APPLIED INFORMATION TECHNOLOGY AND COMPUTER SCIENCE
e-ISSN: 2773-5141

AITCS

Vol. 6 No. 2 (2025) 473-493
https://publisher.uthm.edu.my/periodicals/index.php/aitcs

TrustMyCounsell: A Secure Counselling Platform with Data Anonymization for Privacy Compliance

Quek Sze Yang[1], Nurul Hidayah Ab Rahman[1]*

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

*Corresponding Author: hidayahar@uthm.edu.my
DOI: https://doi.org/10.30880/aitcs.2025.06.02.026

Article Info

Received: 4 August 2025
Accepted: 19 November 2025
Available online: 30 November 2025

Keywords

Data Anonymization, Data Privacy, End-to-End Encryption(E2EE), Online Counselling, Personal Data Protection Act (PDPA)

Abstract

Online counselling has been among the most vital innovations within the mental health industry, particularly during the situation brought about by COVID-19 which there was a higher need to employ virtual means of communication. However, the lack of secure data protection for physical files, privacy concerns, and challenges in meeting Personal Data Protection Act (PDPA) requirements for remote services became apparent, eroding user trust. This study introduced TrustMyCounsell, a secure platform for KKTM Sri Gading, incorporating End-to-End Encryption (E2EE) for private communications and data anonymization to protect personal information. Developed via agile methodology, key modules include user registration, session booking, journaling, homework tracking, and feedback. Comprehensive functional testing confirmed module reliability. Security testing validated E2EE and data anonymization's effectiveness in ensuring confidentiality. User Acceptance Testing (UAT) affirmed the platform's user-friendliness, its success in enhancing trust, and streamlining counselling workflows. TrustMyCounsell offers a user-friendly, secure platform, reducing data breach risks and fostering a confidential environment for users by implementing robust data protection.

1. Introduction

Online counselling has been among the most vital innovations within the mental health industry, particularly during the situation brought about by COVID-19 which there was a higher need to employ virtual means of communication than had been the case earlier. However, counsellors and patient who engaging in counselling platform need to be aware of potential data privacy threats to the sensitive data and private information such as computer viruses, hackers, damage or theft of devices, inadequate security systems or software, unsecured electronic file and phishing scams [1]. The recent Vastaamo Psychotherapy Centre breach incident [2], which exposed sensitive data of 33,000 patients, emphasized the critical importance of robust security practices to protect user confidentiality. Maintenance of the privacy of personal information in counselling platforms is important to limit unauthorized access. Besides that, the report of the counselling session also needs to be protected that may include record, audio and text messages by using safe methods of communication [3]. The confidentiality of personal information is crucial to being protected in the digital era, particularly in the context of online counselling when private discussions and data are shared. The confidentiality guarantees are not only essential to therapeutic partnerships but also required by law [4]. This context reveals a critical problem within the current KKTM counselling system which lacks the robust infrastructure to defend against the data privacy threats discussed. Therefore, implementing a new system where privacy and data security are of paramount importance is essential to protect student confidentiality and trust.

Therefore, this study proposed TrustMyCounsell, a secure counselling management application designed to provide a confidential management platform through data privacy techniques for the booking session, journaling session and feedback session after face-to-face counselling between students, staff and counsellors at Kolej Kemahiran Tinggi MARA (KKTM) Sri Gading. In this application, data privacy techniques such as end-to-end encryption and data anonymization are implemented to prevent sensitive information from being unauthorized sharing or access.

End-to-end encryption (E2EE) is applied to keep the messages private from everyone by ensuring the message only appears in decrypted form for the sender and recipients while only the recipients can access the data. Data anonymization is implemented, which is the process of protecting sensitive information by masking the identifiers that connect an individual to stored data. TrustMyCounsell's clients include end users like students and staffs who are seeking help for personal, academic, mental or career health concerns in a secure environment, counsellors who providing professional support through the application, director who are the head of the counsellor to manage the application who want to monitor the application usage and ensuring compliance with privacy standards. The significance of TrustMyCounsell is to test its ability to provide a safe and secure application for users to engage in counselling services and ensure their personal and sensitive data remains secure. In the context of mental health and personal well-being, confidentiality is not only critical for building trust but also mandated by law. The proposed platform can foster a sense of safety to encourage more students and staffs to seek the help when they need.

The objectives are to design and develop TrustMyCounsell, a counselling management application with data privacy techniques that include end to end encryption, data anonymization and multi factor authentication. This study aims to test TrustMyCounsell through functional and non-functional testing, user acceptance testing, and security simulation scenario.

For the project scope, TrustMyCounsell involves students, staff, counsellor and director who is the head of the counsellors. The application allows students and staff to securely register with Multi-Factor Authentication (MFA), manage profiles with data anonymization for privacy, book counselling sessions, engage in end-to-end encrypted journaling and reflection which can be shared with counsellors, tracking homework, and provide feedback. Counsellors manage their availability, confirm bookings, upload various reports, assign homework, create feedback forms, and view shared journal entries. The director has oversight, for example, by viewing booking details and reports.

The remaining of the paper is organized as follows: Section 2 discusses the domain of study and the study of existing tools. Section 3 describes the agile methodology used in developing the proposed tools. Next, Section 4 discusses the system analysis and design of TrustMyCounsell. Section 5 discusses the implementation and testing. Then, Section 6 discusses about result and discussion while Section 7 concludes the paper.

2. Literature Review

This section explains the literature review of the project. It includes data privacy techniques such as end-to-end encryption and data anonymization and privacy design strategies. A comparison of related existing tools and the proposed tool is also presented. Data privacy ensures that sensitive information is kept away from unauthorized access [5]. To make the counselling management system trusted by user, effective data privacy techniques must be implemented to prevent the sensitive information in digital systems from being exposure and unauthorized access to ensure compliance with legal standards [5]. For instance, Malaysia's Personal Data Protection Act (PDPA) serves as such a legal standard, regulating personal data processing in commercial transactions to protect individuals' interests and compliance with PDPA can be supported by implementing data privacy techniques like data anonymization methods, such as data masking, which hide sensitive information to prevent unauthorized access and meet these regulatory requirements.

2.1 Data Privacy

Privacy by design is a concept in system design that aims of improving the general privacy friendliness of IT systems [6]. Privacy design strategies aim at embedding privacy considerations into the core architecture of systems and services to ensure data protection. These strategies support privacy by design in the software development life cycle [6]. There are eight privacy design strategies including minimise, separate, aggregate, hide, inform, control, enforce and demonstrate [6] and divided into two different categories which are data-oriented strategies and process-oriented strategies [7].

Data-oriented privacy strategies include minimise, hide, separate, and aggregate, while process-oriented strategies include inform, control, enforce, and demonstrate [7]. The minimise strategy limits a system's privacy impact by ensuring that the amount of personal information processed is minimal [6] and limit as much as possible [7]. The hide strategy ensures that any personal information is concealed from plain view, making it difficult to abuse. Separate involves processing or storing personal information in a distributed fashion across different sources, so that complete profiles of a single person cannot be easily constructed. Aggregate involves

processing personal information at the highest possible level of aggregation and with the least possible detail, which makes the data less sensitive by considering it at a group level rather than an individual one [6].

While in process-oriented strategies, inform is the data subjects should be adequately informed whenever personal information is processed [6] in a timely and adequate manner [7]. Control grants data subjects agency over their personal information, as simply informing them is of little value without also providing them with the means to manage its use. Enforce ensures that a privacy policy, compatible with legal requirements, is in place and actively enforced both during the system's development and its ongoing operation. Finally, demonstrate goes one step further than enforce, requiring the data controller to be able to actively prove compliance with the privacy policy and show how it is effectively confirming they are in control [6].

2.2 Data Anonymization

The rapid development of technology has made the information accessed and shared easily [8]. It is a must for protecting Personally Identifiable Information (PII) with the growing number of regulations and concerns regarding data privacy [9]. For instance, data masking can used in protecting the sensitive data and preserving confidentiality while maintaining the trust and integrity of data driven systems [8]. Data masking techniques will remove or hide the identities of the individual [9] to protect user identities while preserving system functionality. Data masking is to mask the characters at predefined positions which replaced by static values such as “X” or “-” or simply removed [9]. For example, data anonymization includes data masking, data generalization and data swapping.

Data generalization is a procedure of replacing the value with less specific, but semantically consistent value. This technique applies at the cellular level where some original values are maintained intact, but with more confusion added. This will amplify the confuse to an attacker to make an inference in sensitive data [10]. Data swapping is a process of rearranging variables within each column randomly. For this example, the attribute name can be used to scramble the data inside the same attribute. This technique cannot be applied for all attributes because the result of research may not be accurate. Thus, the main concern is the probability getting the same value as the original value due to the randomization process [10].

2.3 End-to-End Encryption

End-to-End Encryption (E2EE) is widely used in messaging applications such as WhatsApp[11]. E2EE is to prevent unauthorized third parties from intercepting or tampering with messages. By encrypting data from the sender to the recipient, E2EE provides strong privacy protection by ensuring that user communication remains confidential. In a counselling platform, E2EE can build the user trust in the application's confidentiality measures. There are some algorithms of E2EE that can be used such as Advanced Encryption Standard (AES) [12] and Diffie-Hellman key exchange [13].

AES performs several rounds as each performing transformations by using a round key which generated from the encryption key. The number of rounds depends on the block count and encryption key length. Encryption or decryption starts with a transformation by several rounds and ends with a round which is different. Each round has four transformations which are AddRoundKey, SubBytes, ShiftRows and MixColumns. The 128 bits key length (size) of encryption key would require 10 rounds and it has different key lengths for 128bits, 192bits, and 256 bits [12]. AES is highly secure, fast, and efficient in both hardware and software implementations, making it ideal for protecting large volumes of data. However, being a symmetric algorithm, AES requires both sender and receiver to possess the same key beforehand, which introduces challenges in secure key distribution and management.

Diffie-Hellman (DH) key exchange is a method of digital encryption in which breaking the codes becomes statistically impossible, since the numbers are raised to a particular power to create the decryption keys based on elements that are never physically conveyed. In Diffie-Hellman key exchange, the first party choose the prime numbers g and p and informs the second party of them. The second party then chooses a secret number, a which computes g * a mod p and transmits the result, A. The first party then follows suit, choosing a secret number b and computing the result, B in a manner akin to. The second party is then informed of this outcome. The second party calculates B * a mod p by using the received value B. After that, the first party computes A * b mod p using the received number A. The solution will be the same for both parties regardless of the sequence of exponentiation [13]. Using these values and their private numbers, both parties can compute the same shared secret key without transmitting it directly. This makes DH secure for establishing encryption keys in systems like end-to-end encryption. DH’s limitation is that it does not provide authentication and is vulnerable to man-in-the-middle attacks if used alone without additional protections. It also requires more computational resources compared to symmetric algorithms.

2.4 A Comparative Analysis of Existing Systems

There are three existing counselling related systems studied and reviewed in this part. The purpose is to study how the existing system works and what security features were implemented inside. The systems that were reviewed are Counselling Management System (CMS) UTHM[14], PlusVibes[15] and ThoughtFullChat[16] (see Table 1).

Table 1 *Comparison summary of existing systems*

Feature	Manual Counselling in KKTM Sri Gading	CMS UTHM[14]	PlusVibes [15]	ThoughtFullChat [16]	TrustMyCounsell (Proposed System)
Platform	No, is on paper	Web-based	Mobile-based	Mobile-based	Mobile-based
Can be accessed online	No	Yes	Yes	Yes	Yes
User Registration	Yes, save in files	No but the users' data and account are pulled from UTHM Student database	Yes	Yes	Yes
User Profile Management	Yes, by manually	Yes	Yes	Yes	Yes
Counselling Session Booking	Yes, by manually	Yes	Yes	Yes	Yes
Report	Yes, by manually	No	No	No	Yes
Journaling and Reflection	No	No	No	No	Yes
Homework Setting and Progress Tracking	Yes, by manually	No	Yes	Yes	Yes
Feedback Form	Yes, by manually	No	No	No	Yes
End-to-end encryption	No	Undefined	Undefined	Undefined	Yes
Data Anonymization	No	Undefined	Undefined	Yes	Yes
Multi Factor Authentication	No	Yes	No	No	Yes
Forgot Password	No	Yes	No	No	Yes

Based on Table 1, the manual system cannot be accessed online unlike the proposed system and other existing systems. Most of the existing systems does not have user registration module, report module, journaling and reflection module, homework setting and progress checking module. Manual Counselling in KKTM Sri Gading does not apply any data privacy techniques. For Counselling Management System (CMS) UTHM, PlusVibes and ThoughtFullChat applications, the end-to-end encryption used are undefined since does not any journal or evidence to proof explicitly that these platforms apply it in the system or applications.

While for data anonymization technique are undefined in CMS UTHM and PlusVibes because it does not any journal or evidence to proof explicitly that these platforms apply it in the system or applications. However, data anonymization is being used in ThoughtFullChat application. According to the privacy policy of ThoughtFullChat, the confidential information may be aggregated using computers, artificial intelligence and other IT-enabled tools and will be anonymised to become anonymised data. Anonymised data is not personal data, and it will not be identifiable from anonymised data [13]. In CMS UTHM, it applies MFA which is two-factor authentication (2FA) as password and One-Time Password (OTP) are required before login into the system [17]. But for PlusVibes and ThoughtFullChat, MFA is not being used in the applications after downloading and testing.

3. Methodology

TrustMyCounsell, a counselling management application is developed by using agile software development technique which refers to active and responsive software development [18]. The Agile methodology becomes widespread application in many organizations that have been used the traditional method such as waterfall approach or similar structured software development methods [19]. As shown in Fig. 1, the phases are adopted

Applied Information Technology and Computer Science Vol. 6 No. 2 (2025) p. 473-493

on a smaller scale in the Agile approach and are repeated for each product increment. The increments are then distributed over the iterations and then implemented. At the end of each iteration will be delivered a functional product increment [20]. The phases are adopted on a smaller scale in the Agile approach and are repeated for each product increment. The increments are then distributed over the iterations and then implemented. At the end of each iteration will be delivered a functional product increment [20]. Agile methodology consists of 6 phases: the plan phase, design phase, develop phase, test phase, deploy phase and review phase. The activities and expected outcomes of each phase of the prototyping methodology are presented in Table 2.

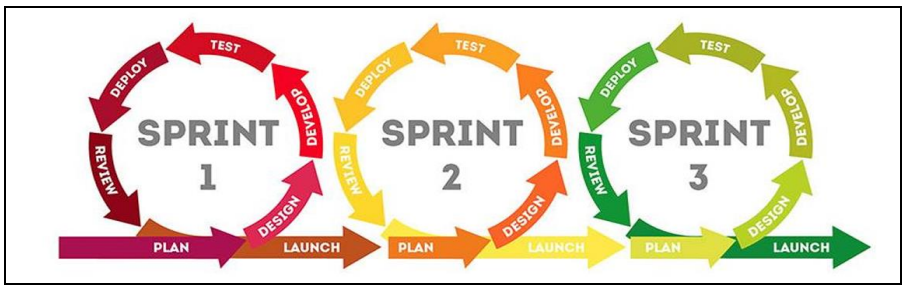


Fig.1 *Agile Methodology* [18]

Table 2 *System Development Activity and Outcome*

Phase	Activity	Outcome
Plan	Title Preparation Prepare proposal Engage with potential end-users Research and compare existing system Prepare a Gantt Chart based on the Agile Model Document problem statements, objectives, scope, and expected outcomes	Proposal Gantt Chart
Design	Create a detailed application architectural Design user interface Define user, functional, and non-functional requirements Define software and hardware requirements Develop UML diagrams (Use case, activity diagram, and sequence diagrams)	Application Architecture Design User, Functional and non functional requirements Software and hardware requirements User interface design UML diagrams (Use case, activity diagram, and sequence diagram)
Develop	Write source code Implement identified features and functionalities Application development	Counselling management application
Test	Implement test plan Assess the application's functionality under various scenarios Fix errors	Test plan results Error log and resolutions
Deploy	Provide installation instructions Adjust and optimize application performance on functionality and security based on real-world scenario	Installation guide Optimized and refined application
Review	Get feedback and evaluation Analyse feedback and suggestions Documentation of the feedback and evaluation results Improve application based on feedback	User acceptance testing form Improved application

The system architecture is used to illustrate the structure and function of TrustMyCounsell. The architecture for TrustMyCounsell is shown in Fig. 2. There are three users including the director, the counsellor, the student and staff. When a user such as director, counsellor, student and staff logs into the system, the system will send a request to the database before allowing the authenticated user to log in. After the user successfully accesses the system, the user can request to manage their modules from the database based on their roles. The user registration module authenticates the users while the user profile management module allows each user to update their profile data. Multi-Factor Authentication (MFA) would be implemented in the user registration module by supplementing the password with a second factor which is an email verification link to ensure that a

user's account remains inactive and inaccessible until they prove ownership of their email account, providing a critical defense against unauthorized access even if credentials are stolen. While for user profile management module, data masking would be applied to obscure Personally Identifiable Information (PII) on the user interface by default, requiring additional authentication such as password re-entry to reveal sensitive details, thus securing user data even during an active session.

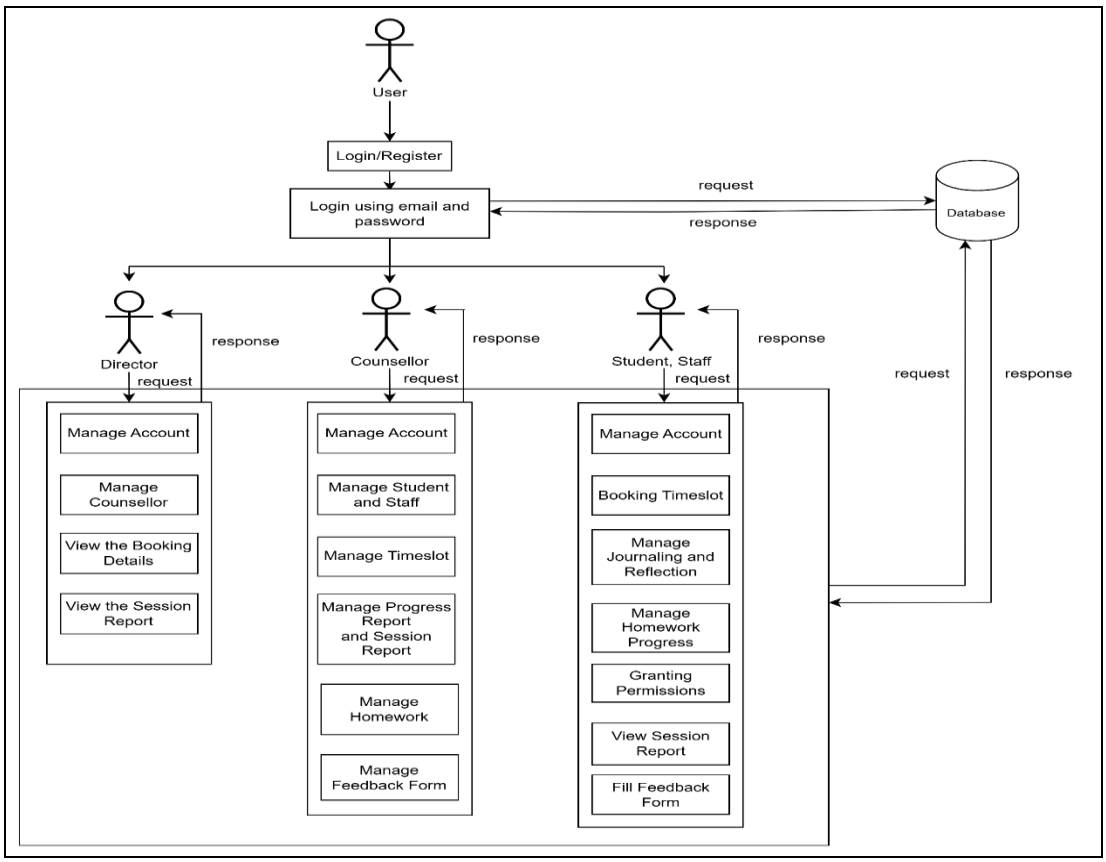


Fig.2 *System Architecture of TrustMyCounsell*

The counselling session booking module enables dual interaction where students book timeslots and counsellors manage availability. Similarly, the report modules allow the counsellors to manage students' progress and session reports, with viewing permission granted to students and directors. The architecture also includes unique grants students access to the sensitive journaling and reflection module for private entries and the ability to control sharing via permissions to their counsellors. End-to-End Encryption (E2EE) would be applied in journaling and reflection modules which means that a student's private entries are encrypted. This renders the data unreadable without having the user's private key and leverages a secure key exchange when a user explicitly grants sharing via permissions to their counsellor. Finally, the homework and feedback modules allow counsellors to manage assignments and forms while students track progress and submit responses, with all data interactions securely handled by the central database.

4. System Analysis and Design

This section explores systematic analysis and design of TrustMyCounsell. The objective is to define system requirements and formulate a well design for the application.

4.1 System Requirements

The requirement analysis is done to understand the system's requirements and to determine the actual function or process of the TrustMyCounsell. Table 3 shows the list of functional requirements, Table 4 shows non-functional requirement analysis and Table 5 show security and privacy requirements analysis.

Table 3 *Functional Requirements*

No	Functional Requirements

1.	The application should be able to provide a login page for all users and a register page for the students and staff.
2.	The application should allow student, staff, counsellor and director to change passwords.
3.	The application should allow student, staff, counsellor and director to update their profile.
4.	The application should allow the director to add, update or delete counsellor.
5.	The application should allow the counsellor to add, update or delete student and staff.
6.	The application should allow the counsellor to add, update or delete available timeslot.
7.	The application should allow the student and staff to add, update or delete booking of the available timeslot.
8.	The application should allow the director and counsellor to view booking details.
9.	The application should allow the counsellor to add, update or delete progress report and session report of the counselling.
10.	The application should allow the director, student and staff to view the progress report.
11.	The application should allow student and staff to add, update or delete their journaling and reflection.
12.	The application should allow student, staff for granting the counsellor the permission for view the journaling and reflection.
13.	The application should allow counsellor to add, update or delete homework for the end-users.
14.	The application should allow student, staff and counsellor to view the homework progress.
15.	The application should allow counsellor to add, update or delete the feedback form of the counselling session.
16.	The application should allow counsellor to view the result of the feedback form.
17.	The application should allow student and staff to fill the feedback form of the counselling session.

Table 4 *Non-functional Requirements*

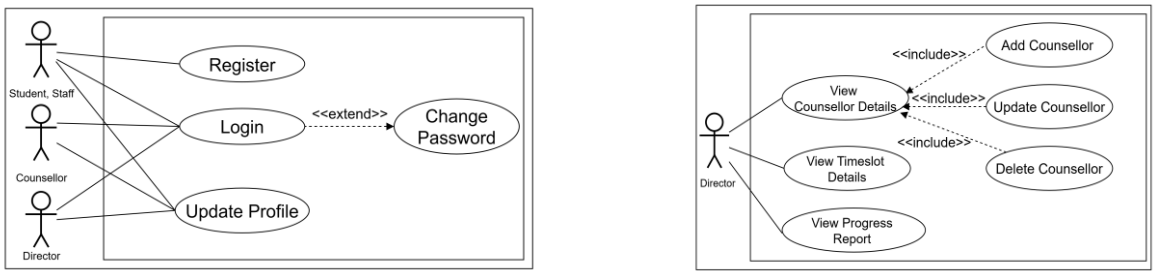
No	Non-functional Requirements
1.	The application should be able to respond promptly under normal operating conditions
2.	The application should be able to support the increasing user loads over time.
3.	The application must provide consistent performance with minimal downtime.
4.	The application should include the interfaces which easy to navigate for users.

Table 5 *Security and Privacy Requirements*

No	Security and Privacy Requirements
1.	The application should be able to authenticate and authorize users' credentials.
2.	The application should apply password complexity with a minimum of 8 characters and a combination of alphanumeric and symbols.
3.	The application should encrypt all the sensitive data and password which storing in the database.
4.	The application should apply data anonymization for sensitive information in the application interface.
5.	The application should apply the session timeout when the user is inactive within three minutes.
6.	The application should apply end-to-end encryption for the session counselling such as journaling and reflection.

4.2 System Analysis

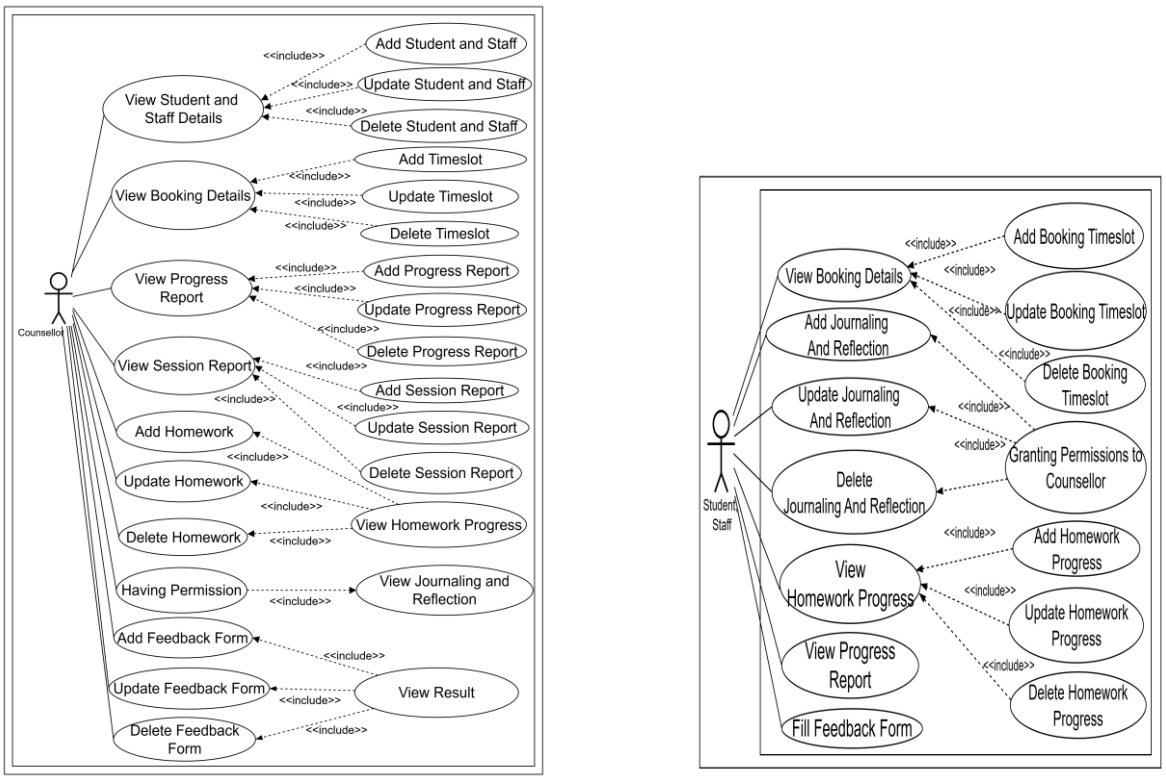
The general use case for each user is shown in Fig. 3(a) that explains director, counsellor, student and staff are required to login into the system first, student and staff need to register if they do not have an account. The users can change their password and update their profile if needed. Fig. 3(b) shows the use case for the director who is the head of the counsellors that can view the booking details and progress report for each student and staff for future reference.



(a) **(b)**

Fig.3 *Use Case Diagram (a) General Use Case for all users; (b) Director*

In Fig. 4(a), the use case diagram of counsellor is shown. The counsellor can CREATE, READ, UPDATE, DELETE (CRUD) for students and staff, available timeslot and view the booking details. The counsellor can CRUD the progress report, session report, homework and feedback form. In terms of homework, the counsellor can view the progress of homework of the student and staff. If the counsellor has permission from the student and staff, they can view and access the journaling and reflection. Fig. 4(b) presents the use case for students and staff. Student and staff can CRUD the timeslot available according to their free time and preferences. They can view the booking details after confirmation. They allow to CRUD for journaling and reflection which can grant the permissions to counsellor to view the journaling and reflection, and the homework progress. Besides, they are allowed to fill feedback form and view progress report.



(a) **(b)**

Fig.4 *Use Case Diagram (a) Counsellor; (b) Student and Staff*

Fig. 5 shows the activity diagram for director. Director is required to enter their email and password then; the application will verify the email and password. If the login is successful, the director can access the application. Director can choose the action to do including managing profile, managing counsellor and viewing the booking details and session report.

Applied Information Technology and Computer Science Vol. 6 No. 2 (2025) p. 473-493

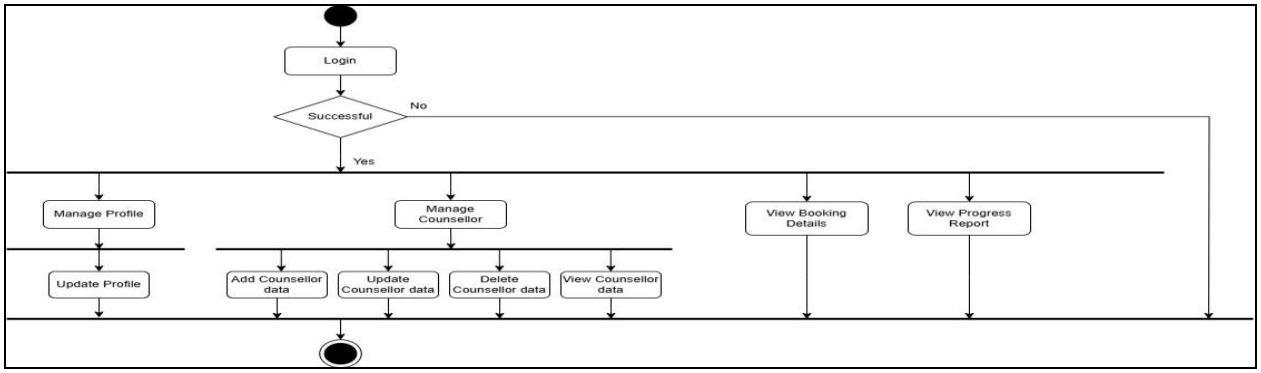


Fig.5 *Activity Diagram Director*

Fig. 6 shows the activity diagram for the counsellor. The counsellor is required to enter their email and password then; the application will verify the email and password. If the login is successful, the counsellor can access it into application. The counsellor can choose the action to do including managing profile, student and staff and the available timeslot. Besides, the counsellor can manage progress report, session report, homework and feedback form. Counsellor can view student and staff homework progress and view journaling and reflection of student and staff if permit by student and staff.

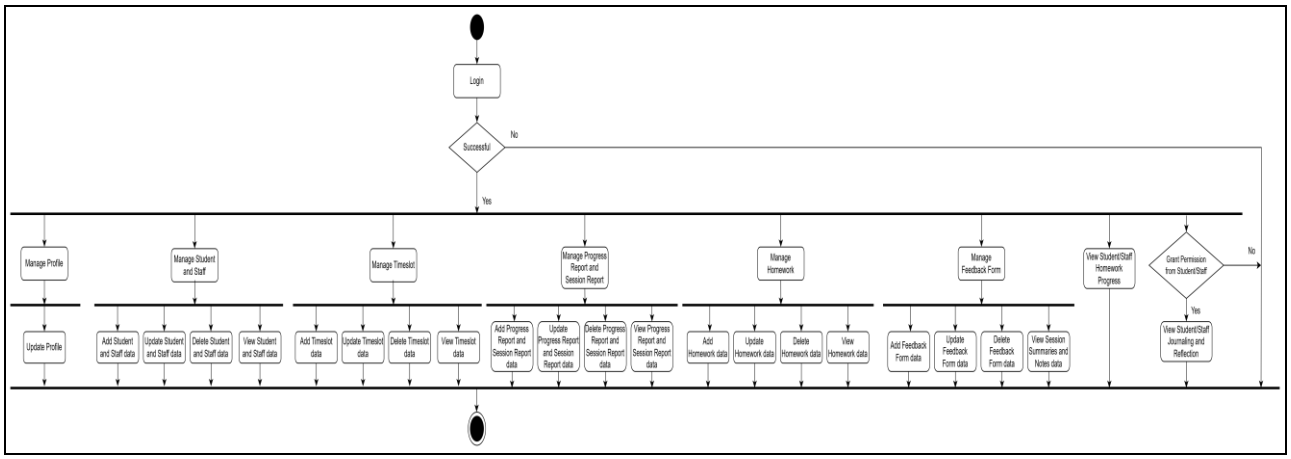


Fig.6 *Activity Diagram Counsellor*

In Fig. 7, the activity diagram for student and staff is shown. Student and staff is required to enter their email and password then; the application will verify the email and password. If the login is successful, student and staff can access into application. Student and staff can choose the action to do including manage profile, book the available timeslot, manage journaling and reflection and homework. Besides, student and staff can grant permission to counsellor to view their journaling and reflection. Student and staff can view progress report and fill feedback form.

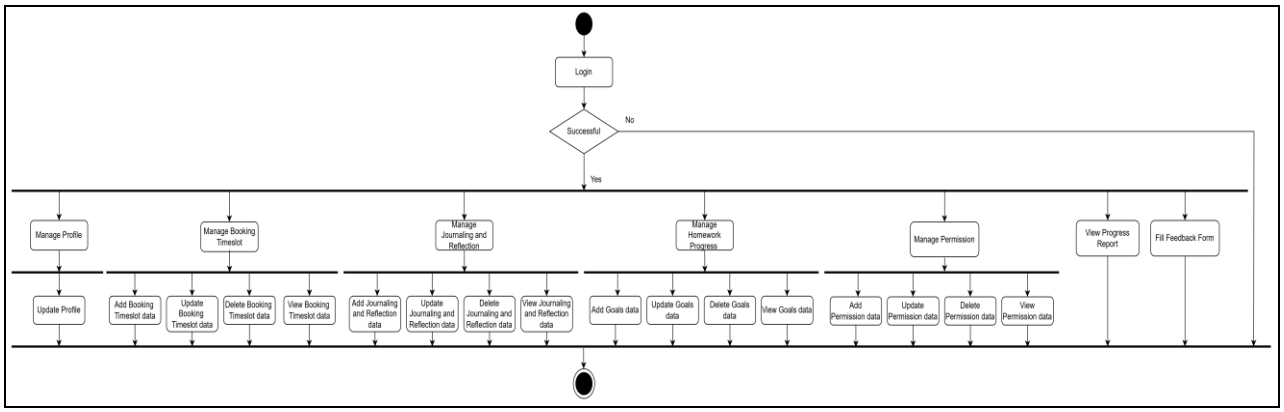


Fig.7 *Activity Diagram Student and Staff*

While Appendix A shows the class diagram for TrustMyCounsell. The class diagram describes the attributes, operations and relationships between the object by modelling the general structure for TrustMyCounsell. The diagram essentially shows how this different user types create, manage, and access specific information modules to facilitate organized counselling service.

5. Implementation and Testing

This section discusses the implementation of TrustMyCounsell. The implementation includes some security features and main modules that will be discussed clearly.

5.1 Implementation of Security Features

The proposed security and privacy features which mentioned in section 1 have been successfully applied on TrustMyCounsell. The security features are used at journaling and reflection, user profile management, signup page and others related modules while privacy features are used at journaling and reflection and user profile management.

TrustMyCounsell uses End-to-End Encryption, starting with Diffie-Hellman to let two parties securely create a shared secret key without anyone else seeing it as in Fig. 8. This shared secret is then used to make an AES key, which encrypts and decrypts sensitive journaling and reflection data. For storage, the user's private Diffie-Hellman key is kept as a hexadecimal string in Firestore, along with public keys and the encrypted data. When the app starts, a function called retrieveKeyPair fetches this hex private key string from Firestore. It then converts this string back into a usable private key, calculates the matching public key, and loads this complete key pair into the app's memory, making the system ready for secure cryptographic operations.

```
Future<bool> retrieveKeyPair(String userId) async {
  try {
    DocumentSnapshot doc = await FirebaseFirestore.instance
        .collection('user_keys')
        .doc(userId)
        .get();
    if (!doc.exists || doc.data() == null) {
      print('User key document not found in Firestore for user: $userId');
      return false;
    }

    var data = doc.data() as Map<String, dynamic>;
    if (!data.containsKey('dhPrivateKey')) {
      print('Private key not found in Firestore for user: $userId');
      return false;
    }

    String privateKeyHex = data['dhPrivateKey'];
    BigInt privateKeyValue = BigInt.parse(privateKeyHex, radix: 16);
    _dhEngine ??= DhPkcs3Engine.fromGroup(DhGroup.g5);

    DhParameter parameter = DhGroup.g5.parameter;
    DhPrivateKey privateKey = DhPrivateKey(privateKeyValue, parameter: parameter);

    DhPublicKey publicKey = DhPublicKey(
      parameter.g.modPow(privateKeyValue, parameter.p),
      parameter: parameter
    );

    keyPair = DhKeyPair(
      publicKey: publicKey,
      privateKey: privateKey,
    );

    _dhEngine = DhPkcs3Engine.fromKeyPair(keyPair!);

    print('Key pair successfully reconstructed for user: $userId');
    return true;
  } catch (e) {
    print('Error retrieving/reconstructing key pair: $e');
    return false;
  }
}
```

Fig.8 *Code of Fetching Key Pair*

If a user's keys are not found, the system generates a new Diffie-Hellman public and private key pair which shows in Fig. 9(a). Both keys are then converted to hexadecimal strings and uploaded to Firestore, making the public key available for others to initiate a key exchange, while also storing the user's private key. To communicate, the app fetches the other party's public key from Firestore. This public key, along with the current user's own private key, is used in a Diffie-Hellman calculation to compute a shared secret as in Fig. 9(b). This shared secret is then converted to bytes and hashed (using SHA-256) to derive a consistent symmetric AES encryption key. Finally, messages are encrypted using this AES key and an Initialization Vector (IV), with the encrypted data and IV bundled together, often as Base64 encoded strings, for storage.

```dart
DhKeyPair generateKeyPair() {
  _dhEngine ??= DhPkcs3Engine.fromGroup(DhGroup.g5);

  keyPair = _dhEngine!.generateKeyPair();
  return keyPair!;
}
```

(a)

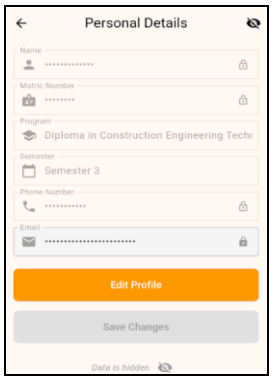
```dart
BigInt computeSharedSecret(BigInt otherPublicKey) {
  if (_dhEngine == null || keyPair == null) {
    throw Exception('Key pair not available. Generate or retrieve key pair first.');
  }

  return _dhEngine!.computeSecretKey(otherPublicKey);
}
```

(b)

Fig.9 *Code for (a) generateKeyPair function; (b) computeSharedSecret function*

In Fig. 10(a), TrustMyCounsell will mask the sensitive user information in its interface by default, showing characters like '•' instead of the actual data which can prevent people from casually seeing private details. A setting will determine if the data is hidden or shown. UI fields use a feature that's turned on or off based on this setting and whether that specific field is meant to be masked. While Fig. 10(b) shows that TrustMyCounsell uses Multi-Factor Authentication (MFA) for sign-up page. This means users must provide a strong password (something they know) and verify their email by clicking a link sent by the app using Firebase Authentication (something they have). Fig. 11 shows the pseudocode for the data masking applied.



(a)

```dart
void _signup() async {
  if (_formKey.currentState!.validate()) {
    try {
      UserCredential userCredential = await _auth.createUserWithEmailAndPassword(
        email: _emailController.text.trim(),
        password: _passwordController.text.trim(),
      );

      await userCredential.user!.sendEmailVerification();

      _showVerificationDialog();
    } catch (e) {
      ScaffoldMessenger.of(context).showSnackBar(
        SnackBar(content: Text('Failed to sign up: $e')),
      );
    }
  }
}
```

(b)

Fig.10 *(a) Interface for data masking; (b) Code for Multi-Factor Authentication*

```
FUNCTION ShowPasswordVerificationDialog():
    DISPLAY a dialog with a password input field and a "Verify" button.
    user_entered_password = GET text from the password dialog
    is_verified = CALL VerifyPassword(user_entered_password)
    IF is_verified is TRUE THEN
        is_data_masked = FALSE
        REFRESH_UI()
    ELSE
        DISPLAY "Incorrect password" error.
    END IF
END FUNCTION

FUNCTION VerifyPassword(password):
    authentication_result = AUTH_SERVICE.reauthenticate(email, password)
    IF authentication_result is SUCCESS THEN
        RETURN TRUE
    ELSE
        RETURN FALSE
    END IF
END FUNCTION

PROCEDURE Main():
    is_data_masked = TRUE
    LOAD_USER_DATA()
    RENDER UI with sensitive_data_fields and toggle_visibility_button
END PROCEDURE
```

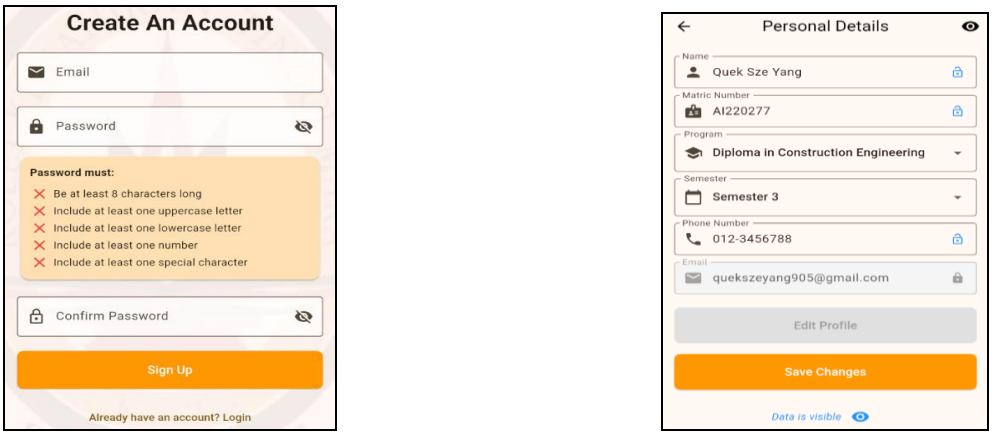
Fig.11 *Pseudocode of Data Masking*

5.2 Implementation of Modules

The main modules' implementation is discussed in this section which include user registration, user profile management, counselling session booking, report, journaling and reflection, homework setting and progress tracking and feedback form. Students and staff can sign up by entering their email and password as Fig. 12(a). While typing the password, a live checklist helps them create a strong one. If everything is correct, a verification

email is sent, and they're guided to the login page. If there are mistakes, a clear message explains how to fix them. They can also easily switch to the login screen if they already have an account.

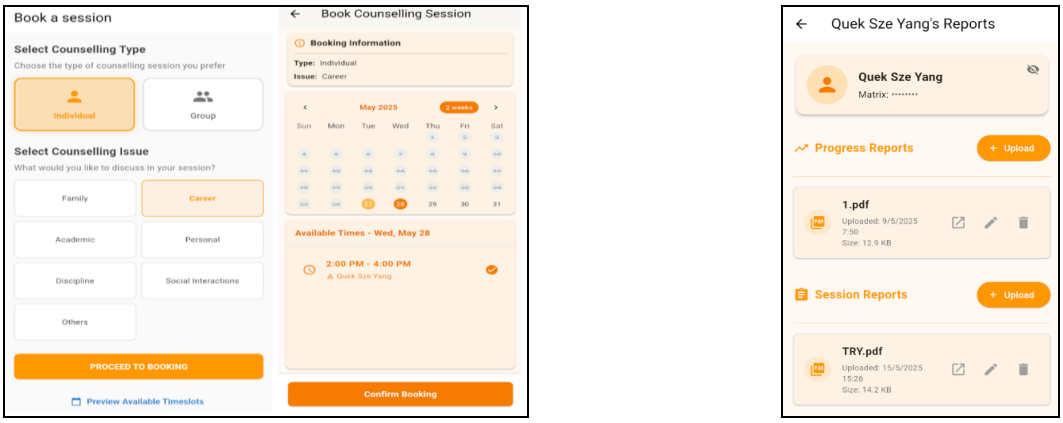
In Fig. 12(b), the users can see their profile information, but the sensitive data is masked by default for privacy. To view this masked information, they tap an eye icon and will prompt them to enter their password for verification. Once verified, they can see all details and edit fields such as their name, program, semester, and phone number (but not their email). Any changes they make can be saved to update their profile. The approach is consistent with established best practices for protecting Personally Identifiable Information (PII) at the presentation layer that is often seen in financial and government applications where sensitive data like account numbers or national IDs are masked by default. This method supports the security principles outlined in Malaysia's Personal Data Protection Act (PDPA) by taking practical steps to prevent unauthorized or accidental access to personal data [21]. Furthermore, it also aligns with OWASP recommendations regarding 'Broken Access Control' [22] by ensuring only the authenticated user can unmask their data and contribute to preventing 'Sensitive Data Exposure' [23] at the user interface level.



(a) **(b)**

Fig.12 *Interface for (a) User Registration; (b) User Profile Management*

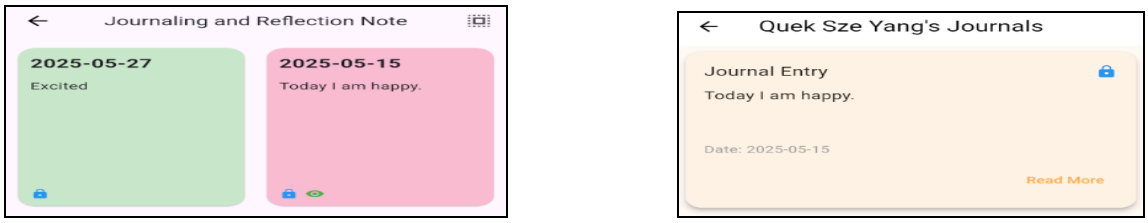
Fig. 13(a) shows the booking modules for students and staff so they can choose their preferred counselling type and issue. On the booking screen, these choices are confirmed at the top. They then pick a date from a calendar, and the screen shows available time slots for that day. Separately, counsellors manage students, and staff reports as shown in Fig. 13(b), which are divided into progress reports and session reports. In each section, counsellors can view, edit the display name of, delete, or upload new report files for specific individuals.



(a) **(b)**

Fig.13 *Interface for (a) Counselling Session Booking; (b) Report*

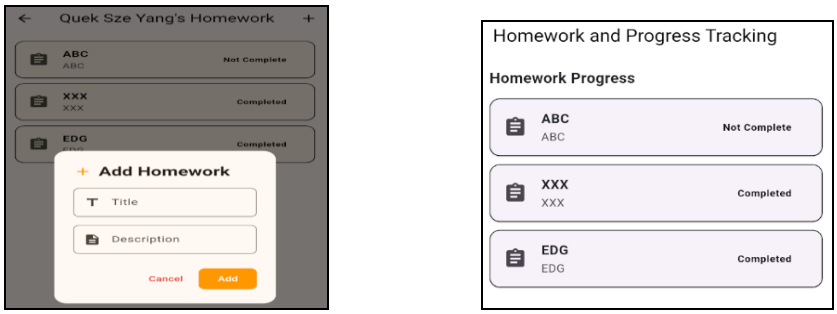
In Fig. 14(a), the students and staff can create, view, edit, and delete their journal entries, which are automatically encrypted for privacy. They can choose to securely share specific entries with their assigned counsellor and can also delete multiple notes at once. Counsellors, in turn, can see new, unread shared journal entries. By selecting an individual's name, counsellors can securely view only the entries that a person has explicitly shared, which the system automatically decrypts for them. This is shown in Fig. 14(b).



(a) (b)

Fig.14 *Interface for Journaling and Reflection of (a) Student and Staff; (b) Counsellor*

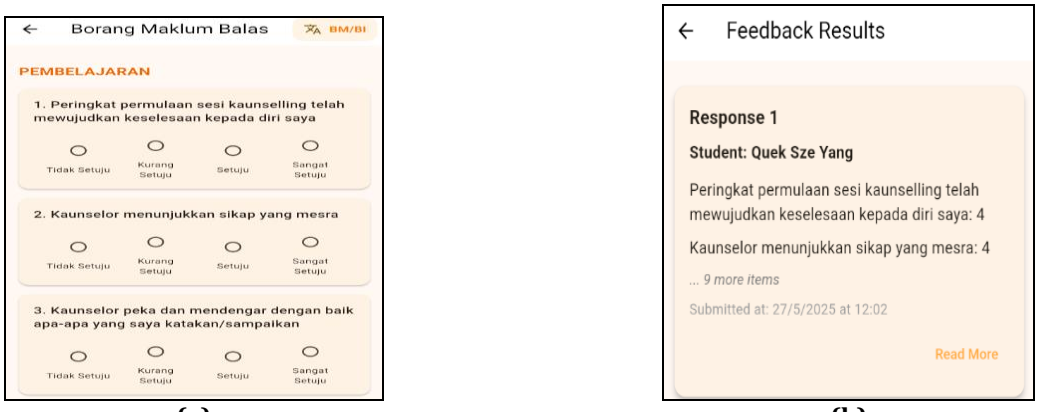
The app also offers a homework module. In Fig. 15(a), the counsellors can view their students, select one, and assign new homework with titles and descriptions. They can also manage existing tasks for that student which check submission status, review submitted work, edit details, delete tasks, or mark them as complete. While in Fig. 15(b), the students and staff see their own assigned homework list, view task descriptions, and submit their work by typing responses or uploading files and can also manage their previously submitted files.



(a) (b)

Fig.15 *Interface for Homework Setting and Progress Tracking of (a) Student and Staff; (b) Counsellor*

The users can fill out a feedback form in Fig. 16(a) by answering questions by selecting an agreement level and others with written suggestions and then submitting their responses. Counsellors, on their end, can create, view, edit, and delete the questions that appear on this form. They also have a separate screen to see all the feedback submitted by students which are shown in Fig. 16(b).



(a) (b)

Fig.16 *Interface for Feedback Form of (a) Student and Staff; (b) Counsellor*

6. Result and Discussion

This section discusses the testing results of the proposed system. Two types of testing results are presented: the test plan result and the user acceptance result. The testing phase encompassed the entire system verify its security and adherence to project requirements.

6.1 Testing Plan Result

The results of the testing plan are presented here. Table 6 displays the result of the functionality test plan, while Table 7 outlines the results of the security test plan.

Table 6 *Test Report of Functional Testing*

Functional Testing Checklist	Pass	Fail
User can login into system with valid email and password.	/	
Error message is shown for invalid input.	/	
The buttons in the system are visible and working well.	/	
All pages in the system working properly.	/	

Table 7 *Test Report of Security Features*

Security Features Testing Checklist	Pass	Fail
Masked out several characters of all information using asterisk symbol (*) in the application interface.	/	
All the sensitive data and password which storing in the database are encrypted.	/	
The session timeout when the user is inactive within three minutes.	/	
End-to-end encryption is applied in modules such as journaling and reflection.	/	

6.2 User Acceptance Testing

User acceptance testing for TrustMyCounsell was conducted physically with 20 participants from Kolej Kemahiran Tinggi MARA including 18 students, one counsellor, and one director by using an online Google Form survey. The Google Form questionnaire can refer to Appendix C. The goal was to evaluate the app's usability, effectiveness, features, user interface, and overall user satisfaction, while also gathering feedback. User feedback on TrustMyCounsell's effectiveness was largely positive. In Fig. 17 the students and staff generally found the app's features worked well, with most selecting 'Agree' or 'Strongly Agree', few neutral responses, and very little negative feedback. While the participating counsellor was extremely positive, rating all specialized features as 'Strongly Agree,' finding them excellent and perfectly suited to their needs without any problems as shown in Fig. 18. Likewise, the director 'Strongly Agree' shows in Fig. 19 with all aspects of the app's user experience, ease of use, and overall usefulness, indicating they found it outstanding.

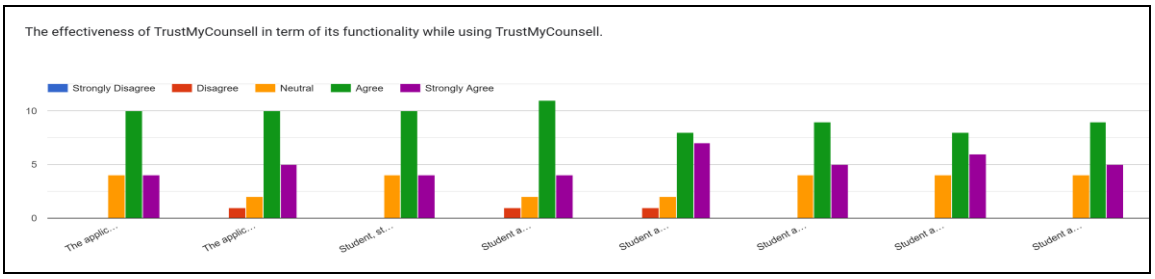


Fig.17 *Result User Acceptance Testing for Student and Staff in functionality*

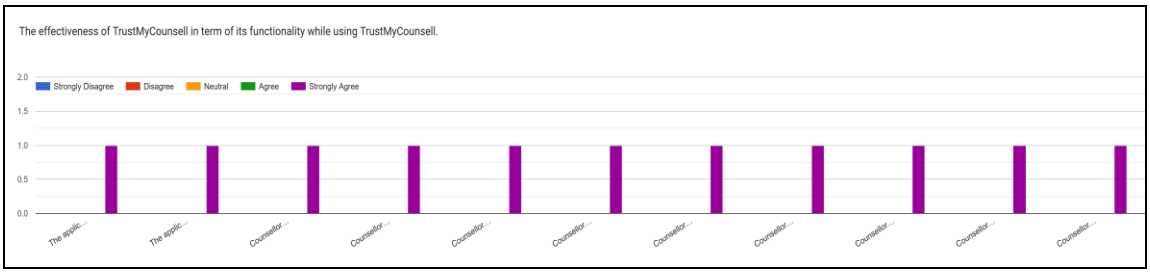


Fig.18 *Result User Acceptance Testing for Counsellor in functionality*

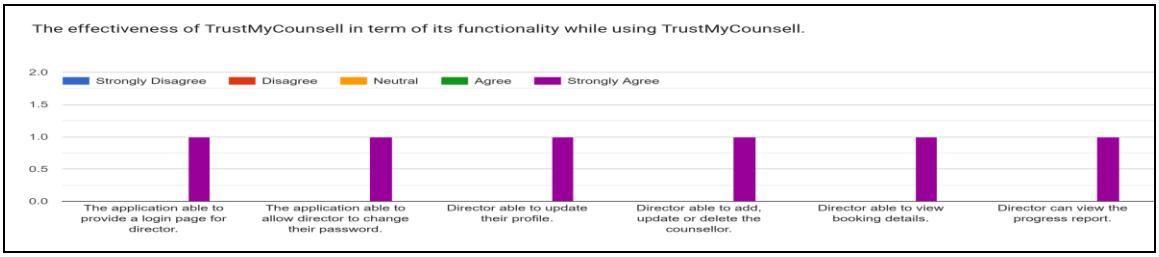


Fig.19 *Result User Acceptance Testing for Director in functionality*

Overall, users felt TrustMyCounsell's security and privacy features were effective. Most students and staff agreed or strongly agreed shown in Fig. 20 with the measures, with some neutral responses and very little negative feedback. The counsellor was neutral which shown in Fig. 21 about specific features like password complexity and automatic logout, perhaps because these did not greatly impact their routine. However, the director was highly satisfied, strongly agreeing that all security and privacy mechanisms, including password rules, data unmasking, and session logout, were excellently implemented as proofing in Fig. 22.

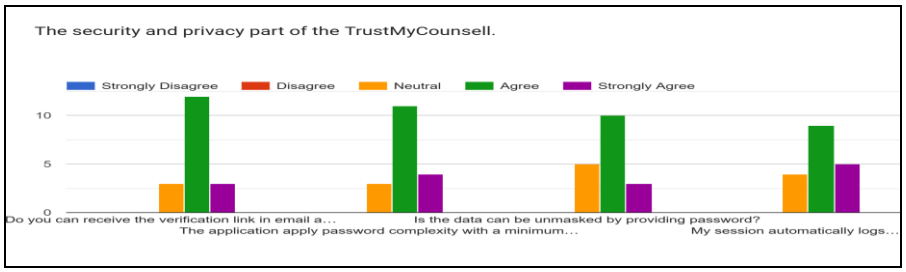


Fig.20 *Result User Acceptance Testing for Student and Staff in security features*

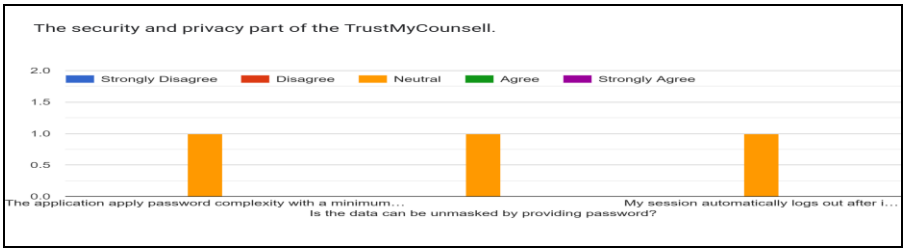


Fig.21 *Result User Acceptance Testing for Counsellor in in security features*

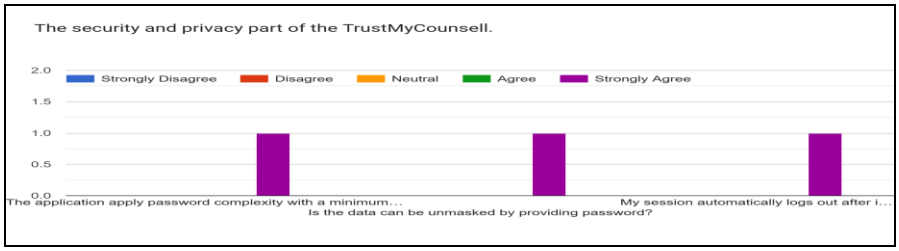


Fig.22 *Result User Acceptance Testing for Director in in security features*

7. Conclusion

TrustMyCounsell project successfully developed a functional mobile application for counselling management at KKTM Sri Gading, with a strong emphasis on security and user privacy. Its main achievement is providing a secure platform that uses End-to-End Encryption (E2EE) for sensitive communications, data anonymization for personal information, Multi-Factor Authentication (MFA), and streamlined counselling management tools designed for students, staff, counsellors, and the director. The project met all its objectives, from designing these privacy features to implementing them using Flutter and Firebase and validating them through user testing.

The key advantages of TrustMyCounsell include significantly enhanced data security compared to less secure systems, a user-friendly interface, and centralized management of counselling activities. This tailored solution aims to increase user trust and encourage more individuals at KKTM to use counselling services. However, the application currently has limitations, such as being mobile-only, requiring an internet connection, and its private key security relying on Firestore's integrity and application access controls.

Future improvements are planned to make TrustMyCounsell even better. These include adding real-time push notifications, critically enhancing security by encrypting private keys on the user's device before storing them, developing a web platform for broader access, and allowing some offline functionality like journal writing. In conclusion, TrustMyCounsell provides a robust and secure foundation for digital counselling at KKTM, with clear paths for future enhancements to further increase its value and security.

Acknowledgement

The authors would like to thank the Faculty of Computer Science and Information Technology, University Tun Hussein Onn Malaysia for its support.

Conflict of Interest

Authors declare that there is no conflict of interest regarding the publication of the paper.

Author Contribution

The authors confirm contribution to the paper as follows: **study conception and design**: *S. Y. Quek, N. H. Ab. Rahman*; **data collection**: *S. Y. Quek, N. H. Ab. Rahman*; **analysis and interpretation of results**: *S. Y. Quek, N. H. Ab. Rahman*; **draft manuscript preparation:** *S. Y. Quek, N. H. Ab. Rahman*. All authors reviewed the results and approved the final version of the manuscript.

References

[1] M. Kendra Cherry, "Online Therapy: Security, Ethics, and Legal Issues." Accessed: Oct. 15, 2024. [Online]. Available: https://www.verywellmind.com/online-therapy-ethics-2795227

[2] A. in Helsinki, "'Shocking' hack of psychotherapy records in Finland affects thousands." Accessed: Oct. 20, 2024. [Online]. Available: https://www.theguardian.com/world/2020/oct/26/tens-of-thousands-psychotherapy-records-hacked-in-finland

[3] Chris McDonald, "Privacy and Security Considerations in Online Counseling Platforms." [Online]. Available: https://pathtohopecounseling.com/privacy-and-security-considerations-in-online-counseling-platforms/

[4] "Online Counseling Data Security: Building Trust in Online Counseling: The Role of Data Security." Accessed: Oct. 15, 2024. [Online]. Available: https://fastercapital.com/content/Online-Counseling-Data-Security--Building-Trust-in-Online-Counseling--The-Role-of-Data-Security.html#Data-Breaches-and-Confidentiality-Concerns

[5] Oluwatoyin Ajoke Fayayola, Oluwabukunmi Latifat Olorunfemi, and Philip Olaseni Shoetan, "Data Privacy and Security in It: a Review of Techniques and Challenges," *Comput. Sci. IT Res. J.*, vol. 5, no. 3, pp. 606–615, 2024, doi: 10.51594/csitrj.v5i3.909.

[6] J. H. Hoepman, "Privacy design strategies," *IFIP Adv. Inf. Commun. Technol.*, vol. 428, pp. 446–459, 2014, doi: 10.1007/978-3-642-55415-5_38.

[7] J.-H. Hoepman, "Privacy Design Strategies (The Little Blue Book) minimise inform control enforce demonstrate Data subject," 2022.

[8] M. F. Adak, Z. N. Kose, and M. Akpinar, "Dynamic Data Masking by Two-Step Encryption," *2023 Innov. Intell. Syst. Appl. Conf. ASYU 2023*, pp. 1–5, 2023, doi: 10.1109/ASYU58738.2023.10296545.

[9] Z. Aslanyan and M. S. Boesgaard, "Privacy Analysis of Format-Preserving Data-Masking Techniques," *2019 12th C. Conf. Cybersecurity Privacy, C. 2019*, no. 4, pp. 1–6, 2019, doi: 10.1109/CMI48017.2019.8962143.

[10] S. Murthy, A. Abu Bakar, F. Abdul Rahim, and R. Ramli, "A Comparative Study of Data Anonymization Techniques," *Proc. - 5th IEEE Int. Conf. Big Data Secur. Cloud, BigDataSecurity 2019, 5th IEEE Int. Conf. High Perform. Smart Comput. HPSC 2019 4th IEEE Int. Conf. Intell. Data Secur.*, pp. 306–309, 2019, doi: 10.1109/BigDataSecurity-HPSC-IDS.2019.00063.

[11] W. Bai, M. Pearson, P. G. Kelley, and M. L. Mazurek, "Improving Non-Experts' Understanding of End-to-End Encryption: An Exploratory Study," *Proc. - 5th IEEE Eur. Symp. Secur. Priv. Work. Euro S PW 2020*, pp. 210–219, 2020, doi: 10.1109/EuroSPW51379.2020.00036.

[12] O. Onome Blaise, O. Awodele, and O. Yewande, "An Understanding and Perspectives of End-To-End Encryption," *Int. Res. J. Eng. Technol.*, no. April, pp. 1086–1094, 2021.

[13] A. Adithya, K. Kulkarni, and S. Saha, "Applications of RSA and AES256 in End-to-End encryption using Diffie-Hellman Key Exchange," *Int. Res. J. Eng. Technol.*, pp. 1217–1222, 2022, [Online]. Available: www.irjet.net

[14] Universiti Tun Hussein Onn Malaysia, "Counseling Management System." Accessed: Nov. 18, 2024. [Online]. Available: https://cms.uthm.edu.my/asas/index

[15] "PlusVibes." Accessed: Nov. 19, 2024. [Online]. Available: https://www.plusvibes.com/

[16] ThoughtFull World Pte. Ltd., "ThoughtFullChat." Accessed: Nov. 19, 2024. [Online]. Available: https://www.thoughtfull.world/

[17] Universiti Tun Hussein Onn Malaysia, "UTHM identity(UTHMid) SINGLE SIGN-ON & SECURE ACCESS." Accessed: Nov. 19, 2024. [Online]. Available: https://uthmid.uthm.edu.my/

[18] A. Sinha and P. Das, "Agile Methodology Vs. Traditional Waterfall SDLC: A case study on Quality Assurance process in Software Industry," *2021 5th Int. Conf. Electron. Mater. Eng. Nano-Technology, IEMENTech 2021*, pp. 1–4, 2021, doi: 10.1109/IEMENTech53263.2021.9614779.

[19] A. Mishra and Y. I. Alzoubi, "Structured software development versus agile software development: a comparative analysis," *Int. J. Syst. Assur. Eng. Manag.*, vol. 14, no. 4, pp. 1504–1522, 2023, doi:

10.1007/s13198-023-01958-5.
[20] C. Fagarasan, O. Popa, A. Pisla, and C. Cristea, "Agile, waterfall and iterative approach in information technology projects," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 1169, no. 1, p. 012025, 2021, doi: 10.1088/1757-899x/1169/1/012025.
[21] T. P. Diraja, "Undang-Undang Malaysia Akta 709 Akta Perlindungan Data Peribadi 2010 Bahagian I," 2010.
[22] OWASP Top 10 team, "A01:2021 – Broken Access Control," 2021, [Online]. Available: https://owasp.org/Top10/A01_2021-Broken_Access_Control/
[23] OWASP Top 10 team, "A02:2021 – Cryptographic Failures," 2021, [Online]. Available: https://owasp.org/Top10/A02_2021-Cryptographic_Failures/

Appendix A

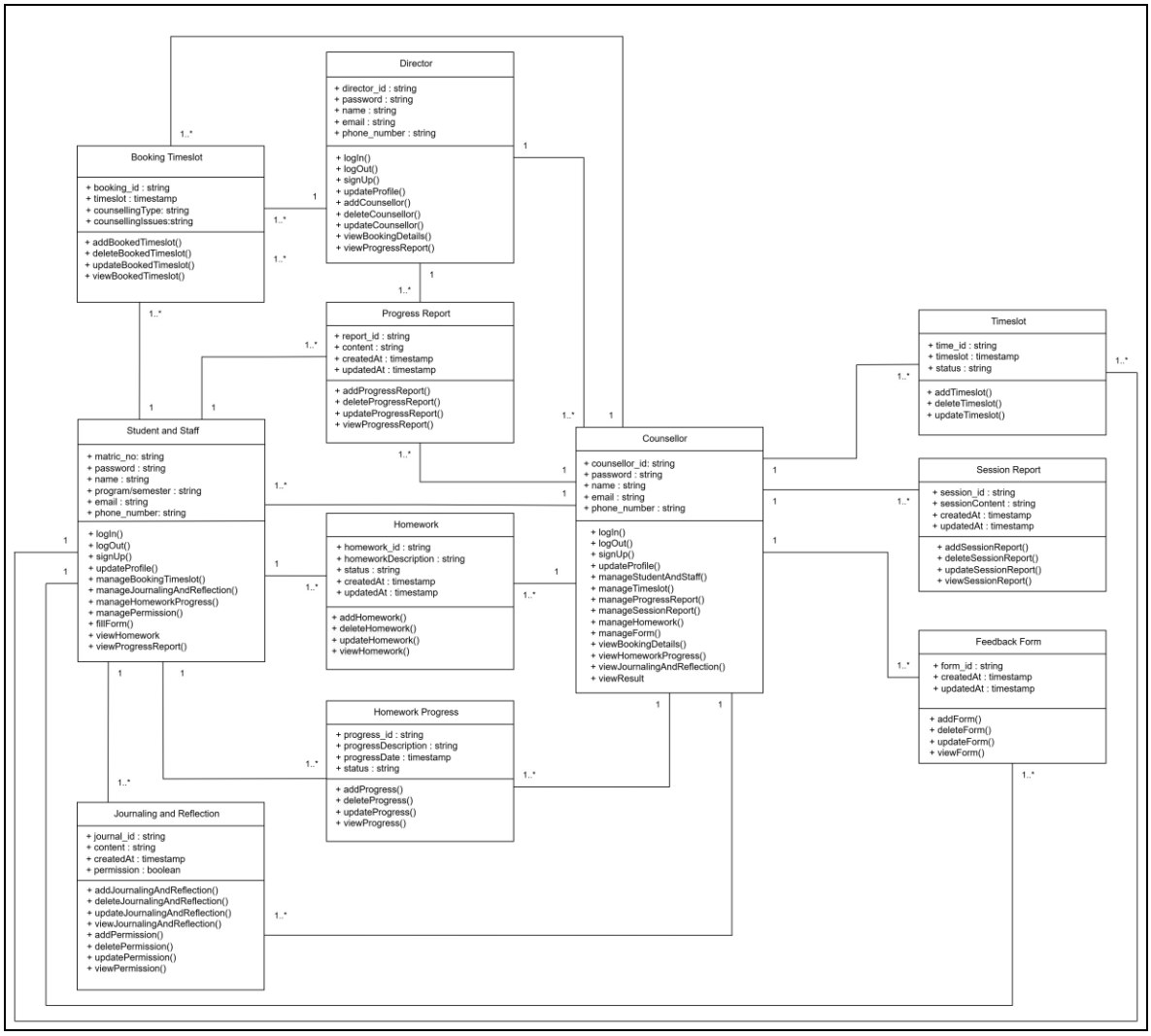
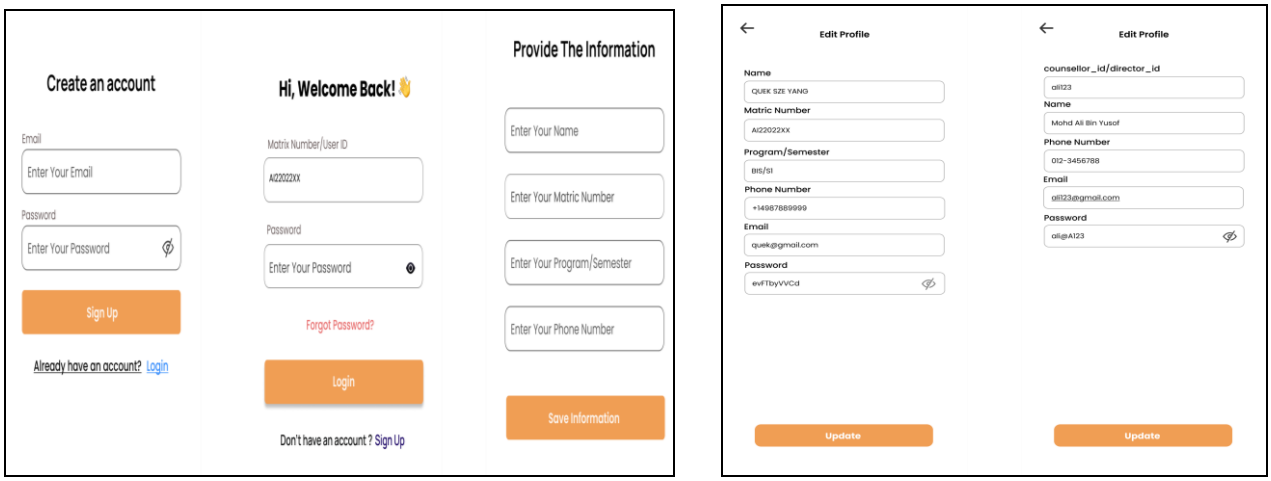


Fig.23 *Class Diagram for TrustMyCounsell*

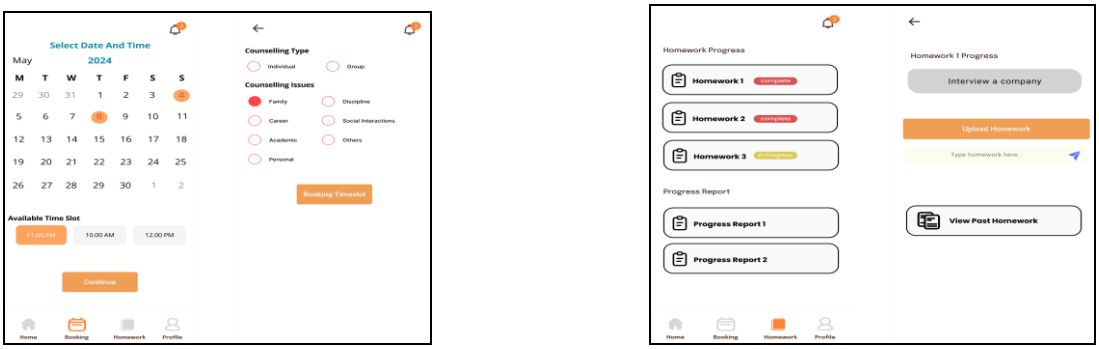
Appendix B



(a) **(b)**

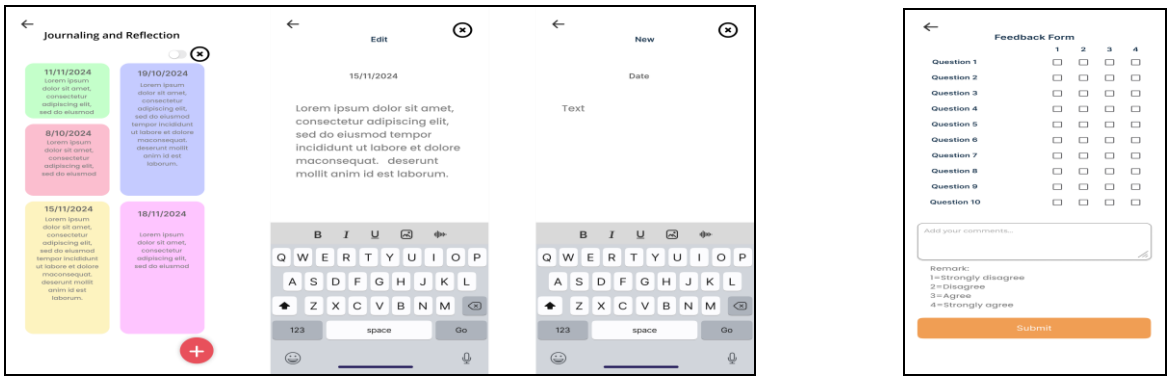
Fig.24 *(a)Login, Signup Page for Student, Staff, Director and Counsellor;(b) Update Page for Student, Staff, Director and Counsellor*

Applied Information Technology and Computer Science Vol. 6 No. 2 (2025) p. 473-493



(a) (b)

Fig.25 *Interface Design for Student and Staff (a)Booking; (b) Homework*

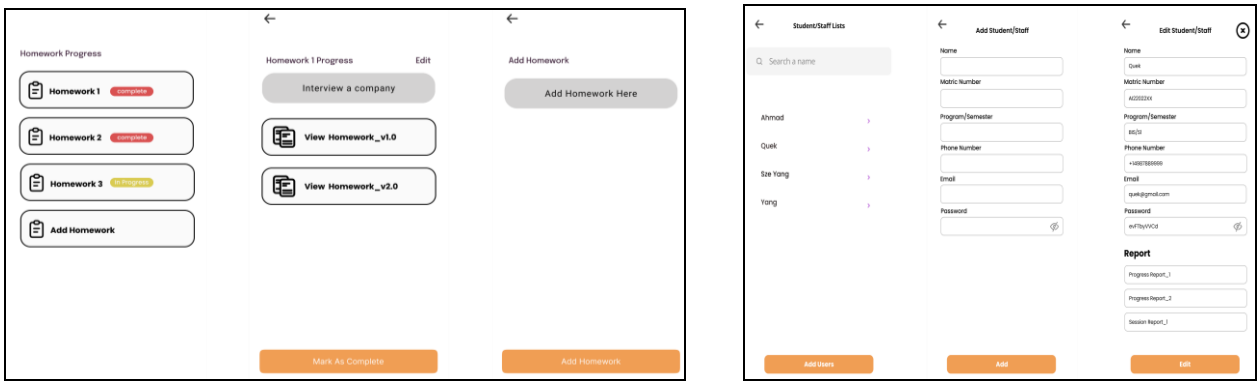


(a) (b)

Fig.26 *Interface Design for Student and Staff(a)Journaling and Reflection; (b) Feedback Form*

(a) (b)

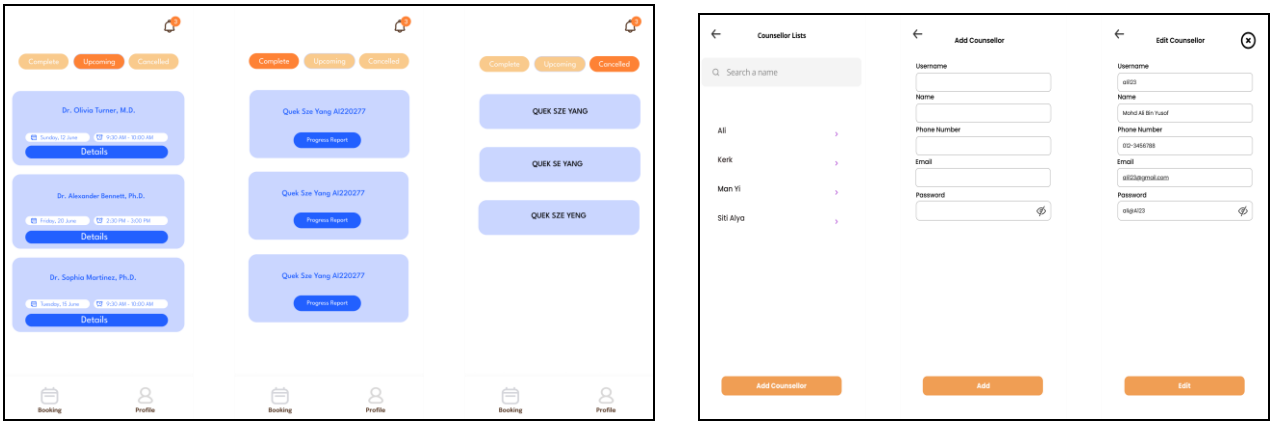
Fig.27 *Interface Design for Counsellor(a)Booking; (b) Upload Report*



(a) (b)

Fig.28 *Interface Design for Counsellor(a)Manage Homework; (b) Manage Student and Staff*

Fig.29 *Manage Feedback Form for Counsellor*



(a) **(b)**

Fig.30 *Interface Design for Director(a)View Booking; (b) Manage Counsellor*

Appendix C

Table 8 Google Form Questionnaire

Questionnaire for student, staff, counsellor and director
The effectiveness of TrustMyCounsell in term of its functionality while using TrustMyCounsell.
The application able to provide a login page and a register page for the students and staff.
The application able to allow student and staff to change their password.
Student, staff able to update their profile.
Student and staff can add, update or delete booking of the available timeslot.
Student and staff can add, update or delete their journaling and reflection.
Student and staff able to grant the counsellor the permission for view the journaling and reflection.
Student and staff able to view the homework progress.
Student and staff able to fill the feedback form of the counselling session.
The application able to provide a login page for counsellor.
The application able to allow counsellor to change their password.
Counsellor able to update their profile.
Counsellor able to add, update or delete student and staff.
Counsellor able to add, update or delete available timeslot.
Counsellor able to view booking details.
Counsellor can add, update or delete progress report and session report of the counselling.
Counsellor can add, update or delete homework for student and staff.
Counsellor able to view the homework progress.
Counsellor can add, update or delete the feedback form of the counselling session.
Counsellor can view the result of the feedback form.
The application able to provide a login page for director.
The application able to allow director to change their password.
Director able to update their profile.
Director able to add, update or delete the counsellor.

Table 8 *(cont).*

Questionnaire for student, staff, counsellor and director
Director able to view booking details.
Director can view the progress report.
The overall satisfaction on the user experience, the level of ease of use and overall usefulness for TrustMyCounsell.
The application able to respond promptly under normal operating conditions.
The application able to support the increasing user loads over time.
The application provide consistent performance with minimal downtime.
The application include the interfaces which easy to navigate for users.
The application is useful for my role.
The application is easy to learn and use.
The application enhances my workflow and efficiency.
The application provides a good user experience.
Does the email verification easy to understand and use?
Does the data masking easy to understand and use?
The security and privacy part of the TrustMyCounsell.
Do you can receive the verification link in email and function well?
The application apply password complexity with a minimum of 8 characters and a combination of alphanumeric and symbols.
Is the data can be unmasked by providing password?
My session automatically logs out after inactivity.