Location Based Attendance System Using Geofencing and Facial Recognition Technology

Rahul Garg, Dr. Anubhuti Mohindra

Jaypee Institute of Information Technology, Noida, India

Abstract

For a long time, hand attendance was a slow and inefficient process. Automated systems offer many advantages to organizations. Accordingly, we have proposed a dual-factor attendance tracking system that combines geographical-location-based tracking using geofencing technology with biometric facial recognition. This system is implemented on an Android mobile application that enforces a secure, session-based authentication flow. While researching the work that has been done in this field, we came across many studies that have implemented similar attendance marking systems using biometrics, Radio Frequency Identification (RFID), and other scanner devices. We eliminated the use of such dedicated hardware and devised a simple and easy-to-use system that uses a user's smartphone for both location verification and identity authentication. The system effectively prevents proxy attendance by requiring users to biometrically verify their identity for each new session.

Keywords: FusedLocationProviderClient API, Geofence, Firebase Realtime Database, Facial Embedding, Convolutional Neural Network (CNN), One-Time Password (OTP), Passwordless Authentication

1. Introduction

Taking attendance is a key part of the educational administration, and a good indicator of student engagement. Unfortunately, taking attendance using a manual method is incredibly inefficient. During a 50-minute lecture, taking attendance manually via roll call can sometimes take 10 minutes and lots of precious instructional time. More importantly, we also know that any manual attendance system has the potential for errors and proxy attendance.

Our attendance applications address these issues by having an app that automates the entire process of taking attendance. We were able to avoid expenses related to use of hardware devices, by using each student's own Android device. The uniqueness of our proposal is the dual-factor authentication approach combined with the contextual session-based attendance approach:

- Simple Authentication: A student starts the session each day by using a mobile one-time passcode (OTP).
- Verifiable authentication: A student must also do facial recognition authentication to verify the student is physically present.
- Autonomous Attendance: Once a student has authenticated, the application uses geofencing to take attendance when the student has dwelled within the virtual classroom's parameters.

This approach gives the user and the institution a secure login with minimum invasiveness of context. By using these concepts, the proposed smart attendance solution is an affordable, scalable and reliable method of attendance tracking in education and beyond.

2. Literature Survey

Over the last decade, automated attendance systems have changed a lot. Researchers have been busy looking for new ways to get rid of the old-fashioned methods of marking attendance by hand. This section provides a detailed look at current research on attendance management systems and explores the various technologies that have been used.

We've seen a lot of research and development on using RFID technology for managing attendance. Ishaq et al. (2023) [6] conducted a comprehensive systematic literature review of IoT-based smart attendance systems using RFID technology and analyzed major research publications in this domain. Their findings highlighted that RFID systems offer reliable identification capabilities, but require additional hardware infrastructure and maintenance costs. The study emphasized that an automated system that uses RFID (Radio-Frequency Identification) can put an end to the issues that come with manual attendance tracking, such as wasted time, proxy attendance, and lost sign-in sheets.

A recent 2023 study presented an automated system for workforce management using RFID. The research demonstrated improved accuracy rates but acknowledged the complexity of managing multiple authentication layers and the associated deployment costs for educational institutions.

Biometric attendance systems, which use unique physical traits like fingerprints or facial recognition, are becoming more popular because they're great at stopping people from clocking in for someone else. A 2024 [8] study showed just how well a face recognition system works, proving that biometrics are a reliable and efficient replacement for old-school attendance methods. Essentially, these systems offer better security than traditional methods because they rely on distinct biological markers that are impossible to fake. Smitha et al. (2020) [9] focused on face recognition-based attendance management systems and achieved significant accuracy improvements under controlled conditions. Research by the 2023 IEEE Conference [10] developed a face recognition-based attendance system using OpenCV, creating an efficient and reliable solution. Manually taking attendance is slow and tedious, so this study tackled that problem by using automated face detection and recognition. Implementation studies [11] have shown that face recognition algorithms for biometric-based time attendance systems can extract facial coordinates and compare them with stored database measurements, returning the closest matching records with high accuracy rates.

Geofencing technology is a powerful new tool for creating smarter apps that respond to a person's physical location. A recent study by Yury and colleagues (2023) [12] introduced a new way to use geofencing for studying human behavior. They showed how this technology can trigger specific events based on a person's location, opening up new possibilities for behavioral research. Their methodology addressed the battery drain issues associated with constant GPS tracking by implementing smart location monitoring algorithms. Geofencing offers a smarter way to handle location tracking, addressing some of the common problems that come with it. Instead of constantly monitoring someone's location, which can drain their phone's battery and collect a lot of private data, geofencing creates virtual boundaries. This approach has proven to be more efficient, reducing the need for expensive hardware, lowering costs, and making it easier to set up. While it's a huge step forward, there are still some kinks to work out. Researchers are actively working on improving the accuracy of location data, making sure it doesn't use up too much battery, and preventing people from faking their location.

Our system integrates a biometric layer directly into a mobile application to address the vulnerability of location-only systems to proxy attendance. Lightweight deep learning frameworks, including Google's ML Kit and open-source DeepFace, have made it easy to use real-time facial recognition on Android phones. The best part is it won't slow down the device. This feature adds an extra layer of security to geofencing, confirming the right student is actually at the location.

Making the sign-in process easier for users is just as important as making our attendance tracking more accurate. If we want people to actually use the system, we need to move past the old-school username and password logins, which are frustrating and prone to problems like forgotten passwords and phishing scams [13][15]. Consequently, passwordless authentication methods have attracted significant attention. One of the most

prevalent methods for mobile applications is One-Time Password (OTP) verification via SMS. OTP-based systems offer a streamlined login experience because users only need access to their registered mobile numbers. When we use this method, it's easier for you to remember your login information. This, along with other security measures, creates a strong and secure system that lets you log in quickly and often without any hassle.

While the research we've looked at shows a lot of progress, it's clear that each technology has its own weaknesses when used by itself. For example, RFID systems work well but come with a lot of expensive hardware. And while biometric systems are great at confirming someone's identity, they don't do much to show their location. This leaves a loophole for misuse from a distance. On the other hand, geofencing is brilliant for ensuring that a smartphone is within a classroom's virtual boundary, but it can not stop a student from simply handing their phone to a friend to mark them present.

This is precisely the gap that our study addresses. We saw a clear problem: existing systems for student check-in weren't quite enough on their own. Geofencing can tell us a device is in the right location, but it can't tell us if the right person is holding it. On the other hand, facial recognition can verify a person's identity but might not be practical to use all the time. Our approach solves this by combining the best of both worlds. We built a mobile app that first uses power-efficient geofencing to confirm the student is physically in the classroom. Then, to make sure it's really them and not a friend, we add a quick facial verification step right on their device. This gives us a system that is both reliable and simple to use. Finally, to make the entire experience smooth and secure from the very first login, we integrate passwordless OTP authentication, eliminating the hassle of forgotten passwords. We're combining these three technologies to build a strong, hardware-independent solution. It's designed to easily and securely verify a student's presence and identity.

3. System Design

The proposed system has two applications:

1. Android application for the student
2. Web Based teacher’s portal

3.1 Architectural design

The architecture consists of an android application, database and teacher’s portal.

- Android application: The application was developed on Android Studio, which automatically marks the attendance of students when they enter any respective geofence after successful facial verification.
- Database: We used Firebase for authentication and for the Firebase real-time database as our primary database for storing attendance and other user and classroom data. (Fig. 5 & 6 show our database schema.)

  We chose the firebase real-time database as our primary database because it is accessible from multiple client devices, scales across multiple databases, and provides real-time syncing, which stores the data locally in case the student is offline and syncs the local data with the database when online.

- Teacher’s Portal: For the teacher’s portal, we used a React framework called Next.js, which fetches data from the Firebase realtime database and presents attendance and other data in a tabular form.

Ethical Considerations and Data Privacy:

We understand that our system handles sensitive location and biometric data, so we're deeply committed to protecting user’s privacy.

We follow these key principles:

- Informed Consent: Before the users start using the app, we want to make sure you know exactly what data we'll be collecting and that you're comfortable with it. We'll ask for your permission first.

- Data Security: All data is encrypted both when it's being sent to servers (TLS) and when it's stored on them (Firebase server-side encryption). Facial data were not stored as images; instead, only irreversible mathematical embeddings were retained.
- Data Minimization: The system only takes the essential data it needs to run. The location is tracked only after a successful session login and only for attendance.
- Data Retention Policy: At the end of each semester, we securely wipe all attendance records from the system.

Functional Requirements	
Platform	• Web, Android
Student Details	• Name • Student Enrolment Number • Course • Batch
Classroom Information	• Classroom Name • Classroom coordinates • Class start, end time
User Authentication	• Passwordless OTP-based login and per-session facial verification
Automatic Session Termination	• User is logged out upon exiting the main campus geofence

Table 1: Functional requirements for the location based attendance system

Functional Requirements	
Security	• Must prevent proxy attendance and presentation attacks.
Usability	• The daily login/verification flow should take < 30 seconds.
Reliability	• System uptime should be > 99.9%
Scalability	• Must scale and reliably serve more than 5,000+ concurrent users during peak usage.

Table 2: Non-Functional requirements

Tables 1 and 2 depict the functional and non-functional requirements for the application to work as desired.

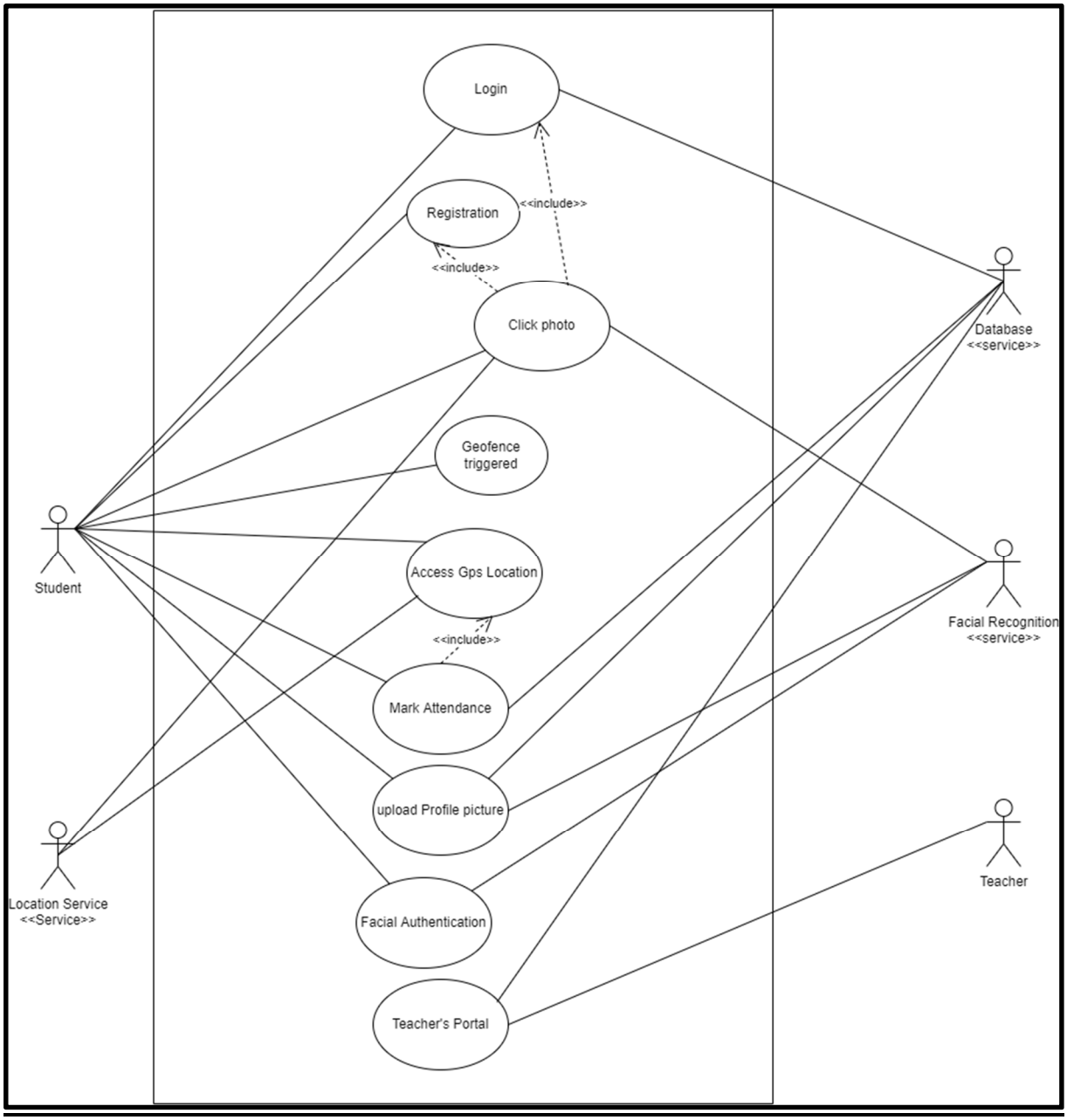

Fig. 1: Use Case Diagram of our application

The use case diagram in fig 1. shows all the user interactions and functioning that takes place in working of this application.

3. 2 Methodology

First, users install the application on their Android device. To begin a new session (once per day), the students entered their registered mobile number. After a user signs up, the system sends a one-time password (OTP) to their phone number via SMS. The user enters this OTP to authenticate the device. After you successfully log in with the OTP, the app will ask you to verify your identity with a face scan. This verification step is required for every new login session to prevent credential sharing and phone hand-offs.

The application captures a live image using the device's front camera to compare it with a pre-registered image of the student stored securely in our database. To verify this, we built a process using DeepFace, a great little open-source library that's both lightweight and powerful. The whole verification process is a multi-stage pipeline that works like this:

1. Face Detection**:** The system first finds the student's face in the captured image, then adjusts it to a standard position, size, and angle. This makes sure the face is perfectly set up for the next step.
2. Facial Embedding Generation: After a face is detected and aligned, a pre-trained deep Convolutional Neural Network (CNN) and the VGG-Face model from the DeepFace framework—process it. This model doesn't just match up pixels. Instead, it creates a unique mathematical signature for a person's face, called a facial embedding. Think of this embedding as a detailed, multi-dimensional fingerprint—a unique vector (like a 128- or 256-number code) that captures all the distinct features of someone's face.
3. Similarity Check: The system then compares the two embeddings to see how closely they match. If the match is close enough, we know it's the right person.
4. A match is confirmed only when the similarity score exceeds a strict threshold. This high bar ensures a reliable and accurate result, minimizing the risk of false positives.

Only upon successful verification is the geofencing service activated for attendance marking. The Firebase real-time database was used to store user details.

Next, the student needs to grant the app permission to use their phone's location. If their location services are off, they'll be prompted to turn them on. Once they give permission, the app automatically finds their current location.

Our app uses your phone's built-in sensors, along with GPS, Wi-Fi, and cell signals, to accurately pinpoint where you are. This multi-source approach is smart about saving batteries; it uses sensors to detect when you are not moving, so it does not have to constantly check your location and waste power. Geofencing Technology automatically marks the attendance of students when they remain in the classroom for a while. This Geofence is characterized by the Latitude and Longitude of the classroom, and its accuracy can be set up by radius. If the student dwells inside the classroom (geofence) exceeding a particular time, attendance will automatically be marked for the respective class. Fig. 3 illustrates the aforementioned geofence transitions.

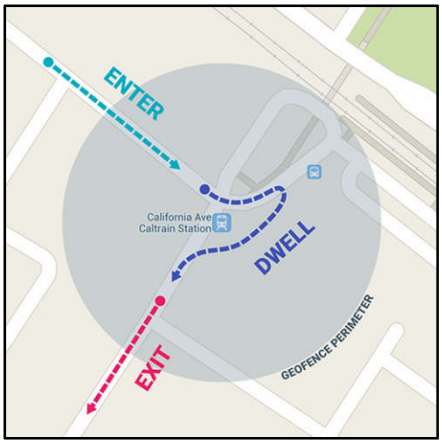

Figure 3: Different Geofence transition events

The attendance history is stored in the firebase real-time database and displayed in the teacher’s portal.

Furthermore, the system monitors the primary geofence around the campus. When the user exits this campus geofence for a predetermined period (e.g., more than 1h, to allow for brief errands), their session is automatically terminated, and they are logged out. This ensures that a new authentication cycle—OTP login followed by facial verification—is required when they return to campus for a new class day.

Potential Issues & Mitigations:

- **GPS Spoofing and Proxy Attendance:** A primary challenge in any location-based system is the potential for GPS spoofing. However, our dual-factor design directly mitigates the most common reason for spoofing, proxy attendance. By requiring mandatory facial verification at the time of check-in, the system ensures that even if a student can spoof their location, they cannot bypass the biometric identity check. This makes proxy attendance infeasible in practice.
- **Battery Consumption:** We used the Geofencing API specifically because it is optimized for low power consumption compared to continuous high-frequency GPS tracking.

4. Results

Results and Analysis

The proposed system was successfully implemented and tested in a real-world campus environment in order to evaluate its performance and reliability. The test involved 25 student volunteers over a period of one week, covering multiple classrooms with pre-configured geofences. The results were analyzed based on accuracy, system latency, and usability.

The application's core functionality is demonstrated in Fig. 4 which show real-time notifications triggered as users enter the geofenced areas for Classrooms. These notifications let us know that our app correctly registered the geofence transition events.

The backend data storage architecture using the Firebase real-time Database proved to be robust and efficient. Figure 4 illustrates the database schema for storing classroom information including its geographical coordinates. Fig. 5 shows the attendance logs, which were timestamped and recorded against student IDs and class names.

Performance Analysis:

To quantify the effectiveness of the system, we measured its accuracy against the geofence radius. A smaller radius increases precision but is more susceptible to GPS drift, whereas a larger radius is more reliable but may incorrectly mark students in adjacent rooms. The 'dwell' time was set to five minutes to ensure that a student had settled in the class before attendance was marked.

Geofence Radius	Successful Detections	False Positives	Missed Detections	Accuracy Rate
15 meters	185	12	18	91.0%
25 meters	201	4	10	95.7%
40 meters	210	15	0	93.3%

Table 3: System Accuracy vs. Geofence Radius (Total 215 test cases)

As shown in Table 3, a radius of 25 meters provided optimal balance, yielding an accuracy of 95.7%. The false positives at this range were minimal, and most issues related to indoor GPS signal inaccuracies were successfully avoided. The 40-meter radius led to an increase in false positives, where students in nearby corridors were sometimes marked as present.

System Latency:

Latency was measured as the time taken from a student entering the geofence to the attendance logged into the Firebase database. The mean latency was recorded as 12.5 seconds. This is well within acceptable limits, as attendance is confirmed only after a 5-minute dwell period, making the initial detection delay negligible.

User Identity Verification:

The facial recognition module was tested to verify its accuracy and user experience. The system correctly authenticated the registered users in over 99% of test cases under various lighting conditions. The verification process added an average of 2.8 seconds to the check-in flow, which was deemed a quick and non-intrusive step by the student volunteers.

The results confirmed that the combined geofencing and facial recognition approach is highly effective for automated and secure attendance.

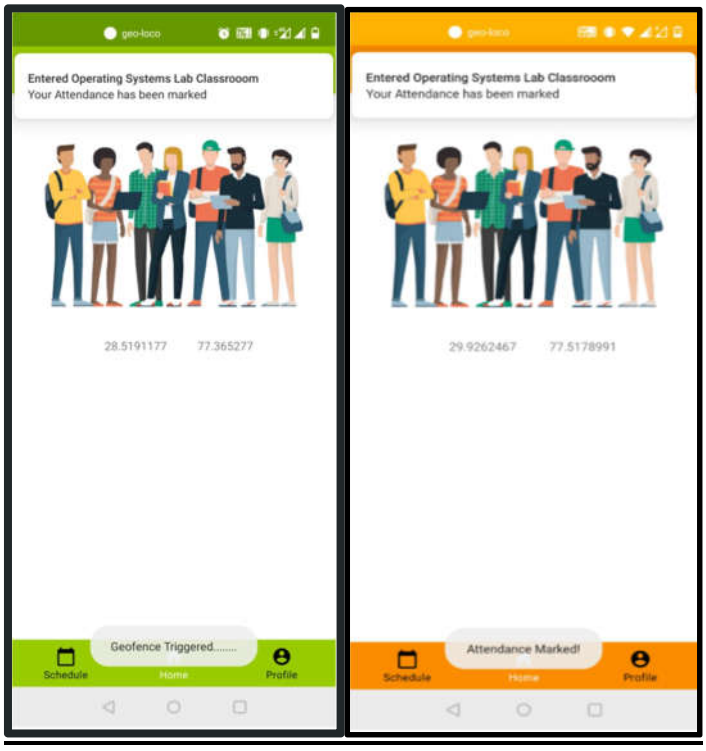

Fig. 4: Real-time notification confirming attendance.

Fig. 5: Database Schema showing the attendance

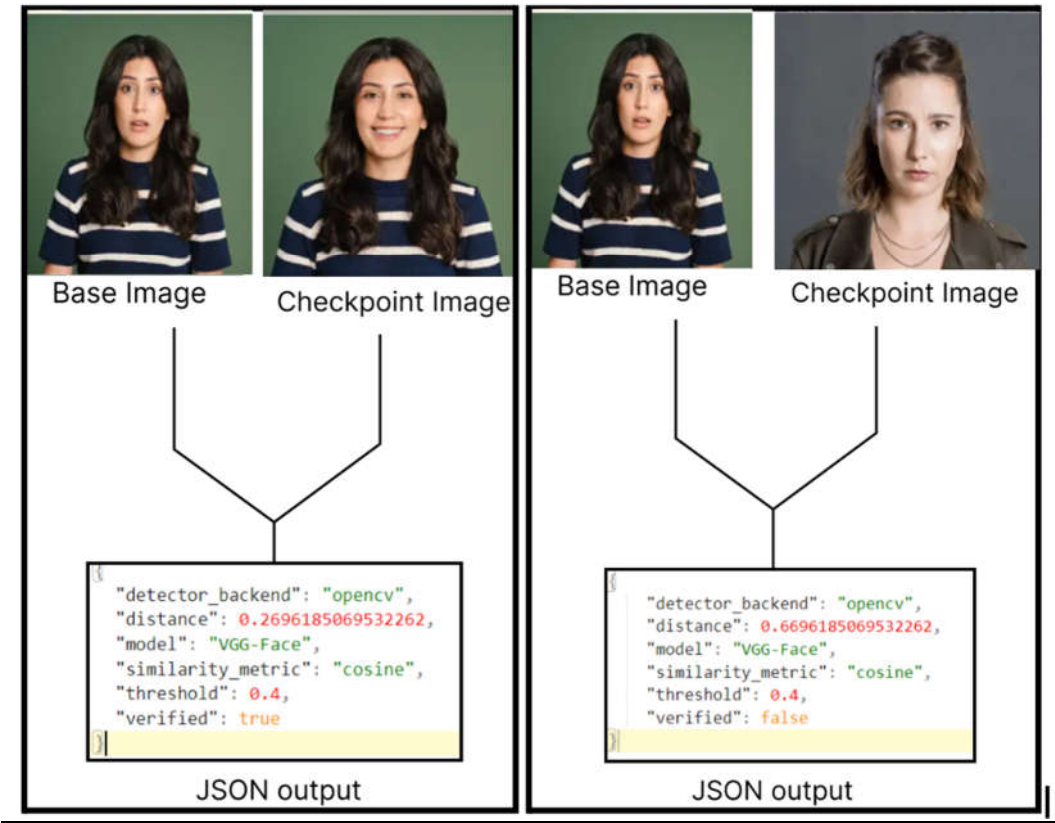

Fig. 6: Output fetched from API calls

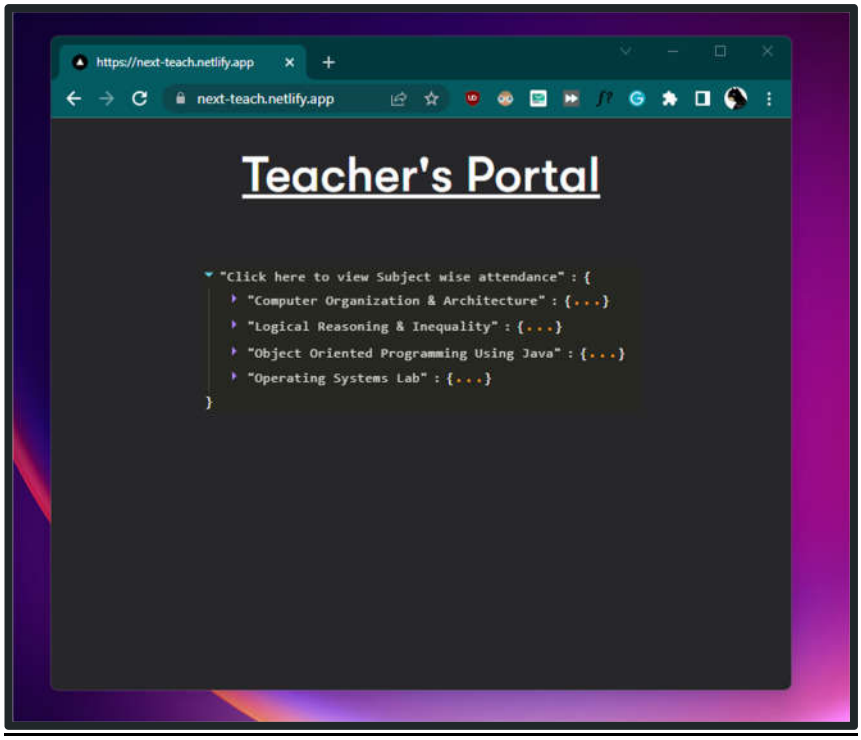

Fig. 7: Teacher's Portal

The JSON output received from various API calls are shown in Fig. 6. The look and features of how the portal will appear to a teacher login is show in Fig. 7.

5. Conclusion

Our application successfully tracks the location of the students and automatically marks them present after they dwell in the geofence for a particular amount of time. User data were also successfully retrieved from the backend. The integration of facial recognition directly addresses the critical flaw of proxy attendance, which is a vulnerability present in location-only systems. This implementation has a positive impact on the management of educational institutes and is a full-proof method to ensure authenticity by removing unfair means while marking attendance by verifying both the student's location via geofencing and their identity via facial recognition.

Automatic Attendance Marking System	Traditional Attendance Marking System
• Records all the data automatically, verifies identity	• Manual marking of attendance
• Provides accurate, proxy-proof results	• Possible human errors
• Saves time because attendance is marked parallelly	• Attendance is marked in one by one fashion
• Saves money, improves productivity	• System cost
• Easy to use	• Ineffective and outdated

Table 4: A Comparison Between Proposed Model and Traditional System Proposed System

6. Limitations and Future Work

No system is without limitations. This research provides a robust proof-of-concept, but further work is required for enterprise-level deployment.

Limitations:

- This study was limited by its small sample size of 25 volunteers.
- Network Dependency: System performance in areas with persistently poor or no network connectivity has not been extensively tested, although Firebase offers offline data caching.

Future Work:

- Scalability Testing: Conduct a large-scale pilot with thousands of users to test the firebase backend and optimize the performance.
- Liveness detection: The facial verification system could be tricked by a high-quality picture or video of the student. To counter this, we can introduce the concept of liveness detection. It is a set of techniques to ensure that the biometric sample is from a live, physically present person. Simple methods include asking the user to do a challenge-response action, like blinking, smiling, or slightly turning their head. The camera of the application analyzes the video feed to confirm this action.
- Integration with University Systems: Develop a secure API to push verified attendance data directly into the institution's official Student Information System (SIS).
- Evaluate demographic fairness by benchmarking false match (FMR) and false non-match (FNMR) rates across sex, race, and age groups, following the NIST FRVT methodology.
- Explore fair score normalization methods demonstrated to reduce gender bias by up to 82%.

References

1. Android Developer Guide: http://developer.android.com/guide/index.html
2. Android API: http://developer.android.com/reference/packages.html
3. Android Developers blog: http://android-developers.blogspot.com/
4. Time and Attendance. [Online]. Available: http://www.en.wikipedia.org
5. Automated Time and Attendance System. Available: http://www.gatekeepersolutions.com
6. K. Ishaq and S. Bibi "IoT Based Smart Attendance System Using RFID: A Systematic Literature Review," *arXiv preprint* arXiv:2308.02591, Aug. 2023. [Online]. Available: https://arxiv.org/abs/2308.02591
7. T. H. Abadal-Salam, T. A. Taha, S. R. Ahmed, S. A. Ahmed, O. K. Ahmed and H. Desa, “Automated RFID-Based Attendance and Access Control System for Efficient Workforce Management,” in Proc. 2023 7th International Symposium on Innovative Approaches in Smart Technologies (ISAS), Istanbul, Türkiye, 2023, doi: 10.1109/ISAS60782.2023.10391615.
8. “Biometric Attendance System Using Face Recognition,” in Proc. 2024 OPJU International Technology Conference (OTCON) — Smart Computing for Innovation and Advancement in Industry 4.0, Raigarh, India, June 2024, doi: 10.1109/OTCON60325.2024.10688314.
9. Smitha; Pavithra S. Hegde; Afshin, “Face Recognition based Attendance Management System,” International Journal of Engineering Research & Technology (IJERT), vol. 9, no. 5, May 2020. DOI: 10.17577/IJERTV9IS050861.
10. D. Joshi, P. Patil, V. Singh, et al., “Face Recognition Based Attendance System,” in Proc. 2023 5th Biennial International Conference on Nascent Technologies in Engineering (ICNTE), Navi Mumbai, India, 2023, pp. 1–6, doi: 10.1109/ICNTE56631.2023.10146718.
11. A. R. S. Siswanto, A. S. Nugroho, and M. Galinium, “Implementation of face recognition algorithm for biometrics based time attendance system,” in Proc. 2014 International Conference on ICT For Smart Society (ICISS), Bandung, Indonesia, 2014, pp. 149–154, doi: 10.1109/ICTSS.2014.7013165.
12. Y. Shevchenko and U.-D. Reips, “Geofencing in location-based behavioral research: Methodology, challenges, and implementation,” Behavior Research Methods, vol. 56, 2024. doi: 10.3758/s13428-023-02213-2.

13. A. Shaji George, “The Dawn of Passkeys: Evaluating a Passwordless Future,” *Partners Universal* Innovative Research Publication (PUIRP), Feb. 25, 2024. DOI: 10.5281/zenodo.10697886. [Online]. Available: https://zenodo.org/records/10697886.
14. Z. Alkhalil, C. Hewage, L. Nawaf and I. Khan, “Phishing Attacks: A Recent Comprehensive Study and a New Anatomy,” Frontiers in Computer Science, vol. 3, art. 563060, Mar. 2021, doi: 10.3389/fcomp.2021.563060. [Online]. Available: https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full.
15. T. Oduguwa and A. Arabo, “A Review of Password-less User Authentication Schemes,” arXiv preprint arXiv:2312.02845, Dec. 2023. [Online]. Available: https://arxiv.org/abs/2312.02845.
16. C. Y. Huang, S. Ma and K. Chen, “Using one-time passwords to prevent password phishing attacks,” Journal of Network and Computer Applications, vol. 34, no. 4, pp. 1292–1301, 2011, doi: 10.1016/j.jnca.2011.02.004.
17. R. Azhaguraj, P. A. Kumar, S. Kadalarasan, K. Karthick, and G. Shunmugalakshmi, “Smart Attendance Marking System using Face Recognition,” in Proc. 2022 6th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2022, doi: 10.1109/ICOEI53556.2022.9776879
18. B. K. Mohamed and C. V. Raghu, “Fingerprint attendance system for classroom needs,” in Proc. Annual IEEE India Conference (INDICON), Kochi, India, Dec. 2012, pp. 433–438, doi: 10.1109/INDCON.2012.6420657
19. A. Qaiser and S. A. Khan, “Automation of Time and Attendance using RFID Systems,” in Proc. International Conference on Emerging Technologies (ICET), Peshawar, Pakistan, Nov. 2006, pp. 60–63, doi: 10.1109/ICET.2006.335928
20. D. B., R. R., S. Hariharan and B. Abishek, “A Hybrid Approach to Attendance Monitoring: Combining Geo Location and Facial Verification,” in Proc. 2024 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS), 2024, doi: 10.1109/ICPECTS62210.2024.10780068.