Journal of Advanced Robotics, Autonomous Systems and Human-Machine Interaction ISSN: 3070-6491

PRIME OPEN ACCESS

Volume 2, Issue 3

Research Article

Date of Submission: 29 May, 2026
Date of Acceptance: 30 Jun, 2026
Date of Publication: 10 July, 2026

Smart Secure: An AI-Driven Network Threat Analysis & Detection Framework

Devesh Krishn*, Aahana Mohanty, Avishkar Nivas, Rakshith C Prakhyath and Giri Vardhan Santhosh Kumar

Student RVCE, India

***Corresponding Author:** Devesh Krishn, Student RVCE, India.

Citation: Krishn, D., Mohanty, A., Nivas, A., Prakhyath, R. C., Kumar, G. V. S. (2026). Smart Secure: an ai-driven network threat analysis & detection framework. *J Adv Robot Auton Syst Hum Mach Interact, 2*(3), 01-05.

Abstract (Problem & Approach)

The rapid growth of network-based services has led to a significant rise in sophisticated cyberattacks that closely resemble legitimate traffic patterns. Traditional signature-based Intrusion Detection Systems (IDS) are increasingly ineffective against such evolving threats, particularly zero-day and behavior-based attacks. This paper presents SmartSecure, a lightweight AI-based real-time Intrusion Detection System that combines offline machine learning training with live packet sniffing for dynamic attack detection. The proposed system captures network traffic, aggregates packets into flows, extracts behavioral features, and classifies traffic using a supervised RandomForest model trained on benchmark intrusion datasets. A real-time backend API streams detection results to a web-based dashboard for visualization and alerting. Experimental evaluation demonstrates that the system effectively detects multiple attack categories including DDoS, brute-force, port scanning, botnet communication, and web attacks while maintaining low computational overhead. The results indicate that SmartSecure bridges the gap between academic IDS research and practical, deployable cybersecurity solutions.

Keywords: Network Security, Real-Time Detection, Behavioural Analysis, Random Forest

Introduction

Modern computer networks face a rapidly evolving threat landscape where cyberattacks increasingly blend into normal traffic behavior. Distributed Denial of Service (DDoS) attacks, brute-force authentication attempts, botnet command-and-control communication, and web-based exploits continue to grow in both scale and sophistication. Traditional intrusion detection tools rely heavily on predefined signatures and static rules, which limits their ability to detect new or modified attack patterns. Machine learning-based IDS have emerged as a promising alternative due to their ability to learn behavioral characteristics of malicious traffic. However, many proposed systems remain confined to offline evaluation, lack real-time feasibility, or require extensive computational resources. This paper addresses these challenges by proposing SmartSecure, an AI-driven IDS designed for real-time deployment on consumer-grade hardware. The system emphasizes behavioral analysis, privacy-preserving packet inspection, and modular design to support practical adoption.

Literature Review

Nawaz, M., Tahira, S., Shah, D., Ali, S., & Tahir, M. (2025). Lightweight machine learning framework for efficient DDoS attack detection in IoT networks.This work proposes a lightweight machine-learning framework for DDoS detection tailored to IoT and edge environments, emphasizing low CPU and memory usage while maintaining high detection accuracy. The study demonstrates the feasibility of real-time detection under constrained resources. However, the framework faces challenges in generalizing across heterogeneous network conditions and does not extensively evaluate performance under diverse real-world traffic patterns or evolving attack behaviors. Mari, A.-G., Zinca, D., & Dobrota, V. (2023). Development of a machine-learning intrusion detection system and testing of its performance using a generative adversarial network. The authors develop a machine-learning-based intrusion detection system and enhance its robustness by generating adversarial traffic using a Generative Adversarial Network (GAN). Their approach highlights the vulnerability of traditional IDS models to adversarial manipulation and shows improved detection after retraining. Nevertheless, the evaluation is limited to the NSL-KDD dataset, and the study lacks real-time deployment analysis and testing on encrypted or high-speed network traffic. Arroju, S., Adunoori, B., Jadhav, R., Jakkula, J., & Sreelakshmi, R. (2025). Detecting web attacks with end-to-end deep learning..This paper presents an end-to-end deep learning

approach for detecting web attacks using stacked denoising autoencoders applied to runtime call-graph traces. The method eliminates the need for manual feature engineering and successfully identifies multiple web-based attacks. Key limitations include reduced explainability of detection decisions and limited evaluation on large-scale production web workloads, where false positives may increase. Mohamed, A. A., Al-Saleh, A., Sharma, S. K., et al. (2025). Zero-day exploits detection with adaptive WavePCA-Autoencoder (AWPA) adaptive hybrid exploit detection network (AHEDNet). The authors introduce a hybrid zero-day exploit detection system combining Adaptive WavePCA, transformer-based autoencoders, and evolutionary optimization techniques. The model achieves strong performance in detecting previously unseen exploits. However, its computational complexity and reliance on multi-stage processing make it unsuitable for lightweight or real-time deployment without further optimization or model compression. De Resende, A. A. M., De Melo, P. H. A. D., Souza, J. R., Cattelan, R. G., & Miani, R. S. (2022). Traffic classification of home network devices using supervised learning.This study focuses on classifying home network device traffic using supervised learning techniques and flow-level features, achieving high classification accuracy in controlled environments. The results demonstrate the effectiveness of behavioral traffic analysis for device identification. However, the evaluation is limited to small-scale home networks and does not consider encrypted traffic, adversarial behavior, or large-scale deployment scenarios. Harini, M. (2025). Command and control traffic detection and mitigation in botnet driven networks. The paper proposes a real-time system for detecting botnet command-and-control traffic using behavior correlation across multiple detection modules. The approach reduces dependence on heavy AI models and is designed for practical deployment. Despite its effectiveness, the system experiences increased false positives in highly dynamic network environments, indicating the need for adaptive thresholding and learning mechanisms. Wu, H. (2024). Heartbleed OpenSSL vulnerability: A forensic case study at a medical school. This work provides a forensic analysis of the Heartbleed OpenSSL vulnerability, detailing its technical operation, impact, and exploitation in a real institutional environment. The study contributes valuable insights into post-incident analysis and vulnerability assessment. However, it focuses primarily on forensic investigation and does not propose automated or proactive detection mechanisms for real-time intrusion prevention. Alosimy, H., AlZaidi, J., Alajmani, S. H., & Soh, B. (2025). An algorithm for detecting brute force attacks on FTP and SSH services utilizing deep learning with probabilistic neural networks (PNN).The authors present a deep learning-based probabilistic neural network optimized with a Bat algorithm to detect brute-force attacks targeting FTP and SSH services. The model achieves exceptionally high accuracy, precision, and recall on benchmark datasets. Nonetheless, the approach is limited to specific protocols, lacks validation on encrypted authentication mechanisms, and requires further evaluation for real-time, multi-service deployment.

System Design And Implementation

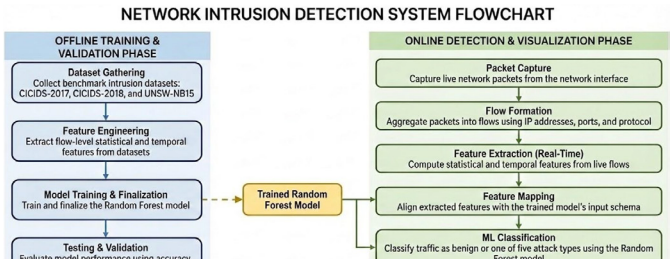
SmartSecure is designed as a modular real-time intrusion detection framework that integrates offline machine learning training with live network monitoring. The system operates entirely on metadata and flow-level features, ensuring user privacy while enabling behavioral detection.

System Architecture

The system consists of the following components (also shown in Figure.1):

- Packet Sniffer
- Flow Aggregation Engine
- Feature Extraction Module
- Feature Mapping and Preprocessing
- Machine Learning Inference Engine
- Decision and Alerting Module
- Web-based Visualization Dashboard

System Implementation



Figure

Backend

The backend is implemented in Python and handles real-time packet capture, flow aggregation, feature extraction, and machine learning–based intrusion detection. Network packets are captured from the host interface and aggregated into flows to enable behavior-based analysis. Flow-level features are mapped to a pre-trained supervised learning model, which classifies traffic as benign or malicious in real time. The backend exposes API endpoints for prediction and live alert streaming, ensuring modular and privacy-preserving operation by analyzing only packet metadata.

Frontend

The frontend is a web-based dashboard developed using modern JavaScript frameworks to visualize detected intrusions and system status. It communicates with the backend through REST and real-time interfaces to display alerts, attack categories, and timestamps. The interface is designed to be lightweight and user-friendly, enabling non-expert users to monitor network security through any standard web browser.

Database and Storage

The system does not rely on a centralized database for real-time detection. Instead, lightweight local storage mechanisms such as structured log files are used to record alerts and flow summaries. This design reduces latency, minimizes resource consumption, and avoids additional security risks. Logged data can optionally be used for offline analysis, evaluation, or future model retraining, while allowing database integration for extended deployments.

Methodology

- **Data Collection**

Network data is obtained through two methods: passive live packet capture and simulated attack traffic. Public datasets such as CIC-IDS2017, UNSW-NB15, and CIC-DDoS2019 are used for offline training.

- **Flow Aggregation and Feature Engineering**

Packets are aggregated into flows using standard 5-tuple identifiers. Flow-level features include packet counts, byte statistics, duration, inter-arrival times, TCP flag counts, and rate-based metrics.

- **Machine Learning Model**

A RandomForest classifier is employed due to its robustness on tabular data, resistance to overfitting, and low inference latency. The model is trained using labeled attack categories and evaluated using accuracy, precision, recall, and F1-score.

- **Real-Time Detection**

Live packets are captured using a lightweight sniffer. Extracted features are mapped to the trained model's input schema and classified in real time. Alerts are generated for malicious flows and streamed to the dashboard.

Results

The proposed SmartSecure intrusion detection system was evaluated using a combination of offline benchmark datasets and controlled real-time attack simulations. The trained RandomForest model demonstrated strong classification performance across multiple attack categories, including DDoS, port scanning, brute-force attempts, botnet communication, and web-based attacks. Experimental results showed high detection accuracy with a low false-positive rate, indicating effective differentiation between benign and malicious traffic. During real-time testing, the system successfully identified simulated attacks with minimal detection latency, confirming its suitability for live network monitoring. Additionally, the lightweight architecture ensured low CPU and memory utilization on consumer-grade hardware, validating the feasibility of deploying the system in small networks and academic environments. These results highlight the effectiveness of behavior-based machine learning for real-time intrusion detection while maintaining efficiency and practical deployability.

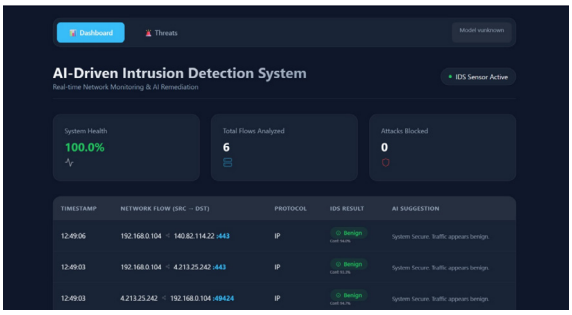


Figure 1: IDS Dashboard – System Health and Traffic Status

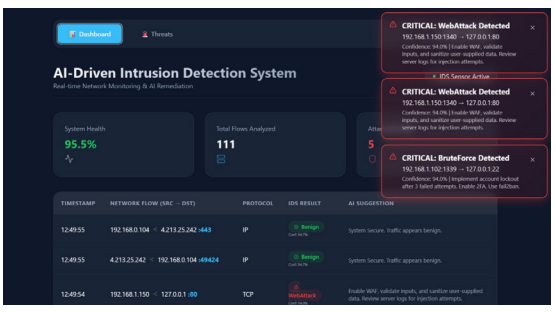


Figure 2: Real-Time Alert Notifications

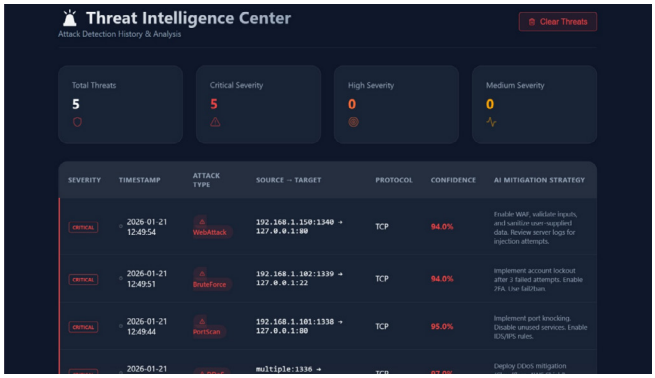


Figure 3: Threat Intelligence Center – Detection Summary

Conclusion

This project successfully designed and implemented a machine learning–based Intrusion Detection System (IDS) capable of monitoring real-time network traffic and detecting multiple types of cyber-attacks. The system effectively captures live packets, processes them through backend preprocessing modules, and classifies the traffic using trained attack-specific machine learning models. The developed system accurately identifies attack categories such as DoS, DDoS, Port Scan, Brute Force, and Web-based attacks, while correctly classifying normal traffic. The integration of a web-based dashboard enables clear visualization of detection results, making the system user-friendly and practical for real-world applications. Overall, the project achieved its primary objectives by delivering a reliable, scalable, and efficient intrusion detection solution that demonstrates the effectiveness of machine learning techniques in network security

Limitations and Scope

The proposed intrusion detection system has certain inherent limitations that should be considered when interpreting results: (i) the system relies on supervised machine learning models trained on publicly available benchmark datasets, which may not fully capture unseen or highly novel attack patterns in real-world networks; (ii) feature extraction is performed at the flow level, which can smooth fine-grained packet-level behaviors and may reduce sensitivity to very short-lived or stealthy attacks; (iii) real-time packet sniffing requires elevated system privileges and sufficient network visibility, limiting deployment in highly restricted or encrypted environments; and (iv) model performance can be affected by class imbalance, traffic drift, and changes in network behavior over time, requiring periodic retraining and tuning. Within these bounds, The IDS is suitable for real-time network monitoring, behavior-based attack detection, educational demonstrations, and deployment in small to medium-scale networks such as campuses, smart homes, and laboratories. However, it is not intended as a replacement for enterprise-grade security infrastructure, deep packet inspection of encrypted payloads, or legally certified forensic analysis systems [1-8].

Outcomes

• The system successfully captures and analyzes live network traffic in real time using packet sniffing and flow-based processing.
• The ML-based IDS can identify major cyberattacks such as DoS/DDoS, port scanning, brute-force attacks, web attacks, and botnet-like behavior.
• Network traffic is automatically converted into flow-level features and classified without manual intervention.
• Lightweight supervised ML models (e.g., Random Forest) demonstrate strong performance with balanced accuracy and reduced false positives.
• A web-based dashboard provides clear alerts, threat categorization, and real-time visual insights for easier security monitoring.
• The system analyzes packet headers and flow metadata instead of payloads, reducing the risk of sensitive data exposure.
• The project shows that AI-driven IDS can be implemented on end devices or small networks with modest computational resources.
• The modular design supports future extensions such as advanced models, encrypted traffic analysis, online learning, and production deployment.
• Provided a transparent and deterministic evaluation pipeline, ensuring consistent results and easy reproducibility for academic and planning applications.

References

1. Nawaz, M., Tahira, S., Shah, D., Ali, S., & Tahir, M. (2025). Lightweight machine learning framework for efficient DDoS attack detection in IoT networks. *Scientific Reports, 15*(1), 24961.
2. Mari, A. G., Zinca, D., & Dobrota, V. (2023). Development of a machine-learning intrusion detection system and testing of its performance using a generative adversarial network. *Sensors, 23*(3), 1315.
3. S. Arroju, B. Adunoori, R. Jadhav, J. Jakkula, and R. Sreelakshmi.(2025).“Detecting web attacks with end-to-end deep learning,” Journal of Computer Allied Intelligence, vol. 3, pp. 36–46,.
4. Mohamed, A. A., Al-Saleh, A., Sharma, S. K., & Tejani, G. G. (2025). Zero-day exploits detection with adaptive

WavePCA-Autoencoder (AWPA) adaptive hybrid exploit detection network (AHEDNet). *Scientific Reports, 15*(1), 4036.
5. De Resende, A. A., De Melo, P. H., Souza, J. R., Cattelan, R. G., & Miani, R. S. (2022, February). Traffic Classification of Home Network Devices using Supervised Learning. *In ICAART (3)* (pp. 114-120).
6. M. Harini, "Command and control traffic detection and mitigation in botnet driven networks," International Journal for Research in Applied Science and Engineering Technology, vol. 13, no. 3, pp. 1038–1043, 2025,
7. H. Wu.(2024). "Heartbleed OpenSSL vulnerability: A forensic case study at medical school," *NJMS Advancing Research IT,* Rutgers University.
8. Alosimy, H., AlZaidi, J., Alajmani, S. H., & Soh, B. (2025). An Algorithm for Detecting Brute Force Attacks on FTP and SSH Services Utilizing Deep Learning with Probabilistic Neural Networks (PNN). *INTERNATIONAL JOURNAL, 13*(6), 1-9.