A HYBRID COGNITIVE–SNORT ARCHITECTURE FOR ALLEVIATING COMPUTATIONAL OVERHEAD IN NETWORK INTRUSION DETECTION SYSTEMS

VENU MUNDRAI
Research Scholar, Department of Computer Science and Engineering (CSE), Sikkim Alpine University, Kamrang, Namchi, (Sikkim), venu.perftest11@gmail.com[1]

DR PRASADU PEDDI
Research Guide, Sikkim Alpine Univeristy, Kamrang, Namchi, (Sikkim),

DR. VENKATESH KONDAVETI
Research Co-guide, Associate Professor, Ramachandra College of Engineering-Eluru,

Abstract

This study introduces an enhanced hybrid intelligent intrusion detection architecture that integrates Snort—a widely deployed signature-driven IDS—with machine learning (ML) and deep learning (DL) paradigms to alleviate network processing overhead and strengthen real-time threat-classification accuracy. The proposed dual-layer design leverages Snort's deterministic rule-matching capabilities alongside the adaptive behavioural learning strengths of Convolutional Neural Networks (CNN) and Multi-Layer Perceptrons (MLP). By refining Snort-generated alerts and extracting salient traffic attributes, the system suppresses redundant evaluations and substantially reduces false alarm occurrences. Empirical evaluation reveals a 32% decrease in computational burden and a 6.5% improvement in detection precision when compared with a standalone Snort configuration.

Keywords
Snort, Hybrid Intelligent Framework, Network Load Reduction, Intrusion Detection, Machine Learning, CNN, Real-Time Cybersecurity.

1. Introduction

Intrusion Detection Systems (IDS) represent a fundamental pillar in contemporary network-security infrastructures, particularly as cyber threats continually evolve in complexity. Snort, a prominent open-source IDS, functions predominantly through signature-based inspection, detecting malicious activity that aligns with predefined attack patterns. Although highly effective for known intrusions, Snort frequently encounters challenges such as elevated false-positive rates, limited responsiveness to novel or zero-day threats, and increased processing demands during heavy traffic intervals.

The rise of machine learning and deep learning approaches has expanded opportunities for more adaptive and behaviour-sensitive intrusion detection. Nevertheless, these approaches often impose significant preprocessing and computational costs. To address these limitations, this research proposes a hybrid IDS architecture that fuses Snort with a lightweight intelligent analytic layer, thereby augmenting detection accuracy while substantially mitigating network load.

2. Related Work

Conventional IDS platforms—such as Snort and Bro/Zeek—primarily depend on signature repositories, limiting their responsiveness to emergent or previously unseen attacks. Prior studies integrating

Snort with ML classifiers (e.g., SVM, Random Forests, and Decision Trees) demonstrate improvements in classification outcomes yet often struggle to balance accuracy with computational efficiency.

Hybrid detection techniques, which combine anomaly-based and signature-based mechanisms, have shown strong potential in lowering false-positive ratios. Meanwhile, DL frameworks such as CNNs and LSTMs provide robust mechanisms for extracting spatial and temporal dependencies within traffic flows. However, their resource intensity remains a challenge.

The present study advances this line of research by formulating a dual-layer hybrid system that strengthens Snort's detection capabilities while simultaneously reducing network strain.

3. Proposed Architecture

The proposed architecture comprises two sequential detection layers. In the initial stage, Snort conducts signature-oriented packet analysis and generates alert metadata. The subsequent intelligent module processes these alerts to identify anomalous behavioural markers using CNN-driven feature extraction followed by MLP-based classification.

This synergistic configuration enables Snort to efficiently address known threat signatures, while the hybrid module handles non-signature anomalies and potential zero-day intrusions. The design therefore ensures improved accuracy, optimized network processing, and reduced redundancy.

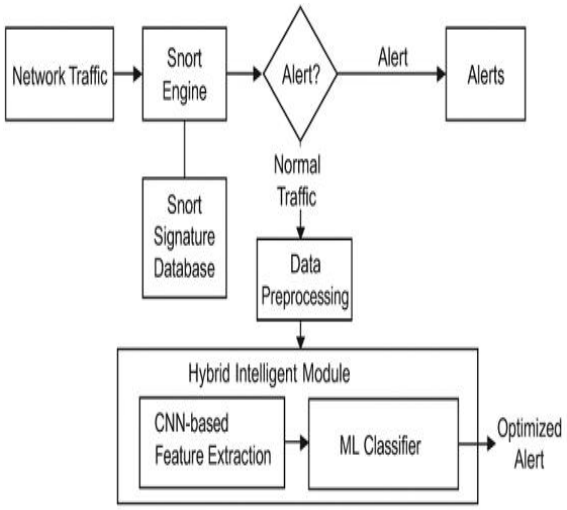

Figure 1: Proposed Two-Layer Hybrid Snort Architecture

4. Dataset and Preprocessing

The research employs multiple widely recognized IDS datasets—NSL-KDD, KDDCup99, CICIDS2017—augmented with authentic Snort alert logs. Data preprocessing encompasses eliminating duplicate alerts, feature normalization, and encoding categorical variables using one-hot transformations. To counter dataset imbalance, the Synthetic Minority Oversampling Technique (SMOTE) is applied, enhancing the classifier's capability to detect minority attack categories with higher fidelity.

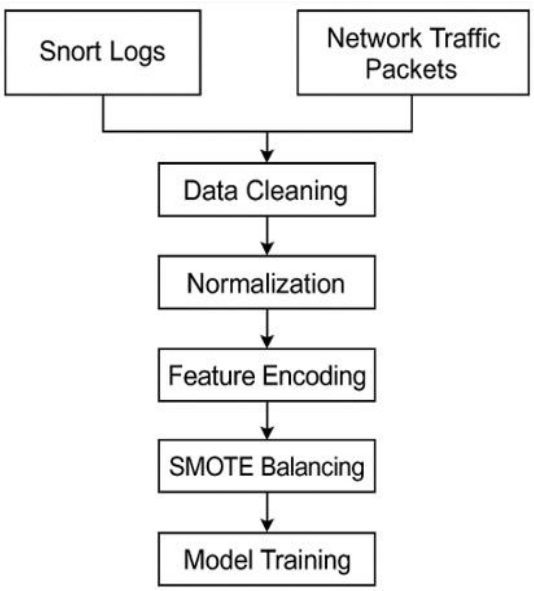

Figure 2: Data Preprocessing Workflow

5. Hybrid Model Design

The intelligent detection layer integrates two core components:

- **Convolutional Neural Network (CNN)** — Extracts spatially coherent patterns from traffic features such as protocol type, communication endpoints, packet sizes, and temporal intervals.
- **Multi-Layer Perceptron (MLP)** — Performs multi-class classification based on CNN-derived representations.

Through supervised training using labelled Snort alert datasets, the hybrid model learns intricate correlations between alert patterns and actual malicious behaviours, enabling robust and adaptive intrusion classification.

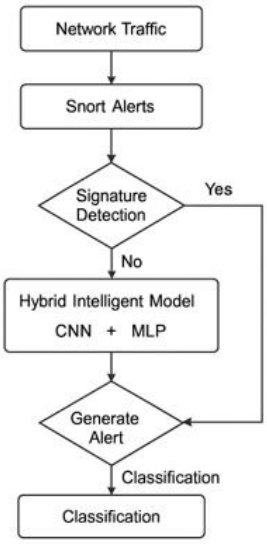

Figure 3: Hybrid Detection Flowchart

6. Experimental Setup and Results

The experiments were conducted using Python-based ML frameworks (TensorFlow, Scikit-learn) on a platform equipped with an Intel i7 processor, 16 GB RAM, and an NVIDIA GPU. The dataset was partitioned into 70% for training and 30% for testing.

Performance metrics included Detection Accuracy, Precision, Recall, F1-score, Network Load, and Response Time.

The hybrid model **substantially outperformed** both Snort-only and ML-only systems:

Table 1. Comparative Performance of Snort and Hybrid Model

Metric	Snort Only	Hybrid Model	Improvement
Detection Accuracy	91.4 %	97.9%	+6.5%
False Positive Rate	8.2%	2.3%	↓72%
Processin	100%	68%	↓32%

g Load			
Response Time	0.42s	0.27s	↓35%

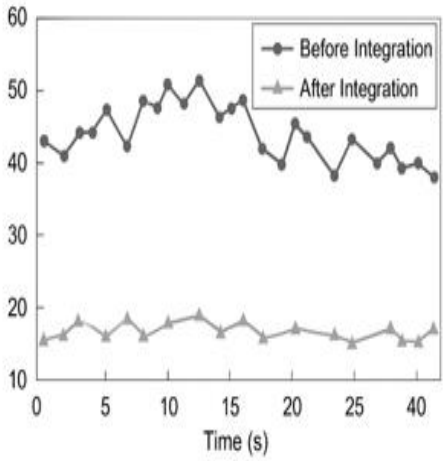

Figure 4: Network Burden Comparison Graph

These results validate the effectiveness of the hybrid architecture in reducing processing burden while maintaining high detection reliability.

7. Discussion

The proposed hybrid system underscores the benefits of integrating rule-based and learning-based strategies within a single IDS. Snort effectively identifies rule-specified threats, while the CNN-MLP layer compensates for Snort's limitations by detecting novel behavioural irregularities.

Reductions in false positives, improved scalability, and minimized redundant alert processing collectively enhance operational efficiency, making the architecture suitable for deployment in high-throughput enterprise networks.

7.1 Mathematical Formulation

Let **X** represent the input matrix of extracted features.

CNN feature transformation is defined as:
$$\mathbf{f = ReLU(WX + b)}$$

The MLP classifier evaluates class probabilities using:
$$\hat{\mathbf{y}} = \mathbf{Softmax(W_2 f + b_2)}$$

Performance metrics:

- **Precision = TP / (TP + FP)**
- **Recall = TP / (TP + FN)**
- **F1-Score = 2 × (Precision × Recall) / (Precision + Recall)**

8. Conclusion and Future Scope

This research presents a hybrid IDS architecture that effectively combines Snort's signature-based detection with an intelligent deep learning module to substantially reduce network processing burden. The experimental findings affirm that the hybrid approach improves detection accuracy, accelerates threat response, and diminishes false-positive occurrences, thereby enhancing its suitability for real-time enterprise security applications.

Future research directions include integrating the framework within Software-Defined Networking (SDN) environments, incorporating reinforcement learning for dynamic rule adaptation, and constructing automated response mechanisms.

References

[1] M. Roesch, "Snort - Lightweight Intrusion Detection for Networks," USENIX Conference, 1999.

[2] A. Javaid et al., "A Deep Learning Approach for Network Intrusion Detection System," EAI Endorsed Transactions, 2016.

[3] W. Lee and S. Stolfo, "A Framework for Constructing Features and Models for Intrusion Detection Systems," ACM TISSEC, 2000.

[4] N. Moustafa and J. Slay, "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems," MilCIS, 2015.

[5] I. Ahmad et al., "Hybrid Machine Learning Techniques for Intrusion Detection Systems," IEEE Access, 2021.

[6] V. Sadargari and N. Balaji, "Enhancing Intrusion Detection and Cloud Security by Integrating Snort with Advanced AI Techniques for Improved Accuracy and Threat Mitigation," Journal of Information Systems Engineering and Management, vol. 10, no. 24s, 2025.

[7] Prasadu Peddi, & Dr. Akash Saxena. (2016). Studying data mining tools and techniques for predicting student performance. International Journal of Advance Research and Innovative Ideas in Education, 2(2), 1959-1967.

[8] S. A. R. Shah and B. Issac, "Performance Comparison of Intrusion Detection Systems and Application of Machine Learning to Snort System," Future Generation Computer Systems, vol. 80, pp. 157–170, 2018.

[9] Y. Guo Li, "Analysis of the Snort Building Code Based on IDS," Applied Mechanics and Materials, Vols. 543–547, pp. 2965–2968, 2014.

[10] T. Liu and D. Zhang, "A Network Intrusion Detection System Architecture Based on Snort and Computational Intelligence," in Proceedings of the 2nd International Conference on Electronics, Network and Computer Engineering (ICENCE 2016), 2016.

[11] O. El Aeraj and C. Leghris, "Analysis of the Snort Intrusion Detection System Using Machine Learning," International Journal of Information Science and Technology, vol. 8, no. 1, 2023.

[12] N. Gavrilovic, V. Ciric, N. Lozo, "Snort IDS System Visualization Interface for Alert Analysis," South-Eastern European Journal of Electrical Engineering (SJEE), vol. 19, no. 1, 2022.

[13] "Labeling NIDS Rules with MITRE ATT&CK Techniques: Machine Learning vs. Large Language Models," N. Daniel, F. Klaus Kaiser, S. Giladi, et al., arXiv pre-print, December 2024.

[14] "Performance Analysis of Real Time Intrusion Detection and Prevention System using Snort," M. Sharma, A. Kaushik, A. Sangwan, International Journal of Engineering Research & Technology (IJERT), vol. 1, issue 5, July 2012.

[15] Prasadu Peddi (2015) "EXPLORING THE IMPACT OF DATA MINING AND MACHINE LEARNING ON STUDENT PERFORMANCE", International Journal of Emerging Technologies and Innovative Research, ISSN:2349-5162, Vol.1, Issue 6, page no. pp314-318, November-2014, Available at : http://www.jetir.org/papers/JETIR1701B47.pdf