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

AITCS

Vol. 7 No. 1 (2026) p. 1147-1164
https://publisher.uthm.edu.my/periodicals/index.php/aitcs

A Secure Web Application for Zura Razak Management System with Image-Based Authentication

Nur Athirah Farhana Mohd Hisham[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.2026.07.01.062

Article Info

Received: 20 July 2025
Accepted: 18 June 2026
Available online: 30 June 2026

Keywords

Image-Based Authentication, Zura Razak Management System, Secure User Login, Order Management, Web-Based System

Abstract

Zura Razak's Enterprise faced issues with its manual order system, such as order delays, inaccurate data handling, and potential threats to customer information security. These problems revealed the need for a more secure and efficient digital solution. In response, a secure web-based system was proposed to replace the manual process. The system incorporates password and image-based authentication, along with encryption, to safeguard sensitive data. With this system, the business aims to process orders more efficiently and accurately while improving data protection. The admin will manage products, sales, categories, orders, customer feedback, and send emails. Customers will log in securely, browse and purchase products, make payments, access order history, submit feedback, and update profiles. The system is designed to enhance efficiency, reduce human error, and strengthen security. Future enhancements may include real-time live chat, shipping integration, and online banking to further improve functionality and user experience.

1. Introduction

The Zura Razak Management System aims to address the challenges faced by Zura Razak Enterprise, a business specializing in Malaysian traditional delicacies, cakes, and pastries, which has been relying on a manual order management system. This system has led to inefficiencies, errors, and security risks. To meet the increasing demand for a secure and efficient online experience, the project focuses on developing a secure web application that automates order management, enhances operational efficiency, and ensures data protection.

The problem statement highlights the challenges of the current manual system, which leads to order oversight, delayed processing, and security vulnerabilities, resulting in customer dissatisfaction. The project's objectives are to design a secure web application with image-based authentication, streamline order management, enhance customers' experience, and improve business operations. The scope of the project includes the development of a web application for order, customer, and product management, as well as secure payment processing, with a focus on security, efficiency, and scalability.

The system will incorporate security features such as image-based authentication, encryption, and graphical passwords to protect sensitive customer data. Additionally, it will provide a user-friendly interface that enhances the customer experience and streamlines order processing. The research questions guiding this study include how image-based authentication can improve security and usability, what key features are necessary for improving order management in small businesses, and how encryption and secure login systems can protect customer data.

The outcomes of the project include a more efficient order management system, improved security through the implementation of image-based authentication, and a user-friendly interface that enhances customer satisfaction.

2. Related Work

This section will explain the literature review on the related topics of authentication, order management system, Open Web Application Security Protocol (OWASP), and comparing similar existing systems.

2.1 Authentication

Authentication verifies a person's claimed identity to ensure secure access to systems and information. Traditional methods like passwords and tokens are being replaced or supplemented by biometric techniques such as fingerprint scanning, facial recognition, and Electrocardiogram (ECG) signals to improve security and convenience [1],[2],[3]. Authentication and authorization work together to keep the website secure. If one is missing, security is weakened. Authentication checks who the user is, but without authorization, the user won't have permission to access certain tasks or pages. Similarly, if only authorization is present without authentication, the user cannot prove their identity to access the site [4].

2.1.1 Password-Based Authentication

Password-based authentication has advanced but continues to face challenges, as users often struggle to remember complex passwords, resorting to weak passwords or memory aids, compromising the security [5]. Traditional text-based passwords are susceptible to attacks such as shoulder surfing, dictionary attacks, and phishing [6].

2.1.2 Image-Based Authentication

Image-based authentication is an advanced and user-friendly approach to securing access to web applications, where users identify themselves by selecting a sequence of images, graphics, or specific points on a grid that serve as their password [7]. One common approach is grid-based authentication, where users create personalized patterns using images. Image-based CAPTCHA plays a crucial role in ensuring that only genuine users interact with a system. It presents users with simple visual challenges, such as selecting specific images or identifying objects, which humans can solve easily but are difficult for bots. This technology effectively distinguishes humans from automated systems, safeguarding against counterattacks like User Datagram Protocol (UDP) floods, which can disrupt networks by overloading traffic or bandwidth [8]. A related system, Cued Click Points, is a cued-recall graphical password method where users click on one point per image in a sequence, with each image depending on the previous click [9]. The click-based scheme faces a common issue called the 'hot-spot' problem, where many users tend to choose the same or similar click points or areas when multiple images are provided [10]. Graphical Image Authentication (GIA) enhances security by requiring users to authenticate themselves through a specific pattern of grid images [11]. Grid-based authentication can enhance the proposed project by providing an intuitive and secure way for users to verify their identity. Instead of entering a traditional password, users click on specific points within a grid of images, which they set up during registration. This method is easier to remember because it uses pictures instead of words or numbers, helping people recall visual patterns more naturally [12]. Overall, grid-based authentication ensures user data and actions stay protected while simplifying the login process by allowing users to select meaningful points on an image, while maintaining enough randomness to prevent attacks [7].

2.1.3 Multi-Factor Authentication

Multi-Factor Authentication (MFA) is a security approach that strengthens the authentication process by requiring users to provide multiple forms of verification before gaining access to a web application. Unlike single-factor authentication, which relies only on something the user knows, like a password, MFA incorporates additional factors to confirm identity. MFA relies on three main principles: (1) knowledge, something that the user knows, like a PIN or password, (2) possession, which is something that the user has, like a mobile phone or token, and (3) inherence where it refers to unique personal traits, such as fingerprints or facial recognition [13]. Multi-factor authentication strengthens security by combining different verification methods [3].

2.2 Open Web Application Security Protocol (OWASP)

The Open Web Application Security Project, or OWASP, is a global non-profit organization that focuses on improving the security of web applications [14]. The OWASP Top 10 is a well-known framework that highlights the most critical security risks to web applications, including vulnerabilities like injection, broken authentication, and sensitive data exposure. It acts as a checklist to ensure website safety and assess the security of web applications [15]. Broken access control is the most exploited vulnerability, as attackers can bypass controls and gain admin rights, allowing them to take over the application. It is crucial to protect login credentials and sessions by using strong passwords, multi-factor authentication (MFA), and automatic logout for

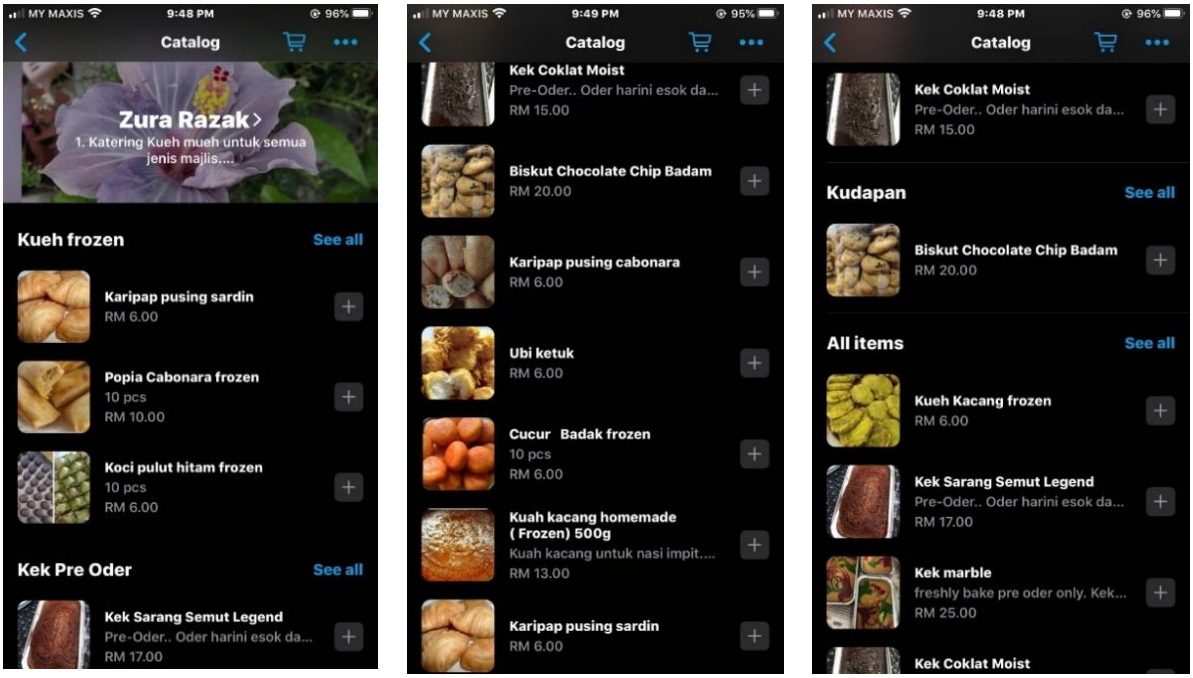
inactive users to prevent unauthorized access [16]. Injection attacks occur when malicious data is sent to a system, often through forms or databases, to execute harmful commands. To protect against these attacks, input validation and sanitization should be used, along with parameterized queries and prepared statements, which treat user inputs as data, not executable code, reducing the risk of SQL injection [17], [18], [19], [20]. Sensitive data, like personal identifiable information (PII), must be protected with encryption to prevent unauthorized access. Strong encryption algorithms like AES should be used to store data securely, and HTTPS should be used for online data transfers to prevent exposure during transmission [21]. A password management policy governs the creation, storage, handling, and transfer of passwords. It sets rules for strong passwords, such as using a mix of letters, numbers, and symbols, and storing passwords securely, such as in a password manager. Encryption should be used when transferring passwords, and regular updates are recommended to maintain security [7].

2.3 Zura Razak Current Management System

Fig. 1 shows Zura Razak Ent's product catalogue. The product catalogue is only accessible through WhatsApp, which means customers need to have Zura Razak's contact to access products and place orders. This can be an inconvenient, lengthy, and tiresome experience, especially for customers who prefer a faster and more convenient way of shopping. Additionally, using WhatsApp alone has some drawbacks, as it is difficult to present the whole range of products in an organized and visually pleasing manner.

From a security perspective, this method is also concerning. Customer orders and personal data shared via WhatsApp are not stored in a centralized, secure system, so they are more exposed to data breaches, miscommunication, or unauthorized access. There is also no official authentication process, so it is harder to verify user identity or protect sensitive transactional data.

Developing a customized online system would address these issues by giving us a more secure, structured, and user-friendly website for browsing and purchasing products. It would also provide us with better data privacy and transaction integrity, significantly improving the customer shopping experience overall.



(a) (b) (c)

Fig.1 *Zura Razak's Products Catalogue*

2.4 Local Pasar

Local Pasar [2] is a website to buy fresh food like fruits, vegetables, and fish directly from local farmers and fishermen. Therefore, it has similar features to the proposed system, which involves an online food ordering system. However, it has several drawbacks compared to the proposed system in terms of security features. For example, Local Pasar does not implement strong password policy. It only asks customers to input the passwords without any validation. Fig. 2 shows the Local Pasar website interfaces.

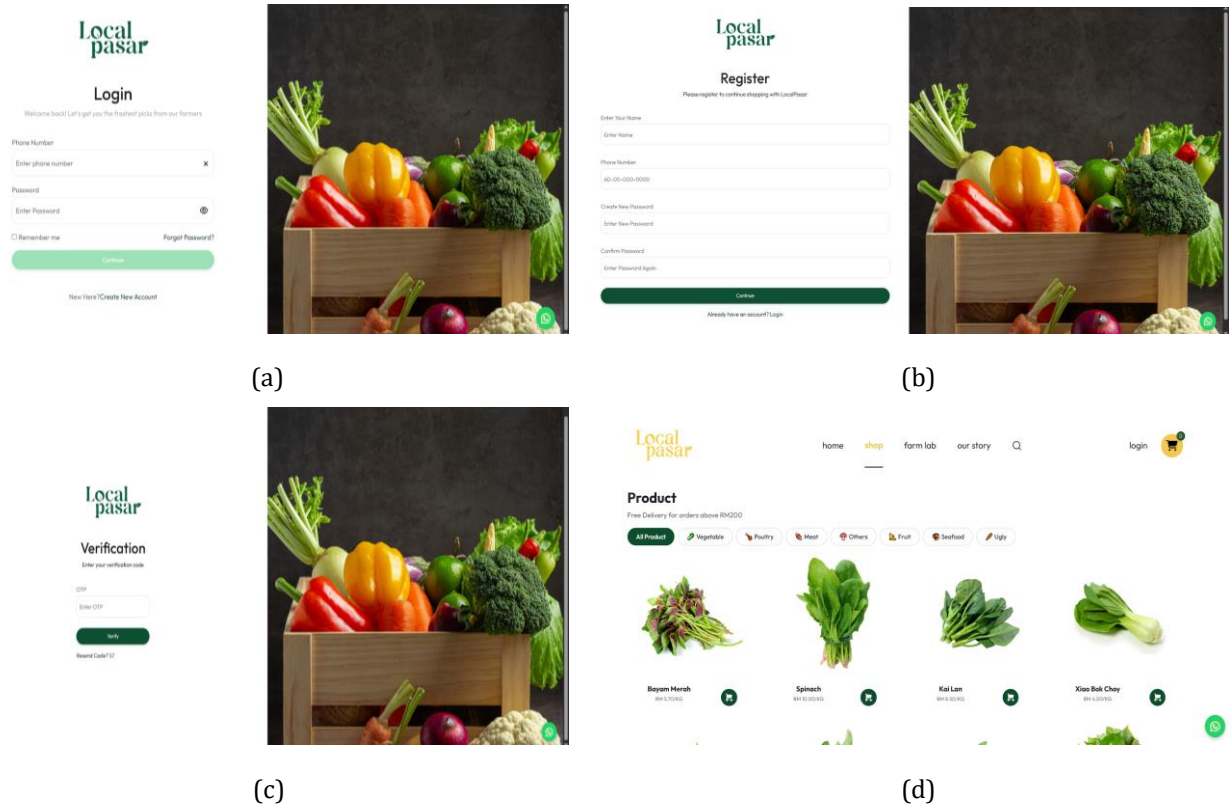


Fig.2 *Local Pasar Interfaces (a) Login; (b) Register; (c) Account Verification; (d) Shopping page*

2.5 Comparison with Existing System

Table 1 shows the comparison between the existing system; current Zura Razak Management System, Local Pasar [22], and proposed System.

Table 1 *Comparison Between Systems*

Characteristics of the System	Zura Razak Current Management System	Local Pasar [22]	Proposed System
Website	×	✓	✓
Login page	×	✓	✓
Strong Password Policy	×	×	✓
Forgot and Reset Password	×	✓	✓
Order Tracking	×	✓	✓
Product Catalogue	✓	✓	✓
Data Encryption	×	NA	✓
Email and Password Login	×	×	✓
Image-Based Authentication	×	×	✓

Zura Razak's management system only provides a product catalogue and takes orders manually through WhatsApp. In contrast, Local Pasar uses a website for online orders, offers order tracking, displays a product catalogue, collects customer emails, and uses One-Time Password for account activation. However, Local Pasar lacks strong password enforcement policy, and email verification. The proposed system will include all these features, except for the location radius setting.

Applied Information Technology and Computer Science Vol. 7 No. 1 (2026) p. 1147-1164

3. Methodology

This section explains the methodology used to develop the Zura Razak Management System, based on the prototype model. The prototype model emphasizes user-centered development. It involves creating an initial version of the system for testing and feedback, helping to clarify requirements and reduce errors. This flexible approach ensures the system aligns with user needs and is easy to use. Fig. 3 shows the prototype model to be used in this proposed system.

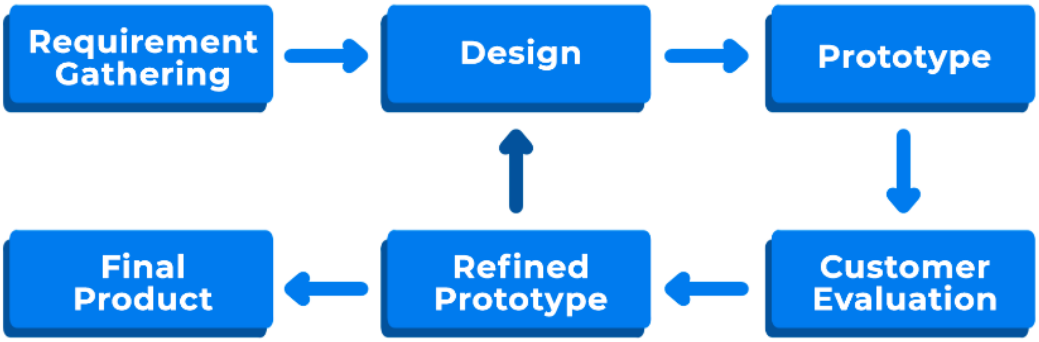


Fig. 3 *Prototype Model [23]*

Requirements are gathered to identify Zura Razak Ent. issues, project goals, and security needs. Interviews with the business owner helped establish a plan for creating a secure and efficient system focused on customer order management. Next, system designs, including sketches and diagrams, are created using tools like Canva. Key pages such as login, product catalog, and order placement are outlined. Database diagrams are also developed to ensure smooth data flow and secure storage. It then proceeds with building the prototype. A working prototype is built using PHP, MySQL, HTML, and CSS, incorporating features like secure login and order management. Mock data is used to test functionality and ensure the prototype meets requirements. The prototype undergoes User Acceptance Testing (UAT), where feedback on usability and functionality is collected. Issues or improvements are identified to refine the system further. Improvements are made based on feedback addressing usability and security issues. Enhanced features like encryption and navigation are added. The process repeats until the prototype meets expectations. The final system includes all required features, such as image-based authentication, secure order tracking, and safe transactions. Rigorous testing ensures functionality and security before deployment.

4. System Analysis and Design

This section outlines the analysis and design process for developing the Zura Razak Management System. It provides an overview of the system development workflow, details the functional and non-functional requirements, and elaborates on the system analysis and system design.

4.1 System Requirements

The purpose of conducting a system requirement analysis is to clearly define and understand the needs and expectations for the system to be developed. This analysis helps ensure that the system meets both the functional and non-functional requirements of the stakeholders, such as Zura Razak Ent., and customers. Table 2 and Table 3 shows the functional requirements and non-functional requirements.

Table 2 *Functional Requirement Analysis*

Module	User	Description
Login	Admin	Logs in using a username and password to management features.
	Customer	Logs in using a username and password, followed by image-based authentication to access basic features like browsing products, viewing orders, and placed an order.
Register	Customer	Filled in personal details and registered the username, password, confirmed password and selected one of the images and click on any one grid within the chosen image.
Product Catalogue	Admin	Manages the product list by adding, updating and removing the product.
	Customer	Browse through the product catalogue, view product details (e.g., description, and price), and place orders for available items.

Table 2 *(cont.)*

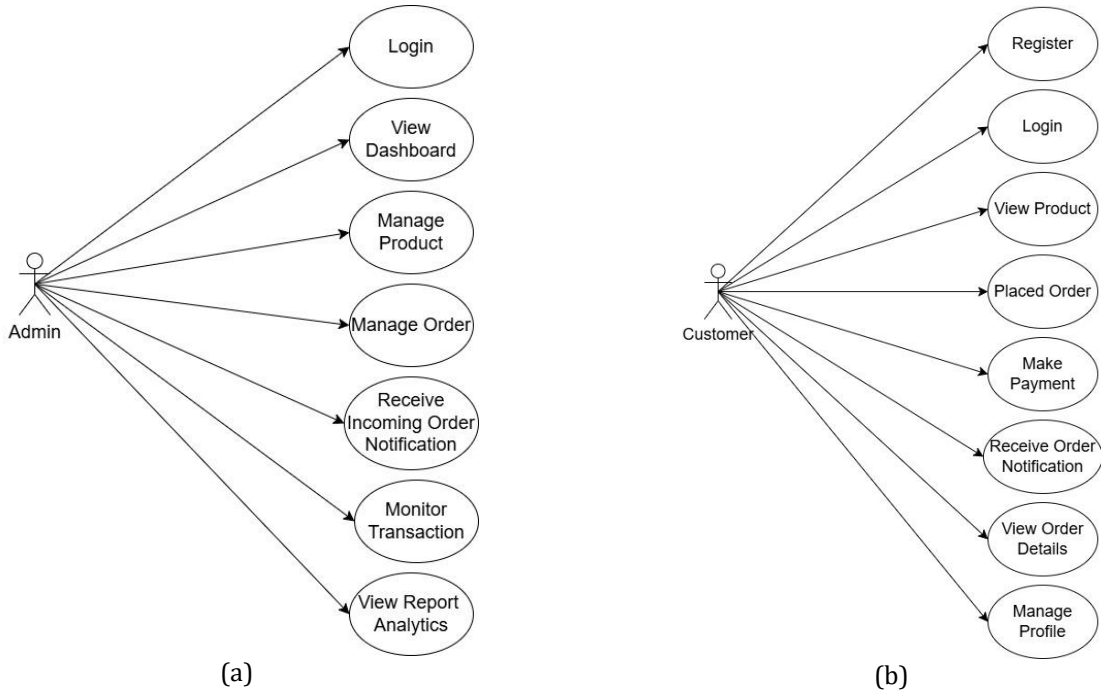
Module	User	Description
Order Management	Admin	Captures new orders from customers, updates order status (e.g., pending, dispatch, completed) and processes payments and ensures order fulfillment.
	Customer	Place new orders, select products, and specify quantities, track the status of their orders (e.g., pending, dispatch, or, completed).
Notification	Admin	Upon a customer's order placement, receive email order notification. This email contains the order details, enabling the admin to efficiently manage and process the order. It also allows admin to response to customer feedback and make it public.
	Customer	Receive email notification with the order details informing the customer's order has been received and is being processed.
Sales Report	Admin	Views detailed sales reports, tracking which products are selling the most and identifying peak sales periods.

Table 3 *Non-Functional Requirements*

Non- Functional Requirement	Description
Performance	The system should load quickly.
Security	The system must protect sensitive data, like passwords and ensure confidentiality of user and the orders information.
Usability	The system should be easy to use, with a simple design and clear options for both admins and customers.
Operational	The system should be accessible when an internet connection is available.

4.2 System Analysis

Fig. 4(a) shows the use case diagram for admin. It shows that the admin is able to interact with the system by logging in to system, then can view the dashboard, manage product, receive incoming order notification, manage order, monitor transaction, and view report analytic. Meanwhile Fig. 4(b) shows the use case diagram from customer. It enables the customer to use the system by registering their account, and logging to the system with their login credential. Hence, they can view the product page, placed an order, make payment, receive order notification, view their order details, and manage their profile.



(a) (b)

Fig. 4 *Use Case Diagram (a) Admin; (b) Customers*

Applied Information Technology and Computer Science Vol. 7 No. 1 (2026) p. 1147-1164

Fig. 5 illustrates the admin's process flow within the Zura Razak Management System, beginning with account registration and login, where their role is identified as "admin" under the User class. After authentication, the admin accesses the dashboard to perform key tasks such as managing product items by adding, editing, disabling active status, or checking availability. The admin also handles order processing through the Order class by updating order status and viewing customer activity. Additionally, the admin generates and views sales reports through the Sales Report class, which summarizes total quantity sold, revenue, and category breakdowns. These interactions emphasize the admin's essential role in managing and maintaining the system.

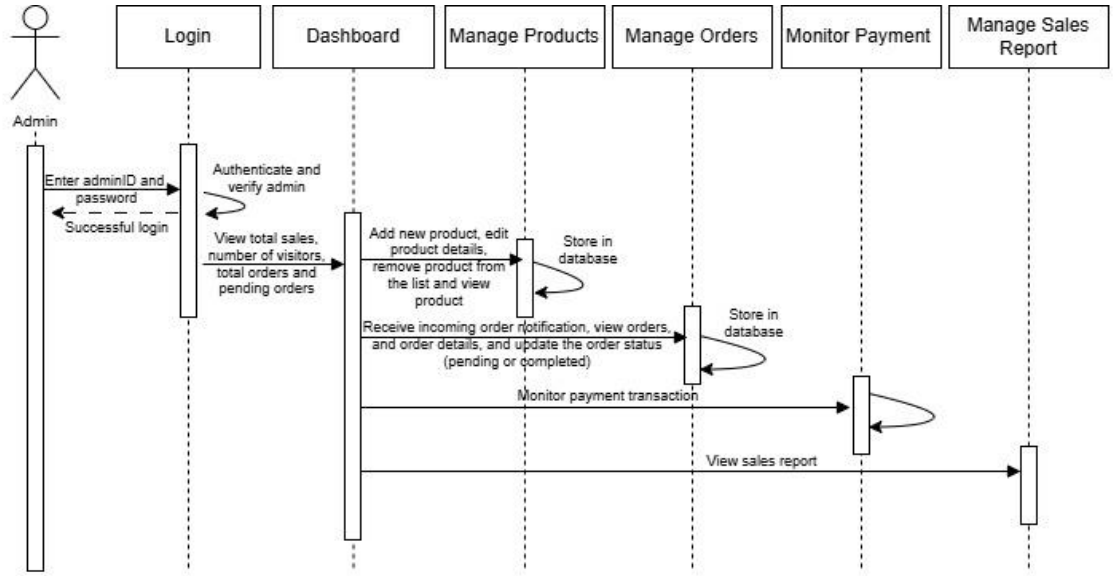


Fig. 5 *Sequence diagram for admin.*

Fig. 6 outlines the customer's journey within the Zura Razak Management System, starting with login and authentication. After logging in, customers can browse and view product details managed under the Product class, including product description and product reviews. Selected items are added to the cart and can proceed to checkout, where the total amount is calculated, and payment is completed via a payment gateway, supporting method like credit card or debit card. Upon successful payment, the system sends a notification confirming the order. Customers can also view order status and update their profile, ensuring a smooth and secure shopping experience.

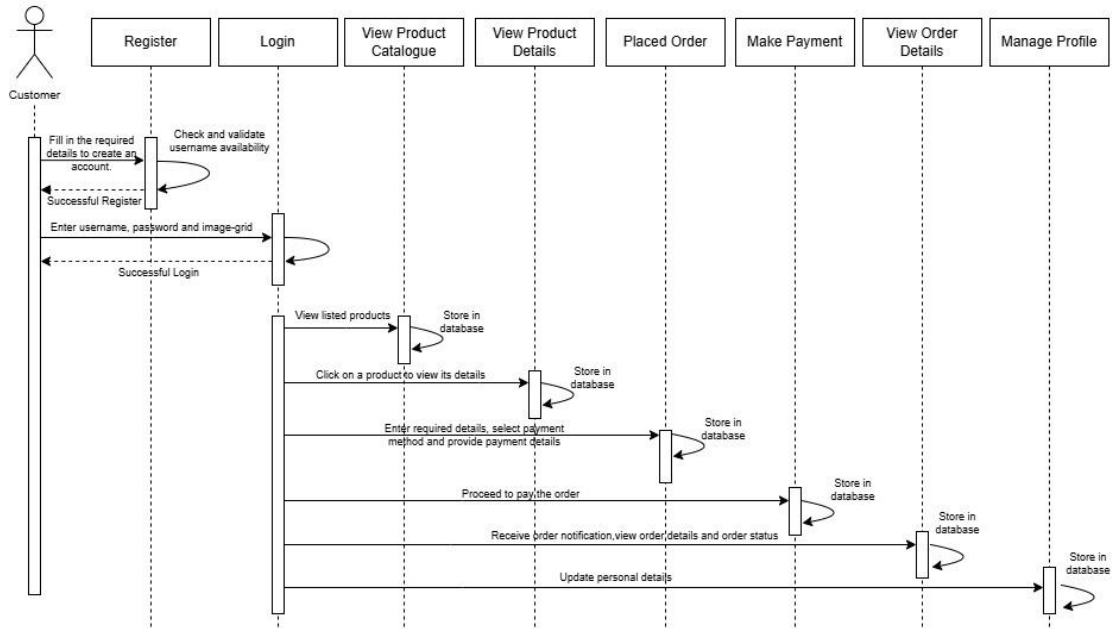


Fig. 6 *Sequence diagram for customer.*

Fig. 7 shows the class diagram for Zura Razak's management system, illustrating how key components like users, orders, products, and payments are connected. It defines the database structure, showing how customers place orders, make payments, leave reviews, and receive notifications, while the system also handles login attempts and admin messages for better security.

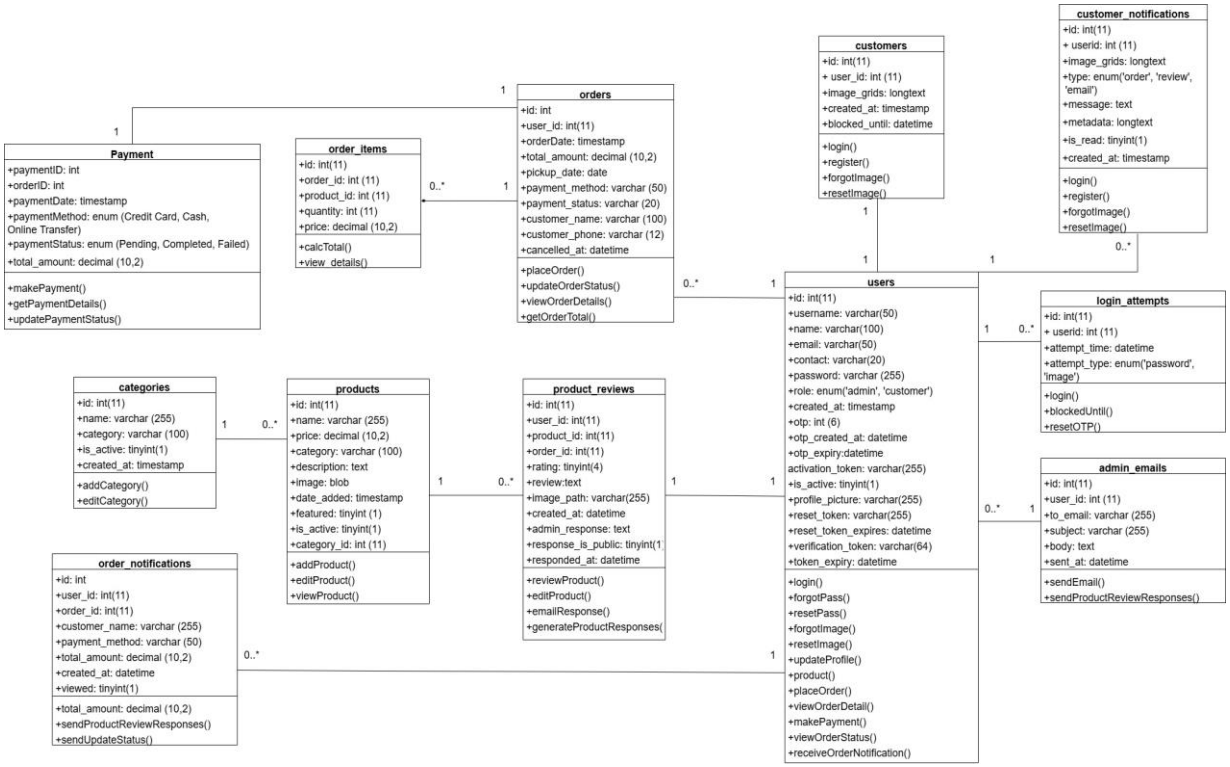


Fig. 7 *Class Diagram*

4.3 System Design

Fig. 8 shows the system architecture for Zura Razak Management System. It shows how Zura Razak Management System is set up and how its components work together. Customers must register and verify their accounts using image-based authentication before logging in, ensuring only authorized users can access the system. Once logged in, customers can browse products, place orders, make payments, and receive order confirmation emails. On the admin side, authorized users can log in, view the dashboard, manage products, monitor orders and transactions, and get notified of new orders. All activities are connected to the database for data storage and updates, ensuring smooth and secure system operations.

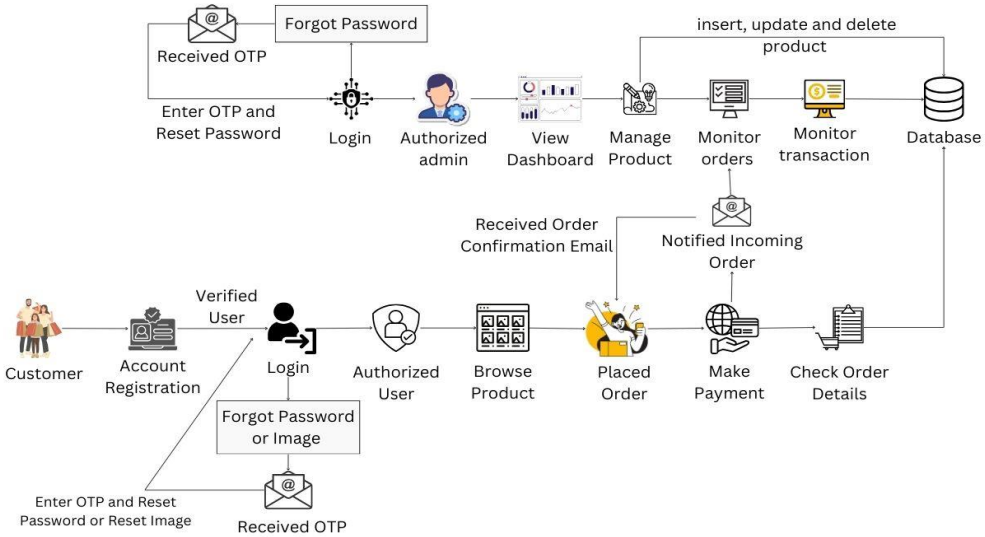


Fig. 8 *System Architecture*

Applied Information Technology and Computer Science Vol. 7 No. 1 (2026) p. 1147-1164

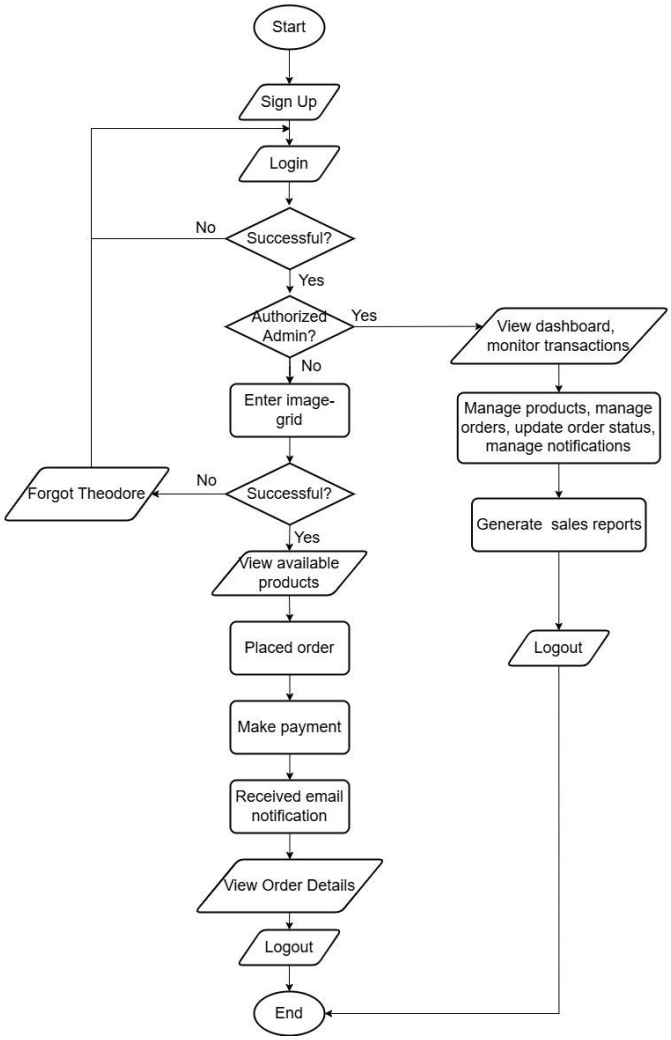


Fig. 9 *Flowchart for Zura Razak Management System*

Fig. 9 illustrates the flowchart of Zura Razak Management System, showing the steps taken by both customers and admins from start to end. The process begins with user registration (Sign Up) followed by Login. If login is successful, the system checks whether the user is an authorized admin. Admins are directed to the admin panel where they can view the dashboard, monitor transactions, manage products, orders, and notifications, and generate sales reports before logging out. For regular customers, login is followed by image-grid authentication to ensure secure access. If the image-grid verification fails, users are temporarily blocked for 3 minutes after three failed attempts. If successful, customers can then browse products, place orders, make payments, and receive an email confirmation. Afterward, they can view order details and log out, completing the process. This flowchart emphasizes both security image-based authentication and role-based access, ensuring smooth and secure navigation for both customers and admins.

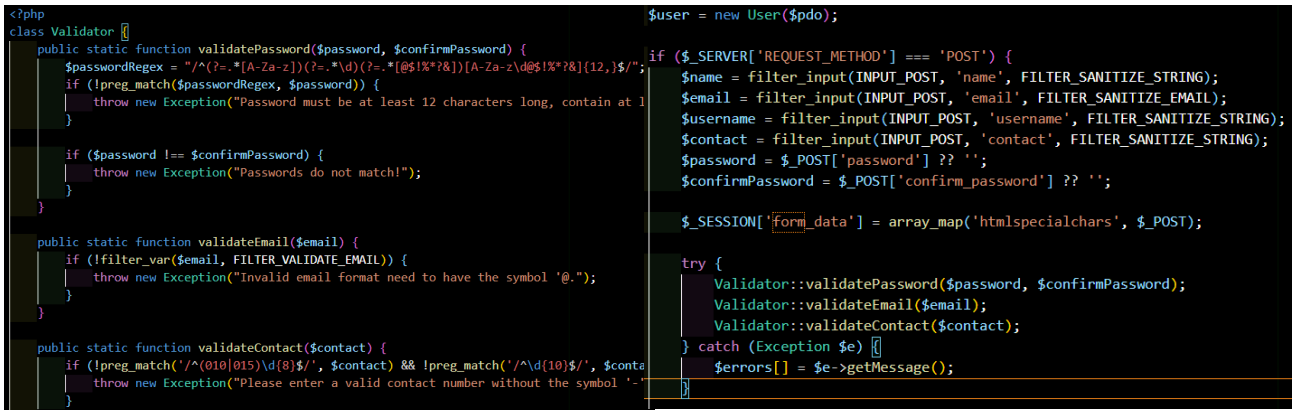
5. Implementation

This section provides a detailed discussion on the implementation of the security modules, user modules, and admin modules, as well as the overall functionality of the Zura Razak management system. It highlights how each module contributes to the system's performance, usability, and security.

5.1 Secure Module Implementations

This section will further discuss the implementation of security module in the system. There are several techniques implemented including data sanitization, data validation, strong password policy, Cross-Site Request Forgery (CSRF), and email verification. The system keeps user data safe by checking and cleaning all inputs. For example, emails, passwords, and contact numbers are checked to make sure they are in the correct format. It also removes any harmful content using built-in PHP filters. Passwords must be strong at least 12 characters long and include upper and lowercase letters, numbers, and symbols. This is shown in Fig. 10 When uploading files like profile pictures, only certain file types are allowed (like JPEG or PNG), and large files are blocked. The

system also checks emails before sending, using secure methods. To protect from fake requests Cross-Site Request Forgery(CSRF), special tokens are used and refreshed often. User sessions are handled safely by clearing data on logout and timing out if inactive for 30 minutes. Any information shown on the website is escaped to stop script attacks. Passwords are never stored as plain text as it is are safely hashed. These steps help keep the system secure from common attacks and protect user information.



(a) (b)

Fig. 10 *Secured the input through (a) Input validation; and (b) Input Sanitization*

Fig. 10 Securing Input by (a) Input Validation and (b) Input Sanitization shows how the system protects itself from hostile data inputs. Input validation is used to check that all inputs from users are in the correct format, e.g., email addresses are valid or compulsory fields aren't empty. Input sanitization is used for cleaning the data by removing or escaping any undesirable characters, thus inhibiting attacks like SQL injection or cross-site scripting (XSS). Both techniques in conjunction with one another ensure that only safe and suitable data is accepted by the system.

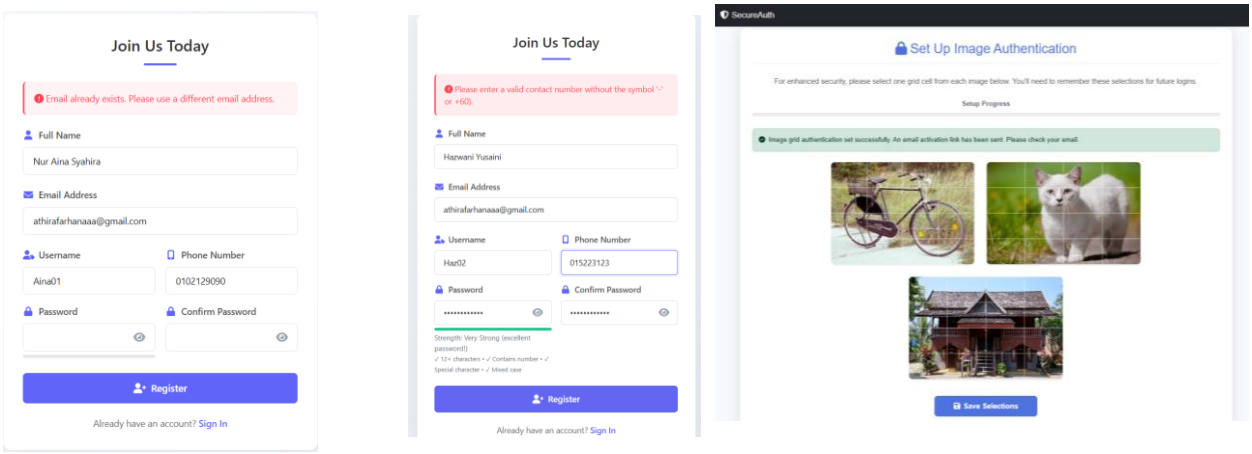
(a) (b)

(c) (d)

Fig. 11 *Image Authentication Implementation (a) Retrieve Image Grid; (b) Authentication Success of Not; (c) Limit Attempt; (d) Shuffle Image Positions*

Fig. 11 shows the Image Authentication Implementation on how the system uses image-based login for added security. When a customer logs in, the system retrieves the images they selected during registration, each divided into a 4x4 grid. The customer must click on the same grid areas they previously chose. After the selections are made, the system checks whether they match the data saved. If the selections are correct, the login is successful; otherwise, a failure message is shown. To protect against repeated guessing, the system limits the number of login attempts up to 3 three times only. If the customer fails all attempts, further access is blocked for 3 minutes for safety. Additionally, the system shuffles the positions of the images and grid tiles during each login attempt to prevent patterns from being memorized or guessed easily by others.

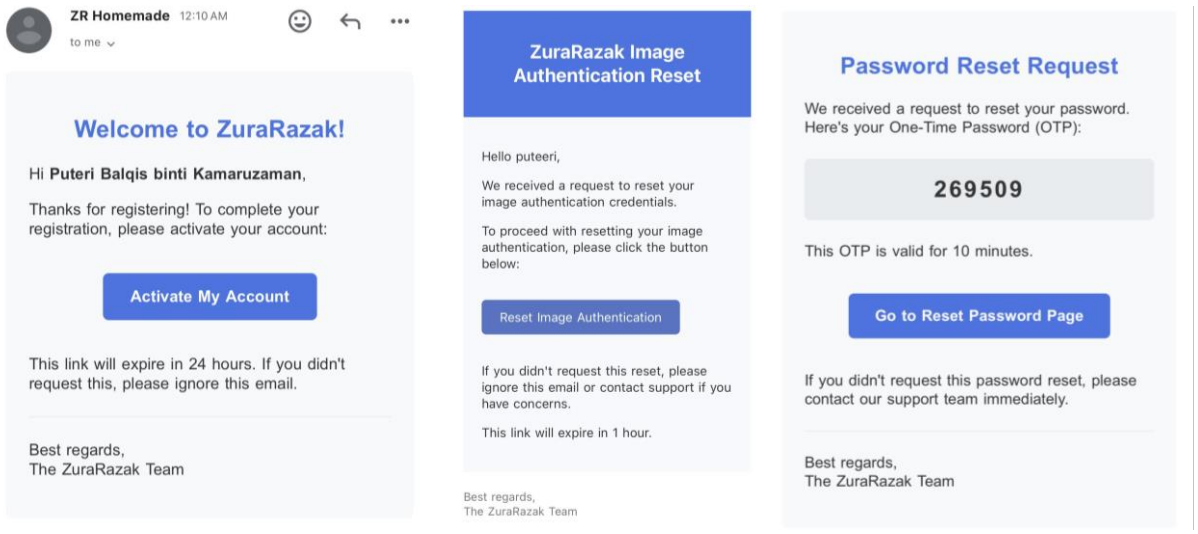
Applied Information Technology and Computer Science Vol. 7 No. 1 (2026) p. 1147-1164



(a) (b) (c)

Fig 12. *Customer Register Interfaces with (a) Input Validation; (b) Email Validation; (c) Image Authentication Setup*

Fig. 12 shows three key steps in the customer registration process where (a) shows the error message that required the users to input other email during the registration as confirmation email will be sent to the customers for activation and verification.



(a) (b) (c)

Fig.13 *Email Notifications (a) Account Activation; (b) Reset Image Authentication; (c) Password Reet Request*

Fig. 13 shows emails sent to customers for account security where After signing up, they get an account activation email to confirm their email address. If they forget their image-based login pattern, they receive an email to reset their image authentication. If they forget their password, a password reset email is sent with a link to create a new one. These emails help keep the account safe and easy to access.

5.2 Implementation of Customer Module

The customer module contains all the important steps that allow users to register, login, browse products available to them, place orders, and manage their accounts. During the registration process, the users fill out their personal details, confirm their email and finally establish image-based authentication for a more secure way of logging in. Once the user logs in to the system successfully, they can view the products available to browse through, add selected items to their cart, use the Stripe payment gateway for checkout, and monitor the orders they place. Customers can update parts of their profiles, reset their passwords, or even reset their image-based authentication option. The module is designed with ease of use and protection in mind. The end goal is to provide users with an easy yet secure shopping experience.

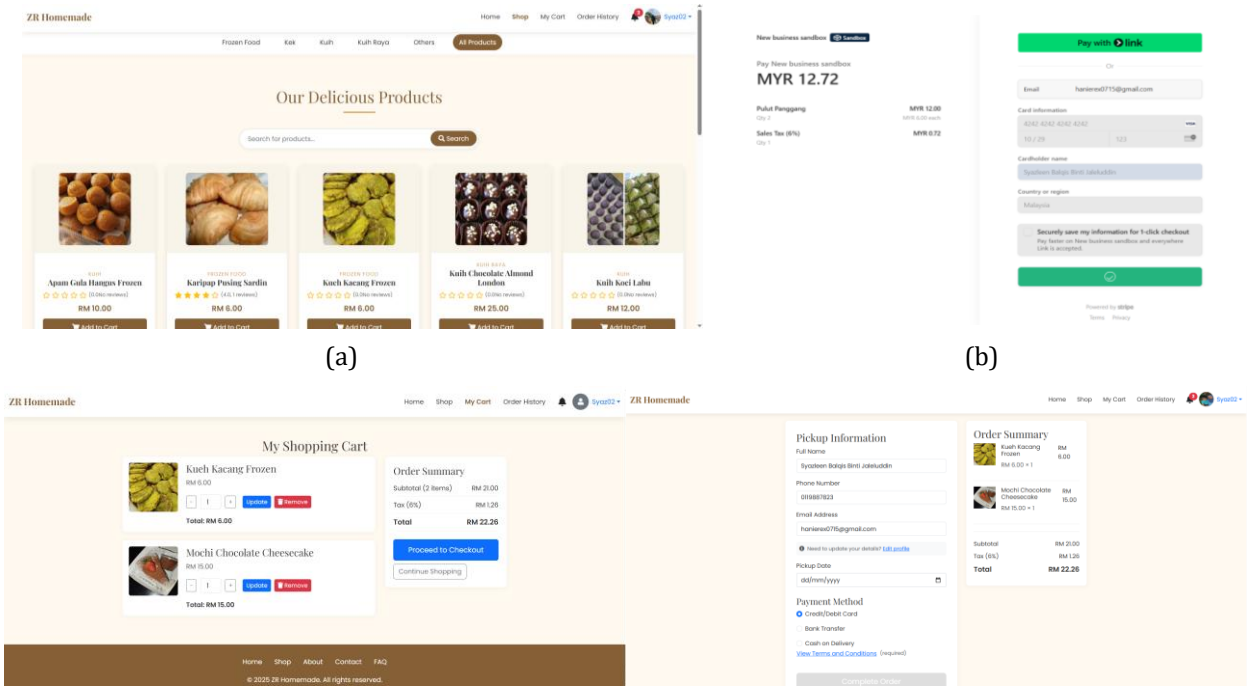


Fig. 14 *Customer Interfaces for (a) Shopping; (b) Payment Gateway; (c) Cart Interface; (d) Checkout Interface*

The customer shopping and payment screens are displayed on Fig. 14. The shopping screen provides customers with options to go through items, place items in their cart, and change their selections. The payment screen shows them the total price and the payment gateway. Both screens allow users to buy and checkout with ease in a simple and smooth way.

5.3 Implementation of Admin Module

The Admin Module supports admins in managing and administering the system in an easy-to-use environment. The module includes a dashboard that provides sales and users statistics, navigate to manage Order and Products, and notification functionality with important updates to the admin. In addition, the module generates reports for sales. The Admin module ultimately simplifies running and managing your business.

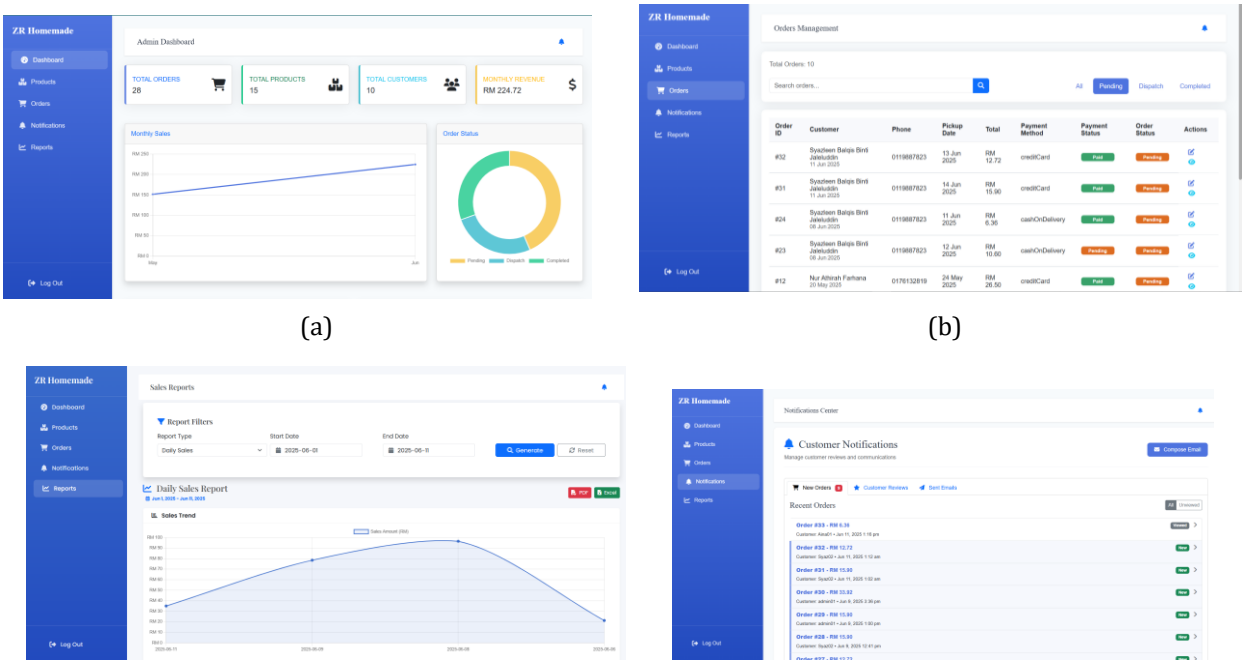


Fig. 15 *Admin Interfaces for (a) Dashboard; (b) Orders Management*

Fig. 15 illustrates the admin interfaces for (a) Dashboard, which provides general information on total products and sales performance, and (b) Orders Management page where administrators can effectively track, process, and update their customer orders., (c) Sales Reports page which allows admin to generate reports based on yearly, monthly, weekly, daily, sales performance, or product performance, (d) Notification page is to allow admin to see any new orders, review the feedback from the customers and send emails to the customers . The admin interfaces will facilitate back-end functions and assist with administrative management.

6. Results and Discussion

The evaluation results of the proposed system are summarized in this section. There are two types of evaluation results provided, the test plan result and the user acceptance result. The evaluation phase involved the complete system and interest in evaluating security and confirming that the project specifications for the system had been delivered.

6.1 Test Plan Result

The successful implementation of our test plan has produced complete results, summarized in two areas. As seen in Table 4, the outcomes of our extensive functionality testing established that all features of the system worked as intended, while achieving the required user expectations. While the results are summary, Table 5 gives explicit reference to the security test plan, in which a primary purpose was to carefully ascertain the level of effectiveness for every security method built into the system. This portion of the testing plan was paramount in understanding how strong the protections we had put in place and each of the contributions made toward security.

Table 4 *Testing Results Table*

Checklist	Expected result	Actual Result
Register- All required fields are in the correct format.	Registration is successful and redirects to image authentication page.	Pass
Login - Correct username and password (admin).	Login successfully and redirect it to admin dashboard.	Pass
Login- Correct username, password image-grid (customers).	Login successfully and redirect to customer homepage.	Pass
Forgot Password or Image - Enter email and username and click submit	**Displays message:** "Password reset link sent."	Pass
Reset Image – Enter OTP sent, new selected image-grid.	**Displays message:** "Image successfully reset!	Pass
Profile - Update information and save.	**Displays message:** "Profile updated successfully."	Pass
Place Order - Add products to cart and confirm order.	**Displays message:** "Order placed successfully."	Pass
Payment - Complete payment	**Displays message:** "Payment successful."	Pass
Product - Add new product/ update product onto the product list.	**Displays message:** "Product added/updated successfully.	Pass
Order – View lists of orders and order details	Displays the lists of all orders and the order details	Pass

Table 5 *Security Test Plan Results Table*

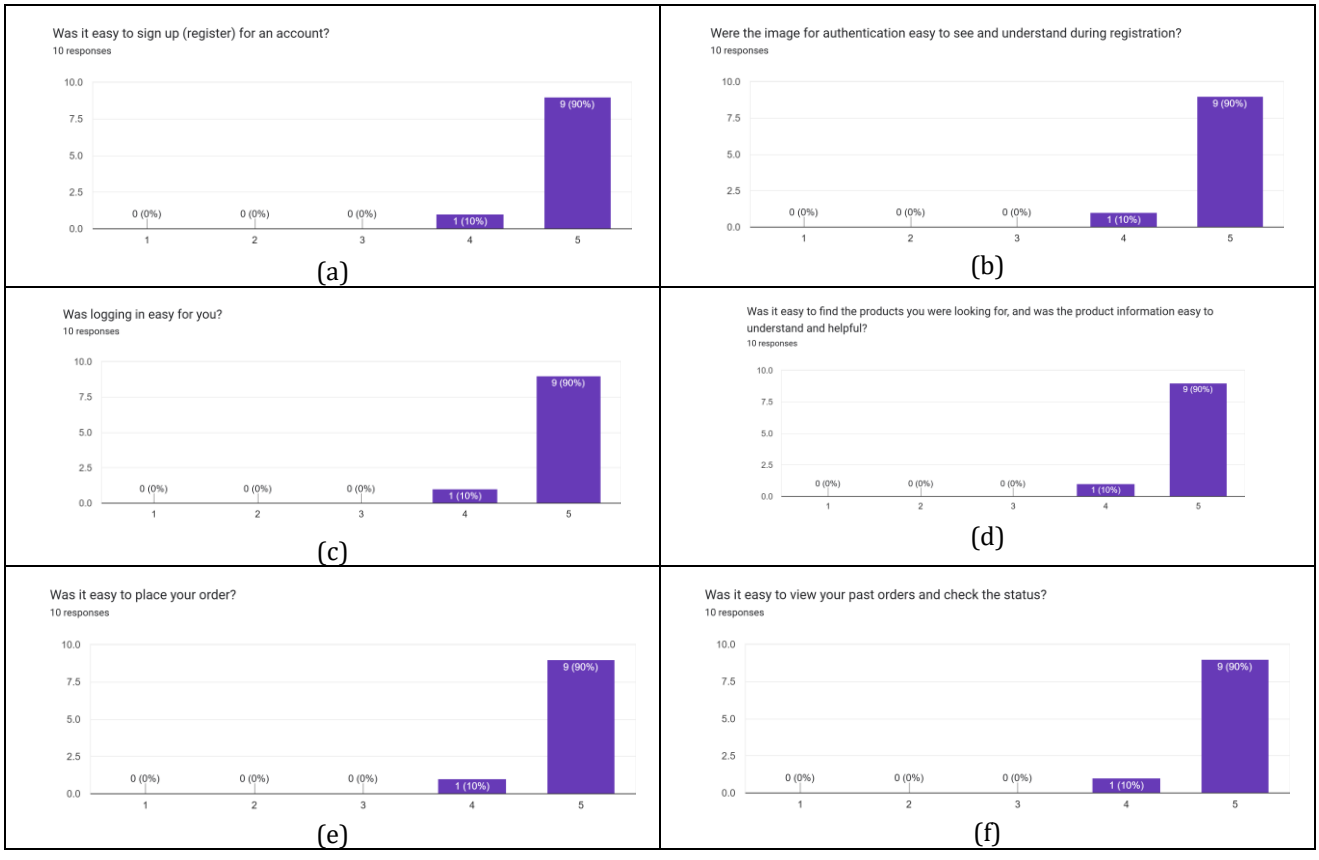
Checklist	Expected result	Actual Result
Admin and customer roles are directed correctly during login.	Proper implementation of user authentications.	Pass
Login requires valid credentials.	Only valid users can access the system.	Pass
Passwords are obscured during input.	Passwords are hidden in the text field.	Pass

Table 5 *(Cont.)*

Checklist	Expected result	Actual Result
Forgot Password or Image - Enter email and username and click submit	**Displays message:** "Password reset link sent."	Pass
Image-based authentication is required for customer login.	Customer selects the image-grid during login, matching the image-grid selected during register.	Pass
Sessions are terminated after logout.	User sessions are destroyed preventing the user from going back to the previous page.	Pass
Input fields enforce specific format for email, phone number, and password.	Field validation prevents invalid inputs.	Pass
System encrypts sensitive data like passwords	Password is securely stored in hashed and salted.	Pass
Session's timeout implemented after 30 minutes of inactivity	Redirect the user to the login page after 30 minutes of inactivity.	Pass

6.2 User Acceptance Test (Customers Module)

Fig.16 (a)-(j) are the findings of the user acceptance test for the customers module. The purpose of conducting this test was to determine the experience of customers interacting with the system. The testing involved evaluating each of the features identified in the customers module. The testing involved 10 customers of Zura Razak.



(a) (b) (c) (d) (e) (f)

Applied Information Technology and Computer Science Vol. 7 No. 1 (2026) p. 1147-1164

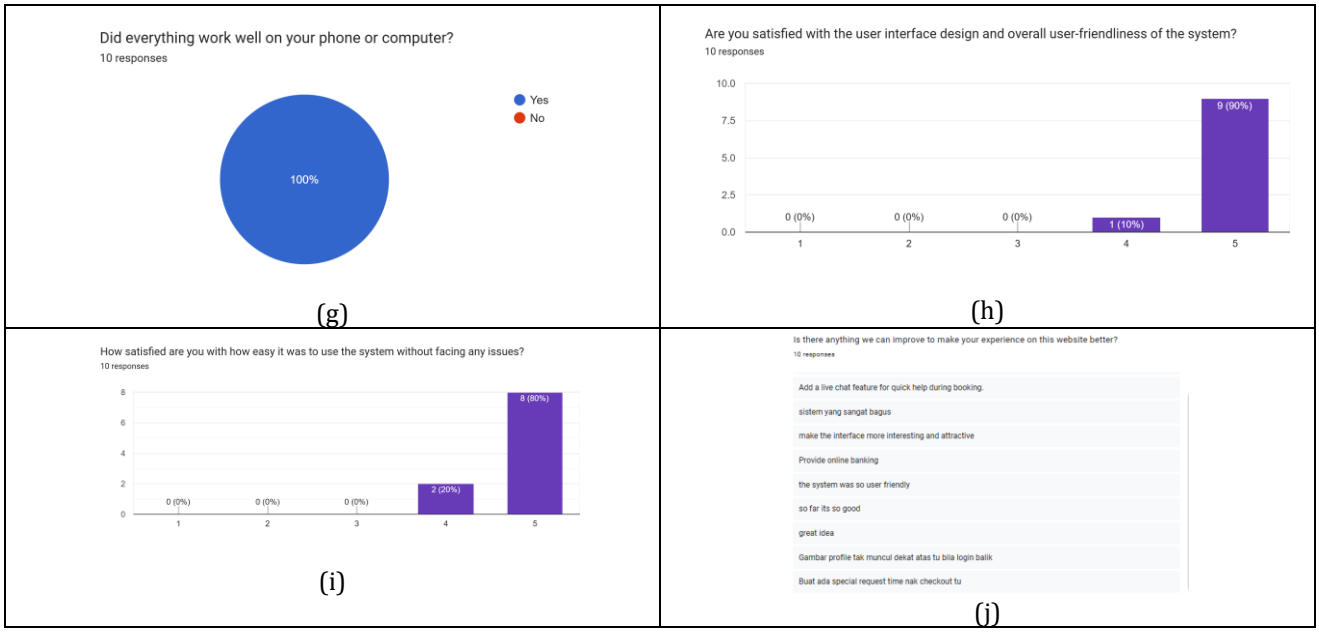


Fig. 16 *Results of User Acceptance Test for Customers (a); (b); (c); (d); (e); (f); (g); (h); (i); (j)*

The User Acceptance Test (UAT) for the Customers Module evaluated key aspects such as usability, functionality, and overall user satisfaction. Feedback was gathered on a 5-point scale for major features where 5 is Very Satisfied and 1 is Very Not Satisfied, while device compatibility was assessed through a yes/no response. Results indicated overwhelmingly positive responses across most areas.

In the registration process in Fig. 16(a), 90% of users rated their experience as "Very Satisfied" (5/5), and the remaining 10% selected "Satisfied" (4/5), suggesting that the process is highly effective with room for minor improvements. Similarly, the image authentication feature based on Fig. 16(b) received no negative feedback, and users reported smooth and secure functionality, indicating the system's security features are working as intended. The Fig. 16(c) which is login process mirrored the registration feedback, with 90% "Very Satisfied" and 10% "Satisfied", pointing to a seamless experience overall with slight potential for refinement.

When it came to Fig. 16(d) product search and information clarity, 90% expressed top satisfaction, while the remaining 10% gave slightly lower ratings, highlighting opportunities to improve filters or enhance product descriptions. The Fig. 16(e)order placement process also received high praise, with 90% very satisfied and 10% satisfied, though further streamlining the checkout process could improve usability for all users. For order history and tracking based on Fig. 16(f), most users were very satisfied with visibility and tracking capabilities, though feedback suggests enhancing status notifications for even greater clarity.

Notably, mobile and desktop compatibility earned a perfect score, with 100% of users based on the Fig. 16(g) confirming flawless functionality across devices, demonstrating strong responsiveness and adaptability. However, based on Fig. 16 (h), the UI satisfaction received varied ratings, with 90% of users indicating they were "Very Satisfied" and 10% "Satisfied". While the majority found the design effective, this variation still points to differing preferences and highlights the importance of refining the UI to better meet all user expectations. Regarding the overall experience, 90% of users rated it as "Very Satisfied", while 10% selected "Satisfied", suggesting the system is highly user-friendly and effective, with only minor issues reported and no critical flaws identified.

Based on the suggestion on Fig 10 (j), user suggestions for improvement centered on introducing live chat support, enhancing UI/UX design, and providing training materials. Positive feedback emphasized the platform's user-friendliness and innovative approach. Based on these findings, it is recommended to prioritize the implementation of real-time support, targeted design enhancements, and workflow refinements. Meanwhile, existing strengths such as cross-device compatibility and seamless login and registration should be maintained. In conclusion, the Customers Module has exceeded expectations in its core functions, and addressing a few specific areas will help deliver an even more exceptional user experience.

In summary, the Customers Module performs well, with strengths in login, order placement, and cross-device functionality. However, UI enhancements, better search filters, and added support features like live chat could further elevate the user experience. The next steps should focus on addressing these areas to ensure continued satisfaction and usability.

6.3 User Acceptance Test (Admin Module)

Fig. 17 are the findings of the user acceptance test for the admin module. The purpose of conducting this test was to determine the experience of the admin interacting with the system. The testing involved evaluating each of the features identified in the admin module.

No.	Questions	Result				
		Very Dissatisfied (1) – Very Satisfied (5)				
Login Module						
1.	Admin can login without issues.					/
2.	Readable text field and masked password.					/
Product Module						
3.	Admin can view product inventory.					/
4.	Admin can add new products, update products and set the availability of the product into inventory.					/
Order Module						
5.	Admin can receive customers' orders.					/
6.	Admin can view customers' orders.					/
Payment Module						
7.	Admin can monitor payment transactions.				/	
Notification Module						
8.	Admin can receive incoming email order notification.					/
9.	Admin can respond to the reviews and choose to make it public or not.				/	
Sales Analytic Module						
10.	Admin can generate sales reports easily through PDF or Excel.					/
Overall System						
11.	Navigation buttons function properly.					/
12.	The system is easy to use.					/
	Recommendations: - Tukar the colour of website to make it more interesting - Buat boleh link ke whatsapp - Nak ada boleh block tarikh - Kalau nak send email tu, ada senarai email customer senang nak pilih2 - Rating star tu bagi nampak cantik sikit					

Fig. 17 *User Acceptance Test Results for Admin*

7. Conclusion

Zura Razak Management System is a web-based platform that is user-friendly, secure, and designed to replace manual processes to improve day-to-day operations. It allows customers to browse products, place orders, make payments using credit card, debit card, or cash, receive email notifications, view order history, and update their profile anytime. The system features image-based authentication for customers, offering an easy-to-remember and more secure alternative to passwords. Passwords are encrypted and salted for enhanced data protection.

Admins can respond to customer reviews and choose which to publish. They also have access to a mobile-responsive admin dashboard with sales report generation by day, week, month, and year, as well as sales

analytics. The admin panel allows for easy management of orders, products, and categories. The system is fully responsive, giving users convenient access anytime, anywhere.

However, there are some limitations in the current system. The payment methods are limited to credit card or debit card, or cash only, with no support for e-wallets or online bank transfers. Additionally, the Zura Razak Management System does not include integrated delivery or shipping functionality. All orders must be collected manually by the customer or arranged externally. The system does not capture delivery addresses, offer courier options, or provide order tracking. This limits the end-to-end convenience for customers who prefer doorstep delivery.

To further enhance the system in the future, features such as CAPTCHA to prevent brute-force attacks, admin change and action logs to track system updates, live chat support for instant help, a wishlist feature for saving favorite items, additional payment methods like e-wallets and bank transfers, and automatic invoice generation and download after payment can be introduced. These improvements would enhance system security, improve customer experience, and streamline business operations.

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.

Author Contribution

This journal requires that all authors take public responsibility for the content of the work submitted for review. The contributions of all authors must be described in the following manner:

The authors confirm contribution to the paper as follows: ***study conception and design:*** *N. A. F. Mohd Hisham, N. Z. Harun;* ***analysis and interpretation of results:*** *N. A. F. Mohd Hisham, N. Z. Harun;* ***draft manuscript preparation:*** *N. A. F. Mohd Hisham, N. Z. Harun. All authors reviewed the results and approved the final version of the manuscript.*

References

[1] M. Pooshideh *et al.*, "Presentation Attack Detection: A Systematic Literature Review," *ACM Comput Surv*, p., 2024, doi: 10.1145/3687264.

[2] M. Hammad, P. Plawiak, K. Wang, and U. Acharya, "ResNet-Attention model for human authentication using ECG signals," *Expert Syst*, vol. 38, p., 2020, doi: 10.1111/exsy.12547.

[3] I. Velásquez, "Framework for the Comparison and Selection of Schemes for Multi-Factor Authentication," *CLEI Electron. J.*, vol. 24, p., 2021, doi: 10.19153/cleiej.24.1.9.

[4] P. Pant *et al.*, "Authentication and Authorization in Modern Web Apps for Data Security Using Nodejs and Role of Dark Web," *Procedia Comput Sci*, vol. 215, pp. 781–790, 2022, doi: https://doi.org/10.1016/j.procs.2022.12.080.

[5] A. Kaur and K. Mustafa, "A Critical appraisal on Password based Authentication," *International Journal of Computer Network and Information Security*, p., 2019, doi: 10.5815/IJCNIS.2019.01.05.

[6] S. A. Sharna and S. A. Ali, "Image Based Password Authentication System," *ArXiv*, vol. abs/2205.12352, p., 2022, doi: 10.48550/arXiv.2205.12352.

[7] S. kapoor, A. Tomar, S. Gupta, R. Kumar Singh, and C. Author, "Enhancing User Privacy And Security Through Image Based Authentication Technique, Educational Administration: Theory and Practice," vol. 2024, no. 5, pp. 11002–11011, 2024, doi: 10.53555/kuey.v30i5.4877.

[8] A. O. Adesina, P. S. Ayobioloja, I. C. Obagbuwa, T. J. Odule, A. A. Afolorunso, and S. A. Ajagbe, "An Improved Text-Based and Image-Based CAPTCHA Based on Solving and Response Time," *Computers, Materials and Continua*, vol. 74, no. 2, pp. 2661–2675, 2023, doi: 10.32604/cmc.2023.031245.

[9] S.Geetha, V.Ranjani, S.Gowthami, and R.Selvarathi, "Click-Based Graphical Password Scheme Using Cued Clicks," 2015. [Online]. Available: https://api.semanticscholar.org/CorpusID:212452147

[10] Y. Meng, "Designing click-draw based graphical password scheme for better authentication," in *Proceedings - 2012 IEEE 7th International Conference on Networking, Architecture and Storage, NAS 2012*, 2012, pp. 39–48. doi: 10.1109/NAS.2012.9.

[11] R. K, T. Bala, S. R, and S. N, "Authentication By Grid Image Pattern," *Int J Res Appl Sci Eng Technol*, p., 2022, doi: 10.22214/ijraset.2022.43658.

[12] K. Pandey, A. Singh, A. Anand, A. Kaushik, and S. N. Gupta, "Enhancement of Password Authentication System Using Vector (Graphical) Images," *2023 International Conference on Artificial Intelligence and Smart Communication (AISC)*, pp. 255–260, 2023, doi: 10.1109/AISC56616.2023.10085057.
[13] R. Saqib *et al.*, "Analysis and Intellectual Structure of the Multi-Factor Authentication in Information Security," Dec. 2021.
[14] OWASP, "OWASP Developer Guide - Introduction," owasp.org.
[15] M. A. Helmiawan, E. Firmansyah, I. Fadil, Y. Sofivan, F. Mahardika, and A. Guntara, "Analysis of Web Security Using Open Web Application Security Project 10," *2020 8th International Conference on Cyber and IT Service Management (CITSM)*, pp. 1–5, 2020, doi: 10.1109/CITSM50537.2020.9268856.
[16] E. Almushiti, R. Zaki, N. Thamer, and R. Alshaya, "An Investigation of Broken Access Control Types, Vulnerabilities, Protection, and Security," in *Advances in Emerging Information and Communication Technology*, A. Shaikh, A. Alghamdi, Q. Tan, and I. M. M. El Emary, Eds., Cham: Springer Nature Switzerland, 2024, pp. 253–269.
[17] T. Ali, R. Dipke, V. Dhanshetti, and N. Gadepally, "Data Leaks Using SQL Injection," *International Journal of Advanced Research in Science, Communication and Technology*, p., 2023, doi: 10.48175/ijarsct-14255.
[18] V. Abdullayev and A. S. Chauhan, "SQL Injection Attack: Quick View," *Mesopotamian Journal of Cyber Security*, p., 2023, doi: 10.58496/mjcs/2023/006.
[19] I. M. M. Alssull and A. A. M. Lusta, "Security Measures Against SQL Injection Attacks," vol. 27, pp. 481–488, 2021, doi: 10.52155/IJPSAT.V27.1.3063.
[20] J. Okesola, A. Ogunbanwo, A. Owoade, E. Olorunnisola, and K. Okokpuji, "Securing web applications against SQL injection attacks - A Parameterised Query perspective)," *2023 International Conference on Science, Engineering and Business for Sustainable Development Goals (SEB-SDG)*, vol. 1, pp. 1–6, 2023, doi: 10.1109/SEB-SDG57117.2023.10124613.
[21] S. K. Lala, A. Kumar, and S. T, "Secure Web development using OWASP Guidelines," *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)*, pp. 323–332, 2021, doi: 10.1109/ICICCS51141.2021.9432179.
[22] "Buy Direct from Farmers | Local Pasar," Localpasar.com, 2025. https://www.localpasar.com/shop/all (accessed Jun. 11, 2025).
[23] GeeksforGeeks, "Prototyping Model – Software Engineering," GeeksforGeeks.