IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13324

WIFI SPOOF DETECTION SYSTEM USING IoT (ESP32)

Varun S[1], Dr. K. Thenmozhi[2]

Department of Information Technology, Dr. N.G.P. Arts and Science College, Coimbatore, Tamil Nadu, India[1]

Professor, Department of Information Technology, Dr. N.G.P. Arts and Science College, Coimbatore, Tamil Nadu, India[2]

Abstract: Wireless communication technologies have become an essential component of modern digital infrastructure, enabling seamless connectivity for individuals, organizations, and smart devices. WiFi networks are widely used in homes, campuses, enterprises, and public environments due to their convenience and accessibility. However, the rapid expansion of wireless networks has also introduced significant cybersecurity challenges. One of the most common threats is WiFi spoofing, where attackers create rogue access points that imitate legitimate networks in order to deceive users and intercept sensitive information.

WiFi spoofing attacks typically involve the duplication of network identifiers such as **SSID (Service Set Identifier)** and the manipulation of **BSSID (MAC addresses)**. These attacks allow malicious actors to perform activities such as **man-in-the-middle attacks, credential theft, data interception, and network monitoring**. Traditional wireless security mechanisms such as WPA2 or WPA3 encryption primarily focus on securing data transmission but often lack effective mechanisms for detecting spoofed access points operating within close proximity.

To address these challenges, this research proposes a **WiFi Spoof Detection System using IoT (ESP32)**. The proposed system uses ESP32 microcontrollers to continuously monitor nearby wireless networks and collect parameters including SSID, BSSID, RSSI (signal strength), and channel information. The system analyzes these parameters to identify suspicious patterns such as duplicate SSIDs with different MAC addresses or abnormal signal strength variations.

The system integrates **IoT hardware monitoring, backend data processing using Python Django, and a PostgreSQL database** for centralized storage and analysis. Additionally, a **React + Vite.js frontend dashboard** provides administrators with real-time monitoring capabilities, enabling visualization of network activities and detection alerts. Experimental implementation demonstrates that the proposed solution provides a **low-cost, scalable, and efficient method for detecting rogue access points and strengthening wireless security in smart environments**.

Keywords: WiFi Spoofing, ESP32, IoT Security, Rogue Access Point Detection, MAC Address Analysis, RSSI Monitoring, Wireless Intrusion Detection, Cybersecurity, Network Monitoring.

I. INTRODUCTION

Wireless networking technologies have become a fundamental component of modern communication systems. WiFi networks enable fast and convenient internet access for a wide range of devices including laptops, smartphones, IoT devices, and enterprise systems. The widespread adoption of wireless connectivity has significantly improved productivity, communication, and digital accessibility across various domains including education, healthcare, business, and government sectors.

Despite these advantages, wireless networks are inherently vulnerable to various security threats due to their open communication environment. One of the most critical threats is **WiFi spoofing**, also known as **rogue access point attacks**. In such attacks, malicious actors create fake wireless networks that imitate legitimate WiFi networks by copying their SSID names. Unsuspecting users may connect to these networks, believing them to be authentic, thereby allowing attackers to intercept data and perform unauthorized activities.

WiFi spoofing attacks can lead to serious consequences including **credential theft, financial fraud, data leakage, and network intrusion**. Attackers can also perform **man-in-the-middle (MITM) attacks**, where they intercept and manipulate communication between users and legitimate servers. Traditional network security mechanisms are often

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13324

insufficient to detect such attacks because they primarily focus on encryption rather than identifying malicious network impersonation.

To address these limitations, there is a need for intelligent and proactive monitoring systems capable of detecting spoofed access points in real time.

This research proposes a **WiFi Spoof Detection System using ESP32 microcontrollers** that continuously scans nearby networks and analyzes their characteristics to detect spoofing attempts. The system combines IoT hardware monitoring with backend processing and visualization tools, creating a comprehensive platform for wireless security monitoring. The proposed system aims to provide a **scalable, affordable, and efficient solution for detecting rogue access points in smart environments**.

II. LITERATURE SURVEY

2.1 WiFi Spoofing Attacks

WiFi spoofing attacks occur when attackers create unauthorized wireless access points that mimic legitimate network identifiers. These rogue access points deceive users into connecting to malicious networks, enabling attackers to intercept sensitive information such as login credentials and personal data. Attackers typically duplicate the SSID (Service Set Identifier) of legitimate networks and modify hardware identifiers such as MAC addresses to impersonate trusted networks. Once users connect to these fake networks, attackers can perform malicious activities including man-in-the-middle attacks, data interception, credential theft, and network monitoring. Previous research has highlighted the significant risks associated with spoofed networks, particularly in public WiFi environments where users may unknowingly connect to untrusted networks [1], [2].

2.2 Wireless Intrusion Detection Systems

Wireless Intrusion Detection Systems (WIDS) are designed to monitor wireless traffic and identify abnormal network behavior within wireless environments. These systems analyze packet transmissions, signal patterns, and network activities to detect suspicious events such as unauthorized access points, unusual traffic patterns, and security violations. WIDS solutions typically operate by continuously scanning wireless channels and comparing network behavior against predefined security policies. However, many existing WIDS solutions rely on specialized hardware devices and complex infrastructure deployments, which can make them expensive and difficult to implement in smaller organizations or educational environments. As a result, researchers have explored lightweight intrusion detection mechanisms that can be implemented using embedded systems and IoT devices [3], [4].

2.3 IoT-Based Security Monitoring

The emergence of the Internet of Things (IoT) has opened new opportunities for distributed security monitoring systems. IoT devices equipped with wireless communication capabilities can be deployed across environments to collect network data and monitor security threats. Microcontrollers such as ESP32 have integrated WiFi modules and sufficient processing power to perform wireless scanning, making them suitable for implementing low-cost intrusion detection solutions. Researchers have explored the use of IoT platforms for monitoring network activities, environmental conditions, and smart infrastructure systems. These devices provide real-time data collection and remote monitoring capabilities while maintaining low deployment costs and energy consumption [5], [6].

2.4 Research Gap

Although previous studies have investigated wireless intrusion detection mechanisms and IoT-based monitoring systems independently, there is limited research focusing on integrating IoT-based wireless scanning with backend analytics platforms for real-time WiFi spoof detection. Existing approaches either rely on traditional network monitoring tools or expensive enterprise security solutions. This research aims to address this gap by developing a system that integrates ESP32-based WiFi scanning, backend data analysis using Python Django, and centralized monitoring through a web dashboard supported by PostgreSQL databases. The proposed system provides a scalable, cost-effective, and real-time approach for detecting spoofed networks and improving wireless security monitoring in smart environments.

III. SYSTEM ARCHITECTURE

The proposed WiFi Spoof Detection System follows a **multi-layer architecture** consisting of hardware sensing components, backend processing modules, and a web-based monitoring interface.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13324

The architecture includes **three ESP32 nodes deployed within the network environment**. These nodes continuously scan nearby WiFi networks and collect parameters such as SSID, MAC address, RSSI signal strength, and channel information. The collected data is transmitted to a backend server for analysis.

The backend server is implemented using the **Django framework in Python**, which processes the incoming data and applies spoof detection algorithms. The server communicates with a **PostgreSQL database** that stores network logs, suspicious activity records, and system monitoring information.

The processed data is presented through a **React + Vite.js frontend dashboard**, which allows administrators to monitor network activities in real time and receive alerts when spoofing attempts are detected.

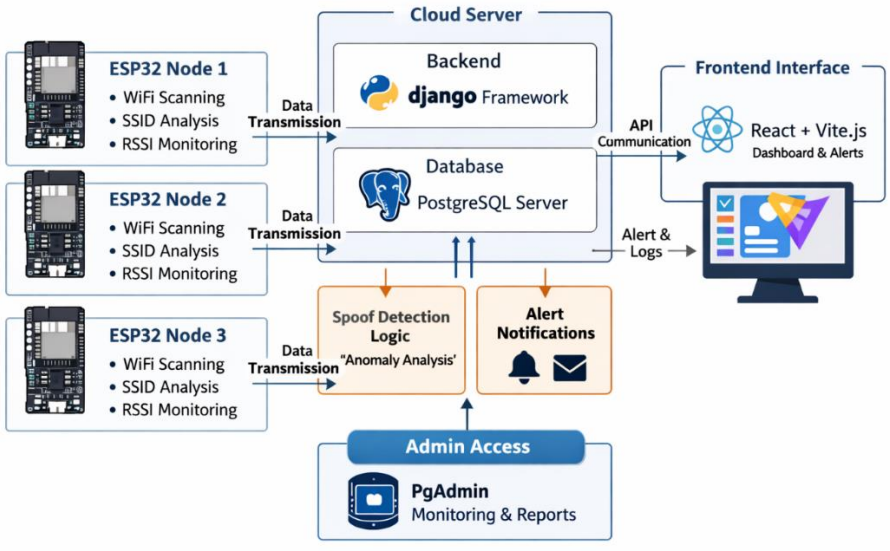

Fig 3.1 System Architecture

3.2 Modules of the Proposed System

Module	Technologies Used	Description
WiFi Scanning Module	ESP32 WiFi Library	Scans nearby networks and collects SSID, BSSID, RSSI
Spoof Detection Module	Embedded C Logic	Detects duplicate SSID with different MAC
RSSI Analysis Module	Signal Threshold Logic	Detects abnormal signal strength variations
Alert Module	Buzzer + LED	Provides real-time warning
Cloud Dashboard Module	HTTP / Firebase	Displays live monitoring data
Database Module	Cloud DB	Stores suspicious logs

Table 3.2.1 Module

3.3 Key Features

Feature	Technology Used	Description
SSID Duplication Detection	MAC Comparison Logic	Detects same SSID with different BSSID
RSSI Anomaly Detection	Threshold Algorithm	Identifies signal manipulation
Real-Time Alert	GPIO Buzzer + LED	Immediate warning
Continuous Monitoring	ESP32 WiFi Scan	Periodic scanning
Log Storage	Cloud Database	Stores attack history
Low Cost Implementation	ESP32 Module	Affordable deployment

Table 3.3.1 Key Features

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13324

3.4 Workflow

The workflow of the **WiFi Spoof Detection System using ESP32** illustrates the sequence of operations involved in detecting suspicious wireless networks and preventing spoofing attacks. The system continuously monitors nearby wireless signals, analyzes network parameters, and generates alerts when abnormal or duplicate networks are detected. The workflow ensures that the monitoring process is automated and capable of operating in real time without requiring continuous manual supervision.

Initially, the ESP32 device is powered on and initializes its internal WiFi module in station mode. Once initialized, the system begins scanning all nearby wireless networks within its coverage range. During the scanning process, the ESP32 collects important parameters including **SSID (Service Set Identifier), BSSID (MAC address), RSSI (signal strength), and channel information**. These parameters are essential for identifying potential spoofing activities.

After the scanning phase, the collected data is processed by the spoof detection logic embedded in the firmware. The system compares network identifiers and detects duplicate SSIDs associated with different MAC addresses. If such a condition is identified, it may indicate the presence of a rogue access point attempting to impersonate a legitimate network.

In addition to SSID comparison, the system also performs **RSSI signal strength analysis**. If the signal strength deviates significantly from expected values or fluctuates abnormally, the system considers the possibility of a spoofing attack or unauthorized access point.

When suspicious behavior is detected, the system triggers an alert using hardware indicators such as a **buzzer and LED notification system**. The detected information is then logged and optionally transmitted to a backend server or cloud database for monitoring and analysis. This structured workflow ensures continuous surveillance of wireless environments and rapid detection of spoofing threats

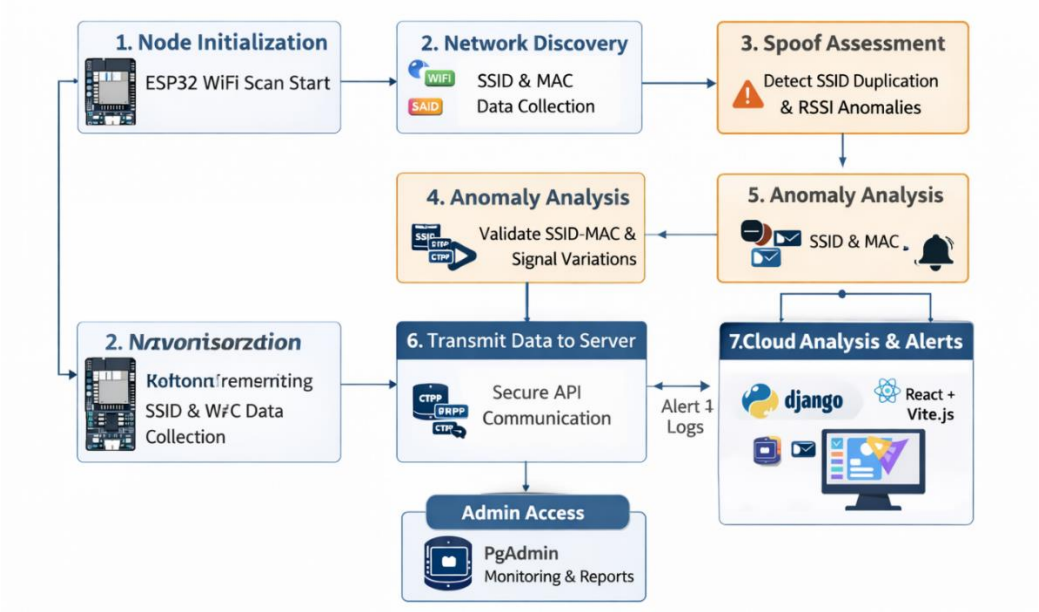

Fig 3.4.1 Workflow

Process Stage	Description
Device Initialization	ESP32 boot & WiFi scan start
Network Scanning	Collect SSID, MAC, RSSI
SSID Comparison	Identify duplicates
MAC Verification	Detect spoofed BSSID
RSSI Analysis	Validate signal anomaly
Alert Trigger	Activate buzzer & LED
Log Storage	Save suspicious entry

Table 3.4.2 Workflow Stages

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13324

IV. DATA FLOW DIAGRAM

The Data Flow Diagram (DFD) represents how information flows through the proposed **WiFi Spoof Detection System using ESP32**. It describes how wireless network data is collected, processed, stored, and monitored within the system. The diagram provides a clear visualization of the interactions between hardware components, detection algorithms, and monitoring interfaces.

The data flow begins with the **ESP32 device scanning nearby wireless networks**. During each scanning cycle, the system gathers network identifiers such as SSID, MAC address, RSSI signal strength, and channel number. This information is temporarily stored within the microcontroller memory for further analysis.

Once the scanning data is collected, it is processed by the spoof detection logic embedded in the system firmware. The detection module compares network parameters and checks for suspicious patterns such as duplicate SSIDs with different MAC addresses or abnormal signal behavior. These conditions may indicate the presence of a rogue access point attempting to impersonate a legitimate wireless network.

If suspicious activity is detected, the system generates alerts and logs the event for monitoring purposes. The detected data can be stored locally or transmitted to a **cloud database or backend monitoring system** using secure communication protocols. This allows administrators to track network activity and analyze security threats over time.
The data flow architecture ensures that wireless network monitoring is performed continuously while maintaining efficient processing and storage of detected anomalies.

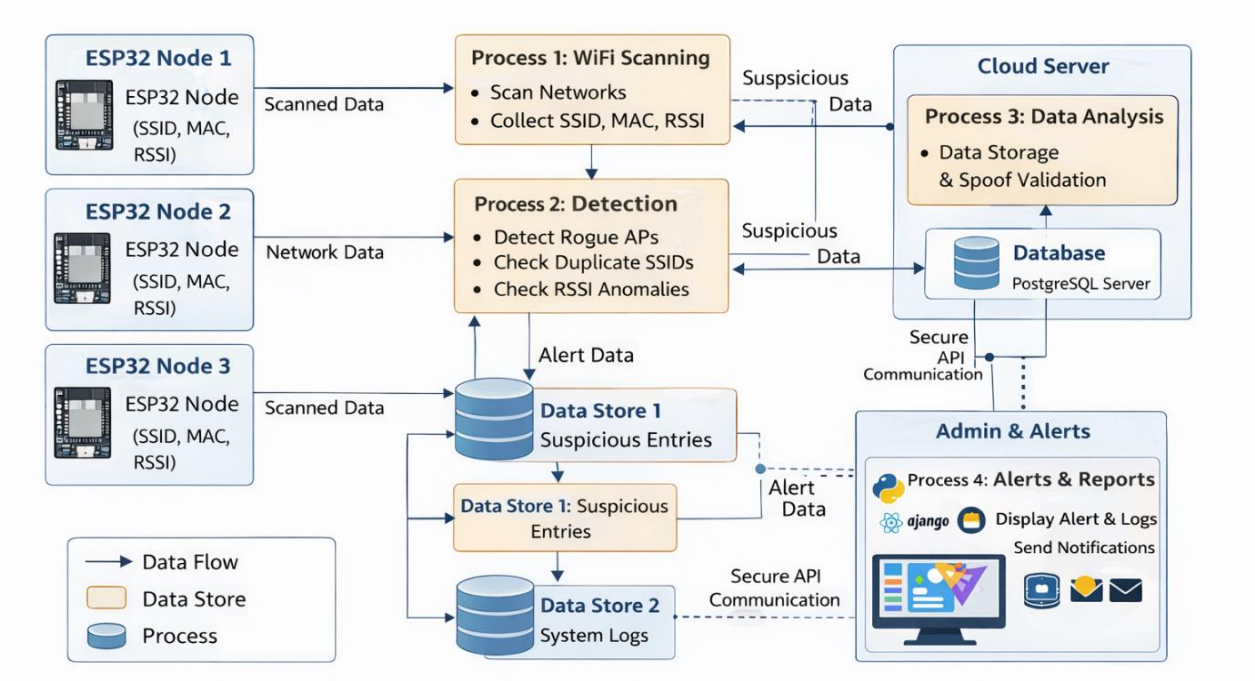

Fig 4.1 Data Flow Diagram

V. METHODOLOGY

The methodology of the proposed system defines the systematic approach used to detect WiFi spoofing attacks. The detection process involves multiple stages including network monitoring, parameter analysis, anomaly detection, and alert generation. Each stage contributes to identifying suspicious wireless networks and preventing unauthorized access.

Step 1: System Initialization
At the initial stage, the ESP32 microcontroller initializes its internal WiFi module and configures it in station scanning mode. This allows the device to monitor surrounding wireless networks without connecting to them. Once initialized, the scanning process begins automatically.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13324

Step 2: Network Data Collection
During the scanning process, the ESP32 collects important network parameters including SSID, BSSID (MAC address), RSSI signal strength, and channel information. These parameters provide valuable information about nearby wireless networks and are essential for identifying anomalies.

Step 3: Duplicate SSID Detection
The collected network information is analyzed to detect duplicate SSIDs. If multiple networks share the same SSID but have different MAC addresses, the system identifies this as a potential spoofing attempt. Rogue access points often mimic legitimate network names to deceive users.

Step 4: RSSI Threshold Analysis
The system also analyzes signal strength values to detect irregularities. Significant deviations in RSSI values may indicate that an attacker is attempting to impersonate a legitimate network from a different physical location.

Step 5: Alert and Logging Mechanism
If suspicious network behavior is detected, the system activates hardware alerts such as a buzzer and LED indicators. The detected information is recorded and optionally transmitted to a backend monitoring platform for further analysis.

Module	Technology	Function
WiFi Scan Module	ESP32 WiFi API	Network scanning
Detection Module	C Logic	Spoof identification
Alert Module	GPIO Control	Warning activation
Logging Module	HTTP API	Cloud data storage

VI. IMPLEMENTATION

The proposed WiFi Spoof Detection System is implemented using the **ESP32 microcontroller platform**, which provides integrated WiFi capabilities and sufficient processing power for real-time network monitoring. The firmware is developed using **Embedded C programming in the Arduino IDE environment**.

The ESP32 device continuously scans surrounding wireless networks and extracts network parameters required for spoof detection. The detection algorithms analyze SSID and MAC address combinations to identify suspicious patterns associated with rogue access points.

Hardware components such as **buzzer modules and LED indicators** are connected to the GPIO pins of the ESP32 to provide immediate alerts when spoofing activity is detected. This allows the system to notify users even without internet connectivity.

For advanced monitoring, the system can transmit collected data to a **cloud-based backend server using REST APIs or Firebase services**. This enables administrators to view network monitoring results through dashboards and generate reports for security analysis.

Module	Technology Used	Purpose
Hardware	ESP32	WiFi scanning
Firmware	Embedded C	Detection logic
Alert System	Buzzer + LED	Local warning
Cloud Backend	Firebase / REST API	Remote monitoring

VII. BENEFITS AND CHALLENGES

7.1 Benefits
The proposed system offers several advantages in improving wireless network security and monitoring capabilities. By using IoT technology and low-cost hardware components, the system provides an accessible solution for detecting spoofed networks in various environments such as campuses, offices, and public WiFi zones.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13324

Benefit	Description
Enhanced Network Security	Detects rogue access points
Low Cost	Uses affordable ESP32
Real-Time Monitoring	Instant alerts
Lightweight System	No heavy infrastructure
Scalable Deployment	Suitable for institutions

7.2 Challenges

Despite its advantages, the proposed system also faces certain limitations related to signal variability and network complexity. These challenges must be considered when deploying the system in large-scale environments.

Challenge	Description
False Positives	Legitimate repeaters may trigger detection
Network Density	High-density areas increase complexity
MAC Randomization	Some devices randomize MAC addresses
RSSI Variability	Signal fluctuations may affect accuracy

VIII. DISCUSSION AND FUTURE WORK

Discussion:

The WiFi Spoof Detection System using ESP32 demonstrates an efficient and practical approach for identifying rogue access points within wireless environments. By continuously scanning nearby networks and analyzing their characteristics, the system can detect spoofing attempts in real time. The use of IoT hardware significantly reduces deployment costs compared to traditional wireless intrusion detection systems.

The proposed system is particularly suitable for environments such as **educational campuses, corporate offices, and public WiFi zones**, where unauthorized access points can pose serious security risks. The integration of alert mechanisms and logging features allows administrators to monitor network activity and respond quickly to potential threats.

Future Work:

Future improvements can further enhance the capabilities of the system by incorporating advanced technologies such as machine learning and automated response mechanisms. Possible enhancements include:

- AI-based anomaly detection models
- Packet-level deep inspection
- Integration with centralized security dashboards
- Mobile application alerts
- Automated deauthentication countermeasures
- BLE and WiFi triangulation-based attack localization

These improvements would increase detection accuracy and enable the system to respond automatically to detected threats.

IX. CONCLUSION

The WiFi Spoof Detection System using IoT (ESP32) provides a **cost-effective and scalable solution for identifying rogue wireless networks and preventing spoofing attacks**. By combining continuous network monitoring, parameter analysis, and real-time alert mechanisms, the system enhances wireless security in modern digital environments.

The integration of IoT devices with monitoring platforms allows organizations to deploy distributed security monitoring systems without requiring expensive infrastructure. The proposed system demonstrates strong potential for implementation in smart campuses, enterprises, and public networks where wireless security is a critical concern.

DOI: 10.17148/IARJSET.2026.13324

REFERENCES

[1]. N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11," *Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2001.

[2]. A. Mishra, M. Shin, and W. Arbaugh, "An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process," *ACM SIGCOMM Computer Communication Review*, vol. 33, no. 2, pp. 93–102, 2003.

[3]. A. Mishra, W. Arbaugh, and M. Shin, "Detecting Rogue Access Points in IEEE 802.11 Networks," *IEEE INFOCOM*, 2004.

[4]. W. A. Arbaugh, N. Shankar, and Y. Wan, "Your 802.11 Wireless Network Has No Clothes," *IEEE Wireless Communications*, vol. 9, no. 6, pp. 44–51, 2002.

[5]. S. Jana and S. K. Kasera, "On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews," *IEEE Transactions on Mobile Computing*, vol. 9, no. 3, pp. 449–462, 2010.

[6]. IEEE Standards Association, "IEEE 802.11 Wireless LAN Standard," IEEE Communications Society, 2020.

[7]. Espressif Systems, "ESP32 Technical Reference Manual," Espressif Inc., 2023.

[8]. Espressif Systems, "ESP32 WiFi API Documentation," Espressif Inc., 2023.

[9]. L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[10]. R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed., Wiley, 2008.

