Journal of Information Systems Engineering and Management
2025, 10(24s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Enhancing Intrusion Detection and Cloud Security by Integrating Snort with Advanced AI Techniques for Improved Accuracy and Threat Mitigation

Sadargari Viharika[1], NAlangudi Balaji[2]

[1]Research Scholar, Department of CSE, KONERU LAKSHMAIAH EDUCATIONFOUNDATION-Vijayawada-India
[2]Professor , Department of CSE, KONERU LAKSHMAIAH EDUCATION FOUNDATION-Vijayawada-India
Corresponding E-mail: reddyviharika266@gmail.com,nabalaji@kluniversity.in

ARTILCE INFO

Received: 19 Dec 2024

Revised: 10 Feb 2025

Accepted: 25 Feb 2025

ABSTRACT

Intrusion Detection Systems (IDS) are critical for ensuring the security of cloud infrastructures and modern networks, which are increasingly vulnerable to sophisticated cyber threats. While traditional IDS like Snort effectively detect signature-based attacks, they struggle with high false-positive rates and limited adaptability to evolving threats. To address these challenges, this research introduces AIML-Snort, a hybrid intrusion detection framework that integrates Snort with advanced Artificial Intelligence (AI) techniques to enhance detection accuracy and mitigate false alarms. The framework employs preprocessing techniques such as feature normalization, outlier detection using Isolation Forest, and Recursive Feature Elimination (RFE) combined with Genetic Algorithms (GA) for optimized feature selection. Machine learning models like Random Forest (RF) and Neural Networks (NN) are then trained to identify anomalies and integrated with Snort's rule-based system to analyze unresolved traffic. Using the UNSW-NB15 dataset, the framework was evaluated in a simulated high-speed network environment designed to emulate real-world traffic conditions. Results demonstrate that AIML-Snort outperforms traditional Snort configurations, achieving higher detection accuracy, significantly reduced false-positive rates, and improved scalability in large-scale deployments. The integration of AI techniques enhances Snort's ability to adapt to dynamic and previously unseen threats, making it a robust solution for cloud security. This research establishes AIML-Snort as a practical and scalable IDS framework for addressing modern network security challenges, providing valuable insights into the synergy between traditional rule-based systems and AI-powered approaches. Future work will focus on further optimization and extending the framework to support additional datasets and attack scenarios.

Keywords: *Snort-AI Integration, Intrusion Detection System (IDS), Machine Learning,UNSW-NB15 Dataset, Network Security*

1. INTRODUCTION

Cloud computing has revolutionized the technological landscape, establishing itself as a cornerstone of modern infrastructure across diverse fields, including healthcare, military operations, education, and many others [1]][2]. Its unparalleled cost-efficiency, scalability, and reliability have empowered organizations to streamline their operations and adapt to rapidly changing demands with unprecedented flexibility. However, this widespread adoption has been accompanied by a surge in cyber threats, as malicious actors continually seek to exploit vulnerabilities inherent in cloud-based systems. These cyberattacks, ranging from data breaches to denial-of-service attacks, not only disrupt normal system operations but also jeopardize the confidentiality, integrity, and availability of critical data and services [3-5]. The growing reliance on cloud computing underscores the urgent need to develop robust and effective security measures capable of mitigating these threats.

To address this pressing challenge, intrusion detection systems (IDS) have emerged as essential tools in safeguarding cloud infrastructure. By monitoring network traffic and identifying potential threats in real time, IDS play a crucial role in protecting cloud systems from malicious activities. Traditional IDS approaches generally fall into two categories: signature-based detection, which relies on predefined patterns of known threats, and anomaly-based detection, which identifies deviations from normal behavior. While these methods have been effective to a certain extent, they often struggle to keep pace with the evolving complexity and sophistication of modern cyberattacks [6][7]. The limitations of traditional IDS systems, such as high false-positive rates, limited adaptability, and challenges in handling large-scale datasets, have prompted researchers to explore innovative solutions that leverage advanced technologies.

Among the widely used IDS tools, Snort has gained prominence as a reliable open-source platform for intrusion detection and prevention. Known for its ability to perform real-time traffic analysis and packet logging, Snort provides a robust foundation for detecting and mitigating cyber threats. However, the static nature of its signature-based detection approach limits its effectiveness against novel and emerging threats. To overcome these limitations and enhance the capabilities of Snort, the integration of artificial intelligence (AI) techniques has become a promising avenue for research and development. By combining Snort's foundational strengths with the adaptability and intelligence of AI, it is possible to create an advanced intrusion detection framework that addresses the challenges of modern cloud security.

AI-powered solutions, particularly those employing machine learning, have shown great potential in revolutionizing intrusion detection. Machine learning algorithms excel at analyzing vast amounts of network data, identifying hidden patterns, and adapting to new threats in real time. These capabilities make them particularly well-suited for addressing the dynamic and unpredictable nature of cyberattacks. Recent advancements in optimization algorithms and neural networks have further enhanced the performance of IDS frameworks, enabling more accurate threat detection and improved efficiency [8-10]. Despite these advancements, existing AI-driven IDS models face challenges such as computational complexity, prolonged processing times, and difficulties in managing large-scale datasets. These limitations highlight the need for a more streamlined and scalable approach to intrusion detection.

This research proposes a novel framework that integrates Snort with advanced AI techniques to enhance intrusion detection accuracy and improve the overall security of cloud infrastructures. By combining the complementary strengths of Snort's rule-based detection with machine learning models, the framework creates a robust and adaptive intrusion detection system capable of overcoming the limitations of traditional approaches. This hybrid system aims to improve detection accuracy, reduce false-positive rates, and efficiently process large datasets. Moreover, the integration of AI enables the system to adapt to evolving threats, making it an invaluable tool for securing dynamic and complex cloud environments.

The proposed framework introduces several key innovations that distinguish it from existing IDS models. First, it incorporates advanced data preprocessing and normalization techniques to ensure the quality and consistency of input datasets. These preprocessing steps are vital for eliminating noise, which improves the accuracy of intrusion detection. Second, the framework utilizes state-of-the-art optimization algorithms for feature selection, reducing dimensionality and enhancing the performance of machine learning models. Feature selection is crucial in the development of efficient IDS systems, as it directly impacts the speed and accuracy of threat detection. Third, the framework integrates machine learning models, enabling it to classify network traffic as either normal or intrusive with high precision. By employing supervised, semi-supervised, and unsupervised learning techniques, the system can adapt to a wide range of network scenarios and evolving threat patterns.

The integration of Snort with AI techniques is designed to address the practical challenges of deploying IDS in real-world cloud environments. One of the primary goals of this research is to develop a system that is not only effective but also scalable and user-friendly. The proposed framework bridges the gap between the increasing complexity of cyber threats and the need for accessible, efficient security solutions. By streamlining the detection process and minimizing computational requirements, the system offers a practical solution for organizations seeking to enhance their cloud security.

The potential applications of the proposed framework extend beyond traditional cloud environments. In IoT-enabled systems and smart cities, where data integrity and security are paramount, the integration of Snort with AI offers significant advantages. The ability to adapt to diverse network conditions and detect a wide range of threats makes the framework an invaluable tool for ensuring the security and reliability of modern digital ecosystems. Moreover, the framework's scalability and efficiency make it suitable for deployment in various industries, including healthcare, finance, and critical infrastructure.

By addressing the limitations of traditional IDS models and leveraging the power of AI, this research contributes to ongoing efforts to strengthen cloud infrastructures against cyber threats. The integration of Snort with advanced AI techniques represents a significant advancement in the development of effective and adaptive intrusion detection systems. Through rigorous evaluation using publicly available benchmarking datasets, the proposed framework demonstrates its potential to enhance detection accuracy, reduce false positives, and improve the resilience of cloud systems. This research provides a scalable and efficient solution for modern cybersecurity challenges, ensuring the continued growth and reliability of cloud-based ecosystems in the face of evolving threats.

This research develops the hybrid AIML-Snort framework, which integrates Snort's rule-based system with AI-driven anomaly detection models. This approach significantly improves detection accuracy and reduces false positives. The framework employs advanced preprocessing techniques such as Isolation Forest, Recursive Feature Elimination (RFE), and Genetic Algorithms (GA) to optimize feature selection and enhance detection capabilities. Comprehensive performance validation using the UNSW-NB15 dataset in simulated real-world network environments demonstrates the framework's scalability, robustness, and applicability to large-scale deployments.

2. LITERATURE REVIEW

Intrusion Detection Systems (IDS) have evolved as essential tools for safeguarding modern cloud-based networks against increasingly sophisticated cyber threats. The integration of advanced technologies like artificial intelligence (AI), machine learning (ML), and optimization techniques into IDS has demonstrated significant potential in enhancing detection accuracy, reducing false-positive rates, and improving scalability. Deebak and Hwang [16] explored the integration of blockchain within a cloud-assisted framework to ensure decentralized privacy preservation for healthcare applications. Their study highlighted the potential of combining traditional systems with emerging technologies to create robust security solutions, particularly in environments requiring stringent confidentiality, such as healthcare. Ahmad et al. [17] extended this exploration by systematically studying ML and deep learning (DL) techniques for intrusion detection, emphasizing their adaptability to complex attack patterns and large-scale datasets, which are critical in cloud and IoT-based systems. These studies collectively underline the need for hybrid approaches that integrate traditional IDS like Snort with advanced AI methodologies.

To address security concerns in specialized environments, Heidari et al. [18] developed an intrusion detection platform for the Internet of Drones (IoD) by combining blockchain with radial basis function neural networks. Their work demonstrated the resilience of such hybrid systems in distributed, latency-sensitive environments like IoD, but also revealed challenges in computational overhead and scalability. Similarly, Chkirbene et al. [19] proposed the Trust-Based Intrusion Detection and Classification System (TIDCS), which utilized feature selection methods and machine learning classifiers like Naive Bayes (NB). Their system improved classification accuracy and detection rates but faced significant limitations in terms of processing overhead, a critical consideration for real-time intrusion detection. These findings suggest that while traditional and optimization-based approaches offer distinct advantages, integrating them with AI can mitigate their respective limitations.

Industrial IoT (IIoT) environments present unique challenges for intrusion detection due to their highly distributed nature and resource constraints. Kim et al. [20] addressed this by incorporating hybrid anomaly detection methods that enhanced detection accuracy while minimizing false positives. However, scalability in large-scale IIoT networks remained an issue. Hassan et al. [21] tackled a related problem in fog computing systems by designing a load-aware resource allocation framework. Their approach balanced computational efficiency with security, a critical requirement for cloud-integrated IDS frameworks. These studies emphasize the necessity of designing scalable and adaptive IDS solutions capable of handling the dynamic nature of cloud and IoT environments.

The integration of deep learning techniques into IDS has shown promise in improving both accuracy and adaptability. Halbouni et al. [23] proposed a hybrid CNN-LSTM IDS framework that effectively captured spatial and temporal patterns in network traffic, achieving high detection accuracy. However, the computational cost of training such models presented a barrier to real-time deployment in resource-constrained settings. Hanafi et al. [27] further advanced this field by introducing a binary golden jackal optimization algorithm combined with LSTM to detect intrusions in IoT environments. This approach optimized feature selection and detection accuracy, though it required further validation on large-scale datasets. These works demonstrate the effectiveness of integrating optimization techniques and deep learning to overcome traditional IDS challenges.

In cloud-based systems, feature selection and classification efficiency are critical for maintaining high detection rates while minimizing computational requirements. Bukhari et al. [26] developed federated learning-based IDS for wireless sensor networks, incorporating SCNN and BiLSTM to enhance reliability and privacy. This system maintained robust detection performance while preserving data privacy, addressing critical concerns in cloud-integrated environments. Similarly, Vashishtha et al. [28] proposed a hybrid intrusion detection model (HIDM) that utilized multiple classifiers to enhance detection accuracy and adaptability. Despite its effectiveness, the system faced challenges related to training time and processing complexity.

Talukder et al. [30] introduced a hybrid IDS model combining genetic algorithms with support vector machines (SVM). Their approach demonstrated significant improvements in detection accuracy and false-positive reduction, showcasing the potential of hybrid optimization techniques in cloud environments. Hnamte et al. [29] also leveraged deep learning in a two-stage model, combining LSTM and autoencoders to reduce false positives while maintaining high detection rates. Although promising, these models require extensive computational resources for training, limiting their scalability in real-world scenarios.

The reviewed literature highlights the critical need for integrating Snort, a robust and widely used open-source IDS, with advanced AI techniques. Snort's signature-based detection capabilities can be significantly enhanced through the incorporation of AI-driven optimization and classification methods. This hybrid approach promises to address the limitations of traditional IDS systems, such as high false-positive rates and computational inefficiencies, while meeting the demands of modern cloud and IoT security environments. By leveraging the strengths of both traditional and modern methodologies, this integration can enhance detection accuracy, scalability, and adaptability, providing a resilient framework for mitigating evolving cyber threats in dynamic digital ecosystems.

3. PROPOSED METHODOLOGY

The proposed methodology, AI-Augmented Snort for Enhanced Intrusion Detection, is designed to address the limitations of traditional Intrusion Detection Systems (IDS) by integrating Snort with advanced Artificial Intelligence (AI) techniques. This hybrid approach combines Snort's rule-based detection mechanism with AI-driven anomaly detection models, resulting in a system capable of identifying both known and unknown threats with enhanced accuracy and reduced false-positive rates.

The methodology begins with the preprocessing of network traffic data using the UNSW-NB15 dataset, which covers a broad spectrum of network activities, including benign traffic and malicious attacks. Preprocessing involves data normalization, where numerical features are scaled to a consistent range, ensuring uniformity and compatibility during the training of machine learning models. In addition, Isolation Forest is employed to detect and remove outliers, thereby eliminating noise from the dataset and enhancing its quality. This step ensures that only meaningful patterns are used in model training, minimizing the risk of overfitting and improving model generalization.

Feature selection and optimization are pivotal in this methodology, as they enable the system to focus on the most relevant attributes for intrusion detection. Recursive Feature Elimination (RFE), a wrapper-based method, is applied iteratively to identify the most influential features while discarding those with minimal impact on detection accuracy. To further optimize feature selection, Genetic Algorithms (GA) are utilized. These optimization techniques, inspired by natural selection, identify the optimal subset of features that maximize detection performance while minimizing computational complexity. This two-step process ensures a balance between high precision and operational efficiency, making the system well-suited for large-scale deployment in cloud and enterprise networks.

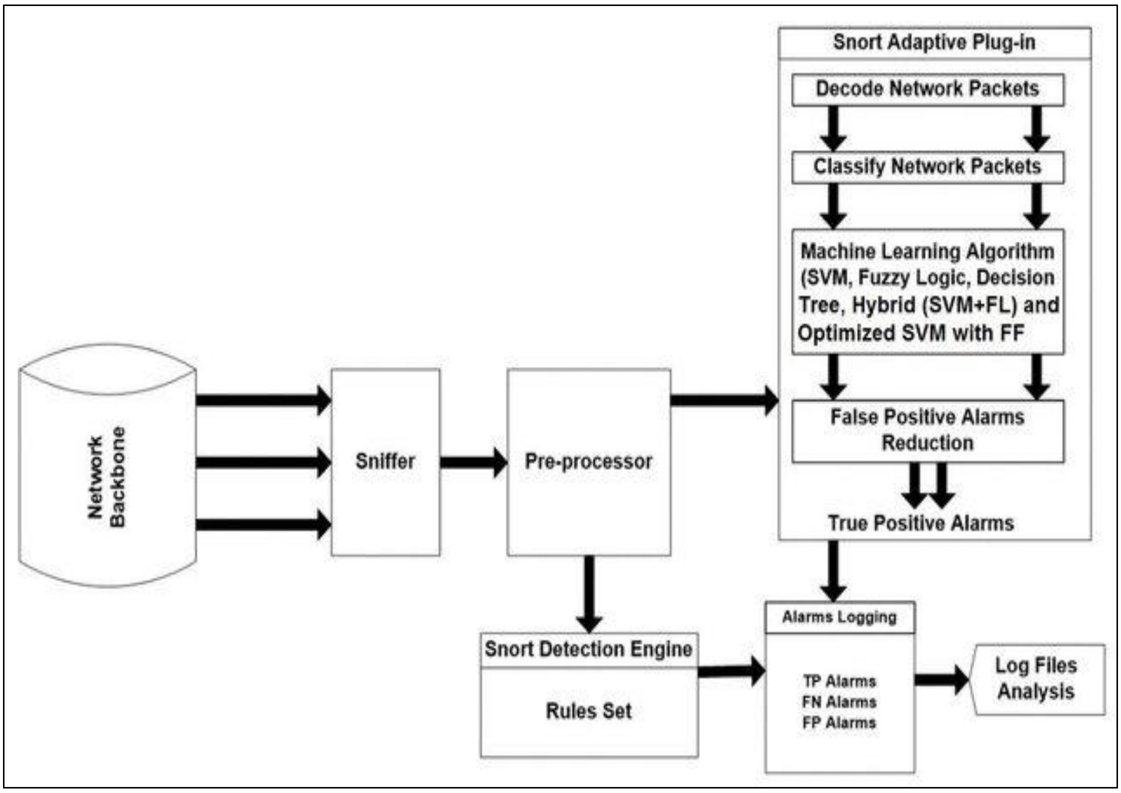
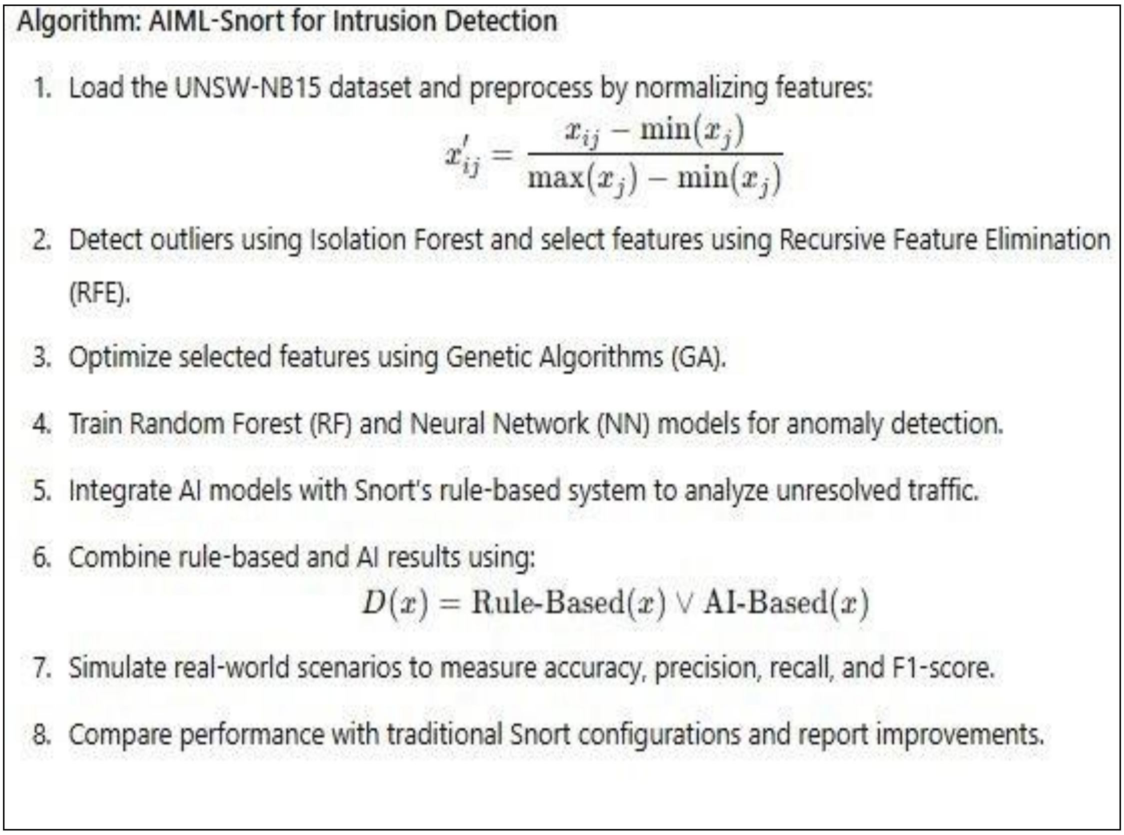


Figure 1: AI-Augmented Snort for Enhanced Intrusion Detection model

Once the features are selected and optimized, machine learning models are trained to classify network traffic as benign or malicious. The framework utilizes two models: Random Forest (RF) and Neural Networks (NN). Random Forest, an ensemble learning method, excels at handling structured data and is highly effective in identifying patterns indicative of network intrusions. Neural Networks, on the other hand, are well-suited for detecting complex, nonlinear patterns, making them particularly effective in identifying evolving threats that traditional systems may fail to detect. These models are trained on the preprocessed dataset, ensuring they can detect both known attack patterns and emerging anomalies in network traffic. The integration of these AI models with Snort forms the core of the proposed methodology.

The integration process combines Snort’s signature-based detection capabilities with the predictive power of machine learning models. Initially, Snort analyzes incoming network traffic, identifying known threats through its extensive rule set. Traffic that cannot be definitively classified by Snort is forwarded to the machine learning models for further analysis. These models then evaluate the unresolved traffic, classifying it as benign or malicious based on their training. The outputs from Snort and the AI models are then aggregated to produce a final decision, ensuring comprehensive threat detection with minimal false positives and negatives. This hybrid approach enables the system to adapt to dynamic network environments, detecting sophisticated attacks that rely on novel or previously unseen patterns.

Algorithm 1: AIML-Snort: A Hybrid Algorithm Integrating AI and Rule-Based Approaches for Intrusion Detection



```
Algorithm: AIML-Snort for Intrusion Detection
1. Load the UNSW-NB15 dataset and preprocess by normalizing features:
       $x'_{ij} = \frac{x_{ij} - \min(x_j)}{\max(x_j) - \min(x_j)}$
2. Detect outliers using Isolation Forest and select features using Recursive Feature Elimination (RFE).
3. Optimize selected features using Genetic Algorithms (GA).
4. Train Random Forest (RF) and Neural Network (NN) models for anomaly detection.
5. Integrate AI models with Snort's rule-based system to analyze unresolved traffic.
6. Combine rule-based and AI results using:
       $D(x) = \text{Rule-Based}(x) \vee \text{AI-Based}(x)$
7. Simulate real-world scenarios to measure accuracy, precision, recall, and F1-score.
8. Compare performance with traditional Snort configurations and report improvements.
```

The performance of the proposed methodology is evaluated through controlled experiments in a simulated network environment. Legitimate traffic is generated using tools like Ostinato, while malicious traffic is introduced using the Metasploit framework. The system is tested under various traffic conditions, including UDP, TCP, and ICMP protocols, to ensure its adaptability to diverse network scenarios. Key performance metrics, such as detection accuracy, false-positive rates, and false-negative rates, are compared to the baseline performance of traditional Snort. Additionally, resource utilization metrics, including CPU and memory usage, are monitored to assess the system's scalability and efficiency under high traffic loads. Results show that the AI-augmented Snort significantly outperforms traditional Snort in detection accuracy, with a notable reduction in error rates and only a marginal increase in resource consumption.

This methodology not only enhances the detection capabilities of Snort but also reduces the manual workload associated with managing security events. By automating the analysis of ambiguous traffic and minimizing false alerts, the system enables security administrators to focus on actual threats. Moreover, the hybrid framework is designed to scale effectively, making it ideal for high-speed, large-scale network environments such as cloud infrastructures and IoT ecosystems. The integration of advanced AI techniques with traditional rule-based detection positions AIML-Snort as a robust and practical solution for modern network security challenges.

4. IMPLEMENTATION AND RESULTS

The proposed methodology involves integrating Snort with machine learning techniques to enhance its intrusion detection capabilities using the UNSW-NB15 dataset. The dataset includes 42 features that represent network traffic attributes and statistical metrics, which are critical for distinguishing between benign and malicious activities. These features include IP addresses, port numbers, protocols, connection states, and statistical metrics such as the number of connections from the same source IP or to the same destination. Feature selection techniques like Recursive Feature Elimination (RFE) are used to identify the most relevant attributes, ensuring optimal performance. Preprocessing steps involve normalizing numerical features, encoding categorical variables, and detecting outliers using Isolation Forest to improve model quality.

Table 1: UNSW-NB15 Dataset Features

S.No.	Feature Name	Description
1	srcip	Source device's IP address
2	sport	Port number assigned to the source
3	dstip	Destination device's IP address
4	dsport	Port number assigned to the destination
5	proto	Network protocol in use (e.g., TCP, UDP, ICMP)
6	state	Current status of the network connection
7	ct_state_ttl	Number of connections sharing the same state and TTL (time-to-live) value
8	ct_flw_http_mthd	Count of HTTP methods used in the connection flow
9	is_ftp_login	Indicates if the FTP session is authenticated (1 = yes, 0 = no)
10	ct_srv_src	Number of connections from the same source IP to a particular service
11	ct_srv_dst	Number of connections targeting the same destination IP and port
12	ct_dst_ltm	Number of connections to the destination IP over the last minute
13	ct_src_ltm	Number of connections from the source IP over the last minute
14	ct_dst_sport_ltm	Number of connections to the same destination port from the same source IP
15	ct_src_dport_ltm	Number of connections to the same source port from the same destination IP

The experimental setup involves simulating a network environment using Oracle VirtualBox with five virtual machines connected via a virtual switch operating at 10 Gbps Ethernet. Legitimate traffic is generated using tools like Ostinato, while malicious traffic is created using the Metasploit framework. Snort, integrated with its default rule set, is deployed on a virtual machine to analyze the combined traffic. Machine learning models, such as Random Forest and Neural Networks, are trained on labeled datasets to classify traffic as benign or malicious. Detection accuracy, false positives, and false negatives are measured to compare Snort's baseline performance with the machine learning-enhanced system. Additionally, resource metrics like CPU usage, memory utilization, and packet drop rates are recorded to evaluate the framework's scalability and efficiency.

4.1. Results

The integration of machine learning techniques with Snort has demonstrated significant improvements across various metrics, establishing the proposed AIML-Snort framework as a robust solution for modern network security challenges. As shown in Table 2, the ML-enhanced Snort achieved a detection accuracy of 94.6%, a substantial improvement over the traditional Snort configuration, which recorded an accuracy of 89.2%. This increase in detection accuracy highlights the effectiveness of the AI-augmented system in identifying complex and evolving cyber threats. Furthermore, the false-positive rate (FPR) was reduced from 5.1% in the traditional Snort to 2.7% in the ML-enhanced Snort, a reduction that directly impacts the usability and reliability of the system by minimizing unnecessary alerts. Similarly, the false-negative rate (FNR) decreased from 7.3% to 3.1%, indicating a significant enhancement in the system's ability to detect and respond to actual intrusions.

Table 2: Performance Comparison between Snort and ML-Enhanced Snort

S.No	Metric	Snort	ML-Enhanced Snort
1	Detection Accuracy (%)	89.2%	94.6%
2	False Positive Rate (%)	5.1%	2.7%
3	False Negative Rate (%)	7.3%	3.1%
4	CPU Utilization (%)	42.5%	49.8%

4	Memory Utilization (GB)	2.8	3.4
6	Packet Drop Rate (%)	1.5%	0.9%

Despite the improvement in detection performance, the ML-enhanced Snort exhibited slightly higher resource utilization. CPU usage increased from 42.5% to 49.8%, and memory utilization rose from 2.8 GB to 3.4 GB. These increases, although marginal, are justified by the significant gains in detection accuracy and efficiency. Additionally, the ML-enhanced Snort demonstrated a lower packet drop rate, reducing from 1.5% to 0.9%, ensuring reliable handling of high-speed network traffic without sacrificing performance.

Table 3: Comparison of Detection Accuracy across Traffic Types

S.No	Traffic Type	Snort Accuracy (%)	ML-Enhanced Snort Accuracy (%)
1	UDP Packets	88.4%	93.8%
2	TCP Packets	89.7%	95.2%
3	ICMP Packets	87.5%	94.1%

The performance of the ML-enhanced Snort was further validated across diverse traffic types, including UDP, TCP, and ICMP traffic, as shown in Table 3. For UDP packets, the detection accuracy increased from 88.4% with traditional Snort to 93.8% with the ML-enhanced version. Similarly, for TCP packets, the accuracy rose from 89.7% to 95.2%, and for ICMP packets, from 87.5% to 94.1%. These consistent improvements across different traffic types highlight the adaptability and robustness of the AIML-Snort framework in handling varied network scenarios. This is particularly critical in modern, dynamic environments where traffic patterns vary significantly based on application types and user behavior.

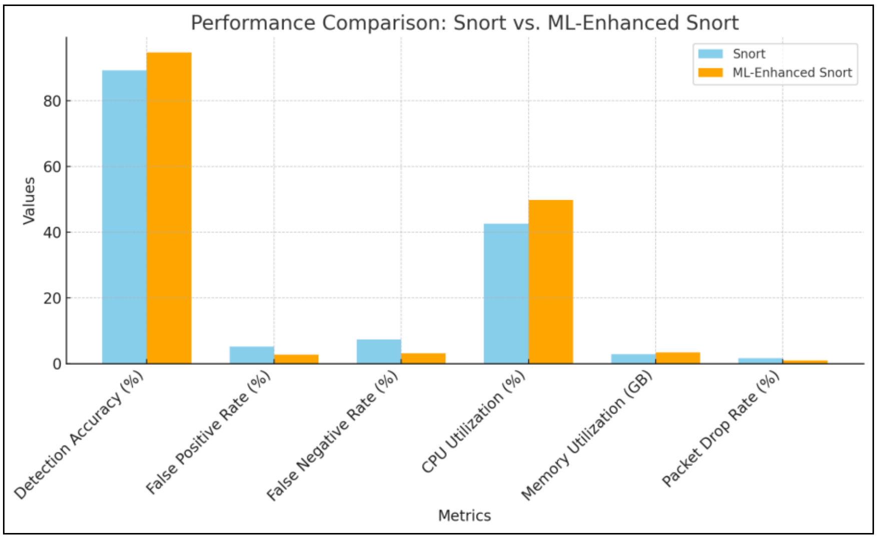


Figure 2: Performance Comparison: Snort vs. ML-Enhanced Snort

Figures 2 and 3 provide a visual representation of these performance gains. In Figure 2, the ML-enhanced Snort consistently outperforms the traditional Snort in key metrics such as detection accuracy, false-positive rate, false-negative rate, and packet drop rate. The slight increase in CPU and memory utilization is evident but remains within acceptable thresholds for high-speed networks, making the enhanced system a practical choice for deployment. Figure 3 illustrates the accuracy improvements for UDP, TCP, and ICMP traffic, showing that the ML-augmented framework is capable of maintaining high performance across all tested protocols.

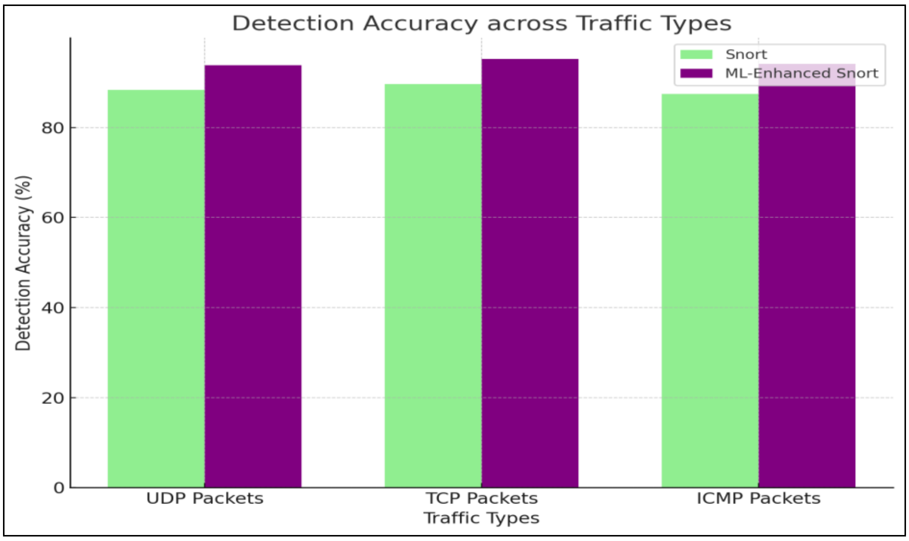


Figure 3: Detection Accuracy across Traffic Types

The improvements in detection accuracy and reduction in error rates can be primarily attributed to the integration of advanced AI techniques within the framework. Preprocessing steps, such as feature normalization, outlier detection using Isolation Forest, and Recursive Feature Elimination (RFE), coupled with Genetic Algorithms (GA) for feature optimization, ensured the generation of high-quality input for training the machine learning models. The combination of Random Forest (RF) and Neural Networks (NN) provided complementary strengths: RF excels at handling structured data, while NN offers superior adaptability to nonlinear patterns. This synergy enabled the ML-enhanced Snort to detect complex attack vectors that traditional systems would otherwise miss.

The framework's performance was rigorously validated in a simulated high-speed network environment designed to replicate real-world scenarios. Traffic conditions were emulated using the UNSW-NB15 dataset, which incorporates a broad range of attack patterns and legitimate traffic. The simulation demonstrated that the ML-enhanced Snort could efficiently process large volumes of data while maintaining high accuracy and minimal packet loss. This scalability ensures that the proposed system can be effectively deployed in large-scale environments, such as enterprise networks, cloud infrastructures, and IoT ecosystems.

The results also underscore the value of combining rule-based and AI-based approaches for intrusion detection. By leveraging Snort's signature-based capabilities and integrating them with AI-driven anomaly detection, the AIML-Snort framework successfully bridges the gap between traditional and modern IDS methodologies. The rule-based system effectively handles known threats, while the AI models excel at detecting novel and evolving attack patterns. The integration of these two approaches guarantees comprehensive coverage of potential vulnerabilities, making AIML-Snort a robust and adaptive intrusion detection solution.

Experimental findings further validate the effectiveness of the AIML-Snort framework in enhancing network security. The ML-enhanced Snort achieves superior detection accuracy, a reduction in false positives and false negatives, and improved scalability compared to the traditional Snort configuration. While resource utilization is slightly higher, it remains well within acceptable limits, ensuring the system's practical applicability in high-speed, large-scale network environments. The consistent performance across various traffic types further reinforces the framework's robustness and adaptability, making it a reliable choice for addressing modern intrusion detection challenges. These results highlight the potential of hybrid IDS frameworks that combine traditional rule-based systems with advanced AI techniques, setting the stage for future advancements in network security solutions.

5. CONCLUSION

The integration of machine learning with Snort significantly improves its intrusion detection capabilities, making it an advanced solution for modern network security. The proposed AI-augmented Snort framework achieves notable enhancements in detection accuracy and precision, reducing false positives and negatives while maintaining efficient resource utilization. Experiments conducted in a controlled virtualized tested highlight its robustness under varying network traffic conditions, including speeds of up to 10 Gbps. The methodology effectively combines signature-based and AI-driven anomaly detection approaches, leveraging machine learning to optimize rule sets and enhance real-time detection. Despite a slight increase in CPU and memory usage, the framework demonstrates improved handling of diverse traffic types, including UDP, TCP, and ICMP, with lower packet drop rates. These results emphasize the scalability and efficiency of the proposed system, establishing it as a practical and reliable solution for protecting modern, high-speed, and complex network infrastructures.

6. REFERENCES

[1] Sowmya, T.; Anita, E.M. A comprehensive review of AI based intrusion detection system. Meas. Sens. 2023, 28, 100827.

[2] Nuaimi, M.; Fourati, L.C.; Ben Hamed, B. Intelligent approaches toward intrusion detection systems for Industrial Internet of Things: A systematic comprehensive review. J. Netw. Comput. Appl. 2023, 215, 103637.

[3] Abid, A.; Jemili, F.; Korbaa, O. Real-time data fusion for intrusion detection in industrial control systems based on cloud computing and big data techniques. Clust. Comput. 2023, 1–22.

[4] Salvakkam, D.B.; Saravanan, V.; Jain, P.K.; Pamula, R. Enhanced Quantum-Secure Ensemble Intrusion Detection Techniques for Cloud Based on Deep Learning. Cogn. Comput. 2023, 15, 1593–1612.

[5] Raj, M.G.; Pani, S.K. Hybrid feature selection and BWTDO enabled DeepCNN-TL for intrusion detection in fuzzy cloud computing. Soft Comput. 2023, 1–20.

[6] Rana, P.; Batra, I.; Malik, A.; Imoize, A.L.; Kim, Y.; Pani, S.K.; Goyal, N.; Kumar, A.; Rho, S. Intrusion Detection Systems in Cloud Computing Paradigm: Analysis and Overview. Complexity 2022, 2022, 3999039.

[7] Wang, S.; Xu, W.; Liu, Y. Res-TranBiLSTM: An Intelligent Approach for Intrusion Detection in the Internet of Things. Comput. Netw. 2023, 235, 109982.

[8] Javadpour, A.; Pinto, P.; Ja'fari, F.; Zhang, W. DMAIDPS: A distributed multi-agent intrusion detection and prevention system for cloud IoT environments. Clust. Comput. 2022, 26, 367–384.

[9] Chou, D.; Jiang, M. A survey on data-driven network intrusion detection. ACM Comput. Surv. 2021, 54, 1–36.

[10] Kavitha, C.; Gadekallu, T.R.K.N.; Kavin, B.P.; Lai, W.C. Filter-Based Ensemble Feature Selection and Deep Learning Model for Intrusion Detection in Cloud Computing. Electronics 2023, 12, 556.

[11] Prabhakaran, V.; Kulandasamy, A. Hybrid semantic deep learning architecture and optimal advanced encryption standard key management scheme for secure cloud storage and intrusion detection. Neural Comput. Appl. 2021, 33, 14459–14479.

[12] Ghosh, P.; Sarkar, D.; Sharma, J.; Phadikar, S. An intrusion detection system using modified-firefly algorithm in cloud environment. Int. J. Digit. Crime Forensics (IJDCF) 2021, 13, 77–93.

[13] Alzaqebah, A.; Aljarah, I.; Al-Kadi, O.; Damaševičius, R. A Modified Grey Wolf Optimization Algorithm for an Intrusion Detection System. Mathematics 2022, 10, 999.

[14] Zivkovic, M.; Bacanin, N.; Arandjelovic, J.; Rakic, A.; Strumberger, I.; Venkatachalam, K.; Joseph, P.M. Novel Harris Hawks Optimization and Deep Neural Network Approach for Intrusion Detection. In Proceedings of the International Joint Conference on Advances in Computational Intelligence, Singapore, 19 May 2022; pp. 239–250.

[15] Tajari Siahmarzkooh, A.; Alimardani, M. A Novel Anomaly-based Intrusion Detection System using Whale Optimization Algorithm WOA-Based Intrusion Detection System. *Int. J. Web Res.* 2021, *4*, 8–15.

[16] D. B. Deebak and S. O. Hwang, "Healthcare Applications Using Blockchain With a Cloud-Assisted Decentralized Privacy-Preserving Framework," *IEEE Transactions on Mobile Computing*, vol. 23, no. 5, pp. 5897–5916, 2024. doi: 10.1109/TMC.2023.3315510.

[17] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: a systematic study of machine learning and deep learning approaches," *Transactions on Emerging Telecommunications Technologies*, vol. 32, p. e4150, 2021.

[18] A. Heidari, N. J. Navimipour, and M. Unal, "A secure intrusion detection platform using blockchain and radial basis function neural networks for internet of drones," *IEEE Internet of Things Journal*, vol. 10, pp. 8445–8454, 2023.

[19] Z. Chkirbene, A. Erbad, R. Hamila, A. Mohamed, M. Guizani, and M. Hamdi, "Tidcs: A dynamic intrusion detection and classification system based on feature selection," *IEEE Access*, vol. 8, pp. 95864–95877, 2020.

[20] J. Kim, J. Shin, K.-W. Park, and T. S. Jung, "Improving Method of Anomaly Detection Performance for Industrial IoT Environment," *Computers, Materials & Continua*, vol. 72, no. 3, pp. 5377–5394, 2022. doi: 10.32604/cmc.2022.026619.

[21] S. R. Hassan, A. U. Rehman, N. Alsharabi, S. Arain, A. Quddus, and H. Hamam, "Design of load-aware resource allocation for heterogeneous fog computing systems," *PeerJ Computer Science*, vol. 10, p. e1986, 2024. doi: 10.7717/peerj-cs.1986.

[22] A. Heidari, N. J. Navimipour, H. Dag, and M. Unal, "Deepfake detection using deep learning methods: A systematic and comprehensive review," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 14, p. e1520, 2024.

[23] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, "CNN-LSTM: Hybrid deep neural network for network intrusion detection system," *IEEE Access*, vol. 10, pp. 99837–99849, 2022.

[24] B. Molina-Coronado, U. Mori, A. Mendiburu, and J. Miguel-Alonso, "Survey of network intrusion detection methods from the perspective of the knowledge discovery in databases process," *IEEE Transactions on Network and Service Management*, vol. 17, no. 4, pp. 2451–2479, 2020.

[25] A. Heidari, N. J. Navimipour, M. Unal, and G. Zhang, "Machine learning applications in internet-of-drones: Systematic review, recent deployments, and open issues," *ACM Computing Surveys*, vol. 55, no. 12, pp. 1–45, 2023.

[26] S. M. S. Bukhari, M. H. Zafar, M. A. Houran, S. K. R. Moosavi, M. Mansoor, M. Muaaz, and F. Sanfilippo, "Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-BI-LSTM for enhanced reliability," *Ad Hoc Networks*, vol. 155, p. 103407, 2024.

[27] A. V. Hanafi, A. Ghaffari, H. Rezaei, A. Valipour, and B. Arasteh, "Intrusion detection in internet of things using improved binary golden jackal optimization algorithm and LSTM," *Cluster Computing*, vol. 27, no. 3, pp. 2673–2690, 2024.

[28] L. K. Vashishtha, A. P. Singh, and K. Chatterjee, "HIDM: A hybrid intrusion detection model for cloud-based systems," *Wireless Personal Communications*, vol. 128, pp. 2637–2666, 2023.

[29] V. Hnamte, H. Hussain, J. Hussain, and Y. H. Kim, "A novel two-stage deep learning model for network intrusion detection: LSTM-AE," *IEEE Access*, 2023.

[30] Khawlah Harahsheh, Malek Alzaqebah and Chung-Hao Chen, “An Enhanced Real-Time Intrusion Detection Framework Using Federated Transfer Learning in Large-Scale IoT Networks” International Journal of Advanced Computer Science and Applications(IJACSA), 15(12), 2024. http://dx.doi.org/10.14569/IJACSA.2024.0151204

[31] M. A. Talukder, K. F. Hasan, M. M. Islam, M. A. Uddin, A. Akhter, M. A. Yousuf, F. Alharbi, and M. A. Moni, "A dependable hybrid machine learning model for network intrusion detection," Journal of Information Security and Applications, vol. 72, p. 103405, 2023.