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

AITCS

Vol. 6 No. 1 (2025) 663-682
https://publisher.uthm.edu.my/periodicals/index.php/aitcs

A Secure Online Booking System with OTP for Sultans Spa Resort

Aoni Ali Mohammed Alghail[1], Shamsul Kamal Ahmad Khalid[1]*

[1] *Fakulti Sains Komputer dan Teknologi Maklumat,*
Universiti Tun Hussein Onn Malaysia, Parit Raja, Batu Pahat, 86400, MALAYSIA

*Corresponding Author: shamsulk@uthm.edu.my
DOI: https://doi.org/10.30880/aitcs.2025.06.01.037

Article Info

Received: 15 May 2025
Accepted: 19 June 2025
Available online: 30 June 2025

Keywords

Authentication, One-Time Password, Online Booking System, Sultans Spa Resort, Account Verification,

Abstract

Sultans Spa Resort in Riyadh, Saudi Arabia, currently relies on phone calls and in-person visits for booking appointments, which limits scalability, efficiency, and security. This traditional approach exposes the system to risks such as unauthorized access and data breaches, compromising sensitive customer information and disrupting business operations. To address these challenges, this project proposes a secure online booking system with advanced features, including one-time password (OTP) authentication to enhance data protection and ensure secure user authentication. Guided by the Agile methodology, the project ensures flexibility, iterative progress, and continuous feedback to meet evolving customer needs and security requirements. The system will automate key spa operations such as appointment scheduling, customer account management, and real-time availability checks, leveraging technologies like HTML, CSS, PHP, JavaScript, and MySQL. This web-based platform aims to streamline booking processes, improve operational efficiency, and deliver a secure and user-friendly experience for customers. The system's functionality and security will be thoroughly validated through alpha and beta testing to ensure reliability and effectiveness. By adopting this system, Sultans Spa Resort seeks to position itself as a leader in the hospitality industry, fostering long-term success, customer loyalty, and robust protection of sensitive customer information.

1. Introduction

In today's digital world, information security is crucial for protecting sensitive data across various sectors, including the spa and wellness industry. Traditional appointment booking methods, like paper records or phone calls, are vulnerable to breaches or unauthorized access, leading to financial losses and reputational damage[1]. Sultans Spa Resort in Riyadh, Saudi Arabia, currently relies on in-person visits or phone calls for bookings. This method limits scalability and efficiency, as customers are restricted to business hours, and staff time is consumed managing bookings. Without an online presence, Sultans Spa Resort struggles to attract new customers and expand its client base. This project aims to develop a secure online booking system for Sultans Spa Resort, enhancing convenience for customers and staff while prioritizing the protection of sensitive customer data. The system will provide a user-friendly platform for scheduling appointments, viewing real-time availability, and accessing other spa services online. Advanced security measures, including one-time password (OTP) authentication, will ensure the confidentiality, integrity, and availability of customer information.

The main problem of Sultans Spa Resort in Riyadh, Saudi Arabia, is the traditional reservation system, which is ineffective and missing security features. This system exposes sensitive customer data to potential breaches, posing significant risks to the spa's reputation and financial stability. These difficulties are made worse

by operational inefficiencies including manual data processing and restricted booking hours. Sultans Spa Resort is also less able to reach a wider audience and successfully compete in the contemporary spa market due to its lack of an internet presence. By improving data security and expediting the booking process, the suggested secure online booking system seeks to address these problems for Sultans Spa Resort.

The primary objectives of this project are to design, implement, and test a secure online booking system using one-time password (OTP) authentication for Sultans Spa Resort, enhancing the booking experience, operational efficiency, and data security. The project focuses on developing a core system with essential functionalities, with future enhancements based on Sultans Spa Resort's needs.

Anticipated outcomes include a convenient platform for customers to browse services, schedule appointments, and manage bookings, significantly improving satisfaction and loyalty. For staff, the system automates scheduling and management, increasing operational efficiency. The system's robust security features, including encryption and OTP authentication, will protect sensitive customer data and reduce breach risks. Additionally, the enhanced online presence will attract new customers and support business growth. This strategic investment prioritizes information security, equipping Sultans Spa Resort to compete effectively, improve customer service, and establishing a strong online presence.

In this documentation, Section 2 discusses related works and existing systems currently available in the market, providing a comparison between these systems and the proposed solution. Section 3 outlines the methodologies employed for the development of this system. Section 4 delves into the System Analysis and Design of the proposed secure online booking system for Sultans Spa Resort.

2. Literature Review

This section reviews literature for Sultans Spa Resort's proposed secure online booking system, focusing on advanced security features like one-time password (OTP) authentication. It highlights the limitations of current booking methods, emphasizing the benefits of computerized systems. The review explores various booking systems across industries, identifying best practices from hotel and resort systems that can be adapted for Sultans Spa Resort.

2.1 Manual vs Computerized System

A n the context of booking systems, choosing between manual and computerized booking systems impacts efficiency and security. Manual systems are cost-effective but error-prone and labor-intensive, lacking scalability and security. Computerized systems automate processes, enhance data security with encryption and OTP authentication, and support real-time updates, providing efficiency and accuracy. For Sultans Spa Resort, adopting a computerized system with robust security measures will improve operational efficiency and customer satisfaction.

2.2 Booking Systems

Booking systems vary widely across industries, each designed to meet specific operational demands. Common types include reservation systems for hotels, airlines, and restaurants, leveraging technology to streamline operations. Modern booking systems integrate advanced features such as web-based interfaces, mobile access, and real-time data management, significantly enhancing operational efficiency and customer satisfaction. This overview highlights the increasing shift towards digital solutions that cater to the evolving expectations of tech-savvy consumers and the critical need for robust security measures to protect sensitive customer information.

2.3 Hotel and Resort Booking System

This study focuses on the implementation of complex booking systems in the hotel and resort industries, which handle everything from room reservations to customer relationship management. These systems improve the visitor experience by offering seamless service from booking to check-out and including features like as dynamic pricing, room inventory management, and client preference monitoring[2]. By analyzing other successful hotel booking systems, the section will highlight best practices that Sultans Spa Resort might adopt, such as integrated customer feedback loops and individualized visitor experiences using data analytics.

2.4 Sultans Spa Resort

Sultans Spa Resort, located in Riyadh, Saudi Arabia, leverages modern technology to enhance guest experiences through its online booking system. This system not only streamlines the reservation process but also ensures robust security measures to protect sensitive customer information.

2.4.1 Services

Sultans Spa Resort offers a diverse range of services designed to promote relaxation and rejuvenation. Guests can enjoy various spa treatments, wellness consultations, and luxurious accommodations. Each service is tailored to meet the unique needs and preferences of each guest, reinforcing the resort's commitment to exceptional care and hospitality.

2.4.2 Problem in Booking Systems

Despite the advantages, Sultans Spa Resort faces significant challenges with its current booking system, including issues like overbooking and mismanagement of customer data. These problems often result in customer dissatisfaction and operational inefficiencies. Addressing these issues, the resort plans to implement a new online booking system equipped with advanced features such as real-time data processing and automation to enhance accuracy and efficiency in reservation management.

2.5 Authentication

Authentication is a critical security feature designed to verify user identity and protect system integrity[3. It typically involves checking credentials at the start of an interaction to ensure only authorized users can access and execute commands. Traditional methods include usernames and passwords, but modern practices incorporate additional layers of security, such as one-time passwords (OTP), biometric verification, and multi-factor authentication, to enhance protection beyond the basic username-password framework[4].

2.6 One-time Password

A one-time password (OTP) is an essential security feature that enhances authentication processes, particularly in web applications and sensitive transactions[5]. OTPs are unique, single-use codes that provide a dynamic layer of security, reducing the risk of unauthorized access even if a user's credentials are compromised. Delivered via secure channels like email or SMS, OTPs strengthen defenses against brute force, dictionary attacks, and phishing. Their ephemeral nature—valid only for a short period—further mitigates risks, ensuring time-sensitive authentication [4]. Effective OTP generation relies on strong algorithms that produce unique, short-lived codes, synchronized with server timestamps for maximum security[6].

2.7 Security Features

The secure online booking system for Sultans Spa Resort is designed to ensure the highest levels of data protection and user privacy. To achieve this, the system integrates a comprehensive suite of advanced security features, crucial for preventing unauthorized access and safeguarding sensitive guest information[7]. Key components include Bcrypt hashing for secure password storage, stringent password complexity rules, session timeouts, and authentication methods such as OTP.

2.7.1 Bcrypt Hashing

Bcrypt is a cryptographic hashing method chosen for Sultans Spa Resort's secure online booking system due to its robust security features. It uses the Blowfish symmetric key block cipher technique, incorporating a salting mechanism and a programmable cost factor to enhance password security[8]. Bcrypt's computational intensity slows down brute-force attacks, providing an additional layer of defense[9]. Its scalability allows for adjustments in computational difficulty, ensuring security measures keep pace with advances in hardware capabilities and evolving cyber threats.

2.7.2 Password Validation

The system enforces strong password policies through rigorous password validation techniques. These policies include requirements for password complexity, such as a minimum length, the inclusion of uppercase and lowercase letters, numbers, and special characters. Such measures ensure that all passwords are robust and resistant to common attacks like password guessing or cracking[10]. The online booking system also provides real-time feedback on password strength, helping users create stronger passwords that significantly enhance their account security.

2.7.3 Session Time-Out

To further protect user data from unauthorized access, the system implements automatic session time-outs. This security feature logs users out of their accounts after a period of inactivity, reducing the risk of unauthorized access on unattended or shared devices. By promptly terminating inactive sessions, the spa ensures that sensitive information remains protected, particularly in environments where a device may be used by multiple people[11]. This feature is not only important for maintaining the security of the user's personal information but also helps in

safeguarding the overall integrity of the booking system from potential security threats. Moreover, session time-outs encourage users to actively manage their login status, which fosters a higher level of awareness regarding security practices. The spa can customize the duration of the time-out period based on the sensitivity of the data being accessed, thereby balancing convenience and security.

2.8 Study of Existing Related Systems

This section examines existing hotel booking platforms to identify features and authentication mechanisms that can enhance the security and efficiency of Sultans Spa Resort's online booking system. By studying established systems like Lotus Desaru Beach Resort & Spa, ByootBay Resort & Club, and Cyberview Resort & Spa, valuable insights are gained for integrating similar improvements into Sultans Spa Resort's system.

2.8.1 Lotus Desaru Beach Resort & Spa Website

Lotus Desaru Beach Resort & Spa, located in Johor, Malaysia, features a user-friendly online booking interface. Visitors can easily set check-in and check-out dates and provide guest details. The registration page simplifies the sign-up process with fields for personal information and an alternative Google sign-up option, enhancing the user experience but raising potential security concern.

2.8.2 ByootBay Resort Website

ByootBay Resort & Club in Cairo, Egypt, offers a luxurious and seamless booking experience. The homepage includes a booking interface that captures essential guest information, along with high-quality images to enhance visual appeal. The registration page ensures accurate guest information collection, supporting a secure and personalized booking process.

2.8.3 Cyberview Resort & Spa Website

Cyberview Resort & Spa in Cyberjaya, Malaysia, combines functionality with visual appeal. The homepage features a booking panel for selecting dates and guest numbers, along with navigation tabs for quick access to resort information. The registration page collects key details to personalize communications and ensure data protection compliance.

2.9 Comparison with the Existing Systems

Table 1 *Analysis between Lotus Desaru, ByootBay, Cyberview, and Sultans.*

Feature Category	Feature	Lotus Desaru Beach Resort & Spa	ByootBay Resort & Club	Cyberview Resort & Spa	Sultans Spa Resort
Booking Functions	Platform Used	Web-based	Web-based	Web-based	Web-based
	User Interface	Yes	Yes	Yes	Yes
	Login Functionality	Yes	Yes	Yes	Yes
	Online Booking	Available	Available	Available	Available
	Booking Cancelation	Limited	Not Available	Available	Available
	Real-time Availability	Yes	Yes	Yes	Yes
Security Features	Password Validation	No	Yes	Yes	Yes
	Session Timeout	Yes	Yes	Yes	Yes
	One-time Password (OTP)	No	No	No	Yes
	Encryption	Basic	Advanced	Advanced	Advanced

Table 1 showcases the booking functionalities and security features of four resorts: Lotus Desaru Beach Resort & Spa, ByootBay Resort & Club, Cyberview Resort & Spa, and Sultans Spa Resort. All resorts utilize web-based platforms with robust user interfaces, enabling convenient online booking and real-time availability checks. However, Sultans Spa Resort distinguishes itself by incorporating advanced security measures such as session timeouts to secure user sessions and the use of One-Time Passwords (OTP) for enhanced registration security. Additionally, while all except Lotus Desaru provide password validation, Sultans Spa Resort employs advanced

encryption techniques, ensuring superior data protection and security in its booking system. These features underscore Sultans Spa Resort's commitment to providing a secure and user-friendly online booking experience [12].

3. Methodology

This section outlines the methodology for developing a secure online booking system with One-Time Password (OTP) authentication for Sultans Spa Resort. The process is detailed from the initial requirement specifications through to system testing, ensuring a thorough approach to building a robust platform. There are many methodologies that can be used to implement this project. However, Agile methodology has been chosen for this project due to its dynamic development environment that can accommodate the specific security requirements and functionality demands of a robust online booking system for Sultans Spa Resort. This method supports the project's aim to deliver a secure, user-friendly, and reliable system, while also allowing for scalability and continuous improvement post-deployment[13].

3.1 Agile Model

The agile model is a modern and flexible software development approach that has replaced traditional methodologies [14]. It emphasizes adaptability to changing project requirements. In this project, Agile was adopted to manage the secure online booking system for Sultans Spa Resort by organizing the work into short, iterative cycles or sprints, allowing continuous feedback and improvements after each phase. Fig. 1 presents the overall process, involving iterative cycles covering planning, requirements analysis, design, development, testing, and deployment. With six structured phases, the agile methodology ensures responsiveness and ongoing value for development teams.

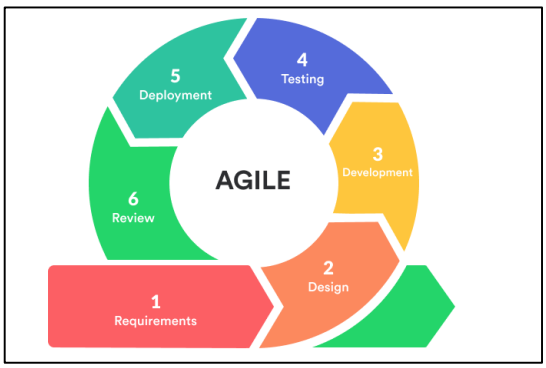


Fig. 1 *The Phases of Agile Model [15]*

3.1.1 Requirements Phase

The Requirements Phase defines the core needs of Sultans Spa Resort's secure online booking system. It focuses on identifying both functional and non-functional requirements. Functional requirements cover system operations, while non-functional ones address performance, usability, and security. The phase also includes planning the project's scope, goals, and resources, with clear timelines to ensure timely delivery.

3.1.2 Design Phase

The Design Phase involves developing the user interface and database structure for the secure online booking system. Based on the requirements, the design includes screens for registration, login, and password reset. The registration feature uses PHPMailer with SMTP to send OTPs for secure email verification.

3.1.3 Development Phase

In the Development Phase, core system features are implemented, including OTP integration for secure user authentication. XAMPP and Visual Studio Code are used for development, with sample data added to test system functionality and interface layout. Regular database backups are maintained to ensure data safety during development.

3.1.4 Testing Phase

The Testing Phase ensures that all features of the booking system function correctly and securely. It includes unit testing, system testing, user acceptance testing, OWASP security testing, and positive scenario testing, all performed on modular components. These tests help identify and resolve issues, improving overall performance.

The goal is to ensure alignment with system requirements, delivering a secure and user-friendly booking experience with OTP authentication.

3.1.5 Deployment Phase

The Deployment Phase involves releasing and installing the system into the live environment. It includes server setup, database upload, and OTP authentication integration. Final testing is completed before deployment, and user training with clear documentation supports system use. Continuous monitoring helps resolve issues and ensures smooth system integration.

3.1.6 Review Phase

The Review Phase focuses on evaluating system performance and gathering user feedback. The feedback is analyzed to identify areas for improvement. Based on the findings, earlier phases may be revisited for refinements, or the system may be finalized if it meets expected standards.

4. System Analysis and Design

This section outlines the design and implementation process of the secure online booking system for Sultans Spa Resort. It covers system architecture, design considerations, and technologies used, aiming to create a user-friendly platform with advanced security features like One-Time Password (OTP) authentication. The section details the step-by-step implementation of core functionalities, focusing on usability, security, and scalability to meet the needs of Sultans Spa Resort and its clients.

4.1 System Requirements Analysis

In developing the secure online booking system for Sultans Spa Resort, requirements are categorized into functional and non-functional types. Functional requirements outline the critical operations the system must perform, including data processing, calculations, and interactions between system components, ensuring thorough coverage of the platform's essential capabilities.

4.1.1 Functional Requirements

This section will describe the functionalities that is going to be developed in the system as shown in Table 2.

Table 2 *Functional Requirements for Sultans Spa Resort*

Module	Functional Requirements	User
Registration	1. Allow users to create accounts. 2. Secure account creation using OTP. 3. System alert for any invalid input.	Customer
Login	Sultans System should allow users able to login using Email, and Password.	Admin/Customer
Booking	1. Allow users to book, view, and cancel appointments. 2. Provide real-time availability of time slots and services.	Admin
Payment	1. Enable secure online payments. 2. Process transactions using integrated payment gateway. 3. Allow users to view Receipt.	Customer
Manage	1. Admin dashboard for managing bookings, user accounts, and system settings. 2. Update booking status by making confirmation of the booked appointment.	Admin

4.1.2 Non-Functional Requirements

This section will describe the requirements that are not directly concerned with the specific functions delivered by the system as shown in Table 3.

Table 3 *Non-Functional Requirements for Sultans Spa Resort*

Module	Non-Functional Requirements
Performance	1. The system should be able to use anytime. 2. Page load time should be under 3 seconds.
Operational	1. The user interface should be intuitive and easy to navigate. 2. The system can handle concurrent users.
Security	1. The password must be a combination of capital letters, small letters, numbers, and characters to meet the strong password requirements. 2. The password is encrypted with Bcrypt.
Usability	1. The system must be able to scale to accommodate future growth in user base and data volume. 2. Modular design to easily add new features.

4.1.3 User Requirements Analysis

In this section, the features and functionalities of the proposed application will be elucidated for the user. User requirements, outlining the tasks achieved by both customers and admins, are presented in Tables 4.

Table 4 *User Requirements Analysis for Sultans Spa Resort*

User	Task Analysis
Customer	• Register and login to the system. • Make a booking. • Make payments for bookings. • View booking and payment status. • View booking status. • Edit profile.
Admin	• Login to the system. • View and manage booking data. • View and manage booking confirmations. • View payment transactions. • View and manage user (customer) data. • View and manage services. • View activity log. • Add services. • Add staff.

4.2 System Analysis

System analysis involves visually representing the data flow and processes within the proposed system using various techniques. For the Sultans Spa Resort online booking system, three primary techniques will be utilized: Context Diagram, Data Flow Diagram (DFD), and Entity Relationship Diagram (ERD). These techniques aim to simplify the understanding of the system's complex elements, which can be challenging to convey through text alone. Visualizing all components allows for easier identification and resolution of potential issues, ensuring the development of a robust and efficient system.

4.2.1 Data Context Diagram (DFD CD)

The Data Flow Diagram (DFD) is a graphical representation of the flow of data within the Sultans Spa Resort Booking System. It illustrates how the system processes and transfers data between various processes and data stores, providing a clear understanding of the system's data management and operational workflow. Fig. 2 illustrates the context diagram for the Sultans Spa Resort Booking System, showing interactions between the admin and customer. Admins manage bookings, rooms, payments, and customer accounts, while customers register via OTP, log in, book rooms, make payments, and update profiles. The diagram provides an overview of secure and efficient system operations.

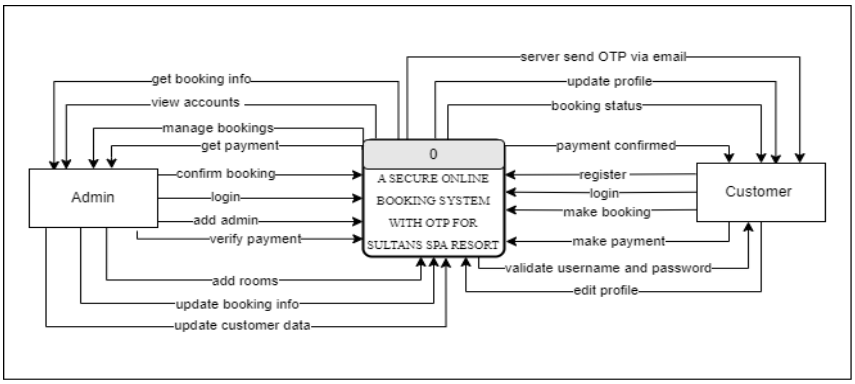
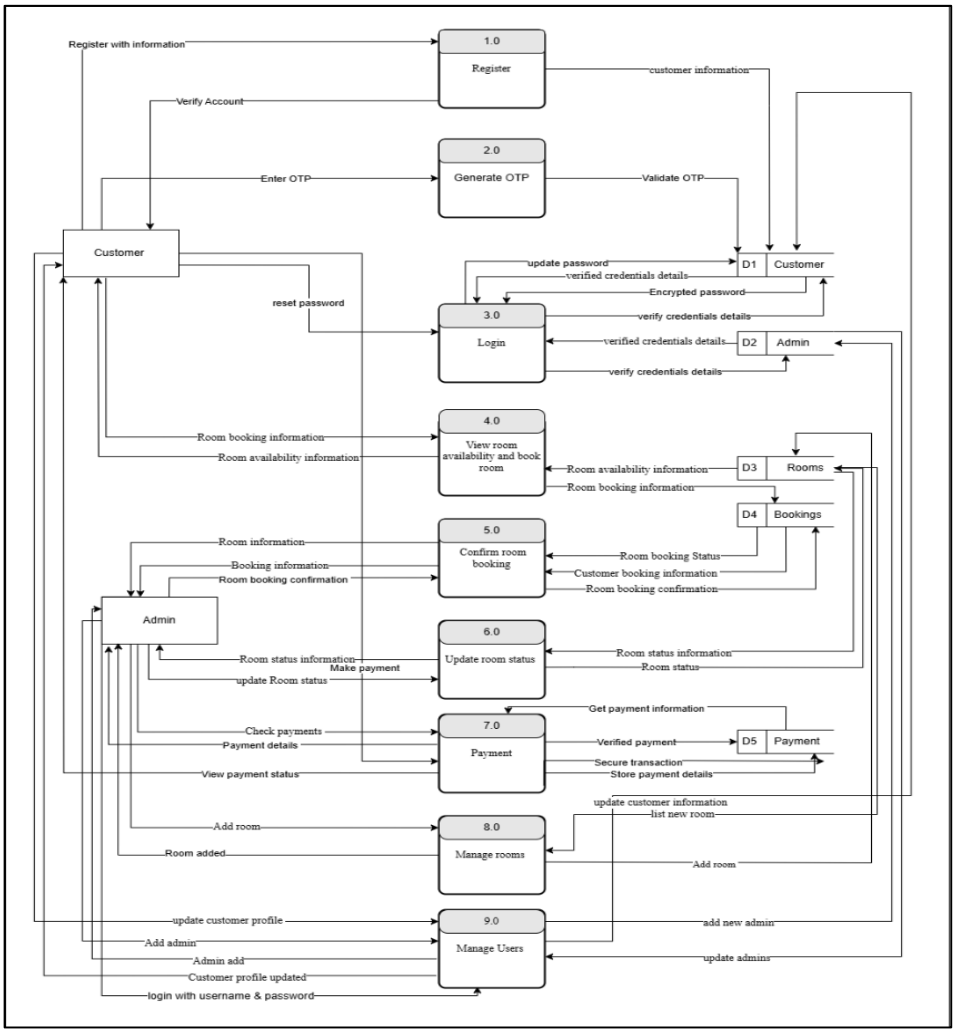


Fig. 2 *Data Context Diagram Sultans Spa Resort*

4.2.2 Data Flow Diagram Level 0

Fig. 3 illustrates the Data Flow Diagram (DFD) Level 0 for the Sultans Spa Resort Booking System. The diagram highlights key processes such as registration, login, room booking, payment, and user management. Customers register using their details and OTP for email verification, log in to view room availability, make bookings, and process payments securely. Admins manage the system by confirming bookings, updating room statuses, adding rooms, and overseeing user profiles. The DFD provides a clear overview of the interactions between customers, admins, and the system, ensuring efficient data flow and robust operational management for the Sultans Spa Resort.

Fig. 3 Data Flow Diagram Level 0 for Sultans Spa Resort



Applied Information Technology and Computer Science Vol. 6 No. 1 (2025) p. 663-682

4.2.3 Entity Relation Diagram (ERD)

An Entity Relationship Diagram (ERD) visually represents the relationships between the entities in a database. It depicts how data within these entities is interconnected. Fig. 4 illustrates the ERD for the proposed system, highlighting the connections and interactions between different data entities.

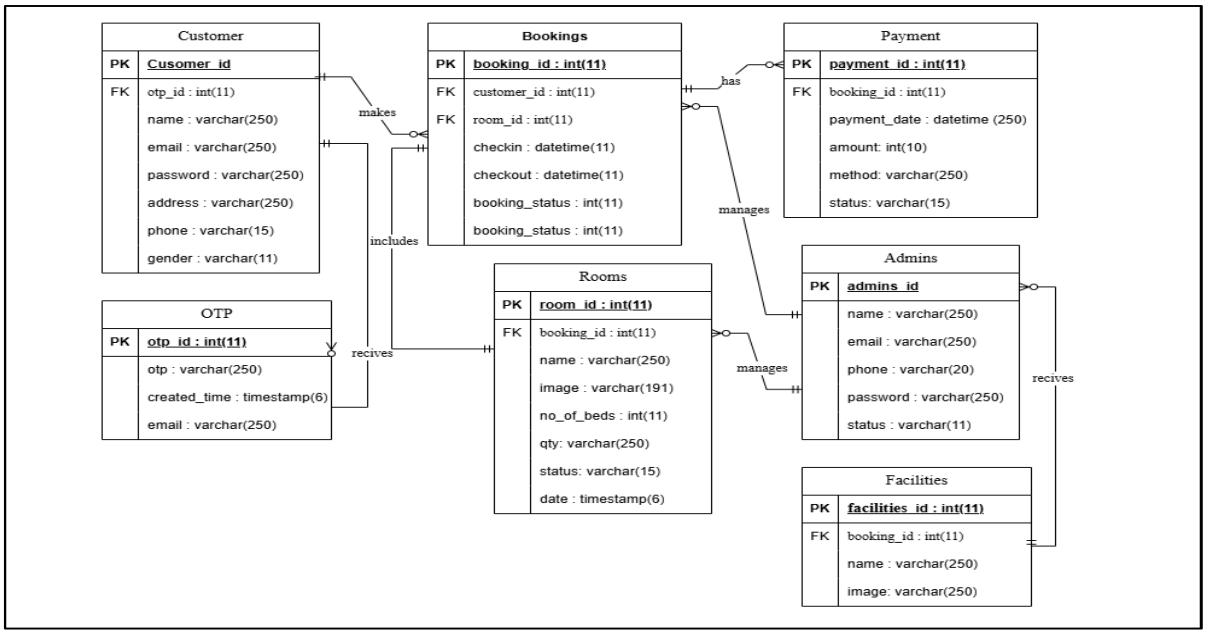


Fig. 4 *Entity Relation Diagram (ERD) for Sultans Spa Resort*

4.2.4 System Flowchart

The flowchart depicted in Fig. 5 illustrates the core processes of the Sultans Spa Resort Booking System for both customers and administrators. For customers, the flow starts at the home page. New customers must register by entering their details and verifying their account via an OTP sent to their email. If the OTP is valid, an account is successfully created. Existing customers can log in, access the homepage, browse available rooms, make room bookings, confirm their reservations, and proceed with secure payment. They can also view and manage their booking details. The process concludes with the customer logging out to maintain account security.

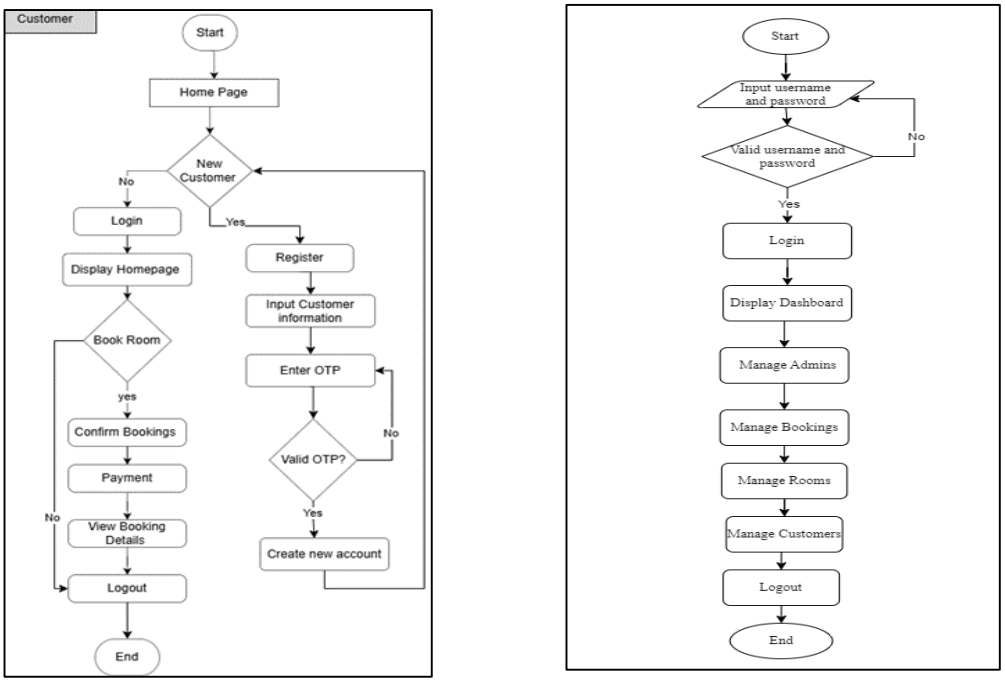


Fig. 5 *Flowchart for Sultans Spa Resort System*

On the administrator side, the flow begins with logging in using a valid username and password. After gaining access, administrators navigate the system through a dashboard interface, enabling them to manage administrative accounts, oversee bookings, update room details, and maintain customer data. The workflow ends with the administrator securely logging out, ensuring the system's integrity. This flowchart provides a detailed visualization of the operational processes, ensuring that both customers and administrators experience seamless and secure interaction with the system.

4.3 System Design

A After thoroughly analyzing all user requirements, the project transitions to the design phase. During this stage, the interface and database for the Sultans Spa Resort Booking System with One-Time Password (OTP) authentication are carefully designed. This step ensures a clear and detailed visualization of the system's structure and functionality, laying a strong foundation before proceeding to the coding phase.

4.3.1 System Architecture

Fig. 6 shows the system architecture of the Sultans Spa Resort Booking System with OTP email authentication. Customer login requires email and password verification, followed by OTP generation and dispatch. Admin login verifies username and password. Admins manage user accounts, rooms, bookings, and payments, while customers can book rooms, update profiles, make payments, and view booking statuses. All activities are securely recorded in the database.

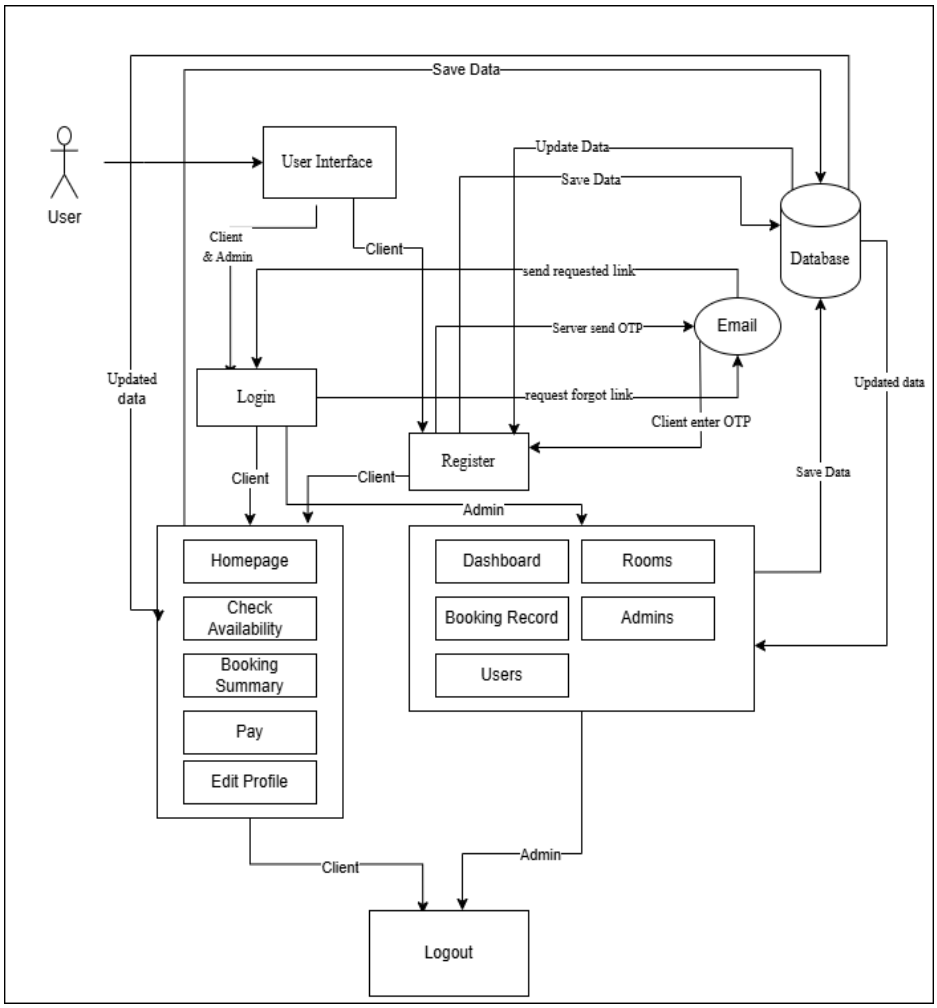


Fig. 6 *System Architecture for Sultans Spa Resort*

Applied Information Technology and Computer Science Vol. 6 No. 1 (2025) p. 663-682

4.3.2 Interface Design

User interface design focuses on creating visually appealing and user-friendly interfaces, balancing aesthetics and functionality for a seamless user experience. In systems like the Hotel Reservation Management System, intuitive interfaces enhance navigation and usability for developers and users alike.

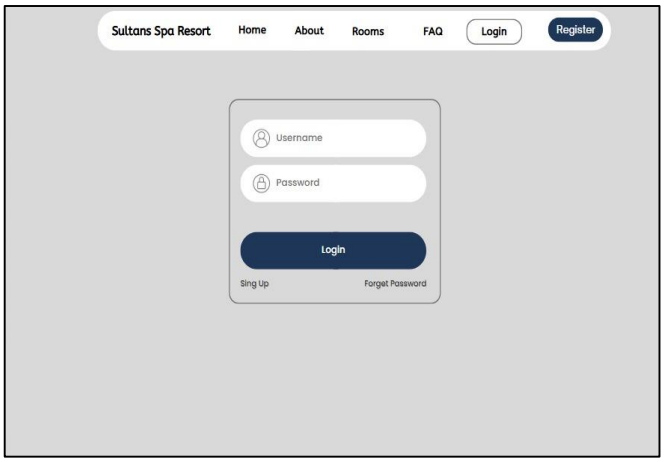


Fig. 7 *Login Interface Page for Customer*

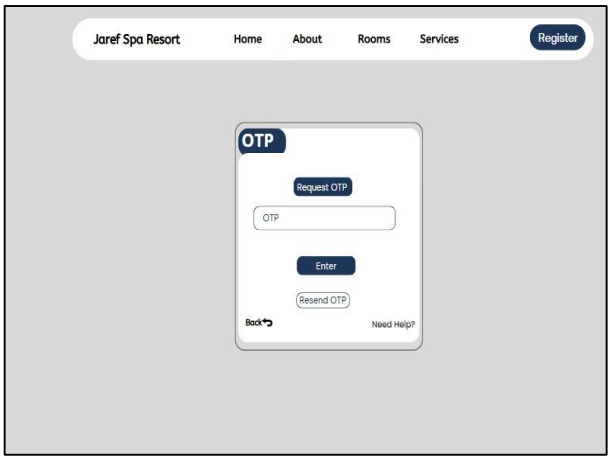


Fig. 8 *OTP Interface Page*

Fig. 7 shows the login interface for customers at Sultans Spa Resort, including fields for entering a username and password, with options to create an account or get help if needed, and Fig. 7 shows the OTP interface page, where customers need to request and enter a one-time password (OTP) to ensure secure registration.

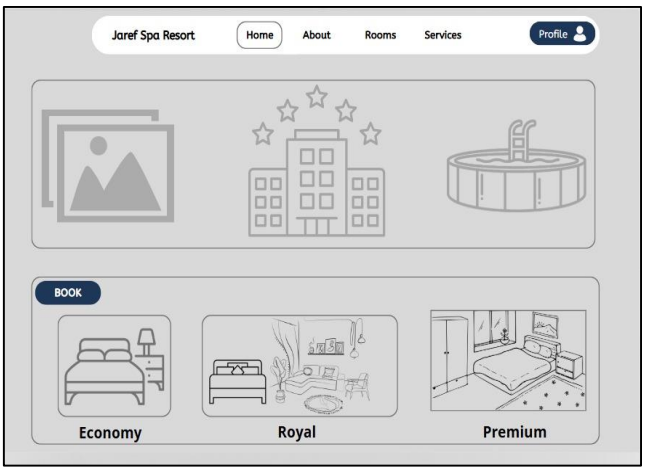


Fig. 9 *Homepage Interface Page for Customer*

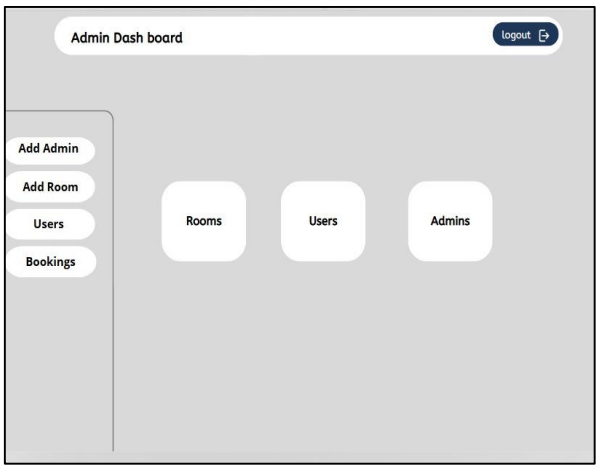


Fig. 10 *Homepage Interface Page for Admin*

Fig. 8 shows the homepage interface for customers, featuring options to book Economy, Royal, or Premium rooms, and Fig. 9 shows the admin dashboard interface, with options to add admins, add rooms, manage users, and handle bookings.

5. Implementation and Testing

This section covers the implementation and testing of Sultans System, detailing the integration of security modules and system properties. Additionally, it presents the results of user acceptance testing to evaluate the system's functionality and performance.

5.1 Implementation of Security Module

This section highlights the security modules integrated into the system, designed to ensure its confidentiality, integrity, and availability. Key security features include One-Time Password (OTP) for enhanced user authentication, Bcrypt Hashing for secure password storage, Password Validation to enforce strong credential standards, and Session Time-Out to protect against unauthorized access. These features collectively strengthen the system's overall security framework.

5.1.1 One-Time Password

Fig. 11 illustrates the generateOTP($phone) function, designed to create a secure 6-digit One-Time Password (OTP) for user authentication. The function begins by converting the phone number to a string and applying the SHA-256 hashing algorithm for robust security. From the hash, numeric digits are extracted and randomized to prevent patterns, ensuring unpredictability. The first six digits are then selected, and if fewer than six, padded with leading zeros to maintain consistency. This process ensures the OTP is secure, reliable, and user-friendly for authentication purposes.

```php
function generateOTP($phone) {
    // Ensure phone number is treated as a string
    $phone = (string)$phone;

    // Hash the phone number using SHA-256
    $hash = hash('sha256', $phone);

    // Extract digits from the hash
    $digits = preg_replace('/\D/', '', $hash);

    // Shuffle the digits to randomize them
    $digitsArray = str_split($digits);
    shuffle($digitsArray);
    $shuffledDigits = implode('', $digitsArray);

    // Take the first 6 digits from the shuffled digits
    $otp = substr($shuffledDigits, 0, 6);

    // Pad with zeros if less than 6 digits
    if (strlen($otp) < 6) {
        $otp = str_pad($otp, 6, '0', STR_PAD_LEFT);
    }

    return $otp;
}
```

Fig. 11 *Partial Code Generating OTP*

Fig. 12 *The OTP Generated and Received by User*

Fig. 12 displays the One-Time Password (OTP) email received by the user for verification purposes. The email, sent from Sultans Spa Resort, contains a unique 6-digit code (220024) generated securely to authenticate the user during the registration or login process. This process ensures secure and reliable account verification, enhancing the overall security of the system.

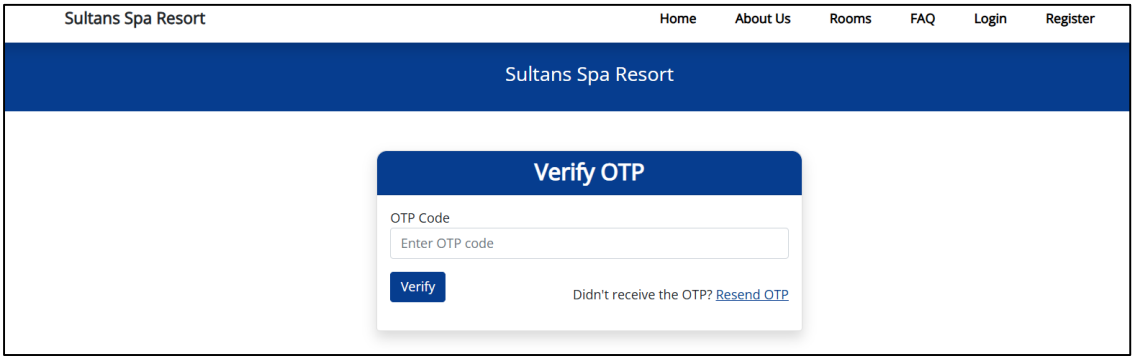


Fig. 13 *One-Time Password (OTP) Verification Page for User*

Fig. 13 illustrates the OTP verification page for Sultans Spa Resort. Users are required to enter the verification code sent to their email to activate their account. If the code has not been received, users can request a new OTP by clicking the Resend OTP link, ensuring a seamless account activation process.

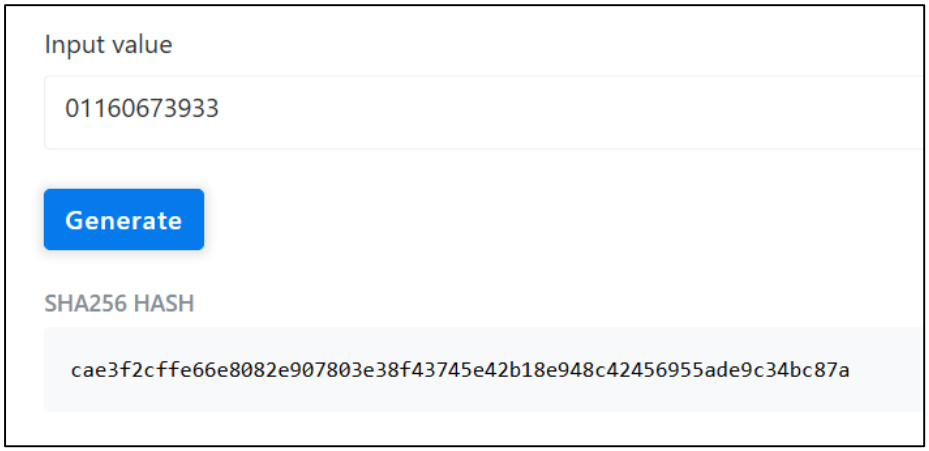


Fig. 14 *SHA-256 hash generator*

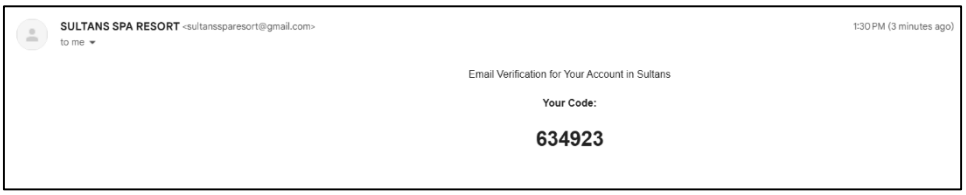


Fig. 15 *OTP email sent to the user*

Fig. 14 and 15 illustrate the process of generating a One-Time Password (OTP) based on the hashed value of a user's phone number, highlighting the system's ability to produce user-specific authentication codes. For demonstration purposes, the OTP generation code was temporarily configured to extract the first six digits from the SHA-256 hash of the phone number. In Fig.14, the phone number "01160673933" is hashed using the SHA-256 algorithm, resulting in a unique 64-character hexadecimal string. The initial six digits of this hash are extracted to create the OTP. Fig. 15 depicts the OTP email sent to the user, showcasing the OTP "634923," which corresponds to the first six digits of the hashed phone number. This process demonstrates the secure linkage between the user's phone number and the OTP, underscoring the system's reliability in generating unique and user-specific authentication codes.

5.1.2 BCRYPT Hashing

```
90          // Hash the password before storing in the database
91          $hashed_password = password_hash($password, PASSWORD_DEFAULT);
92
93          $query = "INSERT INTO users (fname, passport, phone, gender, email, password, active)
94                    VALUES ('$fname', '$passport', '$phone', '$gender', '$email', '$hashed_password', '$active')";
95          $query_run = mysqli_query($con, $query);
96
97          if ($query_run) {
98              $_SESSION['Email'] = $email;
99              include_once('./mail/index.php');
00              $_SESSION['status'] = "Registration successful. Please verify your email.";
01              header('location: verify-otp.php');
02          } else {
03              $_SESSION['status'] = "Something went wrong. Try again.";
04              header('location: register.php');
05          }
```

Fig. 16 *Partial Code for Bcrypt Hashing for Password*

Fig. 16 shows the PHP code implementing Bcrypt for secure password hashing using the `password_hash()` function with `PASSWORD_DEFAULT`. The hashed password is stored in the database through an SQL query. If successful, the system sends a verification OTP email and redirects the user to the OTP verification page. In case of an error, the user is redirected back to the registration page. This ensures secure password storage and a reliable registration process.

id	fname	passport	phone	gender	email	password
1	Hamzah	108583	01160673933	Male	onetow11223@gmail.com	$2y$10$DnAn0DgFOMaULCsOrKjRX.gZxbfGj8.a8nkQNjqDF/W...
52	AONI ALI MOHAMMED MOHAMMED	09617759	01160673933	Male	bi210028@student.uthm.edu.my	$2y$10$mXWg5eU7/pGiOPlymVIF0.p/IcFeunpDWctgR.65wsI...
53	Nasr	456456	1139282725	Male	itsegzix@gmail.com	$2y$10$D7W3KWfkrn/X9xJuOeCQ8.LQYlaNk7gk9LvdH4eFPdE...
54	Hasan Mohammed	0854662	01160673933	Male	hsnforstuday@gmail.com	$2y$10$Q3uO01WqBrABhFPapl4Xf.GFNaLPyKoyW9F3h94O7bN...
56	muaadh	09616667	01160673933	Male	bi220006@student.uth.edu.my	$2y$10$/lP1vNYvDh4fOeCs0Ok9o.m9snJcfnPJNLrotCK4fb2...

Fig. 17 *BCRYPT Hashing for Password in Database*

Fig. 17 shows a sample of user data stored in a database. The passwords are securely stored using the BCRYPT hashing algorithm, ensuring that even if the database is compromised, the passwords remain protected.

5.1.3 Password Complexity

```
56      // Check for password strength
57      $password_errors = [];
58      if (strlen($password) < 8) {
59          $password_errors[] = "Password must be at least 8 characters long.";
60      }
61      if (!preg_match('/[A-Z]/', $password)) {
62          $password_errors[] = "Password must contain at least one uppercase letter.";
63      }
64      if (!preg_match('/[a-z]/', $password)) {
65          $password_errors[] = "Password must contain at least one lowercase letter.";
66      }
67      if (!preg_match('/[0-9]/', $password)) {
68          $password_errors[] = "Password must contain at least one number.";
69      }
70      if (!preg_match('/[\W]/', $password)) {
71          $password_errors[] = "Password must contain at least one special character.";
72      }
```

Fig. 18 *Partial Code for Validation Process for Password Complexity*

Fig. 18 illustrates the source code used to enforce password complexity requirements in the Sultans Spa Resort Booking System. The code begins by checking if the password is at least 8 characters long using the `strlen()` function. If the password is too short, an error message prompts the user to create a longer password. Subsequently, the `preg_match()` function is used to ensure that the password contains at least one uppercase letter, one lowercase letter, one numeric digit, and one special character. For each unmet condition, an error message is generated to inform the user of the specific requirement. This method significantly enhances the security of user accounts by requiring strong, complex passwords, making them more resistant to guessing or brute-force attacks.

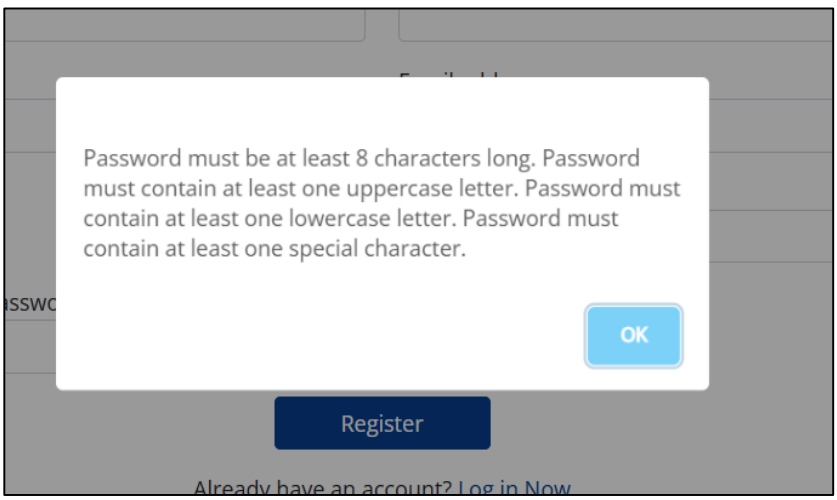


Fig. 19 *The Error Message if User Enter Password That Does Not Fulfil the Password Policy*

Fig. 19 illustrates a user interface for entering and confirming a password, with a validation message indicating the requirements for a strong password. The password must contain uppercase letters, lowercase letters, numbers, and symbols.

5.1.4 Session Time-Out

```php
<?php

// Check if the time elapsed since the last activity is greater than 900 seconds (15 minutes)
if (time() - $_SESSION['last_activity'] > 900) {
    // Unset all session variables
    session_unset();
    // Destroy the session
    session_destroy();
    // Redirect to the login page
    header('refresh:0;url=login.php');
} else {
    // Update the last activity time to the current time
    $_SESSION['last_activity'] = time();
}

```

Fig. 20 *Partial Code for Destroy Session*

Fig. 20 provided PHP code snippet implements a session timeout mechanism to enhance security by automatically logging out users after 15 minutes of inactivity. It checks if the elapsed time since the last recorded activity exceeds 900 seconds (15 minutes). If so, it unsets all session variables using `session_unset()`, destroys the session with `session_destroy()`, and redirects the user to the login page using `header('refresh:0;url=login.php')`. If the session is still active, the code updates the `$_SESSION['last_activity` variable to the current time, ensuring the session remains active with continued user interaction. This mechanism helps prevent unauthorized access to inactive sessions.

5.2 Implementation of System Properties

This section discusses the modules implemented in the Sultans Spa Resort Booking System. The system is composed of four main modules: the login module, registration module, booking module, and admin module. Each module is specifically designed to perform essential functions that are vital to the system's functionality and user experience.

5.2.1 Login Module

Fig. 21 displays the login page for the Sultans Spa Resort Booking System, prompting users to enter their email and password. Fig. 22 presents the corresponding code snippet that handles the login process securely. User inputs are sanitized using `mysqli_real_escape_string()` and matched against database records. Password verification is conducted using `password_verify()`, comparing the entered password with the hashed password stored in the database. If credentials are valid and the account is active, a session is initiated, storing the user's ID, email, and last activity timestamp, and the user is redirected. Inactive accounts trigger an OTP email for activation, redirecting users to the verification page. Invalid credentials result in an error message. This implementation ensures secure authentication, prevents SQL injection, and enhances session management for a seamless user experience.

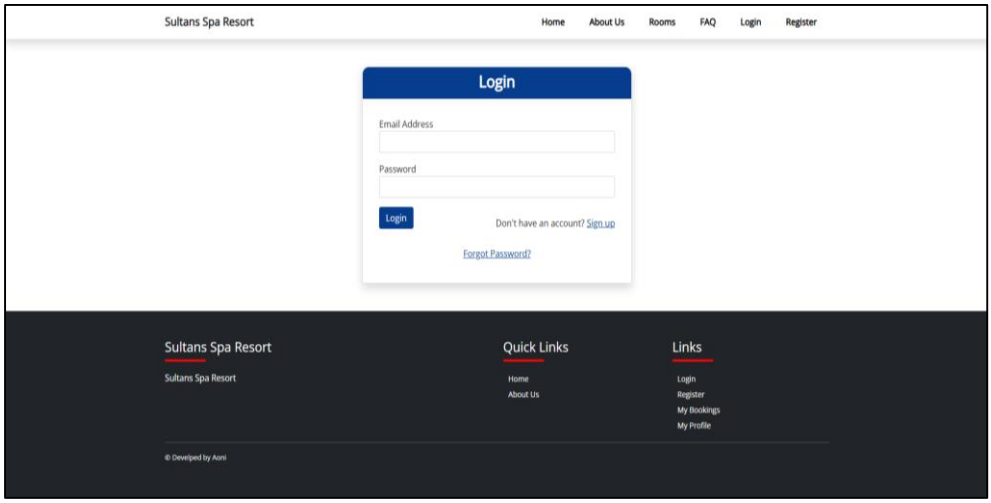


Fig. 21 *Login Page for User*

```php
// User login code
if (isset($_POST['login_btn'])) {
    $email = mysqli_real_escape_string($con, $_POST['email']);
    $password = mysqli_real_escape_string($con, $_POST['password']);

    $query = "SELECT * FROM users WHERE email='$email' LIMIT 1";
    $query_run = mysqli_query($con, $query);
    $row = mysqli_fetch_assoc($query_run);

    if ($row) {
        if (password_verify($password, $row['password'])) { // Verify hashed password
            if ($row['active'] == 1) {
                // Login success for active user
                $_SESSION['auth'] = [
                    'auth_id' => $row['id'],
                    'email' => $row['email'],
                    'fname' => $row['fname'],
                    'passport' => $row['passport'],
                ];
                $_SESSION['login'] = "true";
                $_SESSION['last_activity'] = time(); // Initialize session timeout tracking
                $_SESSION['status'] = "Logged In Successfully";
                header('location: index.php');
            } else {
                // Not active, send OTP
                $_SESSION['Email'] = $email;
                include_once('./mail/index.php');
                $_SESSION['status'] = "Account not activated. Please verify your email.";
                header('location: verify-otp.php');
            }
        } else {
            $_SESSION['status'] = "Invalid credentials";
            header('location: login.php');
        }
    } else {
        $_SESSION['status'] = "Invalid credentials";
```

Fig. 22 *Partial Code for Login Page in User*

5.2.2 Register Module

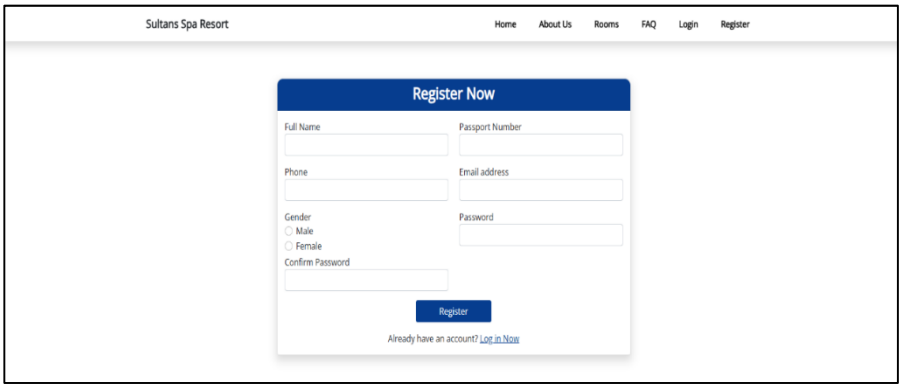


Fig. 23 *Register Page for User*

Fig. 23 illustrates the registration page for the Sultans Spa Resort Booking System, where users are required to provide their first name, passport number, email address, phone number, gender, password, and confirm their password. Additionally, the system sets the user account as inactive by default upon registration to ensure proper email verification before activation.

5.2.3 Booking Module

Fig. 24 displays the room booking page, showing available rooms with images, descriptions, and prices. Users can search for rooms, check availability by selecting dates, and book rooms directly using the Book Now button.

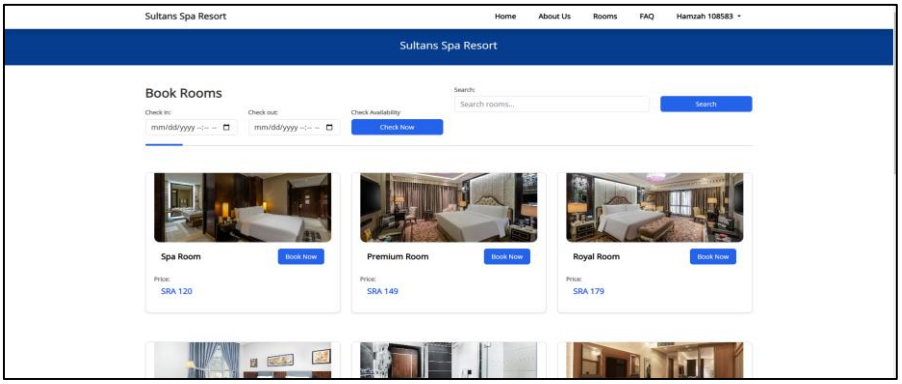


Fig. 24 *Available Rooms for Booking*

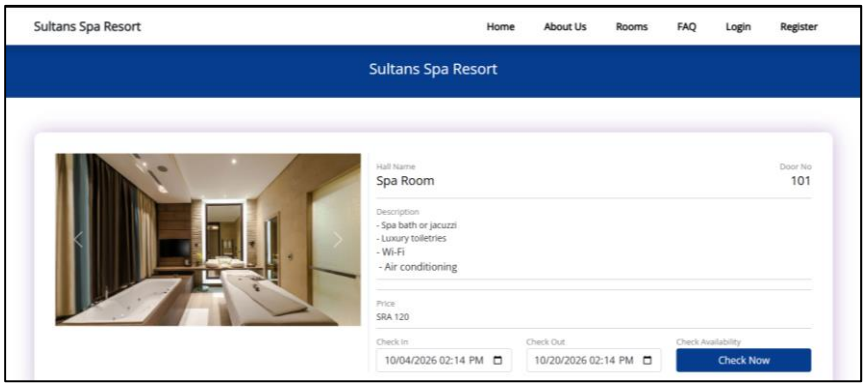


Fig. 25 *Chosen Room for User*

Fig. 25 shows the detailed room page, featuring an image carousel, room descriptions, amenities, price, and door number. Users can check availability by selecting check-in and check-out dates.

5.2.4 Booking Module

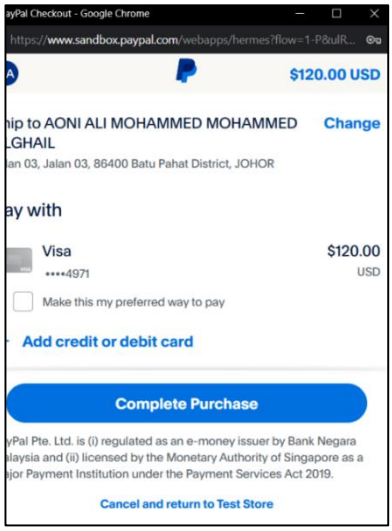


Fig. 26 *Payment Gateway Interface*

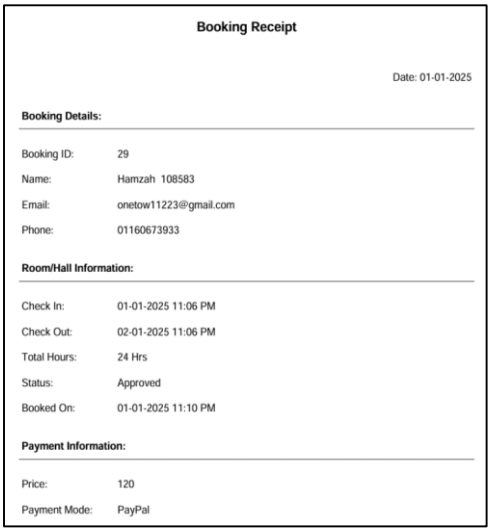


Fig. 27 *Booking Receipt for User*

Fig. 26 shows the PayPal checkout page, where users review their order details and complete payment using a card or PayPal account. Fig. 27 presents a booking receipt with details like booking ID, customer information, check-in/out times, total hours, booking status, and payment method.

5.2.5 Manage Module

Fig. 28 showcases the admin dashboard for Sultans Spa Resort, providing an overview of system metrics, including total rooms, users, admins, and active bookings. It also features quick actions for managing rooms, users, bookings, and settings.

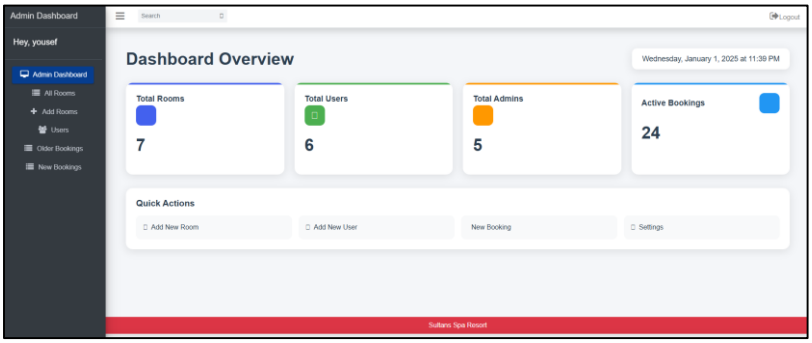


Fig. 28 *Admin Dashboard Overview page*

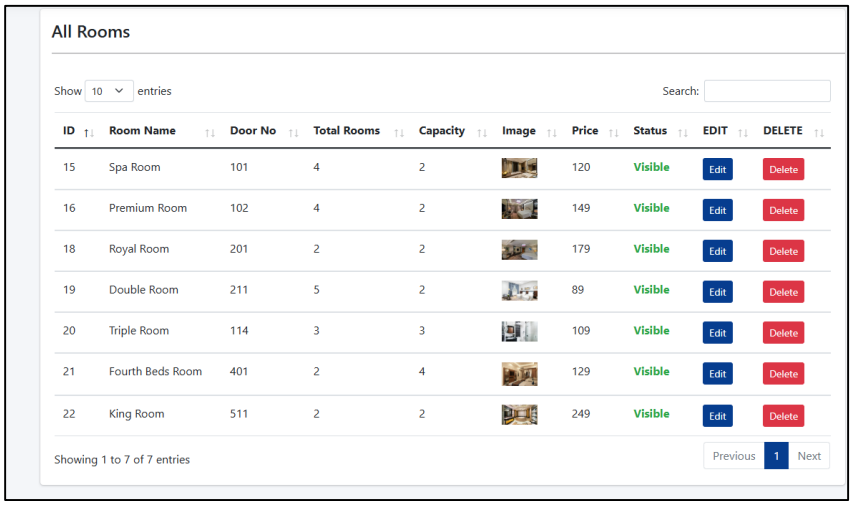


Fig. 29 *All Rooms Management page*

Fig. 29 shows the admin room management page, listing room details like name, capacity, price, and status, with options to edit or delete entries.

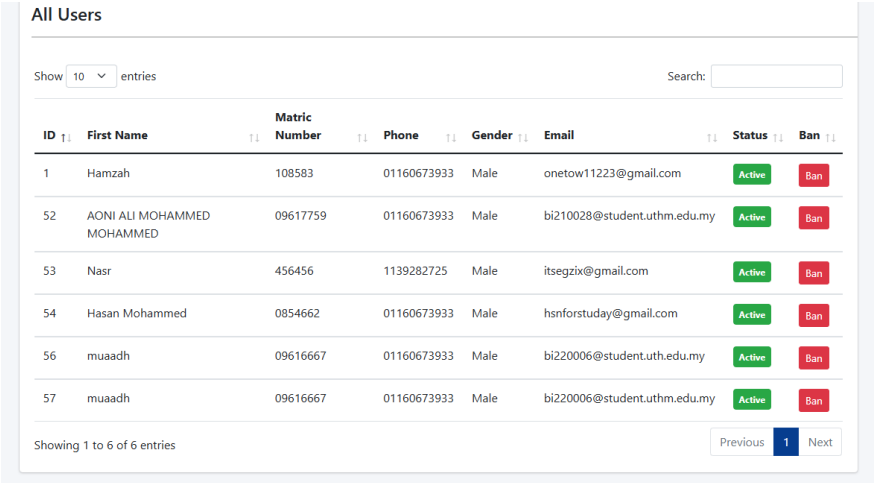


Fig. 29 *User Management page*

Fig. 29 shows the user management page, listing user details such as name, matric number, phone, email, and status, with options to activate or ban accounts.

5.3 Testing

In this section, the testing results of the proposed system are discussed. The testing phase is conducted on the entire system to verify its security and ensure it meets the project requirements.

5.3.1 User Acceptance Testing

This section discusses the user acceptance form, which evaluates the functionality and usability of the Sultans Spa Resort Booking System. The system serves two user types: administrators and customers. Feedback was collected through interviews after system use, with results summarized in Tables 5 and 6.

Table 5 presents the user acceptance form results for users, based on a scale from 1 (Extremely Dissatisfied) to 7 (Extremely Satisfied). The findings show high user satisfaction across all system modules, including the login page, OTP page, Customer Page, and overall system performance.

Table 6 summarizes the user acceptance form results for the Admin of Sultans Spa Resort, using a scale from 1 (Extremely Dissatisfied) to 7 (Extremely Satisfied). The results indicate high satisfaction across all system components, including the login page, Admin dashboard, and overall system functionality.

Applied Information Technology and Computer Science Vol. 6 No. 1 (2025) p. 663-682

Table 5 *User Acceptance Form for customer*

No	Question	Result Dissatisfied 1 -7 Satisfied
Login Page		
1	User can login without problem	7
2	Display message easy to understand	7
OTP Page		
3	User can get OTP via email	7
4	User can enter the correct OTP	7
5	User can use OTP without problem	7
Customer Page		
6	User can check room availability and select their preferred room	7
7	User can confirm a booking and proceed with the reservation process.	6
8	User can make the payment without any issues.	6
9	User can view and edit user information	7
Overall System		
10	Each user can use system without problem	6
11	The interface easy to understand	7
12	The system easy to understand	6

Table 6 *User Acceptance Form for Admin*

No	Question	Result Dissatisfied 1 -7 Satisfied
Login Page		
1	User can login without problem	7
2	Display message easy to understand	6
Admin Page		
3	User can edit, add, and delete rooms	7
4	User can edit, add, and delete bookings	6
5	User can manage payments	7
Overall System		
6	Each user can use system without problem	7
7	The interface easy to understand	7
8	The system easy to understand	6

6. Conclusion

In summary, the Sultans Spa Resort Booking System successfully met its key objectives by incorporating a secure OTP verification feature during user registration, ensuring enhanced security and reliable user authentication. The development process resulted in a secure, user-friendly, and efficient platform for booking spa services, with features like user registration, room booking, and account management rigorously tested and validated. The system provides several benefits, including improved security through OTP verification, a user-friendly interface, streamlined booking operations, scalability for future growth, and enhanced data management. These functionalities collectively improve the overall user experience and operational efficiency while ensuring accurate and up-to-date customer and booking records. Nevertheless, the system has some drawbacks. The initial implementation cost may be a financial hurdle, and its reliance on stable internet connectivity could be a limitation in regions with unreliable access. Furthermore, users familiar with traditional methods may need time and

training to adapt to the new system. Future enhancements could include developing a mobile application to increase accessibility, integrating more payment options through additional gateways, and utilizing advanced data analytics to provide valuable insights into customer preferences, booking patterns, and operational performance.

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 interests regarding the publication of the paper.

Author Contribution

The authors confirm contribution to the paper as follows: ***study conception and design:*** *A. A. M. Alghail, S.K. Ahmad Khalid;* ***data collection:*** *A. A. M. Alghail, S.K. Ahmad Khalid;* ***analysis and interpretation of results:*** *A. A. M. Alghail, S.K. Ahmad Khalid;* ***draft manuscript preparation:*** *A. A. M. Alghail, S.K. Ahmad Khalid. All authors reviewed the results and approved the final version of the manuscript.*

References

[1] "What Is an Online Booking System? (Reservation System Definition)." Accessed: Jun. 12, 2024. [Online]. Available: https://wpamelia.com/online-booking-system/

[2] M. H. Barkadehi, M. Nilashi, O. Ibrahim, A. Zakeri Fardi, and S. Samad, "Authentication systems: A literature review and classification," Telematics and Informatics, vol. 35, no. 5, pp. 1491–1511, Aug. 2018, doi: 10.1016/J.TELE.2018.03.018.

[3] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: A survey," Cryptography, vol. 2, no. 1, pp. 1–31, Mar. 2018, doi: 10.3390/CRYPTOGRAPHY2010001.

[4] S. Istyaq and L. Agrawal, "A New Technique For User Authentication Using Numeric One Time Password Scheme," International Journal of Computer Sciences and Engineering, 2016. Accessed: May 23, 2024. [Online]. Available: https://www.researchgate.net/publication/303739017

[5] E. Erdem and M. T. Sandikkaya, "OTPaaS-One time password as a service," IEEE Transactions on Information Forensics and Security, vol. 14, no. 3, pp. 743–756, Mar. 2018, doi: 10.1109/TIFS.2018.2866025.

[6] M. Busch, N. Koch, and S. Suppan, "Modeling Security Features of Web Applications," Lecture Notes in Computer Science, vol. 8431, pp. 119–139, 2014, doi: 10.1007/978-3-319-07452-8_5.

[7] S. Ş. A. Cem, R. Lychev, and N. Wagner, "General Framework for Evaluating Password Complexity and Strength," Dec. 2015. Accessed: Jun. 12, 2024. [Online]. Available: https://arxiv.org/abs/1512.05814v1

[8] P. Sriramya and R. A. Karthika, "Providing Password Security by Salted Password Hashing Using Bcrypt Algorithm," ARPN Journal of Engineering and Applied Sciences, vol. 10, no. 13, 2015. Accessed: Jan. 02, 2025. [Online]. Available: http://www.arpnjournals.com

[9] B. L. T. Thai and H. Tanaka, "A Statistical Markov-Based Password Strength Meter," Internet of Things, vol. 25, p. 101057, Apr. 2024, doi: 10.1016/J.IOT.2023.101057.

[10] X. He and Q. Wang, "Dynamic Timeout-Based Session Identification Algorithm," 2011 International Conference on Electric Information and Control Engineering, pp. 346–349, 2011, doi: 10.1109/ICEICE.2011.5777587.

[11] Sharma, A., & Saini, H. (2022). "Secure User Authentication Using Enhanced OTP and Email Verification." *International Journal of Computer Applications*, 184(40), 8–12. doi:10.5120/ijca2022912294

[12] Ahmed, M., & Noor, M. (2023). "Comparative Analysis of Online Booking Systems for the Hospitality Sector." *Journal of Web Engineering and Technology*, 21(3), 195–210.

[13] Beck, K., Beedle, M., van Bennekum, A., et al. "Manifesto for Agile Software Development." Agile Alliance, 2021. [Online]. Available: https://agilemanifesto.org/

[14] S. Al-Saqqa, S. Sawalha, and H. Abdelnabi, "Agile Software Development: Methodologies and Trends," *International Journal of Interactive Mobile Technologies*, vol. 14, no. 11, pp. 246–270, 2020, doi: 10.3991/IJIM.V14I11.13269.

[15] "Agile Methodology | by Chathmini Jayathilaka | Medium." Accessed: May 28, 2024. [Online]. Available: https://medium.com/@chathmini96/agile-methodology-30ec4cdf3fc