Applied Information Technology And Computer Science Vol. 4 No. 2 (2023) 283-301

AITCS

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

A Secure Dental Appointment System with One-Time Password Verification and Dual Authentication for Klinik Pergigian Sharifah

Shahirah Azhar[1], Nor Bakiah Abd Warif[1]*

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

DOI: https://doi.org/10.30880/aitcs.2023.04.02.017
Received 30 September 2023; Accepted 07 November 2023; Available online 30 November 2023

Abstract: A web-based dental appointment system is the new standard method and most significant way to handle appointment scheduling complexity. However, existing appointment booking at Klinik Pergigian Sharifah is done manually and is less organised, which may result in any missed scheduled appointment records. A Secure Dental Appointment System is proposed for the clinic in this study. This project aims to develop and test a secure dental appointment system for Klinik Pergigian Sharifah. Additionally, One-Time Password (OTP) verification using email for user registration and dual authentication. A "Completely Automated Public Turing test to tell Computers and Humans Apart" (CAPTCHA) for user login is applied in the system. Basic security approaches include Role-Based Access Control, strong password validation and salt-hashing passwords. This Project uses an iterative waterfall model and includes all necessary phases. The system was effectively established based on system testing and user feedback, and project requirements were met. This project system needs to continuously improve its usability and efficiency with more features and security to offer a sufficient appointment system in the future.

Keywords: Appointment Booking, Dental Clinic, Verification and Authentication

1. Introduction

A web-based dental appointment system is widely used these days [1] and is one of the most essential ways to manage workload. Most dental clinics and healthcare centers are aware of cutting-edge technologies. This helps in task management, particularly when arranging patient dentist appointments. This may have reduced the need for humans to perform necessary jobs [2]. Klinik Pergigian Sharifah was chosen for the project study. According to Klinik Pergigian Sharifah, the dental clinic was founded in 1993 and still conducts dental procedures manually, not entirely relying on online platforms. Dental appointment scheduling and patient registration will be managed by a clerk.

The clerk handles dental appointment booking by hand, including walk-ins, calls, and WhatsApp. The dental appointment method must be well-organised to avoid issues with any overlooked patients' dental appointments. It is challenging to schedule dental appointments [3] simultaneously.

*Corresponding author: norbakiah@uthm.edu.my

This project aims to alternate manual dental appointment booking. The objectives of this project are to design and develop a secure dental appointment system for Klinik Pergigian Sharifah and to test its functionality. The dental appointment system implements security elements including email One-Time Password (OTP) verification for user registration and dual authentication. "Completely Automated Public Turing test to tell Computers and Humans Apart" (CAPTCHA) for user login is applied to ensure only valid users have access. In addition, Role-Based Access Control (RBAC), strong password validation and password hashing with salting are implemented to promote risk reduction [3].

This web-based dental appointment system will provide well-organized dental appointment scheduling for the dental clinic. The patient may arrange their dental appointment via the system rather than sacrificing their time for a walk-in or on-call appointment. This might perhaps save some time.

2. Literature Review

This section will go over the literature review and the elements that will be implemented in this project. This section will also compare the existing systems to the proposed system.

2.1 Online Appointment Scheduling

The dental appointment system is one of the most important technological alternatives for organizing every dental procedure, including patient registration and appointment scheduling. Patients may schedule their appointment date at any time without having to visit the dental clinics and stand in queue. Thus, this could have reduced patient waiting time [4]. This also has implications for dental clinics since they can replace manual procedures with a computerized system in which all patient registration and dental appointment data are stored. All related data could have been more organized in that way.

2.2 Verification

Verification is a process of confirming or validating the accuracy or authenticity of something. This involves checking the information to meet specific requirements or standards. This usually involves sending a verification code via email or SMS. This is where the user must prove they are the legitimate account owner.

2.2.1 Email-OTP

Email OTP is where the OTP is sent to the user's email address. This technique is typically used for user verification and dual authentication. In this case, email-OTP is one of the ways to send a verification code to a legitimate user. This is in which to gain their truthfulness and authenticity.

2.2.2 CAPTCHA

CAPTCHA was designed to secure web information from unauthorized users who use text input to distinguish between authorized human users and illegal computer bot programs. Computers were unable to recognize CAPTCHA, but humans found it quite easy to read and input the text provided in the form. This is to verify between humans and bots to give accessibility to the system.

2.3 Authentication

Authentication is the process of verifying a user's identity. For example, a user who tries to access data, information, or systems [5] needs to be validated. This usually requires users to enter their login or other forms of identification to access. This is intended to ensure only authorised users have access. This is an essential security measure that protects against unauthorised access and security breaches.

2.3.1 Knowledge-Based

Knowledge-based authentication (KBA) involves verifying a user's identity [6] by testing their knowledge that only they should know. This will guarantee that only those with the proper knowledge

can access the system. KBA can be divided into static and dynamic [5], [7]. Static KBA refers to the fixed or inconstantly changing knowledge such as a password set by the user or a security question with a fixed answer known only to the user. Meanwhile, dynamic KBA describes continuously updated or changing knowledge such as a security question with variable answers generated by the system.

2.3.2 Dual Based

Dual-based authentication (DBA) requires users to provide two different types of evidence to verify their identity. By requiring two separate forms of evidence, DBA provides an additional layer of security to gain access. This involves something users know, in the form of their password and username, and something users have, in the form of Email with OTP. This means that user requires their password as one security layer and the OTP that will be sent via their registered email as another security layer.

2.4 Role-Based Access Control

Role-Based Access Control (RBAC) is a critical security feature in a system with multiple users. This type of access control is based on users' roles within an organisation, and it grants access to resources based on the user's role [8]. RBAC can be used to define a user's scope in a system or service [9]. This is where each user will be granted specific access [9] to the system.

2.5 Password Hashing and Salting

Any information transfer process that associates user accounts with access passwords should hash passwords rather than store them in plain text [10]. Hashing is irreversible, it is a very useful method for storing passwords [10]. Small random salt is generated and combined with the password in hashing.

2.6 Comparison with Existing Appointment System

This section will look at the existing appointment systems, such as Klinik Pergigian Sharifah's manual booking system, Setmore.com, and MySejahtera, which are both available online.

2.6.1 Setmore.com

Setmore is a third-party cloud-based system that can personalize online booking appointments, handle client data and appointments, and send reminders with notifications. There are three pricing tiers. The free version has minimal functions. However, the premium and pro plans have more advanced needs.

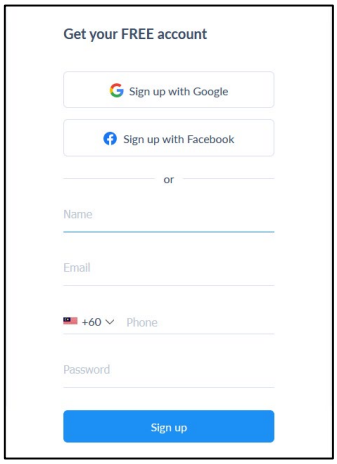


Figure 1(a): User System Sign up and Log in.

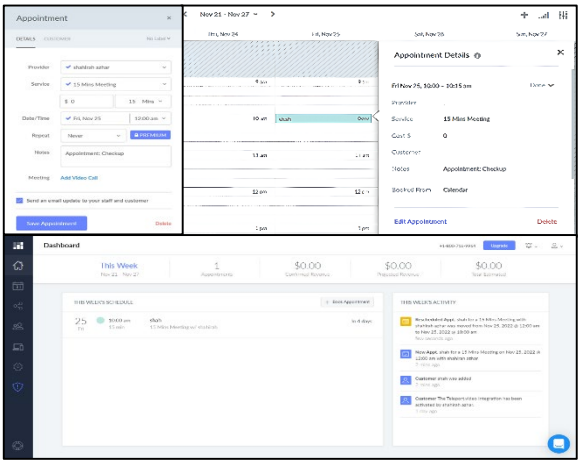


Figure 1(b): Appointment Scheduling and Reminder

Each user must first register and log in to use the Setmore system, as seen in Figure 1(a). A user's full name, email address, phone number, and password are required. The user may also sign up for an

account using a third-party account, such as Facebook or Google Email. Setmore system allows users to schedule appointments. Figure 1(b) shows that the appointment can be booked at any time.

2.6.2 Booking Appointments in MySejahtera App

Malaysian Ministry of Health (MoH) introduced MySejahtera Book Appointments system to enable appointment booking. MySejahtera app is a digital platform created as one measure to help manage the COVID-19 pandemic. MOH upgraded MySejahtera to allow patients to book appointments at KKM.

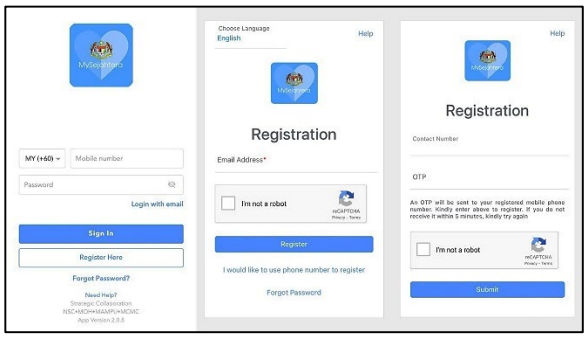


Figure 2(a): User System Registration and Log in.

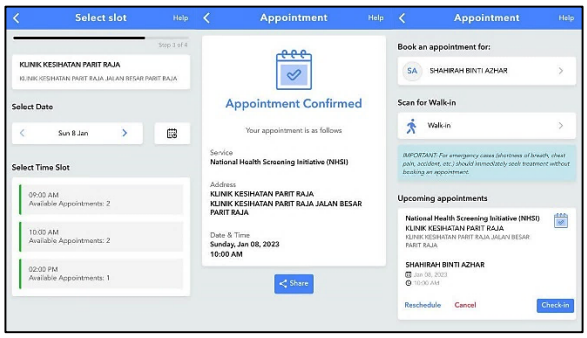


Figure 2(b): Appointment Scheduling and Reminder

Each user must register using an email address or phone number. The user will then receive the OTP. To complete the registration, the user must click on Google reCAPTCHA first. The user must provide their registered contact number or email address, as well as their password to login, as illustrated in Figure 2(a). Users may also make appointments on the slot selection within the available time slots list. Once the appointment slot is set, the user must confirm the appointment as in Figure 2(b).

Table 1: Comparison between The Existing Systems with The Proposed System.

	Klinik Pergigian Sharifah	Setmore.com	MySejahtera	Proposed System
System Type	Manual Booking Appointment	Online Cloud-Based	Digital Platform	Online Web-Based
Registration	Yes, manually	Yes	Yes	Yes
Verification	-	No	- Google reCAPTCHA - Email or SMS OTP upon registration	- Email-OTP upon User Registration - Anti-CopyPaste CAPTCHA
Authentication	-	KBA using Password	KBA using Password	Dual Authentication with password and Email OTP
Access Control	-	Information not available	Information not available	Using RBAC
Password Management	-	Information not available	Information not available	Password Hash with Salt
Strong Password Validation	-	No	Apply for 6 to 25-length characters	Apply for 8-length characters with 1 upper and lowercase letter, 1 number and 1 special character
Appointment Schedule	Yes, manually	Yes	Yes	Yes

Table 1 shows the similarities and differences between the present systems and the proposed appointment system. Setmore.com is an online cloud-based platform and MySejahtera is a digital

platform, Booking Appointments is manually operated. Unlike the existing systems, the proposed system is web-based. The manual booking system only has manual registration and no login interface, whereas the proposed system, setmore.com, and MySejahtera require registration and user login.

The proposed system implements Email OTP for user verification after user registration. Unfortunately, the current manual system lacks one. In contrast to MySejahtera, the Setmore system does not use a Google reCAPTCHA during user registration. Furthermore, the proposed system would apply dual authentication, which includes KBA using password and Email OTP for user login as well as CAPTCHA with anti-CopyPaste feature for human-bot verification. In comparison to the proposed system, the Setmore system used just KBA, which is password and user email, whereas MySejahtera uses password and user phone number or email for login.

The proposed system uses RBAC for access control, providing each user access to their authentication pages. But in contrast to the Setmore system and MySejahtera, access controls and authentication are still used to enhance its security. In comparison to the setmore system, MySejahtera, and the proposed system, the existing system of Klinik Pergigian Sharifah managed appointments manually. To protect the system's credential data, the proposed system will also feature robust password validation with a minimum of 8-length characters that must include upper- and lowercase letters, digits, and special characters, as well as password hashing with salt. In contrast, the MySejahtera system utilises password lengths ranging from 6 to 25 characters, while the Setmore system does not apply strong password validation.

3. Methodology

An iterative waterfall model, which combines elements of the traditional waterfall model with iterative development and focuses on continual improvement in project development, will be employed in this project management system. Each phase of development in the iterative waterfall model is followed by a review and evaluation process, which analyses the progress made and determines whether any changes or adjustments are required.

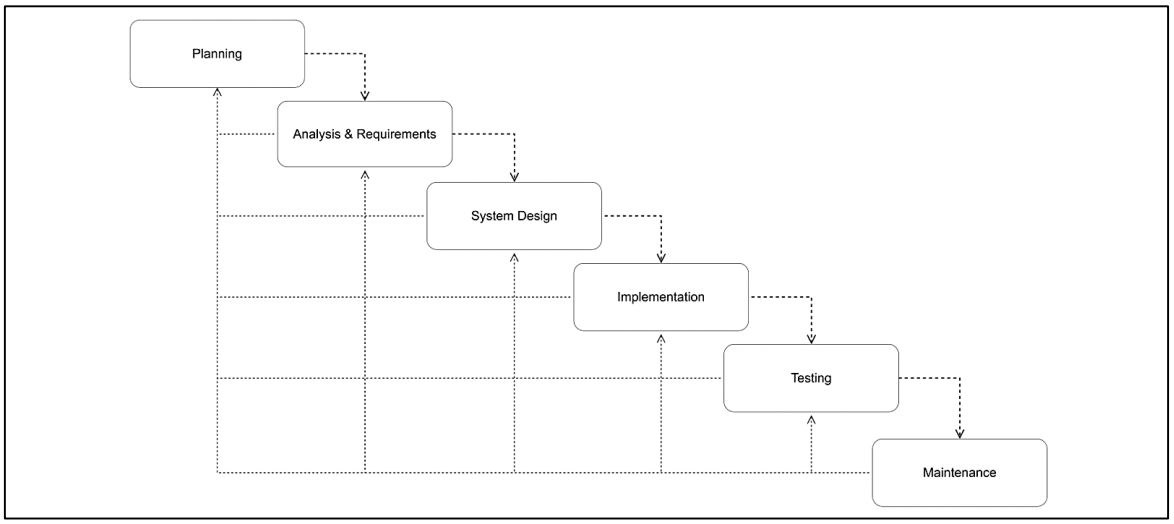


Figure 3: Iterative Waterfall Model

Based on Figure 3, there are phases of the iterative waterfall model in this project management system including planning, analysis and requirements, system design, implementation, testing, and maintenance. Thus, this project development system could be conducted back forward for any continuous improvement and alteration [11] in more adaptable and responsive ways. The phase and task of project system development based on the iterative waterfall model are shown in Table 2. It is significant in standardizing and organizing all the tasks in each project development phase.

3.1 Planning

The planning phase is vital as it will be a guide to managing the project development. This includes determining the scope of the project, project goals, and objectives to achieve the project's goals. The project will collect all information, including the problem statement regarding the appointment booking issue from Klinik Pergigian Sharifah. This is to ensure that the system can resolve the issue for Klinik Pergigian Sharifah. This phase also includes the project plan, which outlines the tasks that must be done to meet the project's objectives.

3.2 Analysis and Requirements

The analysis phase is important in identifying and analyzing every related requirement of the project system. It is compulsory to understand the needs and requirements of the project developments throughout this phase. This phase usually involves gathering and analyzing information from interviews as well as some research from the existing systems to imply in the proposed project system All related information will be used to guide the project's development in subsequent phases.

3.3 System Design

This project system's system design phase provides a pre-development of the project system in a visual form of context. All defining requirements and specifications from the analysis and requirements phase will be transformed into a detailed design context for the project implementation phase later. The requirement analysis phase will entail identifying functional and non-functional requirements. The system flow diagram will provide a clearer picture of system development.

3.4 Implementation

Major project development software, hardware, and programming language requirements apply during the implementation phase. A laptop with an 11th Gen Intel(R) Core i5-1135G7, 2.40 GHz processor and 12 GB RAM will be used. After that, the Klinik Pergigian Sharifah dental appointment system will be created using VScode Studio, MySQL XAMPP Control Panel, PHP, HTML, CSS, and JavaScript.

3.5 Testing

System testing for Klinik Pergigian Sharifah's safe dental appointment system will be conducted including functionality testing, user testing, and user acceptance testing. To make sure the built system works properly, functional testing will be done. The system's ability to be used by the target user, who mainly includes admin, clerk, doctor, and patient, will then be tested by users.

3.6 Maintenance

The maintenance phase is critical since it needs to sustain and maintain the secure dental appointment system once it has been implemented. In this phase, users of the project system typically receive continuing support and help, as well as any necessary updates or system modifications.

4. System Analysis and Design

System analysis and design will cover all the system requirements and design including functional and non-functional requirements as well as illustrate an outline or strategy for a system that needs to fulfil the specific requirements and objectives.

Functional requirements for Dental Appointment System are based on a few aspects of use for the patient, clerk, dentist, and admin. This requires the system to be functioning and easy to use for the users. The functional requirements for a Secure Dental Appointment System for Klinik Pergigian Sharifah are listed as shown in Table 3.

Table 3: Functional Requirement of a Secure Dental Appointment System for Klinik Pergigian Sharifah

Item	Functional Requirement
1	All users should be able to login into the system username, and password with security validation.
2	The system should be able to send OTP by email for user verification.
3	Users, mainly patients should be able to verify their registered email with email OTP before proceed the registration process.
4	Admin should be able to register the clerk, dentist, and patient. The admin should also allow viewing, creating, updating, and deleting all registered lists.
5	Patients and clerks should be able to make a registration for patients and store patients' information in the system.
6	Patients and clerks should be able to book and schedule the available appointment at a time.
7	The clerk should be able to verify the scheduled appointment that has been made by the patient.
8	The dentist should be able to view the list of upcoming scheduled appointments.
9	The system must be able to get from the database and show the registered user list and appointment list.
10	All users should be able to log out of the system.

Non-functional requirements are a crucial factor to be considered when developing any system. This is because it may significantly affect both the success of the system and the overall user experience. The non-functional requirement for a Secure Dental Appointment System for Klinik Pergigian Sharifah is explained in Table 4.

Table 4: Non-functional Requirement of a Secure Dental Appointment System for Klinik Pergigian Sharifah

Non-Functional Requirement	Description
Usability	The system can access when there is an internet connection.
Performance	All users should be able to access the correct assigned pages. The system can allocate the user to the correct session.
Security	- Users can access the system when entering the correct user email and password with security validation and provide OTP sent via email. - Users, mainly patients, should verify their registered email with Email OTP upon the registration process. - All the passwords will be hashed and salt to be stored in the database. - The user needs to clarify the user's human-bot verification through CAPTCHA.

The system flow diagram represents the graphical overview that shows information flow throughout the system and how the system is functioning. It is for understanding a complex system. Figure 4 shows the illustration of the system flow diagram of the proposed system, the secure dental appointment system for Klinik Pergigian Sharifah. There are four types of users in this proposed system which are admin, patient, clerk, and dentist. Each user may view the main page of the dental appointment system, which they need to login into the system first. Meanwhile, the system will validate the correct user email and password before granting access to the system only to the valid user.

Based on Figure 4, this proposed system will implement dual authentication with Email OTP upon user login and RBAC where each user system has their own authority to access data and information. For registration, the patient could have registered themselves through the system. Upon registration, the patient will need to verify their registered email using OTP that will be sent via email. Meanwhile, the clerk may assist in creating and modifying patient registration and appointment scheduling for first-timer or walk-in patients through the system. The admin can register the clerk and dentist. The patient may book or cancel their dental appointment at any available date and time slot through the system for appointment scheduling. For walk-in patients, the clerk can help book appointments through the system. At the same time, the clerk can view and verify patient registration and dental appointments made through the system. Salting and hashing will be used to protect the data credentials and data integrity for all user passwords that are stored in the system.

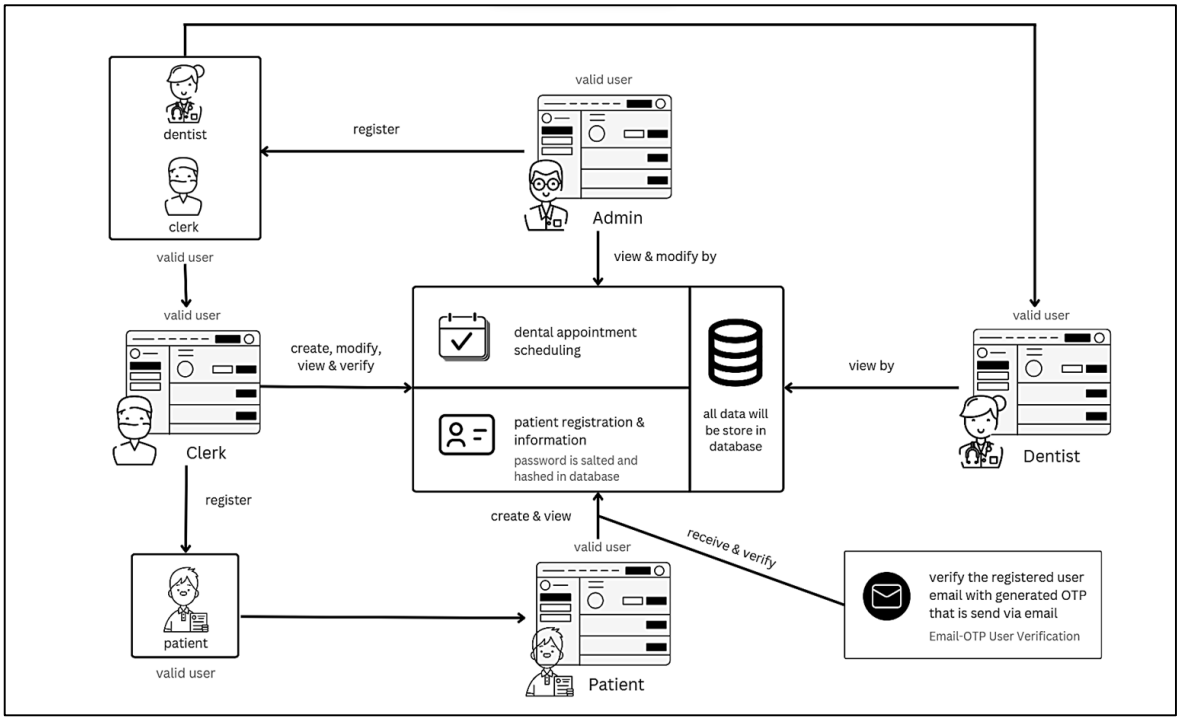


Figure 4: System Flow Diagram of Secure Dental Appointment System for Klinik Pergigian Sharifah

A context diagram is a high-level illustration of the connections between a system and external entities. Figure 5 shows the context diagram of a Secure Dental Appointment System for Klinik Pergigian Sharifah to provide a broad overview of the system flow. It includes admin, patient, clerk, and dentist as the target users of a Secure Dental Appointment System for Klinik Pergigian Sharifah that will utilize the system.

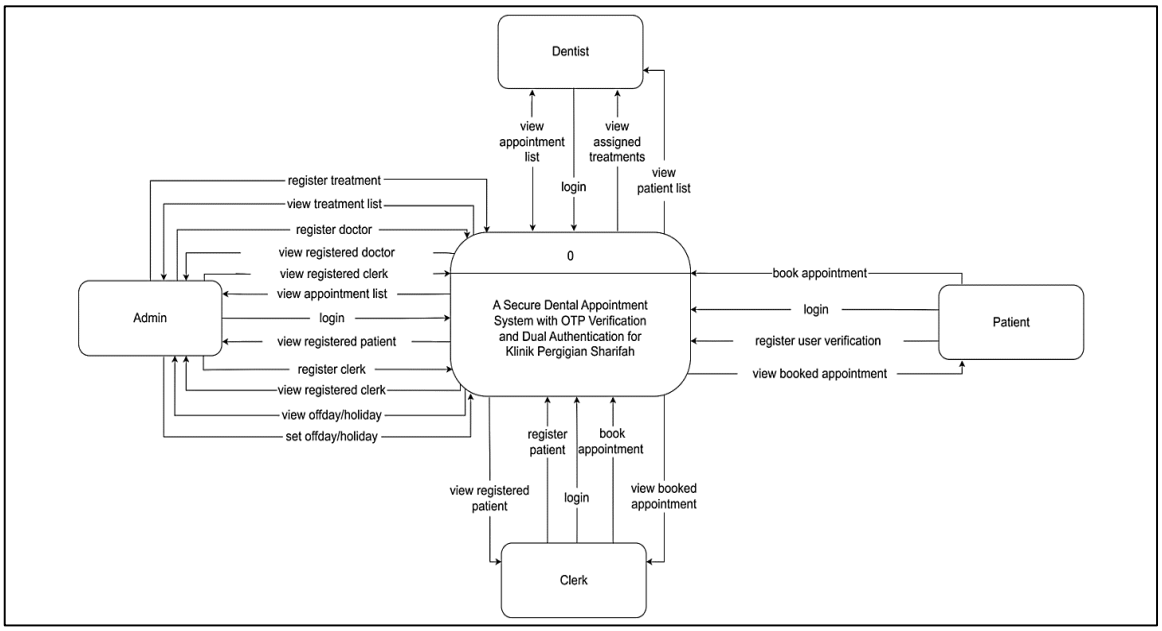


Figure 5: Context Diagram of a Secure Dental Appointment System for Klinik Pergigian Sharifah

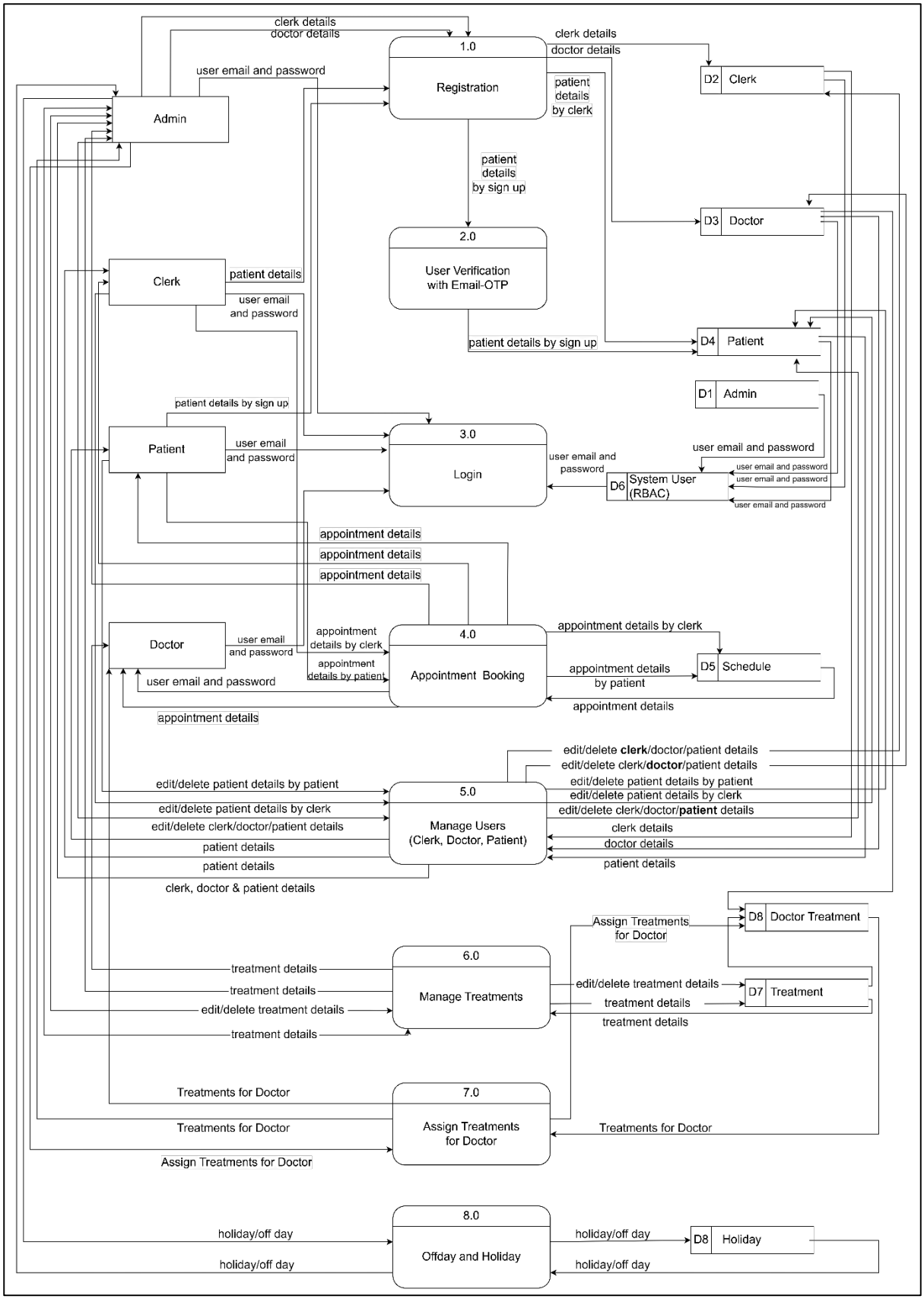


Figure 6: DFD Level 0 of a Secure Dental Appointment System for Klinik Pergigian Sharifah.

Data flow diagram (DFD) is a graphical representation of the flow of data through a system. Figure 6 shows the data flow diagram in level 0 of a Secure Dental Appointment System for Klinik Pergigian

Sharifah with four main entities which are admin, patient, clerk, and dentist. This shows the process of data being stored. Each entity will have varying access data to the page they are authenticated.

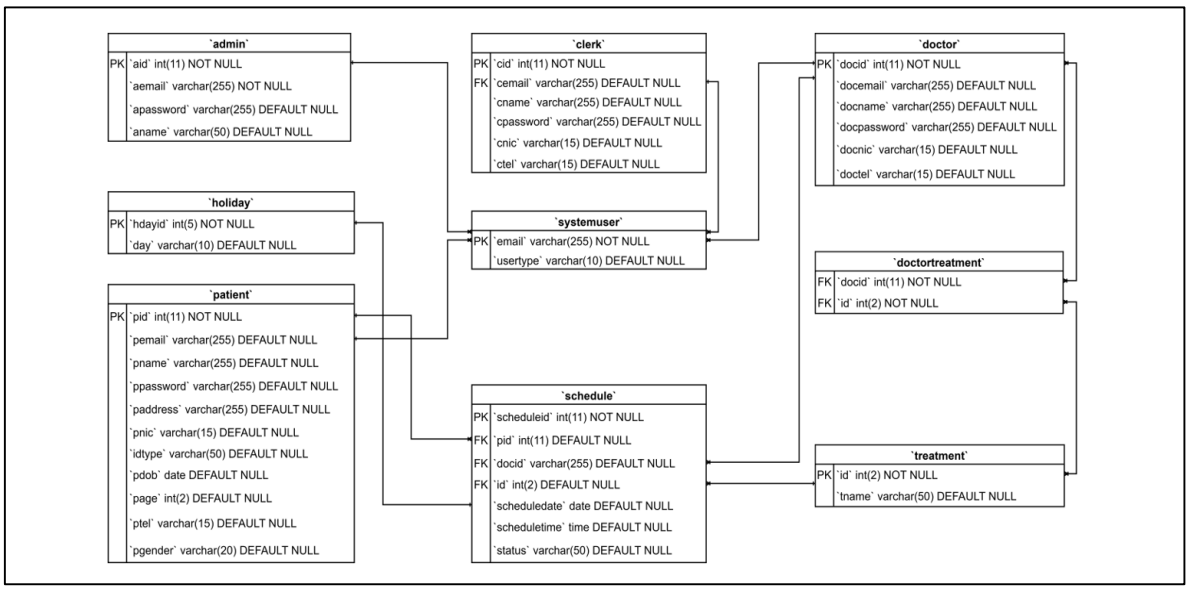


Figure 7: ERD of a Secure Dental Appointment System for Klinik Pergigian Sharifah

The entity relationship diagram (ERD) is used to visibly represent the relationship between entities. Figure 7 illustrates the relationship between entities in a Secure Dental Appointment System for the Klinik Pergigian Sharifah system using an ERD.

5. Implementation and Testing

Implementation entails constructing the system according to the design plans. The process of testing, on the other hand, involves determining whether the software is reliable and produces accurate results. This phase helps in making sure that the system is dependable and performs as intended.

5.1 Implementation

This section will cover the system module that is implemented in the system. This includes the security module, booking module and reporting module. The following sections will describe each module.

5.1.1 Security Module

The security module includes a sign-up and a login module. Both implement different security measures to ensure the system is secure to use and protect user data.

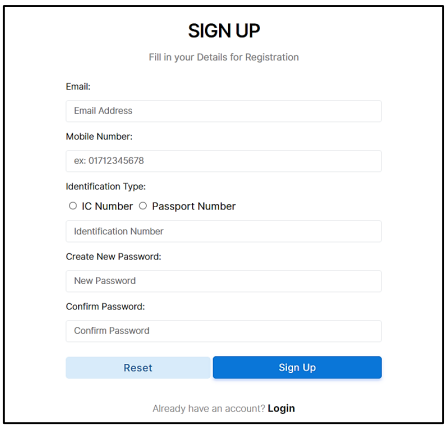


Figure 8(a): Sign-Up Module for User Registration

Figure 8(a) shows that the sign-up page for user registration is mainly for patients. This page indicates security elements including strong password validation, user verification using Email-OTP, and storing hashed passwords with salt in the database after successful user registration.

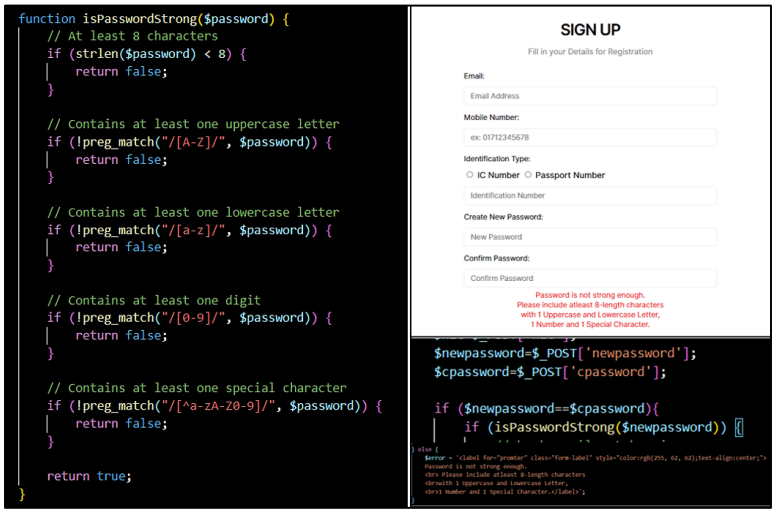


Figure 8(b): Strong Password Validation Upon User Registration

Figure 8(b) shows that strong password validation is implemented during the user registration process. This is where the user needs to follow the valid strong password which is the password should be 8-length or more, contain 1 uppercase and 1 lowercase letter, 1 digit and 1 special character. Otherwise, an error message will be displayed and require the user to input the password by following the strong password validation.

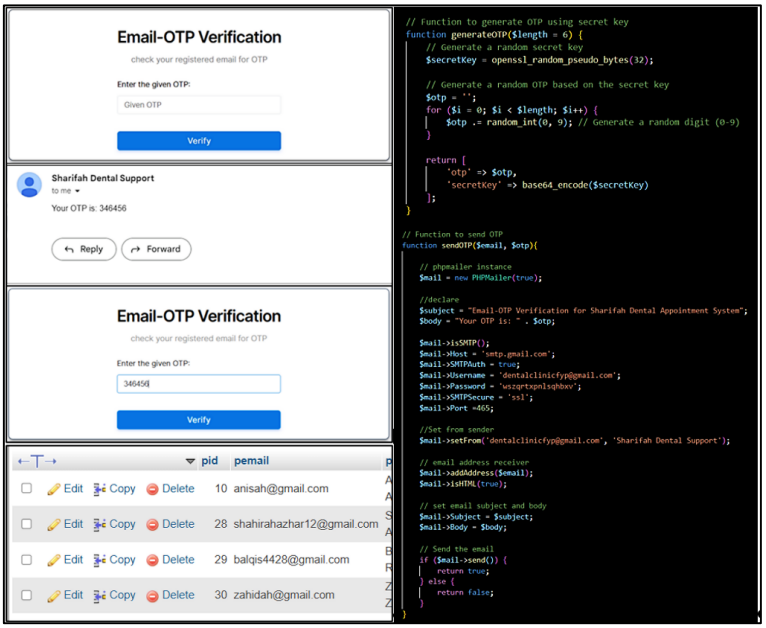


Figure 8(c): Email-OTP Sent via User Registered Email for User Verification

Figure 8(c) shows the Email-OTP verification form right after the user submits the registration form. Then, the verification form requires the generated OTP that has been sent through the user's registered email. It is for verifying the user's valid email before registration is successful. Moreover, the data is not stored in the database system yet as the email has not been verified yet. This is to avoid multiple idle or unused accounts from the registration form. Thus, the user needs to verify their registered email with OTP that has been sent, to proceed with successful registration and the data will be stored in the database.

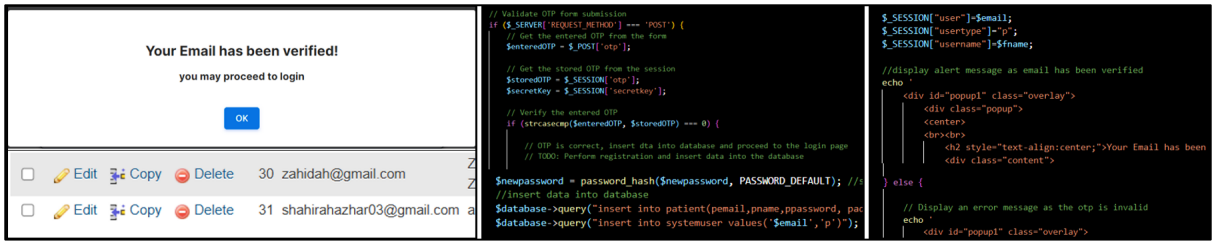


Figure 8(d): Registered Email is Verified

Figure 8(d) shows after the Email-OTP Verification is verified the alert message will appear and redirect the user to the login form as the registration has been successfully made. Also, the data will be successfully stored in the database system as the email has been verified.

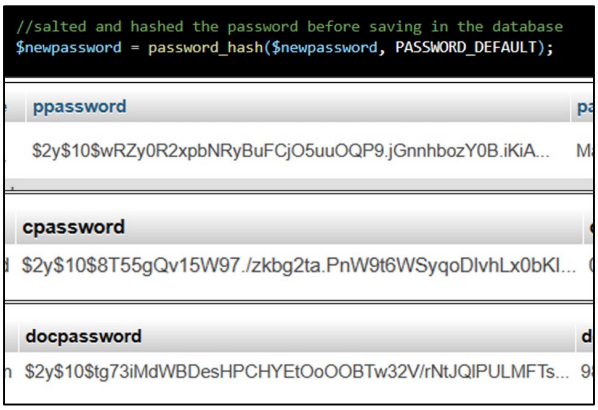


Figure 8(e): Password Hashing with Salt

Password Salting and Hashing are also implemented in this system. It is vital to secure the confidentiality of user data, mainly their password. This is to protect the password from being used by unauthorized people or for unauthorized access. Thus, Figure 8(e) shows that storing passwords with hashing will be able to prevent unauthorized uses, however applying salting and then hashing the password would enhance the security level of storing the password in the database.

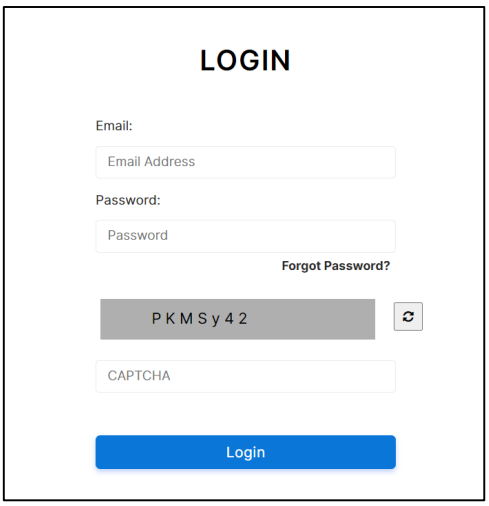


Figure 9(a): Login Module for User Login

Figure 9(a) shows the login page for user login which requires users to input their registered email, password, and CAPTCHA with the anti-CopyPaste feature. This login module has implemented RBAC as well.

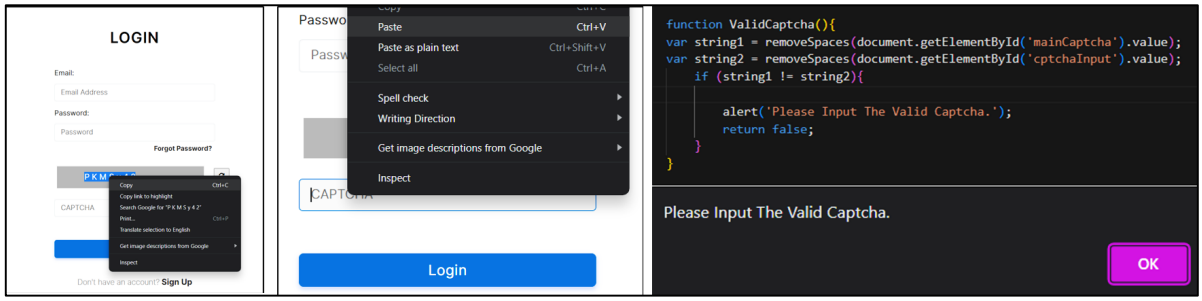


Figure 9(b): Login Page with Anti-CopyPaste CAPTCHA

CAPTCHA which is applied with anti-copy&paste is implemented to protect the availability of the system before the user can login to the system as in Figure 9(b). This shows that the user should not be able to copy the text-CAPTCHA and paste it for input. Despite this, the user needs to input them one by one same as the text-CAPTCHA shown and appear to be a valid CAPTCHA. Otherwise, the alert message will appear as if the input CAPTCHA is invalid.

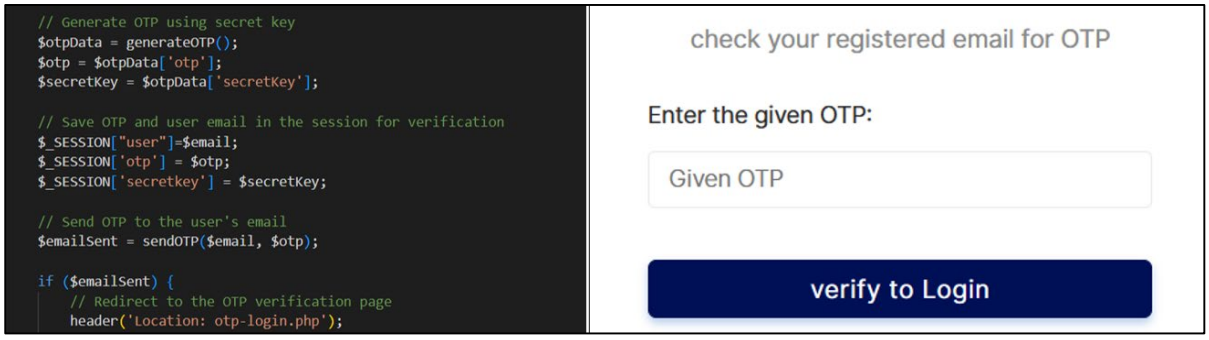
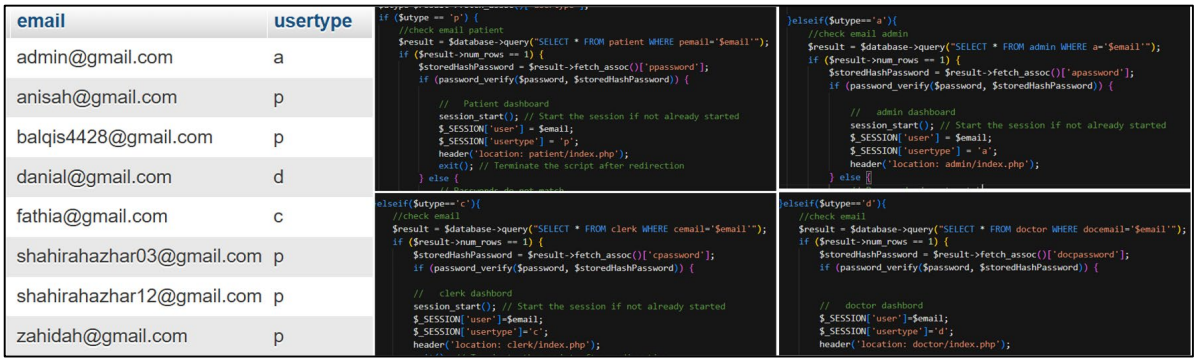


Figure 10: Email OTP upon User Login

Figure 10 shows the code that verifies the type of users of the system and identifies the user's valid registered email before the user will then receive OTP via their email. This is required after the user inputs their email, password, and CAPTCHA. Including OTP that is received via user email acts as another security layer. This means that dual authentication is implemented.



email	usertype
admin@gmail.com	a
anisah@gmail.com	p
balqis4428@gmail.com	p
danial@gmail.com	d
fathia@gmail.com	c
shahirahazhar03@gmail.com	p
shahirahazhar12@gmail.com	p
zahidah@gmail.com	p

Figure 11(a): Authorized Each User to Login with RBAC

Figure 11(a) shows the implemented RBAC for each user where they will be recognized based on their user type which is patient, admin, clerk, and doctor. This in which also indicates a user role for RBAC as well as assigned the user email to indicate the user role for their login phase. Thus, if it shows the condition where the user type is patient it will redirect to the patient dashboard page, otherwise, it will recognize if the user type is admin or clerk or doctor, then it will redirect to their dashboard page as shown in Figure 11(b).

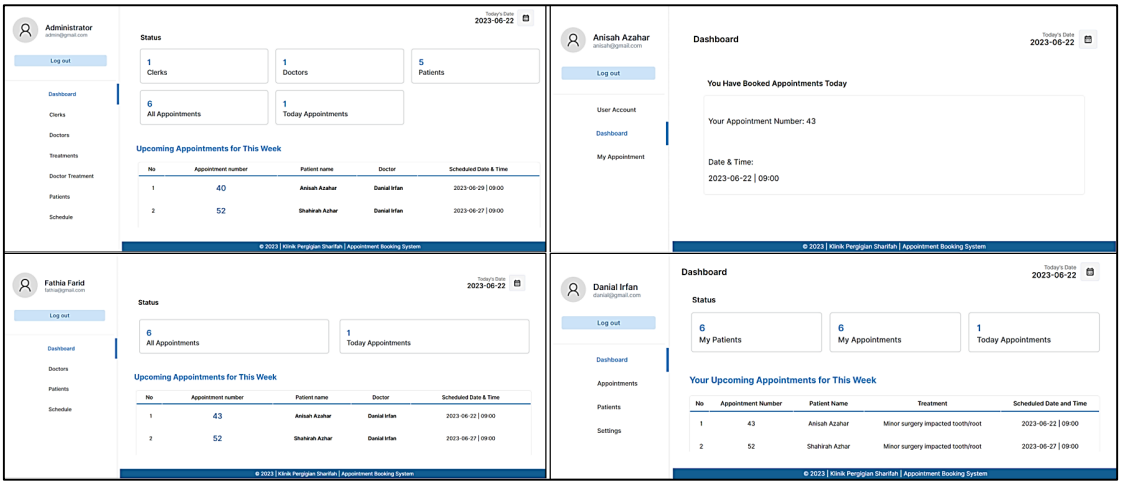


Figure 11(b): Authorized Page for Each User

5.1.2 Booking Module

The booking module involves dental appointment booking and scheduling for patients. The booking appointment can be made by the patient and the clerk.

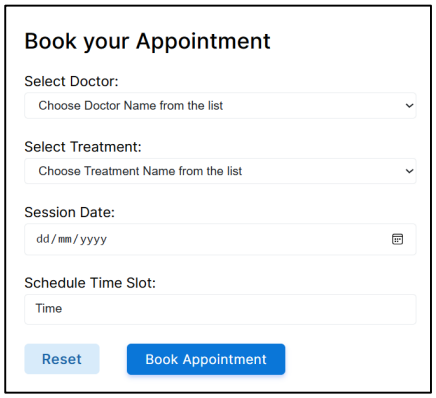


Figure 12(a): Appointments Booking by Patient

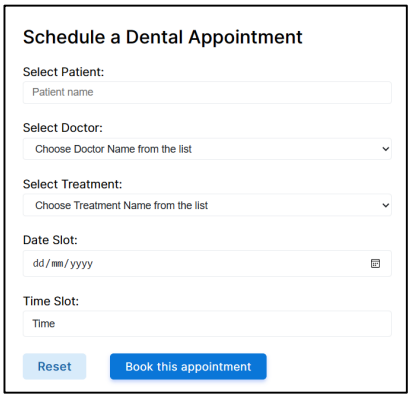


Figure 12(b): Appointments Booking by Clerk

Figure 12(a) and Figure 12(b) show the appointment booking form for the patient that is scheduled by the patient and by the clerk, respectively. The clerk should be able to schedule the appointment for the patient by choosing the available doctor, treatment, date, and time slot. The same goes for this appointment scheduling, if the chosen doctor, treatment, date, and time slot are all available, then the appointment will be successfully booked.

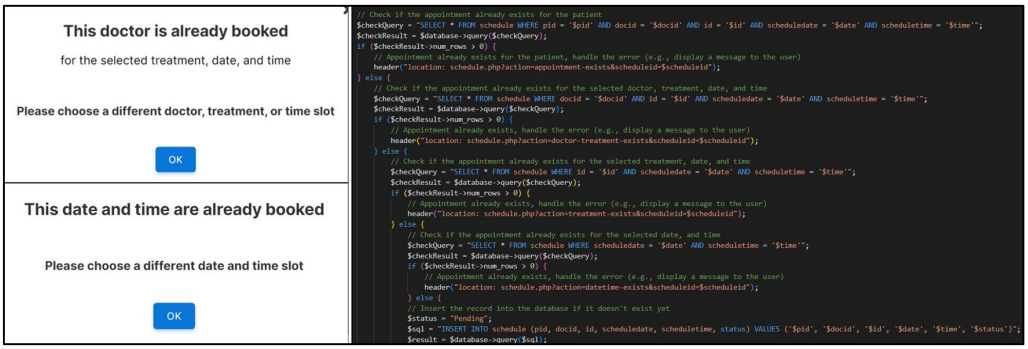


Figure 12(c): Checking for Availability before The Appointment is Successfully Booked

Figure 12(c) shows the implementation of the if-else condition to check the availability of the doctor, treatment, date, and time slot before the appointment if successfully booked by the user, particularly to the patient and clerk. If the doctor, treatment, date, and time slot are all available, then the appointment will be successfully booked. Otherwise, the alert message will be displayed to acknowledge the user.

5.1.3 Reporting Module

Reporting Module will cover the lists of users; clerks, doctors, and patients as well as the list of treatments and assigned treatments for a doctor and booked appointments. However, the reporting module involves different users with different access to the data list.

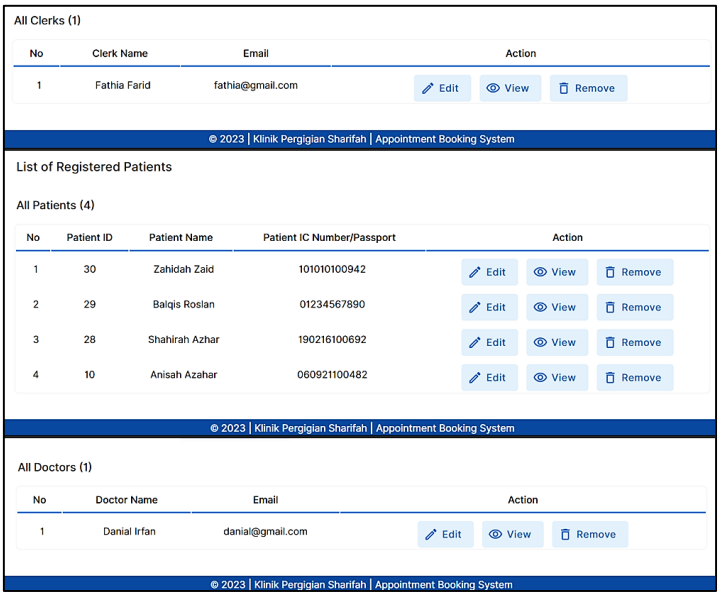


Figure 13(a): List of Registered Users of Clerk, Patient and Doctors

Figure 13(a) shows the list of users that have been registered in the system which are Clerks, Patients, and Doctors. Patient lists can be viewed by the admin, clerk, and doctor for dental appointment purposes. However, the clerk list and doctor list can only be viewed by the admin.

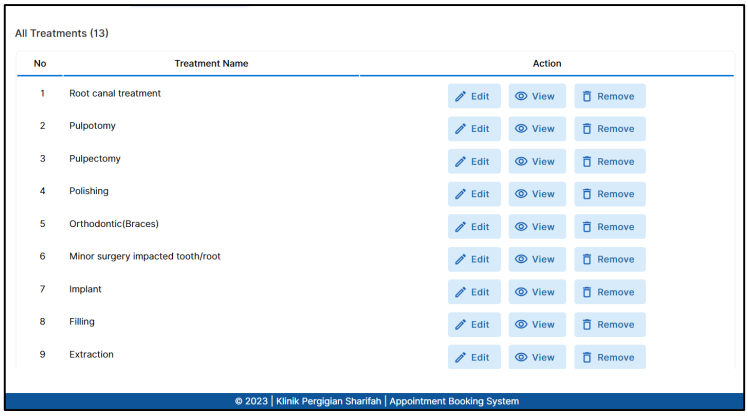


Figure 13(b): List of Treatment

Based on Figure 13(b), the treatment list can only be viewed by the admin. This is because only the admin can register or add the treatments to the data list.

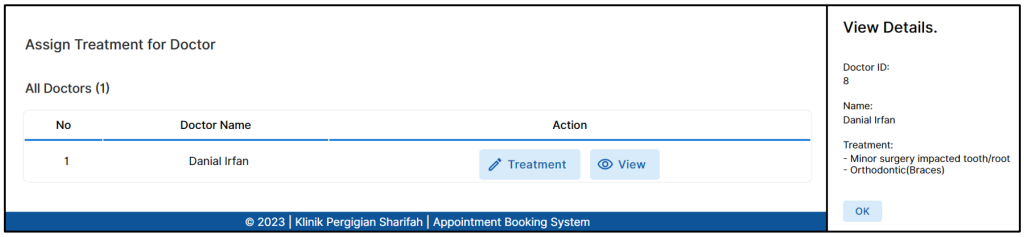


Figure 13(c): List of Assigned Treatment for Doctors

Figure 13(c) shows the list of assigned treatments for doctors. This uses many-to-many relationships as many doctors can be assigned many treatments at a time. Thus, this data list can only be viewed by the admin.

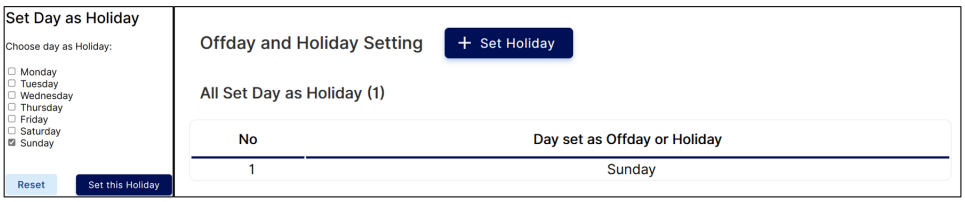


Figure 13(d): List of Off Days and Holidays

Figure 13(d) shows the list of days that are set for off days and holidays. Only the admin could do this setting of off days and holidays. The off day and holiday are set by day from Monday to Sunday. In this case, the dental clinic is closed on Sunday, thus the booking appointment will not be available on the off day and holiday.

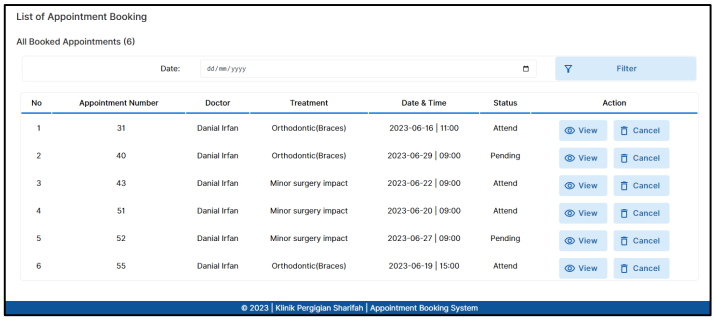


Figure 13(e): List of Booked Appointments

Figure 13(e) shows the list of booked appointments where this can be viewed by the admin and the clerk as they have the authority to view and cancel the appointments. However, doctors and patients also can view the appointments list, but the list will contain only their booked appointments.

5.2 Testing

System testing is essential because it ensures the quality, dependability, and functionality of a system. Thus, this section will include functional testing and user testing of the system.

5.2.1 Functional Testing

Functional testing is conducted by the developer to assess the system's functionality. Each function is carefully created and tested until the desired goals are met. Throughout this phase, the system is tested for overall functionality and security elements. The results of the functional testing are shown in Table 5 and Table 6.

Table 5: Test Case for Functionality

Test Case	Expected Result	Actual Result
Connect database with system	No error message while connecting the database and system.	Pass
Login and Logout can function properly	A system is able to access the login page by entering the user ID and password.	Pass
Email OTP send to user registered email for user verification	Every user is able to be received OTP from their email and use the OTP to be verified.	Pass
Email OTP can send to user registered email for user login	Every user able to be received OTP from their email and use the OTP to be verified.	Pass
SESSION variable can functionally be used	The SESSION variable can be used after the correct user ID and password are inserted.	Pass
Admin able to register clerk and doctor	The registered clerk and doctor are able to insert into the database.	Pass
Admin able to view, update and delete clerk, doctor, and patient.	The registered clerk, doctor, and patient are able to update and delete in the database.	Pass
Clerk able to register patient	The registered patients are able to insert into the database.	Pass
Clerk, doctor, and patient can update their details.	The system successfully updates user details.	Pass
Clerk and patient able to schedule a dental appointment	The system successfully inserts the scheduled appointment into the database.	Pass

Table 6: Test Case for Security

Test Case	Actual Result
Password must be 8-length characters containing at least 1 upper and lowercase letter, 1 number, and 1 special character.	Pass
The system will show error and alert messages.	Pass
Password must not be shown in the text box on the login page.	Pass

5.2.2 User Testing

User testing is carried out and collected using Google Forms, which are distributed to users, primarily the client and other related users including admin, clerk, doctor, and patient as shown in Appendix A. The form is divided into two sections which are user interface testing on a Likert scale of 1 (Strongly Dissatisfied) to 5 (Strongly Satisfied) and user module testing on a multiple-choice scale of Pass or Fail. This aims for user feedback to identify any issues and evaluate the system's functionality and usability.

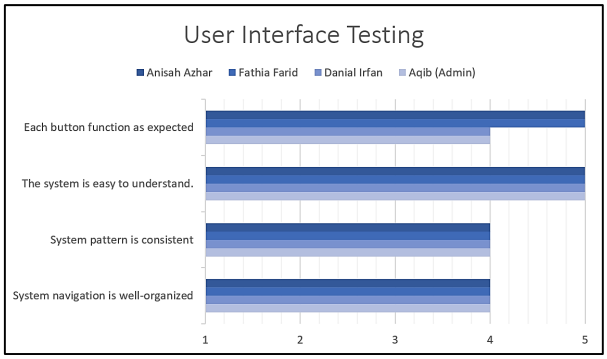


Figure 14: User Interface Testing

According to Figure 14, user interface testing is based on each user. Four people responded represented as Admin, Clerk, Doctor, and Patient. Most respondents answered 4 (satisfied) for each button functions as expected, the system is easy to understand, the system pattern is consistent, and the system navigation is well-organized. Only one respondent rated each button as 5 (Strongly Satisfied), and the system is simple to use.

6. Conclusion

To improve dental appointment booking management and replace the manual system, a secure dental appointment system was created. Email OTP verification for user registration and dual authentication, CAPTCHA for user login, as well as basic security approaches including RBAC, strong password validation and hash passwords with salt, are also implemented. This is crucial to guarantee the system is safe enough to store credential data and to prevent any unauthorized access. This project uses the iterative waterfall model and includes all the essential phases that must be completed.

Furthermore, this system undergoes system testing to test the functionality of the system by the dental clinic and other testers. It has successfully addressed the objectives of designing, developing, and testing a secure system for patients to book dental appointments. The system's advantages, such as online booking and reduced waiting times, have enhanced the overall patient experience. However, to further enhance the functionality, it is recommended to incorporate a payment module for online transactions, implement a security log for system security monitoring, and include a reporting documentation module for comprehensive dental record management. These future improvements would enhance the system's efficiency, convenience, and security, benefiting both patients and the dental clinic in the long run.

Acknowledgements

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

Appendix A

Table 7: User Test for Admin Module

No	Test Case	Actual Result
1	Admin able to register clerk.	Pass
2	Admin able to register doctor.	Pass
3	Admin able to register treatment.	Pass
4	Admin able to assign treatment for doctor.	Pass
5	Admin able to view list of clerks.	Pass
6	Admin able to view list of doctors.	Pass
7	Admin able to view list of patients.	Pass
8	Admin able to view list of treatments.	Pass
9	Admin able to view list of appointments.	Pass
10	Admin able to remove clerks.	Pass
11	Admin able to remove doctors.	Pass
12	Admin able to remove patients.	Pass
13	Admin able to remove treatments.	Pass

Table 8: User Test for Clerk Module

No	Test Case	Actual Result
1	Clerk able to register patient.	Pass
2	Clerk able to schedule and reschedule appointments.	Pass
3	Clerk able to view list of patients.	Pass
4	Clerk able to view list of appointments.	Pass

Table 9: User Test for Doctor Module

No	Test Case	Actual Result
1	Doctor able to view list of assigned patients.	Pass
2	Doctor able to view list of assigned treatments.	Pass
3	Doctor able to view list of assigned appointments.	Pass

Table 10: User Test for Patient Module

No	Test Case	Actual Result
1	Patient able to sign up to the system.	Pass
2	Patient able to login and logout to the system.	Pass
3	Patient able to book and schedule appointment.	Pass
4	Patient able to view list of appointment.	Pass
5	Patient able to cancel the booked appointment.	Pass

References

[1] W. Leung and C. Nøhr, "Improving access to healthcare with on-line medical appointment system," *Studies in Health Technology and Informatics*, vol. 257, pp. 271–276, 2019, doi: 10.3233/978-1-61499-951-5-271.

[2] A. Chaves, T. Guimarães, J. Duarte, H. Peixoto, A. Abelha, and J. Machado, "Development of FHIR based web applications for appointment management in healthcare," *Procedia Computer Science*, vol. 184, pp. 917–922, 2021, doi: https://doi.org/10.1016/j.procs.2021.03.114.

[3] M. Uddin, S. Islam, and A. Al-Nemrat, "A Dynamic Access Control Model Using Authorising Workflow and Task-Role-Based Access Control," *IEEE Access*, vol. 7, pp. 166676–166689, 2019, doi: 10.1109/ACCESS.2019.2947377.

[4] A. J. Lekan and O. S. Abiodun, "Design and Implementation of a Patient Appointment and Scheduling System," *International Advanced Research Journal in Science, Engineering and Technology ISO*, vol. 4, no. 12, 2017.

[5] H. Alhakami and S. Alhrbi, "Knowledge based Authentication Techniques and Challenges," in *IJACSA) International Journal of Advanced Computer Science and Applications*, 2020, pp. 727–732. [Online]. Available: www.ijacsa.thesai.org

[6] T. S. Algaradi and B. Rama, "Static knowledge-based authentication mechanism for hadoop distributed platform using kerberos," in *International Journal on Advanced Science, Engineering and Information Technology*, 2019. doi: 10.18517/ijaseit.9.3.5721.

[7] Y. Albayram, M. M. Hasan Khan, A. Bamis, S. Kentros, N. Nguyen, and R. Jiang, "Designing challenge questions for location-based authentication systems: a real-life study," *Human-centric Computing and Information Sciences*, vol. 5, no. 1, Dec. 2015, doi: 10.1186/s13673-015-0032-3.

[8] H. C. Lee and S. H. Chang, "RBAC-matrix-based EMR right management system to improve HIPAA compliance," *J Med Syst*, vol. 36, no. 5, pp. 2981–2992, Oct. 2012, doi: 10.1007/s10916-011-9776-0.

[9] R. A. Haraty and M. Naous, "Role-Based Access Control modeling and validation," in *Proceedings - IEEE Symposium on Computers and Communications*, Institute of Electrical and Electronics Engineers Inc., 2013, pp. 61–66. doi: 10.1109/ISCC.2013.6754925.

[10] A. H. Montiel, A. F. Martínez, and G. E. Jacinto, "Implementation of Password Hashing on Embedded Systems with Cryptographic Acceleration Unit," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 2, pp. 171–175, 2022, doi: 10.14569/IJACSA.2022.0130221.

[11] V. Chandra, "Comparison between Various Software Development Methodologies," in *International Journal of Computer Applications*, 2015, pp. 975–8887.