

Unifence: A Geofence-Based Hostel Attendance System with Biometric Authentication and Role-Based Access

Devendra Bhavsar
Computer Science & Engineering
JK Lakshmipat University
Jaipur India
devendrabhavsar@jklu.edu.in

Apoorva Dixit
Computer Science & Engineering
JK Lakshmipat University
Jaipur India
apoorvadixit@jklu.edu.in

Pranab Roy
Computer Science & Engineering
JK Lakshmipat University
Jaipur India
pranab.roy@jklu.edu.in

Kartik Sharma
Computer Science & Engineering
JK Lakshmipat University
Jaipur India
kartiksharma@jklu.edu.in

Hafizur Rahaman
Information Technology
IEST Shipur
WestBegal India
rahaman_h@it.iests.ac.in

Anwesha Mondal
Computer Science & Engineering
JK Lakshmipat University
Jaipur India
anweshamondal@jklu.edu.in

Abstract—A system namely “*Unifence*”, - that describes a mobile system for recording hostel attendance – is described in this paper in order to design for detection of proxy attendance for ensuring location-based Realtime verification of students using geofencing and biometric authentication. The system is divided into two major control panel—for students and wardens—both offering distinctive functionalities suited to their respective roles. The main innovations are combining GPS-based geofence tracking, face detection biometrics, and Firebase real-time cloud storage, enclosed into a user-friendly mobile interface. The system carryout strict time windows and location constraints, ensuring only authorized, present users can mark their attendance. This paper also reviews applicable academic work on geofencing and Location-Based Services, (LBS) placing *Unifence* within the wide perspective of mobile computing in academic institutions.

Keywords—*Unifence, Geofencing, firebase, biometrics, Location-Based Services (LBS)*

I. INTRODUCTION

There are several challenges in attendance Management for residential college campuses. These may be proxy attendance, unmonitored entry/exits, and the loads of manual records. There are prospects of resolving the aforesaid issues using advances in geolocation technologies and mobile biometrics,

Unifence handles these challenges by providing:

- enforcement of Geofencing (student must be physically present within hostel premises)
- Validation using Biometrics (for authenticity)
- Role-based dashboards (for students and for wardens)
- Cloud-based data supervision

II. LITRATURE REVIEWS

Inspiration and technological grounding are drawn from research on geofencing, biometric authentication, and mobile-based attendance systems.

A. Geofencing and Context-Aware Systems:

Creation of a virtual boundary around a geographic location – termed as virtual geofencing, and it's a core part of many Location-Based Services (LBS). The next frontier in LBSs is shown by Küpper, Bareth, and Freese. They show the integration of geofencing and background tracking [1]. These technologies allow applications to trigger actions when a user enters or exits a geofence, even when the app is running in the background. The enhancement of context

awareness through geofencing is highlighted in this work, that makes the apps smarter and more responsive to user behavior in physical space. Allowed only is the attendance if the user remains inside the geofence during a specific time – in fact it is the principle to be followed in geofencing.

B. Privacy-Aware Geofencing for Behaviour Tracking:

The methods involving geofencing events (like entering or exiting a location) that can be used to trigger app functions (such as surveys or logs) without transmitting the user's actual GPS coordinates was outlined by Shevchenko and Reips [3]. Relevance and privacy were both ensured— a balance achieved by *Unifence* through processing geofence entry locally. Thereby when conditions are met it updates attendance status without uploading location trails.

C. Machine Learning-Enhanced Geofencing Systems:

It was explored by Kumbar. Machine learning with geofencing to make boundary detection smarter was combined in his work [2]. The size and shape of geofences based on user behavior, time, and activity was dynamically adapted by such systems. While ML-based adaptation is not included till now, its structure is flexible enough to incorporate such enhancements in future versions. example, attendance prediction likelihoods or radius adjustment (done automatically) thresholds that optimizes battery usage.

D. Geofencing in Secure and Sensitive Applications:

Criminal monitoring, fleet tracking, and employee location verification are the major application areas for geofencing. The robustness of geolocation triggers can be observed to be of high significance Mane et al. [9] and Coral et al. [5] deploys hybrid models of GPS and Wi-Fi. This like *Unifence* techniques ensures accurate, tamper-resistant boundary detection.

E. Biometric Integration in Secure Attendance Systems:

Corporate and educational settings widely deploy Biometric attendance systems with fingerprint scanning. However, these are often static and hardware dependent. Secure on-device fingerprint verification without storing sensitive data externally is allowed using application of Mobile-based biometric prompts, like those offered by Android's Biometric Prompt API. [10].

F. Mobile-Cloud Integration in Attendance Applications:

Extensively studied are the Cloud-backed mobile systems., supports real-time synchronization, security rules, and scalable access are supported through Firebase noted in [11]. Firebase Firestore are leveraged by Unifence. This ensures instant updating of attendance records to be secured, and available across devices.

Together, these prior studies provide the foundation for Unifence's key innovations: real-time geofence validation, secure biometric access, role-based dashboards, and cloud-native scalability.

III. SYSTEM ARCHITECTURE

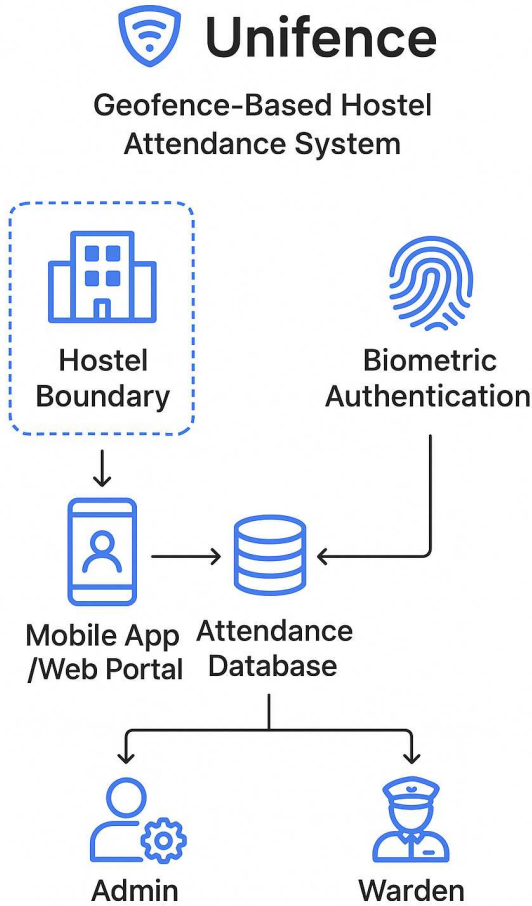


Fig. 1. Basic Architecture of Unifence System

A. Technology Stack

- Platform: Android
- Frontend: XML-based UI with Java/Kotlin logic
- Backend: Firebase Firestore (real-time database), Firebase Authentication
- Geolocation: Google Maps & Android Geofencing API
- Biometrics: Android Biometric Prompt API



Fig. 2. Unifence Home Page for selecting role: Student or Warden

IV. STUDENT WORKFLOW

A. Sign-in / Sign-up

- Students must register using their college-issued email IDs.
- On successful registration, biometric data (fingerprint) is collected and stored locally.

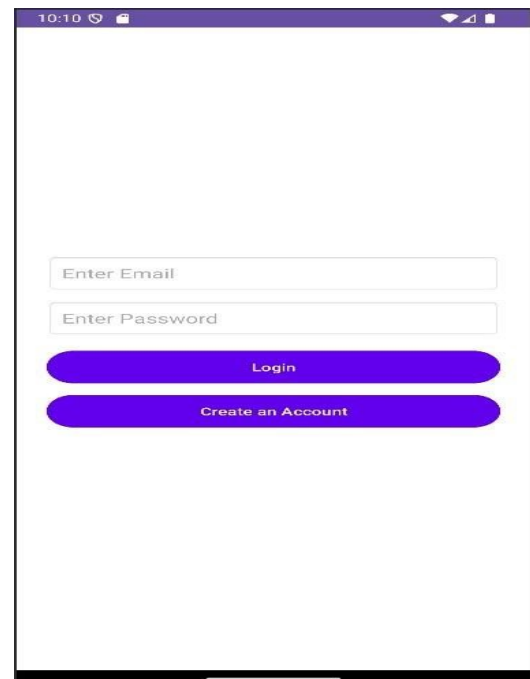


Fig. 3. Email-based log in sign-up screen

B. Student Dashboard

After login, students see:

1. **View Attendance:** Displays historical data from Firebase Firestore in tabular form.

2. **Mark Attendance:** Redirects to a form where students input:

- Name
- Room Number
- Hostel Name

Following this:

- The app checks if the **device is within the geofence**.
- If within the boundary and within the allowed **time slot (10:00–10:30 PM)**:

A fingerprint prompt is triggered.

On successful match, attendance status is updated to

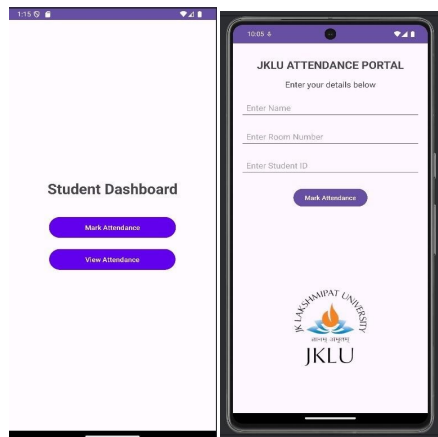


Fig. 4: Student Dashboard and Attendance Form

"Present".

C. Restrictions

- **Time-Locking:** The attendance page is active only during the allowed period.
- **One-Time Marking:** Each user can mark attendance only once per day.
- **Location Check:** Attendance is denied if GPS indicates the user is outside the geofence.
- **Biometric Verification:** checks the user's biometric data, matches and then marks the attendance



Fig. 5. Student Biometric Verification

V. WARDEN WORKFLOW

A. Warden Dashboard Features

1. **View Attendance:** Accesses the same Firestore DB but with editor permissions. Can manually update entries (e.g., marking leave as present).

2. **Set Time:** Allows wardens to set or update the time window for attendance (default is 10–10:30 PM).

3. **Manage Geofence:** Opens a map interface to draw or adjust a **circular geofence** using coordinates.

The system uses Android's Location Manager to define radius and boundaries.

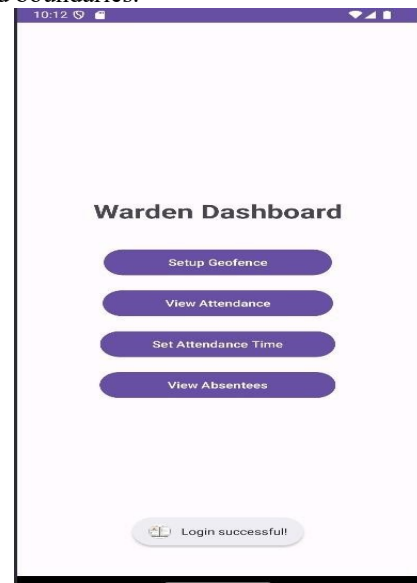


Fig. 6. Warden Dashboard with 4 buttons



Fig. 7. Geofence management map interface

4. View Absentees:

Filters students based on hostel name and date.
Shows a list of those who failed to mark attendance on a given day.

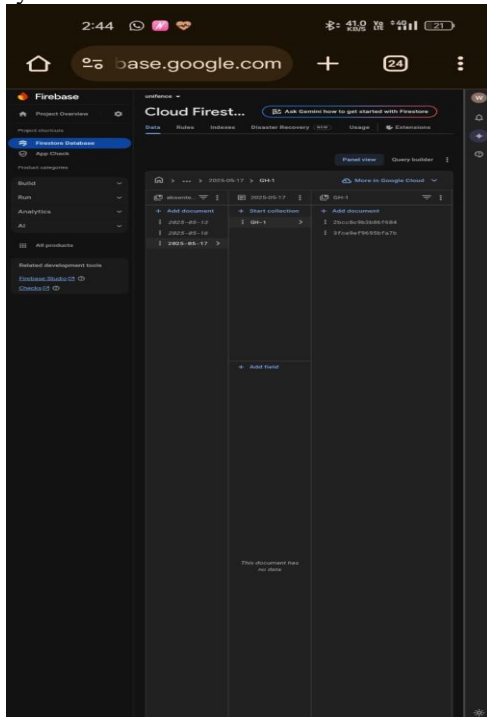


Fig. 7. Absentee report screen with date/hostel filter

- Fingerprint data **never leaves the device**
- Android's secure Keystore API is used for matching

C. Geofencing API

- Maintains a background listener for geofence events
- Notifies app when user enters or exits the defined area
- Energy-efficient: uses Wi-Fi and accelerometer when GPS is off

TABLE I. COMPARATIVE ANALYSIS OF ATTENDANCE SYSTEMS

Feature	Manual System	RFID-Based System	Unifence (Proposed System)
Proxy Prevention	Easily bypassed through roll call or signatures	Can be manipulated if cards are shared	RFID Biometric + Geofence makes proxy marking nearly impossible
Location Verification	No location validation	Can scan card from outside	GPS-based geofence ensures student is physically inside hostel premises
Authentication Method	Verbal confirmation or signature	RFID cards tap only matched at time of attendance	Biometric fingerprint authentication
Time-bound Attendance	Not enforced consistently	Optional via fixed RFID time Readers	Enforced through app logic: Ex. 10:00–10:30 PM only
Dashboard for Admins (Warden)	Paper registers: editing is slow	May have desktop interface with limited control timings	Real-time dashboard to view/edit attendance, configure geofence, set
Attendance Data Management	Stored physically, not easily retrievable	Stored locally or on LAN	Stored securely in Firebase
Scalability	Poor – manual effort increases with scale	Moderate – needs hardware	High – app-based, only software
Tamper Resistance	Low – can be forged	Moderate – tag misuse	High – combines GPS, biometric possible and timed access
Offline Functionality	Works offline	Partially dependent hardware	Requires intermittent internet access for Firebase sync
User Experience (UX)	Tedious, time consuming	Faster than manual but not interactive	Intuitive UI, instant feedback, live records, secure biometrics

VI. DATABASE AND SECURITY MODEL

A. Firebase Firestore

- Real-time syncing of attendance data
- Role-based read/write permissions using Firebase Rules

B. Biometric Security

- GPS Accuracy indoors: Mitigated by allowing some buffer distance around hostels.
- Battery Drain: Optimized by triggering location checks only during active period.

- Network Dependency: Firebase syncs require internet access.

VIII. FIRESTORE DATABASE AND REAL-TIME ARCHITECTURE

Unifence uses Firebase Firestore as its primary backend. Firestore is a NoSQL, document-based real-time database provided by Google that offers several advantages in terms of scalability, security, and live synchronization.

A. Real-Time Data Synchronization

Firestore supports real-time listeners—meaning any changes made to the database (e.g., a student marking attendance, a warden modifying a record) are instantly propagated to all connected clients. This ensures:

- Wardens see the latest updates in attendance as soon as a student record their present in the system.
- Attendance logs are consistent, even across various devices.

This live updating is particularly powerful in educational environments where attendance data must reflect up-to-the-second accuracy, especially in time-restricted scenarios.

B. Role-Based Access Control (RBAC) via Email Invites

One of the latest features of Firestore (via Firebase Authentication + Firestore Security Rules) is its role-based permission system, and it can be modified through email invitations.

C. Roles in Unifence

- Admin: Full access to all data, time settings, and user role assignment.
- Warden (Editor): Can view and edit attendance for their hostel, configure geofence, update timing.
- Student (Viewer): Can only access their own attendance logs and mark themselves present.

This access is enforced by:

- Firebase Authentication: Users must access via verified college emails.
- Custom Claims: Role data is designated in Firebase's backend and enclosed into the user's access token.
- Security Rules: Firestore rules confirms users cannot read or write data prohibited scope.

TABLE II. ADVANTAGES OF USING FIRESTORE IN UNIFENCE

Feature	Description
Scalability	Supports hundreds to thousands of users concurrently without slowdown
Offline Persistence	Automatically syncs data when user reconnects to the internet
Security	End-to-end encryption, access rules, authentication, and audit logs
Role Flexibility	Dynamic permission assignment through email-based invites and custom claims

Realtime Notifications	Enables building alert-based dashboards (e.g., auto alert when student is absent)
Integration	Seamless use with Firebase Cloud Functions, Analytics, and Firebase Hosting

VIII. RESULT OF UNIFENCE SYSTEM TESTING

TABLE III. KEY METRICS FROM PILOT STUDY OF UNIFENCE SYSTEM

Category	Metric	Result / Observation	Remarks / Interpretation
System Performance	Total Check-ins Attempted	600	60 users × 10 days
	Successful Automated Check-ins	582 (97.0%)	High reliability overall
	Geofence Detection Accuracy	96.0%	Accurate GPS-based boundary detection
	Biometric True Acceptance Rate (TAR)	97.5%	Reliable user identity verification
	False Rejection Rate (FRR)	2.1%	Mostly due to wet/damaged fingerprints
	False Acceptance Rate (FAR)	0.34%	Proxy prevention highly effective
	Proxy/ Spoof Attempts Blocked	18 / 20 (90%)	Geo + biometric checks effective
Latency & Efficiency	Median End-to-End Latency	1.2 seconds	Fast user experience
	GPS Fix Time	~0.5 seconds	Variable based on device/network
	Biometric Scan & Match Time	~0.5 seconds	Efficient fingerprint/face match
	Server Sync & Response Time	~0.2 seconds	Stable connection with database
	Battery Consumption Increase	5–7% per day	Acceptable for mobile usage
User Acceptance	User Satisfaction (Rating 4–5)	85%	Majority found system convenient
	Perceived Security (Rating 4–5)	78%	Users trust geo + biometric combo
	Privacy Concerns (Rating 4–5 worried)	12%	Manageable with better transparency
Administrative Feedback	Admin Satisfaction (Rating 4–5)	90%	Found reports accurate and useful
	Ease of Monitoring	High	Real-time logs improved oversight
Failure Analysis	GPS Edge Errors	8 cases	Occurred near building boundaries
	Biometric Scan Failures	12 cases	Due to poor fingerprint quality
	Network Sync Delays	10 cases	Resolved automatically upon reconnect

Summary

- Overall Accuracy: ~95% successful attendance detection

- **Response Speed:** Median latency ~1.2 s per check-in
- **User Acceptance:** 85% satisfied, 78% trust in security
- **Reliability:** Only minor failures at GPS edges and during poor biometric reads

IX. CONCLUSION AND FUTURE SCOPE

Unifence comes up with a secured, intelligent, and trustworthy attendance system for Hostel. By combining biometric(Face Detection) authentication with geofencing and real-time database tools, the system establishes advanced standard for Hostel attendance monitoring. Future work may include:

- Admin analytics panel for trends
- ERP integration for reporting
- SMS/email alerts for absentees
- Optional machine learning to predict attendance patterns

REFERENCES

- [1] A. K pper, J. Freese, and U. Bareth, "Geofencing and background tracking: The next features in LBS," INFORMATIK 2011, Lecture Notes in Informatics, 2011.
- [2] C. Kumbar, "Geo fencing system using machine learning," International Journal of Research Publication and Reviews (IJRPR), 2024.
- [3] A. Shevchenko and U.-D. Reips, "Geofencing in location-based behavioral research," Behavior Research Methods, vol. 56, no. 1, pp. 233–245, 2024.
- [4] J. Hinds, E. J. Williams, and A. N. Joinson, "Contextual behavior and smartphone usage: A study of geofencing to measure context-dependent behavior," J. Behavioral Addictions, vol. 11, no. 1, pp. 45–56, 2022.
- [5] J. Coral et al., "Geo-fencing intervention around gambling establishments: A mobile solution to behavioral risk," J. Med. Internet Res., vol. 22, no. 4, p. e14915, 2020.
- [6] F. Naughton et al., "Context-triggered support to reduce smoking lapses: A randomized controlled trial using geofencing," Addiction, vol. 111, no. 11, pp. 2153–2161, 2016.
- [7] P. Wright et al., "Geofencing in health promotion: A case study in dental care awareness," BMC Public Health, vol. 21, no. 1, p. 456, 2021.
- [8] F. Besoain et al., "Designing a mobile geofencing app to support HIV prevention: The UBESAFE app," IEEE Access, vol. 8, pp. 103122–103132, 2020.
- [9] M. Mane et al., "Geofencing-enabled crime alert system using mobile apps," Procedia Comput. Sci., vol. 185, pp. 705–712, 2021.
- [10] A. Alzahrani and C. Perera, "A survey on access control in the Internet of Things," J. Netw. Comput. Appl., vol. 124, pp. 1–21, 2019.
- [11] Google Firebase Documentation, "Secure your data in Cloud Firestore," 2023. [Online Cited on July 21, 2025]. Available: <https://firebase.google.com/docs/rules>