AITCS

Secure Sunday Briyani Ordering Management System with Two-Factor Authentication

Clarissa Kamaly Stephen Dass[1], Nur Ziadah Harun[1]*

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

*Corresponding Author Designation

Abstract: An online meal ordering system is software that enables restaurants to accept and handle orders sent over the internet. A website that allows customers to examine the menu and place an order and an admin interface that allows the restaurant to receive and fulfil user requests are the two main components of an online food ordering system. The term "web-based online food ordering system with two-factor authentication (2FA)" refers to a system that was created with security measures such as two-factor authentication (2FA). Staffs, customers, and services make up the buying and selling process. The prior online ordering system was web-based without any security features and difficult to locate. Third parties, as well as system users, have simple access to customers' information. Two authentication factors (2FA) are utilized in a web-based online food ordering system with two security feature validation factors. This approach is used to add security elements inside a system. Email verification and CAPTCHA are the types of two-factor authentication that use a random number to add security elements to a system. Captcha Verification is a popular web technique for ensuring that your replies are genuine people rather than a bot designed to spam your page. To establish that they are human, the responder must check a box. Email verification is the process of verifying and authenticating emails to guarantee that they are genuine and will connect to a real person. Overall, this web-based food ordering system provides comprehensive food order administration as well as safety elements that are current with technology.

Keywords: Web-Based Food Ordering System, Two-Factor Authentication, CAPTCHA, OTP.

1.   Introduction

In today's world, where most establishments use automated systems, it is not suitable to have a manual system. They can be destroyed, lost, or misplaced in a variety of ways. For example, a fire or natural calamity could result in the loss of all of the restaurants' data. The staff will have to start from scratch if they want the information restored. This as nutshell, the editing process takes longer than it would if we were working with digital copies. Not only have to organize and save the files, but we also

have to find the information when it is needed. An automated system will allow the staff to complete these tasks without the use of manual labor.

The flaws of the current system can be fixed by developing a computerized system that will enable the staff to reduce the amount of manual work they have to do. The current system does not have any security features and only relies on the staff's documentation. As a result, we can improve the system and solve the limitations of the current manual system. This project aims to create a system that will allow admins to edit menu contents, update food items, add food categories, and check orders that can be managed from the staff side.

The staff and admin can access the system by entering their user Id and password. Users can browse the homepage, about, and contact pages in the user section. To place an order for food, the user must first create an account and then sign in or log in using two-factor authentication. This is to ensure a safe environment for both customers and staff when using the system. It will also have special features like customer feedback, where customers can give reviews on the food they had. It helps to reduce manual work by allowing the staff to easily find the bills and records of the customers. Each user and admin could be identified by their unique details.

Today, restaurant waiters use a paper-based manual method to collect customer orders. This is an issue for restaurant waiters since there is a chance that client information will be lost or duplicated. Sensitive information about staff and customers may use by unauthorized authorities and misuse it. It would also have an impact on the restaurant's reputation in terms of ordering management. The worker's data is kept on paper by a manual system, which makes it difficult for the restaurant's owner to locate worker information, increases the risk of losing the paper, and leads to information theft. Privacy of customers can be violated and breaks the trustworthiness of customers about the restaurant. The loss of confidential documents can cost the restaurant owner dearly. Customers expect their information to be safe. If the restaurant can't keep them safe, they would run the risk of losing them. The first difficulty is that the customer must make contact through telephone to the restaurant to make their orders. This is especially important if the restaurant is well known and busy. Many customers have had the experience of coming to a restaurant where the service is terrible and there is a lack of care from the staff. Paper menus can be unreliable, complicated, and outdated. The restaurant management gives solutions to take advantage of the growing varied sector. This restaurant menu and management framework will eliminate paper waste, make it more viable, and contemplate more significant customer commitment.

Objectives for this project are to create a secure Sunday Briyani management system, to develop a system with two-factor authentication that prevents unauthorized access and maintain the integrity of customers' data, and iii. To test user interface of Sunday Briyani management system.

The major scope of the Sunday Briyani restaurant management system project is to allow activity operators to accept and manage orders with a secure system. The ordering management system's central system features, on the other hand, includes creating accounts, billing, staff data, and fulfilling orders. A customer can order their favorite foods at any time, but that's only a limited option, and restaurants must have an efficient system for serving a large number of customers while making their work easier, as we've addressed. Several modules are included in the restaurant management system, which helps the administrator manage the restaurant more successfully and efficiently. Which are ordering management, payment management, menu management, registration and login management, and delivery management.

End of this project, the system is expected to result as a system that allows the owner to easily promote their foods without the need to constantly update food information, system that includes customers and worker's information and manage through databases and interfaces and a system that developed security features during authentication process of the users. This project effort will improve the productivity of the restaurant management protocol of Sunday Briyani and make it convenient and

easy. The proposed technology will improve accommodation orders, save time and increase financial operations efficiency. Indirectly, this would also save time and money on restaurant expenses. The owner can also give more focus on their business.

2. Literature Review

2.1 Two- factor authentication

There are three stages in two-factor verifications. Which is, "what you have," "who you are," and "what you know." On top of that, two validations are a composite of two of the three verifications [1]. Two-factor validation is a validation method that uses two methods of authentication to create a system with security features that are current with technology advancements. Only one validation factor is used in conjunction with an authentication mechanism. Use a password as an example of a system's security feature. Third parties will be able to easily log into user accounts in this manner [2]. The verification account website is compared to two factor authentication procedures such as producing a six-digit random number (OTP), applying photo verification, and using the verification account website. The two authentication factors also include the use of passwords with high security features. Third parties or hackers will have a hard time obtaining users' personal information if they employ two authentication factors, preventing identity theft [3].

2.3 Password Management

Password management is a set of guidelines and practices that users follow while storing and managing passwords. For maximum password security and to prevent unauthorized access, password management is crucial. At least eight characters, including one capital letter, one lowercase letter, one small letter, one numeric character, and one unique symbol, make up a good password [3].

2.4 Captcha Code Authentication (CAPTCHA)

CAPTCHA is a form of visual verification and identification that uses a challenging Artificial Intelligence (AI) issue to discriminate between humans and bots. CAPTCHA is primarily used to combat auto-bots and click fraud during account registration. Its application may also be used to verify a group of persons who have similar knowledge or skills. However, by asking personal or professional questions, CAPTCHA is difficult to verify a specific individual. Man-In-The-Middle (MITM) attacks can compromise visual human verifiable procedures. CAPTCHA alone is insufficient in the face of a Man-In-The-Middle (MITM) attack. Such visual security relies on the user's cognitive inability to authenticate the other end. By integrating CAPTCHA with OTP, the Extended CAPTCHA Input System (E-CIS) can endure the Real-Time Man-In-The-Middle (RT-MITM) [4]. E-CIS can authenticate a specific individual, which may be utilized in a secure online login scenario.

2.5 Study of Existing Related Systems

Mollagaa Restaurant Ordering System and Indian Palace Ordering System are the two systems. The differences between the proposed system and the existing systems are shown in a comparison table.

2.5.1 Mollagaa Restaurant Ordering System.

Mollagaa Restaurant serves traditional Indian foods which is the main factor to attract many locals and foreigners. The restaurant is located at No.50A, Lebuh Ampang Kuala Lumpur 50050, located about a minute away from the Masjid Jamek train station and 8 – 10 minutes away from Petaling Street and Chinatown. The restaurant is well known among the locals because they serve the best banana leaf rice and briyani in town. The price is affordable and valuable for the food they sell.

Figure 1: The user interface of the Mollagaa restaurant ordering system [6]

As shown in Figure 1, customers can use the system to place their orders. Food is available in two forms which are home delivery and self-collection. Mollagaa restaurant now allows customers to order food online as well at the counter same as the Sunday Briyani ordering system.

There are several options to login which are login with Facebook, login in with google and phone number. The system does not limit the number of logins attempts which will be easier for hackers to hack the system. For the registration form, customers are required to enter their first name, last name, mobile number, email address, and password. The limitation in this login form is there are no specific requirements for password management in the system. Users can enter any password and re-enter the password in confirm password to create the account. The system accepts any short or long passwords.

The system has credit card, debit card, boost, GrabPay Online, Touch 'n Go, eWallet, online banking, Maybank PayQR online and ShopeePay. But unfortunately, cash payments are not accepted for delivery options.

2.5.2   Indian Palace Ordering System.

Indian Palace plates up authentic Indian cuisine with a touch of North and South Indian food. It has Indian culture museum inside the restaurant as a special attraction which will help customers to know about Indian culture. They also provide services like host for events such as birthday, wedding dinner, anniversary and family gathering. Indian Palace is located at 2A-G-18 Quartermile, Solok Mayang Pasir, Bayan Baru, 11950 Bayan Lepas, Pulau Pinang.
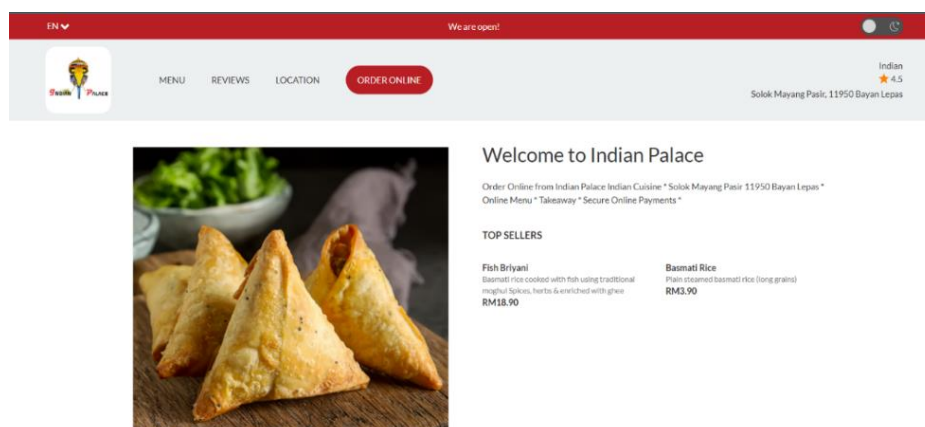

Figure 2: User interface for Indian Palace ordering system [7]

Customers can pick their dish from the menu page and check the reviews about the restaurant as in Figure 2. Customers must order their food on the system and pick-up the orders themselves. Since

the system does not have a login page where customers can enter using their account. In this system, users have to choose their food and proceed with their payment. They allow to pay through credit card and PayPal. In addition, the users have to enter their contact info which are Full Name, Mobile Number and Email Address. The limitations in this system are there is no login interface where any people can order using their fake account and pretend to be someone else. This system does not have any safety features where most of the customers avoid ordering from that system.

2.5.3   Comparison with the Existing Systems

Some of the ideas of the proposed online food ordering system are like those of existing online food ordering systems such as Mollagaa Restaurant Ordering System and Indian Palace Ordering System. In nine categories, Table 1 discusses the different the three systems.

Table 1: Comparison between the existing system with the Sunday Briyani system

	Mollagaa [6]	Indian Palace [7]	Sunday Briyani
Type of Integration	Web-based	Web-based	Web-based
Order type	Delivery and Pick-up	Pick-up	Pick-up
Login	Yes	No	Yes
Authentication methods	▪ Email ▪ Facebook ▪ UserID ▪ Password	-	▪ UserID ▪ Password ▪ OTP verification ▪ CAPTCHA verification
Payment Method	▪ Credit & Debit card ▪ Boost ▪ GrabPay Online ▪ Touch 'n Go eWallet ▪ Online Banking ▪ ShopeePay ▪ Maybank PayQR Online	▪ Credit Card ▪ PayPal	▪ FPX online banking.
Login attempt	No limit	No limit	Three times
Email verification	No	No	Yes
Password requirement	No specific requirements	No specific requirements	Meets all six requirements below: 1. At least 8 characters 2. Mixture of both uppercase and lowercase letters 3. Mixture of letters and numbers 4. Inclusion of at least one special character, e.g., ! @ # ? 5. 5.Do not use < or > in your password 6. 6.Not same as the UserID
Security strength	-	-	OTP and CAPTCHA

3.   Methodology

In 1970, Royce presented the concept of the Waterfall model. The waterfall model is a method for progressively improving software. Its progress may be seen as it flows along with the non-overlapping phases of Requirements Analysis, System Design, Implementation, Testing, and Maintenance step by step. The waterfall model is a sequential life cycle model with no phases that overlap. This signifies that the following step cannot begin until the previous one is completed [5].

The system requirement and analysis activities are included in the waterfall requirement gathering phase. The planning task is to create ten interview questions and conduct an interview with Sunday Briyani restaurant's management. The purpose of the interview question is to learn how the restaurant operates, the things that the restaurant sells, approach to the ordering and payment process, and find out whether the restaurant has ever had a problem with faked orders. Understanding how the restaurant calculates the sales report is essential. To grasp the restaurant's system needs and figure out who the system's most important users are. This information is acquired so that it may be analyzed throughout the system design process.

The purpose of the requirement analysis activity is to examine the data gathered from the restaurant management. The suggested system has four main requirements. Firstly, the system's major priority is that customers be able to order takeout and delivery through the internet. Secondly, the ability for personnel and administrators to place dine-in orders. The third project requirement is to avoid a fraudulent order. Thus, clients must complete the online payment after placing a takeout or delivery order. Allowing workers and administrators to change the menu online is the fourth project criteria.

The proposed system's objectives and scopes are then determined. The design, construction, and testing of the suggested system are the three objectives of this project. The project's scope covers three key users which are the restaurant's client, admin, and employees. In this process, information on hardware as well as software requirements is collected to develop the system. There are four software requirements and two hardware requirements.

A total of five modules are supplied. Ordering, payment, menu, registration and login, and delivery management are the components. The data for this online food ordering system is stored in seven tables which are user, item, order, order item, category, address, and setting. For user interface modules which are registration, login, two-factor authentication, and system logout, this system requires four system pages. Account registration pages are developed for account users to submit their information in order to create an account. A login page is also established for account users where they may input their username and password. Account users will be required to complete a captcha verification in order to log into the system. The last page is where the user log out. After utilizing the system account, account users will log out of the system. A flow chart is used to illustrate the system design. This is to demonstrate the system creation procedure in detail. Chapter 4 will go through the system architecture in the flow chart. The developed system's entities and components are identified. Data names, data kinds, and data quantities are all examples of metadata. Entity Relationship Diagrams (ERD) and data flow diagrams are used to describe all entities (DFD).

In the implementation phase, the design that has been generated is required to deploy into the system. The development of the system necessitates the use of a database. The system is built around the scope and modules that have previously been mentioned. Page development for account users is also performed throughout this procedure. The PHP programming language is used to establish communication between the data and the database.

At the testing stage, system testing is necessary to ensure that the system is functioning properly. The modules of the system will be tested in accordance with the test strategy. To conduct tests on the system, a test plan is required. In the test plan, there are two stages of tests. The first stage is to assess how well the system is working. The security requirement is then put to the test in the second stage. If

an error occurs, the debugging technique is used to ensure that the system continues to function normally. The completed system's performance will be monitored to ensure that the system's processes are working smoothly. System performance is critical during this period for identifying system faults and repairing system damage.

4.   System Analysis and Design

There are two types of requirements that are required for the proposed system which are functional and non-functional as shown in Table 2 and Table 3 respectively.

Table 2: Functional requirement analysis

Module	Functionalities
Ordering • Admin • Customer	• The system can fetch new orders from the database and the user may place orders. • Admin can track the customers' orders.
Payment • Admin • Customer	• The administrator has access to all payment receipts. • Users can pay through the system by online payment after checkout of the cart.
Menu • Admin • Customer	• The system allows the administrator to adjust the pricing as well as add, edit, and delete meals or drinks items from the menu. • The menu may be seen and managed by the customer.
Login • Admin • Customer	• The system allows the users to login into the system using email and password. • Invalid input, such as an incorrect email or password, will cause the system to notify the user.
Register • Customer	• All users should be required to register before they can log in. • Customers should be able to verify their phone number captcha after completing the registration process.

Table 3: Non- Functional requirement analysis

Requirement	Description
Performance of the user interface and system flow	• Depending on user authorization, the system should be in the relevant session. • Time out is enabled after a 20-minute automatic log out.
Operational	• Only when there is an internet connection is the system available.
Security	• Users can only access the system if they have the right email address and password. • Minimum of eight characters, at least one letter, one symbol, or not the same as the username. • Users can access the system after OTP and captcha verification is completed.
Usability	• The system should be straightforward and easy to use

4.1   Data Flow Diagram (DFD)

Figure 3 demonstrates the Sunday Briyani ordering management system's context diagram, or level 0 DFD, which generalizes the system's operation with respect to individual entities.
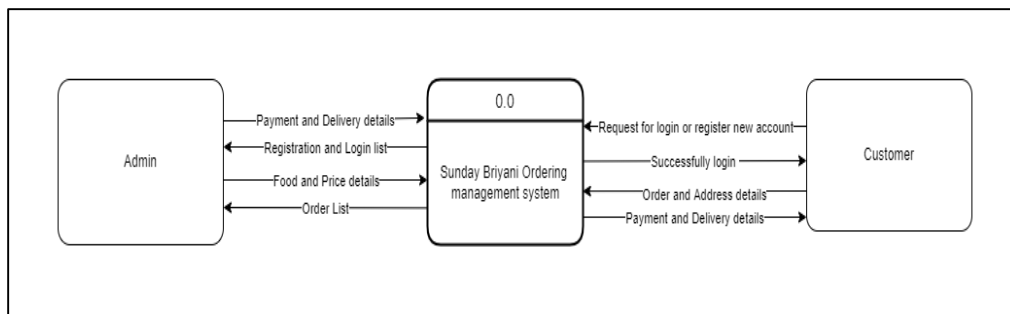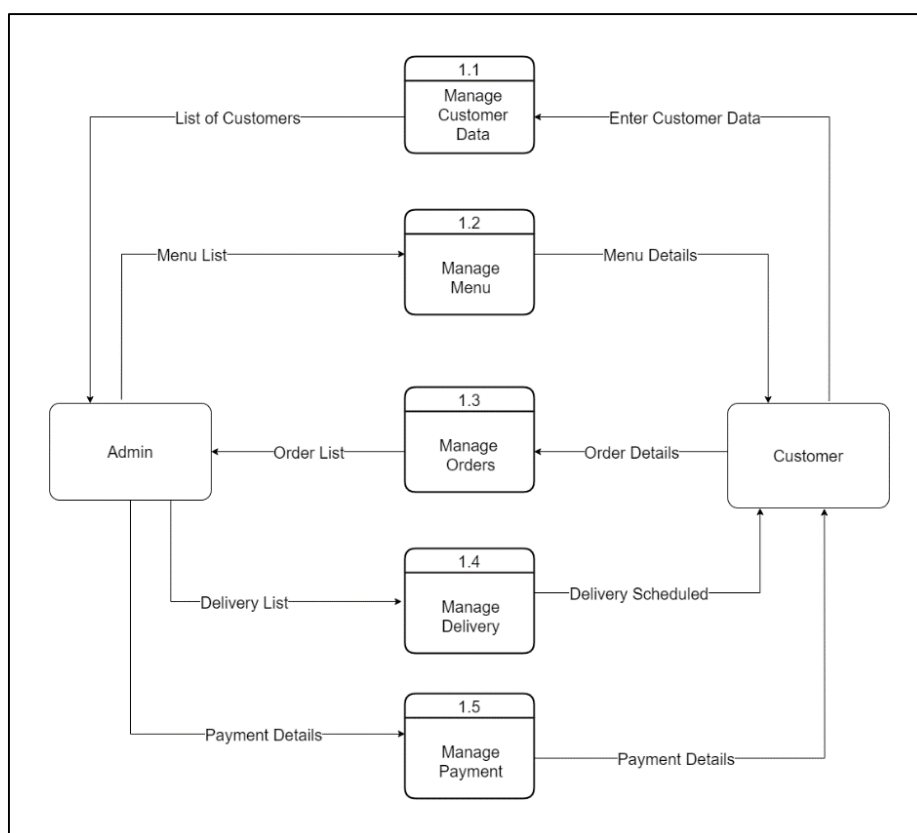

Figure 3: Level 0 DFD

Figure 4: Level 1 DFD

The system's Level 1 DFD is seen in Figure 4. Customer data management, menu management, order management, delivery management, and payment management are among the five procedures in this system.
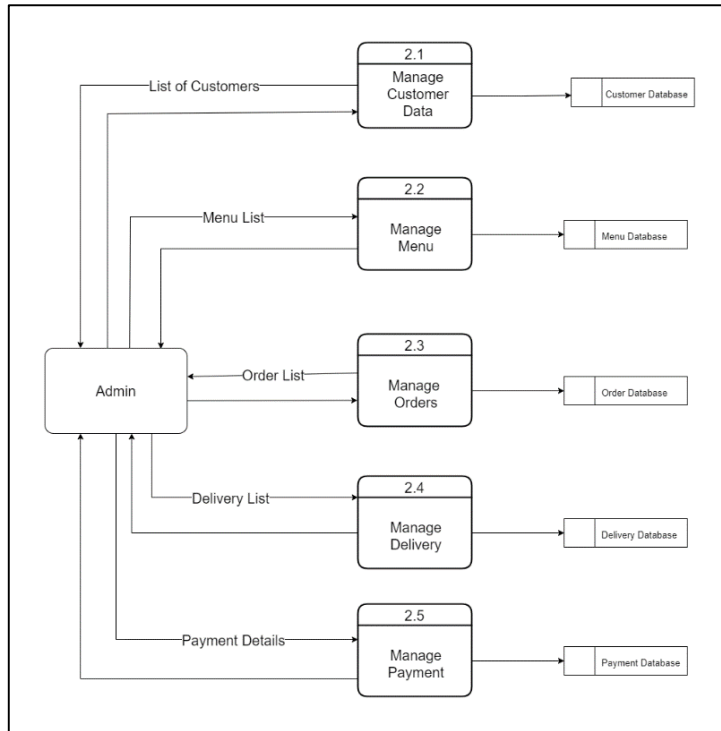
Figure 5: Level 2 DFD of Admin

Figure 5 describes the admin system's Level 2 DFD, which includes five tables: customer, menu, order, delivery, and payment tables.
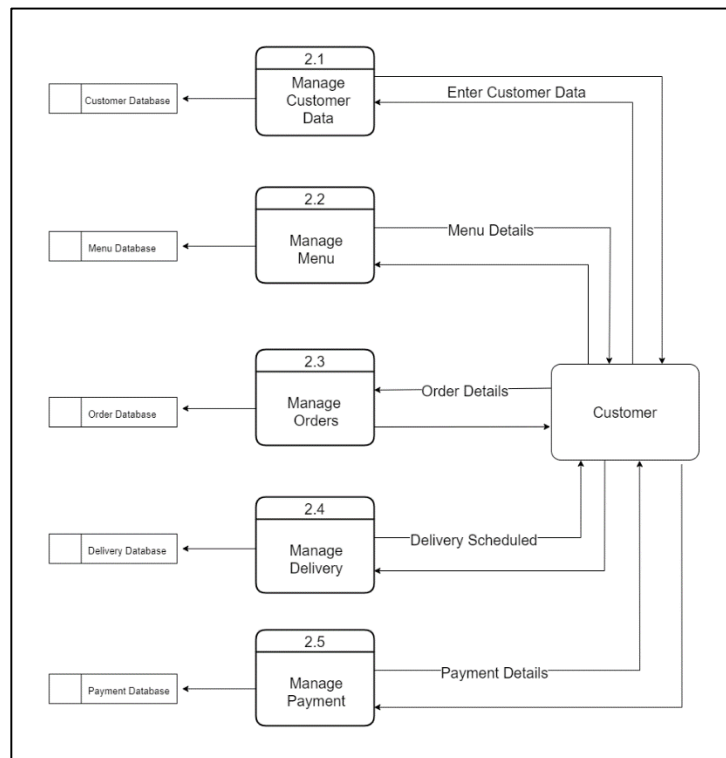

Figure 6: Level 2 DFD of Customer.

Figure 6 represents level 2 DFD of the customer's system. All the data entered by the customers will be saved in the categorized table such as customer, menu, order, delivery and payment.

4.2   Entity Relationship Diagram (ERD)

Nine tables are illustrated in the diagram. Customer, admin, admin_codes, res_category, restaurant, dishes, auth_token, orders, and payment are the tables shown in Figure 7.
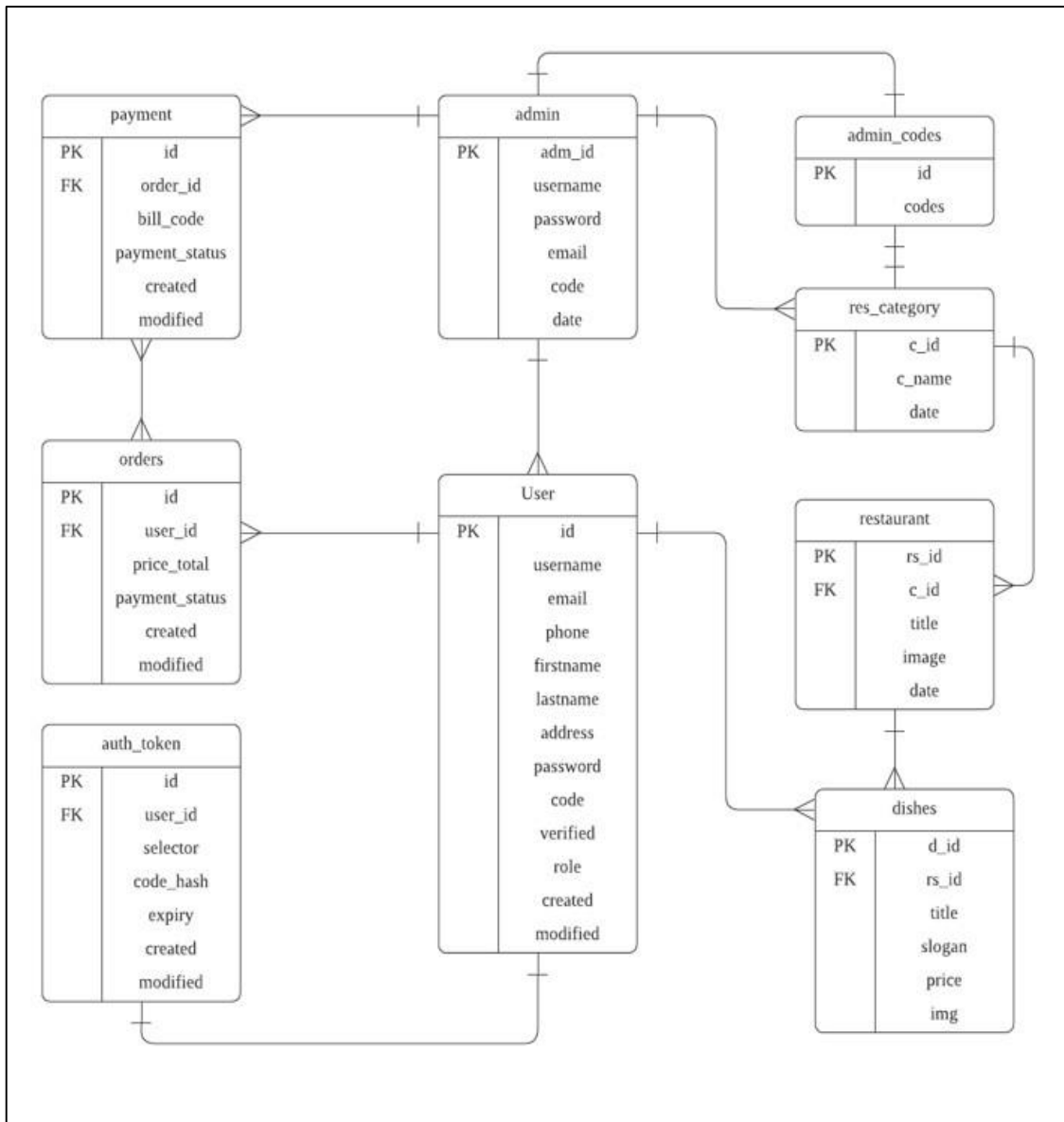

Figure 7: Entity Relationship Diagram for Sunday Briyani system.

4.3   System Design

The system design diagram is part of the overall system architecture. The suggested system's system design diagram is shown in Figure 8.
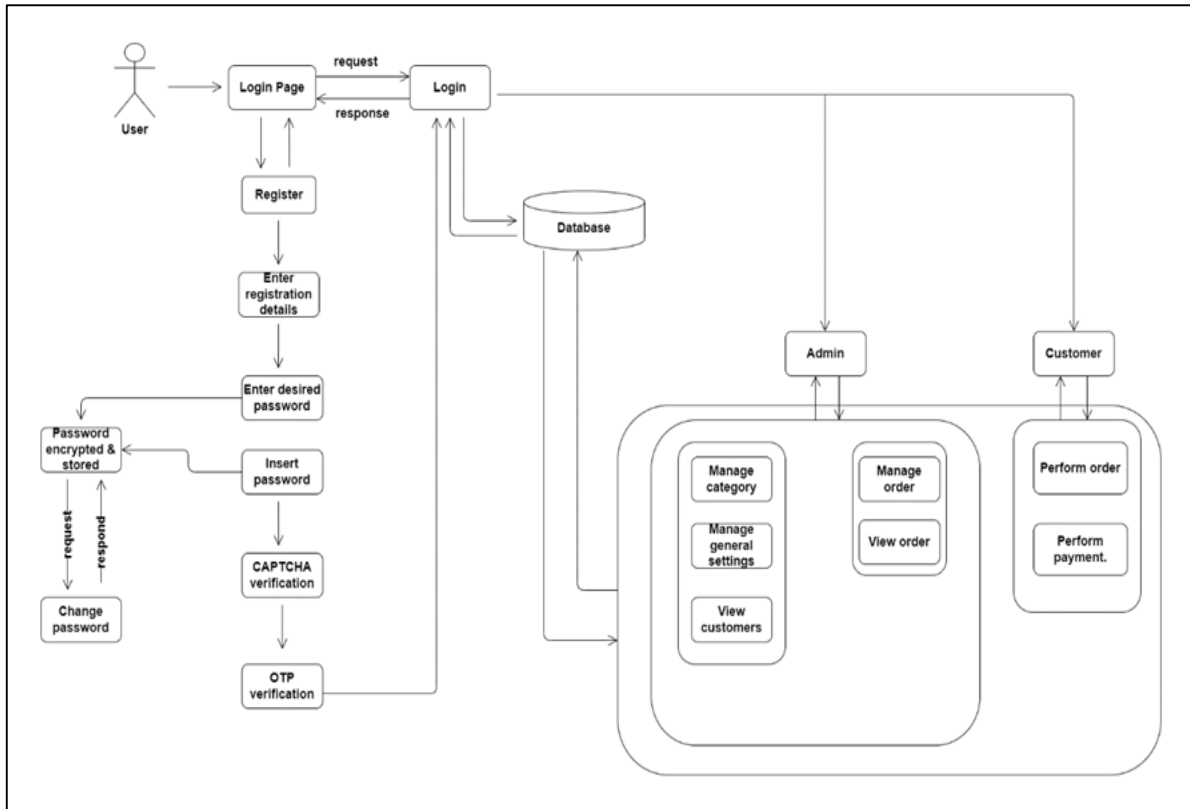
Figure 8: System design diagram for Sunday Briyani system

4.4   Security Requirement Testing

Security requirement testing examines the proposed system's security needs. The security check for the Sunday Briyani Ordering management system is shown in Table 4.

Table 4: Security check for Sunday Briyani ordering management system

Security Requirement	Results
1. Make a printout of the error notice with incorrect credentials, which will say "username or password Incorrect."	Pass/Fail
2. Enforce the difficulty of the password, which should be at least eight characters long.	Pass/Fail
3. Maintain the difficulty of the password where demand the use of alphabetic, numeric, and special characters while constructing a password.	Pass/Fail
4. Password should be obscured in the text box.	Pass/Fail

5.   Implementation

The system for ordering Sunday Briyani was created using Microsoft created Visual Studio Code, a source code editor for Windows. PHP is XML was used to create the designs and layouts for the proposed system. For every module, the database is chosen and phpMyAdmin is used to connect to the suggested system. The security module implemented in the system is detailed in this section. Encryption for the password, strong password requirements, login attempt, captcha, and one-time-passcode (OTP) are the five security modules implemented in this suggested system.

5.1 Database Connection

The database connection is used to link a database to a PHP source code. Figure 9 depicts the proposed system's MySQL database connection in Visual Studio Code. Mysqli connect is used to connect to the database in the proposed system, and phpMyAdmin is used to process CRUD, which stands for create, read, update, and delete data in the module.

```php
1    <?php
2    require_once __DIR__.'/../libs/libs.php';
3
4    //main connection file for both admin & front end
5    $servername = "localhost"; //server
6    $username = "root"; //username
7    $password = ""; //password
8    $dbname = "sunday_briyani";   //database
9
10   $ToyyibPaySecretKey = 'hcxlf2af-sqk3-bt61-0jdy-56ieovix6nah';
11
12   // Create connection
13   $db = mysqli_connect($servername, $username, $password, $dbname); // connecting
14   // Check connection
15   if (!$db) {         //checking connection to DB
16       die("Connection failed: " . mysqli_connect_error());
17   }
18
```

Figure 9: Source Code for Database Connection.

5.2   Implementation of Encryption

The code for password encryption generation is shown in Figure 10. The hash value of the plaintext of the user password is used to generate the key. The hash algorithm's result is no longer predictable after hashing a plain text password with a salt. The hash generated by the same password will no longer be the same. User do not need to save the salt in a database because it is automatically included with the hash.

```php
$_POST[ 'password' ] = password_hash( $_POST[ 'password' ],
PASSWORD_DEFAULT );
```

Figure 10: Source Code for Password Encryption.

5.3   Implementation of Strong Password

The code for implementing a strong password in the system is shown in Figure 11. The system checks the user's supplied password and returns an error if it does not comply with the strong password policy. The minimum and maximum character lengths are set to 8 and 20 characters, respectively. The password must match the regex, which includes the following characters: number, capital letter, tiny letter, and symbol. The password cannot be the same as the username, and no spaces are allowed. If the error return is not null, the system will disregard the entered password, and the user will be required to establish a new password that meets the password policy's requirements.

```javascript
document.addEventListener( "DOMContentLoaded", function() {
        var pwdInput = document.getElementById( "password" ),
            pwdInput2 = document.getElementById( "confirm-password" ),
            input = document.querySelector( 'input[type=password]' );
        pwdInput.oninvalid = function(e) {
            if ( pwdInput.validity.tooShort ) {
                e.target.setCustomValidity( "Must contain minimum 8
characters." );
            } else if ( pwdInput.validity.patternMismatch ) {
                e.target.setCustomValidity( "Must contain number,
uppercase and lowercase letter and special character." );
            }
        };
        pwdInput2.onkeyup = function(e) {
            var value1 = this.value,
                value2 = pwdInput.value;
            if ( value1 != value2 ) {
                e.target.setCustomValidity( "Password do not match" );
            } else {
                e.target.setCustomValidity( "" );
            }
        }
        input.oninput = function(e) {
            e.target.setCustomValidity("");
        };
    });
```

Figure 11: Source Code for Strong Password.

5.4   Implementation of Captcha

```php
<?php
require_once 'connection/connect.php';
function check_recaptcha()
{
        if ( $_SERVER[ 'REQUEST_METHOD' ] != 'POST' ) return;
        $secret = '6LeK_UofAAAAACOoELQwrvR8H-uLPgWiCJOFJmiQ';
        $verifyResponse =
file_get_contents('https://www.google.com/recaptcha/api/siteverify?secret='.$secret.'&response='.$_POST['g-recaptcha-response']);
        $responseData = json_decode($verifyResponse);
        unset($_POST['g-recaptcha-response']);
        if ( !$responseData->success ) {
            global $flash;
            $flash->danger( "The reCAPTCHA wasn't entered correctly. Please try
again." );
            return false;
        }
        return true;
}
if ( check_recaptcha() ) {
    $auth->register( '', true, 'http://localhost/sunday_briyani/verify_email.php'
);
}
?>
```

Figure 12: Source Code for Captcha Implementation.

The reCAPTCHA's source code and user interface is shown in Figure 12 and 13. To prevent automatic login and account creation, reCAPTCHA is used on the login and registration pages. CAPTCHA protects users from spam and password decryption by requiring them to complete a simple test that verifies they are human rather than a computer attempting to access a password-protected account.
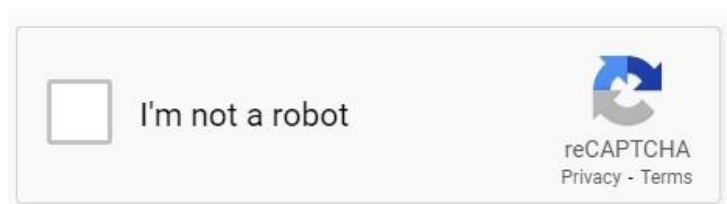

Figure 13: reCAPTCHA verification box.

5.5   Implementation of Email Verification

The source code for email verification in the Sunday Briyani Registration Page is shown in Figure 14. The protocol allows a user to receive a verification link to their registered email id, which when clicked validates the account and redirects the user to the site. This is to prevent highly targeted email assaults in which an attacker impersonates a legitimate/trusted sender to acquire personal data from the receiver.

```
if ( $verifyEmail ) {
                extract( $_POST );
                $verificationLink =
"{$verificationPage}?email={$email}&code={$code}";
                $result = $this->_sendMail( [ $email, $username ],
'email_verification', compact('verificationLink','user'), $mailErrorInfo );
                if ( !$result ) {
                    $user->delete();
                    $this->_redirectCallback( $redirectTo, null, "Message could
not be sent. Mailer Error: {$mailErrorInfo}" ); return;
                } else {
                    $this->flash[ 'success' ] = 'A verification link has been sent
to your email.';

                    $this->_redirectCallback( $redirectTo, $user );
                    return;
                }
            }
```

Figure 14: Source Code for Email verification.

6.   Results and Discussion

Testing is done to see if the system has any bugs or errors. As a result, the system will function as planned, and the software quality will be up to standard. The functionality of the Sunday Briyani ordering system will be evaluated through functional testing and user acceptance testing. The system's testing is covered in this section. Test plan results, penetration test results, and user acceptance form results are the three types of testing outcomes for the proposed system.

6.1   Test Plan Result

The test plan results for Admin and customer are listed in Table 5 and 6, while security check results are presented in Table 7.

Table 5: System Functionality test plan result for Admin

Category	Description	Expected Results	Results
Login	Login with wrong username and wrong password.	Access denied.	Pass
	Login with wrong username and correct password	Access denied.	Pass
	Login with correct username and wrong password	Access denied.	Pass
	Login with correct username and correct password.	Access successful.	Pass
Menu	View menu	View all the listed menu.	Pass
	Add menu	Selected menu added.	Pass
	Update menu	Selected menu updated.	Pass
	Delete menu	Selected menu deleted.	Pass
Customer	View customer	View all the listed customers.	Pass
Order	View Order	View all the listed orders.	Pass
	Add order	Selected order added.	Pass
Settings	Update phone number	Phone number updated.	Pass
	Update delivery address	Delivery address updated.	Pass
	Update personal information	Personal information updated.	Pass
Profile	View profile	View all listed profiles.	Pass
	Update profile	Profile updated.	Pass

Table 6: System Functionality test plan result for Customer.

Category	Description	Expected results	Results
Login	Login with wrong username and wrong password.	Access denied.	Pass
	Login with wrong username and correct password	Access denied.	Pass
	Login with correct username and wrong password	Access denied.	Pass
	Login with correct username and correct password.	Access successful.	Pass
Register	Submit form without any data.	Message: Please complete the mandatory field.	Pass
	Insert password with 20 characters.	Messages appear: Max 10 characters for the password.	Pass
	Confirm password with different password.	Message: Password does not match.	Pass
	Confirm password same password.	Messages appear: Password match	Pass
	Insert valid username, valid phone number, valid password and confirm password with the same password	Successful	Pass

Table 6: (cont)

Category	Description	Expected results	Results
CAPTCHA verification	Insert wrong response.	Message: Incorrect response. Please try again.	Pass
	Insert correct response after 5 minutes from the requested time.	Message: Session expired. Please verify again.	Pass
	Insert correct response.	Verified	Pass
Email verification	Verify email address field is cannot be accessible by clicking on the email field.	Message: Request again.	Pass
	Verify email address field is accessible by clicking on the email field.	Message: Successful	Pass
Menu	View menu	Shows all the listed foods.	Pass
	Add to cart	Added item listed in the cart.	Pass
Cart	View cart	Shows all the listed foods in the cart.	Pass
	Add foods in the cart.	Quantity increases in the cart.	Pass
	Delete foods in the cart.	Quantity decreases in the cart.	Pass
	Total calculation	Sub-total for each food and total price calculated correctly.	Pass
Payment	Choose one type of payment method	Redirect to the selected payment page.	Pass
	Insert valid information for the transaction	Payment successful.	Pass
	Insert invalid information for the transaction.	Payment fails. Redirect to the main payment page.	Pass
Profile	View profile information	Viewed profile	Pass
	Update profile information	Information changed in the profile.	Pass

Table 7: Security check result for Sunday Briyani ordering management system.

No.	Security Requirement	Result
1	Make a printout of the error notice with incorrect credentials, which will say "username or password Incorrect."	Pass
2	Enforce the difficulty of the password, which should be at least eight characters long.	Pass
3	Maintain the difficulty of the password where demand the use of alphabetic, numeric, and special characters while constructing a password.	Pass
4	Password should be obscured in the text box.	Pass

6.2   Penetration Test Result

The summary report of penetration testing performed by the Qualys penetration testing tool is shown in Figure 15. Qualys has given it an A rating. Certificate, protocol support, key exchange, and cipher strength are the four criteria used to assess it. Figure 15 shows the grades awarded for the four categories.

Figure 15: Summary of Qualys penetration testing [8]

Figure 16 shows a vulnerability scan of Quttera. It demonstrates that the website has no harmful, suspicious, or possibly suspicious files. There are a total of 63 files that are clean.

Figure 16: Vulnerability scanning of Quttera [9]

The website is not a suspected phishing page, as shown in Figure 17, because it does not appear to be a fake or replica of another website. The website does not appear to contain harmful code; hence it is not a suspected malware source. The website is not suspected of distributing unwanted software because it does not appear to be attempting to do so.
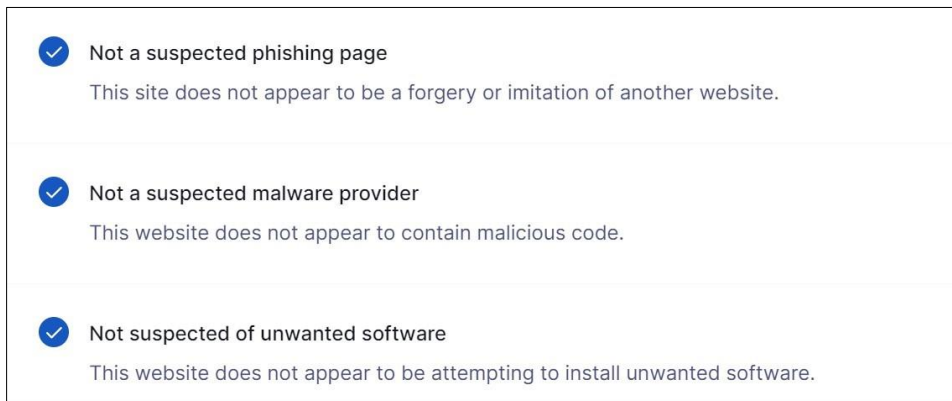
Figure 17: Penetration test result for the phishing and malware [10]

At upguard.com, the penetration test result is shown in Figure 18. The website is not vulnerable to attacks such as Logjam, Heartbleed, or Poodle.
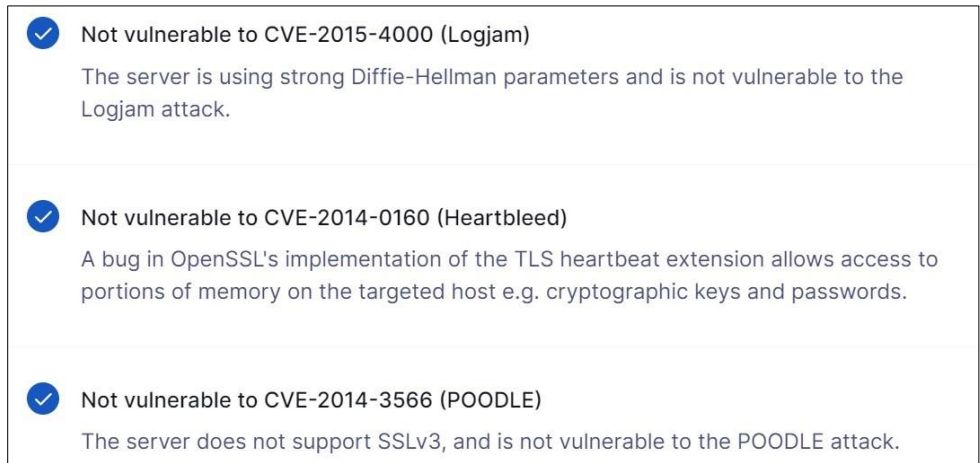
Figure 18: Penetration test result at upguard.com [10].

6.2   User Acceptance Test Result

The final stage of the system testing process is user acceptance testing. Users are given the opportunity to test the system to see if it works as planned during this phase. This is a crucial phase since it allows the system's developer to discover any issues that may arise. Twenty people completed a Google form to test the Sunday Briyani Ordering Management System and provide comments. The user approval form's response is divided into three graphs. The first is the impact of system functionality testing, the second is the result of system design testing, and the third is the security check list. The outcomes of those three graphs are shown in Figure 19, 20, and 21.
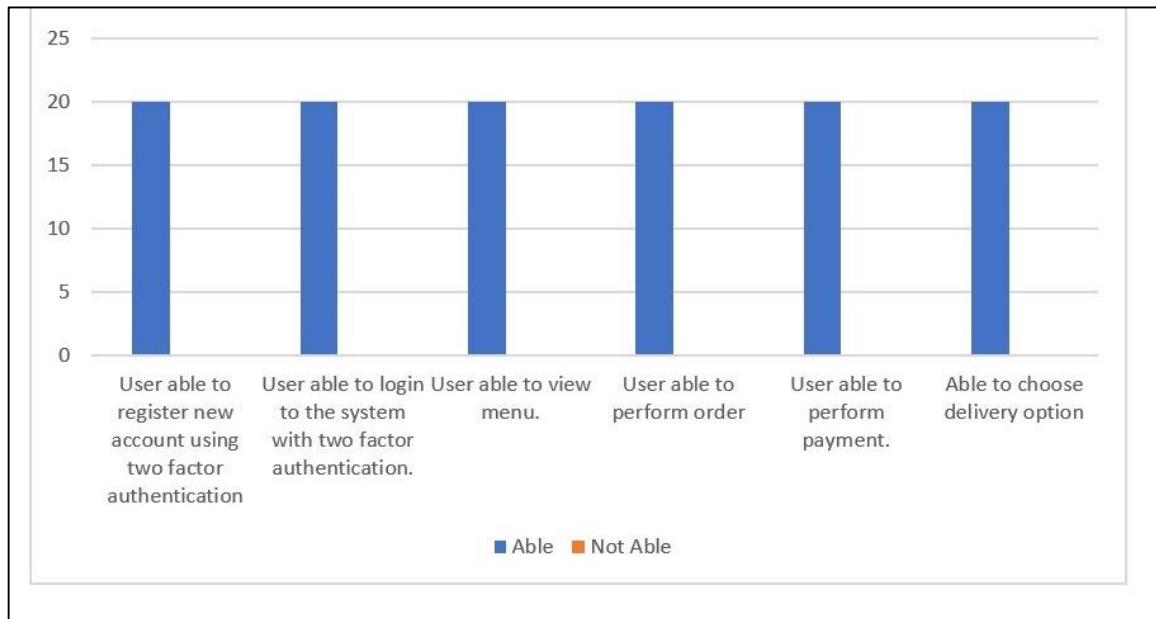

Figure 19: System functionality testing result

The results of the system performance testing are shown in Figure 20. All users will be able to use the function without any issues. The register, login, menu, order, payment, and delivery functions have all been thoroughly tested and proven to work.
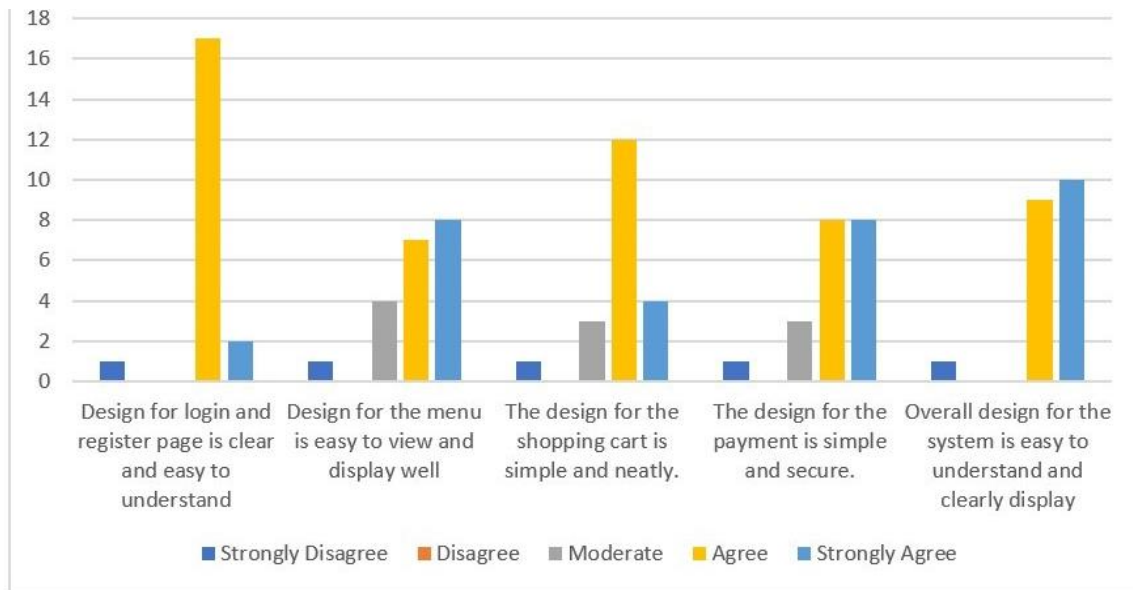
Figure 20: System design testing result

The design for the login and registration page is straightforward and easy to comprehend, according to two respondents highly agree, seventeen respondents agree, and one person strongly disagree. The menu design is easy to view and present properly, according to eight respondents who strongly agree, seven respondents who agree, four respondents who feel moderate, and one respondent who strongly disagree. The design for the shopping cart is basic and tidy, according to four respondents strongly agree, twelve respondents agree, three respondents feel moderate, and one respondent strongly disagree. The general design for the payment is straightforward and secure, according to eight respondents who strongly agree, eight respondents who agree, three respondents who feel moderate, and one person who strongly disagrees. The overall design of the system is easy to understand and clearly present, according to ten respondents who highly agree, nine respondents who agree, and one person who strongly disagree.
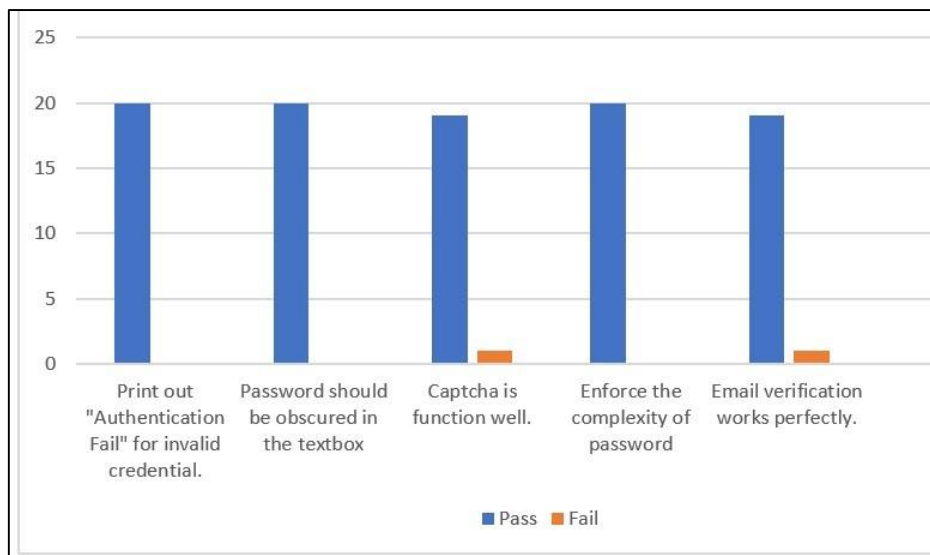

Figure 21: Security checklist test result

The results of the system's security checklist test are shown in Figure 21. Except for one respondent's captcha not working properly and one respondent's email verification not working perfectly, all respondents passed the security checklist.

7. Conclusion

The proposed system's goal is achieved at the end of the development process. Throughout the system development process, project time management and planning are critical to developing and completing the proposed system on time. Overall, the Sunday Briyani ordering system, which is web-based and uses two-factor authentication and email verification, has been effectively deployed in accordance with the scope and objectives established. Some suggestions for improvement can be implemented, and it is convenient to create an online ordering system with the most up-to-date security measures in the future. The use of two-factor authentication can secure the user's personal information, and only account users can log into the system, which is one of the system's advantages obtained from the established system. Users can also view the available dishes and their prices before making a purchase. Admin has the ability to update dish information and collect orders in a more orderly and systematic manner. The Sunday Briyani ordering system allows users to place orders, pay for them, and watch their progress. A strong password policy is enforced by the system, which requires users to establish strong passwords. Password encryption is also used by the system to encrypt the user's password. The captcha is used to prevent accounts from being created automatically.

Acknowledgment

References

[1]   Wordfence. (2021). *Two-Factor Authentication*. https://www.wordfence.com/help/tools/two-factor-authentication/

[2]   Bradley. (2020). *How Does Two-Factor Authentication (2FA) Work?* Merchant Fraud Journal. https://www.merchantfraudjournal.com/two-factor-authentication-work/

[3]   Raponi, S., & Pietro, R. di. (2020). A Longitudinal Study on Web-Sites Password Management (in)Security: Evidence and Remedies. *IEEE Access*, *8*, 52075–52090. https://doi.org/10.1109/ACCESS.2020.2981207

[4]   Kumar, G. A., & Rishav, G. (2021). CAPTCHA Techniques of Secure Web Authentication: A Survey. In *Communication Software and Networks* (pp. 97-117). Springer, Singapore

[5]   Shukla, B., Khatri, S. K., Kapur, P. K., (2017). *2017 6th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions) : September 20-22, 2017, Amity University Uttar Pradesh, Noida, India.*

[6]   Molagaa Restaurant, 2021 [Online]. Available: https://mollagaa.eatmol.com/. [Accessed 23 Oct 2021].

[7]   Indian Palace, 2021[Online]. Available: https://www.gemrestaurant-online.com/IndianPalace/en/menu. [Accessed 23 Oct 2021]

[8]   "Information Security and Compliance | Qualys, Inc.," Qualys.com, 2020. https://www.qualys.com/

[9]   Martin and Martin, "FREE Online Website Malware Scanner | Website Security Monitoring & Malware Removal | Quttera," Quttera.com, 2019. https://quttera.com/

[10]   "UpGuard | Attack Surface and Third-Party Risk Management Software," www.upguard.com. https://www.upguard.com/