Applied Information Technology And Computer Science Vol. 5 No. 1 (2024) 110-123

AITCS

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

Eco Grocer Online Ordering System with Data Retention Policy

Atieleya Batrisha Mohd Yusri[1], Nurul Hidayah Ab Rahman[1]*

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

DOI: https://doi.org/10.30880/aitcs.2024.05.01.007
Received 19 May 2024; Accepted 22 May 2024; Available online 30 August 2024

Abstract: Eco Grocer is a grocer shop that sells daily necessities such as groceries. Currently, Eco Grocer only depends on customers that are shopping physically, and the business is not well-known in Shah Alam, Selangor. By adopting the online ordering system, it helps to widen the market. Eco Grocer online ordering system is an ordering system developed to ease customers to buy necessities. However, it is very risky to provide personal information on online ordering system since there are a lot of data breaches happen not only towards small business, but large organizations are not exceptional. Thus, implementing data retention policy is the best practice to reduce the risk of old unuse data being stolen or exploited by attackers Therefore, this project proposed Eco Grocer Online Ordering System with data retention policy to facilitate secure data management. This project is developed using Object-Oriented Programming with PHP programming language. The system is successfully developed to incorporates four modules that are Sign Up/Log In, Product List, User Profile and Checkout Page. By applying data retention policy on User Profile module, it could reduce the risk of data breach attack. In order to protect the confidentiality of customers' personal information in the database, all the customers' data will be stored for a certain period before it is deleted or archived to the tertiary storage. This system has undergone several testings, including system functionality testing, system design testing and data retention testing. All the testing conducted was successful. It indicates that the system is in a good state in terms of functionality, design, and security.

Keywords: ordering system, data retention, online shopping

1. Introduction

Online shopping has grown as part of people's lives nowadays. It has many benefits which many consumers prefer compared to shopping physically at the shop. Due to the pandemic, businesses that offered online stores were gaining many profits compared to the ones who did not. Online sales are expected to reach up to 5 trillion in 2021 and up to 95% of shopping will take place online by the year 2040 [1]. Customers must provide their personal information such as email, home address and even

*Corresponding author: hidayahar@uthm.edu.my

debit/credit card numbers for online purchase purposes. However, the most stolen items from the system of shopping websites include customers' debit/credit card information and other personal information [2]. Therefore, it is very important to have data retention policy for the website of online stores, especially the ones that allow customers to do payment transactions since it stores many credentials that are confidential and not supposed to be exposed to the unauthorized party.

As many businesses took the initiative to expand the market by offering an online ordering platform, Eco Grocer is no exception. Eco Grocer is a grocery store that is in Shah Alam, Selangor. It sells essentials for daily life such as dairy products, snacks, cleaning supplies, and many more. To widen the market scope, an online ordering system, Eco Grocer Online Ordering System, is developed. The online ordering system is responsible for taking orders from customers and storing customers' personal information. Data retention policy is applied to the Eco Grocer online ordering system to mitigate the risk of data exposure. Data retention is one of the cyber security policy mechanisms to protect the confidentiality of customers' data by setting a period for the information stored, until a certain time before it will be deleted or archived to the tertiary storage [3]. The system scope of the online ordering system consists of four modules which are Login/Sign Up page, User Profile page, Product List page and Checkout page. For user scope, there are four users which are the first-time user, registered user, admin, and the seller. Data retention is applied to manage user accounts and personal information that customer provides to the system including email address, phone number and address.

The objectives of this system are to design and develop Eco Grocer online ordering system with data retention policy, and to test the Eco Grocer online ordering system's functionality, security effectiveness and conduct the user testing.

2. Related Work

2.1 Online Ordering System

Online ordering has become one of the trends for every business to improvise the customers' experiences to shop the products without leaving houses [8]. Having an online ordering system could help not only to promote business limitlessness but also could make business operations smoother and more efficient. In addition, customers usually take time to make payment for their order and it produces a long queue for other customers. By using an online ordering system, customers do not need to wait in a queue since every order has its own unique order number to indicate the sequence of orders.

2.2 Data Retention

A data retention policy outlines what information needs to be archived or stored, where it should go, and for how long. Depending on the needs of the organization, information that has reached the end of its retention period may be deleted or relocated as historical data to secondary or tertiary storage [4]. This policy should be implemented for all systems that hold a lot of data in the database to filter out and only store the data that is still in use and delete for the data that is no longer needed. Data retention also must follow the standard that will determine the system's security is able to face the information security issues.

There are seven principles of Data Protection prescribed by the PDPA 2010 (Act 709). These principles are the guidelines for customers to be aware of what are their rights in providing personal information to any shopping platform. On the fifth principle, it states that all the personal information of consumers should not be stored more than the time of that data needed to the organization [11]. Therefore, Eco Grocer Online Ordering System practices data retention policy towards customers' personal information such as email address, phone number and address. The information will only be kept in the database until it is no longer needed by the Eco Grocer. In this case, Eco Grocer will terminate the data after two years of inactivity. According to retention standards in 2015 Standards set by PDPA, the Retention Principle has mentioned that retention periods will be set based on what

information is being stored. As an example, data that is related to legislative value needs to be disposed of within 14 days. As for personal data that is inactive, the retention period should be set to a minimum of 24 months, which is equivalent to two years [12]. This means, if the customer does not have any login activity to Eco Grocer Online Ordering System for the retention period, which is two years, then the customer's account will be disposed alongside all the personal information that has been provided to the system.

2.3 Study of the Existing System

A study has been conducted on three existing web systems, which are MyDeal, Lotus's and MyGroser. MyDeal is an online retailer that provides a platform for customers to buy a variety of products including home appliances, gadgets, furniture and more. Recently, 2.2 million of MyDeal's customers were affected by a data breach on the website. The full names, addresses and phone numbers of customers were disclosed by the attacker during the attack happened. MyDeal also claimed that the attacker started the attack by using user credentials to gain access to the system [6].

Therefore, it is important to implement data retention to minimize the incident cost of the exposure of customers' personal information. An example of how the impact of the attack can be minimized is by deleting the information that is no longer needed to both customer and organization. Figure 1 shows MyDeal online shopping website.

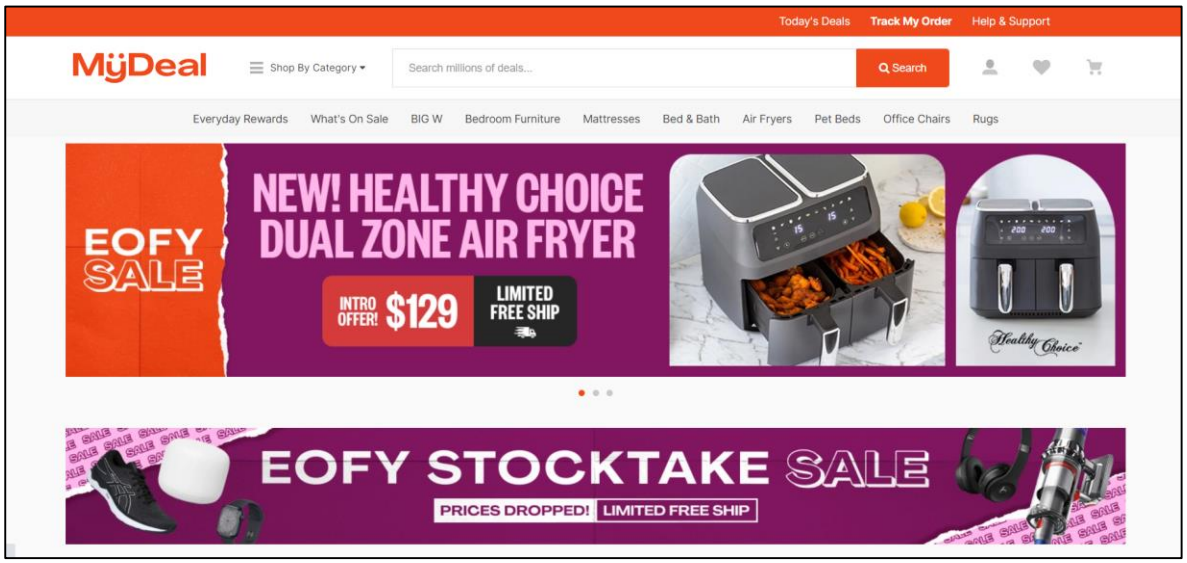

Figure 1: Home Page of MyDeal online shopping website

Lotus's, which used to be known as Tesco, was founded in Thailand. Lotus's is very well-known by Malaysians since it offers affordable prices for groceries, household necessities, and electrical appliances and there are many outlets in Malaysia. The Lotus's website provides an easier way for customers to shop things from Lotus's with only using smartphones or tablets. Lotus's website also offers many payment methods for customers to choose from to do the payment transaction. Figure 2 shows Lotus's online shopping website.

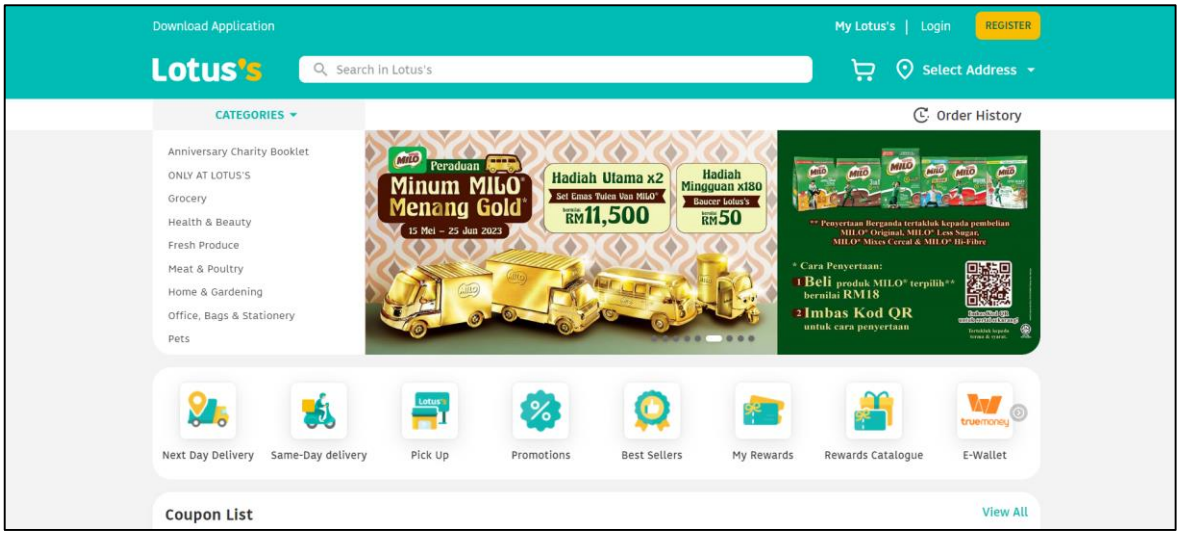

Figure 2: Home Page of Lotus's online shopping website

MyGroser is a platform that provides independent online grocery service only in Klang Valley. It offers a variety of products that customers can purchase including fresh vegetables, snacks, frozen foods, dairy products and many more. This platform also provides delivery to homes and businesses on every daily basis from 9am to 9pm. MyGroser is different from other grocery stores whereby, MyGroser has only cloud stores that have facilities like bakery, chilled rooms and racks to store all the products before delivering it to the customers [9]. Figure 3 shows MyDeal online shopping website.

Figure 3: Home Page of MyGroser

The features chosen in Table 1 are the system features that Eco Grocer Online Ordering System implemented for security purposes. The feature Sign Up/Login is required when user wants to purchase anything from the system. This feature is important because it prevents unauthorized users from accessing user details such as phone number and email address since user needs to provide few sensitive data for the order details. Next, a strong password is an important feature to avoid being a victim of brute-force attack [10]. Eco Grocer does implement this feature, same goes with MyDeal, Lotus's and MyGroser systems. The common requirement for a strong password is a minimum of eight-length characters that includes at least one alphabet, one digit and one special character [13]. Identity verification feature is chosen to be compared to other existing system is because to authenticate whether the user is the one who has done the payment, not botnets. For the retention of data, MyDeal's recent

case proves that MyDeal does not apply data retention towards inactive accounts, causing major breach even for user that does not use the platform anymore. MyGroser's privacy policy does not mention that they practice data retention for customers' personal information. In Lotus's system, it does state in their website's policy, whereby Lotus's does implement data retention but did not mention the period of inactivity for them to eliminate users' information and will do if any special request from the user. All of these existing systems are web-based systems, same as Eco Grocer Online Ordering System.

Table 1: Comparison table of existing systems with Eco Grocer Online Ordering System

System Features	MyDeal	Lotus's	MyGroser	Eco Grocer Online Ordering System
Sign Up/Login	Yes	Yes	Yes	Yes
Strong Password Management	Yes	Yes	Yes	Yes
Data Retention Policy	No	Yes	No	Yes
Platform	Web-based system	Web-based system	Web-based system	Web-based system

3. Methodology

Agile methodology model is a System Development Life Cycle (SDLC) model that is being used in developing this Eco Grocer Online Ordering System. It consists of five phases which are planning, analysis, design, implementation, and testing. The Agile methodology model was chosen for this project because it was designed to facilitate changes and modification requests. It is easier for clients to participate in the development process in order to fulfill the requirements of the Eco Grocer online ordering system. Agile methodology's requirements are broken down into small pieces that can be developed gradually called iterative development. Each iteration can be completed to go through the whole cycle in just a couple of weeks and is known as Time Box. One of the advantages of using agile methodology is it reduces the total time of development to complete the whole project [5].

3.1 Planning

In the planning phase, the objectives and scope of the project are determined. The scope of the system is divided into two which are system and user scope. For system scope, there are four modules while for user scope, it includes four types of users. The types of users are first-time user, registered user, seller and admin. The project requirements such as system and user requirements are also identified.

3.2 Analysis

An interview session with an Eco Grocer representative was held by conducting a few interview questions to understand the business background, current method of how customers are shopping and other related to the business as well. The answer to the interview question was analyzed to gain the real problem and client's needs in the online ordering system. From the analysis, the scope of the system, the users that will be using the system, and other requirements that need to be implemented to the system are identified. This is also the phase where the data retention feature is determined to be implemented to the system, since it holds customer's sensitive information such as name, email address and phone number.

3.3 Design

For the design phase, there are Entity Relationship Diagram (ERD), Context Diagram, Data Flow Diagram (DFD), Sequence Diagram, Use Case Diagram and Activity Diagram. Moreover, in order to achieve successful testing, a test plan is prepared to test and define how the system will work. Test plans play a major role in a successful system because they help to identify the effort, cost and time needed for the project and to determine the requirements and equipment of the system.

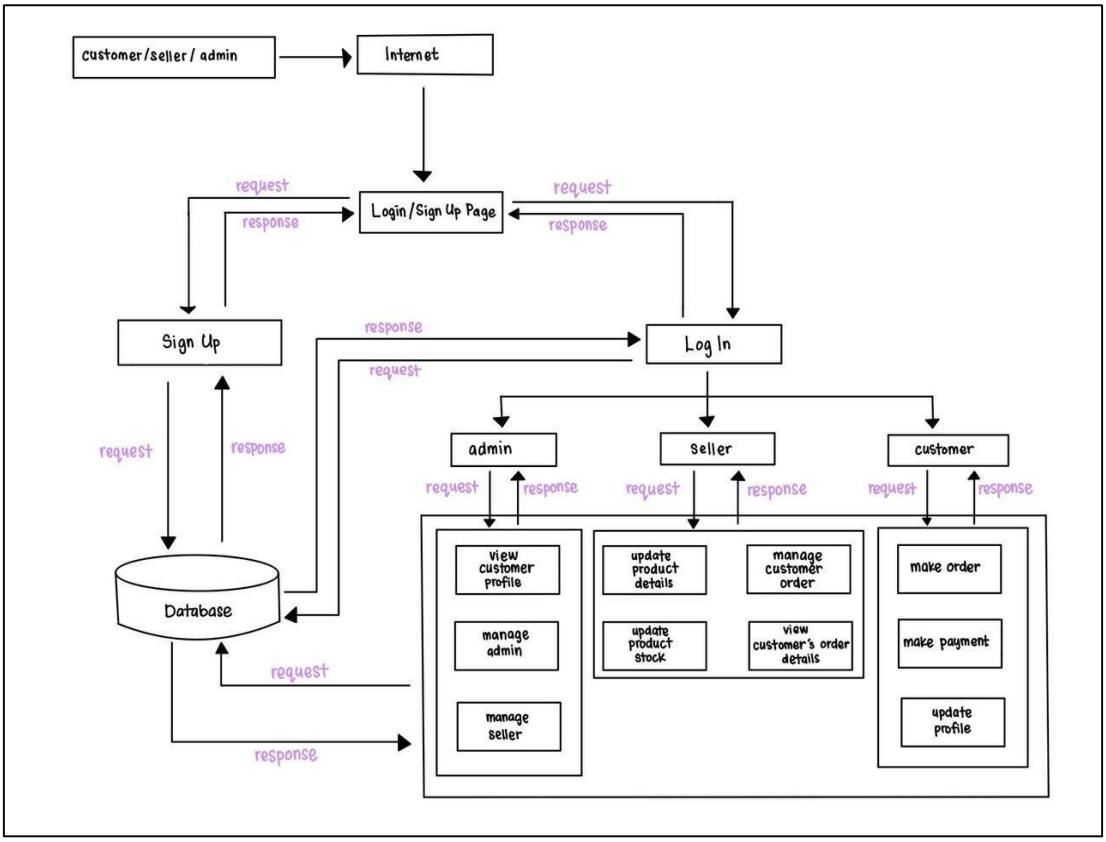

Figure 4: Activity Diagram Eco Grocer Online Ordering System

In addition, an activity diagram in Figure 4 is also designed in this phase, which shows the flow of the online ordering system from one task to another when a customer is using the system.

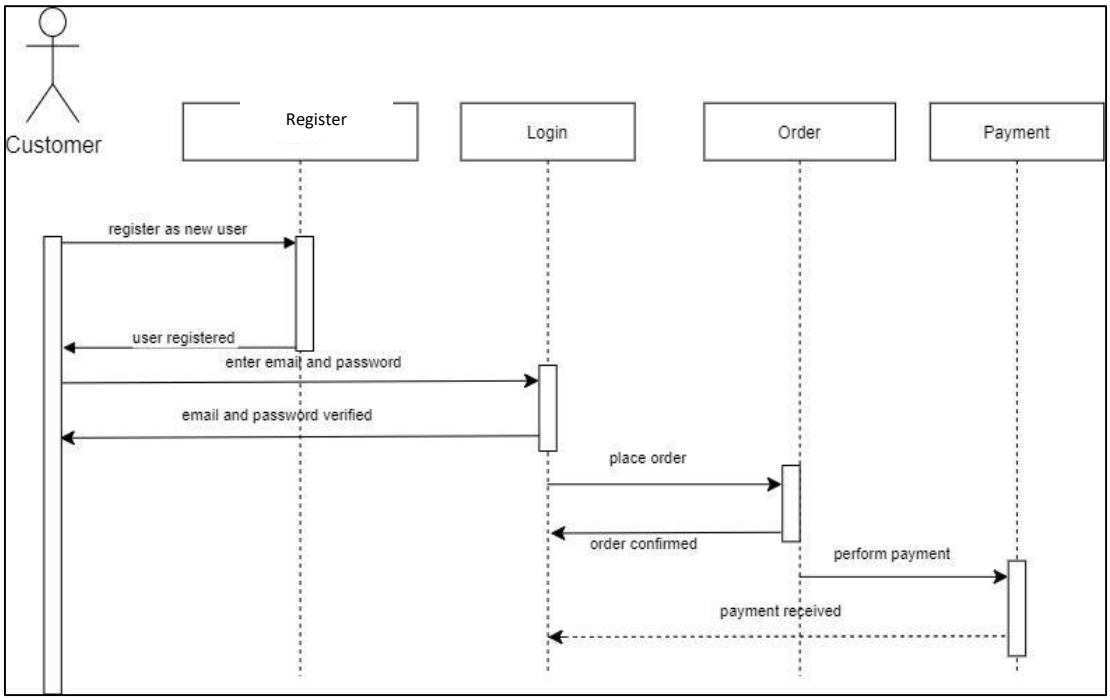

Figure 5: Sequence Diagram Eco Grocer Online Ordering System

The sequence diagram shown in Figure 5 is a representation of the interaction of the objects in the system in sequence which indicates the order of the interaction that happens in the system.

3.4 Implementation

Implementation phase is where all the designs are implemented. The database tables are linked together and connected with the user interface of the system to ensure the system is working when there is any input requested from the customer and output to be fetched from the database. For instance, when customers want to login using username and password registered, the code will determine the input is a match in order to gain access to the online ordering system.

3.5 Testing

In the testing phase, the test plan that has been prepared during the design phase will be used to determine whether the system is well functioning as planned. There are several components that need to be considered during the test plan which are schedule, environment, risk management, tools, scope, resource allocation, exit parameters and defect management. Penetration test is also conducted to identify the vulnerabilities of the system by simulating cyber-attacks to the system that consists of five steps which are planning the goal of the test, scanning the response to the attack, gaining access to identify the vulnerabilities of the system, maintaining the access and analyzing the result.

4. System Analysis and Design

In this section, it discusses the system architecture of Eco Grocer Online Ordering System, activity diagram for customer of Eco Grocer, and requirement analysis which consists of functional and non-functional requirements.

4.1 System Architecture Design

Figure 6 shows the system design diagram of the Eco Grocer Online Ordering System. Since it is a web-based system, the Internet is required for users to use the system. Users need to sign into the system by registering themselves on Sign Up page, while the user that has been registered can fully experience the system by just login to it. While for new admin and seller, they can only register themselves through the first admin, using Manage Admin and Manage Seller functions on Admin Dashboard. Other than managing admin and seller, admin also can manage customer, customer's orders, order details, and update products on website based on availability of the product itself.

For sellers, they do have some similarities access as admin, but seller is not allowed to manage admin and other seller since their access only limited to managing products and orders made by the customers. Unlike admin and seller, customers are required to login to add any products desired into the cart, update their profile account for shopping purposes, perform order and make payment for the order.

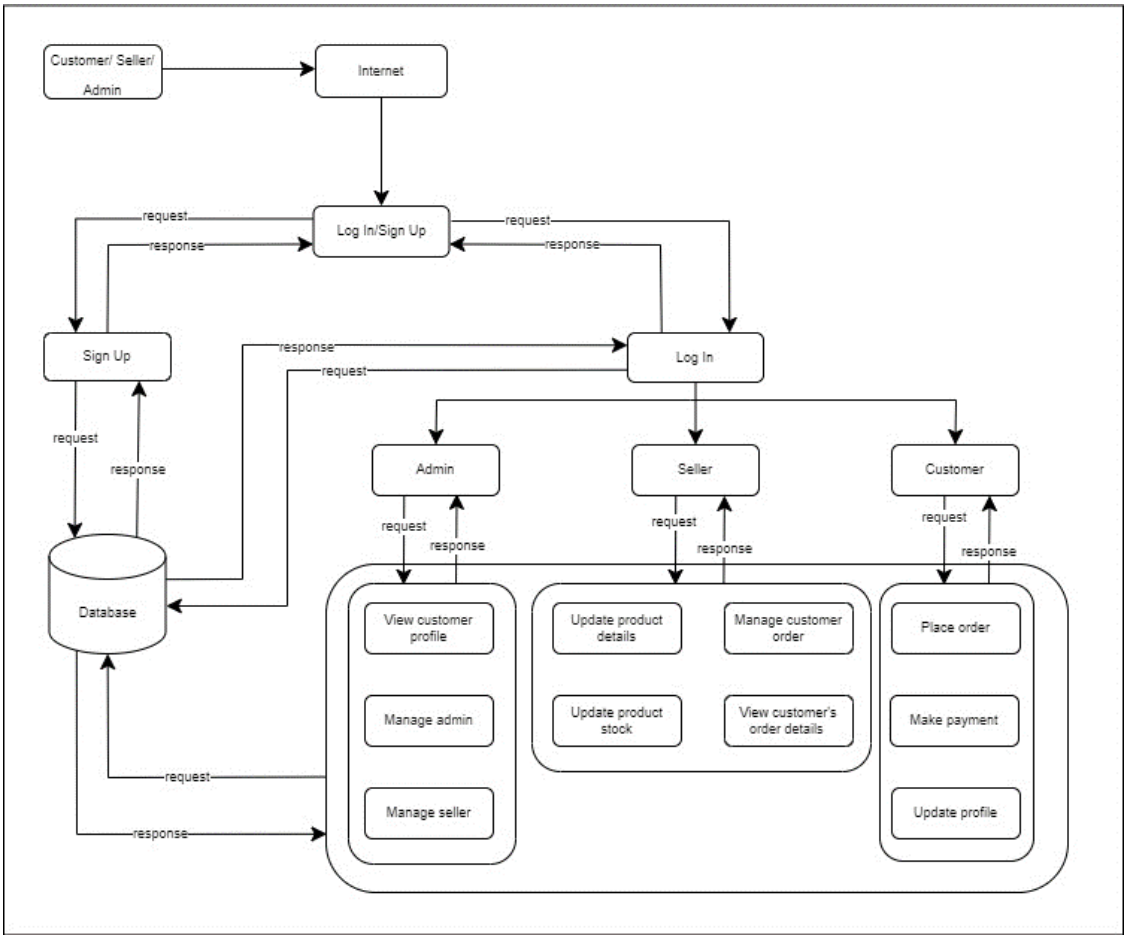

Figure 6: Activity Diagram Eco Grocer Online Ordering System

4.2 Requirement Analysis

There are two types of requirements involved in requirement analysis, which are functional and non-functional requirements. Table 2 shows the functional requirements of Eco Grocer Online Ordering System.

Table 2: Functional requirements

Module	User	Functional Requirements
Login	Admin, Seller, Customers	- The system allows users to login as a user using username and password. - The system will execute a message if the username and password do not match.
Register	Admin, Seller, and Customers	- The system allows users to register by providing a username, email and password. - If the registration is successful, the user will redirect to login page to login.
User Profile	Customers	- The system allows users to update their personal information such as name, phone number and email address.
Add to Cart	Customers	- The system allows users to check out all selected products at once.
Payment	Customers	- The system allows users to perform cash/cashless payment after shopping.
Order	Admin, Seller, and Customers	- The system allows the user to place orders. - The system allows admin and seller to view the orders.

Table 3 shows the non-functional requirements for Eco Grocer Online Ordering System.

Table 3: Non-Functional Requirements

Module	Non-Functional Requirements
Login	- The system allows users to login as a user using username and password. - The system will execute a message if the username and password do not match.
Register	- The system allows users to register by providing a username, email and password. - If the registration is successful, the user will redirect to login page to login.
User Profile	- The system allows users to update their personal information such as name, phone number and email address.
Add to Cart	- The system allows users to check out all selected products at once.
Payment	- The system allows users to perform cash/cashless payment after shopping.
Order	- The system allows the user to place orders. - The system allows admin and seller to view the orders.

5. Result and Discussion

This section discusses the result and discussion for the proposed system. The implementation is where all the features determined in design phase being applied to the system.

5.1 Result

This section discusses the result and implementation of security module in Eco Grocer Online Ordering System.

5.1.1 Implementation of data retention

Figure 7 shows the code for data retention whereby the user account will be deleted after three years of inactivity based on their user id.

```php
<?php

include('connect.php');

$inactive_time = strtotime('-2 years');
$query = "SELECT user_id FROM user_table WHERE last_login < $inactiveTime";

while ($row = $result->fetch_assoc ())
{
    $userid = $row['user_id'];
}

?>
```

Figure 7: Implementation of Data Retention Code

5.1.2 Implementation of encryption

Figure 8 shows the syntax of executing Advanced Encryption Standard (AES) algorithm. The key is generated as shown below.

```php
$secretkey = "ecosecretgrocerkey"; //secret value to encrypt and decrypt
$iv = random_bytes(16);
//random value used to ensure the uniqeness of the encrypted output
```

Figure 8: Key Generation for Advanced Encryption Standard (AES) algorithm code

Figure 9 shows the implementation of AES algorithm for address and phone number of customers. The key that has been generated will be passed to be used to encrypt the plaintext into ciphertext.

```php
$phonenum = $_POST['phone_number'];
$plaintext = strval($phonenum);

$ciphertext = openssl_encrypt($plaintext, 'AES-256-CBC', $secretkey, OPENSSL_RAW_DATA, $iv);

?>
```

Figure 9: Encryption using Advanced Encryption Standard (AES) algorithm code

5.1.3 Implementation of strong password

Figure 10 and Figure 11 show the implementation of a strong password. It will validate the password entered by the user during the registration process. In order to choose a strong password, user needs to apply strong password requirements, which are minimum length of eight characters includes at least uppercase and lowercase letters, 1 digit and 1 special character. If the user's password of choice does not match with the strong password requirements, the system would not accept those as user's password. Thus, the user needs to choose another password that matches all the requirements.

```php
<?php
$password = $_POST['password'];

$minimumlength = 8;
$uppercase = true;
$lowercase = true;
$digit = true;
$specialChar = true;

$errors = []; // to gather all the errors during strong password validation

if (strlen($password) < $minimumlength) {
    $errors[] = "Password must be at least $minimumlength characters long.";
}

if ($uppercase && !preg_match('/[A-Z]/', $password)) {
    $errors[] = "Password must contain at least one uppercase letter.";
}

if ($lowercase && !preg_match('/[a-z]/', $password)) {
    $errors[] = "Password must contain at least one lowercase letter.";
}

if ($digit && !preg_match('/[0-9]/', $password)) {
    $errors[] = "Password must contain at least one number.";
}

if ($specialChar && !preg_match('/[^A-Za-z0-9]/', $password)) {
    $errors[] = "Password must contain at least one special character.";
}
```

Figure 10: Code Implementation of Strong Password

```php
if (!empty($errors)) {
    // Handle the validation errors
    foreach ($errors as $error) {
        echo $error;
        echo '<br>';
    }
} else {
    $hashedPassword = password_hash($password, PASSWORD_DEFAULT);
    $query = "UPDATE user_table SET password = '$hashedPassword' WHERE user_id = '$user_id'";

    $result = mysqli_query($con,$query);
}

?>
```

Figure 11: Code Implementation of Strong Password

5.2 Testing

This section discusses the testing result of Eco Grocer Online Ordering System. The testing conducted includes security evaluation testing, data retention test plan and user acceptance result that is carried out using Google Form. User acceptance test form is distributed to the target user which is client and 20 potential users of ordering system.

5.2.1 Security Evaluation Testing

Security evaluation testing is conducted to test whether the security implementation is well-functioning. Table 4 shows the results of security evaluation testing.

Table 4: Security Evaluation Testing

No	Security Evaluation Elements	Actual Result
1	The password requirements must be a minimum of eight characters with a combination of uppercase, lowercase, number, and special character.	Pass
2	Error message displayed after mismatched username and password does not mention which specific field is incorrect.	Pass
3	Email entered by user must be in email format. (eg: atieleya@gmail.com)	Pass
4	The password entered in registration and login page is obscured.	Pass
5	User account that has been inactive according to retention period cannot be access anymore.	Pass

5.2.2 User Acceptance Results

This section shows the results of user acceptance form that conducted using Google Form to 20 target users.

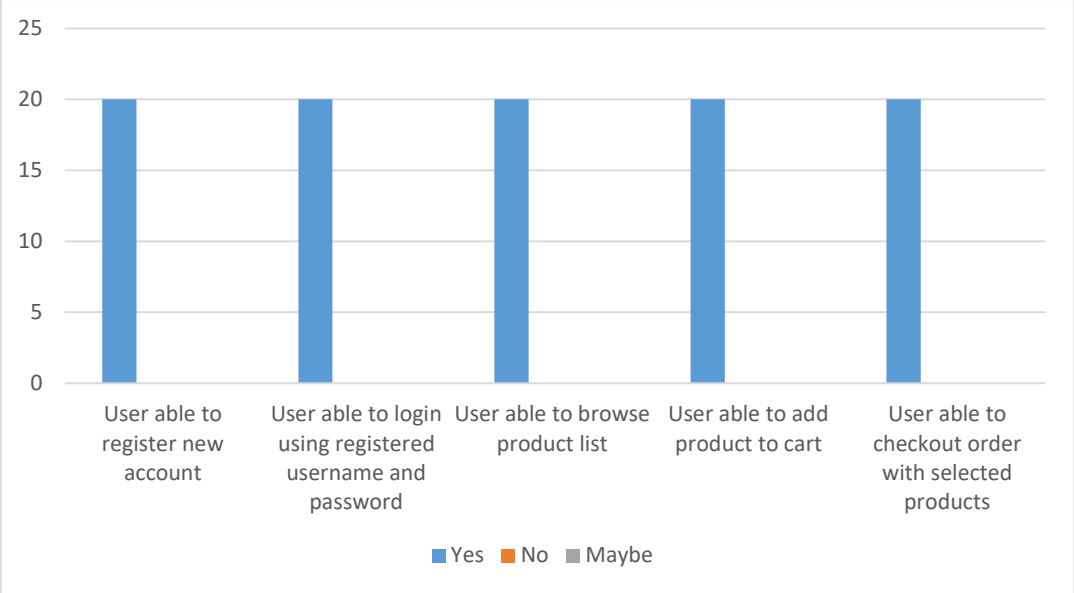

Figure 12: Result of system functionality testing

Figure 12 shows the results of system functionality testing of Eco Grocer Online Ordering System. All responses indicated that users are able to register a new account, login using registered username and password, browse product list, add products to cart and checkout order with selected products.

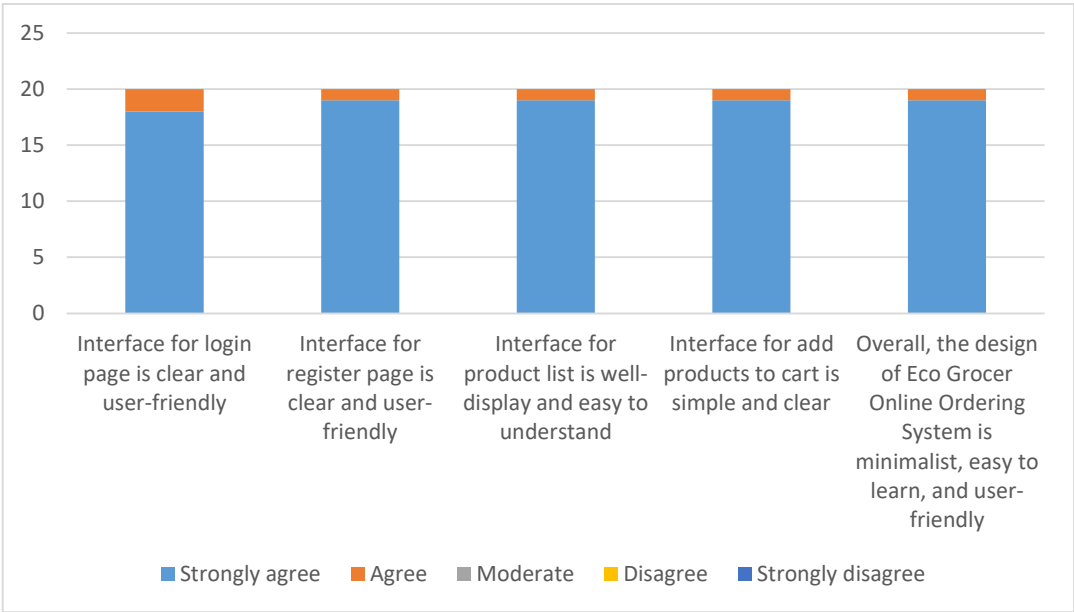

Figure 13: Result of system design testing

Figure 13 shows the results of system design testing of Eco Grocer Online Ordering System. There are 18 users strongly agreeing that interface for login page is clear and user-friendly, while the other two agree. Next, 19 users strongly agree while one user agrees that interface for register page is clear and user-friendly. 19 users also strongly agree that interface for product list is well-displayed and easy to understand, and one user agrees with that. For interface involving adding products to cart is simple and clear, 19 users strongly agreeing, and one user agrees. Lastly, the overall design of Eco Grocer Online Ordering System is minimalist, easy to learn and user-friendly, is strongly agreed by 19 users and agree by one user.

6. Conclusion

Eco Grocer Online Ordering System is an online ordering system that allows users to perform orders based on products they desire without physically going to the store. Other that providing a platform to customers to shop online instead of physically, this system also provides a platform for the admin and seller manage the products and orders effectively since all the orders made by the customers will be organized with its own order ID in database. The system implemented security mechanisms that reduce the impact of confidential data being exploited by attackers, which is a data retention policy. Data retention policy is being applied to the user account and all the sensitive information of customers that stored in the database such as email address, phone number and address. For Eco Grocer, the retention period is set up to two years of account inactivity, then the user account and all provided sensitive data will be deleted from the system.

Other than that, data retention is also implemented since this system does hold a lot of personal data, whereby each of customers' data will be deleted after a certain period of time of inactivity. This will reduce the consequences of any cyber threats that happen in the future. Since cyberthreats are getting more complex and worse consequences, there are few improvements that can be implemented in future to Eco Grocer Online Ordering System. One of it, is, implements multi-factor authentication to authenticate the real user in order to prevent unauthorized users gain access to the account.

Acknowledgement

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

References

[1] T. W. 21/05/2020 and T. Watson, "Online shopping vs in-store shopping – which is better for retailers," *Skywell Software*, 11-Nov-2020. [Online]. Available: https://skywell.software/blog/online-shopping-vs-in-store-shopping/.

[2] K. Peretti, "Data Breaches: What the Underground World of Carding Reveals," Santa Clara High Technology Law Journal, vol. 25, no. 2, p. 375, Jan. 2009, [Online]. Available: https://digitalcommons.law.scu.edu/chtlj/vol25/iss2/4/

[3] B. Posey, P. Crocetti, and A. Burton, "Data Retention Policy: What Is It and How to Build One," TechTarget. https://www.techtarget.com/searchdatabackup/definition/data-retention-policy

[4] D. Wallen, "Data Retention Policy: What It Is and How to Create One," *Spanning*, Dec. 16, 2020. https://spanning.com/blog/data-retention-policy-what-it-is-how-to-create-one/

[5] "Software Engineering | Agile Development Models – GeeksforGeeks," GeeksforGeeks, Jul. 06, 2018. https://www.geeksforgeeks.org/software-engineering-agile-development-models/

[6] L. Abrams, "MyDeal data breach impacts 2.2M users, stolen data for sale online," *BleepingComputer*, Oct. 17, 2022. [Online]. Available: https://www.bleepingcomputer.com/news/security/mydeal-data-breach-impacts-22m-users-stolen-data-for-sale-online/

[7] M. Drolet, "ISO 27001 Certification: What It Is And Why You Need It," *Forbes*, Mar. 23, 2022. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2022/03/23/iso-27001-certification-what-it-is-and-why-you-need-it/?sh=5e33096441a6

[8] K. Viwyaanjali, A. M. Nur Hafizah, J. Norfazlina, and M. I. Asma Zubaida, "Smart Food Ordering System – A Literature Review," City University eJournal of Academic Research (CUeJAR), Art. No. 2682–910X, Dec. 2022.

[9] R. Koh and R. Koh, "Grocery Deliveries Aren't New, But This M'sian Startup Does It Differently With 'Cloud Stores,'" Vulcan Post, Nov. 2019, [Online]. Available: https://vulcanpost.com/680999/mygroser-startup-grocery-delivery-klang-valley/

[10] A. Descalso, "How to Prevent Brute Force Attacks in 8 Easy Steps [Updated]," *Intelligent Technical Solutions*, Mar. 09, 2023. https://www.itsasap.com/blog/how-to-prevent-brute-force-attacks#:~:text=Use%20Strong%20Passwords.,is%20relatively%20easy%20to%20remember.

[11] "Principles of Data Protection – Jabatan Perlindungan Data Peribadi." https://www.pdp.gov.my/jpdpv2/public/principles-of-data-protection/?lang=en

[12] "Six (6) Things Your Business Need to Know on Personal Data Protection in Malaysia - Azmi & Associates," *Azmi & Associates*, Aug. 15, 2022. https://www.azmilaw.com/insights/six-6-things-your-business-need-to-know-on-personal-data-protection-in-malaysia/

[13] "Authentication - OWASP Cheat Sheet Series." https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html