International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

MOBILE APP APPLICATION TO REGISTER BIOMETRIC

PONDEPPA B , SOWMYADEVI T , SOWNDARYA S

[1]*Studuent,Dept.ofElectronicsandCommunicationEngineering,AnnaUniversity,IN*
[2]*Studuent,Dept.ofElectronicsandCommunicationEngineering,AnnaUniversity,IN*
[3]*Studuent,Dept.ofElectronicsandCommunicationEngineering,AnnaUniversity,IN*

Abstract - *The development of a mobile application designed for secure biometric registration and authentication, utilizing Firebase as the backend database. The application aims to streamline user login processes by incorporating biometric features such as fingerprint and facial recognition, enhancing both security and user experience. The application is developed by using Kotlin for the Android platform, making the most of its modern language features for efficient coding practices. Java is employed for specific backend functionalities, ensuring tough manner capabilities. XML is utilized for designing default user interfaces, making the app visually attractive and user-friendly. Key functionalities include user registration, biometric data capture, and secure login mechanisms. By integrating Firebase Authentication and Fire Store, the app ensures secure storage and management of user data, while also supporting real-time data synchronization. This application addresses the growing demand for secure authentication methods in mobile applications, providing a seamless login experience while safeguarding sensitive user information. The proposed solution not only enhances security but also contributes to the convenience of mobile users in an increasingly digital world.*

IndexTerms— *Biometric Authentication, Firebase Database, User Registration, Kotlin, Java, XML Layouts, Fingerprint Recognition, Facial Recognition, User Interface (UI)Design,Secure Login*

1. INTRODUCTION

In today's rapidly evolving technological landscape, the need for secure and efficient identity verification methods has become increasingly critical. This focuses on the development of a mobile application designed to register biometric data based on specific geographic locations. The application aims to provide an innovative solution for identity authentication, particularly in scenarios where location context is essential. By enabling users to securely log in and store their biometric information such as fingerprints and facial recognition data tied to their current physical location, the app enhances both security and user experience.

Utilizing Firebase as the backend infrastructure, the application ensures robust data management through Firebase Authentication and Fire store. Firebase provides real-time data synchronization, allowing users to seamlessly access their biometric information across multiple devices. The integration of Firebase Authentication ensures that user accounts are secure and that sensitive data is protected from unauthorized access. This backend solution is not only scalable but also reliable, making it an ideal choice for applications that require secure data storage.The choice of Kotlin for Android development is significant, as it allows for a modern and brief coding experience. Kotlin features enhance code safety and reduce the possibility of errors, which is crucial when handling sensitive biometric data. Additionally, Java is employed for specific backend functionalities, allowing developers to strong existing libraries and tools that are well-established in the Android ecosystem. This combination of programming languages ensures that the application is both powerful and efficient. XML is utilized for designing the user interface, enabling the creation of automatic and visually layouts. A well-designed interface is essential for enhancing user experience, making navigation ideal and interactions straightforward. The application will feature a user-friendly layout that guides users through the biometric registration process, ensuring clarity and ease of use. Special attention will be given to accessibility, ensuring that users of all backgrounds can interact with the app effectively.

1.1 Background of the Work

The biometric authentication methods, such as facial recognition and fingerprint scanning, alongside a One-Time Password (OTP) mechanism for enhanced security. Developed using Kotlin and Java, the app leverages Firebase for secure user authentication and real-time data storage. GPS integration ensures that biometric registration and door unlocking occur within authorized locations. This combination of technologies creates a robust and user-friendly smart door locking system focused on security and convenience

1.2 Motivation and Scope of the Proposed Work

Biometric registration in colleges is an innovative solution to streamline and enhance administrative processes such as student attendance tracking, access control, and identity verification. Traditional methods, like manual attendance systems or ID card-based authentication, are often time-consuming, prone to errors, and susceptible to misuse. The motivation behind this project is to develop a mobile app

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

that leverages biometric technology to address these challenges efficiently and securely. This project aims to create a scalable and adaptable solution for colleges, reducing inefficiencies while fostering a more secure and technologically advanced campus environment. It has the potential to revolutionize administrative workflows and set a benchmark for institutional modernization.

1. Develop features for users to register their biometric data (e.g., fingerprints) securely. Implement an email-based One-Time Password (OTP) system for user verification during registration processes to enhance security.
2. Utilize GPS and geo-fencing technology to ensure biometric registration is conducted only within designated geographical boundaries. Integrate Firebase Authentication to manage user accounts securely, supporting email verification and password recovery.
3. Create a streamlined process for admin to update or re register their biometric data, including OTP verification.

2. METHODOLOGY

Utilize geofencing technology to establish virtual boundaries around classrooms and lecture halls, enabling automatic attendance detection when students enter the defined areas .Implement a time-based attendance validation component that requires students to check-in within a predefined time window, preventing proxy attendance and encouraging punctuality .Develop a secure backend infrastructure to store and manage attendance data, ensuring the confidentiality and integrity of student records .Design an intuitive and user-friendly mobile application interface, providing students with a seamless experience in managing their attendance, receiving notifications, and accessing their schedules. Incorporate comprehensive administrative reporting features, allowing faculty and staff to monitor attendance patterns, generate attendance reports, and analyze student engagement.

2.1 System Architecture

The user interface design for the mobile app should indicate simplicity and usability, enabling users to navigate effortlessly. Utilizing XML layouts, the app can feature distinct screens for biometric registration, login, and access management, each designed with clarity in mind. Key elements include a straightforward registration form, a camera view for capturing biometric data, and clear buttons for navigation. Kotlin and Java will manage user interactions, ensuring responsive feedback during the registration process. Additionally, visual indicators can guide users through capturing their biometrics correctly. Overall, the design aims to create a secure and engaging user experience while maintaining accessibility.

2.2 Data flow

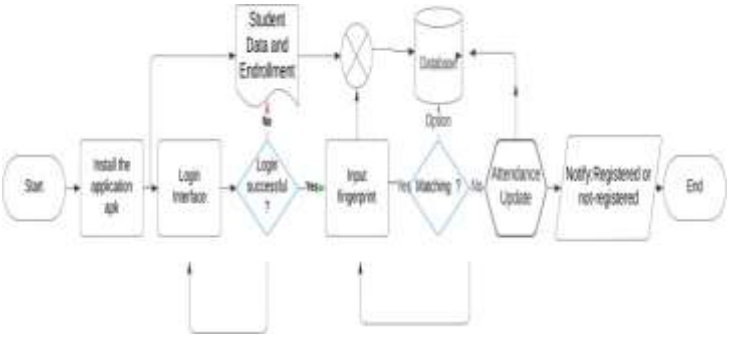
The user registration process for the biometric mobile application begins with the user entering their personal information and biometric data on the registration screen. This data is validated by the application logic implemented in Kotlin and Java. Upon successful validation, a request is sent to Firebase Authentication to create a new user account using the provided email and password. Once the account is created, the user's personal details and a reference to the biometric data are securely stored in the Fire store database. Finally, the user receives a confirmation message and is to navigated to the main dashboard of the application .

2.3 IMPLEMENTATION

The implementation of the technology stack for the mobile app involves several key components. Kotlin and Java are used for developing the app's core functionality, ensuring a tough and efficient codebase. The user interface is designed using XML layouts, providing a clear and responsive experience for users during biometric registration and login. The app integrates the Android Biometric API to facilitate secure capturing of fingerprint or facial data. For backend services, Firebase is utilized, offering safe user authentication and real-time data management through its Real-time Database. Additionally, security measures like data encryption are implemented to protect sensitive biometric information during transmission and storage.

2.4 FLOW CHART

.



3. CONCLUSIONS

In conclusion, the mobile app successfully implements biometric registration and authentication using Firebase, Kotlin, Java, and XML, providing a secure and user-friendly experience. The high accuracy of biometric recognition and efficient data synchronization with Firebase enhance overall functionality. User feedback underscores the app's automatic design and ease of use, making it accessible for a broad audience. The combination of strong security measures and responsive performance positions the app as a reliable solution for location-specific access. Future enhancements will focus on optimizing biometric algorithms and expanding feature sets to further improve user engagement.

Suggestions for Future Work:

1. **Integration of Advanced Biometric Modalities**- Incorporate additional biometric options, such as iris scanning, palm vein recognition, or gait analysis, as device capabilities advance .Explore multimodal biometric registration (combining multiple biometrics like fingerprint and facial recognition) to enhance accuracy and security.

2. **Block chain Integration for Data Security-**Implement block chain technology to create a decentralized and tamper-proof ledger for storing biometric registration records .Enhance transparency and trust in the system by allowing stakeholders to verify the integrity of stored data.

3. **Scalability for Large-Scale Deployments-**Optimize the app to handle large-scale user registration and simultaneous data processing for institutions with thousands of students and staff. Add cloud-based solutions to ensure scalability and efficient storage of biometric data.

REFERENCE

1. Jain, A. K., Ross, A., & Prabhakar, S. (2004). An Introduction to Biometric Recognition . IEEE Transactions on Circuits and Systems for Video Technology , 14(1), 4-20.

2. Sadeghi, A., & Wachsmann, C. (2016). Biometric Authentication: A Survey. IEEE Communications Surveys & Tutorials, 18(3), 1880-1912.

3. Firebase Documentation. (2023) . Firebase Authentication. Available at: [firebase.google.com/docs/auth] (https://firebase.google.com/docs/auth)

4. Google Developers. (2023) . Fingerprint Authentication. Available at: developer.android.com/training/sign-in/biometric-auth

5. Kotlin Documentation. (2023) . Kotlin Programming Language. Available at: [kotlinlang.org](https://kotlinlang.org/docs/home.html)

6. Android Developers. (2023). Building a Simple User Interface with XML. Available at: developer.android.com/guide/topics/ui/declaring-layout

7. Sahu, P. K., & Jagannathan, R. (2018). A Survey on Biometrics and its Applications . International Journal of Computer Applications, 182(39), 1-6.