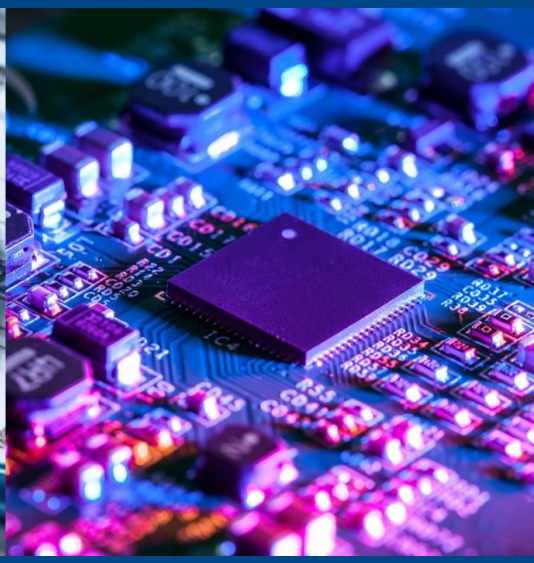
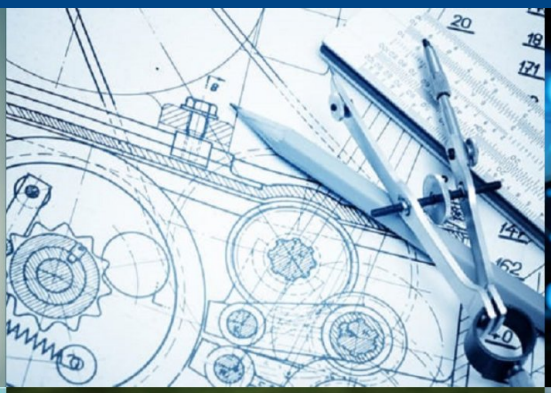
ISSN: 2582-7219

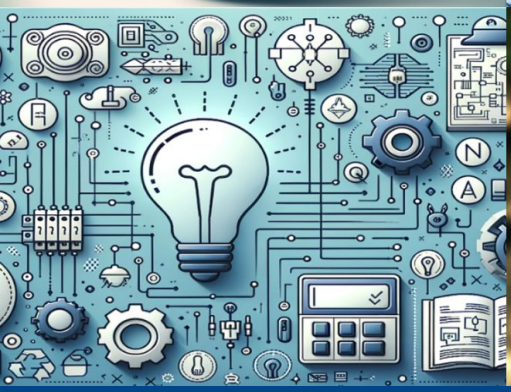




International Journal of Multidisciplinary Research in Science, Engineering and Technology

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



Impact Factor: 8.206 **Volume 9, Issue 4, April 2026**

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904382

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)

Smart AI Interview Trainer Using NLP and Speech Recognition

M. Syed Sirasudeen[1], .M.Mohammed Jallaludin[2]

Department of Computer Application, B.S. Abdur Rahman Crescent Institute of Science and Technology Vandalur, Tamil Nadu, India[1]

Assistant Professor, Department of Computer Application, B.S. Abdur Rahman Crescent Institute of Science and Technology, Vandalur, Tamil Nadu, India[2]

ABSTRACT: The widespread deployment of public Wi-Fi networks in airports, railway stations, educational institutions, shopping malls, and smart city infrastructures has significantly increased cybersecurity challenges. Open wireless networks are highly vulnerable to Denial-of-Service (DoS) attacks, packet flooding, spoofing, unauthorized access, and zero-day exploits. Traditional Intrusion Detection Systems (IDS) rely on signature- based detection methods, which are ineffective against unknown and evolving attack patterns. This paper presents the design and implementation of a Public Wi-Fi Intrusion Detection and Prevention System (IDS/IPS) using the Isolation Forest algorithm for anomaly detection.The proposed system integrates real-time packet capture, statistical traffic feature extraction, unsupervised anomaly scoring, and automated firewall- based IP blocking within a modular layered architecture. The Isolation Forest model identifies abnormal traffic behavior without requiring labeled attack datasets. Experimental evaluation demonstrates effective anomaly detection, low response latency, and reduced computational overhead under real-world traffic conditions. The system provides an intelligent and scalable security solution suitable for public hotspot deployment.

KEYWORDS: Intrusion Detection System, Isolation Forest, Public Wi-Fi Security, Anomaly Detection, Machine Learning, Cybersecurity.

I. INTRODUCTION

The rapid growth of public Wi-Fi services has enhanced digital accessibility in modern society.Transportation hubs, universities, commercial centers, and hospitality environments provide open wireless access to millions of users daily. However, the openaccess nature of public hotspots introduces significant security risks.Public Wi-Fi networks are susceptible to cyber threats such as DoS attacks, packet flooding, port scanning, session hijacking, spoofing, and zero-day exploits. Attackers can exploit weak monitoring systems to disrupt services or steal sensitive information.Traditional IDS solutions depend on signature-based detection, which compares network traffic against predefined attack patterns.

Although effective for known threats, such systems fail to detect new or modified attack behaviors.Machine Learning-based anomaly detection provides an adaptive alternative by analyzing traffic behavior rather than fixed signatures. This research proposes a lightweight and real-time IDS/IPS framework using the Isolation Forest algorithm to detect anomalous traffic patterns and automatically block malicious IP addresses in public Wi-Fi environments.

II. LITERATURE SURVEY

Intrusion Detection Systems (IDS) have evolved from signature-based packet filtering to advanced machine learning–based approaches. Early systems relied onstatic rule databases, which required frequent updates and were ineffective against zero-day attacks.

Statistical anomaly detection methods were later introduced to detect deviations from normal traffic patterns, but fixed threshold techniques often resulted in high falsepositive rates. Supervised machine learning models such as Support Vector Machines, Random Forests, and Neural Networks improved detection accuracy; however, they depend on

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)

labeled datasets and require periodic retraining to adapt to new threats.Unsupervised techniques address these limitations by removing the need for labeled attack data. The Isolation Forest algorithm is particularly efficient, as it isolates anomalies through random feature space partitioning, where rare and distinct instances are separated with fewer splits. Although several studies have applied Isolation Forest to benchmark datasets like UNSW-NB15 with promising results, many focus only on detection. The proposed system enhances existing approaches by integrating real-time anomaly detection with automated firewallbased IP blocking in a unified framework.

Problem Statement

Public Wi-Fi environments are increasingly vulnerable to a wide range of cyber threats due to inherent security limitations. Many existing deployments lack intelligent realtime monitoring capabilities, reducing their effectiveness in promptly identifying malicious activities. Conventional security mechanisms predominantly depend on signature-based or rule-driven detection, which makes them inadequate for recognizing unknown or zero- day attacks. In addition, these systems often require manual intervention after an anomaly is detected, resulting in delayed response and prolonged exposure to threats. The absence of automated IP blocking mechanisms further compromises network protection by allowing suspicious entities to continue interacting with the system. Moreover, static detection frameworks tend to generate high falsepositive rates, increasing operational logging for effective real-time security management.

overhead and reducing overall efficiency. These challenges emphasize the urgent need for a unified IDS/IPS solution that enables centralized, automated, and intelligent traffic analysis while ensuring low computational complexity and enhanced detection performance in public Wi-Fi networks.

III. PROPOSED SYSTEM

The proposed Public Wi-Fi Intrusion Detection and Prevention System (IDS/IPS) is designed using a modular layered architecture consisting of five primary components: Packet Capture Layer, Feature Extraction Layer, Machine Learning Detection Layer, Prevention Layer, and Logging and Monitoring Layer. The Packet Capture Layer continuously monitors and collects real-time network traffic from the public Wi-Fi environment without interrupting normal communication. The captured data is then processed in the Feature Extraction Layer, where lightweight statistical features such as packet count, flow duration, byte rate, and protocol information are computed to represent network behavior efficiently.

These features are forwarded to the Machine Learning Detection Layer, which utilizes the Isolation Forest algorithm to generate anomaly scores and identify suspicious or malicious traffic patterns, including zero-day and previously unseen attacks. Upon detection of abnormal activity, the Prevention Layer automatically initiates a firewall-based IP blocking mechanism to mitigate threats without requiring manual intervention. Finally, the Logging and Monitoring Layer records detection events, blocked IP addresses, timestamps, and system performance metrics, enabling continuous monitoring and administrative analysis. Overall, the system workflow ensures continuous packet capture, statistical feature computation, anomalyscoring, automated IP blocking upon detection, and comprehensive

IV. METHODOLOGY

The system follows a structured machine learning-based detection pipeline. **1. Data Collection**

The UNSW-NB15 dataset is used for model training. During deployment, real-time packets are captured from the Wi-Fi interface.

2. Preprocessing

Selected features include packet rate, byte rate, protocol, and flow duration. Data cleaning involves removing invalid entries and encoding protocol values.

3. Feature Extraction

Traffic behavior metrics are calculated as: Packet Rate = Total Packets / Duration Byte Rate = Total Bytes / Duration These statistical features represent network activity patterns.

4. Isolation Forest Detection

Isolation Forest constructs multiple random trees to isolate anomalies. Anomaly score is computed as:

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904382

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)

$s(x,n) = 2^{(-E(h(x))/c(n))}$

Where E(h(x)) is average path length and c(n) is normalization factor.
Prediction Output:
+1→NormalTraffic
−1 → Anomalous Traffic

5. Prevention Mechanism

If traffic is classified as anomalous, the system generates a firewall rule to block the suspicious IP and records the event in alert logs.

V. SYSTEM ARCHITECTURE

The system is designed using a layered architecture to ensure modularity, security, and scalability. Each layer performs a specific role in monitoring network traffic, detecting anomalies, and preventing malicious activities in real time.

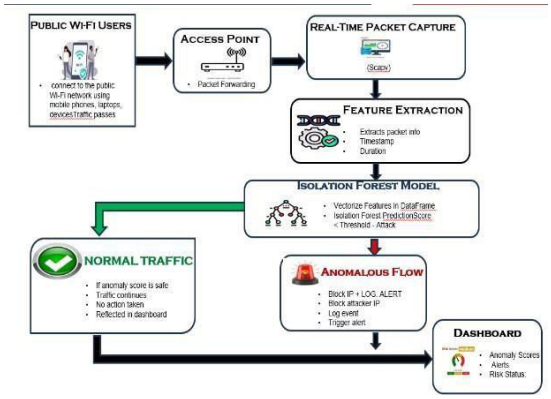


Fig 1 . Architecture Diagram

1. Capture Layer : The Capture Layer collects live network traffic from the public Wi-Fi interface using a packet sniffing mechanism. It records essential metadata such as packet size, protocol type, and timestamp while avoiding full payload storage to reduce overhead. Captured packets are temporarily buffered within a time window for further analysis, ensuring continuous real-time monitoring without affecting normal network performance.

2. Feature Processing Layer : The Feature Processing Layer converts raw packet data into structured statistical features for machine learning. It computes metrics such as packet rate, byte rate, protocol number, and flow duration. These behavioral features represent traffic intensity and communication patterns, and the processed dataset is forwarded to the detection module.

3. Detection Layer(Machine Learning Layer) The Detection Layer applies the Isolation Forest algorithm to evaluate traffic behavior and generate anomaly scores. As an unsupervised model, it detects deviations without requiring labeled data. If traffic is classified as anomalous and crosses the defined threshold, it is flagged for further action, enabling real-time detection of unknown and zero-day attacks.

4. Prevention Layer : The Prevention Layer automatically blocks malicious activity by generating firewall rules for suspicious IP addresses. This immediate response converts the system from passive detection (IDS) to active prevention (IPS), minimizing damage and reducing manual intervention.

5. Monitoring & Logging Layer : The
Monitoring Layer records detected anomalies and prevention actions with details such as timestamp, anomaly score, and blocked IP address. These logs support auditing, attack analysis, and system tuning, ensuring transparency and traceability of operations.

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904382

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)

VI. TECHNICAL STACK

The Public Wi-Fi Intrusion Detection and Prevention System is developed using the following technologies:

1. **Packet Capture :** The system uses the Scapy library for real-time network packet capture and traffic monitoring. Scapy enables sniffing of incoming and outgoing packets from the Wi-Fi interface and extraction of essential metadata such as packet size, protocol type, and timestamp for further analysis.

2. **Backend / Core Processing :** The backend is developed using Python, which manages packet processing, feature extraction, anomaly detection, and prevention logic. The threading module is used to enable parallel execution of packet capture and monitoring processes, ensuring real-time performance without blocking system operations.

3. **Machine Learning :** The Isolation Forest algorithm from Scikit-learn is used for anomaly detection. It identifies abnormal traffic patterns without requiring labeled attack datasets. Pandas is used for structured data handling, and NumPy is used for numerical computations and anomaly score evaluation

4. Dataset : . The UNSW-NB15 dataset is used for training the Isolation Forest model. Relevant traffic features such as packet rate, byte rate, protocol, and duration are selected and preprocessed before model training

5. Prevention Mechanism : The system integrates with Windows Firewall using netsh commands to automatically block suspicious IP addresses. This enables transformation from a passive Intrusion Detection System (IDS) to an active Intrusion Prevention System (IPS).

6. Logging & Monitoring : A log file mechanism is implemented to record detected anomalies, anomaly scores, timestamps, and blocked IP addresses. These logs support security auditing and performance evaluation.

VII. IMPLEMENTATION

The Public Wi-Fi Intrusion Detection and Prevention System is implemented using a modular architecture for real-time monitoring and automated mitigation.

Developed in Python, the system uses Scapy to capture live network packets and extract essential metadata such as packet size, protocol, and timestamp. Traffic data is buffered within a time window, and statistical features including packet rate, byte rate, protocol number, and flow duration are computed. These features are passed to the Isolation Forest model from Scikit-learn to evaluate anomaly scores. Parallel threads ensure simultaneous packet capture and detection without performance interruption. When anomalous behavior crosses the predefined threshold, a firewall rule is automatically generated to block the suspicious IP address. A logging module records anomaly scores, timestamps, and blocked IPs for auditing. All components work together to provide efficient, real-time intrusion detection and prevention in public Wi-Fi environments.

VIII. EXPERIMENTAL RESULTS

The proposed Public Wi-Fi Intrusion Detection and Prevention System was evaluated to assess its detection accuracy, response time, and resource efficiency under normal browsing, high packet-rate traffic, and simulated flooding conditions. The Isolation Forest model accurately classified legitimate traffic while successfully identifying abnormal patterns during DoSlike scenarios based on elevated packet and byte rates. Detected anomalies triggered automatic firewall-based IP blocking in real time. The system maintained low detection latency due to efficient feature extraction and lightweight computation, while CPU and memory usage remained stable during continuous monitoring. Overall, the system demonstrated reliable anomaly detection, rapid mitigation, and efficient resource utilization for securing public Wi-Fi environments.

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904382

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)

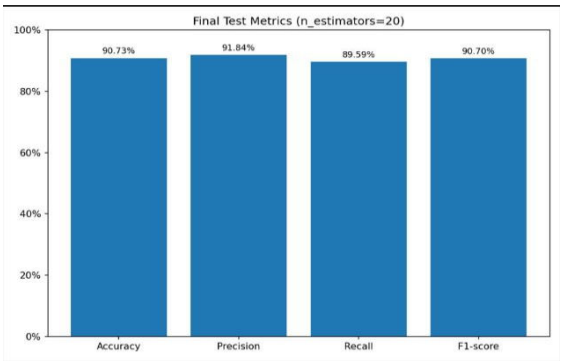


Fig.1.test metrics

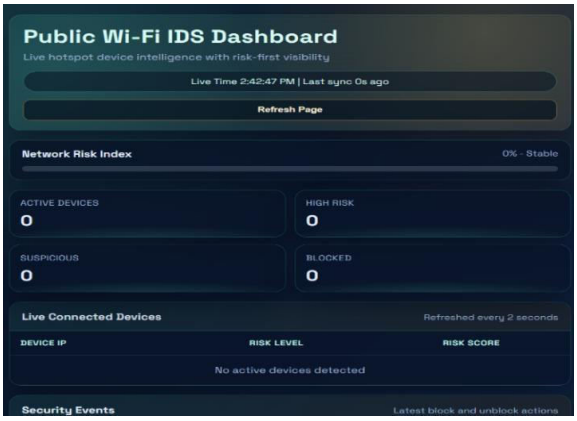


Fig.2. Home Page of intrusion system **Fig.3. Detection Page of intrusion**

IX. DISCUSSION

The proposed Public Wi-Fi Intrusion Detection and Prevention System effectively integrates real-time traffic monitoring, anomaly detection, and automated mitigation within a modular architecture. The use of the Isolation Forest algorithm enables detection of abnormal and zero-day traffic patterns without relying on signature databases or labeled datasets. Feature-based behavioral analysis reduces computational overhead while maintaining detection accuracy. Automated firewall integration transforms the system from passive detection to active prevention, ensuring immediate threat mitigation. Although performance may vary under high traffic conditions and requires proper threshold tuning, the system demonstrates reliable, scalable, and efficient protection for public Wi-Fi environments..

A. Advantages of the Proposed System

The proposed system offers several significant advantages for securing public Wi-Fi environments. By employing an unsupervised anomaly detection
approach, it is capable of identifying zeroday and previously unseen attacks without relying on predefined signatures. The framework supports real-time traffic monitoring combined with automated threat mitigation, enabling immediate response to suspicious activities. Its lightweight statistical feature-based analysis ensures minimal computational overhead, making it suitable for deployment on resource- constrained systems.

An automatic firewall-based IP blocking mechanism enhances proactive defense by preventing continued malicious access once a threat is detected. The system is designed with a modular and scalable layered architecture, allowing easy expansion and integration with additional security components.Moreover, it reduces reliance on manual security intervention, thereby improving operational efficiency. The solution is particularly well-suited for public hotspot environments, where dynamic and diverse user traffic is common. Efficient resource utilization ensures stable CPU and memory usage, maintaining consistent performance even during continuous monitoring operations.

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)

B. Limitations

Despite demonstrating promising performance in public Wi-Fi intrusion detection, the proposed system has certain limitations. The current model utilizes a limited set of traffic features for anomaly detection, which may restrict its ability to capture highly complex or evolving attack patterns. Furthermore, the system focuses solely on anomaly detection and does not provide detailed classification of specific attack categories. Detection accuracy is also influenced by the selection and configuration of threshold values; improper tuning may lead to reduced effectiveness or increased false alarms. The firewall-based response mechanism may differ across operating systems, potentially affecting consistency in deployment and enforcement. In addition, system performance could be impacted under extremely high network traffic conditions due to computational overhead. Finally, periodic evaluation and model tuning are required to maintain optimal performance and adapt to changing network behaviors and emerging cyber threats.

C. Future Enhancement

Several enhancements are envisioned to strengthen the scalability and effectiveness of the proposed system in dynamic public Wi- Fi environments. Future work includes the integration of deep learning–based anomaly detection models to improve detection accuracy and adaptability against sophisticated threats. A multi-class attack classification module will be incorporated to enable precise identification of different intrusion types rather than simple binary detection. Adaptive threshold tuning mechanisms are also planned to automatically adjust detection sensitivity based on changing traffic patterns.

To enhance usability and operational control, a web-based monitoring and visualization dashboard will be developed for real-time analysis and reporting. For large-scale deployments, cloud-based or distributed architectures will be explored to ensure seamless scalability and centralized management. Additionally, advanced traffic analytics and detailed reporting features will be implemented to support informed decisionmaking. Integration with centralized network security management platforms and optimization for high- throughput Wi-Fi infrastructures will further ensure robust performance in enterprise-level and large public network scenarios.

X. CONCLUSION

The proposed Public Wi-Fi Intrusion Detection and Prevention System provides an intelligent and efficient solution for securing open wireless networks against evolving cyber threats. By integrating real-time packet capture, statistical feature extraction, unsupervised anomaly detection using Isolation Forest, and automated firewallbased prevention, the system enables continuous monitoring and rapid mitigation of malicious activities. The behavioral feature-based approach improves detection capability compared to traditional signaturebased methods, particularly for zero-day and unknown attacks. The layered architecture ensures modularity, scalability, and efficient resource utilization, while automated IP blocking enhances overall network security. Overall, the system reduces manual intervention, improves response time, and offers a practical and scalable security framework suitable for modern public Wi-Fi environments.

XI. ACKNOWLEDGMENT

The author sincerely thanks the faculty members and project mentors for their valuable guidance, technical support, and continuous encouragement throughout the development of the Public Wi-Fi Intrusion Detection and Prevention System. Their insights and constructive feedback played a significant role in the successful completion of this work.

The author also acknowledges the support provided by the department and institution for offering thnecessaryinfrastructure andresources to implement, test, and evaluate the system.

REFERENCES

[1] A. L. Buczak and E. Guven, “Recent advances in machine learning-based intrusion detection systems: A review,” IEEE Access, vol. 10, pp. 119452–119470, 2022.M. Almutairi, S. Aldossary, and K. Alharbi, “Anomaly-based intrusion detection using Isolation Forest for network security,” Computers & Security, vol. 118, pp. 102750, 2022.
[2] Y. Zhang, X. Chen, and L. Wang, “Lightweight intrusion detection for IoT and wireless networks using ensemble anomaly detection,” IEEE Internet of Things Journal, vol. 10, no. 4, pp. 3156–3168, 2023.
[3] S. Kumar and P. Sharma, “Real-time network intrusion detection using unsupervised learning techniques,” IEEE

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)

Access, vol. 11, pp. 54872–54885,2023.

[4] H. Alqarni, M. Khan, and T. Ahmad, "Isolation Forest-based zero-day attack detection in wireless networks," Journal of Network and Computer Applications, vol. 220, pp. 103607, 2023.

[5] J. Li, R. Sun, and Y. Zhou, "Scalable anomaly detection framework for high- speed network environments," Future Generation Computer Systems, vol. 145,pp. 233–245, 2024.

[6] M. Rahman and S. Islam, "Adaptive threshold tuning for anomaly-based intrusion detection systems," IEEE Systems Journal, vol. 18, no. 2, pp. 1567–1578, 2024.

[7] K. Patel, D. Shah, and R. Mehta, "Public WiFi security enhancement using machine learning-driven intrusion prevention," IEEE Access, vol. 12, pp. 91234–91248, 2024.

[8] T. Nguyen and A. Kumar, "Deep anomaly detection models for next-generation network security," Computers & Security, vol. 132, pp. 103290, 2025.

[9] L. Hernandez, P. Silva, and J. Gomez, "Hybrid intrusion detection and prevention systems for smart city wireless infrastructures," IEEE Transactions on Network and ServiceManagement, vol. 22, no. 1, pp. 89–102,2025.

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