SMATIKA : STIKI Informatika Jurnal
Accredited Sinta 4 Ministry of Higher Education, Science and Technology Republic of Indonesia SK No. 79/E/KPT/2023
E-ISSN: 2580-6939 || P-ISSN: 2087-0256

Web-Based Attendance System Using Arcface, GPS Validation and Liveness Detection

Diah Arifah P [1*], Alvin Ricardo Laurence [2]

[1,2] *Bhinneka Nusantara University, Faculty of Science and Technology, Department of Informatic Engineering, Tidar Raya Street No.100, Malang, East Java, 65146, Indonesia*

Keyword

ArcFace; Face Recognition; Geofencing; Liveness Detection; Web-Based Attendance System

****Corresponding Author:***
diah@ubhinus.ac.id

Abstract

The development of digital attendance systems requires authentication mechanisms that are not only flexible but also secure against identity and location manipulation. Conventional fingerprint-based attendance systems have limitations in supporting employee mobility and still require dedicated hardware at each workplace location. Existing online attendance systems generally implement GPS validation or face recognition independently and often lack mechanisms to prevent identity spoofing attacks. In addition, computationally intensive models may reduce system efficiency in real-time web environments. Therefore, this study proposes a web-based attendance system that integrates lightweight facial authentication, GPS-based geofencing validation, and passive liveness detection to improve both security and computational efficiency.This study aims to develop a web-based attendance system integrating ArcFace-based facial authentication, GPS-based geofencing validation, and Passive Liveness Detection using MiniFASNet. Experimental evaluations were conducted to assess authentication accuracy, computational efficiency, and spoofing detection capability. The results showed that MobileFaceNet achieved an authentication accuracy of 95.00% with an average inference time of 0.0216 seconds per face. In addition, the implemented liveness detection mechanism effectively detected most spoofing attempts involving photographs and replay videos. The system also achieved a False Acceptance Rate (FAR) of 0% under the evaluated experimental conditions and successfully fulfilled all functional requirements. Therefore, the proposed system provides a secure, efficient, and centralized attendance solution suitable for organizations with high employee mobility.

1. Introduction

Digital transformation in industrial and organizational sectors has increased the demand for attendance systems that are more flexible, efficient, and secure. Conventional biometric systems such as fingerprint scanners are gradually being abandoned because they create queues, depend on dedicated hardware, and limit workplace flexibility [1]. In addition, the implementation of hybrid work patterns and increasing employee mobility require organizations to adopt attendance systems that can be accessed online and in real time. Therefore, web-based attendance systems have become a practical solution that enables real-time attendance recording without dependence on dedicated physical devices [2], [3]. Besides improving attendance flexibility, digital systems also help organizations monitor attendance centrally and support more efficient employee data management [2],[3].

Recent studies have shown that web-based and intelligent attendance systems are increasingly adopted to support flexible working environments and centralized attendance monitoring [4], [3], [5], [6], [7]. The integration of face recognition technology into attendance systems has been widely implemented to reduce fraudulent attendance activities and improve identity validation accuracy [4].However, conventional face recognition systems without liveness detection mechanisms remain vulnerable to spoofing attacks using printed photographs and replay videos [8],[9],[10]. Therefore, several recent studies have introduced liveness detection approaches and lightweight facial authentication architectures to improve the security and efficiency of attendance systems in real-time environments [11], [8], [10].

Although it offers greater flexibility, the implementation of online attendance systems also introduces new challenges, particularly in ensuring the validity of user identity and location. GPS-based location validation using a geofencing approach is required to ensure that attendance is recorded within the designated work area [12]. On the other hand, face recognition-based systems are vulnerable to spoofing attacks, such as the use of photos or videos (*replay attacks*), which may lead to attendance data manipulation[13]. Furthermore, location validation also plays an important role in ensuring that users are physically present within the authorized work area when performing attendance activities. These issues may result in attendance data manipulation if the system is not equipped with additional verification mechanisms.

Previous studies have developed attendance systems based on GPS and face recognition separately [14]-[15]. However, most of these systems were not equipped with liveness detection mechanisms, making them vulnerable to identity manipulation using two-dimensional media. Other studies have introduced CNN-based liveness detection to improve the security of face recognition systems, but they did not integrate location validation or centralized web-based architectures [11], [8]. In addition, several studies still utilize deep learning models with high computational complexity, making them less optimal for real-time implementation on servers with limited resources [16],[17],[12].

Recent studies have demonstrated the growing adoption of intelligent attendance systems integrating facial authentication, geolocation, and anti-spoofing mechanisms to support secure and flexible working environments [14],[5],[18]. However, many existing studies focus on individual components and often rely on computationally intensive architectures or mobile-dependent implementations [12],[14],[19]. Consequently, the integration of lightweight facial authentication, passive liveness detection, and GPS-based geofencing within a centralized web-based architecture remains limited.

Based on these issues, this study proposes the development of a web-based online attendance system that integrates GPS-based location validation using geofencing, facial authentication using face recognition, and liveness detection to improve the security of digital attendance processes. The system is designed using a web-based architecture so that it can be accessed flexibly through various devices and support the needs of multi-branch organizations with high employee mobility [7].ArcFace technology is utilized as a facial feature extraction method, while MiniFASNet is implemented as a passive liveness detection mechanism to help reduce the risk of identity manipulation during the attendance process [20].

Unlike previous studies that focused separately on GPS validation, facial authentication, or liveness detection, this research proposes a centralized web-based attendance system integrating GPS-based geofencing, ArcFace facial authentication, and Passive Liveness Detection [21], [18], [6].

The main contribution of this study lies in the implementation of lightweight artificial intelligence architectures optimized for real-time web environments and employee mobility scenarios. In addition, the proposed system supports both static and dynamic employees while improving resistance against spoofing attacks using two-dimensional media.

The objectives of this study are: (1) to design a web-based online attendance system that supports user identity and location validation, (2) to implement face recognition and liveness detection technologies to enhance the security of digital attendance systems, and (3) to evaluate the effectiveness of the attendance system in supporting flexible and real-time employee attendance management.

2. Research Method

This study adopts the Design Science Research (DSR) approach, which focuses on designing, developing, and evaluating an artifact to solve practical problems. In this research, the artifact is a web-based attendance system integrating GPS validation, ArcFace-based facial authentication, and Passive Liveness Detection. The study consists of problem identification, artifact development, implementation, and evaluation stages.

The research was conducted through two main stages. The first stage was an authentication technology testing phase carried out in a local server environment. At this stage, the performance of ArcFace-based face recognition and liveness detection technologies was evaluated using a self-collected dataset. The testing focused on the system's ability to perform facial authentication, maintain robustness against variations in user visual conditions, and detect potential identity manipulation (spoofing).

The second stage was the implementation and testing phase of the web-based system using Android and iOS mobile devices. The testing was conducted to ensure that system integration functioned properly, including GPS-based location validation, facial authentication, liveness detection, and real-time attendance recording through a web browser. This stage aimed to evaluate the effectiveness of the system in supporting a flexible and integrated digital attendance process within organizational environments.

2.1 Respondent Characteristics

The research respondents consisted of 8 participants who were used as facial image dataset samples during the authentication testing process. The dataset was collected independently using smartphone and webcam cameras under various visual conditions to evaluate system robustness and authentication performance.

Table 1. Characteristic of the Experimental Dataset

Dataset Component	Description
Participant	8 respondents
Genuine facial images	80 facial images
Visual Testing Scenarios	10 conditions per participant
Pose variations	Yaw left/right and pitch up/down
Lighting variations	Bright and low illumination
Occlusion scenarios	Partial facial occlusion
Camera distance variations	Near and far capture distance
Spoofing dataset	Printed photo and replay video
Authentication testing	Genuine and impostor scenarios
FAR testing	Cross-participant validation

The collected datasets were used to evaluate authentication robustness, spoofing detection capability, and the effectiveness of GPS-based attendance validation in real-time web environments.

2.2 Data Collection

The data collection methods were carried out through :

- literature studies related to digital attendance systems, face recognition, geofencing, and liveness detection
- direct acquisition of facial image datasets using device cameras
- collection of spoofing data using photo and video media
- collection of GPS coordinate data for location validation testing

- testing of the web-based system through direct usage simulations.

2.3 Data Validity and Reliability

Data validity was evaluated through system functional testing using the *Black Box Testing* method to ensure that all system features operated according to user requirements. In addition, authentication validity was assessed by measuring the system's ability to recognize user identities and detect spoofing attempts.

Construct validity was ensured by aligning the testing scenarios with the functional requirements of the proposed attendance system. Internal validity was maintained through repeated evaluations under various visual and location conditions. Dataset reliability was supported by collecting facial images under different lighting conditions, pose variations, and camera distances to improve the consistency of the experimental results.

System reliability was tested through repeated evaluations under various visual and location conditions to ensure the consistency of authentication results, GPS validation, and *liveness detection* in the web-based online attendance system.

3. Result and Discussions

This section presents the results of the implementation and testing of the web-based online attendance system developed in this study. The system was designed by integrating GPS-based location validation, facial authentication (*face recognition*), and *liveness detection* to support a more flexible and secure digital attendance process. The discussion focuses on system implementation, integration of the main features, system functionality testing, and evaluation of the system's effectiveness in supporting real-time employee attendance management.

The research results are discussed based on several main aspects, namely web-based system implementation, GPS location validation integration using *geofencing*, implementation of facial authentication and *liveness detection*, system testing using the *Black Box Testing* method

3.1 System Implementation

The system was designed using a web-based three-tier architecture consisting of: (1) Frontend (Client-Side): Developed using Next.js, responsible for displaying the user interface, accessing client hardware devices such as webcams or smartphone cameras, and extracting GPS coordinate data from the web browser; (2) Backend (Server-Side): Developed using the Python Flask framework as a REST API, responsible for executing the Geofencing business logic using the Haversine method, processing AI model inference using MiniFASNet and ArcFace, and managing authentication sessions; and (3) Database: Implemented using a relational database management system (MySQL) to store employee entity data, registered branch location data, 512-dimensional facial embedding vectors, and attendance history logs.

3.1.1 System Design

In this study, both the system design and the data design process were carried out. The attandance system design is illustrated using a Use Case Diagram, as shown in Figure 1

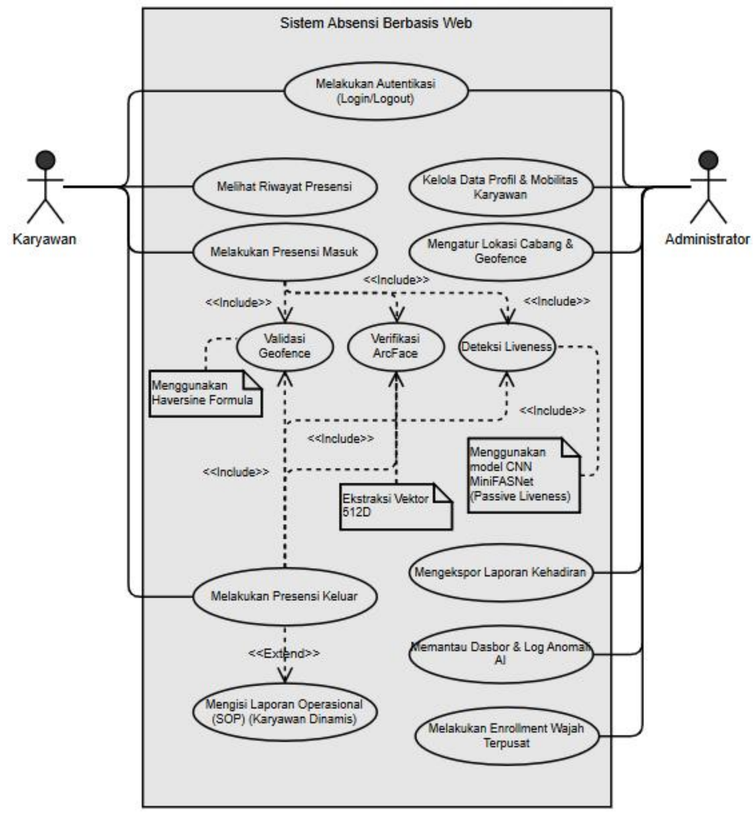

Figure 1. Use case diagram

Furthermore, the data design process was carried out by designing four relational tables with relationships illustrated in the Figure 2.

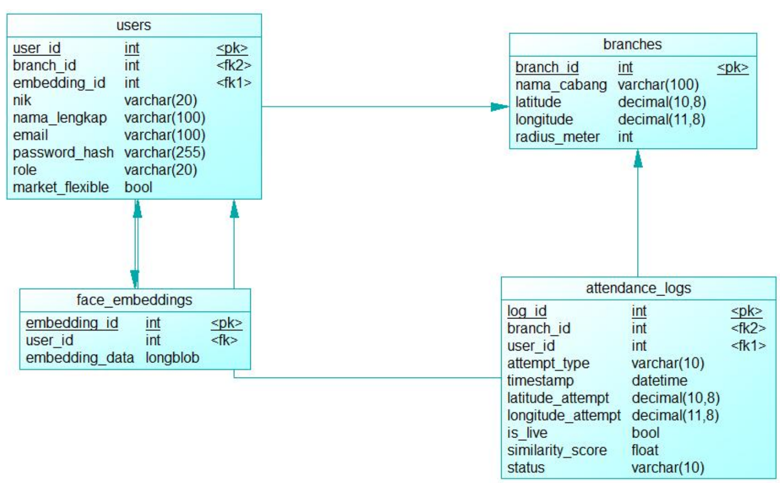

Figure 2. Physical Data Model

3.1.2 User Interface Implementation

The system interface was developed using a responsive design approach to ensure accessibility across desktop and mobile devices. The administrator interface includes login authentication, attendance management, employee management, and attendance report export features, as illustrated in Figure 3.

Meanwhile, the employee interface supports face enrollment and real-time attendance validation using facial authentication and GPS-based location verification, as presented in Figure 4.

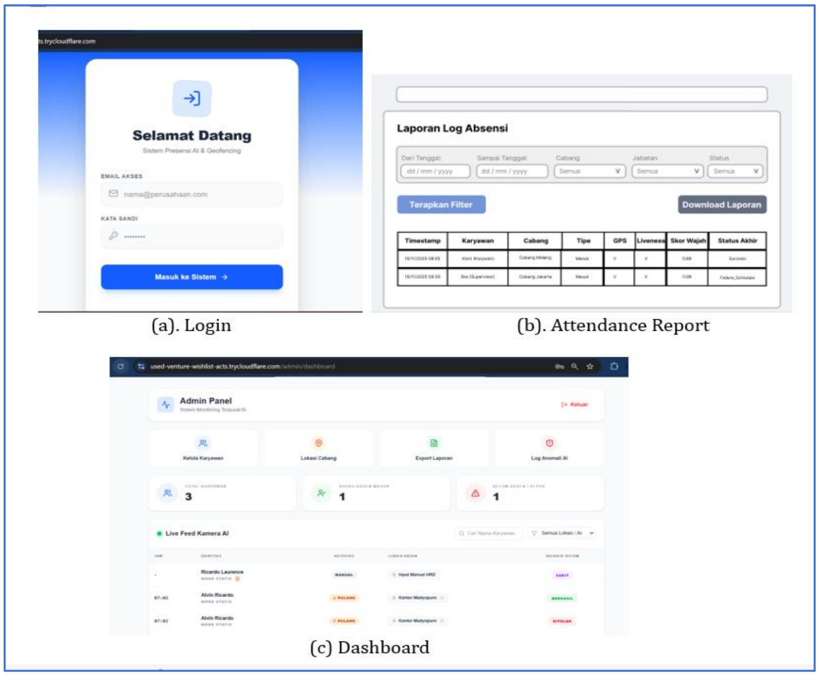

Figure 3. Administrator Interface Implementation

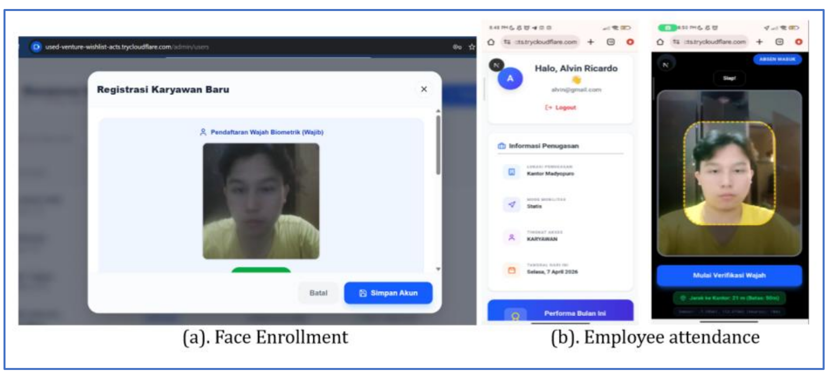

Figure 4. Employee Attendance Interface

3.2 GPS-Based Location Validation Implementation

The implementation of GPS-based location validation was carried out using the *geofencing* method by defining a central coordinate point and a specific radius as the valid attendance area. The system compares the user's current location with the predefined coordinate point to determine whether the attendance process can proceed or should be rejected.

The validation process was performed by calculating the distance between the user's location and the geofencing center point. The distance calculation technique implemented in this system utilized the Haversine Formula [22].This method was used to calculate the distance between two coordinate points based on latitude and longitude values.

Attendance requests were automatically rejected if the calculation results indicated that the user's location was outside the predefined radius. Conversely, attendance requests were accepted if the user was located within the valid geofencing area. The results of the GPS-based location validation testing are presented in the following Table 2.

Table 2. Result of GPS Validation Testing Using Geofencing

Testing Scenario	Distance from Center Point	Geofence Radius	System Response
The user is located at the registered coordinate point	10 meters	50 meters	The attendance button is enabled and displays "Start Face Verification"
The user is located within the geofence area	14 meters	50 meters	The attendance button is enabled and displays "Start Face Verification"
The user is located outside the geofence area	54 meters	50 meters	The attendance button is disabled and displays "Out of Range"

Based on the testing results, the system successfully validated user locations using the geofencing method and Haversine distance calculation. Users located within the predefined geofence radius were permitted to continue the attendance process, whereas users outside the permitted radius were automatically denied access to the attendance feature.

The GPS validation results indicate that the geofencing mechanism was effective in restricting attendance access based on predefined organizational locations. This mechanism is important in preventing remote attendance manipulation and ensuring that users are physically present within the authorized working area. Compared to conventional attendance systems that rely solely on facial authentication, the integration of GPS-based validation provides an additional contextual verification layer for attendance legitimacy [3],[6].

In addition, the implementation of adaptive geofencing policies for dynamic employees allows the system to support operational flexibility without completely eliminating location-based validation controls. This approach is particularly relevant for organizations with mobile employees such as marketing staff or field officers.

Compared with previous mobile-based attendance systems integrating GPS validation and face recognition, the implementation of adaptive geofencing in this study provides greater flexibility for dynamic employees while maintaining location-based attendance control [23].

3.3 Facial Authentication and Liveness Detection Implementation

The *liveness detection* mechanism in the final system was implemented using a passive approach (*Passive Liveness Detection*) based on a Convolutional Neural Network (CNN), namely MiniFASNet. This method was utilized to identify potential spoofing attempts using two-dimensional media such as photographs or video replays during the attendance process. The implementation mechanism of the *liveness detection* process is illustrated in the following Figure 5.

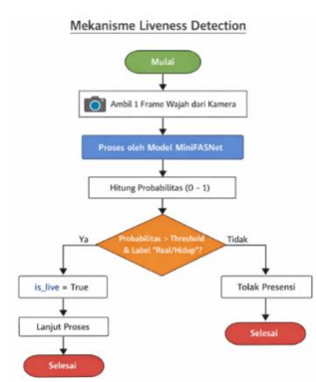

Figure 5. Liveness Detection Mechanism

Furthermore, the integration process of ArcFace, *liveness detection*, and GPS-based validation is illustrated in the following Figure 6.

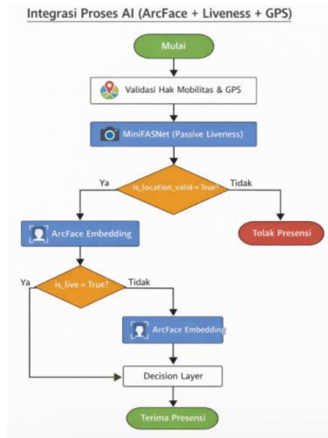

Figure 6. ArcFace, Liveness Detection, and GPS Integration Process

Facial authentication in the system was implemented using a face recognition method combined with Passive Liveness Detection based on MiniFASNet. The system was designed to ensure that the attendance process could only be performed by legitimate users and not through manipulated media such as photographs or videos displayed on other devices. The authentication process begins with GPS-based location validation using the geofencing method. Once the user is confirmed to be within the valid geofence radius, the system displays the “Start Face Verification” button to proceed with the liveness detection and face matching processes.

During the liveness detection stage, the system utilizes the MiniFASNet model to identify spoofing indications based on facial texture characteristics and visual patterns from two-dimensional media [8],[10]. After the face is verified as valid, the system continues the authentication process by calculating the facial similarity level (face similarity) between the user’s face and the facial data stored in the database. To evaluate the system’s capability in detecting identity manipulation attempts, several testing scenarios using photo and video media were conducted. The testing results are presented in Table 3.

Table 3. Result of Facial Authentication and Liveness Detection Testing

Testing Scenario	System Response
The user performed testing using a facial video displayed on a smartphone screen positioned very close to the camera so that only the facial area was visible	The system allowed the attendance process
The user repeated the testing using the same facial video under identical conditions	The system identified a spoofing attempt and rejected the attendance request
The user performed attendance using a facial video displayed on a smartphone screen with the device frame visible	The system identified a spoofing attempt and rejected the attendance request
The user performed attendance using a facial video displayed on a smartphone screen at close range so that the screen frame was not visible	The system detected a facial mismatch with a similarity score of 41%, and the attendance request was rejected
The user used a facial photograph to perform attendance	The system identified a spoofing attempt and rejected the attendance request

Based on the testing results, the system successfully detected most spoofing attempts using photo and video media displayed on external devices. In one testing scenario, the spoofing attempt temporarily bypassed the authentication process when the smartphone screen was positioned extremely close to the camera, making the visual characteristics of the screen difficult for the system to identify. However, during repeated testing under similar conditions, the system successfully detected the spoofing indication and rejected the attendance process.

The experimental results demonstrate that Passive Liveness Detection using MiniFASNet was generally effective in identifying spoofing attempts involving printed photographs and replay videos. The system was able to detect texture inconsistencies, screen reflection artifacts, and visual characteristics commonly found in two-dimensional spoofing media.

However, one testing scenario showed that spoofing attempts could temporarily bypass the authentication process when the replay device was positioned extremely close to the camera. This condition reduced the visibility of screen artifacts and limited the model's ability to distinguish spoofing indicators. Similar limitations have also been reported in previous face anti-spoofing studies involving replay attacks under extreme image acquisition conditions [11], [8].

Despite these limitations, repeated testing demonstrated that the system consistently rejected most spoofing attempts, indicating that the implementation of MiniFASNet significantly improved attendance security compared to conventional face recognition systems without liveness detection [3], [6]. In this study, the liveness detection mechanism was integrated directly into a centralized web-based attendance platform combined with GPS validation and facial authentication.

3.4 Authentication Performance Evaluation

To evaluate the effectiveness and performance of the proposed attendance system, several authentication performance metrics were measured, including authentication accuracy, False Acceptance Rate (FAR), inference time, and spoofing detection capability. The evaluation results are presented in Table 4.

Table 4. Authentication and Liveness Detection Testing

Evaluation Metric	Result
Authentication Accuracy	95%
False Acceptance Rate (FAR)	0%
Average Inference Time	0.0216 second per face
Spoofing Detection Capability	Successfully detected most replay and photo spoofing attemps

To provide a broader perspective on the performance of the proposed system, a comparison with several related studies [18], [15] is presented in Table 5. The comparison focuses on authentication accuracy, False Acceptance Rate (FAR), inference time, and the implementation of liveness detection mechanisms.

Table 5. Comparison with Previous Studies [18],[15]

Study	Accuracy	FAR	Inference Time	Liveness Detection
[18]	98,2%	N/A	N/A	Yes
[15]	97,0%	N/A	N/A	No
Proposed System	95,0%	0%	0.0216s	Yes

Compared with previous studies [18],[15], the proposed system provides competitive authentication performance while integrating GPS-based geofencing and Passive Liveness Detection into a centralized web-based architecture. In addition, the use of MobileFaceNet enables efficient real-time processing with low computational latency.

The performance evaluation results indicate that the proposed attendance system achieved a high authentication accuracy while maintaining low computational latency during real-time attendance processing. The implementation of MobileFaceNet as a lightweight ArcFace backbone enabled efficient facial authentication with an average inference time of 0.0216 seconds per face.

In addition, the system achieved a measured False Acceptance Rate (FAR) of 0% during cross-participant authentication testing, indicating that unauthorized users were consistently rejected under the evaluated experimental conditions. These results suggest that the integration of lightweight facial authentication and Passive Liveness Detection was effective in supporting secure and real-time attendance validation within web-based organizational environments. However, because the experiments involved a relatively small dataset, the obtained FAR value should be interpreted as preliminary evidence of system robustness rather than a conclusive benchmark comparable to large-scale biometric datasets.

3.5 System Functionality Testing (Black Box Testing)

System functionality testing was conducted using the Black Box Testing method to ensure that all features of the web-based online attendance system operated in accordance with the specified functional requirements and business logic. The testing process covered various system usage scenarios involving HR administrators, employees, and unauthorized users (impostors).

Based on the 10 testing scenarios that were conducted, all system features successfully operated according to the expected functionality. The testing results demonstrated that the system was capable of supporting user registration, GPS-based geofencing validation, facial authentication, liveness detection, attendance data management, and attendance report export processes. In addition, the system successfully detected identity manipulation attempts and restricted unauthorized access based on user access privileges. The results of the *Black Box Testing* are presented in Table 6.

Table 6. Result of System Functionality Testing (Black Box Testing)

No	Testing Scenario	Actor	Test Condition/ Input	Expected Result	Status
1.	Registration and Face Enrollment	HR Administrator	Entering employee data and capturing facial images using live capture	User data and facial embeddings are successfully stored in the database	Passed
2.	Branch and Geofencing Configuration	HR Administrator	Modifying location coordinates and geofence radius	Location and radius data are successfully updated in the system	Passed
3.	Successful Attendance (Static)	Employee	Performing attendance within the geofence radius using a valid face	Attendance data are successfully recorded	Passed
4.	Successful Attendance (Dynamic)	Employee	Performing attendance outside the radius with mobility access privileges	The system allows the authentication process and records attendance data	Passed
5.	Operational Report (SOP) Submission	Employee	Performing check-out attendance outside the geofence area	The system requires report submission before saving attendance data	Passed
6.	Failed Geofencing Validation	Employee	Performing attendance outside the radius without mobility privileges	The system rejects the attendance request and displays a warning message	Passed

No	Testing Scenario	Actor	Test Condition/ Input	Expected Result	Status
7.	Failed Liveness Detection (Spoofing)	*Impostor*	Using photos or videos to manipulate the authentication process	The system detects a spoofing attempt and terminates the attendance process	Passed
8.	Failed Identity Authentication	*Impostor*	Using a different face to access another user account	The system rejects facial authentication and denies attendance access	Passed
9.	Attendance History Access	Employee	Accessing the attendance history page on the dashboard	Attendance history data are successfully displayed	Passed
10.	Attendance Report Export	HR Administrator	Exporting attendance data into spreadsheet format	The system successfully generates a downloadable attendance report file	Passed

The Black Box Testing results indicate that the integration between GPS validation, facial authentication, and liveness detection mechanisms functioned consistently within the web-based attendance architecture. The successful execution of all testing scenarios demonstrates that the proposed system is capable of supporting secure and flexible attendance workflows in organizational environments.

In addition, the implementation of centralized attendance management through a web-based platform provides advantages in terms of accessibility, system scalability, and real-time attendance monitoring. This architecture also simplifies attendance management for multi-branch organizations by allowing centralized employee and attendance data management.

3.6 Research Limitations

This research has several limitations. First, the experimental dataset was relatively limited because the testing process involved only 8 participants and was conducted within a controlled environment. Second, the implemented liveness detection mechanism focused only on two-dimensional spoofing attacks using printed photographs and replay videos, without involving three-dimensional spoofing scenarios or infrared-based validation.

The experimental dataset involved only eight participants and was intended primarily for proof-of-concept evaluation rather than large-scale biometric benchmarking. Therefore, the reported authentication accuracy and FAR values should be interpreted as indicative results demonstrating the feasibility of the proposed prototype rather than generalized biometric performance

In addition, authentication performance may still be affected by extreme head poses, excessive lighting variations, and low-quality camera devices. Therefore, future research is recommended to utilize larger datasets, more diverse environmental conditions, and advanced anti-spoofing technologies such as depth sensors or infrared cameras.

4. Conclusions and Future Works

This study successfully achieved the three research objectives. First, a web-based attendance system capable of validating user identity and location was successfully designed and implemented. Second, the integration of ArcFace facial authentication and Passive Liveness Detection using MiniFASNet improved attendance security and achieved an authentication accuracy of 95% with an average inference time of 0.0216 seconds per face. Third, the proposed system effectively supported flexible and real-time attendance management through centralized web-based architecture and GPS-based geofencing validation.

The experimental results demonstrate that the proposed prototype provides a secure and computationally efficient solution for attendance management in organizations with high employee mobility. However, the obtained results are intended as proof-of-concept findings and should be further validated using larger and more diverse datasets.

The integration of facial authentication, *liveness detection*, and GPS-based location validation technologies was successfully implemented into the web-based attendance system functionally. Based on the *Black Box Testing* results, all system features operated according to the specified functional requirements and were capable of supporting secure and flexible employee attendance validation.

Future system development may focus on enhancing *anti-spoofing* security through the integration of depth sensors or infrared cameras to detect identity manipulation using three-dimensional objects. In addition, optimization of facial authentication under extreme head poses and masked-face conditions is also necessary to improve system accuracy across various user scenarios. From a functionality perspective, the system can be further developed by adding field activity proof upload features and implementing *Natural Language Processing* (NLP) technology to support automated validation and activity report recapitulation processes.

5. References

[1] A. M. A. DB, M. Faisal, and M. A. M. Hayat, "Implementasi Hybrid CNN, Facial Landmark dan Liveness Detection pada Sistem Absensi Wajah," *J. Inform. Prog.*, vol. 17, no. 2, pp. 116–120, 2025, doi: 10.56708/progres.v17i2.483.

[2] Z. Cheng, "Design of Face Recognition Course Checking System," *Front. Comput. Intell. Syst.*, 2025, doi: 10.54097/z106h475.

[3] M. A. Khan, M. Alhaisoni, U. Tariq, H. S. Yong, A. Armghan, and S. Kadry, "Human Face Recognition for Attendance Monitoring System Using Deep Learning Approach," *Comput. Mater. Contin.*, vol. 70, no. 2, pp. 2763–2778, 2022, doi: 10.32604/cmc.2022.019558.

[4] W. Nawaz, A. Ahmed, H. Tahir, and S. A. Khan, "Deep Learning-Based Face Recognition Attendance System: A Review and Future Directions," *Appl. Sci.*, vol. 13, no. 5, p. 3124, 2023, doi: 10.3390/app13053124.

[5] D. Sunaryono, J. Siswantoro, and R. Anggoro, "An Android Based Course Attendance System Using Face Recognition," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 33, no. 3, pp. 304–312, 2021, doi: 10.1016/j.jksuci.2019.01.006.

[6] M. Syarif and W. Gunawan, "Attendance System Leveraging Haar Cascade Detection and CNN-Based FaceNet Recognition Technology," *JOIV Int. J. Informatics Vis.*, vol. 9, no. 2, 2025, doi: 10.62527/joiv.9.2.2464.

[7] G. Gadafi, S. Sumarno, and C. Taurusta, "Implementasi Sistem Absensi Pada PG-TK AISYIYAH VI Sebagai Pendataan Absen Guru," *SMATIKA J. Inform.*, vol. 14, no. 2, pp. 284–296, 2024, doi: 10.32664/smatika.v14i02.1333.

[8] S. Khairnar, S. Gite, K. Kotecha, and S. D. Thepade, "Face Liveness Detection Using Artificial Intelligence Techniques: A Systematic Literature Review and Future Directions," *Big Data Cogn. Comput.*, vol. 7, no. 1, p. 37, 2023, doi: 10.3390/bdcc7010037.

[9] L. Li, Z. Xia, J. Wu, L. Yang, and H. Han, "Face Presentation Attack Detection Based on Optical Flow and Texture Analysis," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 4, pp. 1455–1467, 2022, doi: 10.1016/j.jksuci.2022.02.019.

[10] Y. Liu, J. Stehouwer, A. Jourabloo, and X. Liu, "Deep Learning Based Face Anti-Spoofing: A Review," *IEEE Access*, vol. 11, pp. 7090–7125, 2023.

[11] Z. Yu, Y. Qin, X. Li, C. Zhao, Z. Lei, and S. Z. Li, "Deep Learning for Face Anti-Spoofing: A Survey," *IEEE*

Trans. Pattern Anal. Mach. Intell., vol. 46, no. 1, pp. 1–22, 2023, doi: 10.1109/TPAMI.2022.3215850.

[12] S. Chen, Y. Liu, X. Gao, and Z. Han, "MobileFaceNets: Efficient CNNs for Accurate Real-Time Face Verification on Mobile Devices," in *Chinese Conference on Biometric Recognition (CCBR)*, 2018, pp. 428–436. doi: 10.1007/978-3-319-97909-0_46.

[13] E. N. F. Dewi, G. N. Tarempa, A. N. Rachman, and A. Febriansyah, "Sistem Presensi Perkuliahan Mahasiswa Berbasis Face Recognition dengan Metode Liveness Detection," *Indones. J. Comput. Sci.*, 2025, doi: 10.31294/ijcs.v4i2.9876.

[14] S. C. M. Rani, M. D. Sumukha, M. Hariprasad, M. N. Kumar, and J. R. Srinivas, "ML-Driven Automated Professor Presence Monitoring Using GPS Geo-Fencing and Face Liveness Detection," *Int. J. Res. Appl. Sci. Eng. Technol.*, 2025, doi: 10.22214/ijraset.2025.73664.

[15] G. C. Terampe and A. Pramudwiatmoko, "Facial Recognition Performance Evaluation with YOLOv8, ArcFace, and SVM in a Contactless Employee Attendance System," *J. Ris. Inform.*, vol. 8, no. 1, pp. 108–120, 2025, doi: 10.34288/jri.v8i1.465.

[16] S. Jia, C. Hu, G. Guo, and Z. Xu, "Face Anti-Spoofing Based on Deep Learning: Recent Advances and Challenges," *Electronics*, vol. 12, no. 9, p. 2068, 2023, doi: 10.3390/electronics12092068.

[17] Y. Martinez-Diaz, M. Nicolas-Diaz, H. Mendez-Vazquez, L. S. Luevano, and L. Chang, "Benchmarking Lightweight Face Architectures on Specific Face Recognition Scenarios," *Artif. Intell. Rev.*, vol. 54, pp. 6201–6244, 2021, doi: 10.1007/s10462-021-09974-2.

[18] N. Surantha and B. Sugijakko, "Lightweight Face Recognition-Based Portable Attendance System with Liveness Detection," *Internet of Things*, vol. 25, p. 101089, 2024, doi: 10.1016/j.iot.2024.101089.

[19] A. Pawar, R. Hiwanj, P. Koparde, D. Chikmurge, and S. Barve, "Automated Employee Attendance Monitoring Using Liveness Face Recognition and Geofencing in Real Time," in *Proceedings of the IEEE 5th International Conference on Advances in Electronics, Computers and Communications (ICAECC)*, 2023, pp. 1–6. doi: 10.1109/ICAECC59324.2023.10560301.

[20] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "ArcFace: Additive Angular Margin Loss for Deep Face Recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 44, no. 10, pp. 5962–5979, 2022, doi: 10.1109/TPAMI.2021.3087709.

[21] J. P. Sitanggang, J. S. Asri, Hermansyah, and I. Sutanto, "Rancang Bangun Sistem Absensi Berbasis Mobile Dengan Memanfaatkan Pengenalan Wajah (Studi Kasus: PT. Ginsa Inti Pratama)," *JUSTIKPEN*, vol. 5, no. 1, pp. 155–164, 2025, doi: 10.55338/justikpen.v5i1.356.

[22] N. Aloudat and S. Michael, "Location-Based Services Using Geofencing Technology: A Survey," *Futur. Internet*, vol. 14, no. 7, p. 215, 2022, doi: 10.3390/fi14070215.

[23] N. V Prasada and I. Ikrimach, "Employee Attendance System Using Face Recognition and GPS Using Local Binary Pattern Histogram," *Int. J. Sci. Technol. Eng. Math.*, vol. 4, no. 4, pp. 83–107, 2024, doi: 10.53378/ijstem.353133.