Journal of Applied Informatics and Computing (JAIC)
Vol.10, No.4, August 2026, pp. 3761~3774
e-ISSN: 2548-6861

Sequential Multi-Factor Authentication for Attendance Using LBPH and Geolocation

Fitrada Kurnialdi Assrofi Ulla [1]*, Aris Tri Jaka Harjanta [2]*, Bambang Agus Herlambang [3]*
* Informatika, Universitas PGRI Semarang
assrofi.kurnialdi12@gmail.com[1], aristrijaka@upgris.ac.id [2], bambangherlambang@upgris.ac.id [3]

Article Info

Article history:

Received 2026-07-09
Revised 2026-07-27
Accepted 2026-08-11

Keyword:

Attendance System,
Face Recognition,
Geofencing,
Local Binary Pattern Histogram,
Sequential Multi-Factor Authentication.

ABSTRACT

Conventional attendance systems remain vulnerable to proxy attendance, location manipulation, and inefficient administrative processes, while many existing intelligent attendance solutions rely on computationally intensive deep learning models that are less suitable for lightweight web-based implementations. This study addresses these limitations by proposing a web-based smart attendance system integrating GPS-based geofencing and Local Binary Pattern Histogram (LBPH) within a Sequential Multi-Factor Authentication (MFA) framework. The proposed framework also incorporates GPS spoofing detection based on abnormal geolocation properties and IP geolocation consistency to improve resistance against location manipulation. The authentication mechanism performs geofencing validation before facial verification to improve security and avoid unnecessary biometric processing. The system was developed using the Laravel framework integrated with Python-based facial recognition and evaluated through black-box functional testing. Experimental evaluation involving 120 attendance scenarios achieved an overall accuracy of 96.67% while effectively detecting GPS spoofing and presentation attacks with low false acceptance and false rejection rates. The implementation results demonstrated that all major functional modules operated according to the predefined requirements, while the confidence threshold of 40 provided reliable facial verification under moderate environmental variations. These findings indicate that the proposed framework provides a practical, secure, and lightweight solution for web-based attendance management and offers an effective alternative to computationally intensive deep learning-based attendance systems.

I. INTRODUCTION

The rapid advancement of information technology has accelerated digital transformation across various sectors, including attendance management in educational institutions and organizations. Conventional attendance methods based on paper records, signatures, or identity cards are increasingly considered inefficient because they are vulnerable to human error, proxy attendance, data manipulation, and time-consuming administrative processes [1], [2], [3], [4], [5]. To overcome these limitations, modern attendance systems have adopted biometric technologies capable of automatically verifying user identities with higher accuracy and reliability. Among these technologies, facial recognition has attracted significant attention due to its contactless nature, ease of use, and capability to perform real-time authentication. Deep learning-based facial recognition can effectively automate attendance recording while improving identification accuracy and reducing manual intervention [4], [6], [7], [8]. Face recognition has become one of the most widely adopted biometric approaches in attendance systems because of its practicality and continuous technological advancement [9], [10], [11], [12].

In addition to biometric authentication, validating the physical location of users has become increasingly important to ensure that attendance is recorded only when individuals are present at authorized locations. Geolocation technologies such as GPS and geofencing establish virtual boundaries that restrict attendance activities to predefined areas, thereby reducing opportunities for fraudulent practices [13], [14], [15], [16], [17]. The integration of location-aware services into attendance systems has shown considerable potential in improving security and accountability while supporting remote and distributed working environments [18], [19], [20], [21]. Furthermore, advances in web technologies and agile software engineering practices have enabled developers to build scalable attendance applications that are easier to maintain and adapt to evolving user requirements [5], [22], [23], [24], [25].

Numerous studies have proposed intelligent attendance systems based on facial recognition using advanced machine learning and deep learning algorithms. Deep learning-based attendance system employing MTCNN and DeepFace models to automate classroom attendance with high recognition performance [6]. Optimized attendance monitoring through the integration of MTCNN, VGGFace, and Support Vector Machine classifiers, demonstrating effective multi-face recognition in real-time scenarios [22]. Other researchers have explored different architectures such as convolutional neural networks, FaceNet embeddings, and transfer learning techniques to improve recognition robustness under varying environmental conditions [24], [26], [27]. These developments indicate that facial recognition has become one of the most promising technologies for secure and efficient attendance management.

Beyond facial recognition, researchers have also investigated complementary security mechanisms to strengthen attendance authentication. Portable attendance system incorporating liveness detection to mitigate spoofing attacks against facial recognition models [24]. Improved FaceNet architecture based on MobileNetV2 to achieve lightweight and efficient facial recognition suitable for resource-constrained devices [3]. Other studies have integrated GPS, RFID, QR codes, and biometric authentication to provide multi-factor verification and reduce opportunities for attendance fraud [28], [29], [30]. These findings suggest that combining multiple authentication methods can significantly improve the reliability and security of attendance systems.

Despite the significant progress achieved by previous studies, several important research gaps remain. Deep learning-based attendance systems employing MTCNN, DeepFace, VGGFace, or FaceNet primarily focus on improving facial recognition accuracy but generally require high computational resources, making them less suitable for lightweight web deployment [6], [22], [24], [27]. Other attendance systems integrate GPS or geofencing to validate user location; however, location verification is typically implemented as an independent validation mechanism and does not provide protection against browser-based GPS spoofing or coordinate manipulation [7], [21]. Furthermore, previous studies generally evaluate either biometric authentication performance or location validation separately, while limited attention has been given to sequential authentication strategies that combine lightweight facial recognition, geofencing validation, and anti-spoofing mechanisms within a single web-based attendance framework. Therefore, there remains a need for a lightweight attendance system capable of integrating sequential multi-factor authentication, geofencing validation, and spoofing detection while maintaining practical deployment on resource-constrained web environments.

The primary contribution of this study is the integration of a lightweight Sequential Multi-Factor Authentication framework that combines geofencing validation, LBPH-based facial recognition, GPS spoofing detection, and comprehensive security evaluation against both location and presentation attacks.

Based on these identified research gaps, this study proposes a lightweight web-based attendance system that integrates Local Binary Pattern Histogram (LBPH), GPS-based geofencing, and a Sequential Multi-Factor Authentication framework. In contrast to previous studies, the proposed system not only performs sequential location and facial verification but also incorporates GPS spoofing detection based on abnormal geolocation properties and IP-based geolocation verification. Furthermore, the proposed approach is experimentally evaluated using genuine attendance scenarios as well as multiple attack scenarios, including printed-photo attacks, smartphone display attacks, and browser-based GPS spoofing, providing a more comprehensive security evaluation than previous lightweight attendance systems.

II. METHODOLOGY

This study employs the Research and Development (R&D) method with the Extreme Programming (XP) software development approach to design and develop a web-based attendance system integrating the Local Binary Pattern Histogram (LBPH) algorithm and geofencing technology. The research process consists of problem identification, requirements analysis, system design, implementation, testing, and functional evaluation using the black-box testing method. The XP approach was selected because it supports an iterative and flexible development process, enabling the system to adapt efficiently to changing requirements throughout the software development lifecycle.

A. Conceptual Framework

This study is motivated by the limitations of conventional attendance systems, which remain vulnerable to various forms of fraud, including proxy attendance, identity manipulation, and attendance recording from unauthorized locations. Furthermore, the use of a single authentication method has not provided an adequate level of security. Therefore, a mechanism is needed that can simultaneously verify the user's identity and confirm their physical presence within a designated area.

To address these issues, this study proposes the development of a web-based attendance system that integrates the Local Binary Pattern Histogram (LBPH) algorithm for facial recognition with geofencing technology for location validation. The system is developed using the Extreme Programming (XP) methodology, which supports an iterative and adaptive software development process, and is subsequently evaluated through black-box testing to ensure that all system functions operate as intended. The conceptual framework of this research is illustrated in Figure 1.

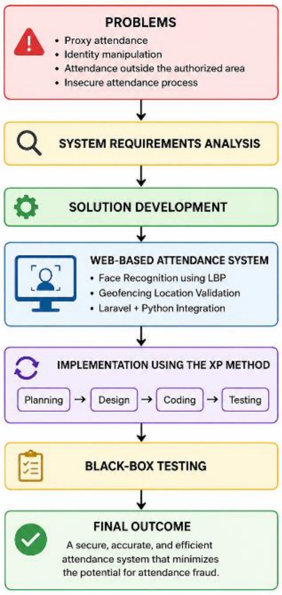

Figure 1. Stages of System Development Using the Extreme Programming (XP) Method

As illustrated in Figure 1, the research begins with the identification of problems commonly found in conventional attendance systems, such as proxy attendance, identity manipulation, attendance submissions from unauthorized locations, and the limitations of existing authentication mechanisms in ensuring the validity of attendance records. These issues form the basis for conducting a system requirements analysis to design a solution capable of improving the security and reliability of the attendance process.

Based on the results of the requirements analysis, a web-based attendance system is developed by integrating the Local Binary Pattern Histogram (LBPH) algorithm for facial recognition and geofencing technology for user location validation. The integration of these two technologies establishes a dual-authentication mechanism that ensures users are not only correctly identified but are also physically present within the designated attendance area. The system development process is then carried out using the Extreme Programming (XP) methodology, which consists of the planning, design, coding, and testing phases implemented iteratively.

In the final stage, the developed system is evaluated using the black-box testing method to verify that each function performs according to the specified requirements and system specifications. Through this conceptual framework, the study aims to produce a web-based attendance system that is more secure, accurate, efficient, and capable of minimizing fraudulent practices in attendance recording.

B. *Research Materials*

The development of the proposed attendance system is supported by a combination of software technologies and hardware components to enable secure and efficient attendance verification. The primary software framework used in this study is Laravel, which serves as the backbone of the web application by managing user authentication, business logic, database operations, and user interfaces. Facial recognition processing is implemented using Python with the OpenCV library, where the Local Binary Pattern Histogram (LBPH) algorithm is employed to extract facial features and perform identity verification. Data management is handled using MySQL, which stores user information, attendance records, and geofencing configurations.

In addition to the software environment, the system relies on standard hardware resources available on user devices. A digital camera or webcam is used to capture facial images during the attendance process, while the device's GPS or browser-based geolocation service provides real-time coordinate information for location verification. The attendance system applies a dual-authentication mechanism, requiring successful validation of both facial identity through the LBPH algorithm and user location through geofencing before attendance is recorded. This integration enhances the reliability and security of the attendance process while maintaining a lightweight implementation suitable for web-based deployment.

For clarity, the main research materials and technologies used in this study are summarized in Table 1.

TABLE I
RESEARCH MATERIALS AND TECHNOLOGIES USED IN THE PROPOSED SYSTEM

Component	Technology	Function
Web Framework	Laravel	Develops the web application, manages business logic, and handles database interactions
Programming Language	PHP	Implements the backend functionality within the Laravel framework
Face Recognition Module	Python with OpenCV	Processes facial images and performs feature extraction

Face Recognition Algorithm	Local Binary Pattern Histogram (LBPH)	Extracts facial texture features and verifies user identity
Database Management System	MySQL	Stores user profiles, attendance records, and system configurations
Location Verification	Geofencing with GPS	Validates whether users are within the authorized attendance area
Image Acquisition	Webcam or Device Camera	Captures facial images during attendance
Development Method	Extreme Programming (XP)	Guides the iterative software development process
Testing Method	Black-box Testing	Evaluates system functionality based on expected outputs

As presented in Table 1, the proposed attendance system integrates multiple software and hardware components to establish a secure and efficient attendance verification mechanism. Laravel functions as the primary web framework responsible for handling business logic, user authentication, and database management, while Python and the OpenCV library are dedicated to image processing and facial recognition tasks. The Local Binary Pattern Histogram (LBPH) algorithm is employed to extract facial texture features and compare them with registered templates for identity verification. In parallel, the geofencing module utilizes GPS coordinates to determine whether users are located within the predefined attendance area before allowing the attendance process to proceed. Attendance records, user information, and system configurations are stored in a MySQL database to ensure data consistency and accessibility. The overall development process follows the Extreme Programming (XP) methodology, enabling iterative refinement and rapid adaptation to system requirements, whereas functional validation is conducted through black-box testing to verify that each module operates according to its intended specifications. The integration of these technologies provides a lightweight, web-based dual-authentication system capable of enhancing both the security and reliability of attendance management.

C. System Development Method

This study employs the Extreme Programming (XP) methodology as the software development approach for designing and implementing the proposed web-based attendance system. XP is an Agile software development methodology that emphasizes iterative development, continuous feedback, close collaboration, and rapid adaptation to changing requirements. It was selected for this research because it enables efficient system development while maintaining flexibility throughout the implementation process.

In general, the XP methodology consists of four primary phases: Planning, Design, Coding, and Testing. These phases are performed iteratively, allowing the system to be continuously refined and improved until it satisfies the specified functional requirements. The overall development process adopted in this study is illustrated in Figure 2.

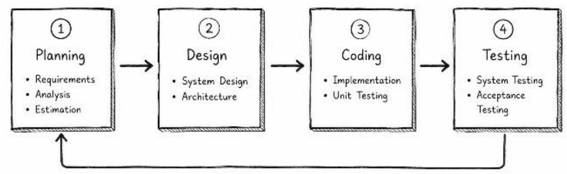

Figure 2. System development stages using the Extreme Programming (XP) methods

1) *Planning*: The planning phase focuses on identifying both the functional and non-functional requirements of the attendance system. During this stage, the core functionalities are defined, including user registration, facial image acquisition, location validation through geofencing, attendance recording, and attendance history management. In addition, the software technologies and development tools are selected, including Laravel as the web framework, Python for image processing, the Local Binary Pattern Histogram (LBPH) algorithm for facial recognition, and MySQL as the database management system.

2) *Design:* The design phase involves creating the overall architecture of the proposed system and defining the interactions among its components. This includes designing the database structure, user interface, system workflow, and communication mechanism between the Laravel-based web application and the Python-based facial recognition module. The dual-authentication mechanism, which combines facial verification and geofencing validation, is also established during this stage.

3) *Coding:* During the coding phase, the designed architecture is implemented into a functional application. The web-based platform is developed using the Laravel framework with PHP, while Python and the OpenCV library are utilized to implement facial recognition based on the Local Binary Pattern Histogram (LBPH) algorithm. The geofencing functionality is integrated into the application to validate the user's geographic location before the facial recognition process is executed. The integration of these technologies enables seamless communication between system modules and supports secure attendance verification.

4) *Testing:* The final phase consists of testing the developed system to ensure that all functionalities operate according to the specified requirements. The evaluation is conducted using black-box testing, where system outputs are verified based on predefined input scenarios without

examining the internal source code. The testing process covers user registration, geofencing validation, facial recognition, attendance recording, and database storage. Through this approach, the reliability of the dual-authentication mechanism and the overall functionality of the attendance system can be effectively validated.

Overall, the implementation of the Extreme Programming (XP) methodology provides a structured yet flexible development process that facilitates iterative refinement and continuous improvement. By integrating Laravel, Python, Local Binary Pattern Histogram (LBPH), and geofencing technologies within the XP framework, the proposed system is expected to deliver a secure, lightweight, and efficient web-based attendance solution.

D. System Architecture and Workflow

The proposed attendance system adopts a web-based architecture that integrates Laravel, Python, Local Binary Pattern Histogram (LBPH), and geofencing to establish a secure dual-authentication mechanism. Laravel serves as the primary framework responsible for handling user management, attendance records, business logic, and database interactions, while Python processes facial recognition tasks using the LBPH algorithm. The integration of these components enables the system to verify both the user's identity and physical location before recording attendance.

To provide a clearer understanding of the interaction among the system components, the overall architecture of the proposed attendance system is illustrated in Figure 3.

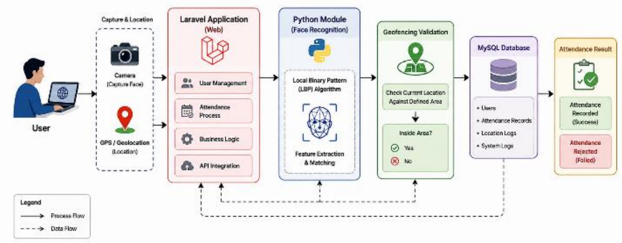

Figure 3. System Architecture of the Proposed Web-Based Attendance System

As shown in Figure 3, the attendance process begins when a user accesses the web application and grants permission to use the device's camera and location services. The camera captures the user's facial image, while the GPS or browser geolocation service retrieves the current coordinates. The captured facial image is then forwarded to the Python module, where the Local Binary Pattern Histogram (LBPH) algorithm extracts facial features and performs identity verification against the registered reference data. Simultaneously, the system validates the user's geographic position through the geofencing mechanism to determine whether the current location falls within the authorized attendance area.

Attendance is successfully recorded only when both authentication processes produce valid results. If the facial recognition process confirms the user's identity and the geofencing validation verifies that the user is located within the predefined boundary, the attendance information, including user identity, timestamp, and location data, is stored in the MySQL database. Conversely, if either authentication process fails, the attendance request is rejected, preventing unauthorized or fraudulent attendance submissions.

The operational workflow of the proposed system is further illustrated in Figure 4, which presents the sequence of activities performed during the attendance process.

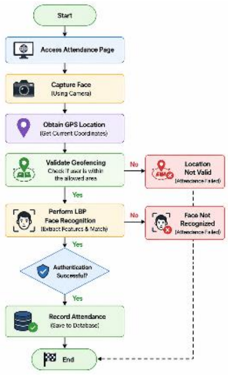

Figure 4. Workflow of the Dual-Authentication Attendance **Process**

The workflow shown in Figure 4 demonstrates that the proposed system implements a dual-authentication strategy by combining biometric verification and location validation before attendance is finalized. This approach enhances system security by minimizing opportunities for attendance fraud, such as proxy attendance or remote check-ins from unauthorized locations. Furthermore, the integration of lightweight LBPH-based facial recognition with geofencing provides an efficient and practical solution that can be deployed in web-based attendance environments without requiring computationally intensive deep learning models.

E. Implementation of Face Recognition and Geofencing

The proposed attendance system integrates two complementary authentication mechanisms, namely Local Binary Pattern Histogram (LBPH)-based facial recognition and geofencing-based location validation. This dual-authentication approach is designed to ensure that attendance can only be recorded when the user's identity has been successfully verified and the user is physically present within the designated attendance area. By combining biometric verification with location-based validation, the system enhances security and minimizes the risk of fraudulent attendance activities.

In general, the authentication process begins when the user accesses the web-based attendance application. The system requests permission to access the device's camera and location services. Once permission is granted, the camera captures the user's facial image while the geolocation service retrieves the current GPS coordinates. The integration of these two validation mechanisms is illustrated in Figure 5.

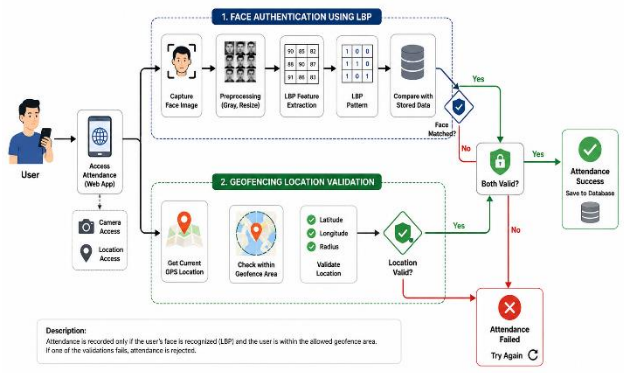

Figure 5. Dual-Authentication Implementation Process Using Local Binary Pattern Histogram (LBPH) and Geofencing

During the facial recognition stage, the captured image is processed using the Local Binary Pattern Histogram (LBPH) algorithm. LBPH extracts local texture features by comparing the intensity value of each pixel with those of its neighboring pixels, producing a binary representation that characterizes the facial pattern. The extracted features are then compared with the registered facial templates stored in the system database to determine the user's identity. LBPH was selected because of its computational efficiency, fast feature extraction capability, and suitability for lightweight web-based applications.

Following facial verification, the system performs geofencing-based location validation. In this stage, the GPS coordinates obtained from the user’s device are compared with the predefined attendance location and its permitted radius. The system determines whether the user is located within the authorized geographical boundary. If the user is outside the specified geofence, the attendance request is immediately rejected even if the facial recognition process is successful. Conversely, when the user is located within the permitted area, the authentication process proceeds to the final verification stage.

Attendance is recorded only when both authentication mechanisms, namely LBPH-based facial recognition and geofencing validation, produce successful results. Once these conditions are satisfied, the system stores the attendance information, including the user identity, timestamp, and location details, in the database. If either validation fails, the attendance transaction is rejected and no attendance record is created, requiring the user to repeat the verification process.

By integrating Local Binary Pattern Histogram (LBPH) with geofencing, the proposed system establishes a robust dual-authentication framework that verifies both user identity and physical presence. This approach provides a higher level of security than single-factor authentication systems while maintaining computational efficiency and ease of implementation. Consequently, the developed solution offers a practical, reliable, and secure web-based attendance mechanism suitable for modern organizational and educational environments.

F. System Testing and Evaluation

The developed attendance system was evaluated to verify that all implemented functionalities operated according to the specified requirements and produced the expected outputs. Since the primary objective of this study was to design and implement a functional web-based attendance application integrating Local Binary Pattern Histogram (LBPH) and geofencing, the evaluation focused on functional testing rather than comparative performance benchmarking. Therefore, the testing process employed the black-box testing approach, which validates system behavior based on input-output relationships without examining the internal source code.

Black-box testing was selected because it enables comprehensive verification of each system function from the end-user perspective. Every feature was tested by providing predefined input scenarios and observing whether the generated outputs matched the expected results. The evaluation covered essential modules of the attendance application, including user authentication, facial recognition, location validation, attendance recording, and database management. The testing scenarios used in this study are summarized in Table 2.

TABLE II
BLACK-BOX TESTING SCENARIOS

No.	System Function	Test Scenario	Expected Result
1	User Login	User enters valid credentials	User successfully accesses the system
2	Face Recognition	Registered face is captured by the camera	User identity is correctly recognized using LBPH
3	Geofencing Validation	User is located within the authorized area	Location validation is successful
4	Geofencing Validation	User is outside the authorized area	Attendance request is rejected
5	Dual Authentication	Face recognition and geofencing are both valid	Attendance is successfully recorded
6	Dual Authentication	One or both validations fail	Attendance is denied
7	Attendance Storage	Successful attendance submission	Attendance data are stored in the MySQL database
8	Attendance History	User accesses attendance records	Attendance history is displayed correctly

As presented in Table 2, the testing scenarios were designed to evaluate the interaction between facial recognition and geofencing within the proposed dual-authentication mechanism. Particular emphasis was placed on ensuring that attendance could only be recorded when both identity verification and location validation were successfully completed. This approach helps prevent unauthorized attendance attempts, including proxy attendance and check-ins performed outside the designated area.

The evaluation results indicated that the implemented functionalities operated as intended under the defined testing scenarios. The integration between the Laravel-based web application and the Python module enabled seamless communication during facial recognition, while the geofencing mechanism effectively verified the user's geographic position before attendance submission. The coordinated operation of these components supports a secure and efficient attendance process.

Overall, the black-box testing results demonstrate that the proposed system successfully implements the intended dual-authentication strategy by combining Local Binary Pattern Histogram (LBPH) and geofencing. The developed application satisfies its functional requirements and provides a practical solution for secure web-based attendance management, with an emphasis on reliability, usability, and fraud prevention.

III. RESULTS AND DISCUSSION

This section presents and discusses the implementation and evaluation results of the proposed web-based smart attendance system. The discussion begins with the implementation of the system and the integration of the Sequential Multi-Factor Authentication (MFA) mechanism, which combines GPS-based geofencing and Local Binary Pattern Histogram (LBPH) face recognition. Subsequently, the functional performance of the proposed system is evaluated through black-box testing, followed by a comparison with previous studies to highlight the contributions of the proposed approach. Finally, the limitations of the current study and potential directions for future research are discussed.

A. System Implementation and Sequential Multi-Factor Authentication

This section presents the implementation results of the proposed web-based smart attendance system developed using the Laravel framework integrated with Python-based Local Binary Pattern Histogram (LBPH) face recognition and GPS-based geofencing. The system adopts a Sequential Multi-Factor Authentication (MFA) mechanism, where each validation stage must be successfully completed before proceeding to the next authentication process. This sequential approach ensures that attendance records are accepted only when both the user's physical location and biometric identity satisfy the predefined requirements.

The developed attendance application provides an integrated environment for user authentication, biometric enrollment, attendance recording, attendance history, leave management, and profile administration. These modules support the implementation of the proposed Sequential Multi-Factor Authentication (MFA) framework while maintaining a lightweight web-based architecture. The main user interface is illustrated in Figure 6, which displays the dashboard after a successful login. The dashboard provides quick access to attendance activities, attendance history, leave requests, and user profile information, while also displaying the current attendance status and real-time system information.

Figure 6. User dashboard of the proposed web-based smart attendance system

As shown in Figure 6, the dashboard serves as the central interface for all attendance-related activities. Before performing attendance, the system verifies that the user's face has been registered. Users who have not completed the registration process are required to enroll their facial data before the attendance feature becomes available.

Figure 7. Single frontal face registration during user enrollment

To improve recognition consistency, the facial image is registered using a fixed frontal position. This controlled enrollment procedure minimizes variations during feature extraction and simplifies the registration process while maintaining reliable verification performance. After the facial image has been successfully captured, the image is transmitted to the server for preprocessing, face detection, feature extraction, and LBPH model generation. Each registered user has an individual facial model stored on the server, allowing personalized biometric verification during subsequent attendance sessions.

Following successful registration, the attendance process begins by activating the camera and retrieving the user's GPS coordinates. The implementation integrates the camera module, GPS service, and LBPH recognition module within a single attendance interface, as illustrated in Figure 8.

Figure 8. Attendance interface integrating camera, GPS, and Local Binary Pattern Histogram (LBPH) modules

As shown in Figure 8, the proposed attendance interface integrates three primary components required for the authentication process, namely the camera module, GPS-based geolocation service, and the Local Binary Pattern Histogram (LBPH) face recognition module. Before performing attendance, users who have not previously registered their facial data are required to complete the face enrollment process by capturing a single frontal facial image. The captured image is then processed to generate an individual LBPH facial model that serves as the biometric reference during subsequent attendance verification. The interface also provides a real-time visualization of the user's GPS position and the predefined geofencing boundary, allowing users to verify whether they are located within the authorized attendance area before initiating the attendance process.

The proposed attendance system adopts a Sequential Multi-Factor Authentication (MFA) mechanism in which authentication is performed through consecutive validation stages rather than simultaneously. The process begins with geofencing validation, where the user's GPS coordinates are compared with the predefined attendance location. Only users located within the authorized attendance radius are allowed to continue to the biometric verification stage. Subsequently, the captured facial image is processed using the Local Binary Pattern Histogram algorithm and compared with the registered facial model. The verification result is then evaluated using a predefined confidence threshold, where attendance is accepted only when the confidence value is less than or equal to 40. This sequential strategy reduces unnecessary biometric processing by executing facial verification only after successful geofencing validation.

During attendance verification, the server continuously calculates the distance between the user's GPS coordinates and the predefined office location. When the calculated distance exceeds the configured attendance radius, the system immediately terminates the authentication process and rejects the attendance request. An example of this validation result is presented in Figure 9, where the user attempts to perform attendance from a distance of 32 m, while the maximum permitted radius is 30 m.

Figure 9. Attendance rejection when the user is located outside the predefined geofencing radius

As presented in Figure 9, the proposed sequential authentication mechanism successfully prevents unauthorized attendance by rejecting users located outside the designated attendance area before executing the facial recognition module. This approach reduces unnecessary computational overhead while simultaneously minimizing the possibility of attendance fraud originating from unauthorized locations.

For users who successfully satisfy the geofencing requirement, the system proceeds with facial verification using the Local Binary Pattern Histogram algorithm. The algorithm compares the captured facial image with the registered facial model and produces a confidence score that represents the similarity between the two facial representations. Unlike probability-based classifiers, the confidence value in LBPH represents a distance metric, where values closer to zero indicate higher similarity between the captured image and the stored facial model. Accordingly, the proposed system defines a maximum acceptance threshold of 40, meaning that attendance is accepted only when the confidence value is ≤ 40, whereas higher values indicate insufficient similarity and result in attendance rejection.

The selected confidence threshold was determined by considering practical implementation conditions encountered during system deployment. Experimental observations revealed that facial recognition performance is influenced by several environmental factors, particularly illumination intensity, camera quality, facial orientation, and background variations. These factors may increase the confidence value even for legitimate users. Therefore, selecting a threshold of 40 provides a practical balance between recognition robustness and system security by maintaining reliable authentication performance while reducing the likelihood of false acceptance.

Preliminary experiments were conducted using confidence threshold values of 30, 35, 40, and 45 to determine an appropriate operating threshold for the proposed attendance system. Among these evaluated values, a threshold of 40 provided the most balanced trade-off between False Acceptance Rate (FAR) and False Rejection Rate (FRR), while maintaining stable recognition performance under moderate environmental variations.

To further validate the selected threshold, the proposed system was evaluated using 120 attendance scenarios involving genuine attendance attempts and multiple spoofing attacks, including GPS spoofing through browser-based coordinate manipulation, printed-photo attacks, and smartphone display attacks. Under the selected confidence threshold of 40, the system achieved an overall accuracy of 96.67%, with a False Rejection Rate (FRR) of 4.00% and a False Acceptance Rate (FAR) of 2.85%. These results indicate that the selected threshold provides an appropriate balance between recognition reliability and authentication security under the evaluated operational conditions.

Overall, the implementation demonstrates that the integration of GPS-based geofencing and LBPH-based facial recognition through a Sequential Multi-Factor Authentication mechanism provides an effective solution for securing web-based attendance systems. By validating the user's location before performing biometric verification, the proposed approach reduces unnecessary biometric processing, strengthens attendance security, and effectively reduces opportunities for attendance manipulation while maintaining lightweight computational requirements suitable for organizational attendance systems.

B. *Functional Testing Results*

The functional performance of the proposed smart attendance system was evaluated using the black-box testing method to verify whether each functional module operated according to the predefined system requirements. Unlike white-box testing, black-box testing evaluates the system based on input-output behavior without considering the internal implementation of the source code. The evaluation covered the primary functionalities of the proposed attendance system, including face registration, geofencing validation, facial verification, attendance recording, attendance validation, and browser permission handling. The summarized testing results are presented in Table 3.

TABLE III
SUMMARY OF FUNCTIONAL TESTING RESULTS

Functional Module	Validation Objective	Result
Face Registration	Generate an LBPH facial model from a single facial image.	Pass
Geofencing Validation	Verify that the user is located within the authorized attendance radius	Pass
Face Verification	Authenticate the registered user using the LBPH algorithm	Pass
Attendance Recording	Successfully perform attendance check-in and check-out	Pass
Attendance Validation	Reject incomplete or unauthorized attendance requests	Pass
Camera/GPS Permission Handling	Prevent attendance when camera or GPS permissions are denied	Pass with Notes

As summarized in Table 3, all major functional modules successfully satisfied the predefined functional requirements. The face registration module successfully captured a single frontal facial image and generated an individual Local Binary Pattern Histogram (LBPH) facial model for each registered user. This model serves as the biometric reference during subsequent attendance verification.

The attendance recording module also performed consistently throughout the evaluation. Both attendance check-in and check-out processes were executed successfully after completing the required validation procedures. In addition, the system correctly enforced mandatory activity descriptions during the check-out process and prevented incomplete attendance submissions. These results indicate that the attendance workflow was implemented according to the designed business rules while maintaining the integrity of attendance records.

The proposed Sequential Multi-Factor Authentication (MFA) mechanism demonstrated stable performance during all functional testing scenarios. The system consistently performed geofencing validation before executing the Local Binary Pattern Histogram facial recognition algorithm. Attendance requests originating from locations outside the predefined attendance radius were immediately rejected without initiating biometric verification. This sequential validation strategy not only strengthens system security but also reduces unnecessary biometric processing by executing facial recognition only after successful geofencing validation.

Furthermore, the LBPH facial verification module successfully authenticated registered users after passing the geofencing validation stage. The system accepted attendance only when the generated confidence score was less than or equal to the predefined threshold of 40, while higher confidence values resulted in attendance rejection. This implementation demonstrates that the proposed threshold provides an effective balance between recognition robustness and security under practical operational conditions.

Among all evaluated scenarios, only the Camera/GPS Permission Handling module was categorized as Pass with Notes. Although the application correctly prevented attendance when users denied browser access to the required camera or GPS services, a minor user interface issue was observed in which the attendance container became empty after the permission request was rejected. Nevertheless, this limitation did not affect the authentication workflow or compromise the security of the attendance process because attendance could not proceed without the required hardware permissions.

Overall, the functional testing results confirm that the proposed attendance system operates reliably across all evaluated functional modules. The successful integration of Laravel, Python, GPS-based geofencing, and Local Binary Pattern Histogram (LBPH) facial recognition demonstrates that the proposed Sequential Multi-Factor Authentication framework effectively supports secure and reliable attendance recording while maintaining stable system performance under normal operating conditions.

C. Biometric Performance Evaluation

To complement the functional evaluation conducted through black-box testing, the proposed attendance system was further assessed using quantitative biometric performance metrics. The evaluation involved five participants who each registered one frontal facial image during the enrollment stage to generate an individual Local Binary Pattern Histogram (LBPH) facial model. During the evaluation, participants performed multiple attendance sessions under moderate indoor illumination, natural facial expressions, and slight head orientation variations while maintaining the frontal facial position established during enrollment. The complete evaluation consisted of 120 attendance scenarios, including 50 genuine attendance attempts, 20 GPS spoofing attempts, 20 printed-photo presentation attacks, and 30 smartphone display presentation attacks. These scenarios were designed to evaluate the robustness of the proposed Sequential Multi-Factor Authentication framework under both normal operating conditions and multiple attack situations.

The biometric performance of the proposed Local Binary Pattern Histogram (LBPH)-based facial recognition system was assessed using Accuracy, False Acceptance Rate (FAR), and False Rejection Rate (FRR). Accuracy represents the proportion of correctly classified authentication attempts, FAR indicates the percentage of unauthorized users incorrectly accepted by the system, and FRR represents the percentage of legitimate users incorrectly rejected during authentication. The obtained evaluation results are summarized in Table 4.

TABLE IV
BIOMETRIC PERFORMANCE EVALUATION RESULTS

Performance Metric	**Value**
Total Evaluation Scenarios	120
Genuine Attendance Attempts	50
GPS Spoofing Attempts	20
Printed-Photo Attacks	20
Smartphone Display Attacks	30
Overall Accuracy	96.67%
False Acceptance Rate (FAR)	2.85%
False Rejection Rate (FRR)	4.00%

Overall, the evaluation dataset consisted of five enrolled users with one registered facial image per participant and multiple attendance attempts captured under moderate environmental variations to simulate practical operational conditions.

As presented in Table IV, the proposed Sequential Multi-Factor Authentication framework achieved an overall authentication accuracy of 96.67%, demonstrating reliable performance under both genuine attendance and attack scenarios. The obtained False Acceptance Rate (FAR) of 2.85% indicates that only a small proportion of unauthorized authentication attempts were incorrectly accepted, while the False Rejection Rate (FRR) of 4.00% shows that the system maintained an acceptable balance between security and usability by minimizing the rejection of legitimate users. These results demonstrate that the selected confidence threshold of 40 provides an appropriate trade-off between recognition reliability and authentication security for the evaluated deployment environment.

Furthermore, the inclusion of printed-photo attacks, smartphone display attacks, and browser-based GPS spoofing demonstrates that the proposed framework was evaluated under more realistic operational conditions than conventional functional testing alone. Unlike conventional functional testing, the proposed evaluation explicitly included presentation attacks using printed photographs and smartphone displays, together with browser-based GPS spoofing, allowing the robustness of the proposed Sequential Multi-Factor Authentication framework to be evaluated under realistic attack conditions. The results confirm that integrating GPS-based geofencing, LBPH facial recognition, and spoofing detection within a Sequential Multi-Factor Authentication framework provides a practical and lightweight solution for secure web-based attendance management.

D. Discussion of Sequential Multi-Factor Authentication

The proposed attendance system employs a Sequential Multi-Factor Authentication (MFA) framework by integrating GPS-based geofencing with Local Binary Pattern Histogram (LBPH) facial recognition. Unlike conventional attendance systems that rely solely on a single authentication mechanism, the proposed approach performs location validation before initiating biometric verification. This sequential validation strategy establishes multiple security layers while simultaneously reducing unnecessary computational processes.

The authentication workflow implemented in the proposed system is illustrated in Figure 10. The process begins with geofencing validation, where the user's GPS coordinates are compared with the predefined attendance location. If the user is located outside the authorized attendance radius, the attendance request is immediately rejected without executing the facial recognition module. Only users who successfully satisfy the location requirement proceed to facial verification using the LBPH algorithm. Finally, the generated confidence score is evaluated against the predefined threshold before attendance is recorded.

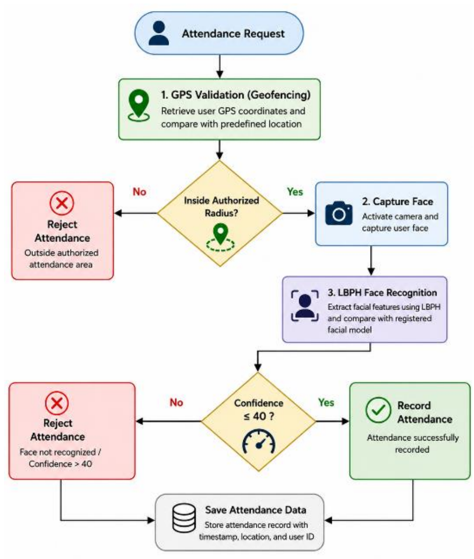

Figure 10. Sequential Multi-Factor Authentication workflow implemented in the proposed attendance system

The sequential arrangement of authentication stages provides several practical advantages compared with executing all validation processes simultaneously. First, validating the user's geographical location before performing facial recognition reduces unnecessary computational workload because the biometric verification module is executed only for authorized attendance requests. Consequently, unnecessary biometric processing is avoided because facial verification is executed only after successful geofencing validation.

Second, the proposed framework improves attendance security by requiring users to satisfy two independent authentication factors simultaneously. Even if an unauthorized individual successfully imitates another user's facial appearance, attendance cannot be completed unless the individual is physically located within the authorized attendance area. Similarly, users located within the designated attendance radius cannot successfully complete attendance unless their facial characteristics match the registered biometric model. This dual-layer validation significantly reduces opportunities for attendance manipulation compared with systems relying solely on location verification or facial recognition.

Another important aspect of the proposed framework is the implementation of the confidence threshold in the LBPH facial recognition module. Unlike probability-based classification models, the confidence value generated by the Local Binary Pattern Histogram algorithm represents a distance metric, where values approaching zero indicate higher similarity between the captured facial image and the stored biometric template. Based on the implementation results, the proposed system adopts a maximum confidence threshold of 40 to determine successful authentication.

The selected threshold reflects practical deployment conditions rather than ideal laboratory environments. During implementation, several environmental factors were observed to influence the confidence score, including illumination intensity, camera quality, facial orientation, and background variations. Among these factors, illumination changes produced the greatest impact because the LBPH descriptor extracts grayscale texture patterns from facial images. Variations in lighting conditions may alter local texture information, causing confidence values to increase even when the same individual performs attendance. Therefore, selecting a threshold of 40 provides an appropriate balance between recognition robustness and authentication security, allowing the system to tolerate moderate environmental variations while maintaining reliable user verification.

The suitability of this threshold is also supported by the experimental evaluation conducted under 120 attendance scenarios. The obtained accuracy of 96.67%, together with an FRR of 4.00% and an FAR of 2.85%, demonstrates that the selected threshold maintains reliable authentication performance while effectively resisting both genuine recognition errors and spoofing attempts.

The proposed Sequential Multi-Factor Authentication framework also offers advantages from a software engineering perspective. By separating location validation and biometric verification into consecutive processing stages, the authentication workflow becomes modular and easier to maintain within the Laravel–Python architecture. Future improvements, such as replacing the LBPH algorithm with more advanced deep learning-based facial recognition models or integrating liveness detection, can be implemented without significantly modifying the geofencing module or the overall authentication workflow.

Overall, the discussion demonstrates that the proposed Sequential Multi-Factor Authentication mechanism contributes not only to improving attendance security but also to reducing unnecessary biometric processing and improving system maintainability. The combination of geofencing and LBPH facial recognition provides complementary security layers that effectively prevent unauthorized attendance while maintaining lightweight computational requirements suitable for web-based attendance systems.

E. Comparison with Previous Studies

Previous studies have demonstrated the effectiveness of facial recognition technologies in improving attendance automation and authentication accuracy. For instance, the study employing MTCNN and DeepFace successfully automated classroom attendance through deep learning-based facial recognition, achieving high identification performance under controlled conditions [6]. Similarly, another study integrated MTCNN, VGGFace, and Support Vector Machine (SVM) classifiers to support real-time multi-face recognition, demonstrating the capability of recognizing multiple individuals simultaneously with satisfactory accuracy [22]. These studies indicate that deep learning-based facial recognition has become a promising approach for intelligent attendance systems; however, such methods generally require higher computational resources and more complex implementation environments.

Several researchers have also explored alternative deep learning architectures to improve recognition robustness under various operational conditions. Portable attendance systems incorporating liveness detection have been proposed to reduce spoofing attacks by ensuring that only genuine facial images are accepted during authentication [24]. Furthermore, FaceNet and other transfer learning approaches have been widely adopted to enhance facial representation and improve recognition performance in challenging environments [24], [26], [27]. Although these approaches achieve excellent recognition accuracy, they remain computationally intensive and often require high-performance hardware for model training and deployment.

Compared with these previous studies, the proposed system adopts a different implementation strategy by utilizing the Local Binary Pattern Histogram (LBPH) algorithm integrated with GPS-based geofencing within a Sequential Multi-Factor Authentication (MFA) framework. Rather than relying solely on increasingly sophisticated facial recognition models, the proposed approach combines biometric authentication with spatial verification, ensuring that attendance is validated only when users are physically located within the authorized attendance area. Moreover, the sequential validation mechanism performs geofencing verification before executing facial recognition, thereby avoiding unnecessary biometric processing for unauthorized attendance requests.

Another distinguishing characteristic of the proposed system is the implementation of a predefined confidence threshold during LBPH-based facial verification. Attendance is accepted only when the generated confidence value is less than or equal to 40, allowing the system to maintain reliable authentication performance despite moderate variations in illumination, facial orientation, and background conditions. Unlike previous studies that primarily emphasized recognition accuracy through increasingly complex deep learning architectures, the proposed system prioritizes a balance between authentication reliability, computational efficiency, and practical deployment in web-based attendance applications.

Overall, the comparison demonstrates that the contribution of this study lies not in replacing state-of-the-art deep learning algorithms, but in introducing a lightweight and practical Sequential Multi-Factor Authentication framework that integrates geofencing and LBPH facial recognition into a unified web-based attendance system. This approach provides an efficient alternative for attendance applications that require reliable security while maintaining low computational complexity and ease of deployment.

F. Research Limitations and Future Work

Although the proposed web-based smart attendance system successfully integrates GPS-based geofencing and Local Binary Pattern Histogram (LBPH) facial recognition within a Sequential Multi-Factor Authentication (MFA) framework, several limitations remain that should be considered when interpreting the results.

First, the proposed system employs the LBPH algorithm, which was selected because of its lightweight computational requirements and ease of integration into a web-based architecture. Although LBPH provides efficient facial recognition suitable for resource-constrained environments, its recognition performance is influenced by environmental factors, particularly illumination intensity, facial orientation, camera quality, and background variations. These conditions may increase the confidence score even for legitimate users, potentially affecting authentication consistency under uncontrolled operational environments.

Another limitation of this study is that the proposed LBPH-based authentication framework was not experimentally compared with other facial recognition methods, such as Eigenfaces, Fisherfaces, FaceNet, ArcFace, or MobileFaceNet, under identical experimental conditions. Therefore, the relative advantages of the proposed approach in terms of recognition performance and computational efficiency cannot yet be objectively quantified. Consequently, the proposed framework should be interpreted as a lightweight implementation rather than a replacement for state-of-the-art deep learning-based facial recognition methods. Future studies should conduct comparative benchmarking using the same dataset and evaluation protocol to provide a more comprehensive performance assessment.

Second, the current implementation applies a fixed confidence threshold of 40 for facial verification. While this threshold demonstrated satisfactory performance during system implementation and functional testing, it was empirically determined based on the deployment environment and may not represent the optimal threshold for different cameras, lighting conditions, or operational scenarios. Future implementations may require adaptive threshold optimization to improve recognition robustness under varying environmental conditions.

Third, the proposed attendance system focuses primarily on functional validation through black-box testing to verify that each module operates according to the specified requirements. Although this study reports quantitative biometric metrics including accuracy, FAR, and FRR, additional evaluation using precision, recall, F1-score, ROC analysis, and larger datasets is recommended to provide a more comprehensive assessment of the proposed authentication framework. Incorporating these evaluation metrics would provide a more comprehensive assessment of the biometric authentication performance.

Furthermore, the current implementation does not include liveness detection or anti-spoofing mechanisms. Although the combination of geofencing and facial recognition significantly strengthens attendance security, the system remains potentially vulnerable to sophisticated presentation attacks involving high-quality facial images or videos. Integrating liveness detection techniques would further improve the robustness of the authentication process.

Based on these limitations, several directions for future research can be proposed. Future studies may investigate the integration of lightweight deep learning-based facial recognition models, such as FaceNet, MobileFaceNet, or ArcFace, to improve recognition performance while maintaining acceptable computational efficiency. In addition, implementing adaptive confidence threshold selection based on environmental conditions may further enhance authentication reliability across different deployment environments.

Future research may also incorporate liveness detection, anti-spoofing algorithms, and additional authentication factors to further strengthen the proposed Sequential Multi-Factor Authentication framework. Moreover, evaluating the proposed system using a larger number of users and conducting performance comparisons under different lighting conditions, camera devices, and operational environments would provide a more comprehensive understanding of the system's scalability and robustness.

Overall, despite these limitations, the proposed system demonstrates that integrating geofencing with LBPH-based facial recognition through a Sequential Multi-Factor Authentication mechanism provides a practical, lightweight, and secure solution for web-based attendance systems. The identified limitations provide valuable opportunities for future enhancements while confirming the feasibility of the proposed approach for real-world attendance management applications.

IV. CONCLUSION

This study proposed and implemented a web-based smart attendance system that integrates GPS-based geofencing and Local Binary Pattern Histogram (LBPH) facial recognition within a Sequential Multi-Factor Authentication (MFA) framework. The system was developed using the Extreme Programming (XP) methodology to support an iterative software development process. Experimental results demonstrated that the proposed Sequential Multi-Factor Authentication framework successfully verified both user location and biometric identity before attendance was recorded. Functional evaluation confirmed that all major system modules operated according to the predefined functional requirements, while the sequential authentication strategy effectively prevented unauthorized attendance attempts and reduced unnecessary biometric processing by executing facial recognition only after successful geofencing validation.

The findings indicate that the proposed Sequential Multi-Factor Authentication framework, which combines lightweight LBPH-based facial recognition, geofencing validation, and GPS spoofing detection, provides a practical alternative to computationally intensive deep learning approaches for web-based attendance systems. The proposed framework enhances attendance security by combining two independent authentication factors while maintaining a lightweight architecture that is suitable for real-world internship and organizational attendance management. Furthermore, the implementation demonstrates that a confidence threshold of 40 provides a reasonable balance between recognition reliability and operational practicality under moderate environmental variations.

Future research should extend the evaluation using larger participant populations, more diverse environmental conditions, and additional biometric performance analyses to further validate the robustness and generalizability of the proposed framework. In addition, integrating liveness detection, adaptive confidence threshold optimization, lightweight deep learning-based facial recognition models, and more advanced GPS spoofing detection techniques could further improve authentication robustness while preserving lightweight deployment characteristics.

REFERENCES

[1] R. Gismara and H. W. Nugroho, “Functional and User Acceptance Evaluation of a GIS-Based Investment Information System,” *Journal of Applied Informatics and Computing*, vol. 10, no. 2, pp. 1321–1328, 2026.

[2] N. A. Ismail *et al.*, “Web-based University Classroom Attendance System Based on Deep Learning Face Recognition.,” *KSII Transactions on Internet & Information Systems*, vol. 16, no. 2, p. 503, 2022.

[3] T.-V. Dang, “Smart attendance system based on improved facial recognition,” *Journal of Robotics and Control (JRC)*, vol. 4, no. 1, pp. 46–53, 2023.

[4] S. Pathan, B. Deka, A. T. Bhattu, L. Bommireddipalli, S. Anandham, and S. Boorla, “A Location and QR Code-Based Solution for Efficient Attendance Management,” in *2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS)*, IEEE, 2025, pp. 859–866.

[5] P. R. F. Kaha, S. B. Rahayu, A. M. Azahari, M. H. M. Halip, and K. Venkatesan, “W@ rk: Attendance application framework using blockchain technology,” in *The International Conference on Data Science and Emerging Technologies*, Springer, 2023, pp. 479–492.

[6] U. D. Essien and G. Ansa, “A deep learning-based face recognition attendance system,” *Global Journal of Engineering and Technology Advances*, vol. 17, no. 1, pp. 9–22, 2023.

[7] C. J. T. Situmorang and P. M. Hasugian, “Development Of A Face Recognition And Geofencing Based Attendance Information System Using The Prototyping Method,” *Jurnal Komputer Indonesia (Ju-Komi)*, vol. 4, no. 01, pp. 66–81, 2025.

[8] G. Aravinda, R. Kshatri, S. Narendiran, J. Dev Darshan, and J. Jijo, "COVID-safe attendance monitoring system using QR codes, geo-location and IOT," in *AIP Conference Proceedings*, AIP Publishing LLC, 2023, p. 040002.

[9] S. Modak, H. Shah, R. Surana, and D. Mishra, "A systematic review of attendance systems based on face recognition," *PARIPEX-Indian Journal of Research*, vol. 11, no. 11, 2022.

[10] J. Nithin, "The Face Recognition Attendance System," in *2025 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI)*, IEEE, 2025, pp. 1–6.

[11] S. Purnama, M. Kamal, and A. B. Yadila, "Application of restful method with jwt security and haversine algorithm on web service-based teacher attendance system," *International Transactions on Artificial Intelligence*, vol. 2, no. 1, pp. 33–39, 2023.

[12] N. V. Prasada and I. Ikrimach, "Employee attendance system using face recognition and GPS using local binary pattern histogram," *International Journal of Science, Technology, Engineering and Mathematics*, vol. 4, no. 4, pp. 83–107, 2024.

[13] N. Nurdin, S. Sahibu, A. Jalil, M. Razak, A. L. Arda, and R. Namruddin, "Integration of RFID and Fingerprint Sensors in an IoT-Based Attendance System," *Journal of Applied Informatics and Computing*, vol. 10, no. 2, pp. 1996–2010, 2026.

[14] R. S. Wijaya, N. Waty, and N. R. Dija, "From Global GPS to Local Waypoints: A UTM-Based GPS-IMU Localization Method for VTOL UAV Navigation," *Journal of Applied Informatics and Computing*, vol. 10, no. 2, pp. 1416–1425, 2026.

[15] K. Chandra and Y. E. Oktian, "Integrated Jewelry Store Management System with Computer Vision-Based Size Prediction," *Journal of Applied Informatics and Computing*, vol. 10, no. 2, pp. 1391–1403, 2026.

[16] D. Venugopal, B. H. Angelin, M. Padmarekha, and P. Subbiksha, "Attendance Recording System Application for Smart Employee Attendance Management," in *2026 IEEE 2nd International Conference on Quantum Photonics, Artificial Intelligence & Networking (QPAIN)*, IEEE, 2026, pp. 1–6.

[17] C. Dhanush, S. S. Chowdhury, and A. K. Shekadar, "Automated Attendance System using RFID and IoT," 2025.

[18] A. Triswantoro, F. M. Dewanto, and A. T. J. Harjanta, "Indonesian Sign Language Application Using Mediapipe and Gated Recurrent Unit in Real Time," *Journal of Applied Informatics and Computing*, vol. 10, no. 2, pp. 1631–1638, 2026.

[19] M. H. M. Kamil, N. Zaini, L. Mazalan, and A. H. Ahamad, "Online attendance system based on facial recognition with face mask detection," *Multimed. Tools Appl.*, vol. 82, no. 22, pp. 34437–34457, 2023.

[20] M. Gudavalli, "Smart attendance monitoring system using multimodal biometrics.," *Sigma: Journal of Engineering & Natural Sciences/Mühendislik ve Fen Bilimleri Dergisi*, vol. 43, no. 1, 2025.

[21] T.-W. Chiang *et al.*, "Development and evaluation of an attendance tracking system using smartphones with GPS and NFC," *Applied Artificial Intelligence*, vol. 36, no. 1, p. 2083796, 2022.

[22] M. E. Ali, A. Diwan, and D. Kumar, "Attendance system optimization through deep learning face recognition," *International Journal of Computing and Digital Systems*, vol. 15, no. 1, pp. 10–12785, 2024.

[23] A. K. Shukla, A. Shukla, and R. Singh, "Automatic attendance system based on CNN–LSTM and face recognition," *International Journal of Information Technology*, vol. 16, no. 3, pp. 1293–1301, 2024.

[24] N. Surantha and B. Sugijakko, "Lightweight face recognition-based portable attendance system with liveness detection," *Internet of Things*, vol. 25, p. 101089, 2024.

[25] S. Vasavi, C. N. Sree, P. Harshitha, and B. Jaswanth, "Child Tracking System in Public Transportation Using RFID and Face Recognition," in *2025 12th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*, IEEE, 2025, pp. 1–6.

[26] P. Kumar, S. L. TA, and R. Santhosh, "Face recognition attendance system using local binary pattern algorithm," in *2023 2nd International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies (ViTECoN)*, IEEE, 2023, pp. 1–6.

[27] A. Rao, "AttenFace: A real time attendance system using face recognition," in *2022 IEEE 6th Conference on Information and Communication Technology (CICT)*, IEEE, 2022, pp. 1–5.

[28] J. Viswanathan, E. Kuralamudhan, S. Navaneethan, and S. Veluchamy, "Smart attendance system using face recognition," *EAI Endorsed Transactions on Scalable Information Systems*, vol. 11, no. 5, 2024.

[29] A. Budiman, R. A. Yaputera, S. Achmad, and A. Kurniawan, "Student attendance with face recognition (LBPH or CNN): Systematic literature review," *Procedia Comput. Sci.*, vol. 216, pp. 31–38, 2023.

[30] K. Painuly, Y. Bisht, H. Vaidya, A. Kapruwan, and R. Gupta, "Efficient real-time face recognition-based attendance system with deep learning algorithms," in *2024 International conference on intelligent and innovative technologies in computing, electrical and electronics (IITCEE)*, IEEE, 2024, pp. 1–5.