WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

Journal homepage: www.ijrpr.com ISSN 2582-7421

# AI Based Packet Sniffer for Secure Traffic Analysis

***Dhivya K, Pooja R, Pooja Nair R V, Praveen B, Surya S J, Yokesh A***

*Computer Science and Engineering (Cyber Security), Sri Shakthi Institue of Engineering and Technology, Tamil Nadu, India.*

**A B S T R A C T**

In the evolving landscape of cybersecurity, the increasing volume and complexity of network traffic demand intelligent solutions for real-time monitoring and threat detection. This project proposes the design and implementation of an AI-based packet sniffer that leverages machine learning algorithms to analyse network packets for potential security threats. Unlike traditional sniffers that rely on manual inspection or static rule sets, the proposed system uses anomaly-based detection to identify suspicious patterns, unauthorized access attempts, and data exfiltration activities. By integrating deep packet inspection with AI-driven traffic classification, the system can accurately distinguish between normal and malicious behaviour, thereby improving the speed and accuracy of threat identification. The packet sniffer is built using Python and employs libraries such as Scapy for packet capturing and Scikit-learn or TensorFlow for AI model integration. This intelligent sniffer not only enhances network visibility but also serves as a proactive security tool capable of adapting to new and evolving threats, making it a valuable asset for modern secure network infrastructures.

Keywords: AI-based, Packet sniffer, Network traffic, Threat detection, Machine learning, Anomaly-based detection, Deep packet inspection, Traffic classification, Scapy, Cybersecurity

## 1. INTRODUCTION

In today's digital age, network security has become a critical concern for individuals, enterprises, and governments alike. With the exponential growth of internet usage, cloud computing, and IoT devices, networks are continuously exposed to a wide range of cyber threats such as malware injection, phishing, data breaches, and denial-of-service attacks. Traditional network monitoring tools often fall short in identifying sophisticated or previously unseen attacks, as they typically rely on predefined signatures or manual analysis. This limitation has led to the growing interest in intelligent traffic analysis systems that can learn and adapt dynamically. Packet sniffers, which are tools designed to intercept and analyse data packets traveling across a network, have long been used for diagnostic and monitoring purposes. However, when combined with artificial intelligence and machine learning techniques, packet sniffers can evolve into powerful tools capable of detecting anomalous behavior and hidden threats in real-time. This project introduces an AI-based packet sniffer that uses deep learning or machine learning algorithms to perform secure traffic analysis by identifying abnormal traffic patterns, suspicious payloads, and unauthorized activitiesThe system aims to not only detect intrusions but also to classify traffic types and flag potential zero-day exploits. By leveraging libraries like Scapy for packet capture and Scikit-learn or TensorFlow for intelligent data processing, the project integrates real-time monitoring with smart decision-making capabilities. Such an approach ensures a proactive stance in cybersecurity, enabling faster response to threats, minimizing human error, and providing deep insights into the behavior of both internal and external traffic.

## *2.* LITERATURE SURVEY

As the Recent research in network security highlights the growing importance of AI and machine learning in enhancing traffic analysis and intrusion detection systems. Traditional packet sniffers like Wireshark and tcpdump are widely used for monitoring, but they lack the intelligence to detect zero-day attacks or evolving threat patterns. Studies such as [1] and [2] have demonstrated that machine learning models, including decision trees, random forests, and neural networks, can significantly improve the accuracy of anomaly detection in network traffic. Authors in [3] explored the use of deep learning for classifying encrypted and unencrypted traffic, showing promising results in identifying malicious payloads. Similarly, [4] proposed an intelligent packet inspection framework using unsupervised learning to detect unknown attacks in real-time. The integration of tools like Scapy for packet capture and Scikit-learn or TensorFlow for model training has become a standard approach in several recent projects [5], [6]. Moreover, literature also emphasizes the challenges of handling imbalanced datasets, high-speed traffic, and feature selection, which are actively being addressed through hybrid detection systems and adaptive learning techniques [7], [8]. Overall, the existing body of work suggests that AI-based sniffers offer a scalable and efficient alternative to rule-based systems for securing modern networks.

## 3. ARCHITECTURAL METHODOLOGY

The proposed AI-based packet sniffer follows a modular architecture that integrates real-time packet capturing tools with backend AI-driven traffic analysis components. The system is designed for scalability, accuracy, and efficient anomaly detection in live network environments. Each module—from data capture and preprocessing to classification, alerting, and reporting—works in coordination to provide a seamless and intelligent network monitoring experience for security professionals.

### *3.1. Data Capture Module:*

This module uses packet sniffing tools like **Scapy** to intercept live network traffic. It captures headers and payloads of each packet in real-time. The captured data is stored temporarily for preprocessing.

### *3.2. Data Preprocessing:*

Uploaded Captured packets are filtered, cleaned, and transformed into a structured format. Important features like IP address, port, protocol, and packet size are extracted. Noise and irrelevant data are removed for better analysis.

### *3.3. Feature Extraction:*

Relevant features are selected to train the AI model effectively. Techniques like PCA or manual selection help identify key attributes. This step ensures reduced dimensionality and improved model performance.

### *3.4. Model Training:*

Machine learning algorithms like Decision Tree, Random Forest, or Neural Networks are trained using labeled datasets. The model learns to distinguish between normal and malicious traffic. Datasets used may include NSL-KDD or custom traffic data

### *3.5. Real-Time Traffic Classification:*

The trained model is deployed to classify incoming traffic in real-time. Packets are labeled as normal or suspicious based on learned patterns. This helps in immediate detection and alert generation.

### *3.6. Alert and Logging System:*

When suspicious traffic is detected, alerts are generated and logs are maintained. The alert system can notify administrators through email or dashboard. Logs store details like timestamp, source IP, and type of anomaly.

### *3.7. Visualization and Reporting:*

A user-friendly dashboard is developed to provide real-time visualization of network traffic and detected threats. It includes interactive graphs, pie charts, and timelines to show traffic types, volume, protocol distribution, and alert frequency. The interface helps network administrators monitor anomalies at a glance and take quick action. Detailed reports containing information about detected attacks, affected IP addresses, and timestamps are automatically generated and can be exported in formats like PDF or CSV.

## 4. CONCLUSION AND FUTURE ENHANCEMENT

In conclusion, the AI-based packet sniffer developed in this project provides an intelligent and efficient solution for secure traffic analysis by combining real-time packet capturing with machine learning-based anomaly detection. It overcomes the limitations of traditional sniffers by adapting to evolving threats and accurately identifying suspicious network behavior. With integrated modules for preprocessing, classification, and alerting, the system ensures proactive threat detection and improved network visibility. This project highlights the growing role of AI in building scalable and resilient cybersecurity tools for modern digital infrastructures.

### *Future Enhancements*

**To further improve the system's performance and scalability, the following enhancements can be considered:**

1. **Advanced Machine Learning Models:** Integrate deep learning techniques and continual learning to improve detection of emerging threats and reduce false positives.

2. **Cloud-Based Deployment:** Deploy the system on cloud platforms like AWS or Azure to enable scalable traffic analysis for large enterprise networks
3. **Encrypted Traffic Analysis:** Incorporate methods to analyse encrypted traffic without decryption, using metadata and behavioral patterns**.**
4. **Automated Threat Response:** Develop modules that not only detect but also automatically respond to threats by isolating affected hosts or blocking suspicious traffic.
5. **Real-Time Dashboard:** Build an interactive dashboard for administrators to visualize live traffic, alerts, and historical trends with customizable filters.
6. **Integration with SIEM Systems:** Enable seamless API integration with Security Information and Event Management (SIEM) tools for centralized monitoring.
7. **Anomaly Explanation Module:** Implement explainable AI features that provide insights into why a particular packet or flow was flagged as suspicious
8. **Multi-Protocol Support:** Extend support to analyse traffic from a wider range of protocols beyond TCP/IP, such as IoT-specific protocols.

**References**

1. Wang, Z., Fok, K.-W., & Thing, V. L. L. (2022). Machine Learning for Encrypted Malicious Traffic Detection: Approaches, Datasets and Comparative Study. arXiv preprint arXiv:2203.09332
2. Wang, H., Zhou, S., Li, H., Hu, J., Du, X., Fu, F., & Yang, H. (2022). Deep Learning Network Intrusion Detection Based on Network Traffic. In Artificial Intelligence and Security (pp. 186–198). Springer, Cham.
3. Bhuvaneswari Amma, N. G. (2022). Network Traffic Classification Using Deep Autonomous Learning Approach. In Security, Privacy and Data Analytics (pp. 183–190). Springer, Singapore.
4. Rehan, H. (2022). Deep Learning for Network Traffic Analysis: Detecting Security Breaches in Real-Time. Advances in Deep Learning Techniques, 2(1), 154–193.
5. Zhang, L., & Wang, J. (2022). Network Traffic Classification Based On A Deep Learning Approach Using NetFlow Data. The Computer Journal, 66(8), 1882–1892.
6. Caville, E., Lo, W. W., Layeghy, S., & Portmann, M. (2022). Anomal-E: A Self-Supervised Network Intrusion Detection System based on Graph Neural Networks. arXiv preprint arXiv:2207. 06819.Pokala,
7. Zeleke, S. N., Jember, A. F., & Bochicchio, M. (2025). Integrating Explainable AI for Effective Malware Detection in Encrypted Network Traffic.
8. Fu, C., Li, Q., & Xu, K. (2023). Detecting Unknown Encrypted Malicious Traffic in Real Time via Flow Interaction Graph Analysis.
9. Wang, Z., Fok, K.-W., & Thing, V. L. L. (2022). Machine Learning for Encrypted Malicious Traffic Detection: Approaches, Datasets and Comparative Study.
10. Farrukh, Y. A., Wali, S., Khan, I., & Bastian, N. D. (2024). XG-NID: Dual-Modality Network Intrusion Detection using a Heterogeneous Graph Neural Network and Large Language Model.