Penerbit UTHM

© Universiti Tun Hussein Onn Malaysia Publisher's Office

JSCDM

Journal homepage: http://penerbit.uthm.edu.my/ojs/index.php/jscdm

Journal of Soft Computing and Data Mining

Jeev Time: Secure Authentication Using Integrated Face Recognition in Social Media Applications

Sanjeevan Mohan[1], Nur Ziadah Harun[1*]

[1]Faculty of Computer Science and Information Technology,
Universiti Tun Hussein Onn Malaysia, Parit Raja, Batu Pahat, Johor, 86400, MALAYSIA

*Corresponding Author

DOI: https://doi.org/10.30880/jscdm.2022.03.02.003
Received 12 May 2022; Accepted 10 July 2022; Available online 08 August 2022

Abstract: Social media facilitates the sharing of ideas and information through the building of virtual networks. Not all user accounts are secured based on the complexity of passwords. Password-only authentication finds it hard to protect a user account's confidentiality, integrity, and availability. Therefore, the face recognition integrated Jeev Time social media application is designed to authenticate the system securely. To develop this application, Object-Oriented Analysis and Design (OOAD) is used as the methodology. This application is developed using React Native framework (JavaScript) and backed by Google's Firebase database. Meanwhile, face authentication uses Google's Face Detection API and React Native's Face API. With face recognition, the face as biometric login is enforced in the authentication process. Therefore, the development of this application will secure the system users from using a weaker approach during authentication and not victimized by unethical social media users yet experiencing the familiar social media application interface and its core functionalities.

Keywords: Social media, face detection, face recognition, authentication, virtual network

1. Introduction

For decades, password authentication has been used to secure a user account. Passwords are still considered good security protection, but only password authentication is not enough to provide tighter security. The common practice among internet users is setting simple passwords. Password cracking methods become better over time, and simple passwords are easily cracked. Currently, social media applications allow users to have more than one account for each user, either directly or indirectly. Consequently, the possibility of creating fake profiles also increases. Many social engineering attacks are being conducted through fake profiles [1].

Ordinary social media users would not mind setting up their accounts with a simple password because they might not be aware of the risks. They will prefer instant login rather than hardly recalling a string of characters during their busy routine. Accounts with weak passwords are being hacked, affecting the victim user and the company's reputation [2]. Social media applications which use only passwords to authenticate their users are prone to social engineering attacks such as phishing. Text-based passwords are easy to steal, and hackers could gain access to user accounts [3]. Therefore, the proposed project aims to integrate face recognition in the authentication process of the social media application to mitigate the risks associated with fake profile issues, weak password settings, and simple authentication weaknesses. This proposed project aims to design, develop and test a social media application with integrated face recognition as the authentication mechanism.

The user scope of this project is the internet users who frequently use social media and need a much more secure and easy authentication process. This project mainly targets securing the registration and login modules. These modules will be integrated with face recognition. In the registration module, users are required to register their faces to create an account. In the login module, users must log in using their faces to authenticate. At the end of the project, a social media application integrated with face recognition in the registration and login modules will be developed [4], [5], [6].

Corresponding author: nurziadah@uthm.edu.my

The rest of the papers are organized as follows: Section 2 describes the work related to the literature review findings. Section 3 presents the project methodology. It describes the analysis and design of the newly developed system. Section 4 describes the implementation phase, and Section 5 presents the results and discussion. The conclusion is provided in Section 6.

2. Literature Review

This section explains the literature reviews that have been conducted for this project. This literature review aims to understand the background and technology used for this application.

2.1 The Authentication Mechanism in Existing Social Media

Username and password authentication is still the standard online authentication method [7]. Some social media applications are still using password authentication. However, text-based passwords are highly vulnerable to attacks, and difficult to recall passwords during authentication time [8].

2.2 Face Recognition

Based on Kaspersky, face recognition is a method of recognizing or verifying a person's identity by looking at their face. Face recognition systems can identify people in images, videos, or real time. Besides that, biometric protection includes face recognition.

Face detection is the first process performed before face recognition. Appearance feature-based face detection can define a discriminating function between face and non-face images based on the extracted features such as pupil, eye comers, nostrils, and corners of lips [9].

Figure 1 shows the face recognition workflow from the input of the image to the comparison between the existing face databases. After the face detection, the input face image will come into this face recognition process. In the pre-processing phase, the face image will be normalized into calculable form. Next, the feature extractor stage extracts each feature from the normalized form to proceed to face comparison. Then, the face recognition algorithm will retrieve the existing face images from the face database and compares them with the input image. If a match is found, it will be classified as 'known', or it will be classified as 'unknown', and this process strictly follows a one-to-one relationship where there must be only one recognized face in the given face database. Moreover, a one-to-one relationship is crucial for the authentication process [10].

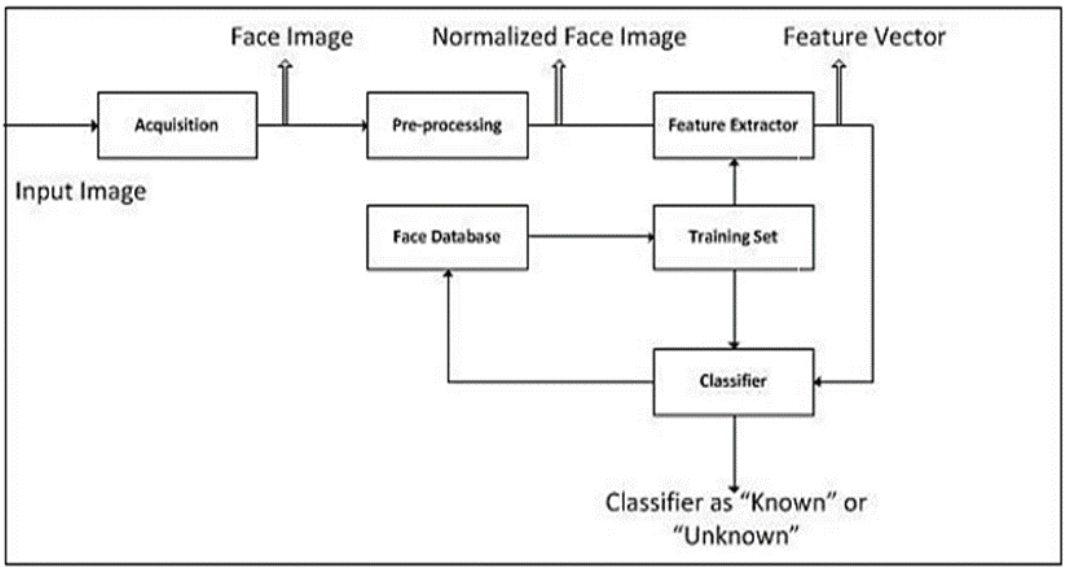

Fig. 1 - Face recognition workflow

2.3 BioID Facial Recognition Mobile Application

BioID Facial Recognition mobile application is available in the Google Playstore. Does it perform face authentication relatively similarly as required for the proposed system? This application aims to lock other applications in a device, and face authentication is required to unlock the respective applications. Figure 2 shows the flowchart of the BioID application from user registration till the authentication process to unlock a locked application [11].

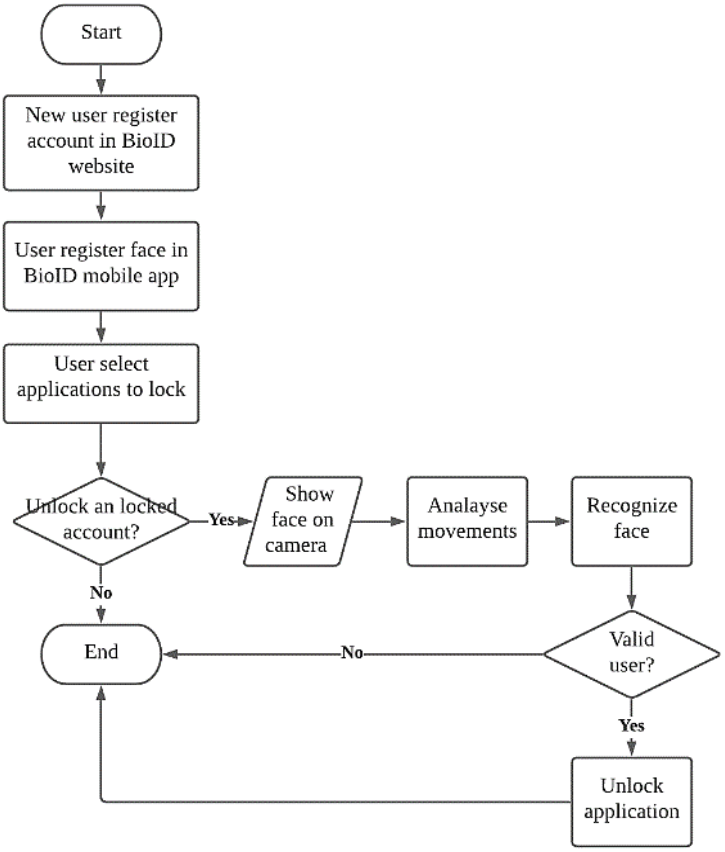

Fig. 2 - BioID application flowchart

The BioID application requires its users to open an account on the BioID website. Then, the user can use their BioID account credentials to log into the application to use their service. Users can set up their other mobile applications to lock with this BioID Facial Recognition app to authenticate using registered faces. BioID application will prompt users to register their faces after login into the application. Then, the user can lock other applications installed on the respective smartphone. Users must authenticate first through the BioID Facial Recognition system when they want to use the locked applications. The user needs to show the face on the camera. Then, the system requests the user to move their head as displayed on the screen to prevent the forgery of the face using images. Once the user is authenticated, the requested action will get executed.

2.4 Apple's Face ID

Face ID is the term used for Apple's facial recognition authentication system. Face ID is used to unlock applications and authorize downloads and transactions within the Apple devices such as iPhones, iPad, and Macbooks. Face ID requires a TrueDepth camera which is built within Apple devices. The camera captures accurate face data by projecting and analyzing thousands of invisible dots to create a depth map of the user's face and captures an infrared image of the face. Then, it transforms the depth map and infrared image into a mathematical representation and compares that representation to the enrolled facial data [16]. To start using Face ID, the user must first enroll their faces. The user needs to glance at the camera to unlock the device using Face ID. Then, the face recognition algorithm compares input face data with the initially registered face data. Once the user is authenticated, he/ she is granted to use the device.

2.5 Comparison with the Existing Systems

Table 1 shows the comparison of existing systems related to the proposed project. This comparison explores existing social media applications' core features and, most importantly, their authentication mechanisms. Facebook is a web application based on freemium social media that can run on multi-platform devices such as mobile phones and desktops. This application uses text-based passwords to authenticate its users. Facebook is offering biometrics as second-factor authentication, but they are not enforcing their users to opt-in. Besides, Twitter is an online news and social networking site where people communicate in short messages called tweets. Twitter is using text-based passwords, too, for user authentication. As an alternative way, Twitter is using third-party account authentication to reduce the creation of new user accounts.

Table 1 - Systems comparison

Features/ System	Facebook	Twitter	Instagram	Proposed System
Password Register	√	√	√	√
Password Login	√	√	√	√ (Disabled by default)
Face register	X	X	X	√
Face login	X	X	X	√
Recover account using email	√	√	√	√ (Face authentication is required to complete the process)
Add post	√	√	√	√
Chatting	√	√	√	√
Add friends / Follow	√	√	√	√
Interact with posts	√	√	√	√

Instagram is an American photo and video-sharing social networking service. Like Facebook and Twitter, Instagram uses a text-based password to authenticate its users. Users can log into Instagram by just using a Facebook account. This authentication approach would become vulnerable if a hacker managed to access the user's Facebook account.

Existing systems have the core functions of social media, such as finding friends, chatting, sharing content among their virtual social circle, and letting other users interact with the posts. Thus, the proposed system will have the core features of existing systems. However, the objective of the proposed project is on the authentication part of the social media application. Existing systems currently use password-based authentication, but this proposed project will have additional face registration and face authentication to enhance the security of the user accounts.

3. Methodology and Design

The Object-oriented Analysis and Design methodology use the Unified Modeling Language (UML) to develop diagrams and provide ready-to-use, expressive modeling examples such as use case and class diagrams. OOAD methodology allows effective management of software complexity by modularity, and the project can be upgraded more easily from small to large systems [12]. OOAD methodology consists of 5 phases: requirements, design, implementation, verification, and maintenance. Table 2 shows each phase and its output during the project development.

Table 2 - OOAD phases and produced outputs

Phase	Task	Output
Requirement	- Problem-related with password authentication is identified in the literature review. - Face recognition integrated social media application is proposed. - A Gantt chart is scheduled. - Identified the proposed system's functional and non-functional requirements	- Project proposal - Gantt chart - Functional requirement - Non-functional requirement
Design	- The proposed system's general system architecture is designed - Use case diagram and specifications of register, login, and other core modules are designed - A high-level system flowchart is designed - User Interfaces (UI) of the proposed system are designed - Database collections and its relationship are designed based on system requirements - System classes are designed - Security and functional test plan are designed - Social media application prototype is designed	- General system architecture - Use case diagram and specifications - System flowchart - Class diagram - Data Model Diagram - Data dictionary - User Interface design - Test plan - Prototype
Implementation	- Database collections using Google's Firebase service, UI, and classes developed using React Native framework are linked together. - The social media application with integrated face recognition is fully developed.	- Social media application with secure authentication using face recognition (Jeev Time)

Verification	-	Unit testing, System testing, Integration testing, and User acceptance testing were conducted.	-	Complete test plan & result - System user manual
Maintenance	-	It has fixed compatibility bugs that did not display texts in Android 11. - Forgot password feature removed for improved security.	-	Existing system with new features available

3.1 General System Architecture

Figure 3 shows the overall workflow of the system for the system users. The system user will start the flow by logging into the system. Firstly, a new user must register to use the system. Once authenticated through face recognition, the user will get into their account. Then the user can manage their posts, friends, chats, and profile.

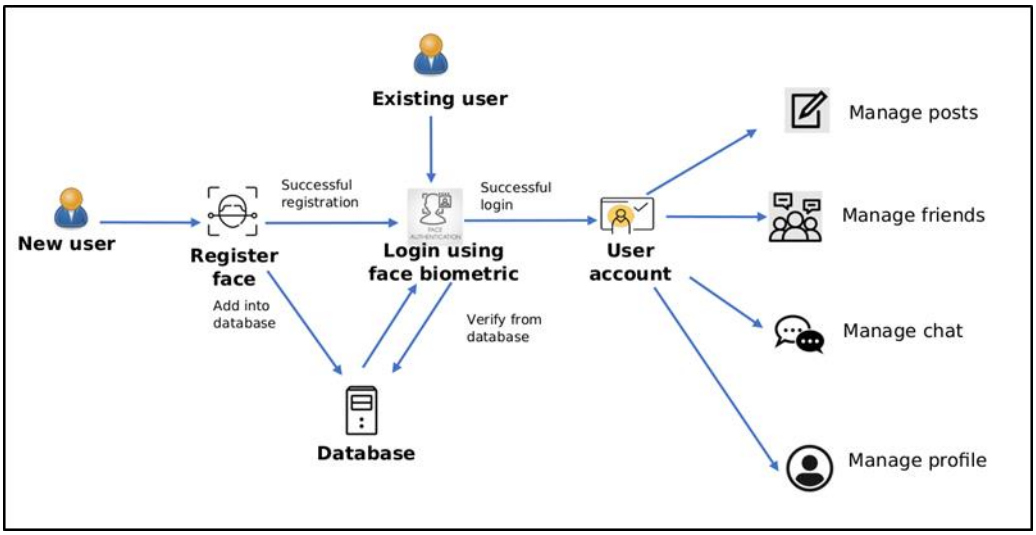

Fig. 3 - General system architecture

3.2 System Requirement

System requirements consist of functional and non-functional requirements. This system consists of 6 functional modules, which are register, login, change password, user profile, chat, and post modules, as shown in Table 3. Meanwhile, the non-functional requirements of this system are security, operation, and performance, as shown in Table 4.

Table 3 - Functional requirements

Modules	Functionalities
Register module	● The system should go to the registration page for a new user. ● The system should require the user face to complete the registration process. ● The system should alert for any invalid input. ● The system should redirect the user to email verification after a successful registration.
Login module	● The system should require for user's face to authenticate. ● The system should check for respective account permission to attempt a login using a password. ● The system should alert for any invalid input. ● The system should redirect the user to the respective account after successful login.
Change password module	● The system should send the change password link to the authenticated email. ● The system should check for the validity of the change password link after being forwarded from the email. ● The system should require for user face to complete the change password action. ● The system should alert for any invalid input.
User profile module	● The system should display its details and settings options in its profile. ● The system should display other users' details and follow their respective accounts' status and chat options.
Chat module	● The system should deliver the messages to the correct recipients.

Post module	● The system should display followers' posts to the authenticated user on the homepage. ● The system should display other users' posts in their respective accounts. ● The system should display owned posts under their profile. ● The system should allow users to create their posts. ● The system should allow deleting their posts. ● The system should allow users to like, comment, and share posts.

Table 4 - Non-functional requirements

Modules	Functionalities
Security	● A user can only create one account under one face. ● The system enforces to set of a password with at least eight characters and mixed characters during registration. ● The system displays similar error alerts for any invalid authentication attempts. ● The system will log any invalid authentication attempts. ● The system disables password login by default. ● The system enforces face login after four failed attempts of a password-enabled existing account. ● The system requires successful email verification to unlock their account for the first time. ● Only authenticated users can enable password login for their accounts. ● Only authenticated users can add and delete their posts and comments. ● Only authenticated user can change their profile picture. ● Only an authenticated user can request for change password link. ● The system requires to face authorization to complete the change password process.
Operational	● The system should be user friendly ● The system should be easily maintained and updated. ● The system should be able to work on 5. x and later versions of android phones.
Performance	● The system should always be usable. ● The system should be able to authenticate users within 10 seconds with a proper internet connection.

3.3 System Overall Design

Figure 4 shows the overall system flowchart of the Jeev Time application. The system flow starts with the registration module. If the user is already registered, he/ she can proceed to the login module. Any failed login attempts will be recorded in the log and display a proper error message. In this system, password login is the alternative way of login, but the user has to enable the password login option under user account settings after logging in. After four failed password login attempts, the user is forced to only face authentication. After successful authentication, the user can start to use the system. The home page always displays the following users' posts. The authenticated user like, comment, and share their posts. Besides, the user can search for other system users to follow, and he/ she can initiate a chat with the newly followed user. Moreover, the authenticated user is able to add a new post, and he/ she also can delete it from his/ her user profile. The user also has control over changing his/ her profile picture. If the authenticated user wants to change the current password, he/ she can go to the settings page and click on the change password option. This option sends the user a change password links to the registered email, and the password can be changed after the successful face authorization attempt. Finally, the user will be logged out from the system after clicking the logout option in settings.

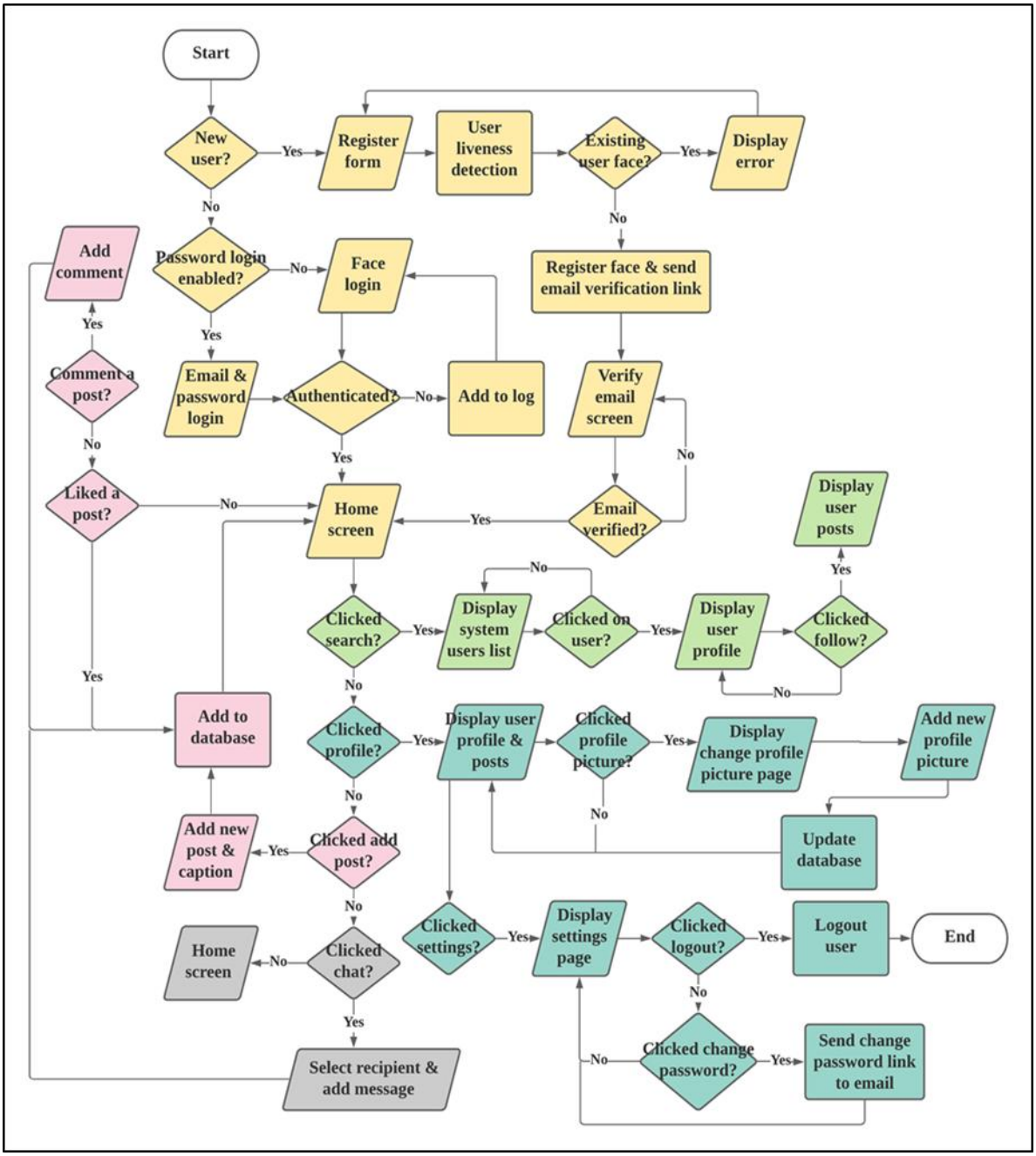

Fig. 4 - System flowchart

Face detection, liveness detection, and face recognition are the authentication mechanisms integrated into the developed application's register and login modules. The pseudocode of face and liveness detection is shown in Figure 5. The authentication mechanism begins with face detection. Once the camera is launched, it will prompt the user to blink his/ her eyes, move the head to the right, move the head to the left, move the head slightly and smile, respectively. The user must complete this liveness detection progress to proceed to the login process. Next, the face data will be passed to the face recognition algorithm.

Figure 6 shows the pseudocode of the face recognition process in the register and login modules. After the complete detection process, the face data will be converted into a calculable format. Then, each image data from the database will be retrieved and converted into the calculable format by the default function. Next, the face comparison loop will start, and the loop will be iterated until the function finds the right match. Then, the system will authenticate the user and redirect them to their respective account. If there is no match found, the loop will be ended, and the system will display an error message and redirect to the login page.

```
START
Launch camera
if face detected:
        if eyes are blinked:
                Fill up the progress bar to 20%,
        if head moved to right:
                Fill up the progress bar to 40%,
        if head moved to left:
                Fill up the progress bar to 60%,
        if head moved slightly:
                Fill up the progress bar to 80%,
        if smile detected:
                Fill up the progress bar to 100%,
                Close camera
                Pass face data to face recognition algorithm
END
```

Fig. 5 - Pseudocode of face and liveness detection

```
START
Convert lively captured face data into a calculable format
Existing face data will be retrieved from the face database
Convert retrieved face data into a calculable format
While comparing both face data
        if face data matches:
                Break face data comparison loop
                Redirect to the respective user account
        else if no face data matches:
                End face data comparison loop
                Display error message
                Record login database
                Redirect to login page
        else
                Continue face data comparison loop
END
```

Fig. 6 - Pseudocode of face recognition

4. Implementation

Figure 7 shows the flow of the register module in Jeev Time application. A new user will fill up his/ her required details and click on 'Sign up'. Then, the user must follow the instructions to complete the head movement pattern. Finally, the user will be registered in the system, and then he/ she will be redirected to the email verification screen.

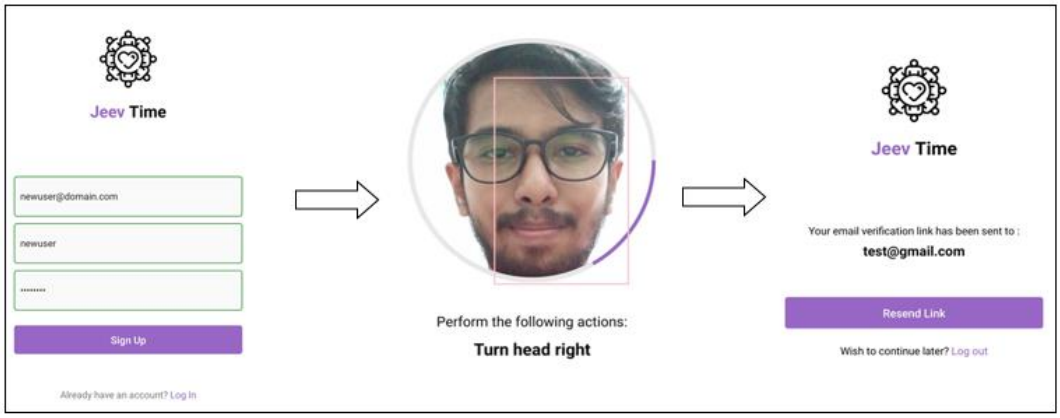

Fig. 7 - Flow of register module

The existing user will show his face on camera, and he/ she will complete the head movement patterns as instructed. Then, the system will find the user account associated with his/ her face. Finally, the user will be authenticated, and he/ she will be navigated to his/ her respective user account.

5. Result and Discussion

This section presents the results and discussion of the developed system. This includes unit testing, integration testing, system testing, and user acceptance testing results. Table 5 shows the result of the unit testing plan for the developed application. This test includes functional and security testing.

Table 5 - Unit testing result

No	Test Plan	Result
1	Login – Input registered face and requested head movements (Accept)	Passed
2	Login – Input registered face but incomplete head movements (Deny)	Passed
3	Login – Input not registered face (Deny)	Passed
4	Login – Show more than 1 faces during face login (Deny)	Passed
5	Login – Use a 2D image to authenticate (Deny)	Passed
6	Login – Use the correct email & password to login into the password of the enabled account (Accept)	Passed
7	Login – Use the correct email & password to login into password disabled account(Deny)	Passed
8	Login – Use the correct email & incorrect password to login (Deny)	Passed
9	Login – Use incorrect email & correct password to login (Deny)	Passed
10	Login – 4 failed attempts using either incorrect email or password (Block Password Login)	Passed
11	Register – Fill up form fields with satisfying requirements (Accept)	Passed
12	Register – Fill up form fields with any unsatisfied requirements (Deny)	Passed
13	Register – Use registered email and a new face (Deny)	Passed
14	Register – Use a new email and registered face (Deny)	Passed
15	Register – Input new face and requested head movements after completing the register form with new email (Accept)	Passed
16	Register – Input face but incomplete head movements (Deny)	Passed
17	Register – Show more than 1 faces during face register (Deny)	Passed
18	Register – Use a 2D image to register your face (Deny)	Passed
19	Email verification – Registered user followed verification link sent to registered email (Accept)	Passed
20	Email verification – Click the back button to go to the user account without verifying (Deny)	Passed
21	Email verification – Logout and login again without verifying the email (Deny)	Passed
22	Email verification – Click resend link button if you did not receive the verification link (Accept)	Passed
23	Email verification – Click on the older verification link after receiving the new link (Deny)	Passed
24	User account – Choose any image from the gallery or camera to update the profile picture (Accept)	Passed
25	User account – Able to enable/ disable password login settings	Passed
26	User account – Able to logout into settings	Passed
27	Change password – Able to receive a link through registered email	Passed
28	Change password – Redirect to the app from changing password link from email (Accept)	Passed
29	Change password – Click the old change password link from the email (Deny)	Passed
30	Change password – Follow the change password link after logging out (Deny)	Passed
31	Change password – Follow the change password link of other accounts (Deny)	Passed
32	Change password – Input new password with requirements satisfied (Accept)	Passed
33	Change password – Input valid face and requested head movements (Accept)	Passed
34	Change password – Input valid face but incomplete head movements (Deny)	Passed
35	Change password – Show more than 1 faces during face authorization (Deny)	Passed
36	Change password – Use a 2D image to authorize face (Deny)	Passed
37	Change password – Show other user's faces during authorization (Deny)	Passed
38	Chatting – Able to send valid messages to the selected recipient	Passed
39	Chatting – Able to receive a message from the recipient	Passed
40	Chatting – Able to search for valid recipient from chat search	Passed
41	Chatting – Able to click on searched chat user	Passed

42	Chatting – Send null message (Deny)	Passed
43	Chatting – Able to notify recipient upon receiving a new message	Passed
44	Add post – Able to select an image from gallery or camera and write a caption	Passed
45	Search user – Able to navigate to a search screen	Passed
46	Search user – Able to retrieve the searched result	Passed
47	Search user – Able to navigate to corresponding user profile	Passed
48	Search user – Able to follow/ unfollow searched user	Passed
49	Post – Able to delete own post	Passed
50	Post – Able to like a post	Passed
51	Post – Able to comment on a post	Passed
52	Post – Send null comment (Deny)	Passed
53	Post – Able to add a new comment in the text box and click send	Passed
54	Post – Able to delete own comment	Passed
55	Post – Able to share the post	Passed

Integration testing ensures all internal and external modules used to develop the system are working properly after being bundled as an android application. Integration testing was done while debugging the application, and Google Play did the full integration testing before it was released in the Google Play store. System testing is done by a professional testing agent on the completed software product before it is introduced to the market. For this application, system testing was done by Google Play. Based on the report of system testing, there are some minor issues in the application stability, performance, and accessibility. But the core focus of this project, security, is showing no issues. The user acceptance test is the product's beta testing done by the end users. This application is already released as a beta version in Google Play store, and a user acceptance form has been distributed among the application testers. Twenty respondents took this test in total. Figure 8 shows more UTHM students engaged in this test than others. Figure 9 shows up to 70% of respondents are aged between 18 and 23.

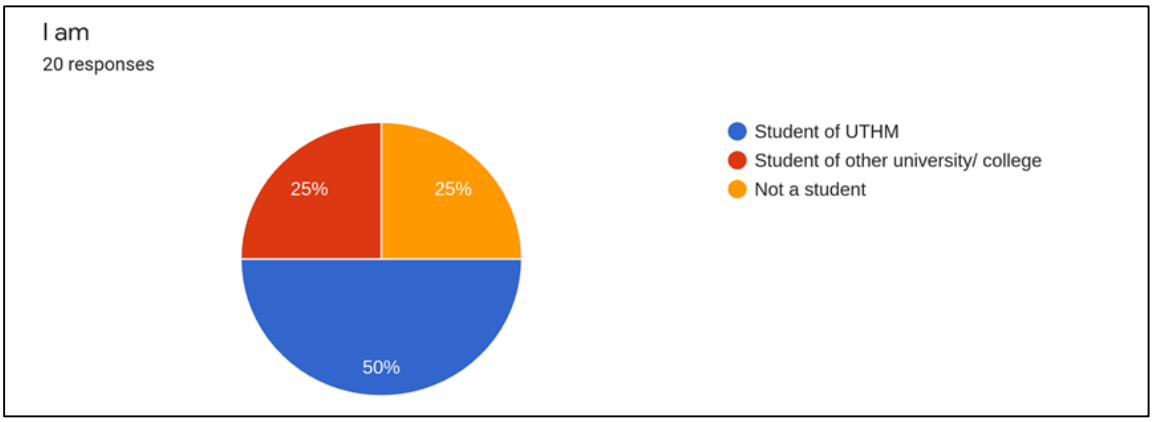

Fig. 8 - Result of type of respondents

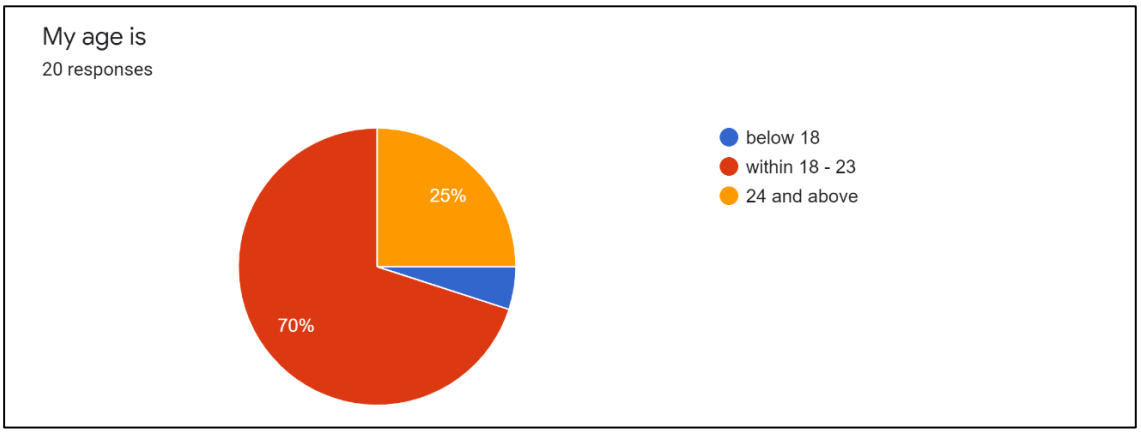

Fig. 9 - Result of the age group of respondents

Table 6 shows the count of respondents who either accepted or rejected the requirements listed. Based on the user acceptance result shown in Table 6, most respondents can launch intended actions through the application. Moreover, most respondents voted on the performance in achieving the user expectation level. Finally, most respondents also accepted that the application is good in security and trustworthiness.

Table 6 - User acceptance testing result

No	Acceptance Requirements	Test result (No. of people)	
		Accept	Reject
1	The system is user-friendly and not confusing	20	0
2	A proper error message is displayed if required fields left blank during the register	20	0
3	The system properly guides the new user to register	20	0
4	Face registration is easy to complete	20	0
5	The system is logging in to the correct user account with a face login	20	0
6	The head pattern is easy to complete	19	1
7	The email verification link is received instantly	20	0
8	The user interface is familiar and easy to understand	20	0
9	The search tool shows the desired result in finding other users	20	0
10	Navigation between pages is smooth and loaded instantly	20	0
11	Able to send and receive chats	20	0
12	Able to like, comment, and share posts	20	0
13	Able to follow other users	20	0
14	Able to add new posts instantly	19	1
15	Has good control over own user account	20	0
16	The security of this system is high, and this application is trustable	19	1

6. Conclusion

The project "Jeev Time: Secure authentication using integrated face recognition in social media application" is developed to mitigate the risks associated with fake profile issues, weak password settings, and other simple authentication weaknesses. This is done by integrating the face recognition feature as the authentication mechanism. The advantages of the developed application are users do not need to remember the password to login into their account. Next, this application does not allow users to have more than one account, and brute force attacks are very difficult to do on this application because password login is disabled by default. Besides, users have both face and password login options to access their accounts. Moreover, the email verification requirement halted the fake email registrations during account creation, and forgot password insecurity is not in this application. Finally, liveness detection during the authentication process prevents spoofing attacks. Contrarily, the disadvantages of the application are the face registration processing time increases linearly with the number of face records in the database because the system compares new face input with all the face records stored in the database. Besides, face login processing time increases linearly with the face records stored in the database because the face recognition algorithm compares the input face with each face record until it recognizes the user. Moreover, a certain amount of device resources, such as memory, processing power, and internet data, will be consumed in face registration and authentication. Finally, the users cannot register or login using faces in dark places. Therefore, future work needs to be done to improve the application in all aspects. Firstly, the face recognition algorithm needs to optimize to consume fewer device resources and reduce the time taken to authenticate the users. Besides, the application needs to provide more user account control to block other users. Finally, the application must prevent multi-device login while logging in to a device.

Acknowledgment

The authors would like to thank the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, for supporting this work.

References

[1] Singh, N., Sharma, T., Thakral, A., & Choudhury, T. (2018). Detection of fake profile in online social networks using machine learning. In 2018 International Conference on Advances in Computing and Communication Engineering (ICACCE), 231-234).

[2] Shan, C. P., Loon, W. H., Win, L. K., Din, D., & Seak, S. C. (2019, April). Automated Login Method Selection in a Multi-modal Authentication System: Login Method Selection based on User Behavior. In 2019 IEEE 9th Symposium on Computer Applications & Industrial Electronics (ISCAIE), 120-124.

[3] Frauenstein, E. D., & Flowerday, S. V. (2016, August). Social network phishing: Becoming habituated to clicks and ignorant to threats?. In 2016 Information Security for South Africa (ISSA), 98-105.
[4] Dollarhide, M. (2019). Social media definition. Investopedia. Available online: http://billscomputerpot. com/menus/windows/SocialMedia. pdf (accessed on 20 July 2020).
[5] Duggan, M., Ellison, N. B., Lampe, C., Lenhart, A., & Madden, M. (2015). Social media update 2014. Pew research center, 19, 1-2.
[6] Duggan, M., Ellison, N. B., Lampe, C., Lenhart, A., & Madden, M. (2015). Social media update 2014. Pew research center, 19, 1-2.
[7] Borchert, B., & Günther, M. (2013, December). Indirect NFC-login. In *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)* (pp. 204-209). IEEE.
[8] Bijoy J. M., Kavitha V. K., Radhakrishnan B. and Suresh L. P. (2017). A Graphical Password Authentication for analyzing legitimate user in online social network and secure social image repository with metadata," 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT), 1-7.
[9] Devadethan S., Titus G. and. Purushothaman S. (2014). Face detection and facial feature extraction based on a fusion of knowledge based method and morphological image processing," 2014 Annual International Conference on Emerging Research Areas: Magnetics, Machines and Drives (AICERA/iCMMD), 1-5.
[10] Indrawan, P., Budiyatno, S., Ridho, N. M., & Sari, R. F. (2013). Face recognition for social media with mobile cloud computing. International Journal on Cloud Computing: Services and Architecture, 3(1), 23-35.
[11] (2021) BioID Facial Recognition (Version 2.2.2) [Mobile app]. Retrieved from Google Play Store. https://play.google.com/store/apps/details?id=com.bioid.authenticator
[12] Booch, G., Maksimchuk, R. A., Engle, M. W., Young, B. J., Connallen, J., & Houston, K. A. (2008). Object-oriented analysis and design with applications. ACM SIGSOFT software engineering notes, 33(5), 29-29.
[13] Kaur P. and Singh A. (2012). User authentication in Social Networking Sites using face recognition. 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, 2012, 773-778.
[14] Miller, D., Sinanan, J., Wang, X., McDonald, T., Haynes, N., Costa, E., ... & Nicolescu, R. (2016). How the world changed social media (p. 286). UCL press.
[15] Ozan E. (2017). Password-free authentication for social networks. 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), 2017, 1-5.
[16] Apple Inc. (2021, September 14). About face ID advanced technology. Apple Support. Retrieved from https://support.apple.com/en-my/HT208108