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

AITCS

Vol. 5 No. 2 (2024) 193-211
https://publisher.uthm.edu.my/periodicals/index.php/aitcs

SecureClean Pro: A Vehicle Detailing Service Booking System Using Enhanced One-Time Password (OTP-X) for Azim AIC Sdn. Bhd.

Sathiaseelan Thiru Kumar[1], Nur Ziadah Harun[1]*

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

*Corresponding Author: nurziadah@uthm.edu.my
DOI: https://doi.org/10.30880/aitcs.2024.05.02.011

Article Info

Received: 11 August 2024
Accepted: 16 October 2024
Available online: 15 December 2024

Keywords

Vehicle Detailing, Booking, Multifactor Authentication, Agile, Optical Character Recognition(OCR)

Abstract

SecureClean Pro is a system that encompasses AZIM AIC SDN BHD's vehicle detailing services booking process management integrated with multifactor authentication. Drawbacks in the existing booking system of the company such as task assignment delays, miscommunications, and inadequate security measures, risking client data confidentiality, integrity and weak authentication. To resolve the deficiencies, the system incorporates Optical Character Recognition (OCR) to ease customer data inputting and verification method, enhanced One-Time Password (OTP-X), and authentication approval link to implement robust multifactor authentication as an extra layer of authentication. Adopting Agile methodology as development methodology and using Laravel framework, this web-based system caters the role of administrator, staff, and customers respectively for managing, get assigned and making the booking. Thus, SecureClean Pro can perform robust user authentication, and improve daily booking operations for the company, making it an essential solution for the underlined problems and business growth.

1. Introduction

In a technologically advanced society, the requirement for effective and streamlined booking management systems is critical. AZIM AIC SDN BHD, a well-known company in the vehicle cleaning service market, understands the need to use cutting edge technologies to improve operational efficiency. As a result, the creation of SecureClean Pro is an essential step in revolutionizing the company's service management process. AZIM AIC SDN BHD's dependence on a manual system has resulted in several operational challenges. Job assignment delays, customer preference misunderstandings, and challenges monitoring cleaning team actions have all become frequent concerns. Furthermore, the lack of a strong authentication method has left critical data vulnerable to illegal access.

SecureClean Pro is set to change AZIM AIC SDN BHD's vehicle cleaning service booking management procedure. This unique solution incorporates cutting-edge OCR technology, allowing for smooth document digitalization and quick data entry [1]. Furthermore, the use of upgraded OTP and push approval authentication guarantees that only authorized workers have access to essential information and more importantly authenticates the user's identification every single time [2] to implement security as the core of this system.

Current system at AZIM AIC SDN BHD has three key flaws based on an interview session with the company's manager. Firstly, the communication and coordination process are inefficient, resulting in delays and miscommunications when allocating duties and communicating client preferences to cleaning workers and

supervisors at their places. Second, the lack of a centralized platform makes it difficult to monitor and account for cleaning team actions in real time. Thirdly, the present system lacks strong authentication measures, exposing sensitive client information to unauthorized access.

The main objective of the system is to design a vehicle cleaning service booking management system with authentication mechanisms, to develop a vehicle cleaning service booking system by integrating OCR technology, enhanced OTP, and push approval authentication mechanisms and to test the functionality of the proposed system through security testing and user acceptance test based on OWASP security guidelines.

The main three key users that have dedicated modules in the system are the administrator, staff and customer. Each user has their respective roles and functions through the system and particularly the administrator contains functions of booking management module, staff comprises functions of task and payment proof updating module while customers have main functionality of booking module. Through these modules and functionalities, prioritizing security mechanisms, SecureClean Pro is intended to be a complete and secure booking system for AZIM AIC SDN BHD to meet their business needs effectively.

In this documentation, Section 2 discusses the literature review of the system including competitive analysis of existing systems, Section 3 contains explanations on the methodology used to build the system while Section 4 describes the system analysis and design whereas Section 5 comprises the overall conclusion about this project respectively.

2. Literature Review

This section will delve into the literature review conducted concerning both the existing web system and the current system utilized by AZIM AIC SDN BHD.

2.1 Introduction to Vehicle Detailing Booking System

As for AZIM AIC Sdn. Bhd, their nature of business is mainly to provide their detailing services for vehicles such as buses, car, lorry and motorcycle. Generally, detailing a vehicle involves various precise steps and procedures to achieve a clean and sparkling outcome. Booking, is described as the action of arranging for accommodations such as hotels or tickets at a specific future time, or the procedure involved in making such arrangements. Vehicle detailing booking system is a proposed one-system-solution for all the flaws the company currently facing as it will be a complete module to support the booking process of detailing services using web-integrated system which incorporates security as the core value which obviously the traditional or current method lacks or failed to practice. Prioritizing security as the core value, the system is set to be a complete detailing service booking medium with strong implementation of authentication measures to authenticate the users with other necessary security elements while not forgetting the optical character recognition (OCR) technology as an added feature.

2.2 Authentication

The process of identifying a user's identity is called authentication. It is the process of linking a set of identifying credentials to an incoming request. The credentials are compared to those stored in an authentication server or on a local operating system file in a database containing the details of authorized users [3]. Credentials can be classified into three factors namely knowledge factors, possession factors and inherence factors [4]. There are a few types of main authentication methods, but Single-factor authentication and Multifactor-authentication are chosen to be discussed in the following subtopics as related to the project's system.

2.2.1 Single -factor Authentication

By using Single-factor authentication (SFA) or also known as One-factor authentication (1FA), an individual may authenticate themselves by matching just one credential. The most common and popular instance of this would be a credential attached to a username or can be identified as password-based authentication. SFA has reduced protection levels. SFA authenticates with just one factor. An attacker may break into the system if they are able to defeat this one constraint as it highly vulnerable authentication [5].

2.2.2 Multifactor Authentication (MFA)

Users must authenticate multiple pieces of verifiable information when using multi-factor authentication (MFA). MFA was created to protect sensitive data with extra security levels and multiple authentication factors are involved. Because several credentials consist of distinct authentication factors that are needed to sign in, it is called multifactor authentication.

2.2.2.1 Dual Factor Authentication (2FA)

Dual-factor authentication, also known as two-factor authentication(2FA) is an evolved next level authentication method from single-factor authentication (SFA). 2FA which is also a type of MFA where all 2FA's are MFAs but not all MFA is a 2FA. 2FA as the name suggests, needs exactly two types of authentication factors to be verified and authenticated by a system. 2FA requires exactly two authentication factors credential while for a MFA mechanism the minimum number of authentication requirement is two. Making system compromises harder is the goal of multifactor authentication (MFA). If a hacker attempts to log in to a system or application with the credentials they know, they will be required to meet additional requirements before they can access the system or application [6].

The proposed system as mentioned earlier incorporates the implementation of 2FA and 3FA on respective modules and parts of the system. It has been planned to have 3FA implementation at the system signing-up module by customer and followed by 2FA each time the users attempt to access or login in the web-based system. The 3FA during the sign-up process includes 3 credentials namely the password, enhanced one-time password and push-notifications approval authentication while the recurring login process will require 2FA consists of password and push-notifications approval authentication. For administrators and staff, the login process is based on 2FA model.

2.2.2.2 Enhanced One-Time Password (OTP-X)

The proposed enhanced one-time password (OTP-X) is a derived and enhanced version of the existing one-time password (OTP) authentication. OTP is categorized under the authentication factor of something you have. An OTP, which stands for one-time password, is like a password but can only be used once. The enhanced one-time password (OTP-X) is meant to have a unique and robust implementation mechanism compared to currently existing OTP methods to provide additional security and resilience for the authentication enforcement in the proposed system. The first uniqueness and enhancement the OTP-X will possess is that it will consist of a combination of alphanumeric and symbols with a length of fixed ten characters. Another key enhancement in OTP-X is that 10 random characters of OTP-X consist of the last four-digit numbers of identity card number of user placed randomly in between the generated OTP. Users will receive the OTP-X through the registered email. This OTP-X is needed every time a user signs up and logs in into the system and authenticated together with password.

2.2.2.3 Authentication approval link

By forcing the user to take direct action to verify their identity or grant access, authentication approval link adds another degree of protection during the first-time login process of the new customer. Authentication approval link, the requirement for the user to actively participate in verifying the login helps prevent unauthorized access even if a password is stolen. This technique is often applied to a variety of authentication systems, especially those that employ web-based interfaces, push notifications, or mobile applications to verify users. Using a reliable gadget or application, the user must click on a button or link to verify their identity or approve a login attempt or transaction [7]. The mechanism of push notification or click approval is simple where a user's login is authenticated when the user enters his or her credentials. A security link or notification is sent to their registered email address which requires the user to confirm the login and verify whether he or she is the one attempting the login [8], [9]. The vehicle detailing booking system is implemented with this extra layer of authentication during the first-time login as a strong identification and reflection of the system's security.

2.3 Optical Character Recognition (OCR)

OCR systems transform physical, printed documents into machine-readable text by combining hardware and software. Text is copied or read by hardware, such as an optical scanner or dedicated circuit board; software then usually does the more complex processing. The four main steps of OCR are image acquisition, preprocessing, text-recognition using pattern matching and feature extraction, and finally postprocessing [10].
In the proposed system OCR is incorporated to validate the user's address details as the system deals with door-to-door booking services. By uploading images of driving license, it is verified as a valid address in the first place and helps the system to read and interpret the information automatically into the details and particulars of user's address.

2.4 Secure Web Application System Features

To establish trust with users, safeguard sensitive information, and ensure the reliability and accessibility of web-based services, it is essential to implement a wide range of robust security measures and protocols [11]. There are several key security features that will be implemented in the system to achieve the necessary security

standards for the goodness of users and the business as security is a not a desire but a need. The security features which are mainly integrated in the built system are based on the Open Worldwide Application Security Project (OWASP) web security testing guidelines as the implemented security features are explained accordingly [12].

2.4.1 Input Validation

Data validation is the procedure of examining and verifying user-entered data using online forms or other input methods to assure its integrity, dependability, and security prior to processing it within an application or system. The importance of input validation rests in its capacity to reduce vulnerabilities that result from user inputs, which attackers frequently exploit to undermine system security. Syntactic validation is responsible for ensuring the accurate syntax of structured fields, such as social security numbers, dates, and currency symbols. Semantic validation is responsible for ensuring the accuracy of data within the given business context [13].

2.4.2 Strong Password Policy

For password management, strong password policy guidelines are followed in the password setting up process and input and output of the password are displayed according to OWASP security guidelines. It needs to be implemented for passwords to have a substantial length, with a minimum suggested size of 12 characters, preferably exceeding this limit. Furthermore, it is advisable to promote complexity by including a combination of capital and lowercase letters, numbers, and special characters, without imposing any restrictions on the specific kind of characters used. Refrain from using passwords that are often used or easily predictable, such as words found in dictionaries, phrases, or patterns that follow a sequence [14].

2.4.3 Secure Session Management

Session management protects user sessions with session IDs, session handling, and session termination, among other things, to keep user activities safe and private. Strong session management depends on following OWASP guidelines and safe code practices. The session ID, a one-of-a-kind number that the server creates when login is successful, lets the user keep interacting without having to log in again and again. Input validation and sanitization are examples of secure session handling practices that help protect against session-related attacks. Using session timeouts and server-side logout tools will make sure that user sessions end properly.

2.4.4 Role-based User Definitions

Role-based user definition is an extensively acknowledged access control paradigm that establishes access privileges based on the specific positions that individuals occupy within an organization. Users are allocated specific roles, such as "admin," "staff," or "customer," which come with predetermined rights or privileges that correspond to their respective tasks. By categorizing users based on their job activities and access requirements, this method streamlines access management, bolstering security and reducing the likelihood of unauthorized access or privilege escalation [15].

2.4.5 Hashing Password in Database

Hashing passwords in a database involves turning plain-text passwords into irreversible, hashed versions prior to storage. One recommended security measure, supported by OWASP and secure coding principles, is to utilize cryptographic hash functions such as bcrypt, for the purpose of generating distinct hash values of a consistent length from user passwords.

2.4.6 Error Handling

When an authentication error occurs, the OWASP guidelines and secure coding principles is crucial to provide generic error messages that do not divulge specific information about which part of the authentication process failed. Employing this approach in error handling enhances security by reducing the risk of exposing critical information that could aid attackers in their attempts to gain unauthorized access to user accounts [16][17].

2.4.7 Account Lockout Mechanism

An account lockout mechanism is a security measure used in computer systems to prevent unauthorized access attempts. The system operates by temporarily deactivating an account following a predetermined number of consecutive unsuccessful login attempts within a specific time, thereby reducing the vulnerability to brute force attacks. Organizations can customize the method to align with their security rules by adjusting parameters such as the threshold for unsuccessful attempts, duration of the lockout period, and reset conditions for the failed

attempt counter [18]. SecureClean Pro is implemented with 2 minutes of account lockout after five failed attempts to login.

2.6 Study of Existing Related Systems

This section contains the analysis of similar web-based systems to a car detailing booking system.

2.6.1 Carwash2u

This web-based system acts as a business site to provide information about their services on car detailing services they provide with number of buttons to book their services throughout the website. The system has 4 main pages which are home, services, price, and contact. The security features or practices on this website are not more than a Hypertext Transfer Protocol Secure (HTTPS) which uses Transport Layer security (TLS) or Secure Sockets Layer (SSL). Other than that, the system lacks login and sign-up modules with no authentication required as the main booking process just through WhatsApp [19].

2.6.2 Carboxad

The web-based system is for Carbox Auto Detailing Sdn. Bhd. The system mainly functions as a platform for customers to make early bookings for the desired service by the company. The website contains simple pages such as 'About Us', 'Reviews', and 'Map' to provide basic information about their business to the users and booking pages for collecting booking by customers. This booking module page contains detailed information about the services offered, a page to choose booking date and time, followed by a summary page of booking details. Although the system contains a login and sign-up module, the implementation of security is very low by using SFA which only requires email and password without any other authentication measures. The website also uses a HTTPS protocol, input validation with error handling when inputting login credentials and registration details and login using third party platforms such as Facebook and Google, but there no other clear security implementation included such as session management [20].

2.4.2 Atomdetailing

This multi-functional website comprises various modules and security is not their core value as the website contains very little safety features and practices, especially on modules that involve user engagement. The website has a booking module that enables users to lock their desired time by providing details such as name, contact number, email and details and saved to Google Calendar if chosen by the user. In terms of security, the login and sign-up modules do not have any dual authentication compared to a SFA which comprises email and password only. This website uses HTTPS protocol and input validation with error handling when inputting user details and login credentials but no session management, and strong password policy measure implementation that can be observed. As an additional feature this website allows third party login using platforms such as Google and Facebook [21].

2.7 Comparison with the Existing Systems

This part comprises the summary of the comparison between the existing car detailing booking system with the proposed system. Table 1 shows the carwash2u system lacks most security features and basic features while Carboxad and Atomdetailing website has basic booking features but lack security features. All three websites have implemented feedback displaying and providing features, but the implementation of security features is almost to none on these websites. Thus, the proposed system is planned to have all the features that a booking system should comprise together with necessary security characteristics based on OWASP guidelines.

Table 1 *Comparison of existing system with the proposed system*

Features/System	Carwash2u	Carboxad	Atomdetailing	SecureClean Pro
Login & Sign-up	X	/	/	/
Booking module	X	/	/	/
Notifications	X	X	X	/
Activity Dashboard	X	/	/	/
Job assigning	X	X	X	/
Schedule calendar	X	/	/	/
Job Progress	X	X	X	/
User role definitions	X	X	X	/
Dual authentication	X	X	X	/
Strong password	X	X	X	/

Table 1 *Comparison of existing system with the proposed system (cont.)*

Features/System	Carwash2u	Carboxad	Atomdetailing	SecureClean Pro
Feedback	/	/	/	/
Session termination	X	X	X	/
Error handling	X	X	X	/
OCR	X	X	X	/

3. Methodology

This chapter provides an explanation of the actions that were carried out in each phase of the project, as well as the utilization of the Agile methodology used in system development.

3.1 Agile Model

Agile Methodology has been chosen as the system development approach for SecureClean Pro. Agile places great emphasis on the ongoing testing and development that occurs across the whole software development lifecycle. It entails the simultaneous development and testing of software, facilitating the seamless conversion of business requirements into software solutions [22]. Agile Development has numerous benefits in comparison to alternative technique models. Agile methodology consists of six main iterative phases namely in the development cycle of the project, namely plan, design, develop, test, deployment, and review phases. Figure 1 shows an illustration of the agile methodology used for SecureClean Pro and Table 2 shows system development workflow using the six phases of Agile methodology.

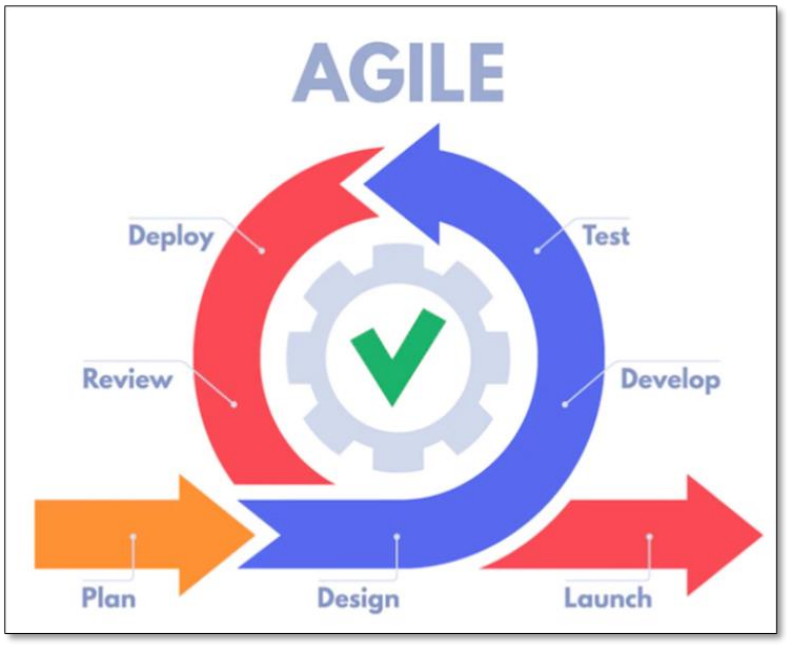

Fig. 1 *Illustration of agile methodology phases [23]*

To address the flaws in AZIM AIC SDN BHD's current system, Agile methodology will guide the development of SecureClean Pro. In the Planning phase, Agile will help pinpoint issues like inefficient communication, lack of real-time monitoring, and weak authentication, while gathering detailed requirements from stakeholders. The Design phase will use Agile's iterative approach to create and refine wireframes and diagrams, integrating real-time messaging, a centralized dashboard, and advanced authentication methods like OCR and enhanced OTP.

The Development phase will see these designs implemented, with continuous integration and feedback loops to ensure the system meets requirements. During the Testing phase, Agile's iterative testing will identify and resolve security and functionality issues, guided by OWASP standards [12]. The Deployment phase will focus on smooth rollout and user training, with Agile facilitating adjustments as needed. Finally, the Review phase will gather user feedback and monitor system performance, allowing for ongoing improvements and ensuring the system effectively addresses the identified flaws. Agile's iterative and adaptive nature ensures that each phase builds on feedback and continuous improvements to overcome the system's weaknesses effectively.

Table 2 *Software development activities and their task*

Phase	Task	Output
Planning	• Find issues with current manual system in AZIM AIC SDN BHD. • Acquiring comprehensive descriptions of issues • Actively engaging stakeholders such as manager, admin, and staff in order to collect requirements. • Outlining the objectives and requirements of the project making a comprehensive proposal for a project	• Project proposal • Develop Gantt chart • Project background • Problem statement • Objectives • Scopes
Design	• Creating design diagrams using Lucid chart and diagrams.net • Creating design wireframes and interfaces using Figma • Designing databases and specifying data organization using context diagrams.	• Use context diagrams, data flow diagrams, entity relationship diagram • Design wireframes illustrating UI components and navigation. • Database design
Development	• Creating databases and interfaces according to design specs using phpMyAdmin and MySQL • Coding and programming to create functional system using HTML, CSS, JavaScript, and PHP • Utilizing IDE Microsoft Visual Studio Code	• Developed Interfaces of the proposed system • Developed Databases of the proposed system Class Diagram • Fully functional system prototype • System components aligned with specified requirements.
Testing	• Implementing security measures • User testing for usability • System functionality test	• Security features • User-tested system • Problems that need repair and solution • Possible vulnerabilities and weaknesses • Security patch and functionality updates
Deployment	• Packaging system components • Providing documentation for installation procedures • Collaborating with system administrators • Supplying instructional materials or user guides	• Packaged system components • Installation documentation • Collaboration with admin and staff • User reference and guidelines
Review	• Extensive system testing • System performance evaluation • Collecting user and stakeholder feedback • Utilizing audit, survey, and monitoring tools	• Evaluated system performance. • User and stakeholder feedback • Insights for system improvement

4. Analysis and Design

This section provides a comprehensive study of the analysis and design elements of SecureClean Pro.

4.1 System Requirement analysis

System Requirement Analysis is a crucial stage in web development and system design which involves a thorough process of discovering, documenting, and specifying the different requirements, limitations, and functions necessary for building a system. This step includes identifying both the functional requirements (what the system needs to do) and the non-functional requirements (such as performance, security, and usability standards) that need to be met and not forgetting the user requirements (what the user needs to do to complete a needed job or task).

4.2 Data Flow Diagram

Data flow diagrams, or DFDs, are illustrations that show how data moves through a system. They are made up of distinct layers that aid in comprehending the functionalities of the system at various abstraction levels. These diagrams are classified into several levels: Context Diagram, Level 0, Level 1, and perhaps more complex levels.

4.2.1 Context Diagram

With the major three entities that are the users of the system, namely the administrator or admin, staff, and the customer, the context diagram that can be found in Figure 2 displays the entire data intake and outflow of the system.

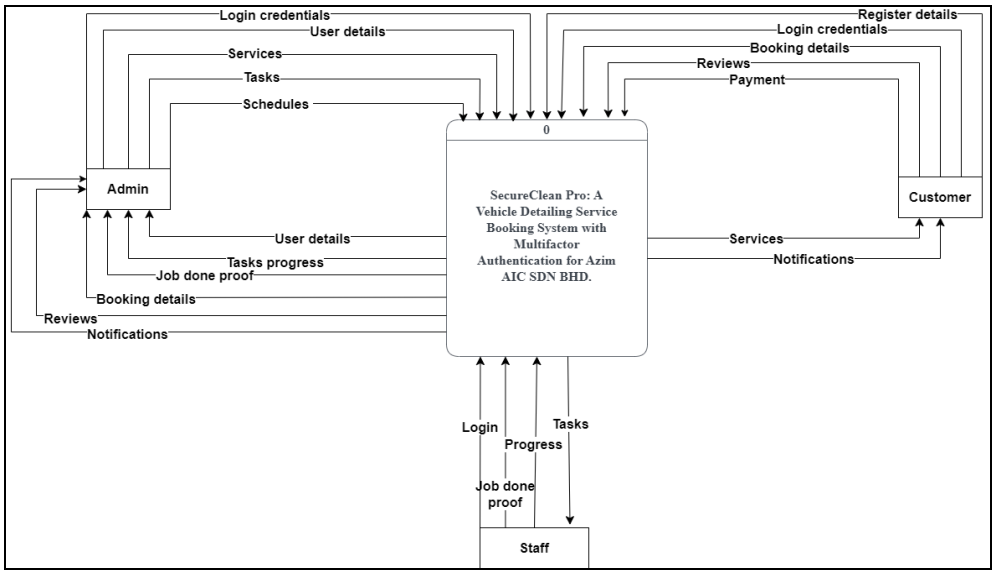

Fig. 2 *Context diagram of SecureClean Pro*

4.2.3 Data Flow Diagram Level 0

Adapted and expanded from context diagram in Figure 2, Figure 3 is a Level 0 DFD of the SecureClean Pro which outlines the main processes of the system with data stores and functionalities of the system with appropriate DFD elements added to represent the data flow more clearly and concisely. The identified main 5 processes of the system based on Figure 3 are the register, login, booking, booking management and task and proof update.

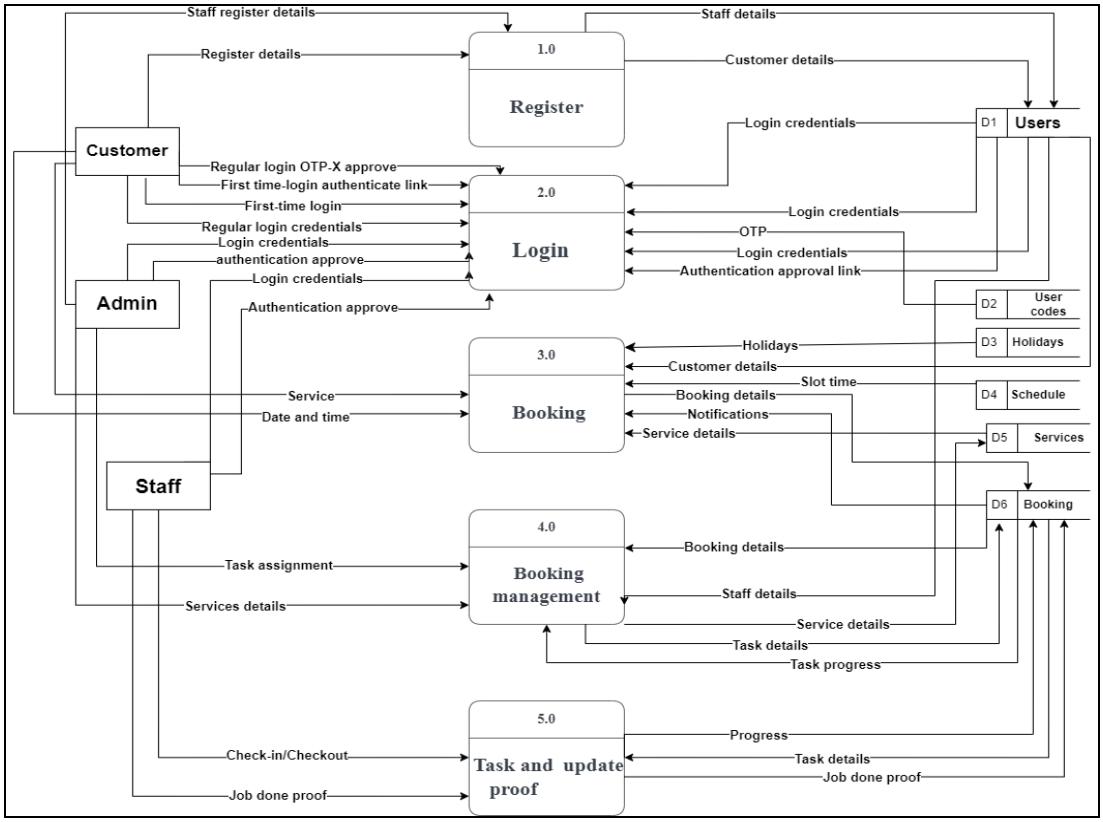

Fig. 3 *Data Flow Diagram Level 0*

Applied Information Technology and Computer Science Vol. 5 No. 2 (2024) p. 193-211

4.2.4 System Flowchart

Flowchart is an overall representation of the system in compact and concise illustration model on how the system begins and goes through the important processes to reach the system functions until the system process ends, and it can be considered as a general chart that shows the data flow representation as the name itself suggests. Figure 4 shows the system flowchart of SecureClean Pro.

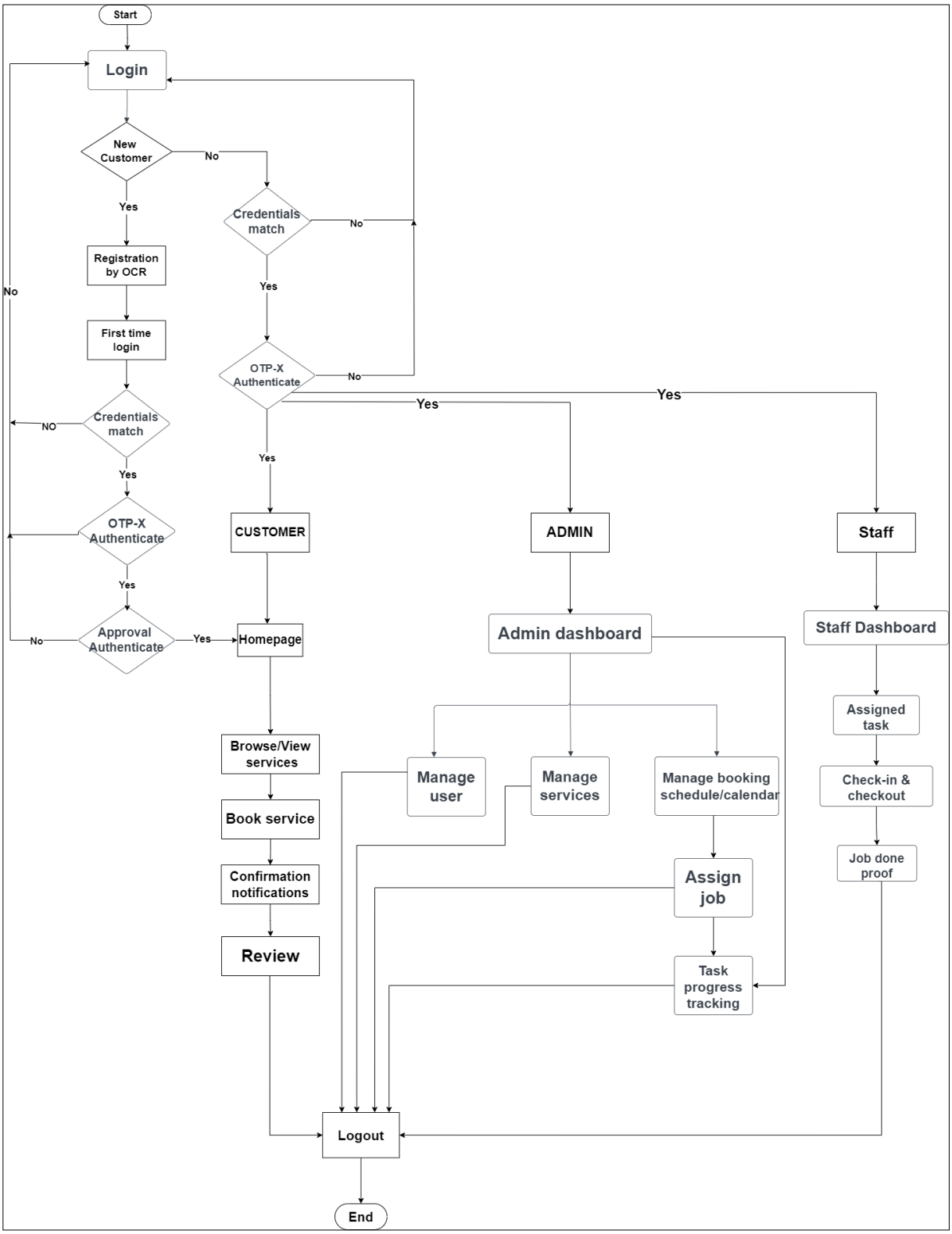

Fig. 4 *System flowchart*

4.3 System Architecture

Azim AIC SDN BHD's automobile detailing services booking, SecureClean Pro's distributed and modular architecture guarantees scalability, dependability, and security. The architecture as in Figure 5 is based on a client-server framework, with a central database connecting the admin, staff, and customer modules. Each module may operate autonomously within the system and communicate with each other through well-defined system architecture because it is created utilizing the modules of the architecture.

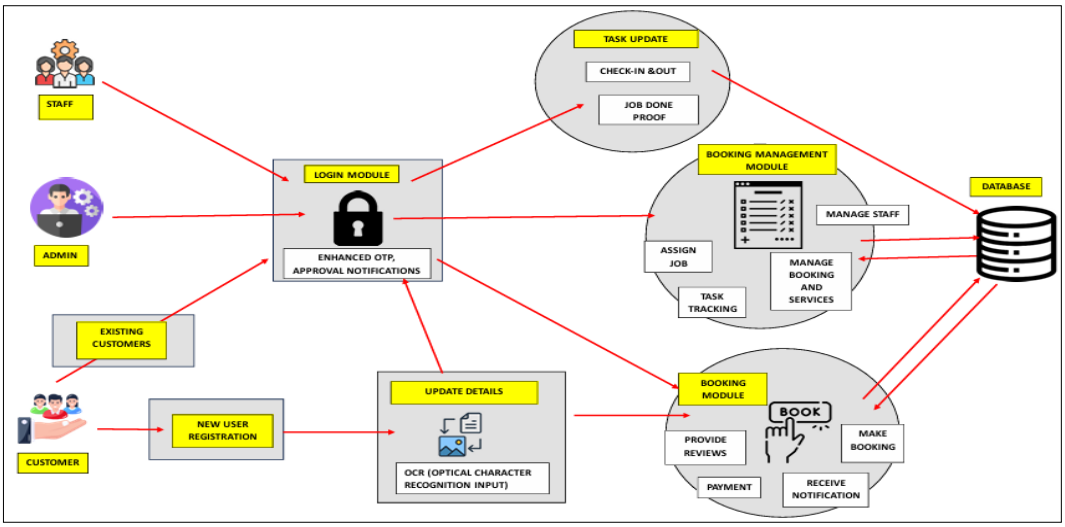

Fig. 5 *System architecture of SecureClean Pro*

4.4 Entity Relationship Diagram

Figure 6 illustrates the entity relationship diagram to establish the architecture of SecureClean Pro.

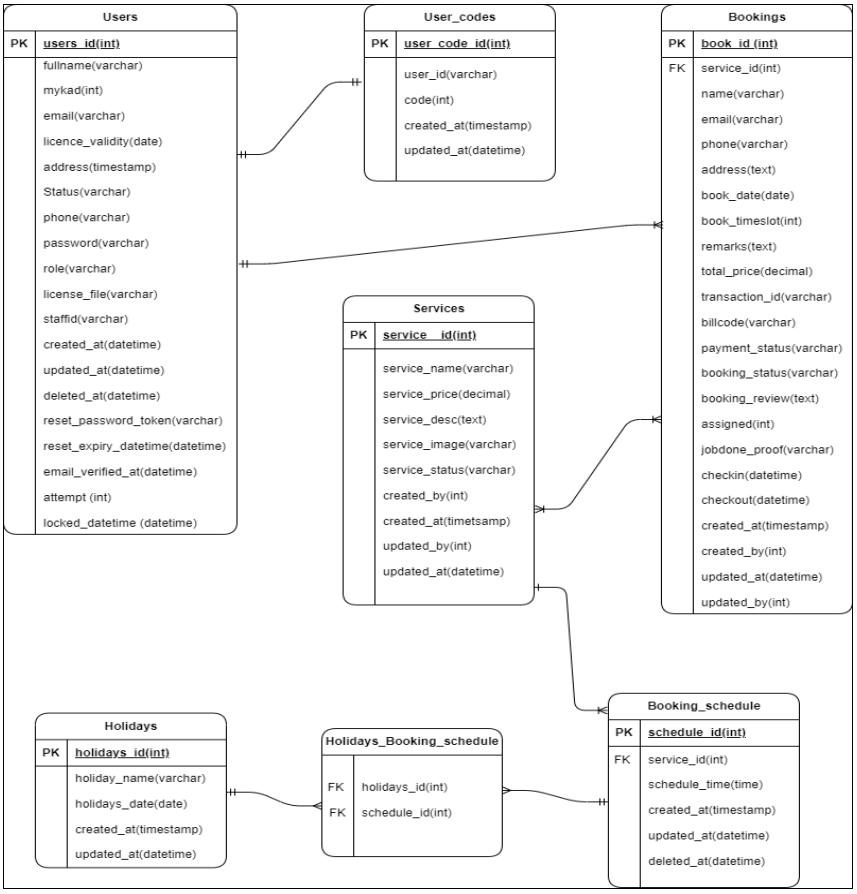

Fig. 6 *Entity relationship diagram*

Applied Information Technology and Computer Science Vol. 5 No. 2 (2024) p. 193-211

4.5 User Interface Design

This part consists of user interface design for the three modules of user, who are the administrator, staff, and the customer of SecureClean Pro. Figure 7(a) shows the login page for all three users name administrator, staff, and customer and followed by Figure 7(b) that shows the booking page and Figure 8(a) and 8(b) that shows the respective dashboard interfaces of admin and staff.

Fig. 7(a) *Login interface design*

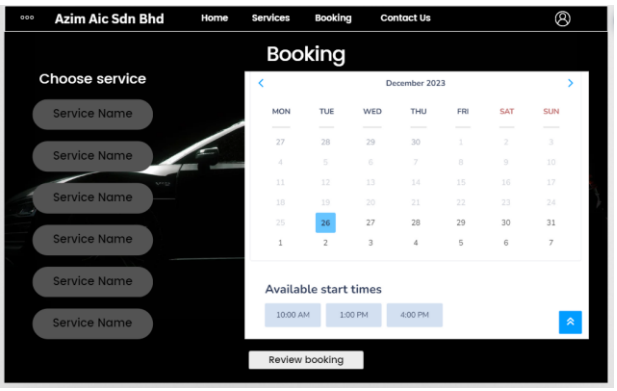

Fig. 7(b) *Booking interface design*

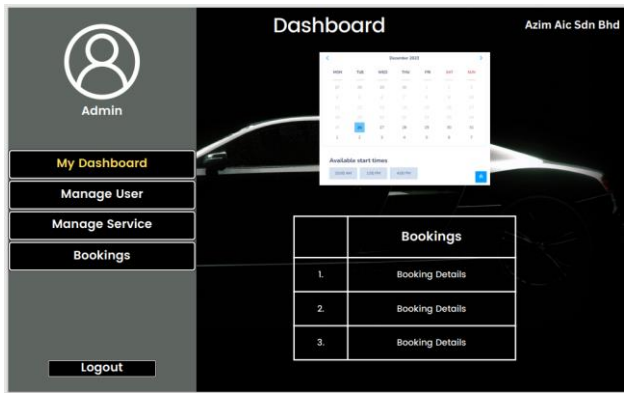

Fig. 8(a) *Admin dashboard Interface*

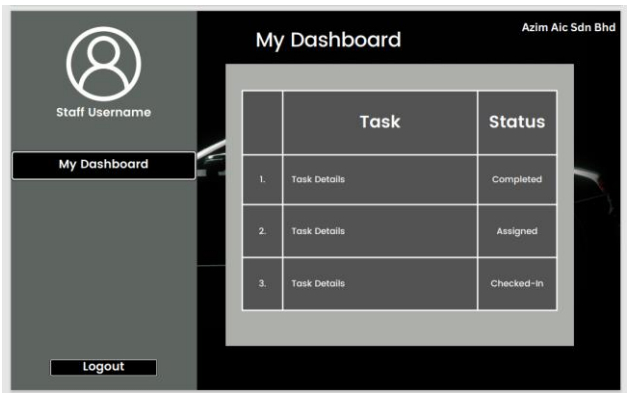

Fig. 8(b) *Staff dashboard Interface*

5. Implementation and Testing

A comprehensive rundown of SecureClean Pro's security features is presented in this section. It discusses the approaches used to protect the system from security attacks. Every security feature is explained in detail, including what it does, how it is put into place, and how it contributes to the system's overall security.

5.1 Enhanced One-Time Password (OTP-X)

This part of the code explains the implementation of the enhanced One-time password algorithm (OTP-X) which is used as the second factor authentication method each time a user is logged into the system after bypassing the first factor credential matching authentication (Figure 9 to Figure 12). This enhanced OTP contains a unique and robust mechanism where it generates a random 10 character but places the first 2 and last 2 digits of a user into it while the other characters are totally random including various symbols, numbers and characters making it very hard to be guessed or even conduct an attack. The code generated is set to expire in 2 minutes, and after expiration user is prompted to request resending the OTP.

```
public function build()
{
    return $this->subject('Vehicle Detailing Booking System 2FA Verification')
                ->view('emails.code');
}
```

Fig. 9 *Code to call generation of email to requester*

```php
public function generateCode()
{
    $characters = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()_+-=';

    $randomCode = substr(str_shuffle($characters), 0, 6);

    $mykad = auth()->user()->mykad;
    $mykadFirstPart = substr($mykad, 0, 2);
    $mykadLastPart = substr($mykad, -2);

    $firstPart = substr($randomCode, 0, 2);
    $middlePart = substr($randomCode, 2, 2);
    $lastPart = substr($randomCode, 4, 2);

    $code = $firstPart . $mykadFirstPart . $middlePart . $mykadLastPart . $lastPart;

    UserCode::updateOrCreate(
        ['user_id' => auth()->user()->id],
        ['code' => $code]
    );
```

Fig. 10 *Code snippet of enhanced OTP's algorithm a forming pattern*

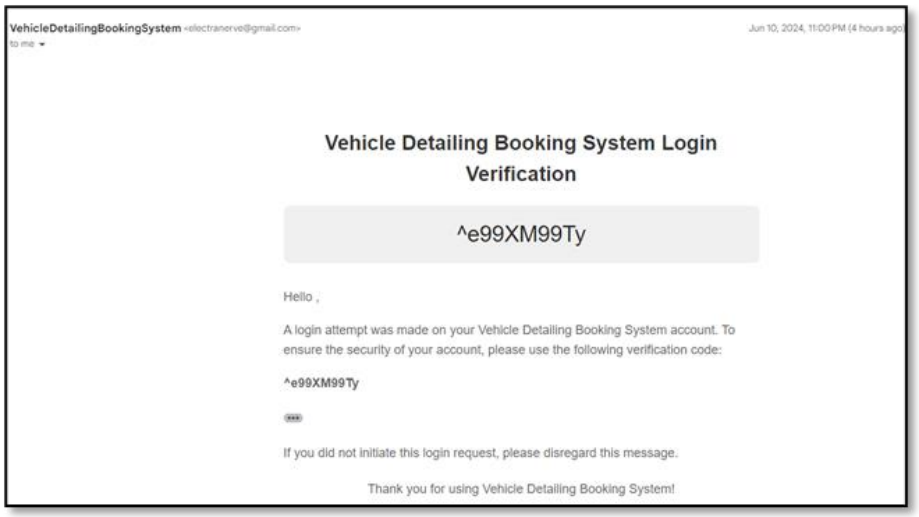

Fig. 11 *Email notification of OTP-X*

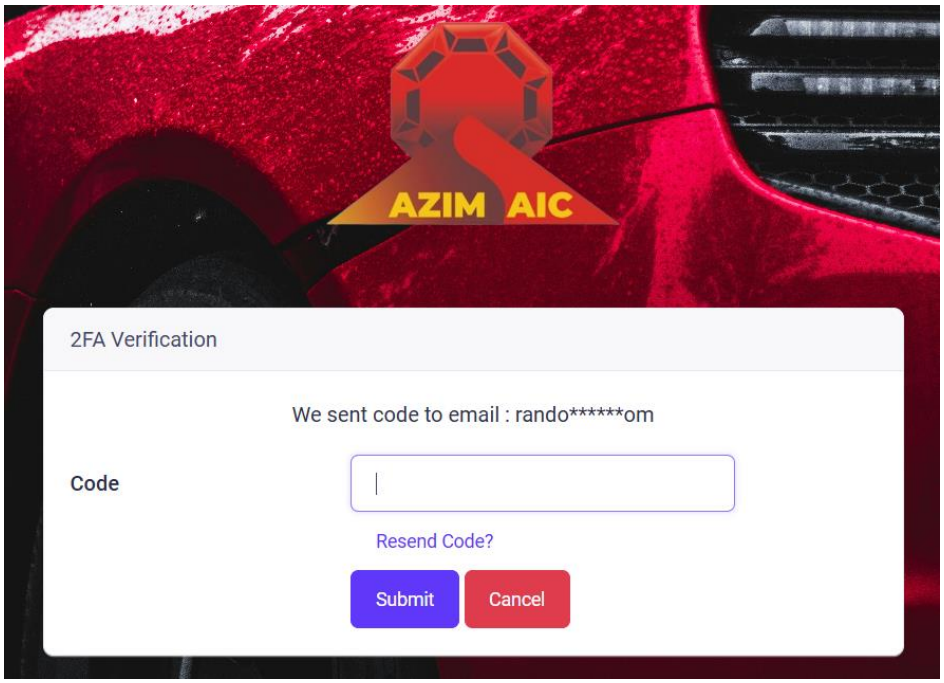

Fig. 12 *System requesting for OTP-X to bypass the second factor authentication layer*

Applied Information Technology and Computer Science Vol. 5 No. 2 (2024) p. 193-211

5.2 Approval Authentication Link

An essential component of SecureClean Pro's security architecture, the Approval Authentication Link adds a third degree of protection to the login process for newly registered users. Users are required to input their credentials at the beginning, and they are checked for accuracy. The second step involves sending a One-Time Password (OTP-X) to the user's registered email address to confirm their identity. Lastly, as the third layer, the user is required to click on an approval authentication link to finish the login procedure. By preventing attackers at the first login, this multi-step authentication process greatly improves system security and guarantees that only authorized users can access the system as in Figure 13 and Figure 14..

```php
use VerifiesEmails;

/**
 * Where to redirect users after verification.
 *
 * @var string
 */
protected $redirectTo = '/signoutcustom';

/**
 * Create a new controller instance.
 *
 * @return void
 */
public function __construct()
{
    $this->middleware('auth');
    $this->middleware('signed')->only('verify');
    $this->middleware('throttle:6,1')->only('verify', 'resend');
}
```

Fig. 13 *Function to generate verification email when customer login for first time*

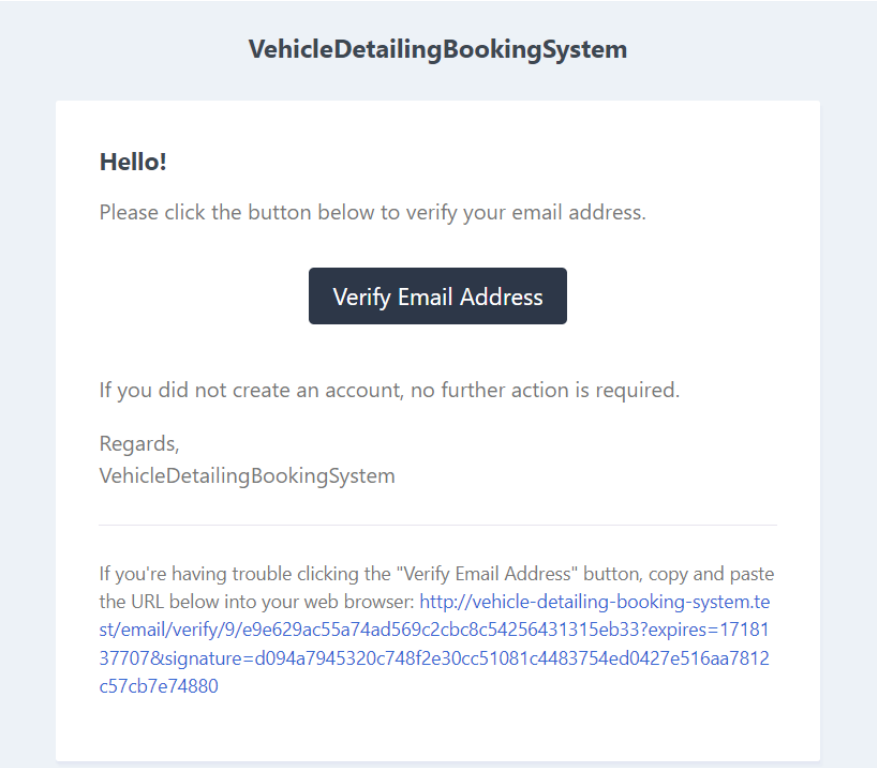

Fig. 14 *Sample of verification email that acts as third layer of authentication before logging in first-time after registration*

5.3 Strong Password Policy

One-way SecureClean Pro reduces these threats and improves its security by making users create strong passwords. This system has a minimum password requirement of 10 characters, which makes it difficult for attackers to compromise the baseline degree of complexity. There must be a minimum of one uppercase letter (A–Z), one lowercase letter (a–z), one number (0–9), and one special character (@$!%*#?&) included (Figure 15).

```
" name="password" id="password"  pattern="(?=.*\d)(?=.*[a-z])(?=.*[A-Z])(?=.*[@$!%*#?&]).{10,32}"
```

Figure 14: *Code Implementation of strong password pattern policy*

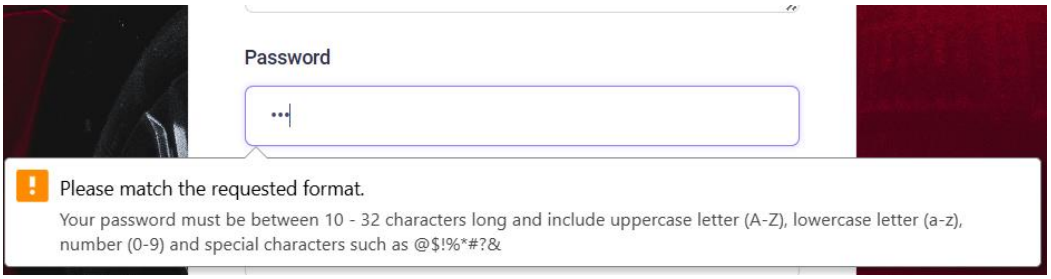

Fig. 15 *Strong password implementation on registration interface*

5.4 Identity Management Based on Role

User access and privileges are carefully managed and assigned based on their roles in SecureClean Pro's identity management system. Admin, Staff, and Customer are the three main user roles defined by the system as in Figure 16 and Figure 17. By limiting user access to exactly what is necessary for their job and using a role-based access control (RBAC) system, we can keep internal dangers at bay and keep things organised in terms of security.

```
if(auth()->user()->role == 'Admin'){

    return redirect()->route('homeadmin');

}
else if(auth()->user()->role == 'Customer'){

    return redirect()->route('homecustomer');

}
else if(auth()->user()->role == 'Staff'){

    return redirect()->route('homestaff');

}
}
```

Fig. 16 *Role definitions before logging in*

Applied Information Technology and Computer Science Vol. 5 No. 2 (2024) p. 193-211

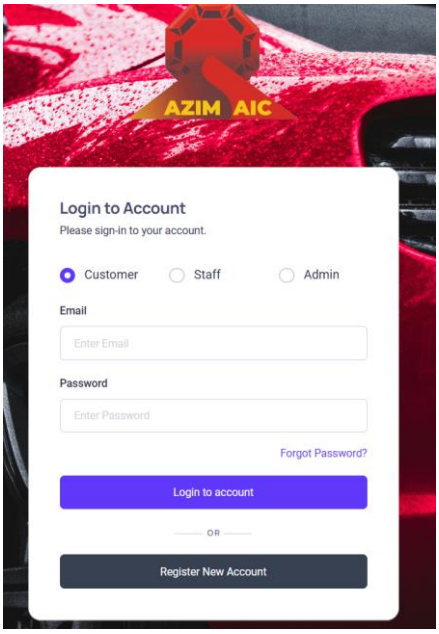

Fig. 17 *Role definitions must be chosen correctly to login.*

5.5 Session Management

The session management security solution in SecureClean Pro, as seen in the following code sample in Figure 18 from the `session.php` configuration file, is crucial for protecting user sessions from potential threats. The setup implements multiple essential security features. Firstly, enabling session data encryption (`'encrypt' => true`) safeguards sensitive information from unauthorized access. The session lifetime is set to a short duration of 15 minutes, as specified by the `'lifetime' => env ('SESSION_LIFETIME', 15) ` configuration. Additionally, the sessions are set to expire when the browser is closed, as indicated by the `'expire_on_close' => true` option. These measures effectively reduce the danger of session hijacking by minimizing the time frame in which attackers can exploit vulnerabilities.

session.php

```
return [
    'driver' => env('SESSION_DRIVER', 'file'),

    'lifetime' => env('SESSION_LIFETIME', 15),

    'expire_on_close' => true,

    'encrypt' => true,

    'files' => storage_path('framework/sessions'),


    'connection' => env('SESSION_CONNECTION'),

    'table' => 'sessions',

    'store' => env('SESSION_STORE'),

    'lottery' => [2, 100],

    'cookie' => env(
        'SESSION_COOKIE',
        Str::slug(env('APP_NAME', 'laravel'), '_').'_session'
    ),

    'path' => '/',

    'domain' => env('SESSION_DOMAIN'),

    'secure' => env('SESSION_SECURE_COOKIE'),

    'http_only' => true,
```

Fig. 18 *Session management implementation code*

5.6 Input Validation

SecureClean Pro utilizes a strong input validation system throughout all its modules, ensuring that input data is validated against the preset rules and formats. This encompasses validations for data type, length, format, and allowable characters. In addition, the system employs server-side validation to enhance client-side validation and ensure security, even in cases when client-side validation fails or is circumvented (Figure 19 and Figure 20).

```
if ($emailcheck > 0) {
    return redirect()->back()->with('errors', 'Email already exist');
} else if ($checkmykad > 0) {
    return redirect()->back()->with('errors', 'IC Number Already Exist!');
} else if ($password != $cpassword) {
    return redirect()->back()->with('errors', 'Password does not match with confirm password!');
```

Fig. 19 *Code snippet to check for valid or available data input that can be inserted into database*

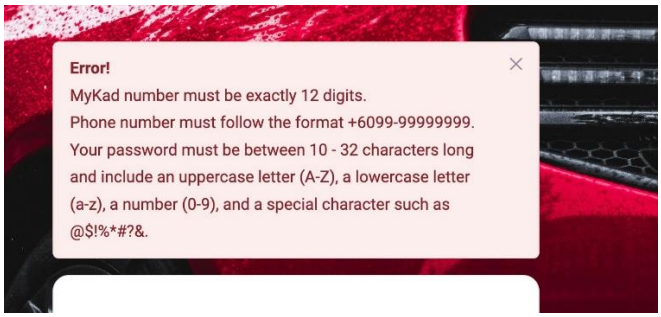

Fig. 20 *Input validation for all inputs during registration*

5.7 Hashing Password in Database

SecureClean Pro uses bcrypt hashing as in Figure 21 and Figure 22 to store user passwords in the database, which is a strong method for password protection. Because of its robust cryptographic features, the bcrypt method is well-known for securely hashing passwords into forms that are computationally impossible to decrypt. By default, the 'rounds' parameter in the given setup specifies 12 computational rounds for bcrypt hashing; however, this value is configurable via the BCRYPT_ROUNDS environment variable. Also, when you authenticate with SecureClean Pro, the'verify' parameter checks the password against its hashed version. This rigorous authentication procedure strengthens the security of user authentication by limiting system access to only authorised users who have supplied valid passwords.

```
'bcrypt' => [
    'rounds' => env('BCRYPT_ROUNDS', 12),
    'verify' => true,
],
```

Fig. 21 *bcrypt algorithm used to create irreversible hash to store password credentials in database*

password
$2y$12$eVdCMF8dNCjIsPrTQpIcTODsWhZ93ut...
$2y$12$IyiM592HaICRr8c10mkOV.cVTmVustjk...
$2y$12$eVdCMF8dNCjIsPrTQpIcTODsWhZ93ut...
$2y$12$Oe.HM82.7BeLMAidXzKt6eZKjGe51n4u...

Fig. 22 *Password stored in database after hashing*

5.8 Error Handling

An essential part of SecureClean Pro's security implementation is error handling, which makes sure that system failures and potential vulnerabilities are handled well to stop malicious actors from taking advantage of them. As a first step in troubleshooting and security risk identification, it employs comprehensive error and exception

recording to monitor and analyse system failures (Figure 23). By using appropriate error messages as in Figure 24 that do not reveal sensitive information, the system further aids in preventing information leakage and reduces the likelihood of attackers taking use of known flaws.

```
        return redirect("/")->withErrors('Whoops! You have entered invalid credentials or incorrect role selected');
    }
}

return redirect("/")->withErrors('Whoops! You have entered invalid credentials');
```

Fig. 23 *Implementation of safe error message*

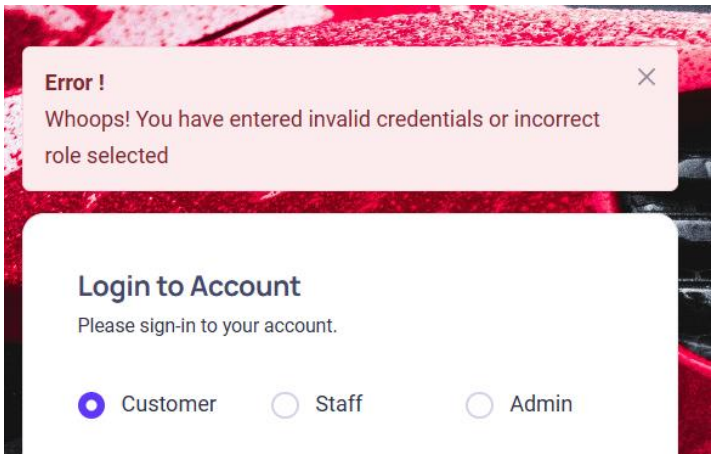

Fig. 24 *Safe error message when error attempt wrong credentials logging in*

5.8 Account Lockout Policy

When a user tries to log in, the system checks their credentials and role, then verifies if the account is locked by examining the 'locked_datetime'. If the account is locked and the lockout period is still active, the code calculates the remaining lockout time and constructs a user-friendly message indicating how long they must wait before trying again. The lockout period is set to 2 minutes and minimum failure attempt of 5 (Figure 25). To determine if an account is locked, the system checks the 'locked_datetime' after the user's credentials and role have been checked. If the lockout period is still active and the account is locked, the code will compute how much time is left until the lockout expires and display an easy-to-understand message letting the user know how long they have to wait before attempting again.

```
    $credentials = $request->only('email', 'password', 'role');

    if (Auth::attempt(['email' => $credentials['email'], 'password' => $credentials['password']])) {

        if (auth()->user()->role === $credentials['role']) {

            if (auth()->user()->locked_datetime != null && Carbon::parse(auth()->user()->locked_datetime)->isPast() == false)
                $lockedDateTime = Carbon::parse(auth()->user()->locked_datetime);

// Calculate the remaining time in minutes and seconds
$remainingMinutes = Carbon::now()->diffInMinutes($lockedDateTime);
$remainingSeconds = Carbon::now()->diffInSeconds($lockedDateTime);

// Extract whole minutes and remaining seconds
$minutes = floor($remainingMinutes);
$seconds = $remainingSeconds % 60;

// Construct the message
$message = "Whoops! Your Account has been temporarily disabled. ";
if ($minutes > 0) {
    $message .= "Please try again after $minutes minute";
    if ($minutes > 1) {
        $message .= "s"; // Pluralize "minute" if needed
    }
    if ($seconds > 0) {
        $message .= " and $seconds second";
        if ($seconds > 1) {
            $message .= "s"; // Pluralize "second" if needed
        }
```

Fig. 25 *Code for disabling account after calculating failure attempts and display error with duration before trying again*

5. Conclusion

The SecureClean Pro: A Vehicle Detailing Service Booking System Using Enhanced One-Time Password(OTP-X) for Azim AIC Sdn Bhd is completed, meeting the project's objectives and requirements. SecureClean Pro enhances productivity and user convenience through automation, improving task efficiency and accuracy. Its multi-layered security framework, integrating OCR technology, enhanced OTP, and authentication links, safeguards customer data effectively. Online booking and real-time notifications enhance customer experience, while resource management tools aid administrators in maintaining service quality and schedules. By eliminating manual operations, the system reduces costs and boosts productivity.

Although SecureClean Pro has many advantages, it does have a few limitations. Initial implementation costs may pose a barrier, particularly for the small organization. Some users may find advanced features challenging, requiring training and ongoing support. Maintenance and updates demand resources and attention, potentially posing ongoing challenges. However, the long-term benefits in productivity, security, and customer satisfaction outweigh these drawbacks.

Future enhancements could include AI-driven predictive analysis for streamlined operations and improved customer service. A mobile app could enhance user access and convenience, while sophisticated analytics could optimize service quality and resource allocation. Integration with related services could further enhance user experience and operational efficiency.

In conclusion, AZIM AIC SDN BHD now has a fully functional booking management system for its vehicle detailing services, thanks to the SecureClean Pro project. With the system's development complete, a major step has been taken towards improving operational efficiency, security, and customer happiness. Nevertheless, it is critical to recognize challenges linked to upfront expenses, technical intricacy, and continuous upkeep. In the future, the system's capabilities will be even better thanks to integration and upgrades, and the company's service standards will be even higher.

Acknowledgement

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

Conflict of Interest

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

References

[1] K. Karthick and S. Chitra, "Review of Optical Character Recognition and its applications," *ARPN Journal of Engineering and Applied Sciences*, vol. 11, no. 5, 2016.

[2] K. G. Paterson and D. Stebila, "One-time-password-authenticated key exchange," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2010. doi: 10.1007/978-3-642-14081-5_17.

[3] "What is Authentication? Definition of Authentication, Authentication Meaning - The Economic Times." Accessed: Nov. 26, 2023. [Online]. Available: https://economictimes.indiatimes.com/definition/authentication

[4] "What Are the Three Authentication Factors? – Rublon." Accessed: Nov. 26, 2023. [Online]. Available: https://rublon.com/blog/what-are the-three-authentication-factors/

[5] "Single-factor, Two-factor, and Multi-factor Authentication | Ping Identity." Accessed: Nov. 26, 2023. [Online]. Available: https://www.pingidentity.com/en/resources/identity fundamentals/authentication/single-factor-two-factor-multi-factor authentication.html

[6] N. Alyousif and S. Alhabis, "The Necessity of Multi Factor Authentication," *Zenodo (CERN European Organization for Nuclear Research)*, vol. 10, no. 2, pp. 46–49, Apr. 2022, doi: 10.5281/zenodo.6472757.

[7] V. Agrawal, R. K. Paliwal, P. Sharma, and A. Shrivastava, "Web Security Using User Authentication Methodologies: CAPTCHA, OTP and User Behaviour Authentication," SSRN Electronic Journal, 2019, doi: 10.2139/ssrn.3360306.

[8] M. Shirvanian and S. Agrawal, "2D-2FA: A New Dimension in Two-Factor Authentication," in *ACM International Conference Proceeding Series*, 2021. doi: 10.1145/3485832.3485910.

[9] H. Te Wu, "Establishing an Integrated Push Notification System with Information Security Mechanism," in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, 2021. doi: 10.1007/978-3-030-92163-7_3.

[10] "What is OCR? - Optical Character Recognition Explained - AWS." Accessed: Nov. 20, 2023. [Online]. Available: https://aws.amazon.com/what-is/ocr/

[11] V. Mdunyelwa, L. Futcher, and J. van Niekerk, "An Educational Intervention for Teaching Secure Coding Practices," in *IFIP Advances in Information and Communication Technology*, 2019. doi: 10.1007/978-3-030-23451-5_1.
[12] "WSTG - Stable | OWASP Foundation." Accessed: Jun. 10, 2023. [Online]. Available: https://owasp.org/www-project-web-security testing-guide/stable/
[13] "Input Validation - OWASP Cheat Sheet Series." Accessed: Dec. 24, 2023. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_ Sheet.html#input-validation-cheat-sheet
[14] H. Hussain, "Password Security: Best Practices and Management Strategies," SSRN Electronic Journal, 2022, doi: 10.2139/ssrn.4136333.
[15] A. S.Gilis and L. Rosencrance, "What is RBAC? | Definition from TechTarget." Accessed: Nov. 26, 2023. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/role-based-access-control-RBAC
[16] "Error Handling - OWASP Cheat Sheet Series." Accessed: Nov. 27, 2023. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Error_Handling_Cheat_Sheet.html
[17] F. Ferragamo, Wichers, J. Bird, and kingthorin, "Improper Error Handling | OWASP Foundation." Accessed: Dec. 28, 2023. [Online]. Available: https://owasp.org/www-community/Improper_Error_Handling
[18] S. K. Lala, A. Kumar, and T. Subbulakshmi, "Secure web development using OWASP guidelines," in Proceedings - 5th International Conference on Intelligent Computing and Control Systems, ICICCS 2021, 2021. doi: 10.1109/ICICCS51141.2021.9432179.
[19] "Carwash2U: Doorstep Car Detailing – Best car detailing service in Malaysia." Accessed: Nov. 15, 2023. [Online]. Available: https://carwash2u-services.com/
[20] "Carbox Auto Detailing Sdn Bhd | Scheduling and Booking Website." Accessed: Nov. 19, 2023. [Online]. Available: https://carboxad.simplybook.asia/v2/
[21] "Atom Detailing | Ceramic Coating & Paint Protection Film Specialists." Accessed: Nov. 19, 2023. [Online]. Available: https://www.atomdetailing.co.uk/
[22] L. Neelu and D. Kavitha, "Software development technique for the betterment of end user satisfaction using agile methodology," TEM Journal, vol. 9, no. 3, pp. 992–1002, Aug. 2020, doi: 10.18421/TEM93 22.
[23] "6 Stages of the Agile Development Lifecycle." Accessed: Dec. 02, 2023. [Online]. Available: https://www.decipherzone.com/blog detail/agile-development-lifecycle