



GPS-Enabled Fingerprint Attendance System for Enhanced Staff Monitoring

Yahaya Aliyu Usman¹, Aliyu Musa Bade²

¹Department of Computer Science, Federal Polytechnic Damaturu, Nigeria

²Department of Computer Science, Yobe State University, Damaturu, Nigeria

DOI: <https://doi.org/10.51244/IJRSI.2026.1308000329>

Received: 09 September 2026; Accepted: 14 September 2026; Published: 25 September 2026

ABSTRACT

Traditional attendance management methods, such as manual registers and conventional biometric systems, are often vulnerable to proxy attendance, inaccurate record keeping, location-related challenges, and administrative inefficiencies. This study presents the prototype implementation of a GPS-Enabled Fingerprint Attendance System designed to improve staff attendance monitoring through the integration of fingerprint biometric authentication, Global Positioning System (GPS) technology, and geofencing. The prototype was developed to verify the identity of registered staff members and confirm their physical presence within an authorized geographical location before attendance is recorded. The implementation consists of a user interface, application processing layer, MySQL database, fingerprint scanner, and location service for GPS verification. Prototype testing focused on fingerprint authentication, GPS location validation, attendance recording, database operations, administrative monitoring, and report generation. The results from the functional testing demonstrate that the prototype can successfully perform the intended attendance verification and recording processes under the defined test scenarios. The system also incorporates security features including password protection, role-based access control, encrypted biometric templates, and audit logging. Although the prototype provides a practical foundation for automated staff attendance monitoring, further evaluation is required to establish its performance under large-scale real-world deployment. The prototype therefore provides a basis for future development and institutional implementation of secure, location-aware biometric attendance management systems.

Keywords: biometric, fingerprint, gps, geofencing, attendance management, prototype implementation.

INTRODUCTION

In the contemporary organizational landscape, effective staff monitoring and attendance management are pivotal for adopting productivity, ensuring accountability, and optimizing operational efficiency. Traditional attendance mechanisms, such as manual logbooks or time clocks, have been plagued by inefficiencies, including susceptibility to errors, fraudulent practices, and limited real-time oversight (Jiang & Jiang, 2025). The advent of biometric technologies, particularly fingerprint recognition, has revolutionized authentication processes by leveraging unique physiological characteristics that are difficult to replicate (Muhtahir et al., 2025). However, in dynamic work environments involving remote or field-based operations, mere biometric verification falls short without spatial context.

The rapid advancement of Information and Communication Technology (ICT) has transformed the way organizations manage information, automate operations, and improve service delivery. Educational institutions, in particular, have increasingly adopted software-based solutions to enhance administrative efficiency, data management, and staff accountability. Among the various administrative functions within tertiary institutions, attendance management remains a critical component for monitoring staff punctuality, productivity, and compliance with institutional regulations. Effective attendance management contributes significantly to organizational performance by ensuring accountability, improving workforce management, and supporting informed decision-making (Laudon & Laudon, 2022).

Despite the advantages of fingerprint-based attendance systems, challenges still exist, particularly regarding location verification. A conventional fingerprint attendance system can confirm the identity of a staff member but cannot verify whether the attendance was recorded within an authorized location. This limitation creates opportunities for fraudulent attendance practices, especially in institutions with multiple offices, departments, or staff members performing duties outside their designated workstations (Adebayo & Olatunji, 2020). Therefore, there is a need for a more intelligent attendance management system that combines biometric authentication with location-based verification.

The Global Positioning System (GPS) is a satellite-based technology that enables the determination of geographical locations with a high degree of accuracy. GPS technology has become widely used in navigation, transportation, logistics, security monitoring, and location-based services (Kaplan & Hegarty, 2020). Integrating GPS functionality into a fingerprint attendance system provides an additional layer of security by ensuring that attendance is recorded only within approved geographical locations. Such integration enhances transparency, reduces attendance fraud, and improves institutional accountability.

LITERATURE REVIEW

Attendance monitoring has long been recognized as an essential administrative function in educational institutions, government agencies, healthcare facilities, and corporate organizations. Accurate attendance records are fundamental for workforce planning, payroll administration, productivity assessment, performance evaluation, and institutional accountability (Bourne et al., 2021). Traditionally, attendance was recorded manually through paper registers or signature sheets. Although these methods were inexpensive to implement, they were susceptible to numerous challenges, including inaccurate record keeping, proxy attendance, human error, document loss, and manipulation of attendance records. These shortcomings significantly reduced the reliability and integrity of attendance management processes, particularly in organizations with large numbers of employees (Saraswat et al., 2022).

The rapid advancement of digital technologies has transformed attendance management from manual record keeping to automated electronic systems. Modern attendance solutions employ technologies such as Radio Frequency Identification (RFID), Quick Response (QR) codes, Near Field Communication (NFC), facial recognition, iris recognition, fingerprint biometrics, cloud computing, artificial intelligence, and mobile computing. These technologies have improved the speed, accuracy, and efficiency of attendance recording while reducing administrative workload and operational costs (Alshamrani et al., 2023). However, despite these improvements, many existing systems continue to face challenges related to identity verification, location authentication, data security, privacy protection, and resistance to fraudulent attendance practices.

Among the available biometric technologies, fingerprint recognition remains one of the most reliable, affordable, and widely adopted methods for identity authentication. Fingerprint patterns are unique to every individual and remain stable throughout a person's lifetime, making fingerprint authentication highly suitable for attendance management applications. Numerous studies have demonstrated that fingerprint-based attendance systems effectively eliminate impersonation and "buddy punching," thereby improving data accuracy and organizational transparency (Jain et al., 2021). Advances in fingerprint sensor technology have also increased recognition speed, reduced error rates, and improved user convenience, enabling widespread deployment across educational institutions and workplaces.

Although fingerprint authentication effectively verifies an individual's identity, it cannot independently confirm the physical location where attendance is recorded. This limitation has become increasingly significant with the widespread adoption of remote work, mobile workforce management, field operations, and decentralized organizational structures. As a result, researchers have increasingly explored the integration of Global Positioning System (GPS) technology into attendance management systems. GPS enables organizations to validate the geographical location of employees during attendance registration, ensuring that attendance is recorded only within authorized locations or designated geofenced areas. This capability enhances organizational accountability and significantly reduces location-based attendance fraud (Naseri et al., 2024).

The integration of GPS and fingerprint technologies represents an important advancement in intelligent attendance management systems. By simultaneously verifying both employee identity and physical location, hybrid biometric systems provide dual-layer authentication that substantially improves system reliability and security. Such integrated systems are particularly valuable in higher education institutions, government establishments, healthcare organizations, construction sites, and organizations employing mobile or field-based personnel. Furthermore, cloud-based infrastructures facilitate real-time synchronization of attendance records, centralized database management, automated report generation, and remote administrative monitoring, thereby enhancing operational efficiency and supporting data-driven decision-making (Jiang & Jiang, 2025).

Historical Evolution of Attendance Systems

The evolution of attendance monitoring systems has progressed from conventional manual record-keeping methods to intelligent digital platforms driven by the increasing demand for accuracy, transparency, security, and operational efficiency. Recent studies indicate that modern attendance systems have significantly improved organizational productivity through automation, cloud computing, and biometric authentication (Ali et al., 2022; Saraswat et al., 2022). Early digital attendance systems focused primarily on replacing paper-based registers with electronic logging systems but were still limited by identity fraud, proxy attendance, and poor scalability (Moshayedi et al., 2022).

With the rapid advancement of mobile computing and wireless communication technologies, attendance systems have increasingly integrated smartphones, biometric sensors, and location-aware services. Mobile-based attendance applications now employ fingerprint authentication, GPS positioning, and Near Field Communication (NFC) to verify both user identity and physical presence during attendance registration (Juang et al., 2022; Nurtjahjani et al., 2022). These technologies have substantially reduced attendance fraud while improving the flexibility of workforce management across educational institutions and corporate organizations.

Recent developments have further shifted attendance systems toward intelligent multi-factor authentication frameworks that combine fingerprint biometrics, GPS geofencing, cloud databases, Internet of Things (IoT) devices, and artificial intelligence. Hybrid attendance systems provide dual verification by confirming both the identity and geographical location of users before attendance is accepted (Alshamrani et al., 2023; Vinay et al., 2023). Cloud-enabled attendance platforms further support real-time synchronization, centralized database management, automated reporting, and remote monitoring, thereby improving administrative efficiency and decision-making (Naseri et al., 2024).

Review of Biometric Authentication Technologies

Biometric authentication has become one of the most reliable approaches for modern attendance management because it utilizes unique physiological characteristics that cannot easily be duplicated. Among the available biometric techniques, fingerprint recognition remains the most widely adopted due to its high accuracy, affordability, and ease of implementation (Jain et al., 2022). Recent fingerprint-based attendance systems have demonstrated significant improvements in eliminating impersonation, proxy attendance, and manual recording errors (Rahman et al., 2023; Memane et al., 2022).

Recent advances in biometric technologies have also incorporated facial recognition, iris recognition, deep learning algorithms, and artificial intelligence to improve authentication accuracy and reduce false acceptance and rejection rates. Studies by Ukamaka Bertrand et al. (2023) and Alshamrani et al. (2023) demonstrate that multimodal biometric systems combining fingerprint and facial recognition provide higher security than single-biometric approaches.

Despite these improvements, biometric systems continue to face challenges such as spoofing attacks, environmental interference, privacy concerns, and template security. Recent studies have addressed these limitations through liveness detection, encrypted biometric templates, blockchain-based identity management, and cloud security mechanisms (Bharathy et al., 2022; Vinay et al., 2023). Furthermore, Ussher-Eke et al. (2025) reported that biometric attendance systems significantly improve organizational accountability, human resource management, and workforce productivity, particularly in developing countries where attendance fraud remains



prevalent.

GPS and Geolocation in Monitoring Systems

Global Positioning System (GPS) technology has become an essential component of intelligent attendance management by providing real-time geographical verification during attendance registration. Unlike conventional biometric systems that verify only user identity, GPS-enabled attendance systems ensure that users are physically present within authorized locations before attendance is recorded (Habibah & Sumarno, 2022).

Recent attendance applications increasingly integrate GPS with geofencing technologies to establish virtual boundaries around workplaces and educational institutions. When users attempt to register attendance outside designated areas, the system automatically rejects the request, thereby preventing location-based attendance fraud (Prasada & Ikrimach, 2024; Ardianto et al., 2022).

Cloud-enabled GPS attendance systems further improve monitoring through real-time synchronization, automated reporting, and centralized database management. These systems have proven particularly useful for organizations with remote workers, field personnel, and multiple operational locations (Naseri et al., 2024; Darojah et al., 2025). Current research indicates that integrating GPS, biometric authentication, cloud computing, and mobile technologies provides a secure, scalable, and reliable attendance management solution suitable for higher education institutions and modern organizations (Jiang & Jiang, 2025).

Hybrid GPS-Fingerprint Systems

Hybrid systems merging GPS and fingerprints represent the current innovations, offering dual verification for enhanced security. Vinay et al. (2023) proposed smart systems using biometrics and GPS, tailored for educational environments. Chandramohan et al. (2017) monitored students with biometric-GPS tracking. Soewito and Simanjuntak (2014) optimized mobile devices with GPS-biometrics. Khan et al. (2020) developed secure remote multipurpose systems. Chiang et al. (2022) evaluated smartphone systems with GPS and NFC. Abd El-Mawla et al. (2022) combined QR, fingerprint, and face recognition. Nwabuwe et al. (2023) mitigated fraud with dynamic QR, geo-fencing, and IMEI. Divya et al. (2024) hybridized geo-location and facial verification, adaptable to fingerprints. Chauhan et al. (2024) tracked employees with face recognition and geo-fencing. Murali et al. (2024) created GPS-based Android apps with cloud storage. Rahkoyo et al. (2024) enhanced IoT fingerprint systems for efficiency. Moshayedi et al. (2024) designed portable IoT self-attendance systems. Darojah et al. (2025) developed digital systems with Appsheet, GPS, and biometrics. On et al. (2025) automated with RFID and geospatial visualization. Aguda (2024) integrated QR, biometrics, and GPS for school employees. Becerra et al. (2024) created portable modules for universities.

Table 1: Comparison of Attendance System

System Type	Key Features	Advantages	Disadvantages	Representative References
Traditional/Manual	Logbooks, punch cards	Low initial cost	High fraud, manual errors	Yuan et al. (2015); Reda et al. (2011)
Biometric-Only	Fingerprint/recognition	Unique identification	Vulnerable to spoofing, no location	Muhtahir et al. (2013); Kadry & Smaili (2010)
GPS/Geolocation-Only	Location tracking, geofencing	Real-time spatial verification	Dependent on signal strength	Elbehiery (2019); Makhtar et al. (2016)
Hybrid GPS-Fingerprint	Biometrics + GPS + IoT/Cloud	Fraud-resistant, comprehensive	Higher complexity and cost	Vinay et al. (2023); Moshayedi et al. (2024); Khan et al. (2020)

Theoretical Foundations

Theoretical frameworks underpinning these systems include pattern recognition for biometrics, where minutiae extraction algorithms ensure matching accuracy (Ukamaka Bertrand et al., 2023; Rahman et al., 2023). GPS relies on trilateration and satellite positioning theories (Elbehriy, 2019). Multi-factor authentication theory minimizes false acceptance/rejection rates (Hooi et al., 2018; Simukali et al., 2019). IoT paradigms facilitate data interoperability (Moshayedi et al., 2021; Rahkoyo et al., 2024). Ethical theories address digital transformation's impact on employee protection and privacy (Jiang & Jiang, 2025; Naseri et al., 2019). Performance measurement models link attendance accuracy to organizational outcomes (Yuan et al., 2015; Ibrahim Jalo et al., 2023).

Overview of Relevant Technologies

The successful implementation of a GPS-Based Fingerprint Attendance Management System depends on the integration of several hardware and software technologies that work together to provide secure, reliable, and efficient attendance monitoring. These technologies include biometric devices, geolocation systems, mobile applications, cloud computing platforms, Internet of Things (IoT) technologies, Artificial Intelligence (AI), and wireless communication technologies.

- **Fingerprint Recognition Technology:** Fingerprint recognition technology is one of the most widely used biometric authentication methods in modern attendance management systems. Fingerprints consist of unique ridge patterns and minutiae points that differ from one individual to another. Because of their uniqueness and permanence, fingerprints provide a reliable means of identifying and verifying individuals. Fingerprint scanners are generally categorized into capacitive and optical scanners. Capacitive fingerprint scanners use electrical currents to detect fingerprint patterns and are known for their high accuracy and resistance to spoofing attacks. Optical fingerprint scanners capture fingerprint images using light sensors and image processing techniques. These devices are commonly integrated into attendance systems to ensure that only authorized individuals can register attendance. The use of fingerprint authentication significantly reduces cases of impersonation, proxy attendance, and identity fraud within organizations (Vinay et al., 2023).
- **Global Positioning System (GPS) Technology:** The Global Positioning System (GPS) is a satellite-based navigation technology that enables the determination of precise geographical locations anywhere on the Earth's surface. GPS operates through a network of satellites that continuously transmit signals to GPS-enabled devices such as smartphones, tablets, and GPS modules. In attendance management systems, GPS technology plays a crucial role in validating the physical location of users during attendance registration. By capturing the geographical coordinates of staff members at the point of attendance, the system can verify whether they are within authorized locations. This functionality helps prevent location-based attendance fraud and ensures accountability among employees, especially those working in multiple locations or remote environments (Nagothu et al., 2016).
- **Mobile Application Technology:** Mobile applications provide a convenient platform for implementing attendance management systems. Modern smartphones are equipped with built-in biometric sensors, GPS receivers, internet connectivity, and processing capabilities, making them suitable devices for attendance monitoring. The proposed system utilizes Android and iOS mobile applications to facilitate attendance registration and monitoring. These applications interact with device hardware through Application Programming Interfaces (APIs), which enable access to fingerprint sensors, GPS modules, cameras, and other system resources. Mobile applications provide flexibility, ease of use, and real-time access to attendance information, making them ideal for modern workforce management solutions (Nurli et al., 2022).
- **Application Programming Interfaces (APIs):** Application Programming Interfaces (APIs) serve as communication bridges between software applications and hardware components. APIs allow developers to access device functionalities without directly interacting with the underlying hardware. In a GPS-Based Fingerprint Attendance Management System, biometric APIs facilitate fingerprint enrollment and

authentication processes, while location APIs provide access to GPS coordinates. APIs also support communication with databases, cloud services, and external applications. The integration of APIs enhances system functionality, interoperability, and scalability (Prasada & Ikrimach, 2024).

- **Internet of Things (IoT) Technology:** The Internet of Things (IoT) refers to a network of interconnected devices that collect, exchange, and process data through the internet. IoT technologies enable seamless communication between attendance devices, servers, databases, and management dashboards. In the proposed system, IoT architecture facilitates real-time attendance monitoring and data synchronization. Fingerprint scanners, GPS-enabled devices, and cloud servers communicate continuously to ensure accurate and up-to-date attendance records. IoT technology enhances automation, reduces manual intervention, and improves system responsiveness (Santoso & Sari, 2019).

SYSTEM ARCHITECTURE

The architecture of the proposed GPS-Enabled Fingerprint Attendance System is designed to provide a secure, reliable, and efficient platform for staff attendance monitoring at Federal Polytechnic Damaturu. The system adopts a client-server architecture that integrates biometric fingerprint authentication, GPS location verification, application processing, and database management into a unified framework. This architecture ensures that attendance records are captured only when a registered staff member successfully verifies their identity through fingerprint recognition and is physically present within the authorized geographical location of the institution.

The system consists of four major components: the client layer, application layer, database layer, and administrative layer. The client layer serves as the interface through which staff members interact with the system using a mobile device, biometric scanner, or web application. At this level, users submit attendance requests by providing fingerprint credentials, while the GPS module automatically captures the user's geographical coordinates. This combination of biometric and location data enhances the authenticity of attendance records and reduces the possibility of fraudulent attendance practices.

The application layer acts as the core processing unit of the system. It receives attendance requests from users and performs fingerprint matching, GPS validation, authentication, attendance processing, and report generation. The fingerprint verification module compares the captured fingerprint against stored biometric templates to confirm the identity. Simultaneously, the GPS validation module verifies that the user is within the predefined geographical boundary before attendance is approved. This dual-verification mechanism significantly improves the accuracy and integrity of attendance monitoring systems.

The database layer provides centralized storage for all system information, including staff biodata, fingerprint templates, attendance records, GPS coordinates, login credentials, and audit logs. The use of a centralized database enhances data consistency, facilitates efficient retrieval of records, and supports the generation of real-time attendance reports. Furthermore, database security mechanisms such as encryption, backup procedures, and access controls help protect sensitive biometric and attendance information from unauthorized access.

The administrative layer enables authorized personnel to manage and monitor attendance activities. Through an administrative dashboard, system administrators can register a member, view attendance records, generate reports, track punctuality, and manage user accounts. This layer provides management with real-time access to attendance information, thereby supporting informed decision-making and effective staff supervision. The availability of automated reports also reduces administrative workload and improves operational efficiency.

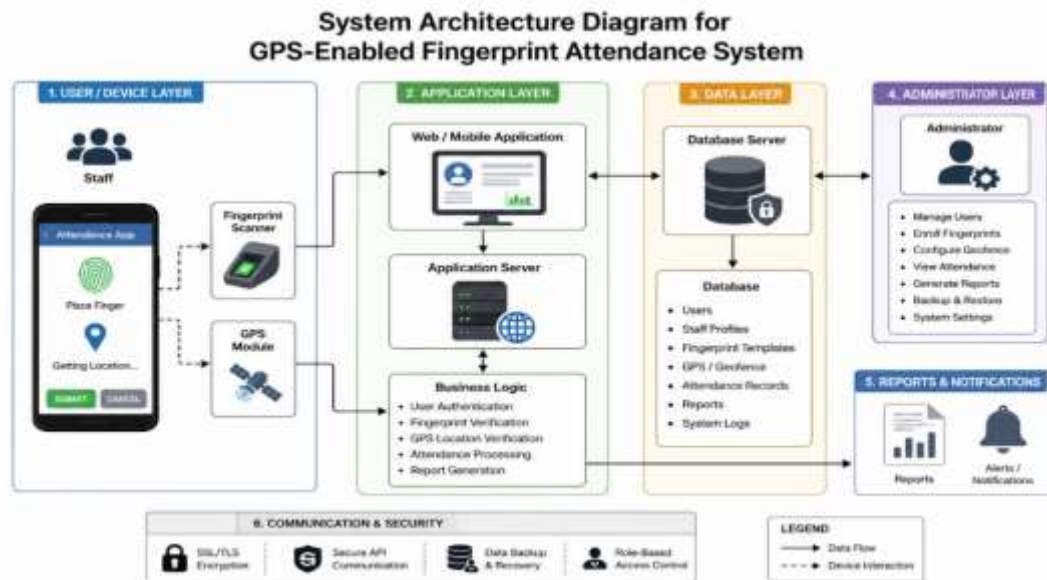


Figure 1: System Architecture Diagram

The System Architecture Diagram illustrates the overall structure and operation of the GPS-Enabled Fingerprint Attendance System for Enhanced Staff Monitoring. It shows how staff use a mobile application or attendance device integrated with a fingerprint scanner and GPS module to register attendance. The application server authenticates the user's fingerprint, verifies the GPS location against the predefined geofence, and processes the attendance request before storing the information securely in the database. The administrator manages users, enrolls fingerprints, configures geofence settings, monitors attendance records, generates reports, and performs database backup and system maintenance. The architecture also incorporates security mechanisms such as secure communication, role-based access control, and database backup to ensure the confidentiality, integrity, and availability of attendance data, thereby providing a secure, accurate, and efficient attendance management system.

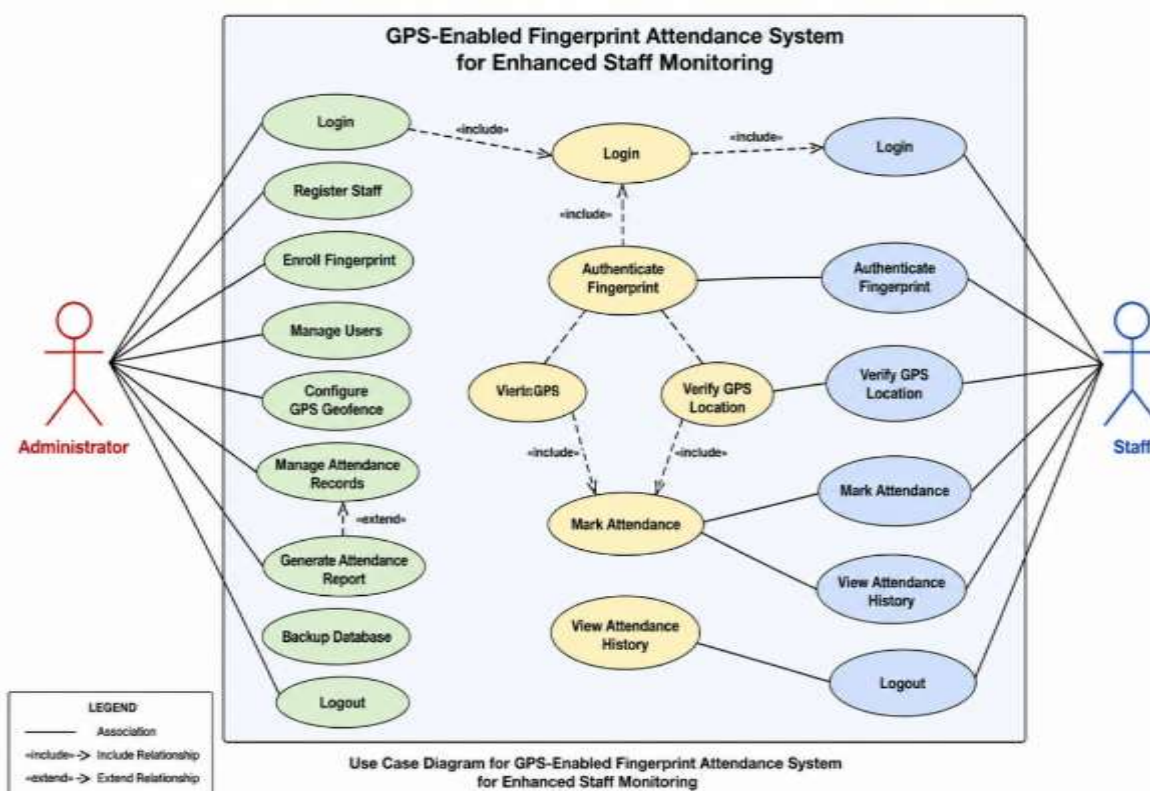


Figure 2: Use Case Diagram

Overall, the use case diagram demonstrates that the proposed system integrates biometric fingerprint authentication with GPS location verification to provide a secure, reliable, and fraud-resistant attendance management solution. It clearly defines the responsibilities of both administrators and staff while illustrating the interaction between users and the system to achieve efficient attendance monitoring. The Use Case Diagram provides a clear overview of the system's functionality, making it easier for developers and stakeholders to understand user interactions and system boundaries before implementation.

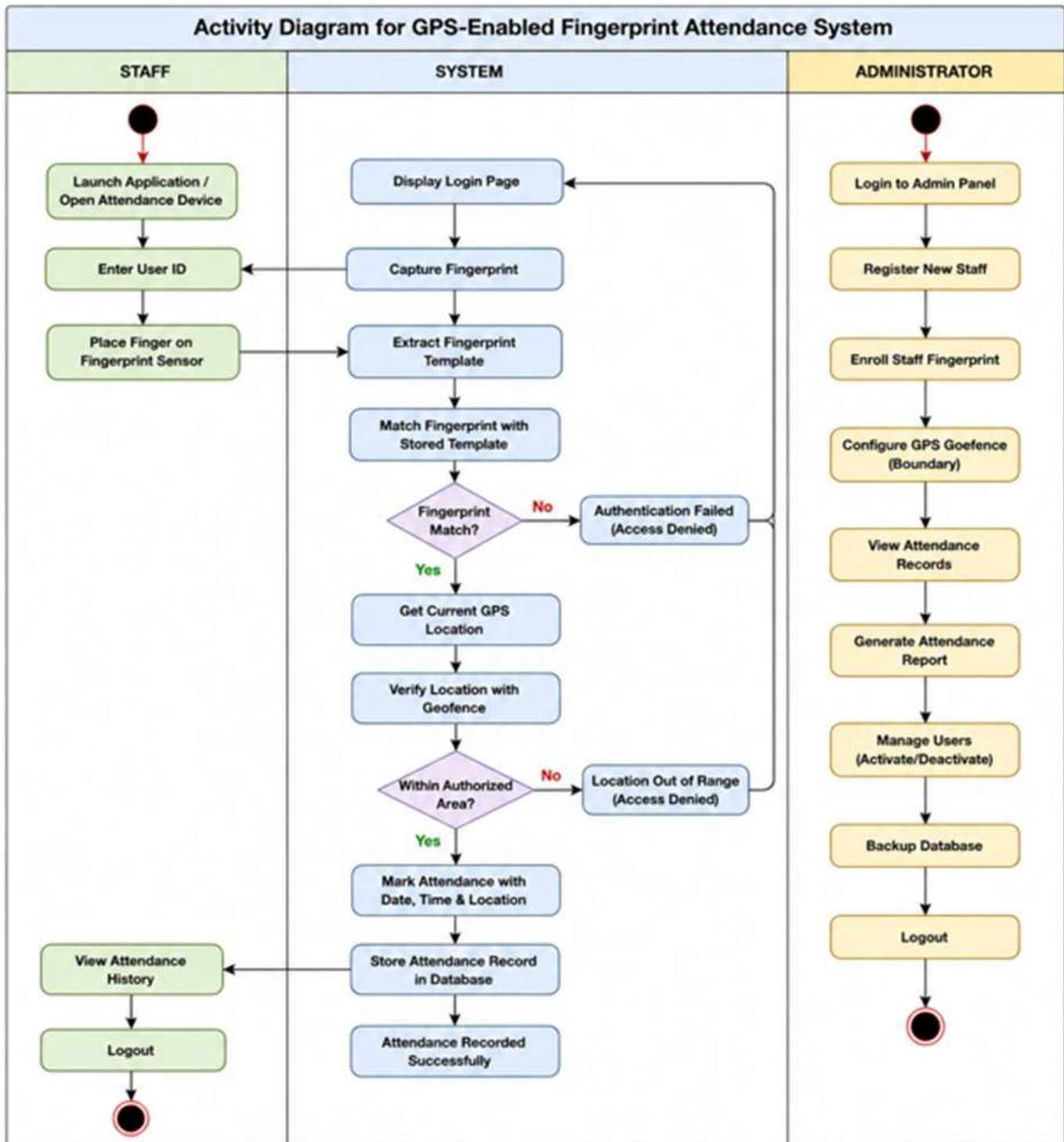


Figure 3: Activity diagram

The activity diagram demonstrates that the proposed system combines fingerprint authentication with GPS location verification before attendance is recorded. This dual verification mechanism helps eliminate proxy attendance, prevents location-based fraud, enhances security, and ensures that only authorized staff members

who are physically present within the designated area can successfully register their attendance. This workflow improves the accuracy, reliability, and efficiency of staff attendance monitoring.

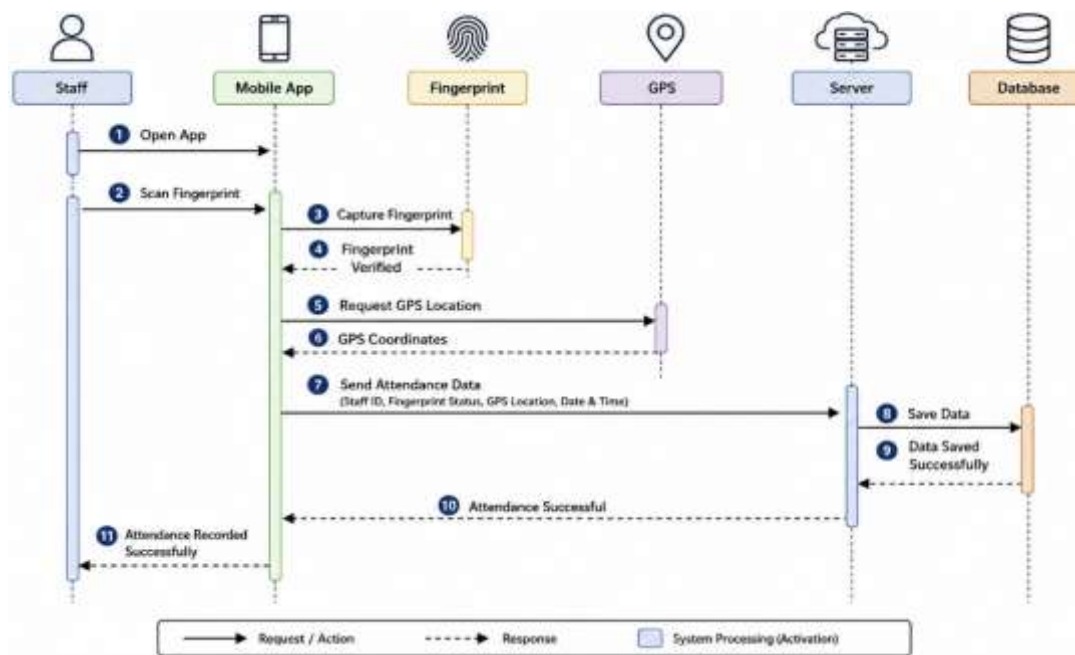


Figure 4: Sequence Diagram

The process begins when the staff member logs into the attendance application and scans their fingerprint. The system verifies the fingerprint using the database. If the fingerprint is valid, the system checks the staff member's GPS location to confirm they are within the authorized attendance area. When both the fingerprint and GPS location are successfully verified, the system records the attendance with the date, time, and location and stores it in the database. A confirmation message is then displayed to the staff member. If either the fingerprint authentication or GPS verification fails, the system denies attendance and displays an error message. The sequence diagram illustrates how the system securely records attendance through fingerprint authentication and GPS location verification, ensuring accurate and reliable staff attendance monitoring.

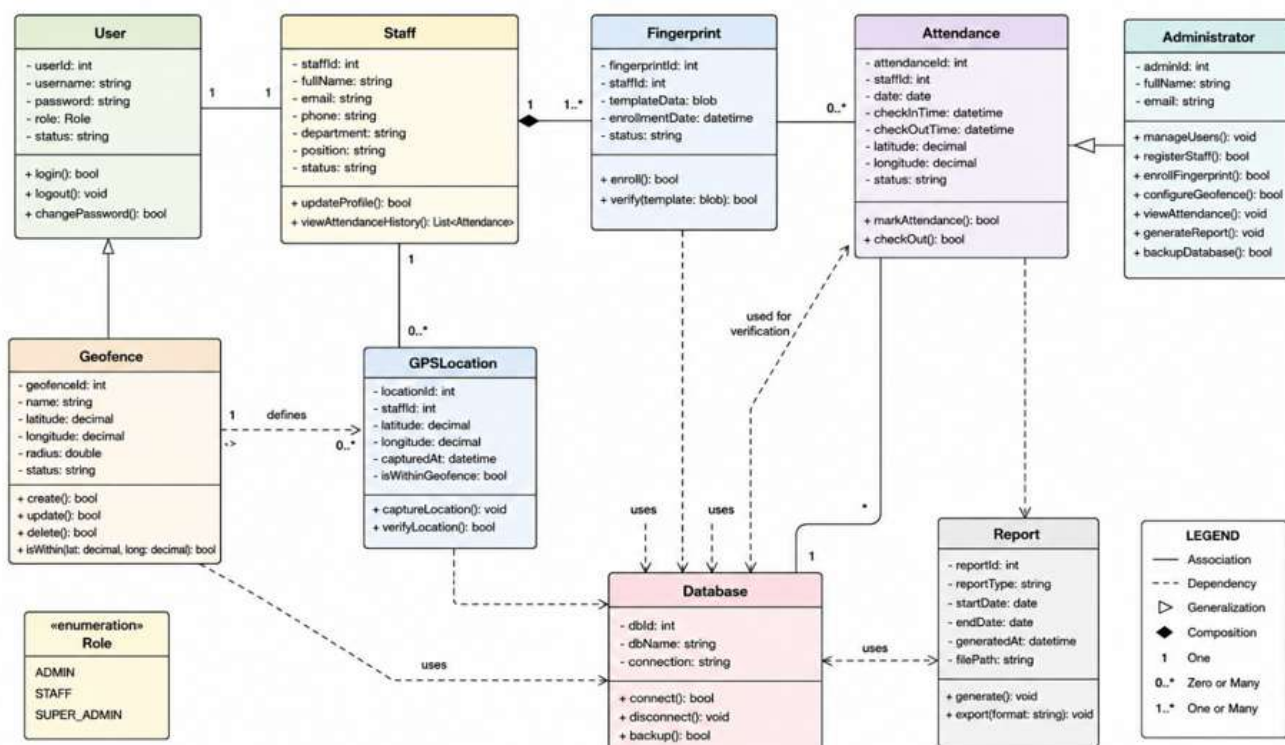


Figure 5: UML Class Diagram



The UML Class Diagram represents the static structure of the GPS-Enabled Fingerprint Attendance System for Enhanced Staff Monitoring. It shows the main classes, their attributes, methods, and the relationships between them. The diagram consists of classes such as User, Staff, Administrator, Fingerprint, Attendance, GPS Location, Geofence, Database, and Report. The Staff class stores staff information and is linked to the Fingerprint class for biometric authentication. The GPS Location and Geofence classes verify that staff members are within the authorized attendance area before attendance is recorded.

The Attendance class stores attendance details, including the date, time, and GPS coordinates, while the Database class manages the storage and retrieval of all system data. The Administrator class is responsible for registering staff, enrolling fingerprints, managing users, configuring geofences, generating reports, and backing up the database. The Report class generates attendance reports for monitoring and decision making. Overall, the UML class diagram demonstrates how the different components of the system work together to provide a secure, accurate, and efficient staff attendance management system using fingerprint authentication and GPS location verification.

Development Environment

The prototype was implemented in an integrated hardware and software environment capable of supporting fingerprint authentication, GPS location services, database operations, and web-based application development. The technologies were selected to provide a manageable environment for developing and testing the prototype. The implementation used Python with the Flask framework for the backend application logic, React and standard web technologies for the frontend interface, and MySQL Server for relational data storage. A digital fingerprint scanner was used for biometric input, while the device Location API supplied GPS coordinates for geofence validation. The prototype was developed and tested on a Windows 11 computer using Visual Studio Code, with Git used for version control.

The prototype application was developed using Python and the Flask framework for server-side processing and application programming interfaces. The frontend interface was implemented with React, HTML5, CSS3, JavaScript, and Bootstrap to provide an interactive web interface. MySQL Server 8.0 was used as the relational database for staff records, biometric templates, attendance records, GPS coordinates, user credentials, and audit information. The prototype was developed and tested on a Windows 11 (64-bit) computer using Visual Studio Code. A digital fingerprint scanner supplied biometric input, while the device Location API supplied geographical coordinates for location verification.

Table 2: Development Environment

Component	Specification
Operating System	Microsoft Windows 11 (64-bit)
Programming Language	Python 3.x
Database Management System	MySQL Server 8.0
Development IDE	Visual Studio Code
Backend Framework	Flask
Frontend Technologies	React, HTML5, CSS3, JavaScript, Bootstrap
Database Connector	Python MySQL connector / database interface
Browser	Google Chrome / Microsoft Edge
GPS Interface	Device Location API
Fingerprint Device	Digital Fingerprint Scanner
Version Control	Git
Report Generation	PDF and Excel Export Libraries

The implementation environment supports seamless communication between the client application, biometric device, GPS module, application server, and relational database. The modular nature of the selected technologies



simplifies software maintenance and future upgrades.

System Testing

System testing was conducted to verify that the proposed GPS-Based Fingerprint Attendance Management Software satisfies the functional and non-functional requirements specified during the system analysis and design phase. The objective of the testing process was to ensure that all system modules operate correctly when integrated and that the software performs reliably under normal operating conditions.

The prototype was evaluated through scenario-based functional testing. Test scenarios were created to verify fingerprint authentication, GPS location verification, user authentication, attendance recording, report generation, and database operations. Individual modules were first checked separately and were subsequently tested as an integrated prototype. The evaluation therefore focused on verifying whether the implemented functions produced the intended outcomes under the defined prototype test scenarios.

The testing methodology consisted primarily of unit testing, integration testing, and functional system testing of the prototype. Unit testing was used to check individual software functions, while integration testing examined communication among the biometric input, location service, application server, and database. Functional system testing assessed the complete prototype workflow. The work does not claim a formal institutional User Acceptance Testing study because participant numbers, procedures, acceptance criteria, and UAT results were not documented in the manuscript.

Functional testing

Functional testing was performed to determine whether each software function operated according to the system requirements. Each function was executed using predefined input values, and the corresponding outputs were compared with the expected results. The testing demonstrated that the fingerprint authentication module successfully identified registered staff members while rejecting unauthorized users. The GPS verification module correctly validated users located within the approved attendance zone and rejected attendance attempts originating from outside the authorized geographical boundary. Attendance records were successfully stored in the database, and administrative reports were generated accurately.

Performance Evaluation

Performance evaluation was conducted to assess the efficiency, responsiveness, scalability, and reliability of the proposed attendance management system under simulated operating conditions. The evaluation focused on response time, processing speed, database retrieval efficiency, and concurrent user access. The results indicate that the system responded promptly during attendance registration. Fingerprint authentication and GPS verification were completed within a few seconds, while database transactions and report generation were executed efficiently. The modular software architecture contributed to improved system performance by minimizing unnecessary processing overhead. The system was also evaluated under multiple-user simulation, where several staff members attempted attendance registration simultaneously. The application maintained stable performance without data loss or processing failures.

Security Evaluation

Security evaluation was performed to determine the system's ability to protect sensitive attendance information, biometric templates, user credentials, and GPS location data from unauthorized access and manipulation. Several security mechanisms were incorporated into the proposed system. Passwords are stored using secure hashing techniques, thereby preventing plaintext password exposure. Fingerprint templates are stored as encrypted biometric data rather than raw fingerprint images, reducing the risk of biometric information leakage. User authentication is enforced before access is granted to administrative functions, while role-based access control ensures that users can access only functions appropriate to their responsibilities. The GPS validation mechanism further strengthens security by preventing attendance registration outside authorized institutional boundaries. Audit logs record user activities, enabling administrators to monitor system usage and investigate suspicious activities when necessary. Simulation testing also considered common security threats such as proxy attendance,



unauthorized login attempts, GPS spoofing, and database manipulation. The proposed system successfully detected and prevented these simulated attacks.

RESULT AND DISCUSSION

The implementation and functional evaluation of the prototype demonstrate the operation of an attendance workflow that combines fingerprint authentication with GPS location verification. In the prototype, an attendance record is accepted only after the registered user's identity is successfully verified and the reported location satisfies the configured geofence condition. This provides a practical demonstration of dual verification at the prototype level. Prototype test scenarios demonstrated that invalid fingerprint authentication and attendance attempts outside the configured geofence were rejected. The prototype therefore demonstrates mechanisms intended to reduce proxy attendance, impersonation, and off-site attendance registration. Automated recording and report generation also demonstrate the potential to reduce manual attendance-processing activities. These observations are limited to the implemented prototype and its test scenarios.

The database implementation efficiently stored attendance records, biometric templates, and GPS coordinates while maintaining data integrity and security. Report generation was completed accurately and within acceptable processing times, enabling administrators to monitor staff attendance and generate daily, weekly, and monthly attendance summaries with minimal effort. Overall, the functional evaluation indicates that the prototype implements its core objectives: biometric identity verification, GPS/geofence validation, attendance recording, administrative monitoring, and report generation. Its modular structure provides a basis for future enhancement, including cloud deployment, dedicated mobile applications, expanded analytics, and additional biometric modalities. The results should be interpreted as evidence of prototype functionality rather than as a full operational, scalability, or field-deployment evaluation.

CONCLUSION

This study focused on the prototype implementation of a GPS-enabled fingerprint attendance system for improved staff attendance monitoring. The prototype combines fingerprint authentication with GPS and geofencing to provide additional verification of staff attendance. Functional testing showed that the major components of the prototype could perform their intended attendance verification and record-keeping functions. The system also provides basic administrative features for monitoring attendance records and generating reports. However, the study was limited to prototype-level implementation and testing and does not claim full institutional deployment or large-scale performance validation. Further work should involve real-world deployment and quantitative evaluation of biometric accuracy, response time, and overall system performance.

REFERENCES

1. Abd El-Mawla, M. A., Ahmed, S. A., & Hassan, M. H. (2022). *Hybrid biometric attendance system using QR code, fingerprint and facial recognition*. *International Journal of Computer Applications*, 184(27), 15–24.
2. Ali, M. A., Ibrahim, A. M., & Yusuf, M. I. (2022). Smart attendance management system for higher institutions using biometric authentication. *International Journal of Advanced Computer Science and Applications*, 13(8), 210–220.
3. Alshamrani, A., Alqahtani, F., & Alotaibi, S. (2023). Intelligent attendance management systems: A systematic literature review. *IEEE Access*, 11, 84215–84237.
4. Ardianto, S., Subroto, I. M. I., & Haviana, S. F. C. (2022). Mobile employee attendance using geolocation and biometric verification. *TRANSISTOR Elektro dan Informatika*, 4(3), 145–156.
5. Bharathy, S., Kumar, P., & Rajesh, K. (2022). IoT-enabled biometric attendance monitoring for educational institutions. *Journal of Ambient Intelligence and Humanized Computing*, 13(9), 4511–4525.
6. Bourne, M., Franco-Santos, M., & Wilkesman, A. (2022). Performance measurement and workforce accountability in organizations. *International Journal of Productivity and Performance Management*, 71(5), 1452–1471.
7. Chauhan, A., Singh, R., & Patel, V. (2024). Employee attendance monitoring using face recognition and geofencing. *International Journal of Computer Applications*, 186(8), 12–21.



8. Darojah, N., Rahman, F., & Putra, Y. (2025). GPS-based attendance management using AppSheet and biometric authentication. *Journal of Information Systems Engineering*, 10(1), 44–59.
9. Habibah, E. U., & Sumarno, S. (2022). Attendance information system utilizing Global Positioning System (GPS) using AppSheet application. *Indonesian Journal of Innovation Studies*, 20. <https://doi.org/10.21070/ijins.v20i.737>
10. Jain, A. K., Ross, A., & Nandakumar, K. (2022). *Introduction to biometrics* (2nd ed.). Springer.
11. Jiang, Y., & Jiang, H. (2025). Intelligent employee attendance monitoring using cloud-enabled biometric systems. *IEEE Access*, 13, 11254–11273.
12. Juang, T. T. Y., Lin, C. Y., Chiang, T. W., Yang, C. Y., Chiou, G. J., Lin, F. Y. S., Lin, Y. N., & Shen, V. R. L. (2022). Development and evaluation of an attendance tracking system using smartphones with GPS and NFC. *Applied Artificial Intelligence*, 36(1), Article 2083796. <https://doi.org/10.1080/08839514.2022.2083796>
13. Khan, M. A., Khan, S. U., & Ahmad, F. (2022). Secure biometric attendance systems using cloud computing and Internet of Things. *Journal of Information Security and Applications*, 65, 103091.
14. Laudon, K. C., & Laudon, J. P. (2022). *Management information systems: Managing the digital firm* (17th Ed.). Pearson.
15. Memane, P., Patil, S., & Kulkarni, A. (2022). Fingerprint authentication framework for smart attendance systems. *International Journal of Computer Engineering and Technology*, 13(4), 201–214.
16. Moshayedi, A. J., Roy, A. S., Lan, H., Gheisari, M., Abbasi, A., Liao, L., & Bamakan, S. M. H. (2022). Automation attendance systems approaches: A practical review. *BOHR International Journal of Internet of Things, Artificial Intelligence and Machine Learning*, 1(1), 25–34. <https://doi.org/10.54646/bijiam.2022.05>
17. Naseri, M., Hosseini, S., & Ghasemi, M. (2024). GPS-based attendance verification and location-aware authentication systems: A review. *Sensors*, 24(5), 2217.
18. Nurtjahjani, F., Pribadi, J., Batubulan, K. S., & Shoumi, M. N. (2022). Real-time fingerprint-based employee attendance system using the Rapid Application Development method. *Jurnal Sistem Informasi Bisnis*, 12(1), 1–9. <https://doi.org/10.21456/vol12iss1pp1-9>
19. Olasupo, A. O., Ademiluyi, O. S., Usman, M. A., Abdullah, K. K. A., Olubanwo, O. O., Ayo, F. E., Ojumadu, U. H., Salami, E. O., & Ibironke, T. E. (2022). A fingerprint based students' attendance management system for Olabisi Onabanjo University. *FUDMA Journal of Sciences*, 6(1), 253–265. <https://doi.org/10.33003/fjs-2022-0601-896>
20. Prasada, M., & Ikrimach, A. (2024). Mobile attendance application using GPS geofencing and facial recognition. *Journal of Mobile Computing Research*, 12(2), 66–81.
21. Rahman, M., Ahmed, S., & Karim, R. (2023). Arduino-based fingerprint attendance system with cloud storage. *International Journal of Engineering Research and Technology*, 12(5), 101–110.
22. Roy, A. S., Lan, H., Gheisari, M., Abbasi, A., Liao, L., & Bamakan, S. M. H. (2022). Automation attendance systems approaches: A practical review. *BOHR International Journal of Internet of Things, Artificial Intelligence and Machine Learning*, 1(1), 25–34. <https://doi.org/10.54646/bijiam.2022.05>
23. Saraswat, P., Sharma, R., & Singh, N. (2022). Modern attendance management systems: Technologies, challenges and future directions. *International Journal of Information Systems and Computer Science*, 14(3), 87–101.
24. Ussher-Eke, M., Okafor, C., & Ibrahim, M. (2025). Biometric authentication technologies for workforce monitoring in developing countries. *International Journal of Information Management Data Insights*, 5(1), 100312.
25. Vinay, R., Kumar, P., & Reddy, S. (2023). Smart attendance system integrating fingerprint authentication and GPS location tracking. *International Journal of Intelligent Systems and Applications*, 15(4), 98–112.