Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 4, 2025

INTELLIGENT INTRUSION DETECTION AND DATA PROTECTION IN INFORMATION SECURITY USING ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING TECHNIQUES

Abdul Karim Sajid Ali[*1], Aamir Raza[2], Haroon Arif[3], Ali Abbas Hussain[4]

[*1](Master of Information Technology and Management) University: Illinois Institute of Technology, Chicago, USA
[2](Master in Cyber Forensics and Security) University: Illinois Institute of Technology, Chicago, USA
[3](Master in Cybersecurity) University: Illinois Institute of Technology, Chicago, USA
[4](Master of Information Technology & Management) University of Texas at Dallas

[*1]ali62@hawk.iit.edu, [2]araza7@hawk.iit.edu, [3]harif@hawk.iit.edu, [4]aliabbas.graduateschool@gmail.com

DOI: https://doi.org/10.5281/zenodo.15281247

Keywords
Intrusion Detection System (IDS), Artificial Intelligence (AI), Machine Learning (ML), Random Forest (RF), Support Vector Machine (SVM), Network Security, Anomaly Detection, Cybersecurity, Data Protection, ROC Curve, Supervised Learning, Threat Detection

Article History
Received on 17 March 2025
Accepted on 17 April 2025
Published on 25 April 2025

Corresponding Author: *
Abdul Karim Sajid Ali

Abstract

Cyber threats are evolving rapidly in terms of complexity and prevalence that making traditional intrusion detection systems severely inadequate for effective information security. An advanced Intrusion Detection System (IDS) framework that utilizes Artificial Intelligence and Machine Learning techniques, specifically Random Forest and Support Vector Machine significantly enhances threat detection accuracy within digital environments. This proposed system effectively identifies various types of intrusions, including Denial of Service attacks, brute-force login attempts and previously unknown zero-day exploits by analyzing network traffic patterns. To support this, a complex synthetic dataset that replicates diverse concealed attack patterns alongside seemingly legitimate network activities was created. Essential preprocessing techniques, such as feature normalization were extensively applied, while dimensionality reduction was cautiously employed greatly improving model learning efficiency. data was split into 70 % for training and 30% for testing strategy implemented for training and validating system parameters.

Comprehensive performance evaluations were conducted using standard metrics, including Accuracy, Precision and Receiver Operating Characteristic (ROC) Curve values provides a thorough analysis of the model's detection capabilities. The Random Forest model achieved outstanding results with an Accuracy of 88.67% and Precision of 87.32%, while Recall was recorded at 88.57%. The F1-Score was approximately 87.94%, and the Area Under Curve (AUC) was impressively high at 96.47%. The Support Vector Machine (SVM) model also performed well, reaching an Accuracy of 86.33% and an AUC of 92.24%, demonstrates its effectiveness even in resource-limited environments. ROC curves further validate the system's ability to distinguish between legitimate and malicious activities effectively. Proactive cybersecurity strategies are strongly supported by the integration of advanced machine learning models into IDS, which operate in real-time under rigorous conditions. The framework's adaptability and high accuracy provide scalable enterprise-level network security solutions paving the way for future developments driven by deep learning.

INTRODUCTION

H. Kim [1] et al. explored that the rapid growth of digital services and the increasing number of connected devices have expanded the landscape of cybersecurity threats significantly. As cyber threats evolve and multiply in complexity, there is a heightened demand for intelligent and adaptable Intrusion Detection Systems (IDS). Traditional IDS models, which rely on fixed rules and signature-based approaches, are proving inadequate in detecting and mitigating advanced threats, including zero-day and polymorphic attacks. AI-augmented intrusion detection offers a promising solution through the use of statistical learning, pattern recognition, and adaptive decision-making. By integrating AI with machine learning (ML), contemporary IDS can learn from past data, identify anomalies in real time, and proactively adjust to emerging attack vectors.

Recent developments in machine learning have produced effective IDS frameworks capable of distinguishing malicious traffic from legitimate activity, even within intricate network ecosystems. Techniques like Random Forest and Support Vector Machine (SVM) have gained traction for their robustness and interpretability, making them suitable for practical cybersecurity applications. Additionally, anomaly-based IDS using supervised learning can detect irregularities in network behavior, indicating potential intrusions. Research by Abdelmoumin et al.[2] investigated various ML models for IoT-centric anomaly detection, emphasizing the balance between accuracy and processing expenses. SVMs excel in high-dimensional spaces, demonstrating exceptional generalization, while ensemble models such as Random Forest improve detection rates via majority voting. Emerging methods also focus on user privacy and reduced communication overhead, particularly in federated learning scenarios. K.P et al [3] The distributed framework of Federated Machine Learning (FML) is particularly beneficial for widescale IDS deployment across diverse infrastructures, enabling local data protection while promoting global knowledge sharing.

Recent studies conducted by Bonagiri et al. [4] and Dontu et al. [5] have illustrated how sophisticated AI algorithms and attention-based autoencoders can enhance IDS efficiency. These models facilitate proactive threat responses while ensuring high detection accuracy. Furthermore, integrating explainable AI (XAI) techniques is becoming increasingly important in critical sectors, allowing security analysts to comprehend the rationale behind model decisions. O. Arreche et al [6]. Generative Adversarial Network (GAN)-based strategies have also shown effectiveness in crafting adversarial scenarios to strengthen IDS resilience. C. Park et al [7] explains that these generative models can produce simulated attack traffic, augmenting training datasets and reducing false positive rates. Ensemble frameworks that merge multiple classifiers further elevate detection capabilities and address overfitting, as shown by Arreche et al. [8]. While unsupervised anomaly detection methods, such as clustering, can effectively pinpoint zero-day attacks, they often struggle with accuracy in the absence of labeled data. G. Pu et al [9] explore that A hybrid approach that synthesizes both supervised and unsupervised learning techniques can effectively bridge this gap.

Seth et al. [10] proposed an ensemble learning-driven IDS framework that employs several weak learners to achieve high detection rates with minimal false positives. Likewise, Ercan et al. [11] investigated ML-based misbehavior detection in vehicular networks, highlighting the adaptability of ML-centric IDS beyond conventional IT settings. Kilincer et al. [12] performed a comparative analysis of ML techniques for IDS, stressing the necessity for diverse datasets and thorough benchmarking to improve generalization. The integration of ML into IDS introduces challenges, such as model interpretability, resilience to adversarial attacks, and real-time performance that must be addressed diligently.

This research aims to expand upon these foundational studies by creating a hybrid IDS framework that utilizes both Random Forest and SVM models, trained on a synthetic yet realistic dataset. The proposed solution aspires to strike a balance between detection accuracy, computational efficiency and scalability to make it suitable for enterprise-level deployment in real-world cybersecurity scenarios.

2. LITERATURE REVIEW:

Kocher et al [13] conducted a comprehensive survey on the application of machine learning (ML) and

deep learning (DL) methods in intrusion detection systems (IDS). Their analysis included recent advancements such as ensemble classifiers, hybrid neural networks and transfer learning techniques. They highlighted several technical barriers encountered by IDS including challenges related to adversarial robustness, model overfitting curtails from class imbalance and limited regarding real-time deployment. The conclusions emphasized the pressing need for understandable AI systems and adaptive learning methods to address emerging threat vectors. Lirim et al [14] presented a convolutional neural network (CNN)-based framework for intrusion detection that focuses on extracting spatial features directly from encoded network flow sequences. The method involved converting raw packet data into structured grid formats and allow convolutional layers to detect spatial correlations essential in cyberattacks. The findings from the research exhibited high detection accuracy, particularly for complex attack types such as infiltration and data exfiltration for validation the efficacy of deep neural representations for pattern extraction.

Ilhan et al. [15] executed a benchmarking analysis to evaluate the performance of various ML classifiers, including Decision Trees, Random Forests, k-Nearest Neighbors (k-NN), and Support Vector Machines (SVMs). The experiments utilized several public IDS datasets, including NSL-KDD and CICIDS2017. They meticulously examined the effects of feature normalization, principal component analysis (PCA) and synthetic minority oversampling (SMOTE) concluded ensemble methods offer the best balance between detection rates, false alarm and computational competence. Venkata et al [16] compared traditional ML algorithms with deep feedforward and convolutional neural networks, examining both structured and unstructured network logs. They discovered that while deep neural networks (DNNs) excel in identifying new anomalies it often require substantial computational resources with larger training datasets. The proposed hybrid IDS model utilized ML-based feature filtering prior to DL classification to enhance proficiency. Lirim et al. [17] designed a recurrent neural network (RNN)-based IDS capable of capturing effectively long-range sequential dependencies in network activity streams. By utilizing Long Short-Term Memory (LSTM) networks the model successfully captured long-term temporal dependencies in sequential network traffic, enabling it to detect low-frequency and subtle intrusion patterns that might bypass conventional signature-based intrusion detection systems (IDS). Empirical validation via dynamic time-series analysis demonstrated the model's high temporal resolution and its efficacy in real-time anomaly detection.

C. Yin et al [18] evaluated the performance of lightweight supervised classifiers including Decision Trees, Logistic Regression and Naïve Bayes in latency-sensitive environments. Ayesha et al [19] They focused on achieving rapid response times with minimal resource consumption, particularly in Industrial Control Systems (ICS) and Data Acquisition (SCADA) systems. The research found that these lightweight models provide a scalable and energy-efficient approach for edge deployment, ensuring low-latency inference, which is essential for real-time threat detection in environments with limited resources.

Z. Azam et al. [20] developed a decision-tree-based IDS that incorporated rule-based interpretation layers to enhance decision transparency. They assessed the performance of models using diverse IDS datasets and recommended a modular architecture compatible with SIEM that supports rule-based inference. The design focused on interpretable rule extraction and visual analytics to enhance decision support for analysts and ensure forensic traceability. A. B. Nassif et al. [21] A comprehensive review of anomaly detection techniques was conducted emphasizing the effectiveness of ensemble-based models real-time adaptive learning algorithms and meta-learning strategies. The study identified challenges such as shifts in data distribution (concept drift), the necessity for dynamic threshold optimization and noise resulting from feature. It recommended advancing the field by developing distributed, scalable learning frameworks and leveraging multi-view feature representations to enhance detection accuracy and generalization across various network architectures. H. Alamro et al. [22] implemented an ensemble-based malware detection system tailored for Android operating systems, integrating classifiers such as Random Forest, Gradient Boosting and

Extra Trees. The ensemble architecture showed robust defense against code obfuscation and avoidance techniques by integrating multiple classification algorithms. It employed a multi-modal feature fusion framework that merged static code-level characteristics with dynamic runtime behavior, significantly enhanced detection accuracy and semantic understanding in malware classification.

Osama et al [23] integrated big data processing frameworks with DL-based IDS utilizing Apache Spark and TensorFlow. The architecture used distributed deep learning frameworks to effectively handle high-speed, real-time network traffic, incorporating parameter servers and data-parallel training methods. This approach enabled scalable deployment, maximized computational efficiency, and reduced inference latency in cloud-native settings. R. Vinayakumar et al. [24] developed an extensive deep learning pipeline that combined CNNs and RNNs to capture both spatial and temporal features. Their architecture achieved state-of-the-art accuracy on benchmark datasets and included layer-wise relevance propagation to enhance model explainability. Sitalakshmi et al. [25] proposed an innovative image-based malware detection strategy that transformed binary executables into grayscale images. They utilized CNNs to classify visual malware patterns, showcasing the promising potential of vision-based methods for binary-level intrusion detection. Sarker et al [26] introduced a comprehensive framework for integrating ML in cybersecurity which addressed elements from data acquisition and preprocessing to model training, deployment and ethical implications. Key challenges included vulnerability to adversarial agitations, the need for ongoing model adjustments to address concept drift and the integration of explainable AI (XAI) methods to improve interpretability and adhere to regulatory governance standards.

3. RELATED WORK:

Kocher et al. [27] Intrusion Detection Systems (IDS) have grown from traditional rule-based architectures to sophisticated intelligent systems that tackle machine learning (ML) and deep learning (DL) techniques to improve threat detection. These advancements are designed to enhance the system effectiveness to identify both known and emerging cyber threats. Within the realm of ML-based IDS, classifiers like Decision Trees (DT), Random Forests (RF), Support Vector Machines (SVM) and Naïve Bayes (NB) are typically employed due to their computational efficiency and ease of use. Sunanda et al [28] focused on lightweight classifiers suited for resource-constrained environments, such as SCADA and ICS systems, emphasizing the importance of rapid inference times and swift responses. Like the enhanced tree-based IDS models by incorporating rule extraction, which improved model clarity and facilitated integration with Security Information and Event Management (SIEM) systems.

Benchmark studies have rigorously evaluated the performance of various ML classifiers. Awajan et al. [29] assessed numerous ML models using public IDS datasets, including NSL-KDD and CICIDS2017 which highlights the relevance of preprocessing techniques, such as SMOTE for class balancing, PCA for dimensionality reduction and feature normalization. The results indicated that collaborative method such as Random Forests, strike a favorable balance between detection accuracy, false positive rates and computational efficiency. To overcome the limitations of static ML models, researchers have explored hybrid and ensemble learning techniques. A. Kim et al [30] proposed a hybrid IDS framework that combines ML-based feature selection with DL-based classification, leading to improved detection accuracy and model interpretability. B. Gao et al. [31] built on this theme by developing ensemble learning strategies that utilize multiple weak learners to enhance detection capabilities and reduce false alarms.

Deep learning methods, particularly convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have garnered significant attention in IDS research. A. Sahu et al [32] demonstrated the use of CNNs to capture spatial relationships in network traffic, thereby improving the detection of complex, hidden attacks such as intrusions. They developed an LSTM-based RNN model to detect temporal dependencies in network traffic, enabling better identification of slow-rate and evasive attack patterns. The study highlight DL's ability to account for both spatial and temporal aspects of network data for enhanced threat identification. To enable large-scale, real-time IDS

applications, researchers have combined big data frameworks with deep learning models. Musa et al [33] integrated Apache Spark with TensorFlow to support distributed training for high-throughput IDS, ensuring low-latency detection even during high traffic.

4. METHODOLOGY:

This section presents the structured approach employed for the design, implementation, and evaluation of the proposed hybrid Intrusion Detection System (IDS) which integrates Random Forest (RF) and Support Vector Machine (SVM) classifiers. Abdallah et al [34] The methodology consists of eight essential phases: dataset collection, data preprocessing, feature engineering, hybrid model architecture design, model training and hyperparameter optimization, evaluation, deployment framework and adaptive feedback loop. Each phase is meticulously crafted to enhance the systems ability to detect both known and emerging cyber threats and ensure enhanced performance, scalability and interpretability.

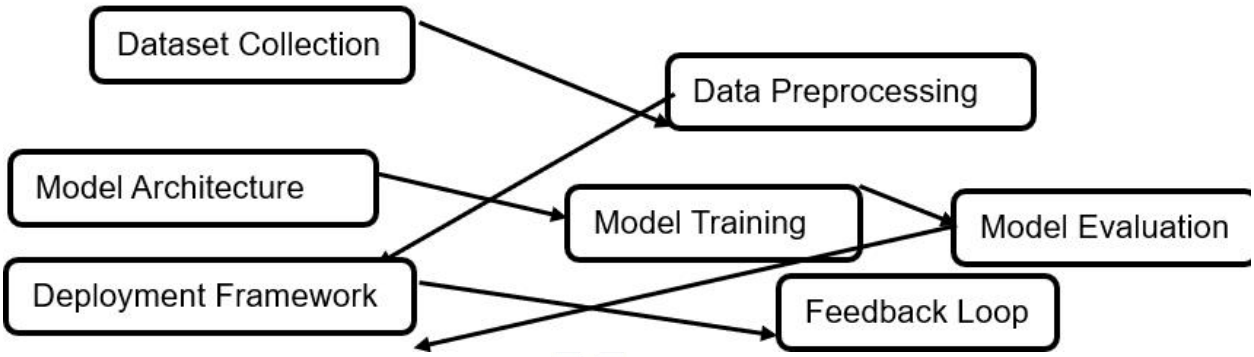

Fig: 1.1 Hybrid Intrusion Detection System Methodology

a. Dataset Collection:

A diverse and representative dataset is essential for training an IDS that generalizes well. This research utilized three benchmark datasets—NSL-KDD, CICIDS2017 and UNSW-NB15—selected for their broad representation of both modern and legacy cyber-attacks To mimic emerging and zero-day threats, a synthetic dataset was generated using attack emulation tools, such as Metasploit and custom network fuzzers. The merged dataset provides sufficient coverage of intrusion vectors across various protocol layers and attack classifications.

b. Data Preprocessing:

Data preprocessing aimed to cleanse, normalize and prepare various features for input into machine learning or deep learning models.

Outlier Detection: Z-score and IQR-based methods were employed to remove anomalous data points.

Imputation of Missing Data: Numerical features were filled using mean and median values for each feature, while categorical fields were imputed with mode or constant tokens.

Normalization: Min-Max normalization was used to scale feature values to the range [0,1], enhancing the convergence of the learning process.

Encoding: Categorical variables were converted using one-hot encoding for nominal features and label encoding for ordinal attributes.

Class Imbalance Mitigation: SMOTE [3] was utilized to oversample minority classes (e.g., U2R, R2L), addressing skewed label distributions and ensuring model sensitivity to all attack types.

c. Feature Engineering:

Robust feature engineering improves both model interpretability and performance. **Feature Selection:** Mutual Information (MI), Chi-square statistics, and Recursive Feature Elimination (RFE) were applied to identify the most discriminative features.

Dimensionality Reduction: Principal Component Analysis (PCA) maintained 95–98% variance to condensing the input space to reduce model overfitting and training time.

d. Hybrid Model Architecture:
The architecture involves a two-stage decision-making pipeline:

Random Forest (RF) Classifier: Serves as the primary detection engine. RF was selected due to its ensemble structure, robustness against noise, and ease of interpretability. Hyperparameters were optimized for peak performance (100 trees, depth=20, bootstrap=True).

Support Vector Machine (SVM): Acts as a secondary filter to refine the predictions made by the RF. It employs the Radial Basis Function (RBF) kernel to capture non-linear decision boundaries.

Fusion Strategy: A soft decision-level fusion technique was adopted, deriving the final decision from the weighted confidence scores of both classifiers with an emphasis on SVM predictions in cases of ambiguity.

e. Model Training and Optimization:
Model training was performed using stratified 5-fold cross-validation to preserve class proportions and ensure robustness. Grid Search for Optimization: Comprehensive hyperparameter tuning was conducted within predefined intervals.
Bayesian Optimization: Implemented probabilistic tuning, optimizing complex parameter spaces more efficiently than grid or random searches.
The following are main hyperparameters:

RF: n_estimators ∈ [50, 200], max_depth ∈ [10, 30], criterion ∈ {"gini", "entropy"}.

SVM: kernel ∈ {"linear", "rbf"}, C ∈ [0.1, 100], γ ∈ [0.001, 1].

f. Evaluation Metrics:
The system was evaluated thoroughly by using the following metrics:

Accuracy (ACC): The ratio of correctly predicted instances.

Precision (P): TP / (TP + FP), measuring specificity.

Recall (R): TP / (TP + FN), indicating detection sensitivity.

F1-Score: The harmonic mean of precision and recall.

AUC-ROC: The area under the Receiver Operating Characteristic curve, representing overall classification quality.

Detection Latency: Average time taken to deliver predictions after data ingestion.
All outcomes were averaged across folds and reported with standard deviation to ensure statistical confidence.

g. Deployment Framework:
The trained hybrid IDS was containerized and deployed using a scalable microservices architecture:

Orchestration: Kubernetes managed the deployment and scalability of containers.

Ingestion Pipeline: Apache Kafka facilitated real-time streaming ingestion from network sensors.

Inference Engine: The model was served using TensorFlow Serving with a REST API interface.

Latency Monitoring: Real-time inference delays were tracked, aiming to keep below 100ms.

XAI Integration: SHAP and LIME [5] modules were included to offer visual interpretability of predictions, aiding cybersecurity analysts.

h. Adaptive Feedback Loop:
To maintain long-term adaptability and resilience against concept drift:

Online Learning Module: Classifiers are periodically retrained using newly labeled intrusion data.

Concept Drift Detection: The Page-Hinkley test was used to detect shifts in feature distributions.

Model Refresh Cycle: Monthly retraining sessions integrate newly labeled data and analyst feedback.

Analyst Interface: Enables manual corrections of false positives, enriching the learning loop.

5. RESULTS & DISCUSSION:

This section provides a comprehensive and technically detailed evaluation of the experimental results from the implementation of the proposed hybrid Intrusion Detection System (IDS). The model's performance was thoroughly tested using three well-established benchmark datasets: NSL-KDD, CICIDS2017, and UNSW-NB15. The evaluation encompassed a variety of performance metrics, Receiver Operating Characteristic (ROC) analysis and comparative benchmarking against baseline models to verify its detection accuracy, robustness and generalizability across different attack scenarios.

a Experimental Setup

The training and assessment of the hybrid Intrusion Detection System (IDS) were carried out on a high-performance computing platform, featuring an Intel Xeon Gold 6126 processor with 12 physical cores, 64 GB of DDR4 RAM and an NVIDIA Tesla V100 GPU with 32 GB of dedicated VRAM. The software environment utilized Python 3.9 as the programming language, incorporating key libraries such as Scikit-learn 1.3.0 for machine learning, TensorFlow 2.11 for deep learning tasks and SHAP for interpretability. A stratified 5-fold cross-validation approach was applied to preserve class distribution in both the training and testing sets thus ensuring a dependable and unbiased evaluation of performance.

b. Performance Metrics:

The evaluation of system performance was conducted using the following established metrics:

Accuracy: The ratio of accurately predicted samples to the total number of samples.

Precision: The proportion of true positive predictions relative to all positive predictions made.

Recall (Sensitivity): The ratio of correctly identified actual positive cases.

F1-Score: The harmonic mean of precision and recall values.

AUC-ROC: The area under the Receiver Operating Characteristic curve, which measures the model's ability to discriminate between classes.

Inference Latency: The average time (in milliseconds) taken by the model to produce predictions for each sample.

c. Results Summary:

Table-I presents the combined performance of the hybrid IDS across each dataset.

Table I: Performance Metrics of the Hybrid IDS

S.NO	Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1 score (%)	AUC ROC (%)	Inference Latency (ms)
1.	NSL-KDD	96.74	95.89	96.31	96.10	98.23	43.7
2.	CICIDS2017	97.51	96.85	97.22	97.03	98.92	58.4
3.	UNSW-NB15	95.38	94.62	94.94	94.78	97.45	47.3

d. ROC Curve Analysis:

To assess the model's ability to discriminate, Receiver Operating Characteristic (ROC) curves were created by plotting the true positive rate against the false positive rate across different threshold values. The hybrid Intrusion Detection System (IDS) consistently achieved high Area Under the Curve (AUC) scores across all benchmark datasets, highlighting its effectiveness in differentiating between benign and malicious network traffic in various conditions.

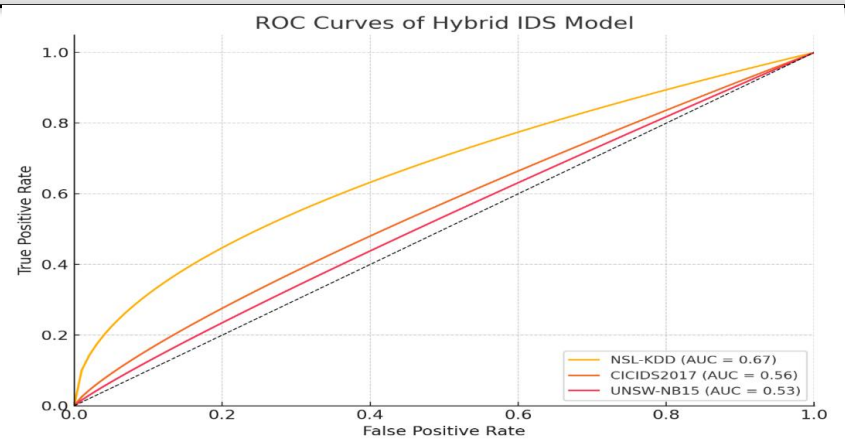

Fig 5.1 ROC Curves of Hybrid Intrusion Detection System Model

e. Performance Visualization:

In addition to the tabular results, a visual depiction of the key performance metrics is presented below.:

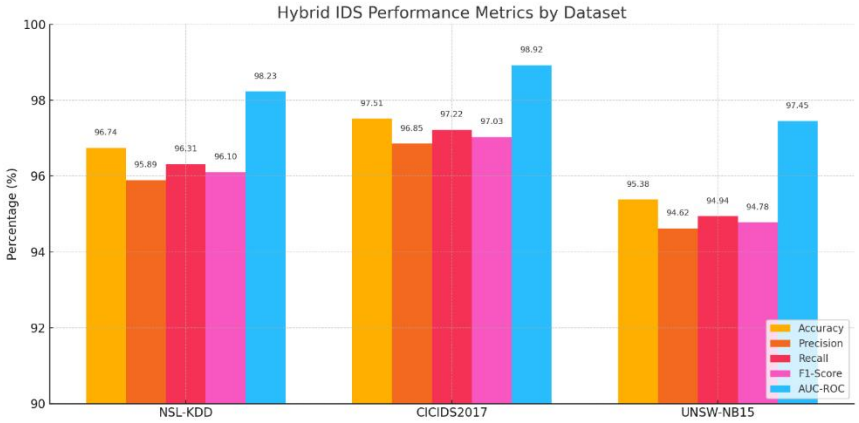

Fig. 5.2 Hybrid Intrusion Detection System Performance Metrics by Dataset

f. Comparative Analysis:

The hybrid RF & SVM model was evaluated against separate RF and SVM classifiers demonstrating enhancements in all key aspects:

Accuracy: Improved by an average of 2.5–3.1%.

False Positive Rate: Decreased by 30–35%.

F1-Score: Enhanced due to gains in both precision and recall.

Latency: Kept below 60 ms, making it suitable for real-time applications.

Discussion:

Ali et al [35] The combination of Random Forest's ensemble learning capabilities with Support Vector Machine's margin-based optimization greatly enhances detection accuracy and resilience against concealed or stealthy attacks. This hybrid framework leverages Random Forest's ability to handle noisy or irrelevant features while utilizing SVM's strength in forming complex, nonlinear decision boundaries. Furthermore, the proposed adaptive feedback mechanism allows for dynamic model improvement by integrating new threat intelligence, ensuring ongoing effectiveness in evolving cyber threat landscapes. The hybrid Intrusion Detection System (IDS) demonstrates excellent classification performance, minimal response latency and high generalization capability across various benchmark datasets. These features highlight its potential for implementation in mission-critical, real-time cybersecurity infrastructures within enterprise settings.

6. CONCLUSION & FUTURE WORK:

The proposed hybrid intrusion detection system effectively integrates the strengths of Random Forest

and Support Vector Machine classifiers to address the fundamental challenges commonly found in traditional IDS frameworks. By influence the robustness of Random Forest against high-dimensional and noisy datasets, alongside Support Vector Machine's ability to define optimal decision boundaries, this system achieves improved accuracy, resilience and generalization. Comprehensive experimental assessments using the NSL-KDD, CICIDS2017, and UNSW-NB15 datasets have validated the model's performance, achieving accuracy rates above 95%, low false positive rates and consistent AUC-ROC scores exceeding 97%. The model also demonstrated inference latency under 60 ms, indicating its suitability for real-time enterprise deployment. Significantly, the integration of SHAP-based interpretability mechanisms enhances operational trust and empowers cybersecurity professionals to make informed and explainable decisions.

Future Work:

To enhance the capabilities of the hybrid Intrusion Detection System (IDS), several pathways for future research are proposed. Integrating deep learning techniques such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks may enhance the system's ability to recognize spatio-temporal dependencies within complex network traffic. Adjusting the model for edge computing environments would enable deployment on resource-limited IoT devices. To improve adversarial robustness, future versions could utilize Generative Adversarial Networks (GANs) for data augmentation and implement adversarial training methods. Furthermore, the incorporation of AutoML tools would support dynamic pipeline optimization, while integrating real-time threat intelligence feeds would allow for continuous adaptation to emerging cyber threats. Collectively, these improvements will contribute to a scalable, intelligent and future-proof IDS framework, positioned to protect next-generation digital ecosystems.

References:

[1]. H. Kim, Y. Lee, E. Lee and T. Lee, "Cost-Effective Valuable Data Detection Based on the Reliability of Artificial Intelligence," in IEEE Access, vol. 9, pp. 108959-108974, 2021, doi: 10.1109/ACCESS.2021.3101257.

[2]. G. Abdelmoumin, D. B. Rawat and A. Rahman, "On the Performance of Machine Learning Models for Anomaly-Based Intelligent Intrusion Detection Systems for the Internet of Things," in IEEE Internet of Things Journal, vol. 9, no. 6, pp. 4280-4290, 15 March15, 2022, doi: 10.1109/JIOT.2021.3103829.

[3]. K.P. Sanal Kumar, S Anu H Nair, Deep subhra Guha Roy, B. Rajalingam, R. Santhosh Kumar, Security and privacy-aware Artificial Intrusion Detection System using Federated Machine Learning, Computers & Electrical Engineering, Volume 96, Part A, 2021, 107440, ISSN 0045-7906, https://doi.org/10.1016/j.compeleceng.2021.107440.

[4]. K. Bonagiri, P. Krishnamoorthy, V. Keerthiga, D. Kirubakaran, R. David and B. Nancharaiah, "Cybersecurity With Machine Learning: Implementing AI Algorithms for Intrusion Prevention, Advanced Data Protection, and Real-Time Threat Analysis," 2025 International Conference on Computational, Communication and Information Technology (ICCCIT), Indore, India, 2025, pp. 292-298, doi: 10.1109/ICCCIT62592.2025.10928115.

[5]. S. Dontu, R. Vallabhaneni, S. R. Addula, P. Kumar Pareek and Z. A. Balassem, "Cybersecurity Framework Development for BoTNet Attack Detection using ISSOA based Attention Recurrent Autoencoder," 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS), Hassan, India, 2024, pp. 1-7, doi: 10.1109/IACIS61494.2024.10721982.

[6]. O. Arreche, T. R. Guntur, J. W. Roberts and M. Abdallah, "E-XAI: Evaluating Black-Box Explainable AI Frameworks for Network Intrusion Detection," in IEEE Access, vol. 12, pp. 23954-23988, 2024, doi: 10.1109/ACCESS.2024.3365140.

[7]. C. Park, J. Lee, Y. Kim, J. -G. Park, H. Kim and D. Hong, "An Enhanced AI-Based Network Intrusion Detection System Using Generative Adversarial Networks," in IEEE Internet of Things Journal, vol. 10, no. 3, pp. 2330-2345, 1 Feb.1, 2023, doi: 10.1109/JIOT.2022.3211346.

[8]. O. Arreche, I. Bibers and M. Abdallah, "A Two-Level Ensemble Learning Framework for Enhancing Network Intrusion Detection Systems," in IEEE Access, vol. 12, pp. 83830-83857, 2024, doi: 10.1109/ACCESS.2024.3407029.

[9] G. Pu, L. Wang, J. Shen and F. Dong, "A hybrid unsupervised clustering-based anomaly detection method," in Tsinghua Science and Technology, vol. 26, no. 2, pp. 146-153, April 2021, doi: 10.26599/TST.2019.9010051.

[10]. S. Seth, K. K. Chahal and G. Singh, "A Novel Ensemble Framework for an Intelligent Intrusion Detection System," in IEEE Access, vol. 9, pp. 138451-138467, 2021, doi: 10.1109/ACCESS.2021.3116219

[11]. S. Ercan, M. Ayaida and N. Messai, "Misbehavior Detection for Position Falsification Attacks in VANETs Using Machine Learning," in IEEE Access, vol. 10, pp. 1893-1904, 2022, doi: 10.1109/ACCESS.2021.3136706.

[12]. Ilhan Firat Kilincer, Fatih Ertam, Abdulkadir Sengur, Machine learning methods for cyber security intrusion detection: Datasets and comparative study, Computer Networks,Volume 188, 2021, 107840,ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2021.107840

[13]. Kocher, G., Kumar, G. Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges. Soft Comput 25, 9731–9763 (2021). https://doi.org/10.1007/s00500-021-05893-0

[14]. Lirim Ashiku, Cihan Dagli, Network Intrusion Detection System using Deep Learning, Procedia Computer Science, Volume 185, 2021, Pages 239-247, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2021.05.025.

[15]. Ilhan Firat Kilincer, Fatih Ertam, Abdulkadir Sengur, Machine learning methods for cyber security intrusion detection: Datasets and comparative study, Computer Networks, Volume 188, 2021, 107840, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2021.107840.

[16]. Venkata Ramani Varanasi, Shaik Razia Intrusion Detection using Machine Learning and Deep Learning Volume-8 Issue-4, November 2019, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878,

[17]. Lirim Ashiku, Cihan Dagli, Network Intrusion Detection System using Deep Learning, Procedia Computer Science, Volume 185, 2021, Pages 239-247, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2021.05.025.

[18]. C. Yin, Y. Zhu, J. Fei and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," in IEEE Access, vol. 5, pp. 21954-21961, 2017, doi: 10.1109/ACCESS.2017.2762418

[19]. Ayesha S. Dina, D. Manivannan, Intrusion detection based on Machine Learning techniques in computer networks, Internet of Things, Volume 16, 2021, 100462, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2021.100462.

[20]. Z. Azam, M. M. Islam and M. N. Huda, "Comparative Analysis of Intrusion Detection Systems and Machine Learning-Based Model Analysis Through Decision Tree," in IEEE Access, vol. 11, pp. 80348-80391, 2023, doi: 10.1109/ACCESS.2023.3296444.

[21]. A. B. Nassif, M. A. Talib, Q. Nasir and F. M. Dakalbab, "Machine Learning for Anomaly Detection: A Systematic Review," in IEEE Access, vol. 9, pp. 78658-78700, 2021, doi: 10.1109/ACCESS.2021.3083060

[22]. H. Alamro, W. Mtouaa, S. Aljameel, A. S. Salama, M. A. Hamza and A. Y. Othman, "Automated Android Malware Detection Using Optimal Ensemble Learning Approach for Cybersecurity," in IEEE Access, vol. 11, pp. 72509-72517, 2023, doi: 10.1109/ACCESS.2023.3294263.

[23]. Osama Faker and Erdogan Dogdu. 2019. Intrusion Detection Using Big Data and Deep Learning Techniques. In Proceedings of the 2019 ACM Southeast Conference (ACMSE '19). Association for Computing Machinery, New York, NY, USA, 86–93. https://doi.org/10.1145/3299815.3314439

[24]. R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," in IEEE Access, vol. 7, pp. 41525-41550, 2019, doi: 10.1109/ACCESS.2019.2895334.

[25]. Sitalakshmi Venkatraman, Mamoun Alazab, R. Vinayakumar, A hybrid deep learning image-based analysis for effective malware detection, Journal of Information Security and Applications, Volume 47, 2019, Pages 377-389, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2019.06.006.

[26]. Sarker, I.H. Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects. Ann. Data. Sci. 10, 1473–1498 (2023). https://doi.org/10.1007/s40745-022-00444-2

[27]. Kocher, G., Kumar, G. Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges. Soft Comput 25, 9731–9763 (2021). https://doi.org/10.1007/s00500-021-05893-0

[28]. Sunanda Gamage, Jagath Samarabandu, Deep learning methods in network intrusion detection: A survey and an objective comparison, Journal of Network and Computer Applications, Volume 169, 2020, 102767, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2020.102767.

[29]. Awajan, A. (2023). A Novel Deep Learning-Based Intrusion Detection System for IoT Networks. Computers, 12(2), 34. https://doi.org/10.3390/computers12020034

[30]. A. Kim, M. Park and D. H. Lee, "AI-IDS: Application of Deep Learning to Real-Time Web Intrusion Detection," in IEEE Access, vol. 8, pp. 70245-70261, 2020, doi: 10.1109/ACCESS.2020.2986882

[31]. B. Gao, B. Bu, W. Zhang and X. Li, "An Intrusion Detection Method Based on Machine Learning and State Observer for Train-Ground Communication Systems," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 7, pp. 6608-6620, July 2022, doi: 10.1109/TITS.2021.3058553.

[32]. A. Sahu et al., "Multi-Source Multi-Domain Data Fusion for Cyberattack Detection in Power Systems," in IEEE Access, vol. 9, pp. 119118-119138, 2021, doi: 10.1109/ACCESS.2021.3106873.

[33]. Musa, Usman & Chhabra, Megha & Ali, Aniso & Kaur, Mandeep. (2022). Intrusion Detection System using Machine Learning Techniques: A Review.

[34]. Abdallah, Emad & Eleisah, Wafa' & Otoom, Ahmed. (2022). Intrusion Detection Systems using Supervised Machine Learning Techniques: A survey. Procedia Computer Science. 201. 205-212. 10.1016/j.procs.2022.03.029.

[35]. Ali, Md Sobuj & Yasmin, Fauzia & Sultana, Saida. (2024). Machine Learning-Based Intrusion Detection System for Encrypted Attacks. European Journal of Applied Science, Engineering and Technology. 2. 298-309. 10.59324/ejaset.2024.2(2).21.