# MOBILE BSED BIOMETRIC ATTENDANCE SYSTEM

RAJSABARI K P 1, SUBASH B K 2, LOGANANTH A 3, SATHYAMOORTHY J 4

*1 Student, Dept. of Information Technology, Bannari amman Institute of Technology, Tamil Nadu, India 2 Student, Dept. of Information Technology, Bannari amman Institute of Technology, Tamil Nadu, India3 Student, Dept. of Information Technology, Bannari amman Institute of Technology, Tamil Nadu, India 4 Professor, Dept. of Computer Science and Engineering, Bannari amman Institute ofTechnology, Tamil Nadu, India*

## ABSTRACT

*Utilizing the widespread use of smartphones and biometric technology, mobile-based biometric attendance systems simplify the process of tracking attendance in a variety of contexts. For precise identification, this approach makes use of each person's distinct biological traits, such as fingerprints or facial features. Employees or students register their biometric data with a mobile application, which securely saves the data, as part of the abstraction process. In order to record attendance, users must first authenticate themselves using the mobile app and their registered biometric data. A centralized database is then notified of the user's presence. The technology lowers the possibility of proxy attendance, increases efficiency, does away with the need for physical attendance registers, and offers real-time tracking. It also provides accessibility and flexibility, enabling users to record attendance from a distance or in different places. In order to manage attendance effectively, businesses and educational institutions can look to mobile-based biometric attendance systems as a contemporary and dependable solution.*

**Keyword***: Mobile-Biometric-Attendance-System Smartphone*

## 1. INTRODUCTION

The way that businesses track and manage employee attendance has been completely transformed by mobile-based biometric attendance technologies. This cutting-edge technology offers a seamless and effective solution for attendance management by fusing the precision and security of biometric authentication with the portability of mobile devices. In-depth discussions of the features, advantages, and ramifications of mobile-based biometric attendance systems for contemporary workplaces are provided in this article.

Conventional approaches to record attendance, including card-based scan systems or manual entry systems, are vulnerable to fraud, time theft, and mistake. Furthermore, they frequently involve administrative overhead and extra hardware infrastructure requirements. In order to overcome these difficulties, mobile-based biometric attendance systems make use of people's distinct biological characteristics and the widespread use of smartphones for authentication. Biometric authentication technology, which confirms people's identities based on their physiological or behavioral traits, is the foundation of mobile-based biometric attendance systems. These systems frequently employ iris scanning, voice recognition, facial recognition, and fingerprint recognition as biometric modalities. Mobile-based attendance apps ensure that only authorized personnel may clock in and out, hence removing the chance of buddy punching and time theft. This is achieved by recording and analyzing these distinct biometric signals. Biometric authentication technology, which confirms people's identities based on their physiological or behavioral traits, is the foundation of mobile-based biometric attendance systems. These systems frequently employ iris scanning, voice recognition, facial recognition, and fingerprint recognition as biometric modalities. Mobile-based attendance apps ensure that only authorized personnel may clock in and out, hence removing the chance of buddy punching and time theft. This is achieved by recording and analyzing these distinct biometric signals.

Second, mobile biometric attendance solutions are incredibly practical and easy to use. With just their cellphones, workers can sign in and out without any additional hardware or access cards. Employees and administrators both benefit from this expedited procedure, which lessens the administrative load that comes with using more conventional approaches to manage attendance. In addition, mobile apps for attendance provide administrators with instant access to staff attendance data, enabling them to track attendance trends, spot patterns, and create thorough reports. Organizations may make well-informed decisions about scheduling optimization, labor management, and resource allocation with this data-driven strategy. Since mobile-based biometric attendance systems enable employees to report their attendance from any place with internet connectivity, they are especially advantageous for firms with remote or mobile workforces. Employees may easily use their smartphones to enter their attendance, whether they are working from home, traveling, or attending off-site meetings. This ensures smooth tracking and adherence to company standards. The use of mobile-based biometric attendance systems, however, also brings up significant issues with data security, privacy, and regulatory compliance. It is imperative for organizations to guarantee that biometric data is gathered, retained, and handled in compliance with applicable privacy laws, such as the California Consumer Privacy Act (CCPA) in the US and the General Data Protection Regulation (GDPR) in Europe. Furthermore, to protect biometric data from misuse or unauthorized access, strong security mechanisms including access limits, authentication procedures, and encryption must be put in place.

## 2.RELATEDWORKS

**M. A. Meor Said et al, (2014)** studied that a fingerprint identification system for student attendance is provided, which enables students to track their presence in class online. It can lessen the number of fraudulent students, who are now primarily completed by the students themselves.

**H. N. Monday, I. D. Dike et al, (2018)** said that both the public and private sectors have seen a significant level of impersonation on a daily basis. Everything that can be assessed about a human being is considered biometrics. A person's fingerprints are a unique biometric type of identification that remain constant throughout their lives.

**B. Soewito, F. L. Gaol et al, (2018)** said that the existing method in place for attendance still has flaws. The first is the lengthy lines that form in front of the attendance machine as employees arrive and depart from work. The second is cheating; an employee may ask a buddy to complete the attendance form. The third is that, for the most part, the attendance system is not linked to the finance department's or human resources software's payment system. The fourth is that workers who are not in the office are unable to complete the attendance procedure.

**X. Zhang, T. He et al, (2019)** said that as mobile Internet technology advances, smartphones running on the Android operating system dominate the market. The problem of smartphone information leaking cannot be solved by conventional encryption technology; instead, Android-based authentication systems with biometric identification are emerging as a more dependable source of information assurance.

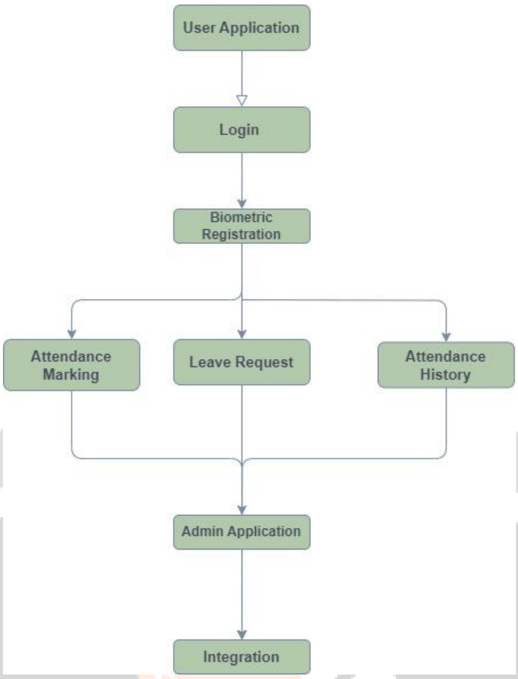
**Dey *et* al., (2014)** said that Users contact a few predetermined cell phones to gain access to the system. A new user is guided through the registration process using an interactive voice response (IVR) system, while an enrolled user is guided through the verification steps. For user authentication, the system employs i-vector based speech modelling and text independent speaker verification with MFCC capabilities. The effects of session/environment variables are normalized using within class.

## 3. OBJECTIVE

- The careful selection of appropriate biometric authentication technologies is the first stage in putting the mobile-based biometric attendance system into operation.
- This entails assessing several solutions, such as facial recognition, iris scanning, or fingerprint scanning, taking accuracy, dependability, and interoperability with mobile devices into account. The creation of an intuitive mobile application starts as soon as the right technology is selected.
- Using platform such as Android Studio and framework like Spring Boot the application is made to make it easy for staff members to record their attendance by using their biometric characteristics.
- Biometric systems prioritize security, and strong security controls are in place to protect sensitive biometric information.
- This involves putting in place safe enrollment procedures to collect and safely store biometric data from workers. Biometric data is protected during transmission and storage via encryption techniques, reducing the possibility of data breaches or illegal access.
- The privacy and integrity of employee data are preserved by ensuring compliance with data protection laws during the development and deployment stages
- Administrators can instantly obtain attendance records thanks to real-time data synchronization techniques included into the system.
- This makes it possible to track attendance status effectively and make labor management decisions on time. Thorough user assistance and training are crucial steps in the implementation process. Staff members receive instruction on utilizing the mobile application for biometric attendance tracking, guaranteeing their familiarity with and comprehension of the technology's features.
- In order to handle any problems or queries that may come up throughout the system's adoption and use, ongoing technical assistance is also offered.

## 4. PROPOSED WORK

### 4.1 FLOW CHART



### 4.2 DATA COLLECTION AND PREPARATION

Users like IT staff, administrators, employees, and other stakeholders provide input, requirements, and user insights during the data collection process for mobile-based biometric attendance systems using Admin application. Mobile survey solutions are used to conduct surveys in order to facilitate this process, enabling stakeholders to conveniently submit feedback from their mobile devices. Using admin application to collect the data from the user like employees or students Storing their information manually in database. Providing information to admin easy can put attendance in the admin application. Admin application used for real time data collection.

To guarantee the strength and integrity of the application's security features, extensive security testing was carried out during the development phase of the mobile-based biometric attendance application. The security testing operations are described in this paper, along with the methodologies employed, the test cases that were run, the results, and the mitigation techniques.

**Methodologies for Security Testing:** A combination of penetration testing, white-box testing, and black-box testing were used in the security testing process. In order to evaluate the application's behaviour from the viewpoint of the end user without being aware of its internal workings, black-box testing was utilized. In order to find potential vulnerabilities, white-box testing entailed examining the source code and architecture of the program. To replicate actual assaults and assess the application's resistance to different security risks, penetration testing was done.

**Tests and Scenarios:** To address several facets of security, such as authorization, data encryption, network security, and authentication, a thorough collection of test cases and scenarios was created. Test scenarios included confirming that biometric authentication methods function as intended, making sure data is transmitted securely over the network, and evaluating access controls to stop unauthorized users from accessing private data.

### 4.3 SELECTION OF COMPONENETS

**User Interface (UI):** By utilizing Google's Material Design for Buttons and Other UI Components, a user-friendly and intuitive user interface is created to guarantee.

**Database:** Used a reliable database system, Firebase, Realm Databases, to hold secure information users, and organization programs. The data will be stored in Realm Database and synchronized to the cloud using Firebase on mobile devices.

**Connectivity:** Using firebase and realm features, the program may function both online and offline as many rural regions may have spotty internet access.

**Analytics and Reporting:** Include analytical tools to provide reports and insights from the gathered data, assisting farmers and decision-makers.

**Mobile App Development Framework:** Application created as in native mobile application using Android Studio.

**Programming Language:** For the backend process, Java and Kotlin, Spring framework were used. Google Material Design was utilized on the front end.

**Management System:** For effective data storage and retrieval, choose a dependable DBMS like Firebase or Realm.

**Authorization:** Google Authorization and Firebase were both used for authorization and Spring Security. The app's user can log in using an existing email.

## 4.4. USER INTERFACE DEVELOPMENT

The user interface (UI) development for a mobile-based biometric attendance application necessitates a seamless and intuitive design to ensure user adoption and satisfaction. The UI should prioritize simplicity and efficiency, with clear navigation and minimalistic yet informative layouts. Key components include a user-friendly login screen with biometric authentication options, such as fingerprint or facial recognition, for enhanced security and convenience. Once logged in, the main dashboard should display relevant information like attendance records, upcoming schedules, and any notifications. A smooth and responsive interface is crucial, allowing users to easily mark attendance, view past records, and make any necessary updates. Additionally, incorporating features like real-time attendance tracking and push notifications for reminders can enhance the user experience. Customization options for personal preferences and accessibility features should also be integrated to cater to diverse user needs. Through thoughtful UI design, the mobile biometric attendance application can offer a seamless and efficient experience for both administrators and users alike.

## 4.5. TASK ORGANIZATION AND REPORTING

Task organization and reporting for a mobile-based biometric attendance application involve efficient management of tasks and generation of comprehensive reports. This encompasses scheduling shifts, assigning tasks to employees, and tracking attendance data. The application should facilitate easy organization of tasks through intuitive interfaces, allowing administrators to allocate resources effectively. Additionally, robust reporting features enable the extraction of valuable insights, such as attendance trends and employee performance metrics. By streamlining task organization and reporting, the application enhances productivity and facilitates informed decision-making for businesses.

## 5. RESULT ANALYSIS

Result analysis for a mobile-based biometric attendance application involves examining various metrics and data points to derive insights into attendance patterns, employee behavior, and system performance. Firstly, the application should provide detailed reports on attendance records, including attendance rates, tardiness, and absenteeism trends over time. Administrators can analyze this data to identify patterns and address any issues related to attendance compliance. Moreover, the biometric data collected by the application can be analyzed to detect anomalies or discrepancies, such as instances of buddy punching or unauthorized access attempts. This analysis enhances security measures and ensures the integrity of attendance data. Furthermore, result analysis may involve comparing attendance data with other relevant factors, such as project timelines, workload distribution, or external factors like weather conditions or public holidays. This allows businesses to correlate attendance patterns with productivity levels and make informed decisions regarding resource allocation and scheduling.

Additionally, user engagement metrics, such as app usage frequency and feature utilization, can be analyzed to gauge user satisfaction and identify areas for improvement in the application's usability and functionality. Overall, result analysis for a mobile-based biometric attendance application enables businesses to optimize workforce management strategies, improve operational efficiency, and ensure compliance with attendance policies.

## 6. FUTURE WORK

Future work for mobile-based biometric attendance applications involves further enhancing security measures, expanding biometric authentication options, and integrating advanced analytics capabilities. To bolster security, continuous advancements in biometric technology should be leveraged, such as multi-modal biometrics combining facial, fingerprint, and iris recognition for heightened accuracy and fraud prevention. Additionally, exploring blockchain technology for storing and verifying biometric data can enhance data integrity and privacy protection. Furthermore, future iterations of the application could integrate predictive analytics to forecast attendance patterns and optimize staffing levels accordingly. Moreover, incorporating machine learning algorithms can help in identifying anomalies or suspicious activities in attendance records, improving overall system reliability. Collaborations with academic and industry partners can drive research and development efforts to push the boundaries of innovation in mobile-based biometric attendance applications, ultimately leading to more robust, efficient, and secure solutions for businesses and organizations.

## 7. CONCLUSION

In conclusion, the development and implementation of a mobile-based biometric attendance application offer significant benefits to organizations seeking efficient workforce management solutions. By harnessing the power of biometric technology, this application ensures accurate and secure attendance tracking while enhancing user convenience through mobile accessibility. The user interface design prioritizes simplicity and functionality, facilitating seamless interaction for both administrators and employees. Task organization and reporting features streamline workflow management and provide valuable insights for informed decision-making. Overall, the application optimizes resource allocation, improves productivity, and fosters a culture of accountability within the organization. As businesses continue to embrace digital transformation, investing in a mobile-based biometric attendance application emerges as a strategic imperative for modern workforce management. Its ability to enhance efficiency, security, and user experience makes it an invaluable tool in today's dynamic business landscape, empowering organizations to thrive in an increasingly competitive environment.

## 8. REFERENCES

[1] B. Soewito, F. L. Gaol, E. Simanjuntak and F. E. Gunawan, "Attendance system on Android smartphone," 2015 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC), Bandung, Indonesia, 2015, pp. 208-211, doi: 10.1109/ICCEREC.2015.7337046.

[2] B. Soewito, F. L. Gaol, E. Simanjuntak and F. E. Gunawan, "Smart mobile attendance system using face recognition and fingerprint on smartphone," 2016 International Seminar on Intelligent Technology and Its Applications (ISITIA), Lombok, Indonesia, 2016, pp. 175-180, doi: 10.1109/ISITIA.2016.7828654.

[3] Adal, N. Promy, S. Srabanti and M. Rahman, "Android based advanced attendance vigilance system using wireless network with fusion of bio-metric fingerprint authentication," 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, Korea (South), 2018, pp. 1-2, doi: 10.23919/ICACT.2018.8323701.

[4] S. U. Masruroh, A. Fiade and I. R. Julia, "NFC Based Mobile Attendence System with Facial Authorization on Raspberry Pi and Cloud Server," 2018 6th International Conference on Cyber and IT Service Management (CITSM), Parapat, Indonesia, 2018, pp. 1-6, doi: 10.1109/CITSM.2018.8674293.

[5] H. N. Monday, I. D. Dike, J. P. Li, D. Agomuo, G. U. Nneji and A. Ogungbile, "Enhanced attendance Management System: A Biometrics System of Identification Based on Fingerprint," 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2018, pp. 500-505, doi: 10.1109/IEMCON.2018.8614776.

[6] X. Zhang, T. He and X. Xu, "Android-Based Smartphone Authentication System Using Biometric Techniques: A Review," 2019 4th International Conference on Control, Robotics and Cybernetics (CRC), Tokyo, Japan, 2019, pp. 104-108, doi: 10.1109/CRC.2019.00029.

[7] J. R. Kwapisz, G. M. Weiss and S. A. Moore, "Cell phone-based biometric identification," 2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), Washington, DC, USA, 2010, pp. 1-7, doi: 10.1109/BTAS.2010.5634532.

[8] A. S. Shahab and R. Sarno, "Android Application for Presence Recognition based on Face and Geofencing," 2020 International Seminar on Application for Technology of Information and Communication (iSemantic), Semarang, Indonesia, 2020, pp. 208-213, doi: 10.1109/iSemantic50169.2020.9234253.

[9] H. Tok, N. S. Batur, R. Tüzen, H. İ. Yıldırım and S. Demirci, "A Novel ZigBee Based Mobile Fingerprint Student Attendance System," 2019 4th International Conference on Computer Science and Engineering (UBMK), Samsun, Turkey, 2019, pp. 492-497, doi: 10.1109/UBMK.2019.8907221.

[10] Chennattu, Sebastian, Aditya Kelkar, Aaron Anthony and Sushma Nagdeote. "Portable Biometric Attendance System " 2019 4th International Conference on Information Systems and Computer Networks (ISCON) (2019): 245-249.