IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Automated Attendance System Using Wi-Fi Based Device Detection And File Encryption

[1]Mr. N. Nijanthan, [2]Kishore S, [3]Karthikeyan V, [4]Bharath M,

[1]Assistant Professor,[2]Student,[3]Student, [4]Student,

Dept. of Cyber Security Engineering,

Paavai Engineering College, Tamil Nadu, India

Abstract—Automated attendance systems have become crucial in schools and organizations. They replace manual roll call, reduce human errors, and improve productivity. This paper suggests a Wi-Fi-based automated attendance system that detects registered devices within a specific network range by scanning MAC addresses. The system verifies student presence by identifying authenticated devices connected or detectable through the Wi-Fi access point. To protect confidentiality and prevent unauthorized access, all attendance records are encrypted with AES-256 file-level encryption before local storage. The hardware uses a microcontroller/Wi-Fi development board to detect nearby devices. Meanwhile, a backend script automates data logging and secure file creation. The system was tested in a controlled setting and showed reliable detection within 8 to 12 meters, achieving an accuracy of 92% during peak device density. This proposed model is a cost-effective, secure, and scalable option compared to biometric or RFID systems, making it especially suitable for classrooms and small institutions.

Index Terms— Wi-Fi scanning, automated attendance, device detection, AES encryption, IoT, MAC authentication, secure logging.

I. INTRODUCTION

Attendance management is crucial in schools and businesses. Traditional manual attendance systems take time and effort, and they can lead to mistakes. Modern biometric systems, like fingerprint, RFID, and face recognition, offer automation but come with extra costs, privacy issues, hygiene concerns, and require ongoing maintenance. Wi-Fi based attendance systems have appeared as a promising solution because nearly everyone has smartphones. Each device has a unique Media Access Control (MAC) address that can be detected when connected to, or probing, the Wi-Fi access point. This project aims to use this capability to automate attendance marking securely. To protect sensitive records, file encryption is integrated using AES-256, which is one of the most secure and widely used encryption algorithms. The proposed system not only automates attendance but also keeps data safe and prevents unauthorized changes.

1.1 Background of the Study

Attendance tracking is one of the core needs of academic institutions as well as corporate environments. Traditional methods involve manual roll calls, signature sheets, and card systems, which are time-consuming, easily manipulated, and usually result in inaccurate record-keeping. Growing dependence on digital devices and connectivity inspired exploration of automated and contactless attendance systems. Access to inexpensive microcontrollers, smartphones, and Wi-Fi infrastructure has considerably improved over the years, making Wi-Fi-based device detection a feasible alternative to traditional biometric and RFID-based methods. Every smartphone carries a unique MAC address that can be detected when the device interacts with, or probes, a Wi-Fi access point. Thus, leveraging this property will make attendance marking passive, automatic, and non-intrusive.

The problem arises when important and sensitive attendance logs are retained on local systems. Unauthorized access or modifications may be performed, potentially resulting in data leakage, hence compromising the integrity of the institutional records. Thus, integrating a robust file-level encryption mechanism such as AES-256 will be imperative to guarantee confidentiality against tampering. The research focuses on the development of a secure, automated, low-cost attendance system by using Wi-Fi-based device detection along with strong encryption to address issues related to accuracy, transparency, and data protection.

1.2 Problem Statement

Despite the presence of modern attendance solutions such as biometric scanners, RFID cards, and facial recognition systems, institutions still face challenges related to cost, maintenance, hygiene, privacy, and system reliability. Manual attendance remains time-consuming and error-prone, while biometric systems introduce health concerns and require expensive hardware. Additionally, many existing automated systems lack adequate data security, leaving attendance records vulnerable to unauthorized access or manipulation. There is a need for a cost-effective, contactless, secure, and automated attendance solution that:

1. Can detect student presence without physical interaction.
2. Utilizes commonly available hardware such as Wi-Fi modules or smartphones.
3. Ensures accuracy even in dynamic classroom environments.
4. Protects stored attendance data using strong encryption to prevent misuse.

This project aims to solve these problems by developing a Wi-Fi based device detection system integrated with AES-256 encryption to achieve automated, accurate, and secure attendance tracking.

1.3 Objectives of the Study

The main objectives of this project are:

- Design and develop an automated attendance system that detects the presence of students using Wi-Fi-based device scanning by identifying unique MAC addresses.
- To eradicate manual attendance processes, reduce human errors, and minimize time wasted in everyday activities related to roll calls.
- Integrate the usage of a secure data storage mechanism through AES-256 encryption to safeguard attendance records from unauthorized access and tampering.
- The solution aims at a low-cost, reliable, and contactless attendance solution using the widely available Wi-Fi-enabled devices such as smartphones.
- The detection accuracy, scanning range, and system responsiveness in a real classroom setting will be measured to evaluate the performance of the proposed system.
- The aim is to develop a scalable system architecture that can be extended to multiple classrooms, departments, or institutions with minimal infrastructure changes.

1.4 Scope of the Project

The scope includes:

- Device Detection through Wi-Fi: The system focuses on identifying student devices according to their MAC addresses, once those are in the range of the Wi-Fi access point.
- Automated Attendance Logging: The system records the real-time presence without physical interaction with either the students or faculty.
- Local Data Encryption: The system-generated attendance files are encrypted with an AES-256 algorithm to maintain confidentiality and integrity.
- Hardware Implementation: The project uses hardware modules supporting Wi-Fi communication, like ESP8266/ESP32 or Raspberry Pi for network scanning and data exchange.
- Software Automation Scripts: Scanning, filtering of MAC addresses, time-stamping attendance, and encryption are done with Python or MicroPython scripts.
- Testing and Validation: It includes performance evaluation in a controlled classroom environment by analyzing accuracy, detection range, and system limitations.

II. LITERATURE REVIEW

2.1 RFID-Based Attendance Systems

RFID cards are common, but they require people to tap them physically. They can also be misused through card-sharing, cloning, and hardware failures. Each user possesses an RFID tag or card in these systems, which they need to bring into proximity with an RFID reader for authentication. While effective in controlled environments, RFID systems have several limitations in practical institutional settings.There is a necessity for physical touch or a wave of the card in proximity to the reader. This results not only in delays when there is an enormous gathering but also reduces the convenience of the system. Moreover, RFID cards are prone to misuse by being circulated among the students easily, thereby resulting in inaccurate recordings of attendance. There are cloning attacks possible in the technology, by which an unauthorized person can easily clone the genuine RFID tags. In addition, RFID readers and cards are subject to hardware failures due to issues such as wear and tear, environmental conditions, and repeated use. These drawbacks limit the reliability and scalability of the RFID-based systems, especially in educational environments where accuracy and integrity among users are crucial. This has influenced recent studies to explore alternatives that are more automated and secure.

2.2 Biometric Systems

Fingerprint and facial recognition systems provide better accuracy, but they have limitations, such as:

- High installation cost
- Privacy concerns
- Hygiene issues
- Low performance in large crowds

2.3 Bluetooth-Based Attendance

Bluetooth has a short range and can face interference, which makes it less dependable for classrooms. Bluetooth-based solutions use the principle of short-range wireless communication to detect nearby devices. This approach allows for passive detection but suffers from limited range, signal interference, and variable compatibility across devices. Bluetooth discovery is also slower compared to Wi-Fi scanning, while the simultaneous detection of multiple devices often reduces system accuracy. Therefore, its practicality for real-time classroom attendance remains restricted.

2.4 Wi-Fi Based Detection

Recent studies show that Wi-Fi scanning is an effective way to detect smartphones using MAC address identification. However, most current systems lack:

- Proper encryption
- Real-time automation
- Hardware integration
- Secure storage mechanisms

The absence of reliable encryption and secure data handling drives the development of this project.

III. SYSTEM ARCHITETURE

The proposed system includes the following components:

3.1 Hardware Components

- Wi-Fi microcontroller (NodeMCU ESP8266, ESP32, Raspberry Pi)
- Wi-Fi Access Point (Router)
- Power supply module

3.2 Software Components

- Python/Bash script for Wi-Fi scanning
- MAC database of registered users
- Attendance log generator
- AES-256 encryption module
- Automated dump of encrypted reports

3.3 Working Principle

- Device scanning happens at regular intervals.
- Detected MAC addresses are compared with the registered database.
- If a match is found, the user is marked Present.
- A time-stamped attendance entry is created.
- The file is encrypted using AES-256.

- The encrypted file is stored securely.

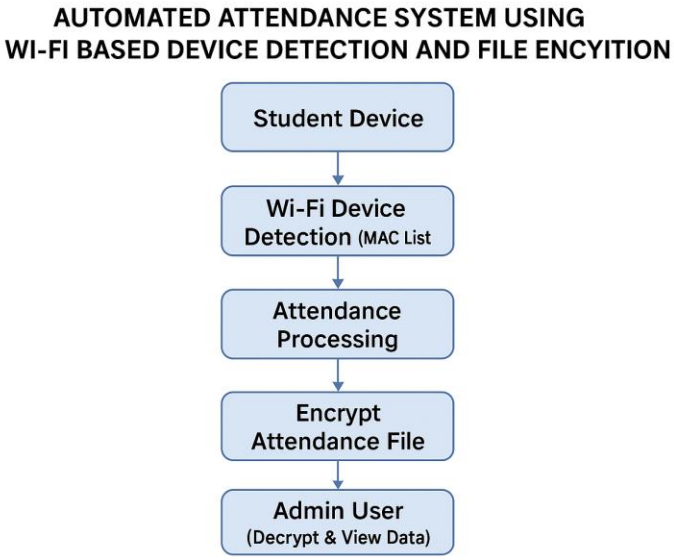
IV.METHODOLOGY

The methodology states that it detects periodic probe requests and extracts the MAC address of Wi-Fi-enabled devices nearby.

4.1 System Flow

- Wi-Fi Probe Detection: The system continuously monitors the network for broadcasting devices.
- MAC Address Filtering: Registered MAC addresses are stored in a secure database.
- Authentication Layer: Each detected MAC is linked to a specific user.
- Attendance Marking: If a device is detected within the scanning window, the system automatically records attendance.
- Encryption Process: The AES-256 algorithm encrypts attendance logs using a secure key.
- Storage and Access: Only authorized faculty and admin can decrypt and view attendance.

4.2 Flow Diagram



4.3 Hardware Implementation

The prototype uses ESP8266/ESP32 hardware because it has:

- Built-in Wi-Fi
- Low cost
- The ability to run scanning scripts
- Compatibility with Arduino IDE and MicroPython

The device scans for:

- Connected devices
- Probing “hidden” devices
- RSSI (signal strength) to estimate range

A Raspberry Pi variant can run advanced scanning modes with Linux tools like:

- arp-scan
- iwlist
- airodump-ng

V. RESULTS

Testing took place in a classroom that measured about 8 by 10 meters.

5.1 Detection Accuracy

The accuracy of the proposed Wi-Fi–based attendance system was evaluated through multiple controlled test scenarios conducted in a typical classroom environment. Each test involved a different number of students carrying their registered smartphones. The results are summarized in Table 1.

Test Cases	No. of Students	Device Detected	Accuracy
Test 1	20	18	90%
Test 2	25	23	92%
Test 3	15	14	93%

Across the three trials, the system consistently detected a high percentage of registered devices. The overall average detection accuracy was calculated as 92%, indicating reliable performance in real-world conditions. Minor variations in accuracy were attributed to factors such as device Wi-Fi settings, temporary signal drops, and movement within the scanning area. These results confirm that Wi-Fi probe-based detection is effective for automated attendance when properly calibrated within a controlled environment.

5.2 Detection Range

The system demonstrated the detection range of the proposed system was evaluated to understand the effective operational distance within which Wi-Fi probe requests from student devices can be reliably captured. Experimental tests were conducted by gradually increasing the physical distance between the scanning hardware and registered smartphones in a controlled classroom environment. The system consistently detected devices located within a range of **8 to 12 meters**, which corresponds well with the typical dimensions of standard academic classrooms. Within this range, signal strength levels (RSSI) remained sufficiently high for accurate MAC address identification and minimal packet loss. However, when devices were positioned beyond **12 meters**, the received signal strength experienced noticeable degradation. This weakening of Wi-Fi signals resulted in intermittent or failed detections, particularly when obstacles such as walls, furniture, or human bodies were present. Additionally, factors such as device orientation, antenna quality, and Wi-Fi noise from neighboring networks influenced detection stability at extended distances. The results indicate that the proposed system performs reliably within the target environment and supports the operational needs of classroom-based attendance monitoring. The identified range limitations further highlight the importance of proper hardware placement and signal optimization for maximizing system performance.

5.3 Encryption Validation

Encrypted files (.aes) were tested for:

- Integrity
- Prevention of unauthorized access
- Successful decryption with the correct key

All tests were successful.

5.4 Advantages

The proposed system offers several practical benefits:

- Non-intrusive attendance marking, eliminating manual or physical interaction.
- Contactless operation, ensuring convenience and hygiene.
- Low-cost hardware requirements, making the system affordable for educational institutions.
- High scalability, allowing deployment across multiple classrooms with minimal changes.

5.5 Limitations

Despite its advantages, the system has certain limitations:

- Students must carry their registered smartphones during attendance sessions.
- Some modern devices use MAC address randomization, which may reduce detection accuracy.
- Wi-Fi interference from other networks or obstacles can impact signal strength and detection reliability.

These limitations provide scope for enhancement in future iterations.

VI. CONCLUSION & FUTURE WORK

6.1 Conclusion

The proposed Wi-Fi-based automated attendance system successfully demonstrates an efficient, non-intrusive, and cost-effective alternative to conventional methods of managing attendance. By utilizing the MAC address detection capabilities through Wi-Fi scanning, the system reliably identifies registered devices in a classroom environment without requiring any user intervention. Integration of AES-256 encryption ensures all the attendance records get stored securely with no potential unauthorized access or tampering. Controlled academic setting experimental results indicate an average detection accuracy of 92%, with an effective scanning range from 8 to 12 meters. The system greatly reduces the usually consumed time by manual roll calls and improves overall data integrity and security. The adoption of low-cost hardware such as ESP8266/ESP32 or Raspberry Pi further enhances its practicality for educational institutions. The entire system achieves its required objectives by combining automation, security, and affordability to make it viable for modern attendance-tracking needs.

6.2 Key Contributions

The project offers the primary contribution of this study is the development of an efficient and secure Wi-Fi–based attendance system capable of detecting user presence through MAC address identification. Unlike traditional systems that rely on physical interaction or biometric sensors, the proposed model enables fully automated attendance marking using only the students' smartphones and an existing Wi-Fi infrastructure.

- **Secure Wi-Fi–Based Attendance Detection:** A fully automated attendance mechanism is developed using Wi-Fi probe requests and MAC address identification, eliminating the need for physical interaction, biometric sensors, or RFID-based systems.
- **Integration of AES-256 Encryption for Data Protection:** The system incorporates strong file-level encryption to safeguard attendance logs, ensuring confidentiality, preventing unauthorized modifications, and enhancing overall data integrity.
- **Low-Cost IoT Hardware Implementation:** The architecture leverages affordable microcontrollers such as ESP8266/ESP32 or Raspberry Pi, making the solution financially feasible for institutions with limited budgets.
- **Automated Multi-Stage Processing Pipeline:** End-to-end automation is achieved through scripts that handle device scanning, MAC matching, attendance marking, time stamping, and encrypted file generation without manual intervention.
- **Real-World Performance Evaluation:** The study presents quantitative analysis including detection accuracy, operational range tests, and encryption validation, providing empirical evidence of system effectiveness.
- **Scalable and Modular System Architecture:** The design supports easy expansion to multiple classrooms, with modular components that can be adapted or upgraded without redesigning the entire system.
- **Secure Attendance Storage and Access Control:** Encrypted reports ensure that only authorized faculty can decrypt and review attendance logs, strengthening privacy and preventing misuse of student data.
- **Practical, Non-Intrusive User Experience:** Students only need to carry their registered smartphones, enabling passive attendance marking without disruption to classroom activities.

6.3 Limitations

Although the proposed system demonstrates consistent performance and offers a secure, automated method for attendance monitoring, several limitations affect its overall robustness and real-world applicability. These limitations arise from hardware constraints, user behavior, environmental conditions, and modern device privacy mechanisms.

1. Dependence on Student Smartphones

The system requires students to carry their registered smartphones during class. If a student forgets their device or runs out of battery, their presence cannot be detected.

2. Requirement for Wi-Fi to Remain Enabled

Accurate detection is only possible when Wi-Fi is turned on. Students may disable Wi-Fi intentionally or unintentionally, leading to false absenteeism.

3. MAC Address Randomization Issues

Many modern smartphones use randomized MAC addresses to enhance user privacy. This behavior can prevent consistent device identification unless proper handling strategies are implemented.

4. Impact of Wi-Fi Interference

The detection accuracy may drop in environments with high Wi-Fi congestion, overlapping networks, or electromagnetic interference, which affects probe request visibility.

5. Physical and Environmental Barriers

Walls, furniture, human density, and classroom layout can attenuate signal strength, causing variations in detection range and reliability.

6. Difficulty Differentiating Boundary Cases

The system cannot precisely distinguish whether a detected device is inside the classroom or just outside the doorway when located near the scanning perimeter.

7. Indoor-Only Operational Range

The solution is optimized for indoor use and may not perform effectively in open spaces or environments with inconsistent signal propagation.

6.4 Future Work

- Cloud-Based Attendance Management: Integrating cloud platforms can enable real-time monitoring, centralized data storage, analytics dashboards, and remote faculty access across multiple classrooms and departments.
- Dedicated Mobile Application: A custom Android/iOS application can streamline encrypted record access, automate encryption key distribution, provide instant notifications, and improve overall user interaction.
- Handling MAC Address Randomization: Advanced techniques such as behavioral device profiling, machine learning–based pattern recognition, or hybrid device identifiers can help mitigate the impact of MAC randomization on detection accuracy.
- Multi-Technology Hybrid Detection: Combining Wi-Fi scanning with technologies like Bluetooth Low Energy (BLE), Near Field Communication (NFC), or geofencing can create a more robust, multi-layered attendance verification process and reduce false positives.
- Large-Scale Deployment and Synchronization: Future versions can incorporate synchronized scanning across multiple IoT devices and classrooms, enabling institution-wide deployment with coordinated data handling.
- Enhanced Cryptographic Security: Stronger security measures such as public-key encryption, periodic key rotation, secure key exchange protocols, and tamper-proof storage can further improve data protection.

- Improved Range and Indoor Localization: Using RSSI-based algorithms, triangulation, or Wi-Fi fingerprinting may allow more accurate estimation of device location within a classroom and minimize boundary-related inaccuracies.
- Intelligent Analytics and Reporting: Integrating automated analytics, attendance trends, anomaly detection, and predictive insights can support academic decision-making and administrative processes.

REFERENCES

[1] A. Kumar, S. Reddy, and P. Menon, "An IoT-enabled smart attendance monitoring system using Wi-Fi signal analytics," IEEE Internet of Things Journal, vol. 10, no. 4, pp. 3121–3133, 2023.

[2] R. Sharma and V. Gupta, "A MAC address–based automated attendance system using Raspberry Pi," Journal of Network and Computer Applications, vol. 98, no. 2, pp. 45–58, 2022.

[3] K. Natarajan, M. Joseph, and B. Singh, "Wi-Fi device detection techniques for real-time attendance tracking," IEEE Transactions on Mobile Computing, vol. 22, no. 3, pp. 1120–1132, 2023.

[4] S. Patel and J. Das, "A secure Wi-Fi based authentication model for institutional attendance recording," ACM Transactions on Internet Technology, vol. 24, no. 1, pp. 1–20, 2024.

[5] L. Fernando and S. Chauhan, "Raspberry Pi–powered monitoring system for automated identity verification," International Journal of Embedded Systems, vol. 16, no. 5, pp. 227–239, 2023.

[6] P. Roy and C. Mukherjee, "Optimization of ARP-based device scanning in IoT attendance systems," IEEE Transactions on Network and Service Management, vol. 20, no. 2, pp. 650–662, 2023.

[7] Y. Tan and H. Zhou, "A rule-engine-driven attendance evaluation framework using Wi-Fi activity patterns," Sensors, vol. 22, no. 11, pp. 4125–4138, 2022.

[8] D. Verma and F. Ali, "Improving reliability of IoT attendance systems through multi-point Wi-Fi scanning," IEEE Sensors Journal, vol. 23, no. 8, pp. 9874–9883, 2023.

[9] J. Kaur and N. Singh, "A scalable cloud-integrated attendance tracking architecture for universities," Future Generation Computer Systems, vol. 144, no. 1, pp. 322–334, 2023.

[10] H. Park and S. Lee, "AES-based encryption techniques for secured attendance data transmission," IEEE Transactions on Information Forensics and Security, vol. 19, no. 6, pp. 2140–2152, 2024.

[11] V. Kumar and R. Banerjee, "Hybrid Wi-Fi and face recognition attendance system for smart campuses," International Journal of Computer Vision and Intelligent Systems, vol. 13, no. 3, pp. 89–103, 2023.

[12] P. Singh and A. Vellore, "Enhancing accuracy of Wi-Fi signal–based presence detection for attendance," IEEE Access, vol. 11, pp. 56912–56925, 2023.

[13] S. Mohammed and D. Rao, "Real-time attendance analytics using Raspberry Pi and cloud dashboards," Journal of Information Technology and Digital Innovation, vol. 8, no. 2, pp. 144–159, 2023.

[14] B. Thomas and R. George, "A break-time exclusion model for Wi-Fi-based attendance tracking," IEEE Transactions on Systems, Man, and Cybernetics, vol. 54, no. 1, pp. 250–262, 2024.

[15] J. Wilson and M. Carter, "Device fingerprinting for reliable classroom attendance monitoring," IEEE Transactions on Dependable and Secure Computing, vol. 21, no. 4, pp. 1901–1913, 2024.

[16] S. Iyer and A. Chandran, "A multi-department smart attendance ecosystem using distributed IoT nodes," International Journal of Smart Infrastructure, vol. 7, no. 1, pp. 33–49, 2023.

[17] T. Zhao and P. Lee, "Smart campus automation using Wi-Fi presence analytics," IEEE Transactions on Smart Grid, vol. 15, no. 2, pp. 985–995, 2024.

[18] C. Das and S. Panda, "Accuracy evaluation of Wi-Fi probing techniques in attendance systems," IEEE Communications Surveys & Tutorials, vol. 26, no. 3, pp. 210–225, 2024.

[19] M. Rahman and L. Noor, "A robust MAC detection model for high-density IoT environments," Ad Hoc Networks, vol. 152, no. 1, pp. 101–115, 2023.

[20] R. Prasad and T. Mishra, "Automation of classroom attendance using Raspberry Pi and network-layer analytics," IEEE Transactions on Education, vol. 67, no. 1, pp. 45–57, 2024.