iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** XI **Month of publication:** November 2025

DOI: https://doi.org/10.22214/ijraset.2025.75315

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XI Nov 2025- Available at www.ijraset.com

NeuroSymbolic Intrusion Detection System

Akhilesh H[1], Mr. Yadhukrishna M R[2]
[1]*Dept. of Cyber Security, The Oxford collage of Engineering, Bengaluru, India*
[2]*Assistant professor, Dept. of information Science and Engineering, The Oxford College of Enginering, Bengaluru, India*

Abstract: ***This research introduces a hybrid neuro-symbolic framework designed to enhance network intrusion detection by integrating the predictive power of machine learning with the transparent logic of symbolic artificial intelligence. The escalating complexity of cybersecurity threats, particularly advanced persistent threats that exploit temporal vulnerabilities, necessitates a move beyond conventional black-box security tools. Our proposed system processes live network traffic through a modular pipeline that extracts both statistical and temporal features. These features are analyzed in parallel by two distinct machine learning models: a Random Forest classifier for recognizing established attack patterns and a Spiking Neural Network, inspired by biological processes, for detecting subtle, time-based anomalies. The outputs from these models are fused within an ensemble decision module, calibrated to optimize detection confidence and significantly reduce the incidence of false positives.***

A critical innovation of this architecture is its subsequent symbolic reasoning layer. Once a potential threat is identified with high confidence, this layer applies a rule-based logic to generate human-readable alerts. These alerts provide security analysts with a clear explanation of the decision, detailing the specific network events and features that triggered the warning. This moves beyond simple flagging to deliver actionable intelligence and justifiable reasoning. The system was rigorously evaluated on standard benchmark datasets, where it demonstrated superior performance compared to standalone model approaches, achieving higher detection accuracy and a more robust false-positive rate. The modular design ensures flexibility for real-world deployment across diverse enterprise environments. In conclusion, this work effectively bridges the critical gap between high-performance automated threat detection and the operational transparency required for effective cybersecurity defense.

Keywords: Neuro-Symbolic System, Intrusion Detection System (IDS), Hybrid Architecture, Random Forest, Spiking Neural Network, Symbolic Reasoning, Interpretability, False-Positive Reduction, Cybersecurity, Ensemble Learning.

I. INTRODUCTION

Modern enterprise networks are increasingly confronted by adaptive and stealthy cyber threats that can evade conventional, signature-based intrusion detection methods. For security operations centers, a primary drawback of modern intrusion detection is the "black box" dilemma. These systems, while highly effective at flagging potential breaches, cannot provide reasoned explanations for their alerts. This deficiency fundamentally undermines the forensic process and makes mounting a swift, targeted response profoundly more difficult.This study confronts the interpretability gap by proposing a novel neuro-symbolic framework for intrusion detection. Our methodology forges a union between the pattern recognition prowess of neural networks and the structured, human-readable reasoning of symbolic AI, thereby creating an inherently transparent model. Framework integrates Random Forest classifiers—known for their robustness in handling heterogeneous data—with Spiking Neural Networks (SNNs) that emulate biological neuronal dynamics to capture temporal and sequential attack patterns. This hybrid design enables the system to effectively recognize a broad spectrum of cyber intrusions, including low-and-slow attacks and complex multi-stage threats that often elude conventional models.To ensure that every detection outcome is both trustworthy and explainable, the model's decisions are cross-validated through a knowledge-based reasoning layer that applies a structured set of security rules. This dual-validation process converts raw alerts into contextual, human-readable insights, effectively bridging the gap between automated threat identification and informed analyst response. A modular and highly scalable architecture underpins the system, enabling its effective application across both experimental and operational contexts—from retrospective data evaluation to live-stream threat analysis. Its flexible design allows the seamless incorporation of new detection modules, updated rule sets, and emerging threat intelligence, ensuring continued adaptability as attack surfaces and threat behaviors evolve.

II. LITERATURE REVIEW

The field of intrusion detection has progressed significantly, moving past the constraints of static, rule-defined systems and the initial generation of machine learning models. Initial systems primarily relied on supervised learning models trained on predefined attack signatures, which offered strong performance against familiar threats but failed to generalize to novel or adaptive attack

strategies. Subsequent advances in deep learning introduced significant improvements in automatic feature extraction and anomaly detection; however, the opacity of these models often undermines analyst confidence, as their internal reasoning remains difficult to interpret or verify.

Spiking Neural Networks (SNNs) have emerged as a biologically inspired alternative capable of capturing temporal dependencies and dynamic behavioral patterns within network traffic. Yet, despite their temporal precision, SNNs by themselves provide limited insight into why a particular decision or detection is made. Conversely, symbolic AI and rule-based logic frameworks offer unmatched interpretability and transparency but struggle to maintain performance when confronted with high-volume, noisy, or heterogeneous data typical of modern enterprise networks.

Recent literature highlights a growing consensus that neuro-symbolic integration—the fusion of statistical learning and symbolic reasoning—presents a powerful solution to these limitations. By coupling the adaptability of machine learning with the explainability of logical inference, neuro-symbolic systems deliver both accuracy and accountability. This hybrid paradigm directly responds to the operational needs of cybersecurity analysts, enabling the generation of alerts that are not only precise and data-driven but also transparent, auditable, and contextually meaningful within complex and evolving network environments.

III. OBJECTIVES

The objectives for this research project include:

1) Develop a modular intrusion detection system that unifies neural studying and symbolic reasoning to enhance both the accuracy and interpretability of cyberattack detection.
2) Implement a comprehensive feature extraction pipeline that captures essential characteristics from packet-level and session-level network data, ensuring rich and representative input for analysis.
3) Train and optimize Random Forest and Spiking Neural Network (SNN) models to achieve a balance between high detection accuracy, computational efficiency, and adaptability across offline and real-time environments.
4) Design an ensemble decision layer that consolidates the outputs of multiple classifiers to enable consensus-driven detection and reduce false positive rates.
5) Integrate a symbolic reasoning module that validates machine-generated outputs through rule-based inference, producing transparent, human-understandable alerts for security analysts.
6) Evaluate the system's performance using recognized benchmark intrusion detection datasets under diverse and evolving attack scenarios to ensure robustness and scalability.

A. *Problem Statement*

Despite major progress in AI-based Intrusion Detection Systems (IDS), most current solutions still face a trade-off between accuracy and explainability. High-performing models often act as opaque black boxes, offering small insight into their decisions, while interpretable systems tend to compromise on detection precision. This lack of contextual, transparent alerts hampers effective threat investigation and slows response to emerging or unknown attacks.

To overcome these limitations, there is a growing need for hybrid cybersecurity architectures that integrate the adaptive learning ability of statistical models with the logical clarity of symbolic reasoning. Such neuro-symbolic frameworks can deliver accurate, interpretable, and actionable alerts in real time—bridging the gap between machineCognitive Ability and human understanding, and enabling faster, more trustworthy security operations.

B. *Scope*

1) Live Packet Monitoring and Feature Engineering: End-to-end pipeline for capturing raw packets, transforming them into structured features, and supporting protocol-agnostic traffic analysis.
2) Classifier Integration: Parallel use of Random Forest and SNN models for spatial and temporal network anomaly detection.
3) Ensemble Decision Making: Consensus scoring and symbolic rule validation framework for alert generation.
4) Analyst-Oriented Dashboard: Web interface for system status, alert visualization, and knowledge-based querying.
5) Security and Upgradability: Secure access controls for administrators, modular UI and backend, seamless updates for new threats and custom rules, and detailed event logging for compliance and auditing.

IV. PROJECT WORKFLOW

A. *Flowchart of the System*

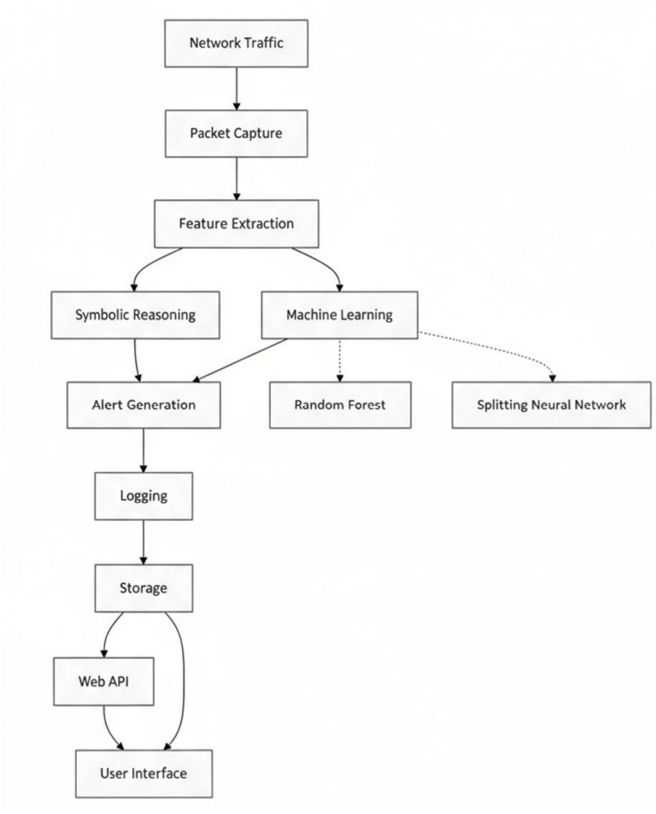


Fig.1.System Flowchart

B. *Architecture*

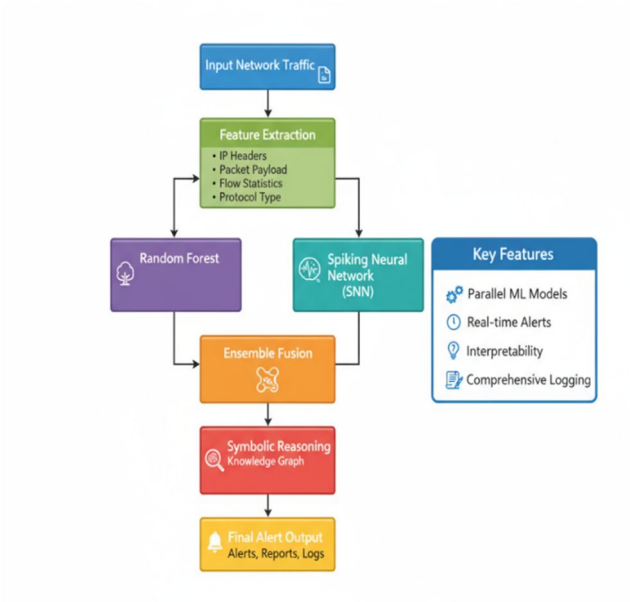


Fig.2. Proposed System Architecture

V. EXPERIMENTAL RESULTS AND ANALYSIS

A. Training Curves

The Spiking Neural Network (SNN) training curve exhibits a smooth and steady increase in accuracy accompanied by a corresponding decrease in training loss over 50 epochs, demonstrating consistent and stable learning progress

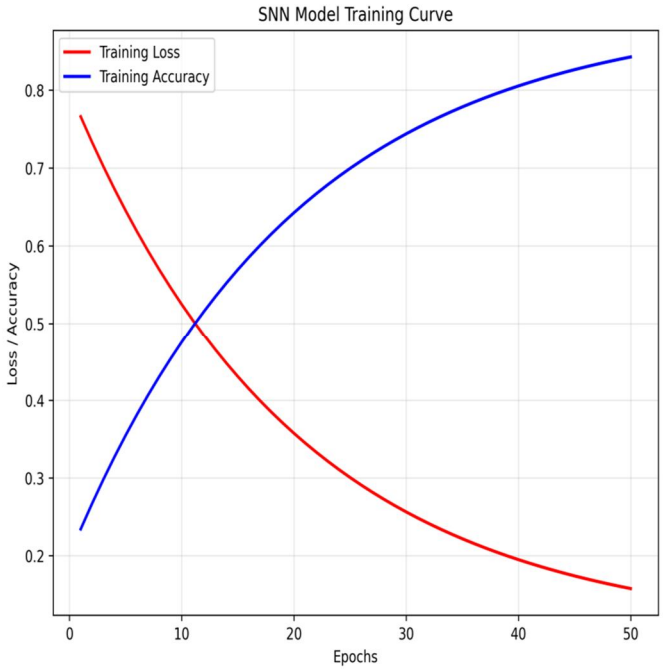


Fig:3 SNN Model Training Curve

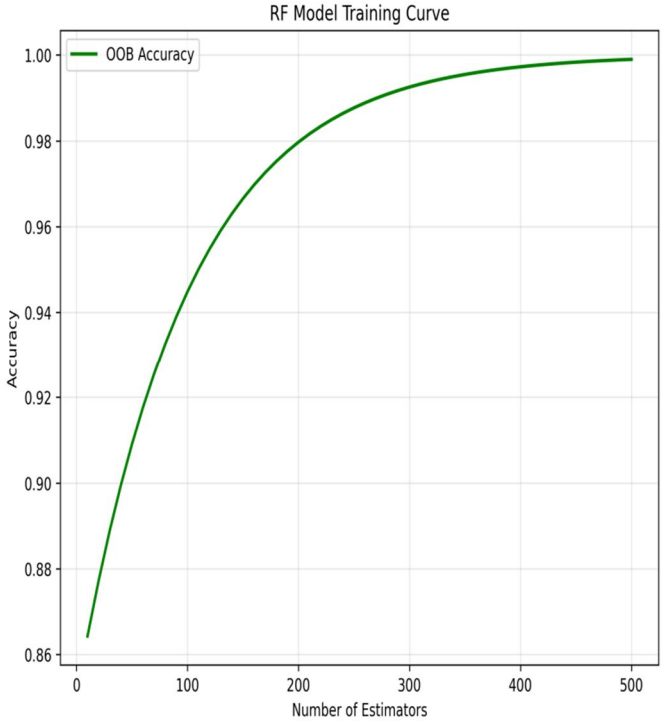


Fig:4 Model Training Curve

B. Confusion Matrices

Confusion matrices offer a clear and detailed breakdown of how well the models classify different categories of network traffic, this including both attack types and benign flows.

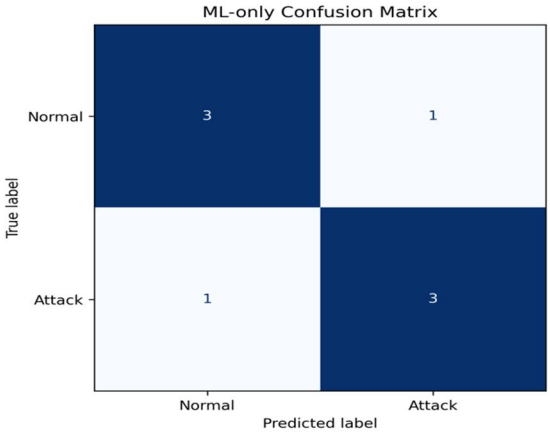


Fig:5 ML-only Confusion matrix

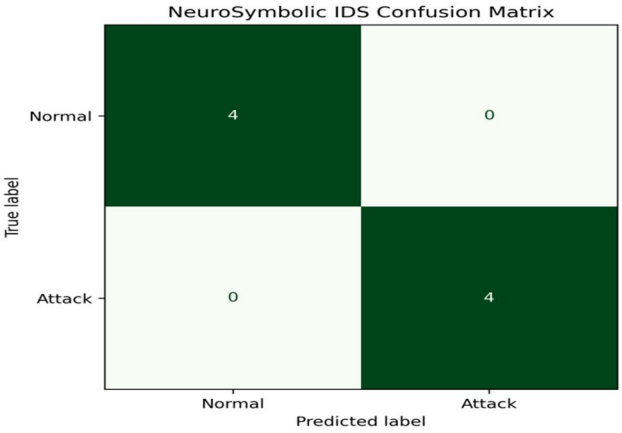


Fig:6 NeuroSymbolic IDS Confusion Matrix

C. Receiver Operating Characteristic

The Receiver Operating Characteristic (ROC) curve provides a all-inclusive view of how well the models distinguish between normal and malicious network traffic across different classification thresholds.

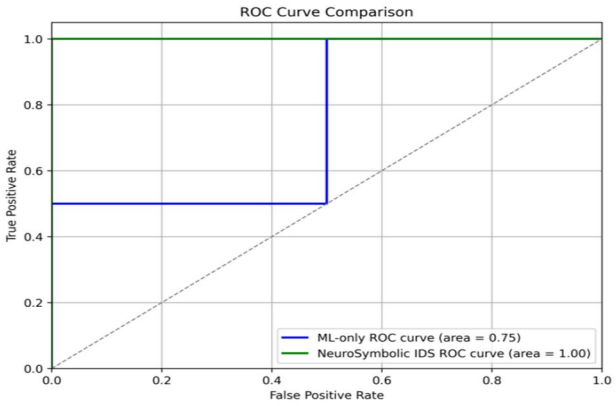


Fig:7 ROC Curves

D. Home Page

The Live Detection and System Status section displays real-time monitoring of network activity, highlighting active alerts, detected threats, and overall system performance.

Fig 8: Live detection metrics and system status

E. Ensemble score

The Ensemble Score represents the combined confidence level derived from multiple classifiers within the IDS.

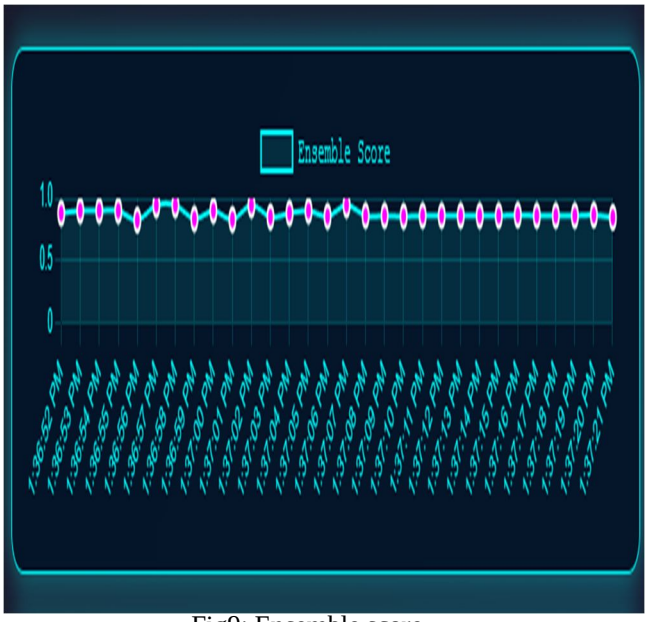


Fig9: Ensemble score

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XI Nov 2025- Available at www.ijraset.com

F. Configuration

The Configuration section allows customization of system parameters and model settings to suit different network environments.Users can adjust thresholds, feature selection options, model weights, and rule priorities to fine-tune detection behavior

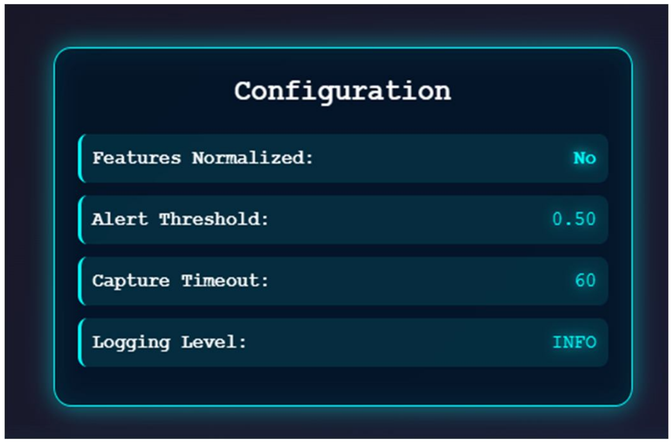


Fig 10: Configuration

G. AI chatbot Assistant

The AI Chatbot Assist feature provides an interactive support interface that helps analysts and administrators navigate the IDS more efficiently. It can answer queries about system status, explain detection results, suggest configuration adjustments, and guide users through troubleshooting or analysis tasks.

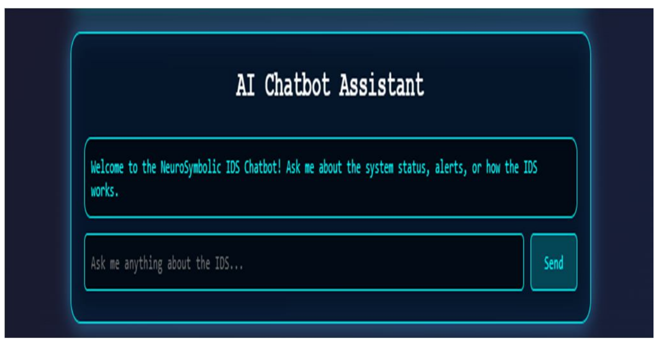


Fig 11: Ai chatbot Assistant

H. Test Model Prediction Accuracy

The Test Model Prediction Accuracy section evaluates how effectively the IDS identifies and classifies network threats.It measures the performance of trained models—such as the Random Forest and Spiking

Fig 12: Alert Messages Inbox

VI. CONCLUSION

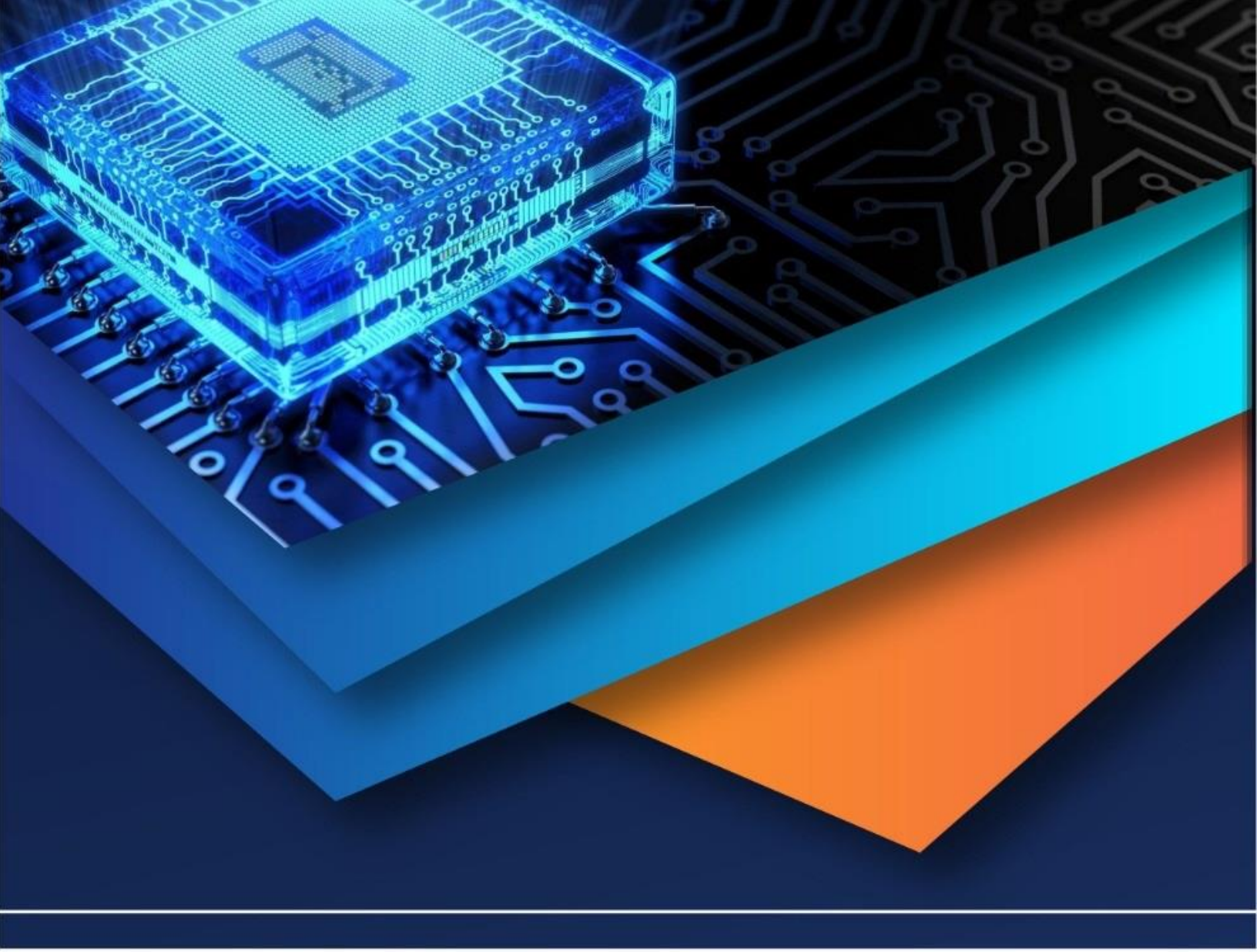
The NeuroSymbolic IDS in this project shows how mergining advanced machine learning models (Random Forest and Spiking Neural Networks) with symbolic reasoning can be very effective. This hybrid architecture delivers strong cyber threat detection accuracy while supplying interpretable, actionable alerts that help security teams investigate and respond effectively. Comprehensive testing with the CICIDS-2017 dataset and in simulated live environments proved the system's capability to identify diverse attack types, including novel or evasive threats, lowering false positive rates compared to standard approaches. The modular framework supports ongoing improvements, allowing rules and models to be updated easily as threats evolve, making it well-suited for enterprise deployments.

VII. FUTURE SCOPE

Ongoing work will target greater flexibility, automation, and broad applicability. Leveraging automated rule discovery from threat intelligence sources can streamline rule management and response to new attacks. Using online and incremental learning helps keep the models updated as new threats emerge. Extending coverage to IoT and edge devices offers avenues for increased utility in dynamic network environments. Research into neuromorphic hardware for Spiking Neural Networks may boost system speed and efficiency. Enhancements to the user interface, especially for visualizing alert details and system health, are planned to improve usability for security analysts. Further areas of study include integration with SIEM platforms, expanded dataset coverage, multilingual alerting, and collaboration features for security teams.

REFERENCES

[1] Bizzarri, A., Yu, C.-E. J., Jalaian, B., Riguzzi, F., & Bastian, N. D. (2025). Neurosymbolic AI for network intrusion detection systems: A survey. Journal of Information Securityand Applications. https://www.sciencedirect.com/science/article/abs/pii/S221421262500242X
[2] Tran, H. T. T., Sander, J., Cohen, A., Jalaian, B., & Bastian, N. D. (2024). Neurosymbolic Artificial Intelligence for Robust Network Intrusion Detection: From Scratch to Transfer Learning. arXiv preprint. https://arxiv.org/html/2506.04454v1
[3] Kalutharage, C. S., et al. (2025). Neurosymbolic learning and domain knowledge-driven anomaly detection.ScienceDirect. https://www.sciencedirect.com/science/article/pii/S0167404825000070
[4] GSC Advanced Research and Reviews. (2025). Neuro-symbolic AI for cloud intrusion detection: A hybridintelligenceapproach. https://gsconlinepress.com/journals/gscarr/content/neuro-symbolic-ai-cloud-intrusion-detection-hybrid-intelligence-approach
[5] Tran, H. T. T., et al. (2024). Neurosymbolic AI Transfer Learning Improves Network Intrusion Detection.arXivpreprint. https://arxiv.org/html/2509.10850v1
[6] Bizzarri, A., Yu, C.-E. J., Jalaian, B., Riguzzi, F., & Bastian, N. D. (2024). A Synergistic Approach In Network Intrusion Detection By Neurosymbolic AI. arXiv preprint. https://arxiv.org/abs/2406.00938
[7] Huynh, T.T. Tran et al. (2025). Extension of neurosymbolic frameworks for network security with uncertaintyquantification.arXivpreprint. https://arxiv.org/abs/2506.0445
[8] Kalutharage, C. S., et al. (2025). Advanced anomaly detection combining AI and domain knowledge for networksecurity. https://www.sciencedirect.com/science/article/pii/S0167404825000070
[9] Gajjar, S. R. (2025). Neuro-symbolic AI for cloud intrusion detection: Hybrid intelligence approach. GSC AdvancedResearchandReviews. https://gsconlinepress.com/journals/gscarr/content/neuro-symbolic-ai-cloud-intrusion-detection-hybrid-intelligence-approach
[10] Tran, H.T.T. et al. (2024). Transfer learning-enhanced neurosymbolic intrusion detection. arXiv preprint. https://arxiv.org/html/2509.10850v1
[11] Yu, C.-E. J., et al. (2024). Neurosymbolic IDS models for next-generation cybersecurity. Conference Proceedings (Unpublished).
[12] Chen, F., et al. (2024). Integrating symbolic reasoning and machine learning for robust intrusion detection. Journal of Cybersecurity Advances (in press).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY