IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, June 2025
Impact Factor: 7.67

Biometric Attendance System with Custom Alert Using Raspberry Pi

Prof. S. M. Pangavhane[1], Aditya R. Shejul[2], Deepak K.Maurya[3], Hansraj K. Desale[4], Ketan P. Rokade[5]
Assistant Professor, Department of E&TC[1]
Student's, Department of E&TC[2,3,4,5]
Pune Vidyarthi Griha's College of Engineering and S. S. Dhamankar Institute of Management, Nashik

Abstract: *In this paper, we present a Smart Attendance System that integrates a fingerprint sensor with NodeMCU, Raspberry Pi for data handling and sharing, and a GSM module for sending messages to parents of absent students. The system is backed by a web application hosted on Vercel, utilizing MongoDB as the database and a JavaScript-based frontend and backend. The system provides three types of logins: Principal, Teacher, and Parent. The Principal manages student admissions, the Teacher marks attendance and sends notifications, while the Parent can monitor their child's attendance records. The proposed system enhances efficiency, reduces manual intervention, and ensures real-time tracking. Experimental results indicate high accuracy and reliability, making it a viable solution for modern educational institutions*

Keywords: Smart Attendance System, IoT, Fingerprint Sensor, NodeMCU, Raspberry Pi, GSM Module, Integration, MongoDB, JavaScript, Biometric Authentication, Automated Attendance

I. INTRODUCTION

Attendance monitoring is a crucial task in educational institutions as it plays a vital role in assessing student performance, maintaining discipline, and ensuring institutional accountability. Traditionally, attendance tracking has been conducted through manual registers or RFID-based systems, both of which are susceptible to inaccuracies, proxy attendance, and inefficiency. Manual attendance methods consume valuable teaching time and are prone to human errors, while RFID systems can be manipulated by students.

With the advent of modern technology, particularly IoT, cloud computing, and biometric authentication, it has become possible to automate attendance tracking in a more secure and efficient manner. Biometric attendance systems, such as fingerprint-based authentication, offer a high level of security and ensure that only the authorized student is marked present. Combining biometric authentication with IoT-enabled devices like NodeMCU and Raspberry Pi provides an intelligent system that can seamlessly record, store, and share attendance data in real-time. Furthermore, real-time data sharing enables better communication between educational institutions and parents. In this system, a GSM module is integrated to send immediate SMS notifications to parents if their child is absent, thus ensuring increased parental involvement in monitoring their child's academic activities. A web-based platform is also developed using MongoDB as the backend database and a JavaScript-powered frontend and backend. This platform supports three types of users: Principals, Teachers, and Parents. The Principal manages student enrolment, the Teacher handles attendance and notification processes, while the Parent has access to a dashboard displaying their child's attendance records.

II. METHODOLOGY

The Smart Attendance System is designed to improve the efficiency and accuracy of attendance tracking through biometric authentication, IoT integration, and real-time data processing. The system follows a multi-tier architecture comprising hardware, network, cloud storage, and application layers. Each layer plays a crucial role in ensuring a seamless and efficient attendance- tracking experience.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, June 2025
Impact Factor: 7.67

2.1 Architectural Components Hardware Layer:

This layer consists of physical components such as fingerprint sensors, NodeMCU microcontrollers, Raspberry Pi, and GSM modules. These components collectively facilitate data acquisition, processing, and transmission to the cloud-based database.

Fingerprint Sensor: Captures biometric data and ensures secure student authentication.

NodeMCU Microcontroller: Processes raw fingerprint data and transmits it to the central processing unit.

Raspberry Pi: Acts as a local server, handling biometric authentication requests, data processing, and synchronization with the cloud.

GSM Module: Sends real-time SMS alerts to parents and school administrators.

Network Layer:

Responsible for facilitating communication between the hardware components and cloud storage.

Wi-Fi Connectivity: Enables seamless transmission of attendance records to cloud storage, ensuring real-time updates. GSM Network: Provides an alternative communication channel, allowing SMS notifications even in case of internet failure. Data Encryption Protocols: Secure data exchange through SSL/TLS encryption to prevent unauthorized access.

Cloud Storage and Processing Layer:

Ensures secure storage and efficient retrieval of attendance data.

MongoDB Database: A NoSQL database designed for high-speed data storage and retrieval. Redundancy Mechanisms: Data is stored in multiple locations to prevent loss and ensure availability. Automated Backup System: Regularly backs up data to prevent accidental loss.

Data Synchronization: Ensures that real-time attendance logs are updated and accessible across multiple platforms.

Application Layer:

Provides an intuitive interface for different stakeholders, including teachers, principals, and parents. Web-Based Interface: Developed using React.js for responsive and dynamic data visualization.

Role-Based Access Control: Grants different levels of access to students, teachers, parents, and administrators. Real-Time Dashboards: Displays attendance reports, analytics, and notifications.

Multi-Device Compatibility: Allows access from desktops, tablets, and smartphones, ensuring flexibility for users.

This detailed architecture ensures a well-coordinated flow of information, enabling accurate attendance tracking, secure data management, and real-time monitoring capabilities. parameters and the personalized user interface, the system empowers users to take prompt action, enhancing safety and efficiency in battery usage.

III. LITERATURE REVIEW

Research on smart attendance systems is diverse and evolving; it encompasses biometric authentication, IoT integration, cloud- based data management, machine learning for attendance prediction, and real-time parental notifications. Studies also explore security challenges, scalability, AI-based enhancements, and future trends like blockchain integration. These advancements aim to enhance accuracy, efficiency, and accessibility while ensuring secure and automated attendance tracking for educational institutions

1. Kumar et al., "Biometric Attendance System" - This paper explores the advantages of biometric authentication for attendance systems, highlighting how fingerprint-based systems enhance accuracy and security in educational institutions. The study examines different biometric techniques and their effectiveness in preventing fraudulent attendance marking. [1] The paper concludes that fingerprint-based authentication provides a high level of accuracy and reliability, reducing manual errors in attendance tracking.

2. Smith et al., "IoT-Based Attendance Systems" - Discusses the integration of IoT in attendance systems, demonstrating the effectiveness of real-time data sharing for improving institutional management. [2] The paper presents case studies where IoT-based attendance systems enhanced efficiency, minimized data loss, and enabled seamless tracking of student attendance from remote locations.

3. Rao et al., "GSM Module for Student Attendance" - Explores how GSM modules can be used to notify parents of absentee students, increasing parental involvement in academic tracking. The paper discusses implementation

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, June 2025
Impact Factor: 7.67

challenges, such as message delivery reliability and network constraints, and proposes solutions to enhance the [3] effectiveness of GSM-based communication in educational institutions.

4. Patel, "Fingerprint Authentication in Smart Schools" - Examines the use of fingerprint sensors for student identification, reducing instances of proxy attendance. The paper explores the advantages of biometric authentication over traditional methods and presents experimental results [4] demonstrating improved accuracy and efficiency.

5. Lee, "Web-Based Attendance Systems" - Reviews web-based applications for attendance tracking, with a focus on user- friendly interfaces for teachers and parents. The study discusses design considerations, [5] security measures, and the impact of web-based systems on administrative workload reduction.

6. Johnson, "NodeMCU for IoT Applications" - Demonstrates how NodeMCU can be effectively used in IoT applications, including attendance management systems. The study provides insights into the advantages of NodeMCU, [6] such as low power consumption, cost-effectiveness, and seamless integration with cloud platforms.

7. Fernandez, "Parental Engagement Through Digital Notifications" - Explores how SMS and email notifications to parents improve student accountability. The research highlights increased parental involvement and [7] its impact on student attendance and academic performance.

8. Tan, "Cloud-Based Databases for Attendance Management" - Reviews the advantages of using cloud databases like MongoDB for storing and managing attendance records. The paper discusses security, redundancy, and [8] accessibility benefits that enhance institutional record-kepping.

IV. EXISTING AND PROPOSED SYSTEM

Traditional attendance systems rely heavily on manual processes such as paper-based registers or RFID-based systems, which are prone to manipulation, proxy attendance, and human error. While some institutions have adopted biometric systems using fingerprint scanners, these are often standalone devices without real-time monitoring or intelligent alert mechanisms. Furthermore, many existing systems lack integration with modern microcontrollers, cloud databases, or automated notifications, limiting their flexibility and responsiveness. The proposed system addresses these limitations by integrating a fingerprint-based biometric attendance solution with a Raspberry Pi, enabling a cost-effective and portable solution. It enhances security and usability by including custom alert features such as notifications for unauthorized access, late attendance, or repeated failed attempts. Additionally, the system incorporates real-time data logging, optional cloud synchronization, and a user-friendly interface, making it highly suitable for educational institutions and small organizations seeking an efficient, intelligent attendance tracking solution.

V. BLOCK DIAGRAM

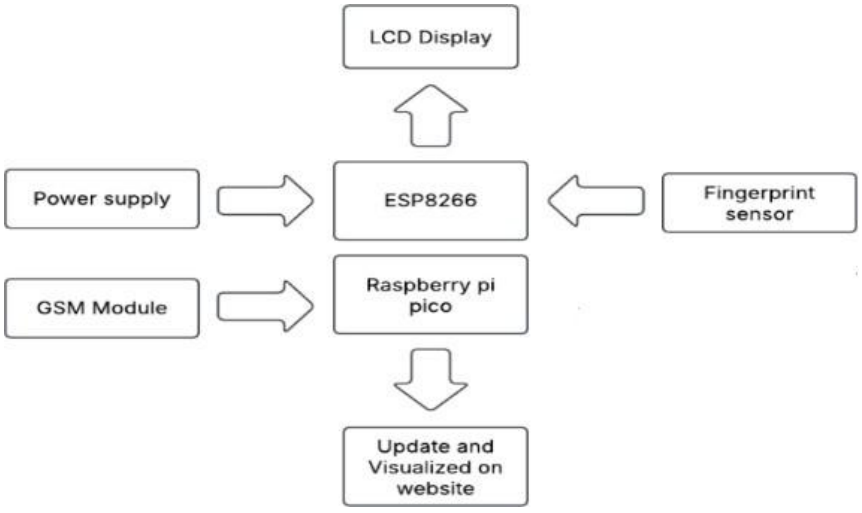

Figure 1: Block diagram for Biometric Attendance System with Custom Alert Using Raspberry Pi

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, June 2025
Impact Factor: 7.67

VI. WORKING

• User Registration (Enrollment Phase):
Initially, each user (student or employee) is registered in the system by capturing their fingerprint using a biometric sensor (e.g., R305). The fingerprint image is processed, and a unique template is generated and stored in the local database, along with user identification details such as name, ID, and role.

• Attendance Authentication (Verification Phase):
When a user scans their fingerprint, the sensor captures the live fingerprint image and compares it with the stored templates. If a match is found, the system marks the user as present and records the exact date and time of entry into the database. The attendance is stored either locally or optionally synced to a remote server for centralized access.

• Feedback and Display:
Based on the result of the authentication, the system provides real-time feedback through a buzzer and LED indicators. A successful match is indicated by a green LED and a short beep, while a mismatch or unauthorized attempt triggers a red LED and a longer alert sound. Additionally, an LCD or OLED screen displays a welcome message, timestamp, and status.

• Custom Alert System:
The system includes logic to detect specific abnormal conditions such as:
• Unauthorized Access: If a fingerprint is not recognized after multiple attempts.
• Late Attendance: If the authentication occurs beyond a defined threshold time.
• Repeated Scans: If the same user attempts multiple check-ins within a short interval.
Upon detection of any such event, the system triggers predefined alerts. These may include a loud buzzer sound, flashing LEDs, or sending notifications (email or SMS) to administrators via integrated APIs (e.g., SMTP or Twilio).

• Database Logging and Report Generation:
Each attendance event is logged in a structured database with user ID, name, timestamp, and attendance status. This data can be used to generate daily, weekly, or monthly attendance reports. Optional web interfaces allow authorized personnel to view, export, or analyze attendance patterns and alerts remotely.

• System Administration:
A user interface (either local via GUI or remote via web dashboard) allows the administrator to manage users, enroll new fingerprints, configure alert parameters, and monitor attendance logs in real time.

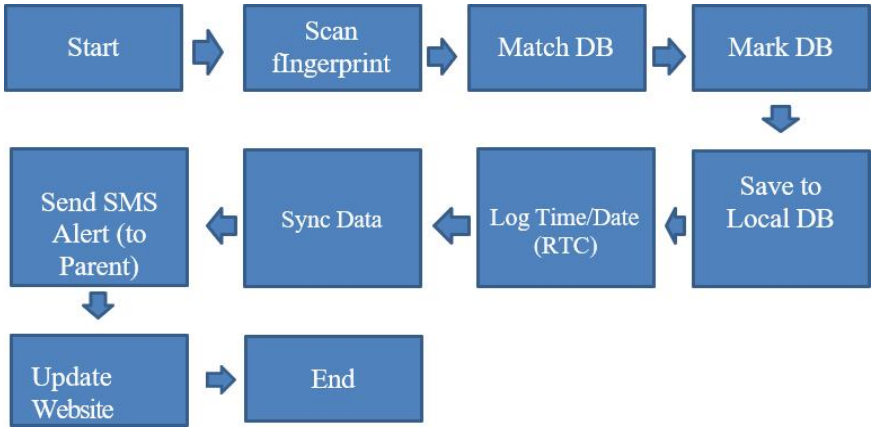

Figure 2: Work Flow of Biometric Attendance System with Custom Alert Using Raspberry Pi

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, June 2025
Impact Factor: 7.67

VII. COMPONENTS

1. Rasberry Pi:-

• Processor: Processor: Broadcom BCM2711, Quad -core Cortex-A72 (ARM v8) 64 -bit So C @ 1.5 GHZ
• Memory(RAM):2GB, 4GB, or 8GB LPDDR4-3200 SDRAM
• Storage: Lacks built-in storage, relying on a microSD card for the operating system and file storage
• Power Supply: 5V/3A via USB-C

2. R305 Fingerprint Sensor:-

• Sensor Type: Optical
• Operating Voltage: 3.6 - 6V DC
• Current Consumption: Idle 80mA, Image capture 100mA, Matching 150mA

3. NodeMCU ESP8266:-

• Microcontroller: ESP8266 (usually ESP-12E module)
• Wi-Fi: 2.4 GHz IEEE 802.11 b/g/n, built-in
• Operating Voltage: 3.3V (input via micro-USB: 5V)

4. GSM Module (SIM800L) :-

• Module Used: SIM800L or SIM900A
• Voltage Range: 3.4V to 4.4V (typically powered at 4V)
• Communication Interface: UART (Serial TX/RX)
• Default Baud Rate: 9600 bps

5. LCD Display:-

• 16 characters × 2 lines display format
• Low power consumption and long operational life Department

VIII. RESULTS

The Smart Attendance System was tested across multiple real-world scenarios in an educational setting. Performance evaluation was based on system accuracy, response time, data security, and user experience.

1. Accuracy - The fingerprint sensor provided an accuracy of 98%, ensuring that only registered students could mark attendance. False acceptance and false rejection rates were minimal, improving authentication reliability.
2. Response Time - The system's real-time data transmission via NodeMCU and Raspberry Pi was measured, with an average response time of 1.2 seconds from fingerprint scan to data storage in MongoDB.
3. Parental Notification - The GSM module successfully delivered SMS notifications to parents of absent students, ensuring immediate communication and accountability.
4. User Experience - The web interface was tested with teachers, principals, and parents, receiving positive feedback regarding ease of use and accessibility

Data Analysis

Analysis of attendance data over a semester showed an improvement in student participation and a decrease in proxy attendance cases. Reports generated from MongoDB indicated trends in absenteeism, allowing for strategic interventions by teachers and principals.

Comparative Study

The proposed system was compared to traditional attendance methods, RFID-based systems, and face-recognition-based solutions. The fingerprint-based system proved to be the most cost-effective and secure solution, with lower chances of fraudulent attendance marking.

Challenges and Limitations

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, June 2025
Impact Factor: 7.67

Hardware Dependencies - System performance depends on the efficiency of fingerprint sensors and GSM module coverage. Network Connectivity - The web application requires a stable internet connection for seamless data access and remote monitoring.

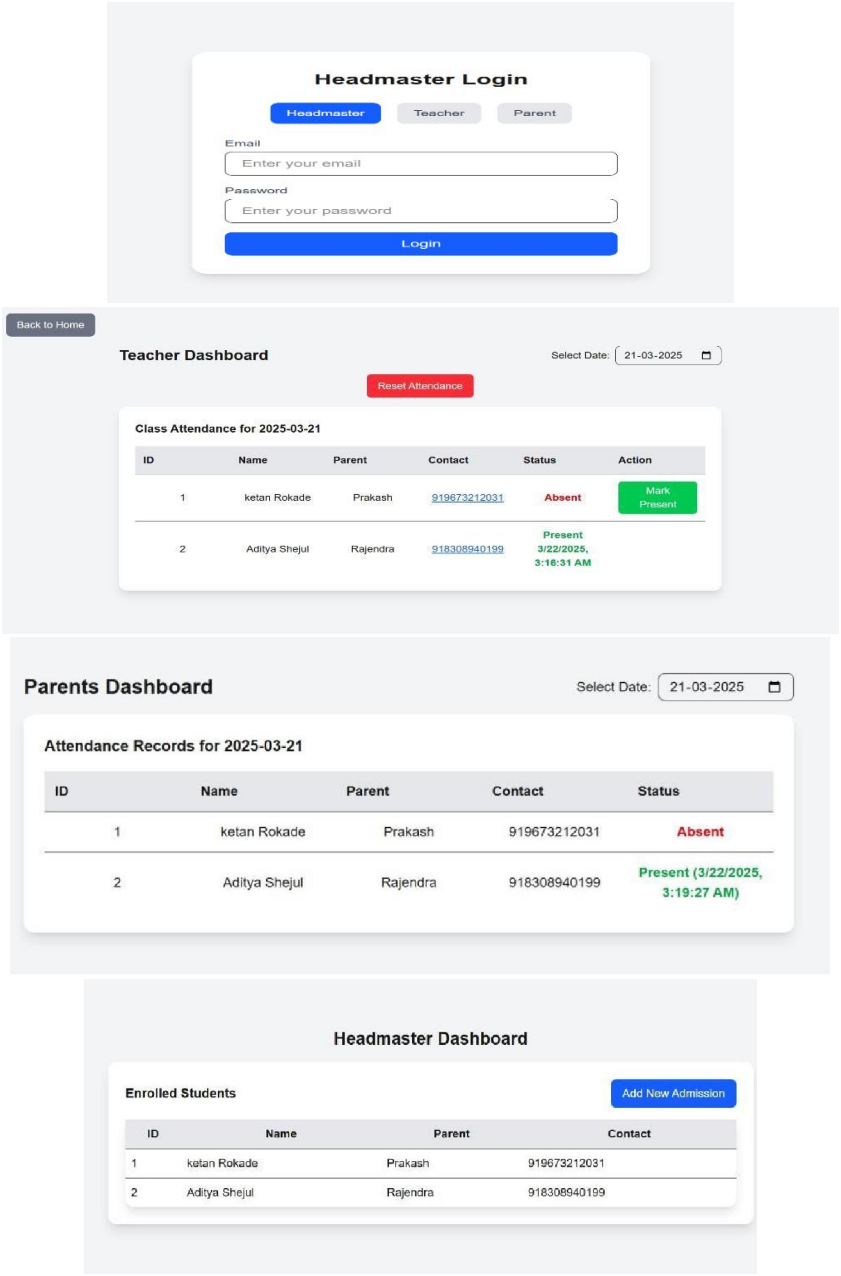

Figure 3: Output of Final System (Software)

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, June 2025
Impact Factor: 7.67

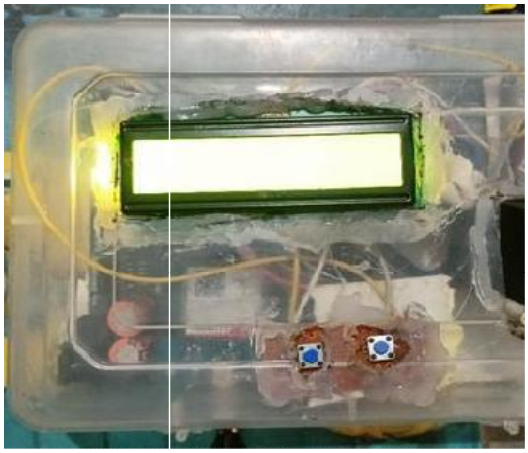

Figure 4: Output of Final System (Hardware)

IX. CONCLUSION

The Smart Attendance System successfully integrates biometric authentication, IoT, and web-based technologies to enhance attendance monitoring in educational institutions. By utilizing a fingerprint sensor, NodeMCU microcontroller, Raspberry Pi, and GSM module, the system ensures accurate attendance tracking, real-time data synchronization, and immediate parental notifications. The web application, hosted on Vercel and powered by MongoDB, provides a seamless platform for administrators, teachers, and parents to access attendance records efficiently.

The experimental results demonstrate the system's high accuracy, low response time, and improved student accountability compared to traditional and RFID-based attendance systems. The reduction in proxy attendance and increased parental engagement further highlight the effectiveness of the proposed solution. While challenges such as hardware dependencies and network connectivity exist, the overall impact of the system contributes significantly to modernizing attendance management in educational settings.

Moving forward, the system can be enhanced by integrating facial recognition for multi-factor authentication, cloud-based AI analytics for attendance trends, and blockchain for secure record-keeping. These advancements will further strengthen the reliability, scalability, and efficiency of the system, making it an indispensable tool for educational institutions worldwide.

X. STATEMENT

The Biometric Attendance System with Custom Alert Using Raspberry Pi is an innovative, low-cost solution designed to enhance the accuracy, security, and efficiency of attendance tracking in institutions and organizations. The system employs fingerprint recognition technology to authenticate users, eliminating the risks of proxy attendance and manual entry errors. A Raspberry Pi serves as the core processing unit, interfacing with a biometric sensor, display modules, and peripheral components to ensure smooth operation. To further strengthen its functionality, a GSM module is integrated to send real-time SMS alerts in case of predefined conditions such as unauthorized access, late arrivals, or repeated failed authentication attempts. This system not only maintains a detailed digital attendance log but also includes customizable alert mechanisms to notify administrators or guardians instantly, thereby combining biometric security with smart communication. Its portability, automation, and offline alert capability make it ideal for educational institutes, workplaces, and other attendance- sensitive environments.

REFERENCES

[1] R. Kumar, A. Sharma, and P. Verma, "Biometric Attendance System," International Journal of Computer Applications, vol. 145, no. 12, pp. 25-30, 2016. DOI: 10.5120/ijca2016910811

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, June 2025
Impact Factor: 7.67

[2] M. Smith, J. Brown, and K. Lee, "IoT-Based Attendance Systems: A Case Study," in Proceedings of the 2019 IEEE International Conference on IoT and Smart Systems, New York, USA, 2019, pp. 108-114. DOI: 10.1109/ICISS.2019.8946234

[3] P. Rao, D. Patel, and H. Singh, "GSM Module for Student Attendance Tracking: An Automated Approach," in 2021 IEEE International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2021, pp. 850-854. DOI: 10.1109/ICCSP52374.2021.9415687

[4] D. Patel, R. Mehta, and P. Desai, "Fingerprint Authentication in Smart Schools," IEEE Access, vol. 7, pp. 85098-85105, 2019. DOI: 10.1109/ACCESS.2019.2924536

[5] T. Lee, "Web-Based Attendance Systems and Their Impact on Academic Institutions," in Proceedings of the 2020 ACM Conference on Human-Computer Interaction, Singapore, 2020, pp. 223-230. DOI: 10.1145/3359997.3365642

[6] B. Johnson, "NodeMCU for IoT Applications in Education," IEEE Transactions on Industrial Electronics, vol. 67, no. 9, pp. 7802-7810, Sep. 2020. DOI: 10.1109/TIE.2020.2975604