

Enhancing Enterprise Mobile Security with Multi-Profile Biometric Authentication

Siok Yee Tan¹, Yu Chien Lim² and Ali Kahwaji³

¹Center for Artificial Intelligence Technology, Faculty Information Science and Technology, Universiti Kebangsaan Malaysia, 43800 Bangi Malaysia

²Faculty Information Science and Technology, Universiti Kebangsaan Malaysia, 43800 Bangi Malaysia.

³Creative Technologies and Services Industries, Nelson Marlborough Institute of Technology, 322 Hardy Street, Nelson 7010, New Zealand

Email: esther@ukm.edu.my, a186912@siswa.ukm.edu.my, ali.kahwaji@nmit.ac.nz

Abstract—In today's ever-changing technological landscape, mobile devices such as phones and tablets play a vital role in storing large amounts of personal and corporate information, making them prime targets for security breaches. In workplaces where shared devices are common, the risk of information leakage increases, especially when relying solely on password protection. To address this challenge, this project introduces Multi-FR Lock, a powerful voice and facial recognition security application designed for Android devices. Unlike traditional facial recognition locks that are limited to authenticating a single user, Multi-FR Lock supports multiple user profiles, allowing for secure device sharing among employees. This application is specifically designed to lock and secure sensitive applications as specified by administrators. To access these locked applications, users must pass facial and voice recognition tests. This dual-level security method significantly improves protection against unauthorized access. Administrators are responsible for recording employee information and managing facial and voice data in a connected database, ensuring that only authorized users can update or modify stored biometric data, thereby maintaining data integrity. Developed on Android Studio and Java, with PHP, HTML, JavaScript, and Firebase for the web-based administration platform, Multi-FR Lock stands out in the field of mobile security solutions. By providing a secure and convenient way to manage access to devices in a shared environment, it offers significant benefits to businesses and organizations looking to prevent information leaks and improve overall security.

Index Terms— application's lock, facial recognition, security, voice recognition.

I. INTRODUCTION

In the modern era, mobile devices have become indispensable tools in both personal and professional settings. Their versatility and convenience have led to widespread use across various fields, including education, healthcare, and corporate environments [1]-[3]. Mobile devices facilitate communication, enhance productivity, and provide access to a wealth of information and applications. In the workplace, mobile devices are often shared among multiple workers, making it easier to access work-related applications and data from anywhere at any time [4], [5]. However, this widespread use raises significant security concerns. Shared devices can easily become targets for unauthorized access, leading to data breaches and loss of sensitive information.

The sensitive corporate data, personal information, and proprietary applications could be compromised if not adequately protected [6]. This issue underscores the growing importance of advanced security measures, such as face recognition a biometric authentication technology, which is increasingly being integrated into various applications due to its reliability and user convenience [7].

As reliance on mobile applications continues to grow, the need for robust security mechanisms becomes increasingly critical. Mobile devices and applications have become prime targets for cyber-attacks, making security a paramount concern [8], [9]. Traditional security measures, such as passwords and PINs, are often insufficient in preventing unauthorized access. They are prone to being forgotten, guessed, or stolen, which can lead to unauthorized access and data breaches [10]. Biometric authentication methods, including fingerprint and facial recognition, have emerged as superior alternatives, offering enhanced security and user experience. Biometric authentications provide a more secure and convenient method of authentication because they are unique to each individual and difficult to replicate [7]-[11]. Among these, face recognition stands out due to its non-intrusive nature and high accuracy in verifying user identities [12]. This biometric method provides a higher level of security compared to traditional methods, addressing the vulnerabilities associated with passwords and patterns [11]. Moreover, face recognition systems are increasingly being used in mobile applications for secure login, access control, and fraud prevention, highlighting their growing importance in the security landscape [13]. This project aims to develop Multi-FR Lock, a powerful multi-user facial recognition lock application designed to enhance the security of workplace devices. In today's fast-paced technological landscape, mobile devices such as phones and tablets are critical for storing vast amounts of sensitive personal and corporate data, making them prime targets for security breaches especially in workplaces where devices are shared among multiple users. Multi-FR Lock tackles this challenge by offering dual-level protection through both facial and voice recognition, ensuring that only authorized users can access sensitive applications. The primary objectives include identifying workplace security needs, developing a system to securely manage and store the biometric data of multiple users, and evaluating the system's usability. The application also logs user activity, providing detailed records of access times, user data, and application details. Additionally, the web component of Multi-FR Lock allows administrators to manage staff data and view activity logs, facilitating efficient oversight and troubleshooting. Utilizing Firebase for real-time database and storage, the application ensures secure and reliable data handling. Multi-FR Lock represents a significant advancement in mobile security solutions, specifically tailored for workplace environments where shared devices are common. By integrating dual-layer biometric authentication and comprehensive administrative controls, this application not only enhances security but also simplifies device management. The use of real-time data handling through Firebase further solidifies its reliability, making it a crucial tool for preventing information leaks and ensuring the integrity of sensitive data. As organizations increasingly rely on mobile technology, Multi-FR Lock provides a robust and adaptable solution to meet evolving security needs.

II. BACKGROUND STUDY

Automatic face recognition technology, which originated in the 1960s, began with the development of early semi-automatic systems. These initial methods involved analyzing facial features in images, calculating distances and ratios, and comparing them to standard reference points found in all faces. Although these early systems were basic, they laid the groundwork for the sophisticated facial recognition technologies we use today. Over the decades, the technology has undergone significant advancements, evolving from simple image processing techniques into highly complex algorithms capable of recognizing and verifying identities with increasing accuracy [14]. Today, face recognition technology is widely utilized across various platforms, including Android, iOS, and Windows, primarily for enhancing device security and user authentication [15]. Its integration into everyday devices has made it a cornerstone of modern security practices. As the technology continues to advance, the accuracy and reliability of facial recognition systems are also improving, making them an essential tool in both personal and professional settings. Despite these advancements, most existing face recognition locks are designed for single-user devices. While this design works well for personal use, it falls short in workplace environments where devices are frequently shared among multiple users. In such settings, relying on a single-user face recognition system can lead to security vulnerabilities and administrative challenges. For instance, the need to repeatedly log in and out or manually switch user profiles can be both time-consuming and inefficient, potentially leading to lapses in security [16]. This gap highlights the need for a more versatile solution that can manage the facial data of multiple users on shared devices. The Multi-FR Lock project aims to address this issue by developing a multi-user face recognition lock application specifically designed for Android devices. This application is intended to improve security in workplace environments where devices are

commonly shared. By allowing multiple users to securely access the same device through facial recognition, Multi-FR Lock offers a practical and efficient solution to the challenges faced by businesses and organizations in maintaining the security of shared devices. This development represents a significant step forward in adapting face recognition technology to meet the specific needs of modern workplace environments.

The subsequent section will explore the tools and technologies integral to the development of the Multi-FR Lock application, specifically focusing on Google ML Kit, the VOSK model, and Firebase. This discussion will detail how these components are utilized to enhance facial and voice recognition capabilities, ensure secure data management, and support real-time processing."

A. Google ML Kit

The Google ML Kit Face Detection API is a robust tool designed to equip developers with advanced facial recognition capabilities for mobile applications [16]. Utilizing machine learning, this API can detect faces in images and videos with high accuracy and efficiency, identifying facial landmarks, classifying expressions, and determining head orientation. These features make it a comprehensive solution for various applications, from enhancing security to improving user interaction [17]. Built to operate seamlessly on both Android and iOS platforms, the API leverages Google's machine learning expertise to deliver real-time performance, even on low-powered devices. By offering advanced features such as face contour detection and tracking, the Google ML Kit Face Detection API enables the development of sophisticated applications capable of recognizing and analyzing multiple faces simultaneously, thereby enriching the user experience [18].

In the context of the Multi-FR Lock project, the Google ML Kit Face Detection API plays a critical role in enhancing the application's security functionality. The API's advanced capabilities for detecting and mapping facial landmarks are crucial for accurately identifying and differentiating between multiple users, which is particularly important in workplace environments where devices are shared among employees. The API's ability to perform real-time facial recognition under challenging conditions, such as varying lighting or angles, ensures that the Multi-FR Lock application remains reliable and efficient, providing robust security without compromising the user experience.

Moreover, the API's compatibility with both Android and iOS platforms allows the Multi-FR Lock application to be deployed across a wide range of devices, making it adaptable to various workplace settings. By integrating the Google ML Kit Face Detection API, the Multi-FR Lock project is equipped to deliver high accuracy in user authentication, thereby enhancing the overall security of mobile devices. This integration ensures that the application meets the high standards required for secure, multi-user access on shared devices, solidifying its role as a sophisticated and secure mobile security solution [18], [19], [20].

B. VOSK Model

The VOSK Model is an advanced speech recognition engine designed to transcribe spoken language into text, distinguished by its capability to perform offline speech recognition, making it particularly suitable for applications where privacy and low latency are paramount [21]. Supporting multiple languages and offering real-time transcription, VOSK is ideal for interactive applications that require immediate and accurate voice processing. Built on deep neural networks and leveraging the Kaldi toolkit, VOSK is optimized for various environments, including those with background noise, and can run efficiently on low-resource devices such as mobile phones and embedded systems. This makes it a popular choice for developers aiming to incorporate robust voice recognition into their applications [22].

The VOSK Model operates by converting spoken words into text through a series of processing stages. Initially, audio input is captured and converted into a waveform, which is segmented into short frames. These frames are analyzed to extract features that represent the characteristics of the speech signal, which are then fed into a neural network model trained on extensive spoken language datasets. The model predicts phoneme probabilities, which are used to construct words and sentences through a decoding process that takes into account language context and structure. The resulting text transcription can be utilized for various applications, including voice commands, transcription services, and language learning tools [23], [24].

In the context of the Multi-FR Lock project, the VOSK Model contributes significantly by providing the voice recognition component of the application. Its ability to operate offline ensures that the voice recognition functionality can be used in environments where internet connectivity is limited or where privacy concerns are critical. The real-time transcription capabilities of VOSK are essential for enabling swift and accurate user authentication, complementing the facial recognition provided by the Google ML Kit Face Detection API.

By integrating the VOSK Model, Multi-FR Lock offers a dual-layered security system that combines facial and voice recognition, enhancing the overall security of workplace devices. This integration ensures that only

authorized users can access sensitive applications, further safeguarding against unauthorized access in environments where devices are shared among multiple users. The robustness of VOSK in handling various environmental conditions, such as background noise, also ensures reliable performance, making it a key component in delivering a secure and efficient mobile security solution.

C. Firebase

Firebase, a comprehensive application development platform provided by Google, offers powerful tools for backend services, including the Realtime Database and Firebase Storage [25]. The Firebase Realtime Database is a NoSQL cloud database that enables developers to store and sync data between users in real-time. This means that any changes in the data are immediately reflected across all clients, providing a seamless and interactive user experience. It is particularly useful for applications that require real-time updates, such as chat applications, collaborative tools, and live data dashboards [26]. The database is designed to handle large amounts of data and can scale with the application's growth, ensuring efficient performance regardless of the number of users.

Firebase Storage, on the other hand, is used for storing and serving user-generated content, such as photos, videos, and other files. It is built on Google Cloud Storage and offers robust security features, including Google security standards for encryption and authentication, ensuring that user data is safe and secure [27]. Developers can easily upload and download files directly from the client, and Firebase Storage handles the complex tasks of file storage, including redundancy, scaling, and high availability. This makes it an ideal choice for applications that require the handling of large media files or need to provide a reliable and scalable storage solution.

The Realtime Database and Firebase Storage work seamlessly together to provide a comprehensive backend solution for modern applications. For instance, in real-time communication applications, Firebase Realtime Database can manage the exchange of messages, while Firebase Storage can handle multimedia files shared during the communication [28]. This integration ensures that all data, whether text or media, is synchronized and available to all users in real-time. Additionally, the implementation of NoSQL Realtime databases, such as Firebase Realtime Database, has proven to be effective in various applications, providing reliable and efficient data management systems [29]. The combined capabilities of Firebase Realtime Database and Storage make them essential components for developing dynamic, scalable, and secure applications.

III. RESEARCH METHOD

The Multi-FR Lock project utilizes an elicitation technique as its research method, designed to thoroughly understand user needs and confirm the essential functionalities required for the application. To achieve this objective, a comprehensive questionnaire was developed, focusing on the security management needs for mobile devices in modern workplace environments. This survey was conducted among teachers, staff, and students at Universiti Kebangsaan Malaysia (UKM), as well as employees from external organizations. A total of 37 respondents participated in the survey, providing valuable insights into the current challenges and expectations surrounding mobile device security. The questionnaire was structured using a Likert scale to capture a detailed range of responses, from strongly disagree (1) to strongly agree (5), ensuring a clear understanding of participant perspectives. This approach allowed for precise measurement of attitudes towards both existing mobile security practices and the proposed Multi-FR Lock application. The demographic breakdown of the respondents included 56.8% female and 43.2% male participants. Regarding their working status, 40.5% were students, 35.1% were employees, 13.5% were staff members, and 10.8% were lecturers. The survey results provided critical recommendations and perspectives on current mobile device security management, directly informing the development of Multi-FR Lock. These findings were instrumental in refining the application's features to better meet the security needs of diverse user groups, particularly in workplace settings where device sharing is common. Table 1 presents the research analysis of the user needs for the proposed face recognition application lock.

The research analysis presented in Table 1 highlights significant concerns regarding mobile device security in both workplace and university environments. The data indicates that mobile devices are frequently used and commonly shared among users. This frequent use and sharing underscore the necessity for robust security measures. However, the satisfaction with current security measures is notably low, with a mean of 2.38, reflecting widespread dissatisfaction among respondents. Support for facial recognition locks is relatively high (mean = 3.86), and there is a strong agreement (mean = 4.03) that alternative authentication methods, such as passwords, are easily compromised, indicating a preference for more secure and advanced authentication methods. The analysis also reveals dissatisfaction with existing facial recognition application, which are seen as failing to meet specific workplace needs (mean = 2.30) and providing inadequate security (mean = 2.19). A

significant drawback of these existing application is their limitation to a single user's data, with a mean agreement of 4.03 on this issue. In contrast, the proposed Multi-FR Lock application is positively received, with respondents showing strong support for its features. There is a clear preference for Multi-FR Lock to support multiple facial profiles (mean = 3.97), provide user guidance (mean = 4.03), and disable alternative authentication methods such as passwords (mean = 4.08). Additionally, the inclusion of double-layer biometric authentication (mean = 3.86) and the capability to record user activity (mean = 3.84) are also supported. Respondents agree that access to the Multi-FR Lock database should be restricted to administrators (mean = 4.08), ensuring secure management of biometric data. Overall, there is a consensus that Multi-FR Lock could significantly enhance mobile device security in workplace environments. The necessity of developing this application is strongly supported, with a mean agreement of 4.00, reflecting a clear demand for a more secure, multi-user facial recognition solution that addresses the identified shortcomings in existing security measures.

TABLE I. USER NEEDS ANALYSIS FOR MULTI-FR LOCK APPLICATION

No.	Questions	Mean	Standard Deviation
1.	How frequently do you use your mobile device in both work and university environments?	4.16	1.09
2.	How common is the practice of sharing devices with colleagues or classmates in your work or university setting?	4.00	1.130
3.	How satisfied are you with the current security measures implemented on mobile devices in your workplace or university?	2.38	1.341
4.	Do you support the use of facial recognition locks on mobile devices in your workplace?	3.86	1.294
5.	Do you agree that alternative authentication methods in existing facial recognition locks, such as passwords, are easily crackable?	4.03	1.166
6.	Do you agree that existing facial recognition lock apps meet the specific needs of your workplace?	2.30	1.244
7.	Do you agree that facial recognition locks can provide a faster and more convenient authentication method?	3.92	1.163
8.	Are you satisfied with the security provided by existing facial recognition lock apps?	2.19	1.330
9.	Do you agree that the limitation of existing facial recognition lock applications to a single user's data is a significant drawback?	4.03	1.323
10.	Do you agree that Multi-FR Lock should have the capability to store data for multiple facial profiles?	3.97	1.280
11.	Do you agree that Multi-FR Lock should provide guidance to new users regarding the registration of facial data and personal information?	4.03	1.118
12.	Do you agree that Multi-FR Lock should disable alternative authentication methods such as passwords?	4.08	1.090
13.	Do you agree that Multi-FR Lock should have the capability to record user login and logout times?	3.84	1.344
14.	Do you agree that Multi-FR Lock should include double-layer biometric authentication?	3.86	1.273
15.	Do you agree that access to the Multi-FR Lock database and adjustments should be limited exclusively to administrators?	4.08	1.064
16.	Do you agree that Multi-FR Lock can enhance mobile device security in the workplace?	3.86	1.159
17.	Do you agree that the security level offered by Multi-FR Lock aligns with your needs for work and classes?	3.97	1.190
18.	Do you agree that Multi-FR Lock should be installed on mobile devices used within the workplace?	4.22	0.886
19.	Do you agree that Multi-FR Lock should be installed on mobile devices used within universities?	3.89	1.370
20.	Do you agree on the necessity of developing Multi-FR Lock?	4.00	1.155

A. Development Tools for Multi-FR Lock

The development of the Multi-FR Lock application integrates several essential tools and technologies to ensure robust functionality, security, and a seamless user experience. The primary Integrated Development Environment (IDE) employed for this project is Android Studio, the official IDE for Android development. Android Studio offers a comprehensive suite of tools tailored for building, testing, and debugging Android applications, making it the ideal platform for developing complex and efficient mobile solutions. The application is developed using Java, a versatile and widely-adopted programming language that provides extensive libraries and robust support for Android development. Java's rich ecosystem allows developers to build secure and high-performing applications, making it well-suited for implementing the sophisticated features of Multi-FR Lock.

For biometric authentication, Multi-FR Lock utilizes two powerful tools: Google ML Kit and the VOSK Speech Recognition toolkit. The Google ML Kit's Face Detection API plays a critical role in the application's ability to identify and authenticate users through facial recognition. This API leverages advanced machine learning to detect and analyze facial landmarks in real-time, ensuring both speed and accuracy in user authentication. It is capable of handling multiple facial profiles, making it ideal for the application's multi-user environment. Complementing the facial recognition capability, the VOSK Speech Recognition toolkit adds a layer of voice recognition to the application. VOSK is an open-source toolkit optimized for real-time voice recognition, which is crucial for the application's dual-layer biometric authentication system. By combining facial and voice recognition, Multi-FR Lock significantly enhances security, offering a more secure and reliable method of user verification compared to traditional authentication methods.

On the backend, Firebase Realtime Database and Firebase Storage are used to manage and secure the application's data. Firebase Realtime Database, a cloud-hosted NoSQL database, supports real-time data synchronization across multiple devices. This feature is particularly important for Multi-FR Lock, as it ensures that user data—including facial and voice biometric information, application lock statuses, and user activity logs—is consistently updated and available in real-time. Firebase Storage works alongside the Realtime Database to handle the secure storage of user-generated content, such as facial images and voice samples. It employs advanced security measures, including data encryption and user authentication, to protect sensitive information, ensuring that the application meets stringent security standards.

The web-based administration platform of Multi-FR Lock is developed using standard web technologies, including HTML, CSS, and JavaScript. This platform provides administrators with a responsive and user-friendly interface to manage user data, monitor activities, and configure application settings. The combination of these web technologies ensures that the administrative tasks are handled efficiently and intuitively, allowing for effective management of the application.

In summary, the integration of Android Studio, Java, Google ML Kit, VOSK, Firebase, and standard web technologies forms a comprehensive development framework for Multi-FR Lock. This combination of tools ensures that the application is not only secure and reliable but also user-friendly and capable of meeting the complex security needs of modern workplaces and educational institutions.

B. Framework of Multi-FR Lock

The Multi-FR Lock application operates on a sophisticated framework designed to provide robust security through dual-layer biometric authentication. The process begins during the user registration phase, where biometric data is captured and processed to create secure, personalized profiles. Specifically, the application utilizes the device's camera in conjunction with the Google ML Kit Face Detection API to analyze key facial features such as the eyes, nose, and mouth. This analysis results in the creation of a biometric template, a unique digital representation of the user's facial characteristics. Simultaneously, the VOSK Speech Recognition toolkit captures the user's voice to generate a distinct voice print, another form of biometric data that enhances security. Both the facial biometric template and the voice print are securely stored in the Firebase Realtime Database, alongside the user's personal information. This centralization of biometric data in Firebase ensures that authentication is consistent and reliable across multiple devices, crucial for maintaining security in environments where devices are shared. The use of Firebase also supports real-time data synchronization, meaning that any updates or changes to user data are immediately reflected across all connected devices.

This feature is particularly important in multi-user settings, where the integrity and availability of biometric data are critical.

For application locking, Multi-FR Lock employs the Android Package Manager to enumerate and display a list of all installed applications on the device. Users or administrators can then select which applications to secure. The lock status of each application is managed locally on the device using Shared Preferences, which allows individual devices to maintain unique lock settings while still relying on the shared biometric data stored in Firebase. This flexibility ensures that the application can adapt to different security needs across various devices, making it a versatile solution for both workplace and university environments.

When a user attempts to access a locked application, Multi-FR Lock initiates the authentication process by activating the device's camera to capture a real-time facial image. This image is then compared against the stored facial biometric template using the Google ML Kit Face Detection API.

At the same time, the VOSK toolkit processes the user's voice sample, comparing it to the stored voice print. Access to the application is granted only if both the facial recognition and voice recognition processes return a positive match. This dual-layer authentication significantly reduces the risk of unauthorized access, offering a higher level of security than traditional single-factor methods like passwords or PINs.

Moreover, Multi-FR Lock logs all authentication attempts, including details such as the application name, user ID, login time, and logout time. These logs are stored in Firebase, allowing for real-time synchronization and monitoring. Administrators can access and review these logs via a web interface developed using HTML, CSS, and JavaScript. This interface provides a user-friendly platform for managing and overseeing mobile device security, enabling administrators to track application usage and ensure that only authorized users are accessing sensitive information.

The comprehensive security framework of Multi-FR Lock not only addresses the limitations of existing facial recognition applications but also enhances overall mobile device security in multi-user environments. By combining the capabilities of Google ML Kit, VOSK, Firebase, and Android's native tools, Multi-FR Lock offers a sophisticated, reliable, and user-friendly solution for safeguarding sensitive applications on shared devices. Figure 1 illustrates the flowchart of the Multi-FR Lock, showcasing the detailed process from biometric data capture to authentication and monitoring.

This framework ensures that every step, from user registration to application access, is securely managed, providing peace of mind for organizations and educational institutions that rely on mobile devices for critical operations. The consequences of not implementing such a robust system are significant, as it could lead to unauthorized access, data breaches, and potential loss of sensitive information, which Multi-FR Lock effectively mitigates.

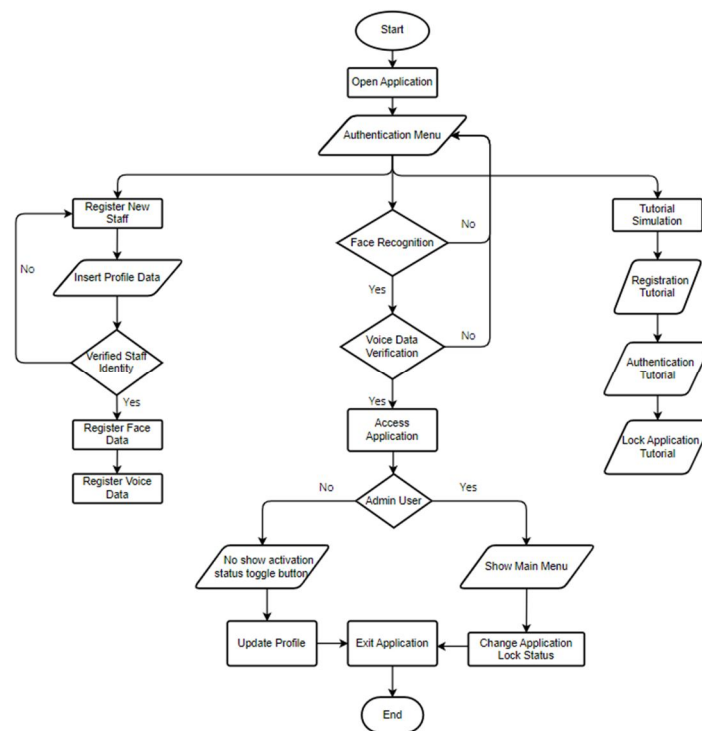


Figure 1. Flowchart of Multi-FR Lock

IV. OUTPUT AND USABILITY TESTING

Multi-FR Lock is an innovative multi-user facial recognition application designed to enhance the security of mobile devices, particularly in workplace environments. The system comprises two main components: the mobile application and a web-based interface. As shown in Figure 2, the mobile application features an application lock that lists all installed applications on the device within the main menu, with the lock status of these applications being controlled exclusively by the admin user. When an application is locked by the admin, access is granted only after the user successfully undergoes dual-layer biometric authentication, which includes both face and voice recognition using the VOSK recognition model. This ensures that only authorized users, who's facial and voice data are registered in the system, can access the locked applications. The application is designed to accommodate multiple users, making it ideal for shared devices in professional settings. Additionally, the application records detailed user activity logs such as application names, staff IDs, login times,

and logout times which are securely stored in Firebase Realtime Database and Storage for comprehensive tracking and monitoring.

Figure 3 illustrates the web-based interface of Multi-FR Lock, which is exclusively accessible to admin users. This interface allows administrators to manage staff data, including inserting, updating, and deleting information in the staff list database. The website also provides an overview of user log activities, enabling admin users to monitor access and usage patterns and promptly address any security issues. The use of Firebase for database and storage ensures real-time synchronization and reliable data management, supporting the seamless operation of the application. By integrating advanced biometric authentication methods and robust data management, Multi-FR Lock offers a powerful solution to enhance mobile device security in environments where multiple users share devices. This ensures that sensitive information remains protected and that only authorized personnel can access critical applications, effectively addressing the significant security challenges faced by modern workplaces.

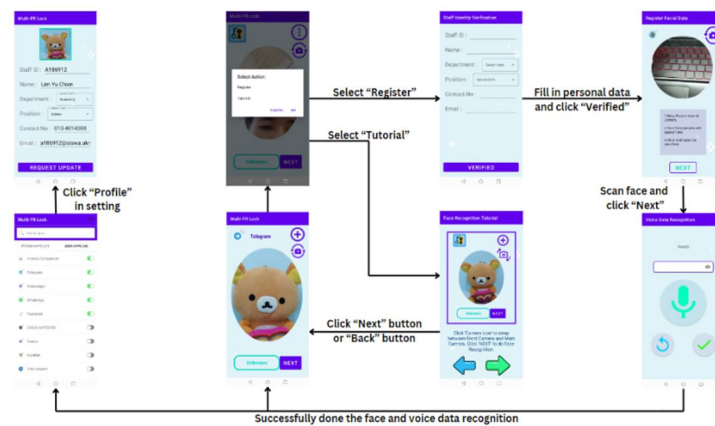


Figure 2. Interface of Multi-FR Lock Mobile application

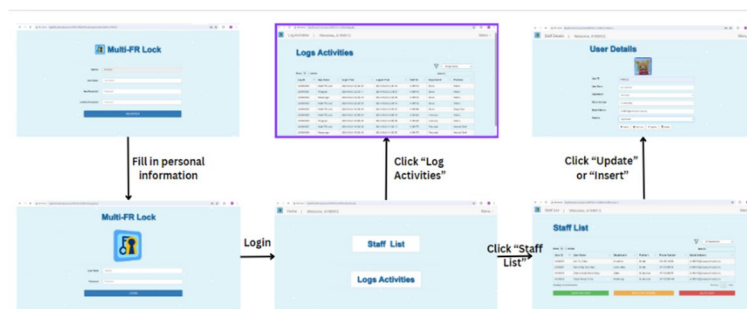


Figure 3. Interface of Multi-FR Lock Web-Based Administration Platform

The usability testing for the Multi-FR Lock application was conducted with a comprehensive approach, aiming to identify any potential errors at an early stage in the development process. A detailed survey was designed and administered to gather user feedback on various aspects of the application, such as usability, ease of use, learning facility, application aesthetics, and overall user satisfaction. A total of 30 users, comprising workers, staff, lecturers, and students from Universiti Kebangsaan Malaysia (UKM), participated in the survey. These participants included 19 male and 11 female users, with the majority aged between 18-25 years (40%), followed by 26-35 years (23.3%), 36-45 years (30%), and a smaller group aged 45 years and above (6.7%).

The statistical analysis of the usability testing, as summarized in Table 2. The participants tested the Multi-FR Lock application and then provided their feedback through a questionnaire consisting of 25 questions. These questions were carefully designed to assess the application's performance across multiple dimensions, including its usability, user-friendliness, aesthetic appeal, and effectiveness in securing mobile devices. The survey results revealed overwhelmingly positive feedback across all evaluated aspects. The mean scores for various usability factors, such as application usability, ease of use, learning facility, application aesthetics, and user satisfaction, consistently hovered around 4.90 and above as shown in Table 2. This indicates that users found the Multi-FR Lock application highly effective in meeting their needs.

In terms of robustness, the application demonstrated a high level of reliability, with no significant issues of failure, lag, or being stuck reported by users. The biometric authentication processes, which include both facial and voice recognition, were particularly well-received, with users praising the accuracy and efficiency of these features.

The dual-layer authentication system, supported by the VOSK recognition model, ensured that only authorized users could access the locked applications, thereby enhancing the security of the devices. Furthermore, the ease of use was a standout feature, with users appreciating the application's simple and intuitive design. The clear icons, diagrams, and responsive interface made it easy for users to navigate and operate the app's features. The learning curve was minimal, thanks to a clear and concise tutorial that allowed users to quickly grasp how to use the application. Aesthetically, the application was well-received, with users commending its simple, neat, and visually appealing interface. The colors and fonts used were described as comfortable, and the layout was well-organized, avoiding any visual clutter that could lead to fatigue during extended use.

Overall, the high mean scores and low standard deviations across all questions suggest that the Multi-FR Lock application is not only effective in enhancing mobile device security but also delivers a smooth, user-friendly experience that is both efficient and aesthetically pleasing. The positive reception across all evaluated aspects underscores the application's potential as a powerful tool for securing mobile devices in environments where multiple users share devices. This ensures that sensitive information remains protected and that only authorized personnel can access critical applications, addressing the significant security challenges faced by modern workplaces.

TABLE II: STATISTICAL ANALYSIS OF USABILITY TESTING FOR MULTI-FR LOCK APPLICATION

Question	Mean $\pm$ SD
App Usability	4.90 $\pm$ 0.348
This application increases the security level of mobile devices.	4.90 $\pm$ 0.305
This application can store face data and profile information of multiple users.	4.90 $\pm$ 0.403
This application has no problem of failure, lag or being stuck.	4.90 $\pm$ 0.305
The facial recognition and voice authentication in this application is accurate.	4.90 $\pm$ 0.403
This application does not take much time to use.	4.90 $\pm$ 0.305
Ease of Use Application	4.91 $\pm$ 0.338
The application is user friendly.	4.93 $\pm$ 0.254
The steps to perform face and voice recognition are simple and short.	4.87 $\pm$ 0.434
The icons and diagrams used are clear and easy to understand.	4.90 $\pm$ 0.305
The app is responsive and quick in its response.	4.93 $\pm$ 0.254
All functions provided in the application are easy to operate	4.90 $\pm$ 0.403
Application Learning Facility	4.94 $\pm$ 0.239
The tutorial provided by the application is simple and clear.	4.97 $\pm$ 0.183
Users can quickly learn how to use this application.	4.97 $\pm$ 0.183
Users feel confident using this application after the first try.	4.90 $\pm$ 0.305
Users understand the main functions of this application in a short time.	4.97 $\pm$ 0.183
The user interface of this application is easy to remember.	4.90 $\pm$ 0.305
Application Aesthetics	4.95 $\pm$ 0.228
The user interface of this application is simple and neat.	4.93 $\pm$ 0.254
The user interface of this application is very beautiful and attractive.	4.93 $\pm$ 0.254
The colors and fonts used in the application provide a comfortable experience for users.	4.93 $\pm$ 0.254
The interface of this application is well organized and not too dense.	4.97 $\pm$ 0.183
The application interface does not cause visual fatigue for the user	4.97 $\pm$ 0.183
User Satisfaction	4.95 $\pm$ 0.256
Users are satisfied with the overall function of this application.	4.97 $\pm$ 0.183
This app makes users want to share it.	4.93 $\pm$ 0.254
This application meets the user's expectations in terms of efficiency and performance.	4.97 $\pm$ 0.183
Users are satisfied with the interface design of this application.	4.90 $\pm$ 0.403
Users are satisfied with the level of security provided by this application.	4.97 $\pm$ 0.183

V. DISCUSSION

The Multi-FR Lock application represents a significant advancement in mobile device security, particularly in environments where shared device usage is common, such as workplaces, educational institutions, and other collaborative settings. By incorporating dual biometric authentication such as facial recognition using Google ML Kit and voice recognition with the VOSK model, the application sets a high standard for ensuring that only authorized users can access locked applications. This dual-layer authentication method considerably strengthens

security by requiring both facial and voice verification, thereby minimizing the risk of unauthorized access. The system's ability to support multiple users further enhances its utility, making it an ideal solution for efficiently and securely managing shared devices.

The integration of Firebase Realtime Database and Storage is another key feature, providing robust data management and real-time synchronization capabilities. This integration allows for comprehensive tracking of user activity, including the specific applications accessed, associated staff IDs, login times, and logout times. This level of detailed monitoring not only improves security but also provides valuable insights for administrators managing device usage in a shared environment.

Despite these strengths, the Multi-FR Lock application does have some limitations that could impact its broader adoption and overall effectiveness. One notable limitation is its current availability only on the Android platform. This restriction narrows the potential user base, excluding iOS and Windows users who could benefit from the application's advanced security features. Expanding the application's compatibility to include these platforms would significantly broaden its reach and impact.

Another concern is the reliance on password authentication for the web platform. While passwords are a common security measure, they are also vulnerable to breaches, as they can be easily compromised through various means such as phishing or brute-force attacks. To mitigate this risk, the application could implement layered authentication methods for the web interface, such as combining strong passwords with biometric recognition or two-factor authentication. This would provide an additional layer of security, making it more difficult for unauthorized users to gain access.

Additionally, the requirement for an internet connection for user authentication poses a challenge in areas with unstable or unavailable connectivity. This limitation can hinder the application's usability in certain scenarios, such as remote locations or situations where internet access is intermittent. To address this, the application could incorporate offline authentication capabilities, possibly through technologies like temporary data storage, offline encryption, or periodically renewable authentication tokens. Such features would allow users to access the application even without an active internet connection, thus enhancing its usability and reliability in a wider range of environments.

VI. FUTURE DIRECTION

With the rise in demand for user privacy and data protection, there are advancements in mobile security biometrics. This change is spearheaded by behavioral biometrics which helps to identify a user continuously the moment the user logs in through the pattern, specifically created by a user like the speed and gestures used while typing or the way a device is used. While static biometrics only helps identify a user a single time, behavioral systems help in risk mitigation as they constantly validate the identity of the user and can help in preventing potential threats. Mobile banking apps for instance use this after the user logs into his account to ensure that the logged in account is the only one accessing the mobile device.

Also, with integration with smart devices and IoT devices the biometric landscape is getting larger. Interconnected systems across wearable devices for example smart watches or AR glasses makes the use of biometric authentication unique. Devices can also be linked to mobile phones or work devices where authentication for the user can be made on the basis of users heart rate of activity providing a safe environment. This also provides a wider scope for biometrics while in turn also increasing security.

AI is improving biometric accuracy by adapting systems to operate in a variety of conditions, such as low light or a partial obstruction. Innovations such as liveness detection, powered by AI, ascertain true users through a method that also identifies spoofing attempts, making for a much stronger authentication process. For example, artificial intelligence based facial recognition systems managing security in high risk places had proven performance reliability and are capable of adapting in the hardest environment to keep a track of security.

This is how Blockchain technology is shaping the future of biometric data management. With decentralized networks, blockchain keeps biometric templates secure and tamper-proof. This helps alleviate concerns about centralized data breaches and gives users more control over their own information. Blockchain-based biometric credential-focused decentralized digital wallets further add to this to privacy and security factor whilst moving away from traditional passwords.

Increasingly, multi-modal biometric authentication is becoming a benchmark in the field, blending methods such as fingerprint and voice recognition to bolster reliability and minimize errors. This layered strategy proves especially valuable for safeguarding sensitive corporate and government systems. Imagine a system that grants access to critical files only after successfully verifying both a fingerprint and a voice sample, a level of protection that significantly reduces the likelihood of breaches.

Altogether, these innovations point to a future where biometric solutions are not just more secure but also seamlessly integrated into daily life. As behavioral biometrics, wearable integration, AI advancements, blockchain technology, and multi-modal systems converge, they redefine the standards of mobile security. With these technologies maturing, we can look forward to a world where data protection is both stronger and more user-friendly, offering a robust defense against the ever-evolving threats of the digital age.

VII. CONCLUSION

The Multi-FR Lock application marks a significant step forward in mobile device security, particularly in environments that require shared device usage, such as workplaces and educational institutions. By utilizing dual biometric authentication such as facial recognition with Google ML Kit and voice recognition via the VOSK model the application ensures that only authorized users can access sensitive applications. The use of Firebase Realtime Database and Storage further strengthens the application's ability to track and manage user activity in real-time, making it a robust tool for shared device security. However, its current availability only on Android limits its user base, excluding potential users from iOS and Windows platforms. To enhance Multi-FR Lock's effectiveness, future developments should focus on expanding platform compatibility to iOS and Windows, implementing stronger web authentication methods, and enabling offline authentication to accommodate users with limited internet access. By addressing these issues, Multi-FR Lock can better serve a wider audience and solidify its position as a leading mobile security solution, ensuring sensitive information remains protected and only authorized personnel can access critical applications in multi-user environments.

REFERENCES

- [1] Tan, S. Y., Lee, K. J., & Lam, M. C. (2020). A Shopping Mall Indoor Navigation Application using Wi-Fi Positioning System. *International Journal*, 9(4).
- [2] Lam, M. C., Lim, S. M., & Tan, S. Y. (2023). User Evaluation on a Mobile Augmented Reality Game-based Application as a Learning Tool for Biology. *TEM Journal*, 12(1).
- [3] Tan, S. Y., & Arshad, H. (2023). Performance Evaluation of Marker Recognition Algorithm for Mobile Augmented Reality in The Real Environment. *Asia-Pacific Journal of Information Technology & Multimedia*, 12(2).
- [4] M. Suzeren, R. Rajikan, N. Alaudin, S. N. Sannusi & M. S. Hamiddudin. (2019). Usability and effect of Mobile Application (Mobile Apps) in UKM Student Orientation Week. *Journal of Student Personnel*, 22(1), 93-101.
- [5] Abd Samad, M. R., Iksan, Z., & Khalid, F. (2022). Needs Analysis: Development of Year Five Science Mobile Applications for Rural National Schools in Malaysia. *Jurnal Pendidikan Sains Dan Matematik Malaysia*, 12(1), 1-15.
- [6] I. A. Elgendy, W. -Z. Zhang, Y. Zeng, H. He, Y. -C. Tian and Y. Yang. (2020). Efficient and Secure Multi-User Multi-Task Computation Offloading for Mobile-Edge Computing in Mobile IoT Networks. *IEEE Transactions on Network and Service Management*, vol. 17, no. 4, pp. 2410-2422.
- [7] Imaoka H, Hashimoto H, Takahashi K, Akinori F, Ebihara, L. JianQuan, Akihiro H, Yusuke M and Kazuyuki S. (2021). The future of biometrics technology: from face recognition to related applications. *Asia Pacific Signal and Information Processing Association*, Vol. 10, E9, p 1-13.
- [8] W. Pawel, L. Lukasz. (2020) Mobile Security: Threats and Best Practices, *Mobile Information Systems Article*, 8828078, 15 pages.
- [9] A. C. Cevahir & T. K. Beyza. (2022). The current state and future of mobile security in the light of the recent mobile security threat reports. *Article in Multimedia Tools and Applications*, 82(2023), 20269–20281.
- [10] A. K. Sikder, L. Babun, Z. Berkay, A. Acar, A. Hidayet, M. C. Patrick, E. Kirda, A. S. Uluagac. (2020). Kratos: Multi-User Multi-Device-Aware Access Control System for the Smart Home. *ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ACM, 12 pages.
- [11] M. E. Maoeretz, R. Arief, E. Abdurachman, A. Trisetarso. (2022). Mobile Device Security: A Systematic Literature Review on Research Trends, Methods and Datasets. *Journal of System and Management Sciences*, 12(3), 66-78.
- [12] M. F. Mustapha, N. Maisarah, S. Haslini, M. A. Malik & M. Rahimie. (2022). A survey on video face recognition using deep learning. *Journal of Quality Measurement and Analysis*, 18(1), 49-62.
- [13] S. Singha & S.V. Prasad. (2018). Techniques and Challenges of Face Recognition: A Critical Review. *International Conference on Advances in Computing and Communication*, 143 (2018) 536–543.
- [14] P. Kaur, K. Krishan, S. Sharma & T. Kanchan. (2020). Facial-recognition algorithms: A literature review. *Medicine Science and the Law*, 60(2): 131–139.
- [15] T. S. Srinivas, T. Goutham, & K. Senthil (2022). Face Recognition based Smart Attendance System Using IoT. *International Research Journal of Engineering and Technology (IRJET)*, 09(03), 182–186.
- [16] R. Paliwal, P. J. Vishal. (2021). Face detection system using machine learning. *International Journal of Advanced Research in Computer Science*, vol. 12, no. 2, 18-24.
- [17] Google (2024). ML Kit – Google for Developers. Available at: <https://developers.google.com/ml-kit/>. Accessed 22 April 2024.

- [18] K.H. Rahouma & A.Z. Mahfouz. (2021). Applying Mobile Intelligent API Vision Kit and Normalized Features for Face Recognition Using Live Cameras. *International Conference on Artificial Intelligence and Computer Vision*, Vol. 1377, No. 1, pp 413–429.
- [19] K. Supriya, H. Rohan, T. Shubham, Y. Dhumane & P. Rajhans. (2023). Driver Drowsiness Detection System using Google ML Kit Face Detection API and Flutter. *International Research Journal of Engineering and Technology*, vol. 10, no. 5, pp 905-909.
- [20] Yowen, J. J. L. Martinez & A. A. Purwita. (2023). Secure Mobile Facial Recognition Attendance System with Edge Computing: A Comparative Study of Face Recognition Models for Android Application Integration. *International Conference of Computer Science and Information Technology*, 10364492, pp. 1-6.
- [21] VOSK (2024). VOSK Offline Speech Recognition API – Alpha Cephei. Available at: <https://alphacephei.com/vosk/>. Accessed 10 May 2024.
- [22] T. Asma, W. Sebastien, A. Yassine & S. Severine. (2022). Evaluation of the efficiency of state-of-the-art Speech Recognition engines. *Procedia Computer Science*, 207 (2022) 2242–2252.
- [23] L. RuiXin, W. RenJie & Z. Jian. (2023). Human-computer interaction based on speech recognition. *International Conference on Machine Learning and Automation*, 20230429, p 102-110.
- [24] Y. C. Julio & S. Makoto. (2022). Evaluation of Offline Automated Speech Recognition for English as Second Language Learning Application. *EdMedia & Innovate Learning Online*, 19-25.
- [25] Google (2024). Firebase|Google's Mobile and Web App Development Platform. Available at: <https://firebase.google.com/>. Accessed 4 April 2024.
- [26] C. Pankaj, Y. Vaibhav, A. Gaikwad. (2021). Firebase - Overview and Usage. *International Research Journal of Modernization in Engineering Technology and Science*, e-ISSN: 2582-5208.
- [27] Axmadjonov M.F. & Mirzaraximov M. A. (2022). Firebase in Real-Time Systems based on Client Server Technology. *Scientific Journal Impact Factor*, Vol. 2, No. 1, pp 146-150.
- [28] C. Nilanjan, C. Souvik, D. Aakash & N. Asoke. (2018). Real-time Communication Application Based on Android Using Google Firebase. *International Journal of Advance Research in Computer Science and Management Studies*, Vol. 6, No. 4, pg 74-79.
- [29] I. Z. Hasibuan1 & Triase. (2022). Implementation of NoSQL Realtime database system using Realtime Firebase database on Ourticle application. *Sibatik Journal*, vol. 2, no. 1, pp 1-23.