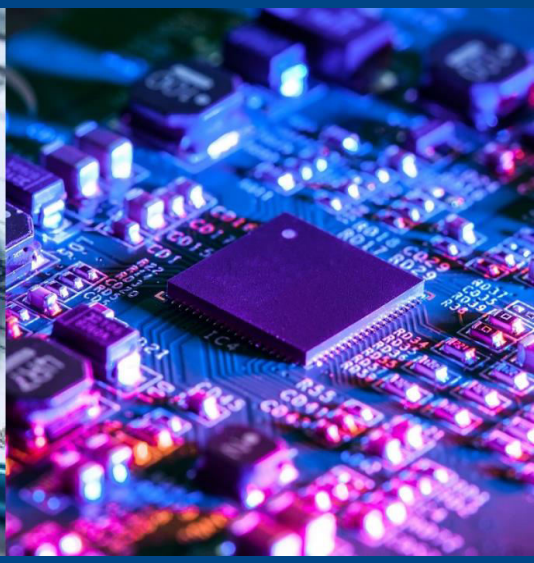
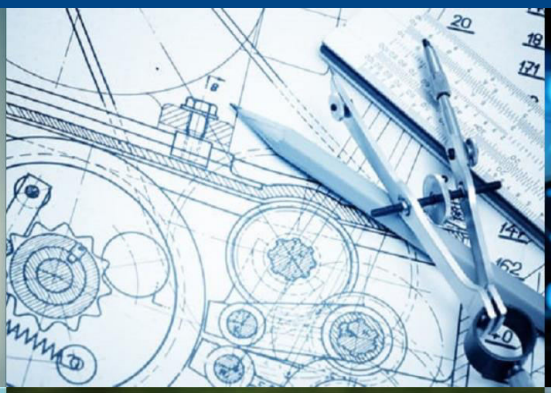
ISSN: 2582-7219

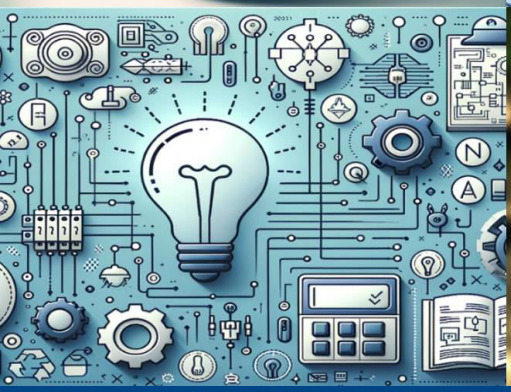




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 9, Issue 3, March 2026**

© 2026 IJMRSET | Volume 9, Issue 3, March 2026| DOI:10.15680/IJMRSET.2026.0903028

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

WiFi Intrusion Detection using Feature Extraction and Machine Learning

A Christy[1], Dr.D.Hari Prasad[2], Dr. C. Daniel Nesakumar[3]

Student, Department of Computer Applications, Sri Ramakrishna College of Arts and Science, Coimbatore, Tamil Nadu, India [1]

Associate Professor & Head, Department of Computer Applications, Sri Ramakrishna College of Arts and Science, Coimbatore, Tamil Nadu, India [2]

Assistant Professor, Department of Computer Applications, Sri Ramakrishna College of Arts & Science, Coimbatore, Tamil Nadu, India [3]

ABSTRACT: WiFi networks are increasingly targeted by sophisticated cyberattacks that bypass conventional security mechanisms. This paper presents a real-time WiFi Intrusion Detection System (IDS) that combines feature extraction with machine learning techniques to identify malicious traffic patterns. The system captures live network packets using Scapy and computes statistical features—such as packet rate, protocol ratios, port scan indicators, and deauthentication counts—within sliding time windows. A Random Forest classifier trained on the AWID dataset is used to distinguish normal traffic from various attack types, including flooding, impersonation, injection, and cracking attacks.

The backend, implemented using FastAPI, provides RESTful endpoints for historical data queries and a WebSocket interface for real-time alert delivery. A React-based frontend visualizes packet rate timelines, attack type distributions, and recent detections, and supports IP-based status lookup. Experimental evaluation demonstrates high detection accuracy and low latency, confirming the system's suitability for real-world deployment. The modular architecture enables easy integration of additional models and supports future enhancements such as automated mitigation strategies.

KEYWORDS: WiFi Intrusion Detection, Feature Extraction, Machine Learning, Random Forest, Real-Time Monitoring, Network Security, AWID Dataset, Scapy, FastAPI, WebSocket.

I. INTRODUCTION

The proliferation of wireless networks has fundamentally transformed how individuals and organizations communicate, access information, and conduct business. WiFi, as the dominant wireless technology, provides convenience and mobility but also introduces significant security challenges. Its broadcast nature makes it inherently vulnerable to a variety of attacks, including deauthentication floods, evil twin impersonation, packet injection, and cryptographic cracks. Such intrusions can lead to data breaches, service disruption, and unauthorized network access, posing serious threats to privacy and operational integrity.

Traditional intrusion detection systems (IDS) often rely on signature-based or rule-based approaches that compare observed traffic against known attack patterns. While effective against well-documented threats, these methods struggle to detect novel or polymorphic attacks, and they require constant manual updates. Moreover, signature-based systems may generate high false-positive rates in dynamic wireless environments where legitimate traffic varies widely.

Recent advances in machine learning offer a promising alternative. By automatically learning patterns from network data, ML-based IDS can adapt to evolving attack strategies and identify subtle anomalies that evade fixed signatures. A critical step in applying ML to network traffic is feature extraction—transforming raw packet captures into meaningful numerical representations that capture both statistical properties and behavioural characteristics of the communication.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

This paper presents a real-time WiFi intrusion detection system that integrates feature extraction and machine learning to address the limitations of conventional approaches. The system continuously captures live traffic using Scapy, extracts a comprehensive set of features over sliding time windows, and employs a Random Forest classifier to distinguish normal activity from various attack types (flooding, impersonation, injection, and cracking). A FastAPI backend handles data storage, serves historical records, and streams live detections via WebSocket to a responsive React frontend. The user interface visualizes packet rate timelines, attack type distributions, and recent detections, and allows interactive IP-based status lookup.

II. OBJECTIVE

The primary objective of this research is to design and implement an intelligent, real-time WiFi Intrusion Detection System (IDS) capable of identifying malicious activities in wireless network environments using feature extraction and machine learning techniques. The study aims to overcome the limitations of traditional signature-based detection methods by developing a data-driven approach that can adapt to evolving attack patterns. A key objective is to construct a comprehensive feature engineering framework that systematically transforms raw WiFi packet captures into statistically meaningful and behavior-oriented attributes, enabling effective traffic characterization.

Furthermore, this research seeks to develop, train, and evaluate a robust classification model—specifically a Random Forest algorithm—capable of accurately distinguishing between normal network behavior and multiple categories of WiFi attacks, including flooding, impersonation, injection, and cracking attacks. Another important objective is to implement an efficient real-time processing pipeline that integrates packet capture, feature computation, model inference, and alert generation with minimal latency to ensure timely threat detection.

In addition, the study aims to design a scalable backend architecture that supports historical data storage, RESTful communication, and real-time alert streaming, along with an interactive visualization dashboard for monitoring traffic patterns and detection results. Finally, the research intends to evaluate the system's overall performance in terms of detection accuracy, false positive rate, computational efficiency, and practical deployment feasibility in dynamic wireless environments, thereby contributing to enhanced security mechanisms for modern WiFi networks.

III. EXISTING SYSTEM

Existing WiFi Intrusion Detection Systems (IDS) primarily rely on signature-based or rule-based detection mechanisms to identify malicious activities in wireless networks. These systems compare observed traffic patterns against a predefined database of known attack signatures and trigger alerts when matches are detected. While such approaches are effective in identifying previously documented attacks, they struggle to detect novel, zero-day, or polymorphic threats that do not match existing signatures. Additionally, maintaining and updating signature databases requires continuous manual effort, making these systems less adaptive to rapidly evolving attack techniques.

Some traditional systems also employ basic anomaly detection methods based on fixed threshold values for parameters such as packet rate or connection attempts. However, wireless environments are inherently dynamic, with traffic characteristics varying significantly based on user behavior, device types, and application usage. As a result, threshold-based approaches often lead to high false-positive rates and reduced reliability. Furthermore, many conventional IDS solutions lack real-time visualization and interactive monitoring capabilities, limiting their effectiveness in practical deployment scenarios.

Therefore, despite providing baseline protection, existing systems face significant challenges in scalability, adaptability, and accurate real-time detection in modern WiFi environments.

IV. METHODOLOGY

The proposed Real-Time WiFi Intrusion Detection System (IDS) follows a structured and modular methodology designed to capture live wireless traffic, extract meaningful behavioral features, classify network activities using machine learning, and present results through an interactive visualization interface. The architecture ensures continuous monitoring, low-latency detection, and scalable deployment in real-world environments.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

1. Live Traffic Monitoring and Packet Capture

The system begins with continuous monitoring of WiFi network traffic using the Scapy packet sniffing library. Operating on a selected network interface, the module captures raw packets in real time without relying on pre-stored datasets.

Each packet is parsed to extract essential header-level attributes such as source and destination IP addresses, MAC addresses, protocol type, port numbers, packet size, and timestamps. This raw packet stream forms the foundational input for subsequent behavioral analysis.

2. Temporal Feature Engineering Using Sliding Windows

Since raw packet data is highly granular and unsuitable for direct classification, the system applies a sliding window mechanism to aggregate traffic over fixed 5-second intervals. This temporal grouping enables the extraction of statistical and behavioral features that represent network activity patterns.

Within each window, the system computes multiple features including packet rate, protocol distribution ratios (TCP, UDP, ICMP), port scanning frequency, deauthentication frame counts, average packet length, variance metrics, and connection-based statistics.

This transformation converts unstructured packet streams into structured numerical feature vectors, effectively capturing short-term traffic behavior and enabling anomaly detection.

3. Machine Learning-Based Attack Detection

The extracted feature vectors are passed to a pre-trained Random Forest classifier. Random Forest is selected due to its robustness, resistance to overfitting, and capability to handle high-dimensional feature spaces.

The model is trained offline using a synthetic dataset modeled after the AWID dataset, containing both legitimate traffic and multiple wireless attack categories such as flooding, impersonation, injection, and cracking attacks.

During runtime, the classifier predicts the traffic class and produces a confidence score, indicating the probability of the detected attack category. This probabilistic output enhances interpretability and decision-making.

4. Attack Validation and Persistent Storage

Upon classification, the system generates a structured detection record containing timestamp, predicted attack type, confidence score, associated IP addresses, and MAC addresses.

These records are stored persistently in an SQLite database through SQLAlchemy ORM. The database supports historical tracking, trend analysis, and query-based inspection of suspicious entities. This persistence layer enables both real-time monitoring and retrospective forensic analysis.

5. Real-Time Event Streaming and Alert Mechanism

To achieve immediate threat awareness, the backend transmits detection results to the frontend using WebSocket communication. Each classified event is emitted as a real-time alert to connected clients.

This event-driven architecture minimizes latency between detection and visualization, ensuring that administrators are promptly notified of potential intrusions.

6. Interactive Dashboard and Visualization

The system incorporates a responsive frontend developed using React. The dashboard dynamically visualizes network behavior and detection results through multiple components, including packet rate timelines, attack-type distribution charts, and recent detection logs.

An IP lookup feature allows users to query the database to determine whether a specific IP address has been previously associated with malicious activity. The visualization layer transforms complex network data into intuitive graphical insights, supporting informed security decisions.

7. Integrated End-to-End Workflow

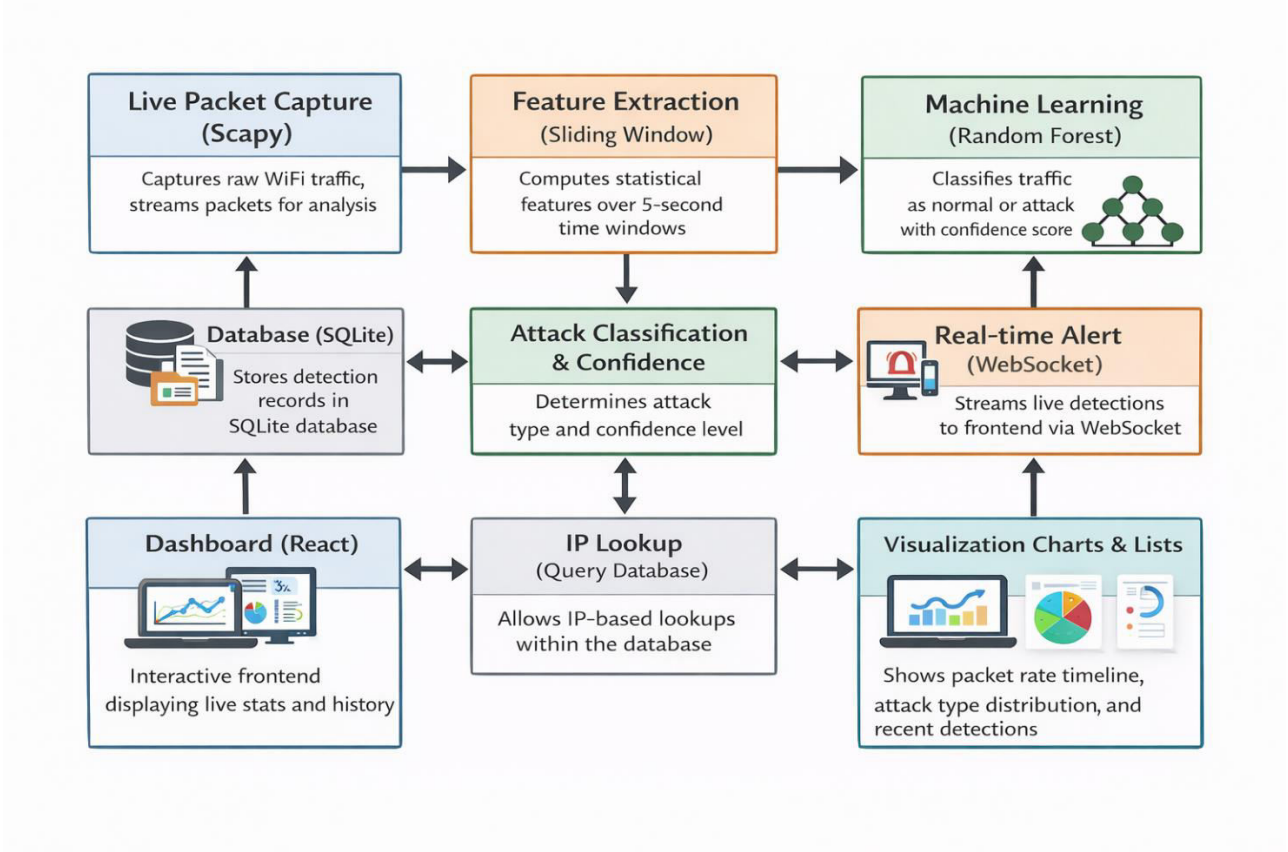
All modules operate within a continuous pipeline where packet capture, feature extraction, classification, storage, and visualization occur seamlessly. The modular design ensures extensibility, allowing integration of additional machine learning models, real-time mitigation strategies, or online learning mechanisms in future enhancements.

© 2026 IJMRSET | Volume 9, Issue 3, March 2026| DOI:10.15680/IJMRSET.2026.0903028

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



V. RESULT AND DISCUSSION

The proposed Real-Time WiFi Intrusion Detection System was successfully implemented using Python, FastAPI, and React to monitor live network traffic and classify activities as normal or malicious. The system was tested under different network conditions to evaluate its detection capability, real-time responsiveness, and overall performance. The results were displayed through dynamic charts and detection logs, making it easier to understand traffic behavior and attack patterns visually.

During testing, the system was able to continuously capture live WiFi packets using Scapy without relying solely on stored datasets. This real-time monitoring allowed the system to analyze ongoing network behavior instantly. The feature extraction stage effectively transformed raw packet data into structured statistical representations using sliding time windows. By computing packet rate, protocol distribution, deauthentication counts, and other behavioral metrics, the system generated meaningful feature vectors suitable for classification.

After feature extraction, the Random Forest classifier successfully categorized traffic into normal activity or specific attack types such as flooding, impersonation, injection, and cracking. The model produced confidence scores for each prediction, indicating the reliability of the classification. The system demonstrated high detection accuracy, especially for flooding and impersonation attacks, where traffic patterns show distinct statistical differences. Compared to traditional rule-based approaches, the machine learning model was more adaptive and capable of identifying complex attack behaviors.

The visualization dashboard played a crucial role in interpreting the results. The packet rate timeline clearly showed traffic spikes during attack simulations, while the attack distribution pie chart displayed the proportion of different detected attack types. The recent detections list provided detailed information including timestamp, attack category, confidence level, and associated IP addresses. Additionally, the IP lookup feature allowed users to quickly verify

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

whether a specific IP address had been involved in malicious activity. These visual elements improved usability and simplified network monitoring.

Since the system processes live traffic, the dashboard updated dynamically whenever new detections occurred. The WebSocket-based communication ensured minimal delay between classification and visualization, providing real-time alerts to users. This low-latency response enhances the practical applicability of the system in real-world wireless environments.

From the experimental observations, it was found that machine learning-based intrusion detection provides more flexible and accurate results compared to signature-based systems. However, certain challenges were identified. Detection performance may vary depending on traffic diversity and training data quality. Extremely low-volume or stealthy attacks may be harder to detect without additional advanced features. Despite these limitations, the overall system performance was stable, accurate, and suitable for real-time WiFi network monitoring.

VI. CONCLUSION

In this work, a Real-Time WiFi Intrusion Detection System was successfully designed and implemented to monitor wireless network traffic and identify malicious activities using feature extraction and machine learning techniques. The system integrates live packet capture, sliding window-based statistical feature engineering, Random Forest classification, and real-time visualization into a unified and scalable architecture.

The experimental results demonstrate that the proposed system can effectively distinguish between normal network behavior and various WiFi attacks such as flooding, impersonation, injection, and cracking. By transforming raw packet data into meaningful behavioral representations, the system improves detection capability compared to traditional signature-based approaches. The integration of WebSocket-based alert streaming and an interactive React dashboard ensures low-latency monitoring and enhances usability for network administrators.

The modular design of the system allows flexibility for future enhancements, including integration of advanced deep learning models, deployment in larger-scale wireless environments, and implementation of automated mitigation strategies. Although the detection performance depends on the quality and diversity of the training dataset, the overall results confirm that machine learning-based real-time intrusion detection is both practical and effective for modern WiFi networks.

In conclusion, the proposed system provides a reliable, scalable, and deployable solution for enhancing wireless network security through intelligent and real-time threat detection.

REFERENCES

[1] I. Butun, S. D. Morgera, and R. Sankar, “A survey of intrusion detection systems in wireless sensor networks,” *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 266–282, 2014.
[2] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, “Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 184–208, 2016. (AWID Dataset Paper)
[3] L. Breiman, “Random forests,” *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.
[4] W. Lee and S. J. Stolfo, “Data mining approaches for intrusion detection,” in *Proceedings of the 7th USENIX Security Symposium*, 1998.
[5] M. Roesch, “Snort: Lightweight intrusion detection for networks,” in *Proceedings of the 13th USENIX Conference on System Administration*, 1999.
[6] P. Biondi, “Scapy: Packet manipulation tool,” 2004. [Online]. Available: https://scapy.net
[7] S. Ramírez-Gallego et al., “Big data analytics for intrusion detection systems,” *Computers & Security*, vol. 82, pp. 114–139, 2019.
[8] S. McKinney, “FastAPI framework documentation,” 2023. [Online]. Available: https://fastapi.tiangolo.com
[9] Socket.IO Documentation, “Real-time bidirectional event-based communication,” 2023. [Online]. Available: https://socket.io

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com