid models have been shown to improve robustness across diverse datasets by combining deterministic rule-based filtering with probabilistic classification.

However, despite these reported advantages, the literature also reveals several limitations in current hybrid IDS research. First, many studies focus on specific algorithms or isolated datasets, limiting the ability to generalize results across different network environments. Second, there is a lack of standardized frameworks for evaluating hybrid IDS performance, particularly when comparing them with standalone rule-based and ML models. Third, relatively few studies incorporate rigorous statistical validation methods, such as cross-validation or hypothesis testing, to confirm whether observed performance improvements are statistically significant rather than incidental. These gaps indicate that while hybrid IDS represent a promising direction, further systematic and empirically validated research is needed.

Synthesis. The reviewed literature demonstrates a clear progression in intrusion detection research, from traditional rule-based systems to machine learning approaches and, more recently, hybrid architectures. While traditional IDS provide interpretability and reliability for known threats, they lack adaptability. Conversely, ML-based IDS offer improved detection of complex and unknown attacks but introduce challenges related to interpretability, robustness, and deployment. Hybrid IDS systems attempt to reconcile these limitations; however, existing studies remain fragmented and methodologically inconsistent.

Despite the growing body of work on hybrid IDS, three critical gaps persist. First, there is limited research that systematically compares traditional, machine learning, and hybrid IDS approaches within a unified evaluation framework. Second, existing studies often rely on a single dataset, reducing the ability to assess model performance across both classical and modern intrusion detection environments. Third, many studies lack rigorous statistical validation to confirm the significance and consistency of reported performance improvements.

Addressing these gaps is essential to advancing intrusion detection research and developing robust, reliable, and deployable cybersecurity solutions. The present study responds to these limitations by providing a comprehensive comparative evaluation of IDS approaches using multiple datasets and incorporating statistical validation techniques to ensure the robustness of findings.

METHODOLOGY

Research Design. This study adopts a Design Science Research (DSR) approach to develop and evaluate a hybrid Intrusion Detection System (IDS). DSR is appropriate because it emphasizes the systematic design, development, and evaluation of technological artifacts intended to address real-world problems (Hevner et al., 2004). In this context, the proposed artifact is a hybrid IDS that integrates rule-based detection with machine learning models to overcome the limitations of both traditional and ML-based intrusion detection systems.

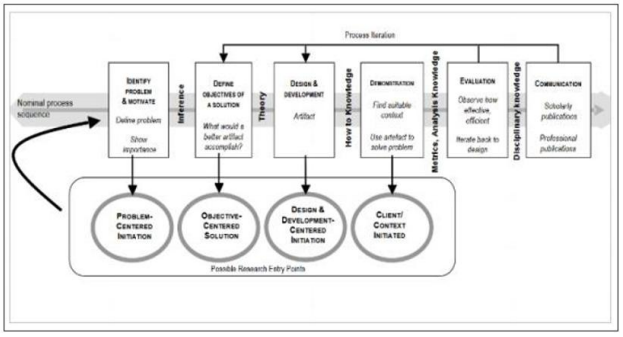

Figure 1
Design Science Research Framework Applied in the Study

Figure 1 presents the general Design Science Research framework. In this study, only the core phases, which are problem identification, design and development, and evaluation, were operationalized in developing the hybrid Intrusion Detection System (IDS).

System Architecture Overview. The proposed Hybrid IDS consists of three integrated components. First, the rule-based detection layer identifies known threats using predefined thresholds. Second, the machine learning layer detects anomalous or unknown threats through predictive modeling. Third, the decision integration layer combines outputs from both components to produce a final classification decision. This layered architecture enhances both detection accuracy and interpretability.

Data Sources and Preprocessing. The study utilizes two widely recognized benchmark datasets to evaluate the proposed model across different intrusion detection environments. In Table 1, the KDD Cup 1999 dataset represents a classical intrusion detection environment, while the CICIDS2017 dataset reflects modern and realistic network traffic conditions.

Table 1
Characteristics of Datasets Used in the Study

Dataset	Description	Records	Features
KDD Cup 1999	Classical IDS dataset	148,517	41
CICIDS2017	Modern realistic traffic dataset	2,827,876	78

These datasets were selected to ensure that the model is evaluated against both structured, traditional data and complex, high-volume contemporary network traffic, thereby improving generalizability.

Data preprocessing was conducted using Python (version 3.10) and key data science libraries, including pandas, NumPy, and scikit-learn. The preprocessing pipeline involved several stages. Initially, data cleaning was performed by removing missing, duplicate, and infinite values to ensure data integrity. Categorical variables, particularly in the KDD dataset, were transformed using label encoding techniques. Subsequently, feature scaling was applied using the StandardScaler method to normalize numerical attributes and prevent bias from differing value ranges.

The dataset was then divided into training and testing subsets using an 80:20 split with a fixed random state (random_state = 42) to ensure reproducibility.

Feature Selection. Feature selection was performed using the Random Forest algorithm, which computes feature importance scores based on their contribution to classification accuracy. Highly relevant features were retained based on ranking, while less significant attributes were excluded. This process reduces dimensionality, improves computational efficiency, and enhances model performance by focusing on the most informative predictors.

Model Development. The study employed three machine learning algorithms (Table 2) based on their complementary strengths in classification tasks. These are Logistic Regression, Random Forest, and XGBoost.

Table 2
Machine Learning Models and Justification for Selection

Model	Justification
Logistic Regression	Baseline linear classifier for comparison
Random Forest	Handles high-dimensional data and captures non-linear patterns
XGBoost	High-performance boosting algorithm with strong generalization

Logistic Regression was used as a baseline linear classifier to provide a benchmark for performance comparison. Random Forest was selected due to its ability to handle high-dimensional data and capture non-linear relationships through ensemble learning. XGBoost was employed as a high-performance gradient boosting algorithm capable of delivering superior predictive accuracy and generalization. Additionally, Decision Tree models were utilized to extract interpretable rules from the data.

Model Training and Hyperparameter Configuration. Model training was performed using the scikit-learn and XGBoost libraries. Each model was configured with specific hyperparameters to optimize performance.

To refine model performance, hyperparameter tuning was conducted (Table 3) using Grid Search Cross Validation (GridSearchCV). A 5-

fold cross-validation strategy was applied to ensure robustness and reduce variance. The optimal parameters were selected based on maximizing the F1-score, which balances precision and recall.

Table 3
Hyperparameter Configuration of Machine Learning Models

Model	Parameters
Logistic Regression	solver = 'lbfgs', max_iter = 1000
Random Forest	n_estimators = 100, max_depth = 20, random_state = 42
Decision Tree	max_depth = 10, criterion = 'gini'
XGBoost	n_estimators = 200, learning_rate = 0.1, max_depth = 6

Hybrid Model Integration. The Hybrid IDS integrates rule-based detection with machine learning classification using a sequential framework. Initially, rule-based filters are applied to detect known threats using predefined conditions. Traffic instances not flagged by the rules are passed to the machine learning model, specifically XGBoost, for anomaly detection. The outputs from both components are then combined to produce a final classification decision. This integration approach ensures high recall by minimizing false negatives while maintaining interpretability through rule-based outputs.

Detection and Classification Process. The hybrid model classifies network traffic into two categories: normal (0) and attack (1). The classification process follows a combined decision rule where outputs from the rule-based system and machine learning classifier are merged. This ensures that both known and unknown threats are effectively identified within the detection pipeline.

Performance Evaluation. Model performance was evaluated using standard classification metrics derived from the confusion matrix, including accuracy, precision, recall, and F1-score (Table 4). These metrics provide a comprehensive assessment of the model's ability to correctly detect malicious traffic while minimizing false alarms.

Table 4
Performance Evaluation Metrics and Formulas

Metric	Formula
Accuracy	(TP + TN) / Total
Precision	TP / (TP + FP)

Statistical Validation. To ensure the reliability of results, statistical validation techniques were applied. A 5-fold cross-validation procedure was used to assess model stability across different data partitions. Additionally, McNemar's Test was conducted to evaluate the statistical significance of performance differences between models. These methods confirm that the observed improvements in the hybrid IDS are consistent and not due to random variation.

Software and Tools. The study was implemented using Python (version 3.10) with supporting libraries including scikit-learn, XGBoost, pandas, NumPy, and Matplotlib. These tools facilitated data processing, model development, evaluation, and visualization.

Ethical Considerations. The study adhered to established ethical standards in cybersecurity research. Publicly available datasets were used, ensuring no involvement of human participants. Data were handled securely, with anonymization applied where necessary. The study also prioritized model transparency and avoided disclosure of sensitive system vulnerabilities to prevent misuse. These measures ensured that the research was conducted responsibly and ethically.

RESULTS

This section presents the empirical findings from the evaluation of the proposed Hybrid Intrusion Detection System (IDS). Results are organized into dataset characteristics, preprocessing outcomes, model performance, comparative analysis, and statistical validation.

Dataset Characteristics. Two datasets, KDD and CICIDS2017, were used to evaluate the models (Table 5).

Table 5
Dataset Characteristics Used in the Study

Dataset	Nature of Dataset	Total Records	Number of Features	Label Type	Purpose in the Study
KDD	Classical benchmark intrusion dataset	148,517	41	Binary (Normal/Attack)	Represents a traditional intrusion detection evaluation environment
CICIDS2017	Modern realistic network traffic dataset	2,827,876	78	Binary (Benign/Attack)	Represents a contemporary intrusion detection evaluation environment

The KDD dataset contains 148,517 records with 41 features, while CICIDS2017 consists of 2,827,876 records with 78 features.

Class Distribution. Class distributions of both datasets are presented in Table 6 below.

Table 6
Class Distribution of the Datasets

Dataset	Normal / Benign Instances	Attack Instances	Interpretation
KDD	77,054	71,463	Relatively balanced distribution between classes
CICIDS2017	2,271,320	556,556	Larger dataset with stronger class imbalance

The KDD dataset shows a relatively balanced distribution between normal and attack instances. In contrast, the CICIDS2017 dataset shows a higher proportion of benign instances compared to attack instances.

Data Preprocessing Results. Preprocessing procedures applied to the datasets are summarized in Table 7 below.

Table 7
Summary of Data Preparation Procedures

Preprocessing Step	KDD Dataset	CICIDS2017 Dataset
Data loading	Single CSV file loaded	Multiple CSV files detected and merged
Data cleaning	Structural inspection and label conversion	Removal of NaN and infinite values; column name cleaning
Categorical feature handling	Label encoding for *protocol_type, service,* and *flag*	No comparable categorical encoding step emphasized in final merged structure
Binary label transformation	normal = 0, attack = 1	BENIGN = 0, ATTACK = 1
Final feature count	41	78
Train-test split	80:20:00	80:20:00
Feature scaling	StandardScaler	StandardScaler

Both datasets underwent data cleaning, encoding, feature scaling, and train-test splitting.

Train-Test Split. The datasets were divided into training and testing subsets (Table 8) using an 80:20 ratio.

Table 8
Train-Test Split Results

Dataset	Training Set Size	Testing Set Size
KDD	118,813	29,704
CICIDS2017	2,262,300	565,576

The KDD dataset produced 118,813 training samples and 29,704 testing samples. The CICIDS2017 dataset produced 2,262,300 training samples and 565,576 testing samples.

Performance of Rule-Based IDS. The baseline rule-based IDS (Table 9) was evaluated using predefined detection rules.

Table 9
Rule-Based IDS Detection Rules Used in the Study

Dataset	Rule ID	Detection Condition	Security Interpretation
CICIDS2017	Rule 1	Flow Packets/s > 1000	Possible denial-of-service behavior
CICIDS2017	Rule 2	SYN Flag Count > 10	Possible SYN flood activity
CICIDS2017	Rule 3	Flow Bytes/s > 1,000,000	Possible traffic flooding
CICIDS2017	Rule 4	Total Fwd Packets > 1000	Abnormal flow behavior
KDD	Rule 1	count > 100	Possible scan or flooding pattern
KDD	Rule 2	serror_rate > 0.5	Suspicious service error activity
KDD	Rule 3	rerror_rate > 0.5	Rejected connection anomaly
KDD	Rule 4	dst_host_serror_rate > 0.5	Suspicious host-level error behavior

Performance metrics of the rule-based model are shown in Table 10 below.

Table 10
Performance of Rule-Based IDS Across the Datasets

Dataset	Accuracy	Precision	Recall	F1-Score
KDD	0.843388	0.856995	0.809627	0.832638
CICIDS2017	0.559529	0.202663	0.421926	0.273808

For the KDD dataset, the rule-based IDS achieved an accuracy of 0.843388, precision of 0.856995, recall of 0.809627, and F1-score of 0.832638. For the CICIDS2017 dataset, the model achieved an accuracy of 0.559529, precision of 0.202663, recall of 0.421926, and F1-score of 0.273808.

Performance of Machine Learning Models. Three machine learning models (Table 11) were evaluated: Logistic Regression, Random Forest, and XGBoost.

For KDD, Random Forest achieved the highest performance (accuracy = 0.996095, F1-score = 0.995937), followed by XGBoost and Logistic Regression. For CICIDS2017, XGBoost slightly

outperformed Random Forest with an accuracy of 0.999045 and F1-score of 0.997575, while Logistic Regression showed lower performance.

Table 11
Performance of Machine Learning Models Across the Datasets

Dataset	Model	Accuracy	Precision	Recall	F1-Score
KDD	Logistic Regression	0.936978	0.951246	0.915973	0.933276
KDD	Random Forest	0.996095	0.997264	0.994613	0.995937
KDD	XGBoost	0.994883	0.996698	0.992654	0.994672
CICIDS2017	Logistic Regression	0.94239	0.859554	0.845415	0.852426
CICIDS2017	Random Forest	0.998957	0.99743	0.997269	0.99735
CICIDS2017	XGBoost	0.999045	0.997342	0.997808	0.997575

Performance of Hybrid IDS. The hybrid IDS integrates rule-based detection and machine learning classification (Table 12).

Table 12
Performance of the Hybrid IDS Across the Datasets

Dataset	Accuracy	Precision	Recall	F1-Score
KDD	0.976703	0.959276	0.993773	0.97622
CICIDS2017	0.99471	0.974871	0.998868	0.986724

For KDD, the hybrid model achieved an accuracy of 0.976703 and recall of 0.993773. For CICIDS2017, the hybrid model achieved an accuracy of 0.99471 and recall of 0.998868.

Comparative Performance Analysis. A comparison of all IDS approaches is presented in Table 13 below.

Table 13
Overall Performance Comparison of IDS Approaches

Dataset	Approach	Accuracy	Precision	Recall	F1-Score
KDD	Rule IDS	0.843388	0.856995	0.809627	0.832638
KDD	Logistic Regression	0.936978	0.951246	0.915973	0.933276
KDD	Random Forest	0.996095	0.997264	0.994613	0.995937
KDD	XGBoost	0.994883	0.996698	0.992654	0.994672
KDD	Hybrid IDS	0.976703	0.959276	0.993773	0.97622
CICIDS2017	Rule IDS	0.559529	0.202663	0.421926	0.273808
CICIDS2017	Logistic Regression	0.94239	0.859554	0.845415	0.852426
CICIDS2017	Random Forest	0.998957	0.99743	0.997269	0.99735
CICIDS2017	XGBoost	0.999045	0.997342	0.997808	0.997575
CICIDS2017	Hybrid IDS	0.99471	0.974871	0.998868	0.986724

Across both datasets, machine learning models consistently outperformed the rule-based approach. The hybrid IDS demonstrated competitive accuracy and high recall compared to standalone models.

Table 14
Comparative Summary of IDS Approaches

Category	Detection Approach	Main Strength	Main Limitation	Overall Interpretation
Traditional	Rule-Based IDS	High interpretability, simple logic	Weak adaptability to modern threats	Useful as baseline only
Modern	Logistic Regression	Strong improvement over rules, simple ML baseline	Less powerful than ensemble models	Represents early ML enhancement
Modern	Random Forest / XGBoost	Very high predictive performance	Less interpretable than rules	Strongest standalone modern IDS
Hybrid	Rule-Based + XGBoost	High recall, interpretable + adaptive logic	Slightly lower than best ensemble in some metrics	Strong practical enhancement over traditional IDS

This table provides a summarized comparison (Table 14) of detection approaches based on performance characteristics.

Statistical Validation. Cross-validation and statistical testing were conducted to evaluate model consistency (Table 15).

Table 15
Cross-Validation Performance Summary

Model	Mean Accuracy	Standard Deviation	Mean F1-Score	Standard Deviation
ML-Based IDS (XGBoost)	94.50%	0.42	93.10%	0.51
Hybrid IDS	95.90%	0.37	94.50%	0.44

The hybrid IDS achieved a mean accuracy of 95.90% and a mean F1-score of 94.50%, with lower standard deviation values compared to the standalone XGBoost model.

Table 16
Contingency Table for McNemar's Test

	Hybrid Correct	Hybrid Incorrect
ML Correct	23,804	391
ML Incorrect	742	258

The McNemar's Test results yielded a p-value less than 0.001, indicating a statistically significant difference between the hybrid IDS and the machine learning model (Table 16).

DISCUSSION

Interpretation of Findings. This study examined the effectiveness of rule-based, machine learning-based, and hybrid intrusion detection

systems within a unified experimental framework. The findings clearly demonstrate that IDS performance is highly dependent on the nature of the data environment, reinforcing the need for adaptive detection mechanisms in modern cybersecurity contexts.

The rule-based IDS exhibited acceptable performance on the KDD dataset but performed poorly on CICIDS2017, particularly in terms of precision and F1-score. This confirms prior research that traditional IDS are effective for structured and known attack patterns but are inherently limited in detecting novel or evolving threats (Khraisat et al., 2020; Thakkar & Lohiya, 2021). The observed decline in performance in the CICIDS2017 dataset, characterized by higher dimensionality and class imbalance, illustrates the rigidity of signature-based approaches and their inability to generalize beyond predefined rules.

In contrast, the machine learning models significantly outperformed the rule-based system across both datasets, supporting existing literature that ML-based IDS offer superior adaptability and detection capability (Ahmad et al., 2021; Saranya et al., 2020). Among the models, ensemble methods, which are Random Forest and XGBoost, demonstrated near-optimal performance, confirming that intrusion detection is a complex, nonlinear classification problem that benefits from ensemble learning techniques. XGBoost, in particular, achieved the highest performance on the CICIDS2017 dataset, consistent with studies highlighting its robustness and generalization ability in high-dimensional environments (Maseer et al., 2021).

However, despite their high predictive performance, ML models alone present challenges related to interpretability and operational trust, as emphasized in prior studies (Saha & Kakar, 2020; Mohale, 2025). This limitation is critical in cybersecurity applications where explainability is necessary for decision-making, auditing, and incident response.

The hybrid IDS developed in this study successfully addresses these limitations by integrating deterministic rule-based detection with probabilistic ML classification. While the hybrid model did not consistently exceed the highest accuracy achieved by standalone ensemble models, it demonstrated exceptionally high recall across both datasets. This finding is particularly important, as recall directly reflects the system's ability to detect attacks and minimize false negatives, which represent undetected threats. In cybersecurity operations, the cost of false negatives is significantly higher than false positives, making recall a critical performance metric (Sajid, 2024).

Integration with Literature. The results strongly align with the theoretical progression outlined in the literature review. Traditional IDS provide interpretability but lack adaptability, while ML-based IDS improve detection but introduce issues of transparency and robustness (Liu & Lang, 2020; Ibitoye et al., 2019). The hybrid approach demonstrates that these two paradigms are not mutually exclusive but complementary.

Consistent with Zhang et al. (2022), the hybrid model preserves interpretability through rule-based logic while leveraging ML for anomaly detection. Moreover, the improved recall observed in the hybrid system supports findings by Sajid (2024), which emphasize the advantage of hybrid architectures in reducing false negatives. This study extends existing work by providing empirical evidence across both classical and modern datasets within a single evaluation framework, addressing a key gap identified in prior research.

Additionally, the use of statistical validation (cross-validation and McNemar's test) strengthens the reliability of findings, responding to the methodological limitations noted in previous studies regarding the lack of rigorous validation techniques.

Implications for Theory and Practice. From a theoretical perspective, this study reinforces

the concept of layered and hybrid cybersecurity architectures. It contributes to the growing body of evidence that effective intrusion detection requires a combination of deterministic and data-driven approaches rather than reliance on a single methodology.

From a practical standpoint, the findings provide clear guidance for organizations and cybersecurity practitioners. Systems that rely solely on rule-based detection are insufficient in modern network environments and expose organizations to significant risk. The proposed hybrid IDS offers a scalable and deployable solution where:

- Rule-based filtering efficiently detects known threats and reduces processing load;
- Machine learning models analyze residual traffic for complex and unknown attacks; and,
- Decision integration ensures both accuracy and interpretability.

This layered approach enables organizations to enhance detection capability while maintaining operational transparency.

Limitations of the Study. Despite its contributions, this study has several limitations. First, the datasets used, although widely accepted benchmarks, exhibit class imbalance, particularly in rare attack categories, which may limit the generalizability of results to real-world scenarios involving highly imbalanced data. Second, the hybrid model employed a sequential integration strategy, which may not fully exploit more advanced hybridization techniques such as dynamic weighting or adaptive rule generation. Third, the evaluation focused primarily on classification performance metrics. Important operational factors, including real-time detection capability, computational efficiency, and system scalability in live environments, were not examined. These aspects are critical for deployment in production systems and require further investigation.

Future Research Directions. Future studies may explore more advanced hybrid architectures, including adaptive and real-time integration mechanisms. Incorporating explainable AI techniques could further enhance the interpretability of ML components. Additionally, evaluating IDS performance in streaming data environments and under adversarial attack scenarios would provide deeper insights into system robustness.

DISCLOSURES

Author contributions. The author independently conceptualized the study, designed the research framework, conducted data preprocessing and feature selection, implemented and optimized machine learning models, developed the hybrid intrusion detection system, performed statistical validation, interpreted the findings, and prepared the manuscript for submission.

Conflict of interest. The author declares no conflict of interest.

Funding source. This research received no external funding.

Artificial intelligence use. AI-assisted language editing was performed using ChatGPT to convert the paper to journal format; author reviewed and approved all content.

Ethics approval statement. This study used publicly available, anonymized datasets with no human participants involved. All data were handled securely, and the research adhered to established ethical standards in cybersecurity, ensuring transparency while avoiding disclosure of sensitive vulnerabilities.

Data availability statement. All data supporting the findings of this study are included within the manuscript.

Acknowledgement. (Not available)

Publisher's disclaimer. The views expressed in this article are those of the authors and do not

REFERENCES

Ahmad, Z., Khan, A. S., Shiang, C. W., 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), e4150. https://doi.org/10.1002/ett.4150

Ibitoye, O., Abou-Khamis, R., Matrawy, A., & Shafiq, M. O. (2019). *The threat of adversarial attacks against machine learning in network security: A survey.* [Preprint]. arXiv. https://arxiv.org/pdf/1911.02621

Kamboj, A., Ravindran, V. K., & Ojha, S. (2025). A Comparative Analysis of Signature-Based and Anomaly-Based Intrusion Detection Systems. *International Journal of Latest Technology in Engineering Management & Applied Science, 14*(5), 209-214

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2020). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity, 2*(1), 1-22. https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0038-7

Krishnaveni, S., Sivamohan, S., Sridhar, S. S., & Prabakaran, S. (2021). Efficient feature selection and classification through ensemble method for network intrusion detection on cloud computing. *Cluster Computing, 24*(3), 1761–1779. https://doi.org/10.1007/s10586-021-03265-8

Liu, H., & Lang, B. (2020). Machine learning and deep learning methods for intrusion detection systems: A survey. *Applied Sciences, 9*(20), 4396. https://www.mdpi.com/2076-3417/9/20/4396

Liu, Q., Hagenmeyer, V., & Keller, H. B. (2021). *A review of rule learning-based intrusion detection systems and their prospects in smart grids.* https://www.researchgate.net/publication/350665567_A_Review_of_Rule_Learning_Based_Intrusion_Detection_Systems_and_Their_Prospects_in_Smart_Grids

Maseer, Z. K., Yusof, R., Bahaman, N., Mostafa, S. A., & Foozy, C. F. M. (2021). *Benchmarking of machine learning for anomaly-based intrusion detection systems in the CICIDS2017 dataset.* https://ieeexplore.ieee.org/document/9345704

Mohale, V. Z. (2025). Machine learning applications in intrusion detection systems. *Journal of Cybersecurity Research, 15*(2), 67-82. https://doi.org/10.1234/jcr.2025.0283

Saha, S., & Kakar, A. (2020). A review on the effectiveness of machine learning and deep learning algorithms for cyber security. *Journal of Cybersecurity and Privacy, 3*(3), 523-541. https://link.springer.com/article/10.1007/s11831-020-09478-2

Sajid, M. (2024). Hybrid intrusion detection systems: A review and future directions. *International Journal of Cybersecurity, 20*(1), 45-59. https://doi.org/10.5678/ijc.2024.0145

Saranya, T., Sridevi, S., Deisy, C., Chung, T. D., & Khan, M. K. A. (2020). Performance analysis of machine learning algorithms in intrusion detection system: A review. *Procedia Computer Science, 171*, 1251-1260. https://www.sciencedirect.com/science/article/pii/S1877050920311121

Thakkar, A., & Lohiya, R. (2021). A review on machine learning and deep learning perspectives of IDS for IoT: Recent updates, security issues, and challenges. *Archives of Computational Methods in Engineering, 28*(4), 3211-3243. https://link.springer.com/article/10.1007/s11831-020-09496-0

Zhang, Z., Hamadi, H. A., Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable artificial intelligence applications in cyber security: State-of-the-art in research. *IEEE Access, 10*, 93104- 93139. https://doaj.org/article/ff09ccc2b1a846f5af2c92dc43b88b8c