Applied Information Technology And Computer Science Vol. 4 No. 1 (2023) 019-039

AITCS

Homepage: http://publisher.uthm.edu.my/periodicals/index.php/aitcs
e-ISSN :2773-5141

Implementation of Multi-Factor Authentication on A Vaccination Record System

Teh Yu Fung[1], Sofia Najwa Ramli[1*]

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

*Corresponding Author Designation

DOI: https://doi.org/10.30880/aitcs.2023.04.01.002
Received 24 July 2022; Accepted 27 May 2023; Available online 30 June 2023

Abstract: The vaccination Record System was widely used worldwide during the pandemic of COVID-19 and led to information leakage and faking of vaccine certificates. This study aims to design, develop, and evaluate an android-based vaccination record system with multi-factor authentication named Jom-Vaccine. At the same time, the scopes of the research focus primarily on its security mechanism by implementing multi-factor authentication such as password authentication, One-time password (OTP) authentication and fingerprint recognition. The proposed application is developed by adopting prototype modelling and using Android Studio, Firebase and Java language. The findings show that the proposed application can increase the security level by preventing unauthorized access to the application and preventing leakage of sensitive data. The faking of digital certificates is prevented through the implementation of biometric authentication. Jom-Vaccine achieves a good result from the user acceptance form, biometric performance evaluation, and test plan. Overall, the vaccination record system with multi-factor authentication succeeds in achieving all the objectives set in the project.

Keywords: Vaccination Record System, Multi-factor Authentication, Fingerprint Recognition

1. Introduction

Due to the pandemic of COVID-19, Vaccination Record System was developed to record the vaccination record of its users. There are two examples of vaccination record systems, MySejahtera used in Malaysia and Trace Together used in Singapore. The app will track the COVID-19 outbreak in the country. Moreover, each citizen must receive the COVID-19 vaccine to decrease disease symptoms.

There are many COVID-19 vaccines, but the World Health Organization approves only seven vaccines such as Moderna, Pfizer/BioNTech, Janssen (Johnson & Johnson), Oxford/AstraZeneca,

Corresponding author: sofianajwa@uthm.edu.my

Sinopharm, Sinovac and Covishield. Different vaccines require different injection doses [1]. With the help of a vaccination record system, users can manage their vaccination records easily. Since the vaccination record system holds users' sensitive data, a system developer should emphasize the security features implemented into the system.

Since the vaccination record system holds a huge number of users' sensitive data, it will easily target unauthorised users to obtain those sensitive data. Faking of COVID-19 vaccine certificate raises after an announcement from Tan Sri Muhyiddin Yassin about who are fully vaccinated will be allowed the freedom for activities from 10 August 2021 upon showing their COVID-19 digital certifications. Besides that, many types of vaccines will also cause users hard to manage their vaccination records.

This project was focus on developing a secure Vaccination Record System named Jom-Vaccine by implementing a security mechanism using multi-factor authentication. There are about five modules inside the proposed application, and it will be referred from MySejahtera. The interface will be created using HCI knowledge to improve the user experience. The proposed system can help users manage the vaccination record easily. The test plan and user acceptance form will be used to make sure the proposed android-based vaccination record system is able to achieve all the objectives. The proposed application can be used in real-world scenarios with further implementation.

The rest of this paper is organized as follows. Section 2 presents related works of the proposed application, which are two-factor authentication, fingerprint recognition, and the comparison between the proposed application and the existing systems. Section 3 describes the methodology used to build the proposed application. Section 4 will explain the implementation while section 5 shows the result and discussion of the proposed application. Lastly, section 6 presents the concluding remarks for future works.

2. Related work

This section discusses the related work for the study, which are two-factor authentication and fingerprint recognition.

2.1 Two-factor Authentication

Two-factor authentication is a security mechanism that needs two different forms of identification to gain access to something [2]. The second form of identification can be categorized into three. The first category is "something you know", which refers to the personal identification number (PIN) such as answers to "secret questions" or using a unique keystroke pattern. The second category is "something you have", which refers to the credit card, hardware tokens, or phone number. "Something you are" will be the last-second factor for two-factor authentication. This category is the most secure factor because of biometric patterns such as fingerprints, voiceprints, facial, retina, or iris patterns. This factor is secure because the physical characteristics of each human being are unique [3].

2.2 Fingerprint Recognition

The modern history of fingerprint identification began in the late nineteenth century with the establishment of identification bureaus tasked with maintaining accurate records on individuals indexed [4]. The automatic process of comparing a saved fingerprint pattern with an input fingerprint to determine human characters is fingerprint recognition. Although fingerprint recognition has been used for a decade, it is currently one of the most widely used biometrics. This is because fingerprint recognition can verify identity quickly and precisely [5]. Fingerprints can be determined by three features. The first feature is fine features which are the carriers of "uniqueness" due to its random solid pattern. Delicate features, known as minutiae, are located at the ends and bifurcate the finger lines. Next, coarse features have substantial genotypic impacts and can be used to pre-sort a big data set during identification. Examples of coarse features are whorls, loops, and arches. The third feature is called pore

structure, which is rarely used because it exhibits considerable quality variations in the scanning procedure [6].

2.3 Comparison of the proposed system and the existing system

Table 1 compares the features of the existing vaccination record system and the proposed application (Jom Vaccine). Two existing systems, MySejahtera, used in Malaysia and TraceTogether, used in Singapore. The Ministry of Health (MOH) manages the MySejahtera application, but the Malaysian government is the owner. TraceTogether is developed by the Government Technology Agency of Singapore (GovTech) to address the COVID-19 outbreak in Singapore [7]. Besides, TraceTogether can also detect close contact of COVID-19 patients [8].

Table 1: Systems' comparison

Features	MySejahtera	TraceTogether	Jom-Vaccine
Login	Yes	No	Yes
Register New User	Yes	Yes	Yes
Strong password for registering a new account	No	No password is needed	Yes
Insert health record	Yes	No	Yes
Provide vaccine information	Yes	No	Yes
Digital certificate	Yes	Providing a link to the Sing pass app to view the vaccination certificate	Yes
Authentication before access to digital certificate	No	No	Yes
Encryption of sensitive data	Yes	Yes	Yes
Biometric Authentication	No	No	Yes

Table 1 shows the comparison between two existing systems with the proposed system. All three systems have login modules, register new user modules, and encryption of sensitive data. However, the password for registering an account on MySejahtera [9] is not strong because MySejahtera only limits the length of the password to the range of 6 to 25 characters, and the user of TraceTogether does not require a password to register an account. In the proposed system, the user needed to use a strong password, including one uppercase letter, number, and a special character.

Both MySejahtera and the proposed system stored sensitive data such as health records because they require users to insert their health records. TraceTogether website shows that TraceTogether only collects the identification and contact details and app analytic data, and no result shows TraceTogether collects users' health records [10]. On the other hand, three vaccination record system does provide information on the COVID-19 vaccine. In addition, users can find information about the approved vaccine used in their country.

Furthermore, the digital certificate will be shown in MySejahtera [11] and the proposed system, but not on TraceTogether. TraceTogether will only show the vaccination status of the users, but it provides a link to the Sing pass app to view the COVID-19 certificate. Biometric authentication will only be implemented in the proposed system which users need to authenticate using fingerprints to verify their identity.

3. Methodology/Framework

A prototype model is a software development approach in which a prototype is built, tested, and redesigned before attaining a suitable prototype. This model is a foundation for creating the final framework or application [12]. One of the advantages of this method is lowering the effort required to design the final system because the final method is added after all the criteria have been established. Besides that, prototyping can determine the system functionalities because it allows the user to access the prototype [13]. Therefore, the prototype model was suitable for this project's methodological mode. Figure 1 shows the prototype model that used to develop the application.

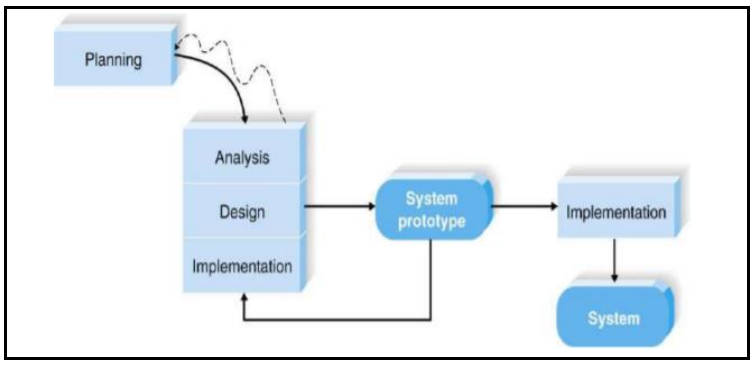

Figure 1: The prototype model [12]

3.1 Planning Phase

The planning phase is the first phase that initiates the whole project and gathers information on the topic. The purpose of the planning phase is to ensure the success of a project and make sure it runs smoothly. The proposal and Gantt chart are the two outcomes of the planning phase.

3.2 Analysis Phase

The analysis phase is the second phase in which its key inputs are deliverables from the planning phase. The technological method for analysing and designing the proposed application is Object-Oriented Analysis and Design (OOAD). It is an iterative stage of analysis that discovers functional and non-functional requirements and ensures that the proposed application's functionality matches the project's objectives.

The functional and non-functional requirements are gathered to ensure the quality of the application. The functional requirement describes the system's behaviour to the end-user, as displayed in Table 2. The non-functional requirements determine the system's quality attributes, as exhibited in Table 3.

Table 2: Functional requirement of the proposed application

Functional Requirement	Description
Login	• The application should allow users and admin to log in with valid credentials.
Register	• The application should allow a new user to register a new account.
Search for Vaccine Information	• The application should allow users to search the information about vaccination.
Insert Health Record	• The application should allow users to insert their health records.
View Digital Certificate	• The application should allow users to view their digital vaccination certificate after verifying their identity using a fingerprint.
Manage Vaccine Information	• The application should allow admin to manage add, delete and update the vaccine information.

View Profile	• The application should allow users and admin to view profile.
Change Password	• The application should allow users and admin to change password.

Table 3: Non-functional requirements of the proposed application

Non-Functional Requirement	Description
Operational	• Only available for the Android operating system mobile devices. • The application requires Android mobile device have a fingerprint sensor.
Security	• Strong password management, the password should include at least one upper-case and lower-case letter, number, and special symbol. • User's personal data should be encrypted before being stored inside the database. • Passwords should not include symbol "+" and "=" to prevent SQL injection attack. • Passwords are hashed using the SHA-512 algorithm. • Users can only access to the system with valid credentials • Fingerprint recognition is used to verify a user's identity for login and view digital certificate.
Performance	• Apply knowledge of Human-Computer Interaction on the design of interface to increase user experience

Furthermore, the user requirements of the proposed application are shown in Table 4 to display the list of operations that the end-user should perform. Therefore, the user and admin are the end-user for the proposed application.

Table 4: User requirement of the proposed application

No	User Requirements
1	Users and admin should be able to log in to the application.
2	Users should be able to register a new account.
3	Users should be able to insert a health record.
4	Users should be able to view their digital vaccine certificate.
5	Users should be able to search for vaccine information.
6	Users and admin should be able to view profile.
7	Users and admin should be able to change password.
8	Admin should be able to add, delete and update the vaccine information.
9	Users and admin should be able to logout.

3.3 Design Phase

Unified Modelling Language (UML) diagrams were used to outline the system functions and behaviours, such as the System Architecture diagram, Use Case Diagram, Sequence Diagram, Activity Diagram, Class Diagram and Entity-Relationship Diagram. This is because the proposed application is designed based on UML specification Object Oriented. The Use Case Diagram can produce high-quality software because it defines the relationship between the system and the user.

From the use case diagram of the proposed application, as displayed in Figure 2, eight actions can be performed by the user while the admin has five actions to perform. For example, both can log in, log out, view their profile, and change passwords. But admin has the higher access right to manage the vaccine information.

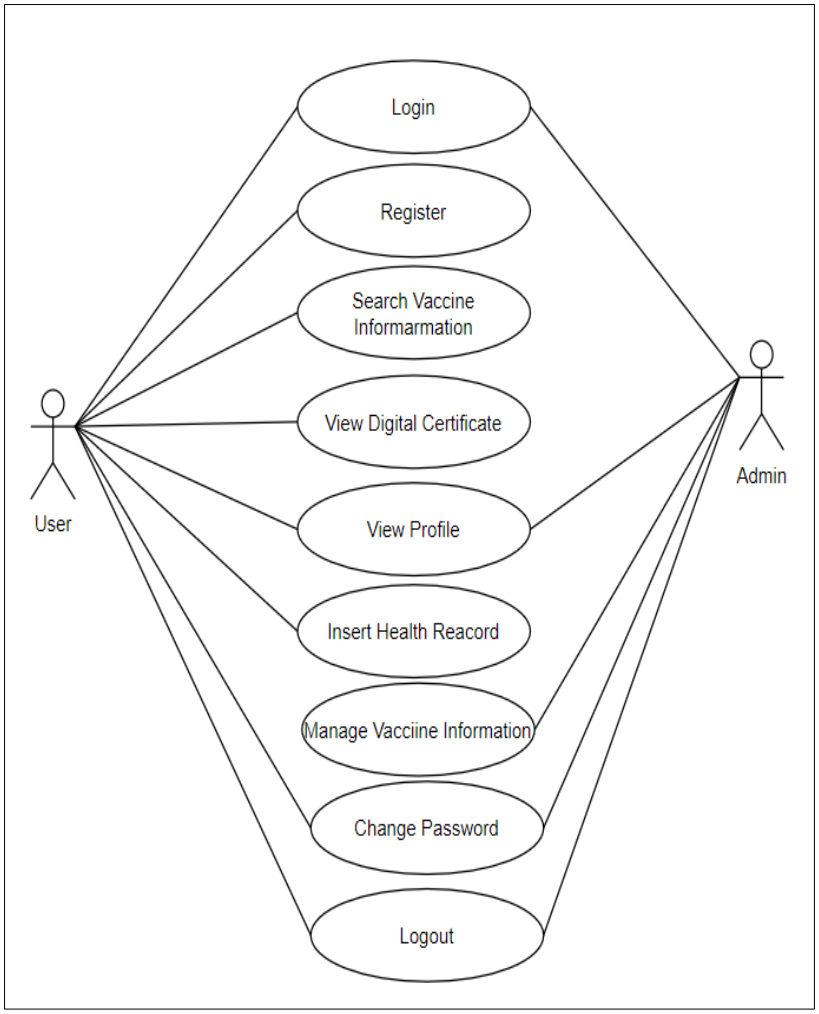

Figure 2: Use case diagram of the proposed application

The activity diagram represents the operational workflows and the user's activity. Figure 3(a) shows the activity diagram of the user. First, new users must create a new account by providing a username, IC number, email, phone number, passwords, and fingerprint patterns. Input validation will be used to validate user input. After that, users need to verify their phone number by inserting the One Time Password sent by the application via SMS. After registering successfully, the user must log in with the new phone number and password. After login with valid credentials, the user will enter the home page and perform the activity, including searching vaccine information, inserting health records, viewing the digital certificate, or viewing the profile. If users wish to view their digital vaccine certificate, biometric authentication is needed before they perform the action. Therefore, users need to verify their identity using fingerprints. Next, users can enter their passwords under the profile page if they wish to change their passwords. The passwords will be validated by verifying the old password, checking the complexity of the new password, and checking the confirmed password with the new password. After finishing all the tasks user can log out of the application.

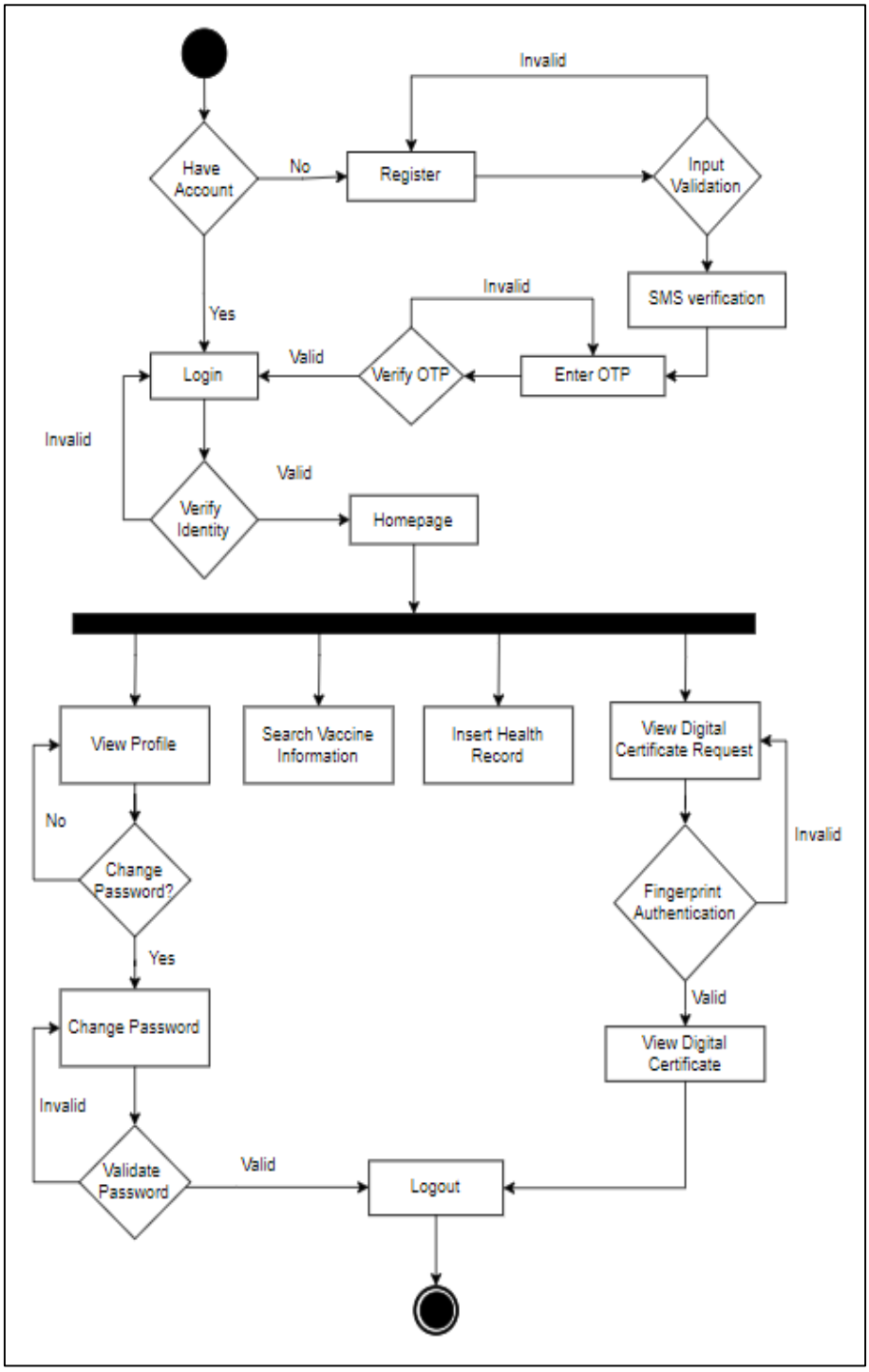

Figure 3(a): Activity diagram for user

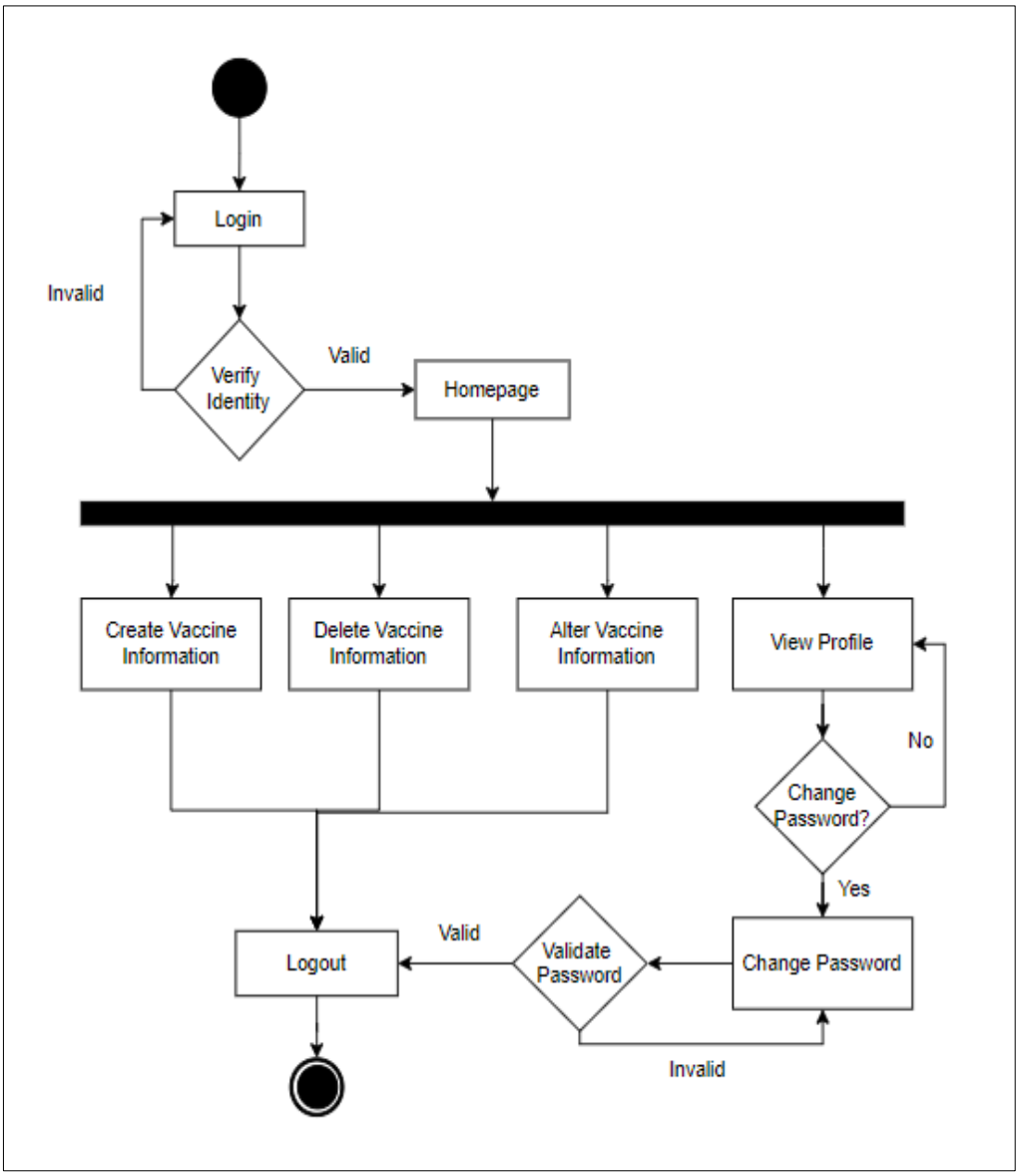

Figure 3(b): Activity diagram for admin.

Figure 3(b) shows the activity diagram of admin. First, an admin needs to log in with valid credentials. Then, the admin can only log in with proper credentials. Then, the admin can create, delete, and alter the vaccine information on the home page. The admin can also change their password, and the password will be validated to ensure its complexity. Lastly, the admin can log out as their wish.

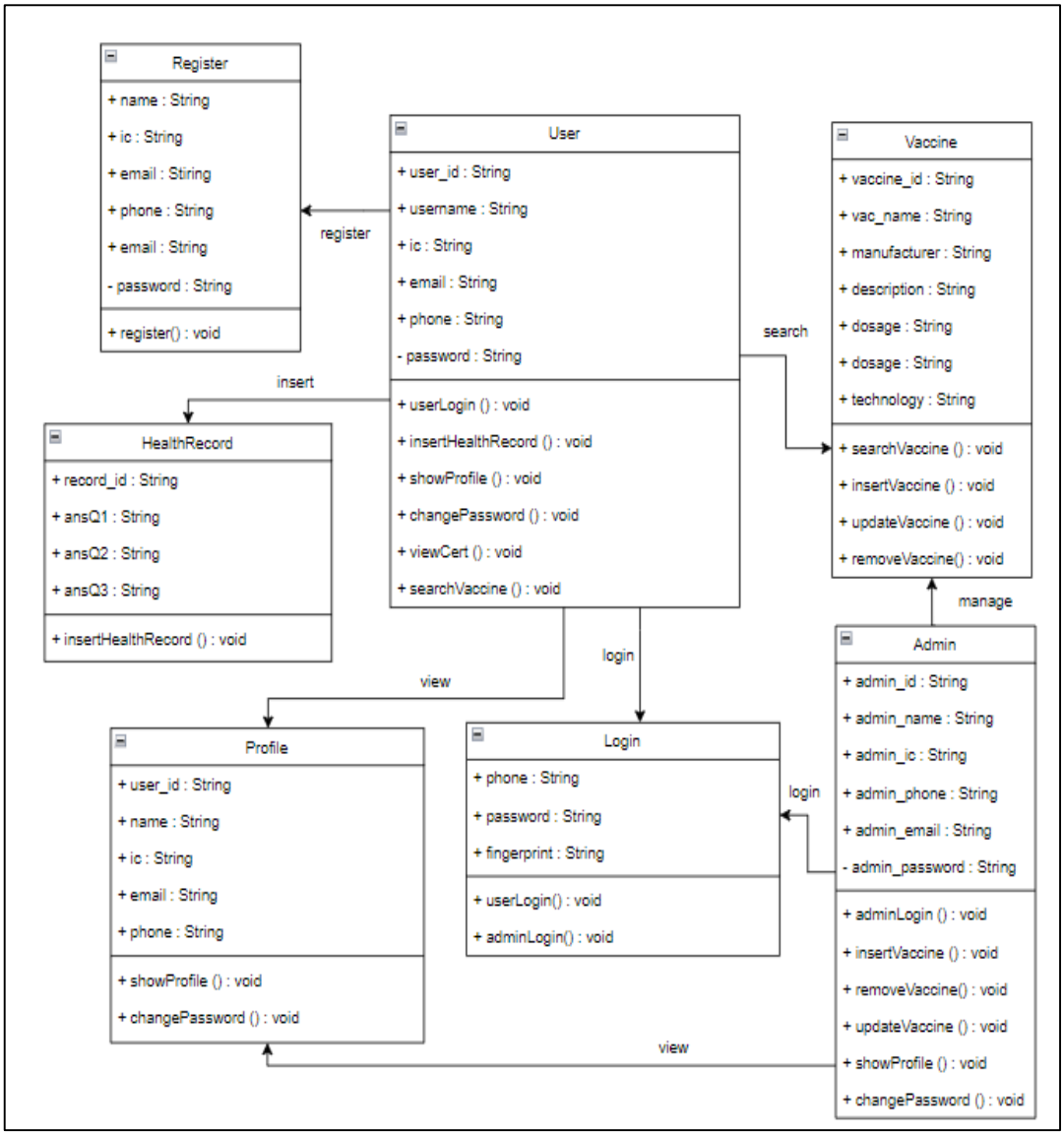

Figure 4: Class diagram

Figure 4 shows the class diagram for the proposed application. It shows the structure of the system by showing the relationship of various classes. Each class include its attributes and methods. There are seven classes for the proposed application, including two access levels: the user and admin. Users can insert health records, view digital certificates, view profiles, register, log in, search for vaccine information, and change passwords. The admin can also manage vaccine information, change passwords, and view profile.

3.4 Implementation Phase

The deliverable from the design phase is significant for the implementation phase. The development of the proposed application started after the database and interface of the system were designed. There are some hardware and software requirements used to build the proposed application. Hardware requirements are displayed in Table 5, and software requirements are displayed in Table 6.

Table 5: Hardware requirement of the proposed application

Hardware Requirement	Specification
Model	HP Pavilion Laptop 15-cs0xxx
Central Processing Unit (CPU)	Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz 1.80 GHz
Graphic Processing Unit (GPU)	NVIDIA GeForce MX150
Operating System (OS)	Window 10 64-bit Operating System
Random Access Memory (RAM)	16GB

Table 6: Software requirement of the proposed application

Software	Specification
Microsoft Word 2019	• Used for documentation
Mendeley Reference Manager	• Used for citation
Microsoft PowerPoint 2019	• Used for the presentation slide
Edraw Max	• Used to generate Gantt chart
Draw.io	• Used to draw the Entity-Relationship Diagram (ERD), wireframe, use case diagram, process flow diagram, sequence diagram, activity diagram, and class diagram.
Android Studio	• Used to develop the android application.
Firebase	• Used to store and retrieve data.
Wireframe.cc	• Used for interface design of the proposed application.

The proposed application was developed using Java Programming Language, an object-oriented language and Android Studio IDE. Extensible Markup Language (XML) will be used for the front-end design of the proposed application. In addition, Firebase is being utilized to connect the proposed application to the database. The database will be hosted on the server of Google Data Center. A simple prototype will be constructed initially to allow the user to test the system and provide complete feedback to the developer to improve the performance of the system.

3.5 Testing Phase

After the system is developed, a test plan will be carried out to test the proposed system in terms of functionality and security. The aim of the testing is to examine or run the code in different environments [14]. Errors and bugs will be fixed to ensure the performance of the proposed application. In addition, a user acceptance form will also be used to get feedback from the user after using the application.

4. Implementation

After the system was designed, the proposed application was implemented using Android Studio, Java programming language, and XML language for the front-end design. In addition, the proposed application will connect to a Realtime Database called Firebase to store users' data. The interfaces and the code segments of the proposed application will be discussed in this section.

Figure 5(a) shows the login interface of the user. Before accessing the application, users need to authenticate themselves to prevent unauthorized access to the system. The password will be obscured in the input field, and the proposed application will block the user after three times of failed login attempts. Moreover, a new user needs to register a new account by providing a username, IC number, email address, phone number and a strong password. Users need to verify the phone number through SMS authentication. The user will be redirected to the user's home page, as displayed in Figure 5(c).

There is COVID-19 related information on the home page displayed using a slide show and posters. Furthermore, there are real-time data retrieved from COVIDNOW websites, such as active cases, vaccination progress and the death cases due to COVID-19. In addition, there is a navigation bar located

at the bottom to redirect the user to other pages as well, including the home page, vaccine information page, health record page, digital certificate page, and profile page.

Figure 5(a): Login interface for user

Figure 5(b): Login interface for user

Figure 5(c): Home page of user

Furthermore, user can view their digital certificate on the proposed application. The digital certificate interface is shown in Figure 6(a). Before users access their digital certificate, the user needs to verify their identity through fingerprint recognition. A dialog will prompt to request the user's fingerprint pattern, as shown in Figure 6(b). The digital certificate will only be displayed if the user verifies their identity successfully. Figure 6(c) shows the sample of the user's digital certificate.

Figure 6(a): Digital certificate interface

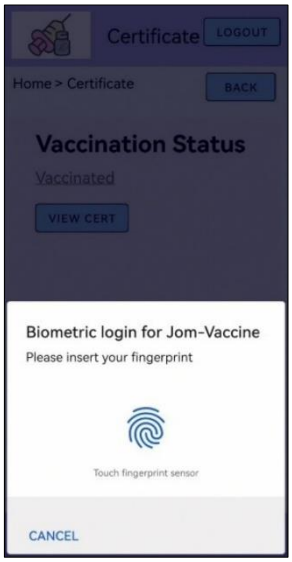

Figure 6(b): Digital certificate interface

Figure 6(c): Digital certificate sample

Figure 7 shows the code segment for the biometric authentication process of the proposed application. A dialog will be prompt if the user clicks the “view cert” button on the certificate page. If the digital device does not have a fingerprint sensor, an error message “Fingerprint does not exist” will display. If not, a message will display to request the user’s fingerprint pattern. The proposed application will compare the received fingerprint pattern to the fingerprint stored in the user’s mobile device. If the authentication succeeds, the proposed application will call displayedCert() to display the user’s digital

certificate. However, authentication failure will be shown to the user if there is an incorrect fingerprint or other error.

```
BiometricManager biometricManager = BiometricManager.from(this);
switch (biometricManager.canAuthenticate( authenticators: BIOMETRIC_STRONG | DEVICE_CREDENTIAL)) {
    case BiometricManager.BIOMETRIC_SUCCESS:
        Log.d( tag: "MY_APP_TAG",  msg: "App can authenticate using biometrics.");
        break;
    case BiometricManager.BIOMETRIC_ERROR_NO_HARDWARE:
        Toast.makeText( context: Certificate.this,  text: "Fingerprint Sensor not exist", Toast.LENGTH_SHORT).show();
        break;
    case BiometricManager.BIOMETRIC_ERROR_HW_UNAVAILABLE:
        Toast.makeText( context: Certificate.this,  text: "Fingerprint Sensor not available", Toast.LENGTH_SHORT).show();
        break;
    case BiometricManager.BIOMETRIC_ERROR_NONE_ENROLLED:
        // Prompts the user to create credentials that your app accepts.
        final Intent enrollIntent = new Intent(Settings.ACTION_BIOMETRIC_ENROLL);
        enrollIntent.putExtra(Settings.EXTRA_BIOMETRIC_AUTHENTICATORS_ALLOWED,
                value: BIOMETRIC_STRONG | DEVICE_CREDENTIAL);
        startActivityForResult(enrollIntent, REQUEST_CODE);
        break;
}
executor = ContextCompat.getMainExecutor( context: this);
```

Figure 7: Code segment of biometric authentication

Besides, the user can view the vaccine information on the vaccine info page shown in Figure 8(a). All the vaccines will be labelled with their name in the box. Furthermore, a search field allows users to search the vaccine's name using keywords. Figure 8(b) shows the search vaccine process. Users can view the vaccine information in detail by clicking the name of the vaccine. Then, the user will be redirected to the vaccine description page, as displayed in Figure 8(c). The vaccine information includes name, manufacturer, the technology used, dosage and description.

Figure 8(a): Vaccine info interface

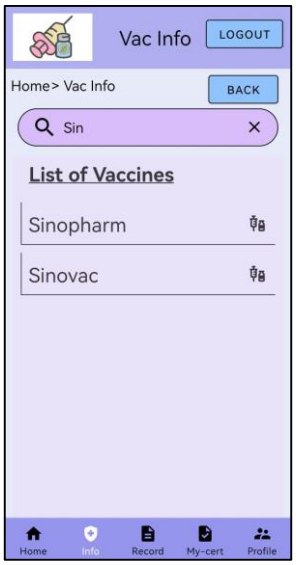

Figure 8(b): Searh vaccine process

Figure 8(c): Vaccine description page

The second target user of the proposed application is the admin. Admin has the higher privilege of managing the vaccine information published to the user on the vaccine information page. The admin login interface is shown in Figure 9(a), while Figure 9(b) shows the home page of the admin. Admin's home page contains the vaccination progress and death cases in Malaysia.

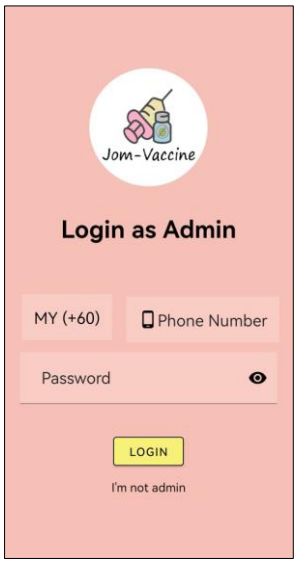

Figure 9(a): Login interface of admin

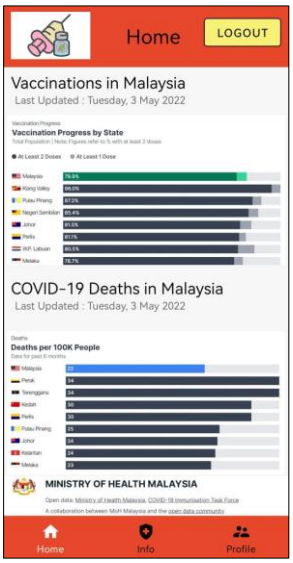

Figure 9(b): Home page of admin

5. Results and Discussion

This section discusses the testing results obtained during the testing phase. Functional testing, user acceptance testing, and biometric performance evaluation were carried out in this phase. Testing is required to ensure that the system meets its objectives and scopes and prevent any bugs or errors that have not been resolved.

5.1 Functional Testing

A test plan can effectively mitigate test risks and ensure smooth implementation. Table 7 shows the testing result of the proposed application, and Table 8 shows the result of the security checklist for the proposed application.

Table 7: Testing result of the proposed application

No	Functions	Test Case	Expected Result	Actual Result
1	Registration	Users insert incomplete data input	An alert message will display if the text field is empty.	Pass
		Users insert invalid email format	An alert message will display if the format of email is invalid.	Pass
		Users insert invalid phone format	An alert message will display if the format of phone is invalid.	Pass
		Users insert phone number that already exist	An alert message will display if the phone number exist in database.	Pass
		Users insert invalid IC format	An alert message will display if the format of IC number is invalid.	Pass
		The password insert by user does not meet the requirement of strong password policy.	An alert message will display if the password does not meet the strong password policy in term of length, and upper/lower case, special character and number.	Pass
		Users enter the incorrect OTP	An alert message will display if the OTP is incorrect.	Pass

Table 7: (cont)

No	Functions	Test Case	Expected Result	Actual Result
1	Registration	Users enter the correct OTP	A message "Registered successfully" will display and redirect user to login page	Pass
2	Login	Users insert incomplete data input	An alert message will display if the phone number or password is empty.	Pass
		Users insert invalid phone format	An alert message will display if the format of phone is invalid.	Pass
		Users insert invalid password format	An alert message will display if the password does not meet the strong password policy in term of length, and upper/lower case, special character and number.	Pass
		Users insert incorrect password or phone number	An alert message will display if the password or phone number is incorrect, but the error message does not directly indicate which authentication data is incorrect.	Pass
		Users insert valid phone number and password	Redirect user to home page	Pass
3	View vaccine information	Users enter the vaccine info page	Display all the vaccine from database	Pass
		Users search vaccine using upper case	Display vaccine according to user input Display "No result" if the vaccine does not exist.	Pass
		Users search vaccine using lower case	Display vaccine according to user input Display "No result" if the vaccine does not exist.	Pass
4	View digital certificate	Users scan an incorrect fingerprint pattern	Display message "Not recognised"	Pass
		Users scan a correct fingerprint pattern	Display the digital certificate	Pass
5	Insert health record	Users leave the question blank	An alert message will display if there is one question blank.	Pass
		Users does not agree to privacy policy	An alert message will display if user does not check the checkbox of privacy policy.	Pass
		User's health record exists in database	Display a message "Record updated".	Pass
6	View profile	Users enter the profile page	Display username, IC number, email, and phone number.	Pass
7	Manage vaccine	Admin click on the "ADD" button	Redirect admin to the add vaccine page	Pass
		Admin leave the input field blank	An alert message will display if one of the input fields is blank	Pass

Table 7: (cont)

No	Functions	Test Case	Expected Result	Actual Result
7	Manage vaccine	Admin click on the edit vaccine	An edit dialog pops up and redirect admin to the edit vaccine page if admin select the confirm button from the dialog.	Pass
		Admin click on the delete icon	A delete dialog pops up	Pass
8	Change password	Users leave the input field blank	An alert message will display if there is one input field blank.	Pass
		Users insert the incorrect wrong password	An alert message will display if the old password is incorrect.	Pass
		Users insert invalid password format for new password	An alert message will display if the new password does not meet the strong password policy in term of length, and upper/lower case, special character and number.	Pass
		Confirm password does not match the new password	An alert message will display if the confirm password does not match with the new password	Pass
		Confirm password match with the new password and correct old password	A message "Change Password Successfully" will display	Pass
9	Logout	Users select "Cancel" button	Close the logout dialog	Pass
		Users select "Confirm" button	Logout successfully and redirect to the login page	Pass
		Users select close button	Close the logout dialog	Pass

Table 8: Testing result of the proposed application

No	Check List	Actual Result
1	Ensure the error message does not directly indicate which authentication data is incorrect. For example, an error message should not show "incorrect password" or "incorrect phone number".	Pass
2	Ensure the complexity of the password for registering an account. The password should contain at least one upper case and lower-case letter, one number and one special character.	Pass
3	Ensure the password inserted by the user does not contain SQL injection attack symbols such as "= or +".	Pass
4	Enforce the length of the password between 10 to 20 characters.	Pass
5	Passwords should be obscured in the textbox.	Pass
6	Two-factor authentication is used for higher security. Apply fingerprint recognition to verify the user's identity.	Pass
7	Block user after three times of failed login attempts to prevent brute force attack	Pass

The test plan results show that the proposed system achieved all the expected results for all modules, such as login and logout for both admin and user, view vaccine information, view digital certificate, insert health record, view profile, and manage vaccine and change password. Besides that, the proposed application also reached the security checklist to ensure its security.

5.2 User Acceptance Testing

User acceptance testing form was created using Google Form and distributed to 30 android phone users to get their feedback. The user acceptance testing aims to evaluate the proposed application regarding interface, features, and security. The Google Form was separated into five questions for interface evaluation, seven questions for features evaluation, and seven questions for security checklist. The result of the user interface evaluation is shown in Table 9, while Table 10 shows the result of the application features evaluation. Lastly, the result of the security checklist was tabulated in Table 11. Besides, the result from Table 9, Table 10 and Table 11 were transferred into a bar graph to display the result graphically, as shown in Figure 10, Figure 11 and Figure 12.

Table 9: Result of user interface evaluation

No.	Features	Ranking					Total
		1	2	3	4	5	
1	Easy to use and understand	0	0	2	5	23	30
2	Navigation	0	0	1	12	17	30
3	Interface design	0	0	10	6	14	30
4	Text (font family, font size)	0	0	2	10	18	30
5	Layout for the content (colour, background)	0	0	3	8	19	30

Table 10: Result of application features evaluation

No.	Acceptance Requirement	Ranking					Total
		1	2	3	4	5	
1	The system can execute from start to end.	0	0	0	14	16	30
2	Users can register a new account.	0	0	1	15	14	30
3	Users can login to the application with their phone number and password.	0	0	3	7	20	30
4	Users can search for vaccine information.	0	0	2	11	17	30
5	Users can insert health records.	0	0	2	10	18	30
6	Users can view digital certificates.	0	0	1	12	17	30
7	Users can log out from the application.	0	0	2	11	17	30

Table 11: Result of security checklist for the proposed application

No	Security Requirement	Number of results		Total
		Pass	Fail	
1	Print out error message “incorrect credentials” for invalid credential.	30	0	30
2	Ensure the complexity of the password including at least one uppercase and lowercase letter, one number and one special character.	30	0	30
3	Enforce the length of the password is between 10 to 20 characters.	30	0	30
4	Print out error message “No SQL injection symbol is allowed” once detected from user input.	30	0	30
5	Password is obscured in the input field.	30	0	30
6	Print out error message “Not Recognized” for invalid fingerprint.	30	0	30
7	Block user for five minutes after three times of failed login attempts	30	0	30

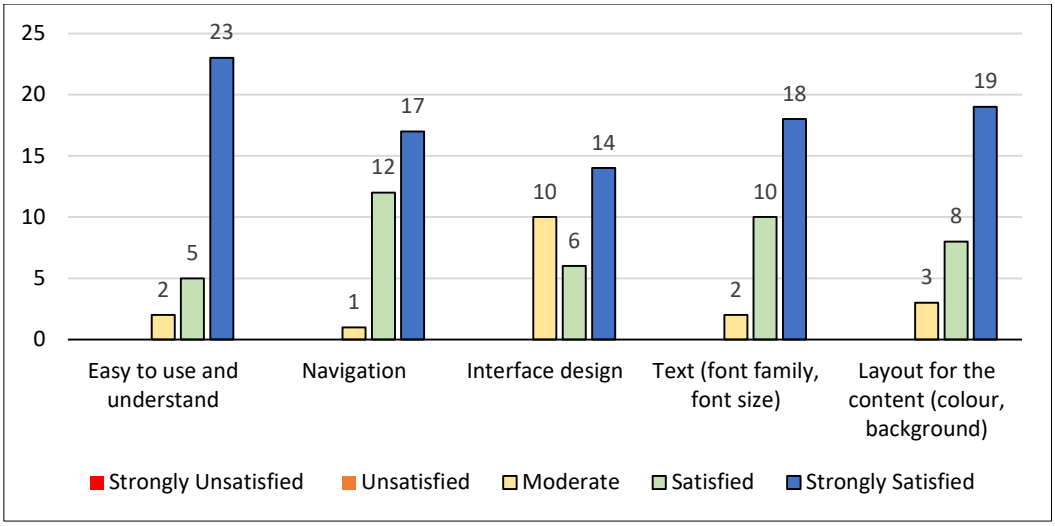

Figure 10: Interface satisfaction level of Jom Vaccine

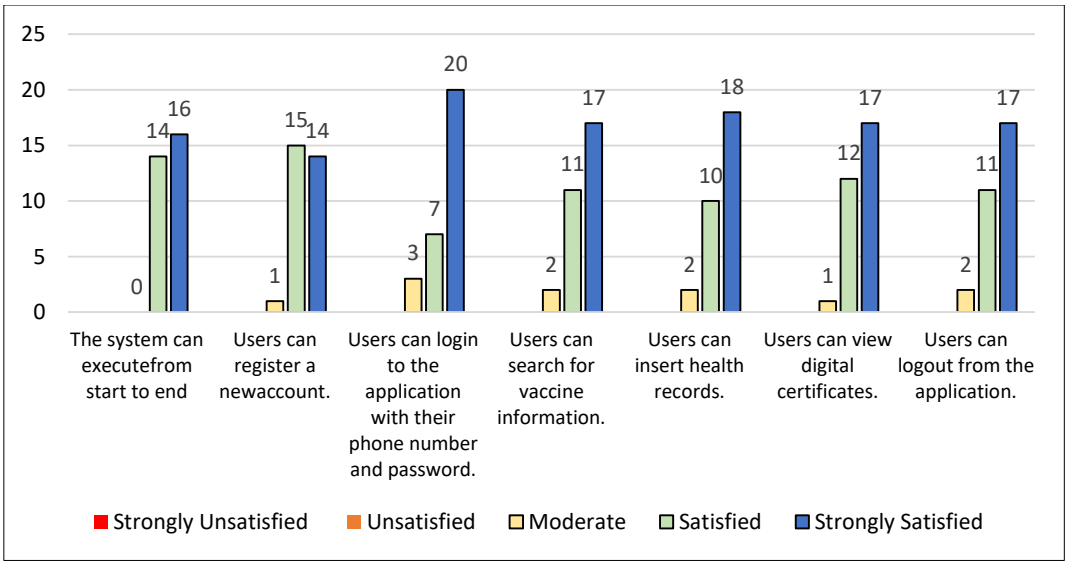

Figure 11: Functionality satisfaction level of Jom Vaccine

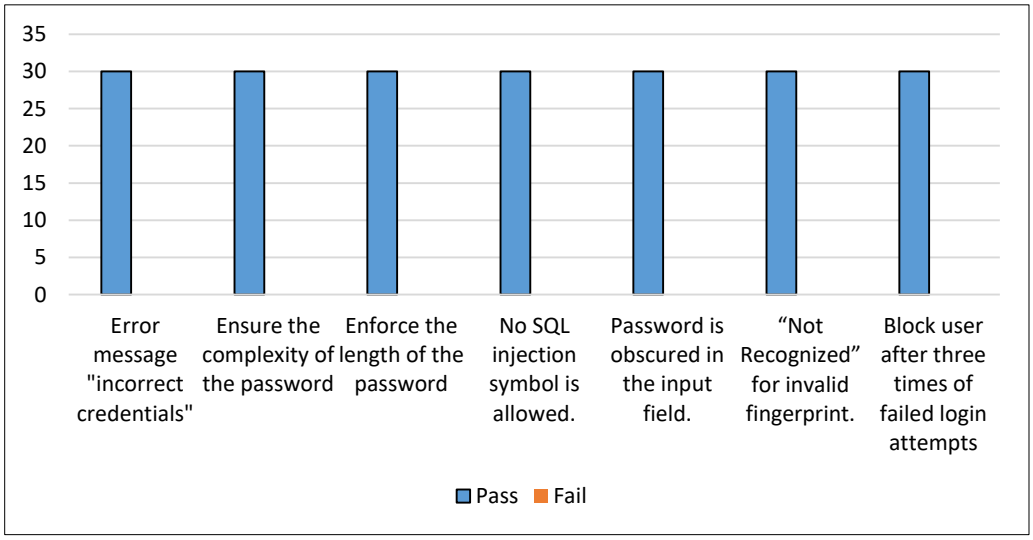

Figure 12: Security checklist of Jom Vaccine

From Figure 7, most users rate "5" for the application's interfaces with ease of use, navigation, text, and content layout. However, 10 respondents rate the interface design as “moderate” because the layout changed due to different phone sizes. Furthermore, more than three-quarters of users are satisfied with the application's features based on Figure 8, the application features evaluation. There is no user dissatisfied with the application's interfaces and features. Figure 9 shows the result of the security checklist of the application. 30 out of 30 respondents choose the "Pass" option. In other words, the proposed application fulfilled the security checklist.

5.3 Biometric Performance Evaluation

The false acceptance ratio (FAR) is a metric for calculating a biometric security system's average number of false positives. It determines the rate at which unauthorised or illegitimate users are verified on a particular system to measure and evaluate the efficiency and accuracy of a biometric system. The FAR is calculated by dividing the number of false acceptances by the number of identification attempts.

The formula of FAR as in (1),

$$FAR = \frac{FA}{TA} \tag{1}$$

FAR = False Acceptance Rate
FA = Number of False Acceptance (false positive)
TA = Total Number of Attempts

The false rejections rate (FRR) can be defined as the percentage of time that a valid user is rejected by the system (Azad, 2008). A false negative outcome is obtained when false rejection occurs because the user is labelled as an intruder. The less often the false rejection occurs, the lower the biometric performance of the biometric device.

The formula of FRR as in (2),

$$FRR = \frac{FR}{TA} \tag{2}$$

FRR = False Rejections Rate
FR = Number of False Rejections (false negative)
TA = Total Number of Attempts

The experiment is carried out 100 times, and the number of false acceptances is 1. From equation Eq. 1, $FAR = \frac{1}{100} = 0.01$. The false rejection rate will calculate using the formula Eq. 2, $FRR = \frac{2}{100} = 0.02$. The False Acceptance Rate of the proposed application is 0.01, which means that the biometric device allows 1 percent of false attempts to access the proposed application. However, the False Rejection Rate of the proposed application is 0.02, which means the biometric device rejects 2 out of 100 of true attempts to access the proposed application.

6. Conclusion

The project has achieved all the objectives, which are to design, develop and evaluate an Android-based Vaccination record System with multi-factor authentication. In addition, all the functional and non-functional requirements were fulfilled to increase the application's security level. For example, the sensitive data is encrypted, and the password is hashed before being stored in the database. Furthermore, multi-factor authentication such as SMS authentication and biometric authentication can prevent unauthorized access to the application. Lastly, the faking of the digital certificate can be prevented if biometric authentication is compulsory to verify a user's identity.

After the proposed application was developed, it underwent a test plan to fix bugs and ensure the proposed application's functionality. Besides that, the proposed application also undergoes user acceptance testing to evaluate its design, functionality, and security. The result shows that the proposed application got a good result from 30 random android phone users.

However, there are several disadvantages of the proposed application. First, the proposed application is only available on the android device with a fingerprint sensor. Since the proposed application aims to implement biometric authentication, the feature of the proposed system is less than those of the existing application, such as a QR code scanner. Next, the proposed application cannot ensure the integrity of the digital certificate of users because the digital certificate does not apply to a digital signature.

There are some recommendations to overcome the proposed application's weakness. First, the proposed application shall be able to support all operating systems, including iOS. Besides fingerprint recognition, the proposed application shall provide facial recognition while verifying their identity. Users will have more choices other than using fingerprint patterns. A digital signature can be implemented in each digital certificate to protect the certificate's integrity. Lastly, more functions such as QR code scanner, managing dependents, and scheduling vaccine appointments will be added to the proposed application to build a full-functioned application.

Acknowledgement

The authors would like to thank the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia for its support and encouragement throughout the process of conducting this study.

References

[1] P. K. Lakshmi, C. H. Saroja, and S. Bhaskaran, “Recent trends in vaccine delivery systems: A review INTRODUCTION,” International Journal of Pharmaceutical Investigation, no. 2, 2011, doi: 10.4103/2230-973X.82384.

[2] C. Z. Acemyan, P. Kortum, J. Xiong, and D. S. Wallach, “2FA might be secure, but it’s not usable: A summative usability assessment of Google’s two-factor authentication (2FA) methods,” Proceedings of the Human Factors and Ergonomics Society, vol. 2, pp. 1141–1145, 2018, doi: 10.1177/1541931218621262.

[3] M. H. Eldefrawy, M. K. Khan, K. Alghathbar, T. H. Kim, and H. Elkamchouchi, “Mobile one-time passwords: two-factor authentication using mobile phones,” Security and Communication Networks, vol. 5, no. 5, pp. 508–516, May 2012, doi: 10.1002/SEC.340.

[4] T. bin Azad, “Introduction to Security,” Securing Citrix Presentation Server in the Enterprise, pp. 1–67, 2008, doi: 10.1016/B978-1-59749-281-2.00001-9.

[5] M. Sarfraz, “Introductory Chapter: On Fingerprint Recognition,” Biometric Systems, Feb. 2021, doi: 10.5772/INTECHOPEN.95630.

[6] S. Deokar and S. Talele, “Literature Survey of Biometric Recognition Systems,” International Journal of Technology and Science, vol. 1, no. 2, 2014.

[7] Z. Huang, H. Guo, Y. M. Lee, E. C. Ho, H. Ang, and A. Chow, “Performance of Digital Contact Tracing Tools for COVID-19 Response in Singapore: Cross-Sectional Study,” JMIR Mhealth Uhealth, vol. 8, no. 10, Oct. 2020, doi: 10.2196/23148.

[8] A. Kapoor, S. Guha, M. Kanti Das, K. C. Goswami, and R. Yadav, "Digital healthcare: The only solution for better healthcare during COVID-19 pandemic?," Indian Heart Journal, vol. 72, no. 2, pp. 61–64, Mar. 2020, doi: 10.1016/J.IHJ.2020.04.001.

[9] (2021). MySejahtera (Version 1.0.449) [Mobile app]. Retrieved from Google Play Store. https://play.google.com/store/apps/details?id=my.gov.onegovappstore.mysejahtera. [Accessed Dec 12, 2021].

[10] (2021). TraceTogether (Version 2.11.0) [Mobile app]. Retrieved from Google Play Store. https://play.google.com/store/apps/details?id=sg.gov.tech.bluetrace. [Accessed Dec 12, 2021].

[11] G. Karopoulos, J. L. Hernandez-Ramos, V. Kouliaridis, and G. Kambourakis, "A Survey on Digital Certificates Approaches for the COVID-19 Pandemic," IEEE Access, vol. 9. Institute of Electrical and Electronics Engineers Inc., pp. 138003–138025, 2021. doi: 10.1109/ACCESS.2021.3117781.

[12] K. E. Kendall, J.E. Kendall, Systems analysis and design. 9th ed., New Jersey: Pearson Education., 2014.

[13] R. Ganpatrao Sabale and A. Dani, "Comparative Study of Prototype Model For Software Engineering With System Development Life Cycle," IOSR Journal of Engineering (IOSRJEN), vol. 2, no. 7, pp. 21–24, 2012. [Online]. Available: www.iosrjen.orgwww.iosrjen.org. [Accessed Dec 21, 2021].

[14] T. bin Azad, "Introduction to Security," Securing Citrix Presentation Server in the Enterprise, pp. 1–67, Jan. 2008, doi: 10.1016/B978-1-59749-281-2.00001-9.