Applied Information Technology And Computer Science Vol. 4 No. 1 (2023) 205-223

AITCS

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

Fingerprint and Qr Code Based Authentication System at Pusat Servis Komputer JB

Muhammad Fadhli Jamal[1], Nordiana Rahim[1]*

[1]Fakulti Sains Komputer dan Teknologi Maklumat,
UniversitiTun Hussein Onn Malaysia, Parit Raja, BatuPahat, 86400, MALAYSIA

*Corresponding Author Designation

DOI: https://doi.org/10.30880/aitcs.2023.04.01.013
Received 00 Month 2020; Accepted 27 May 2023; Available online 30 June 2023

Abstract: The existing device registration and collection system for a service at Pusat Servis Komputer JB (PSKJB) is outdated and unsafe. The premise typically employs a receipt, which is easily misplaced, and people frequently forget to bring or take the receipt while retrieving their device. When someone steals another person's information and uses it to commit fraud, this old system is easy to game. As a result, this paper discusses an approach to a system that requires a customer or user to present a combination of more than one credential to verify their identity. For this authentication system, a combination of fingerprint authentication and QR code was chosen as a method. It works by tracing the ridge and valley pattern on your finger, and a successful match indicates that your identity has been verified and access has been granted. A QR code is a pattern that represents various bits of data. It is a data-encoded card that can be scanned to verify the customer's identity. This paper provided an overview of PSKJB's customer authentication system, which uses fingerprint and QR code authentication.

Keywords*:* Multifactor Authentication, Fingerprint, QR Code

1. Introduction

Typically, customer authentication is handled by the customer management system. It validates a customer's identity by authorizing a human-to-machine transfer of credentials to confirm the customer's authenticity [1]. Customer authentication consists of two important elements. First is identification, which is to prove the customer's identity. Next is the authentication which means customers must provide evidence that they are who they claim to be. The customer management system is a collection of all the systems, processes, and applications required to manage customer relations. It assists businesses in staying in touch with customers, streamlining processes, and increasing profits [2].

Authentication methods such as key generation, passwords, and encryption have all failed in the past, leaving data vulnerable to intruders and black hat hackers [3]. It is a system that uses a feature extractor, sensors, and matching parts or modules to apply recognition algorithms to a specific biometric

Corresponding author: nordiana@uthm.edu.my

pattern. The sensor scans the biometric trait and outputs a digital representation. The check and control are done to ensure that the output sample for feature extraction and matching modules is reliable and safe.

The fingerprint recognition scanners work by tracing the ridge and valley pattern on a finger. The information is then compared to a list of registered fingerprints on file by the device's pattern matching software. A successful match indicates that an identity has been verified and thus access has been granted [4]. There are a few methods of capturing fingerprint data, including optical sensors, capacitive sensors, and ultrasonic sensors. The first method involves making a photocopy of the finger to achieve crisp line contrast as the information is recorded by a light-sensitive scanner to create a digital image, while the second method uses electricity to determine fingerprint patterns [4]. Lastly, the ultrasonic sensor works via sound waves.

Another method of authentication is to use a QR code. It's a matrix barcode that uses a combination of spacing as a quick response code. When a QR code is scanned, it provides access to information [5]. A QR code is made up of several components. A pixel pattern is created by combining those parts. The purpose of the elements inside the pattern is to carry specific information through the code, such as the print direction, timing, error tolerance, and empty spaces to distinguish the code.

The reason this system was developed is because at the moment, PSKJB uses a traditional method for customer authentication. To authenticate the customer, the premise uses a simple receipt. To begin, when a customer sends their device for services, such as a laptop or printer, the receptionist will write down the customer's personal information, such as name, phone number, type of service, and device model number, on two pieces of receipt. The customer will receive the original receipt, while the technician will retain a copy. The issue is that if a customer arrives at the store without bringing their receipt, it is difficult to determine who is the true owner of the device.

Next, there is no system in place to manage customers and their devices. When there are too many devices of the same brand and model in the technician room, the problem arises. To distinguish them from other devices, the devices are simply tagged with a sellotape with a customer's name written on it. Due to a lack of tagging, the technician may accidentally give the laptop to the wrong customer. As a result, data theft from a mistakenly taken laptop by an unauthorized customer who took another laptop or computer is a possibility. Hence, this system is mainly focussing on device registration and collection after got a service at PSKJB.

The objectives of this project are to develop a computer shop management system with multifactor customer authentication using biometric recognition and QR code for PSKJB that can authenticate the customer identity. The objective of this project are as follows:

1. To design a multifactor authentication for a computer shop management system.
2. To develop a system for PSKJB with multifactor authentication system by utilizing a fingerprint recognition technology and QR code scanner.
3. To test and evaluate the performance of the multifactor customer authentication using biometric recognition and QR code.

The following pages is organized as follows: Section 2 focused on related work of fingerprint recognition and QR code. Section 3 will discuss more details about the methodology, followed by Section 4 is conclusion.

2. Overview of Biometrics and QR Code

Biometric authentication is a method of verifying a person's identity by using a physical feature of their body. Fingerprint recognition, face recognition, iris and retina recognition, hand geometry recognition,

voice identification, and other physical characteristics are just a few of the human physical characteristics that can be used for biometric authentication [6].

Biometric authentication has long been viewed as the way of the future, with the expectation that it will largely replace other forms of authentication and access control currently in use [7]. Biometric systems can be used in two ways. The first is verification, which involves determining whether or not a person is who they claim to be. The system will verify the person's identity in this mode by comparing the captured biometric data to a sample stored in the database. The second step is identification, which entails identifying the person and searching the database's samples for a match [7].

The biometric authentication process using biometric involves comparing a person's physical characteristics to a database sample. When the user uses a biometric authentication device, the physical traits match the stored sample in the database, for example, the authentication is considered successful [8]. It is one of the most effective authentication methods currently in use, but it very relies on physical characteristics such as fingerprints, facial patterns, iris or retinal patterns to verify user identity.

2.1 Types of Biometrics

The type of characteristics evaluated, such as physiological attributes or behavioural singularities to determine how biometric authentication techniques are classified. Physiological biometrics is based on classifying a person based on data obtained from their face, fingerprints, retina, and iris, which are all parts of the human body [7]. Table 1 show types of biometrics

Table 1: Types of Biometrics

Types of Biometrics	Description
Fingerprint	Reading the fingerprint, feature extraction, data saving, and comparison are the four main functions of fingerprint identification technology. The fingerprints are scanned first, then it will be necessary to pre-transform the image to make it much clearer. Following that, fingerprint recognition creates feature data in the form of numbers that switch directions. That is, fingerprints could change into feature data, but feature data could not change into fingerprints, and two different fingerprints could not produce the same feature data [8].
Facial	Facial recognition is a way to determine the similarity between two face images. Facial recognition works by converting a face image into a numerical expression known as a template, which can then be used to compare the similarity of different face images [9].
Iris	A technique for determining the unique patterns in people's irises, or colored circles in their eyes [10]. Iris recognition scanners work by shining invisible infrared light on the iris to pick up unique patterns that aren't visible to the naked eye. The lines and colors of the eye are then analyzed to create a bit pattern that encodes the information in the iris.
Voice	A process of converting a speech signal into a sequence of words using a computer algorithm [11]. It works by breaking down a speech recording's audio into individual sounds, analyzing each sound, using algorithms to find the most likely word fit in that language, and then transcribing those sounds into text.

2.2 Fingerprint Recognition Methods

There are three common methods of fingerprint authentication are used which is Minutiae-based method, Correlation-based method, and Wavelet Transform-based method [12]. The loop, the whorl, and the arch are the three basic patterns of fingerprint ridges. A loop is formed when a ridge enters one side of the finger, curves, and exits on the same side of the finger as it entered. A whorl is a pattern that occurs when ridges form in a circular pattern around a central point. Finally, an arch is a pattern in

which the ridge enters one side of the finger, rises in the centre to form an arch, and then exits the other side. Figure 1 show the example image of fingerprint loop, whorl, and arch.

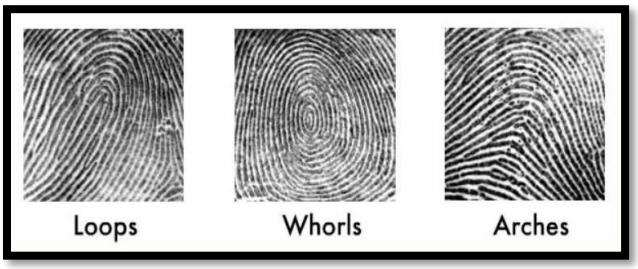

Figure 1: The image of fingerprint loops, whorls, and arches (https://www.uh.edu/engines/epi2529.htm)

2.2.1 Minutiae-Based

The methods that are based on minutiae are the most common method in fingerprint recognition. This is due to their close resemblance to forensic methods in fingerprint comparison, which are accepted as legal identification guides in many countries [13]. This method represents the fingerprint by its local features like, terminations and bifurcations called as minutia. Minutiae are small points of interest in the fingerprint image. The minutiae-based method does the recognition in two stages that is minutiae extraction and minutiae matching. To reliably extract the minutiae features, the minutiae-based method requires extensive preprocessing operations. Image enhancement, segmentation and thinning, and false minutiae detection are among the preprocessing operations [14]. This method is ideal for fingerprint matching because each fingerprint has a spatial distribution that is extremely different from the other. This method extracts a set of minutiae points that are distinguished by different types of presentation in the fingerprint image, such as ridge orientation and skin pores. The fingerprints are matched using an alignment-based method after the real minutiae points have been extracted. It calculates the total number of matched minutiae by aligning the two sets of minutiae points [13].

2.2.2 Correlation-Based

The pixel values of the images are used in the correlation based fingerprinting algorithm. It makes use of the user's fingerprints' grey scale information. This algorithm chooses a template, then correlates its pixel values with the pixel values of all the images in the template database, then looks for the maximum value in the so-called obtained correlated data that is greater than our threshold score. The template's correct match from all the images in the database is determined by the maximum score of all the correlated data [15]. This method belongs to the category of area based matching algorithms in which image pixels are compared and then matched. This method takes less time and requires less data pre-processing than Minutiae-based methods, but it is found to be less accurate. This method uses the fingerprints' rich grey scale information. It selects the appropriate templates in the elemental fingerprint first, then searches for them in the secondary print using a template matching algorithm. The template positions of both the primary and secondary print are then compared. It is capable of handling low-quality images, unlike minutiae-based techniques. For instance, the one from which no pertinent details can be gleaned. It also aids in the handling of fingerprints that are not uniformly shaped or have distortions.

2.2.3 Wavelet Transform-Based

This technique recognizes fingerprints using an image-based approach. The wavelet transform is the base. Wavelets offer a diverse set of approaches that can be used to solve a variety of signal processing problems, resulting in a wide range of potential applications [16]. The fingerprint patterns are matched using wavelet domain features taken straight from the grayscale fingerprint image. Image enhancement, directional filtering, ridge segmentation, ridge thinning, and minutiae extraction are just some of the techniques available.

2.3 Existing Work

Biometric authentication [17] is the use of a user's biological features. It's done by capturing a user's biological characteristics with a camera, scanner, or sensor. The captured biological feature will be compared to a registration template because the user biological feature registered in advance is known as an authentication technique for identity verification. The biometric authentication devices will adjust the camera's exposure and the intensity of the illumination provided during the capture of an image biometric for authentication based on the intensity of the external light on the object to be captured.

Meanwhile a biometric authentication device, according to Yukihiro Abiko [18], is a biometric information acquiring unit that generates a plurality or partial images. Each partial image captures a different aspect of the user's biometric data. A unit for calculating the correlation value between a portion of biometric information represented on one partial image and registered biometric information. It also has a partial similarity update unit that is based on the correlation value for one partial image and at least one other partial image acquired before the one partial image. The degree of similarity between the registered biometric information and portions of biometric information represented on a single partial image is represented by the partial similarity.

Krishna Kumar et al. [19] stated that fingerprints are a great source for identifying individuals. One of the earliest forms of biometric identification is fingerprint recognition. The quality of fingerprint images and the extraction of minutiae play a significant role in the automatic identification and verification process. In general, the minutiae extraction algorithm begins with preprocessing to improve image quality without affecting the image's local and global properties. The features core and delta, as well as minutiae, which represent the end of ridge or bifurcation, can be used to describe the fingerprint image. The matching algorithm's performance can be harmed by missing or false minutiae.

Falguni Suthar et al. [20] mentioned that Biometrics is the process of automatically identifying a person based on certain physical or behavioural characteristics. Protecting partial access systems from malicious attacks is perhaps the most important application of perfect personal identification. Because of the long history of fingerprints and their widespread use in forensics, fingerprint recognition systems have received the most attention of all the currently used biometric techniques. This paper addresses the issue of selecting the most advantageous fingerprint matching algorithm in order to design a system that meets the required performance and accuracy specifications, as well as introducing the fundamentals of biometric technology from a pattern recognition perspective and conveying recent advances in this field, particularly in the context of security, privacy, and forensics.

2.4 QR Code

A QR code, which stands for ‘quick response,’ is a type of matrix bar code or two-dimensional code that can hold data. A QR code is a type of barcode that stores information as a series of pixels in a square-shaped grid and can be read easily by a digital device that is designated to be read by a mobile phone. It consists of a special pattern like a crossword puzzle arranged in a square pattern on a white background [21]. The QR code holds an information such as text, website link or any kind of data.

2.4.1 How QR Code Works

A QR code is a data-encoded barcode that can be scanned. The term "encoded" refers to the process of transforming data into a certain format. QR codes transform numeric and alphanumeric characters into a unique two-dimensional pattern like a crossword puzzle on a square layout. When an optical scanner passes over those squares, it reassembles the data into its original form. In addition, A QR code can store a total of 7,089 numbers. It is made up of 4,296 alphanumeric letters that are mixed with numbers and alphabets. It also contains 2,953 bytes of binary numbers and 1,817 Kanji characters [22]. Furthermore, the error correction function can recover up to 30% of the code if it is damaged or read incorrectly. The structure can easily be expanded to accommodate the size of the data to be recorded.

2.4.2 Dynamic QR Code

A dynamic QR code is preferable compare with a static QR code. It gains more functionality and flexibility because of this. It can be updated, modified, and changed as many times as the user wants after it's generated, without requiring the user to generate a new QR code for their product's URL. This is because, unlike the static QR code, the dynamic QR code stores the URL redirection rather than the destination URL. It can also track and measure statistics like the number of scans performed, the location, and the operating system used.

2.4.3 Static QR Code

Once a static QR code has been generated, it cannot be changed. These are things like URLs, email address, and text that don't collect any tracking data. Its lack of uniqueness is a disadvantage, as is the fact that it may not provide for analytics on how many times the code has been scanned.

2.4.4 QR Code Elements

The positioning detecting markers, alignment marking, timing pattern, version information, format information, data and error correction keys, and quiet zone are all components of a QR code structure. Table 2 shows the QR code elements meanwhile in Figure 2 shows the QR code with elements[23].

Table 2: QR code elements

Elements	Description
Position detection pattern	This element can be found in the upper left, upper right, and lower left corners, accordingly. This allows a scanner to correctly identify and decode the code at rapid speeds while also displaying the information's encoded direction. In general, they help in recognizing the presence and location of the QR code in a picture.
Alignment marking pattern	This element marker is smaller than the location detection markers, and it's used to assist balance out QR codes created on a rough surface. It also relies on the symbol's size; the larger the symbol, the more coordination patterns are required.
Timing pattern	This element is used to determine the data matrix's scale. It's identified by dotted lines that span the QR both horizontally and vertically to design the data grid specifically.
Version information	The QR code version is specified with this element. It's also aligned with position detection patterns.
Format information	To make scanning the code faster, this element is positioned along the position detecting patterns. It gives details on the error correcting codes and mask pattern that were used.
Data and error correction area	The real data content stored in the QR code, as well as data error correction codes, are both included in this element. The QR version has an impact on the number and size of blocks assigned to data as well as error correction codes. The data can be harmed by up to 30% in this situation.
Quiet zone	This feature is required to distinguish the QR code from its surroundings. To improve comprehension when scanning the program, the structure was placed alongside the element that was previously shared with white space.

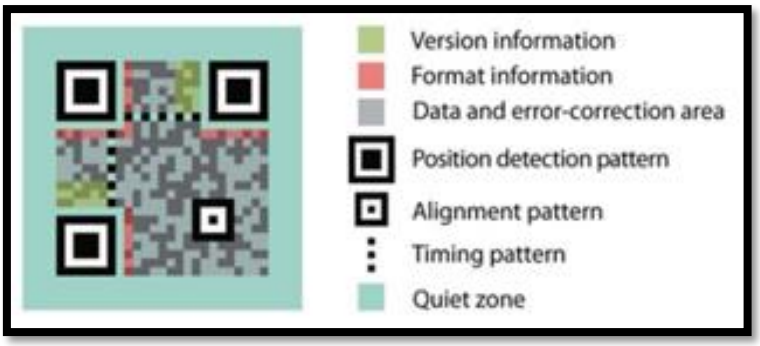

Figure 2: QR code elements [24]

2.5 Comparison of Existing System with the Proposed System

Table 3 shows the comparison between the existing customer authentication system and proposed authentication system.

Table 3: The Comparison between the existing customer authentication system

	Current System at PSKJB	AwareABIS	Proposed System
Speed	Slow	High	medium
Biometric	No	Yes	Yes
QR Code	No	No	Yes
Implementation Cost	No	High	Medium
Ease of use	Easy	Hard	Medium
Verification	No	Yes	Yes
Identification	No	Yes	Yes
Privacy	No	Yes	Yes

3. Object Oriented Methodology

Object-oriented methodology (OOM) is a set of steps that begin with analysing the customer's needs and requirements and ends with designing an application or system that meets those requirements using object-oriented programming. The proposed project has five phases which is Requirement gathering and Analysis, Design, Implementation, Testing, and Maintenance. Figure 3 shows the object-oriented analysis and design method.

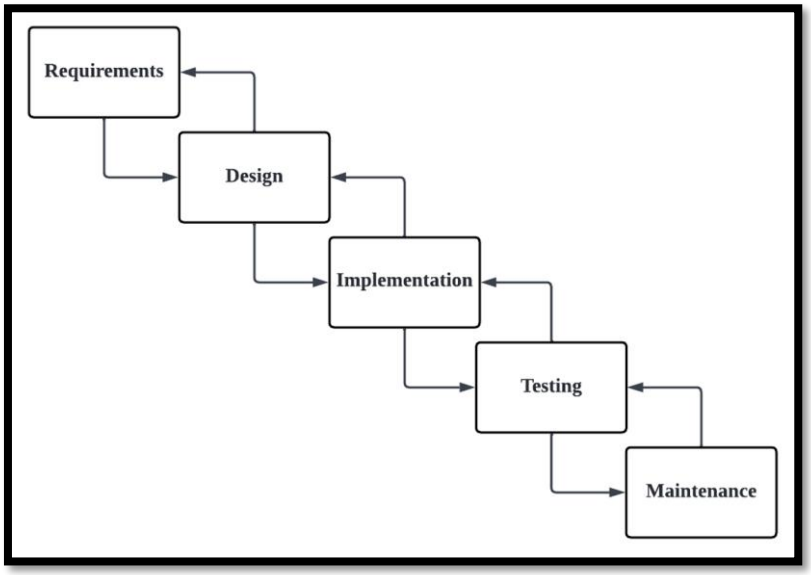

Figure 3: Object Oriented Methodology

3.1 Project System Requirement

The hardware and software requirements are the most important factors to consider when developing a system. In order to ensure that the system's performance is fault-free and error-free, these two requirements are interdependent. Table 4 and Table 5 shows the software and hardware requirements for this project.

Table 4: Hardware Requirements

Hardware Type	Hardware Specifications
Device Name	Asus ROG Strix G15 (Laptop)
Processor	Intel(R) Core (TM) i7-10750H CPU @ 2.60GHz 2.59 GHz
Installed RAM	16.0 GB
System	64-bit operating system, x64-based processor
Storage	500GB Solid State Drive
Fingerprint Scanner	HID Digital Persona U.are.U 4500 Fingerprint Reader

Table 5: Software Requirements

Software Type	Software Specifications
Operating System	Windows 10 Home Single Language
Code Compiler	Visual Studio 2022
Programming Language	C#
Database	Microsoft SQL Server
Documentation	Microsoft Office 365
Drawing & Design	Microsoft Visio, Wondershare EdrawMax

3.2 Functional Requirement

Functional requirements are features that must be built into a system for users to be able to use it to meet their needs. It specifies the system's behaviour when confronted with a specific scenario or scenarios. Table 6 shows the functional requirements for the proposed system.

Table 6: Functional Requirement of The Proposed System

Module	Functionalities
Admin	i. Login ii. Register customer information iii. Capture customer fingerprint iv. Generate QR code
Customers	i. Register information. ii. Scan Fingerprint iii. Check service status
Authentication	i. Fingerprint recognition ii. QR code scanner

3.3 Non-Functional Requirement

The operational security, software performance, and usability are one of the non-functional requirements of the proposed system are described in this section. It describes how a system should work without regard for its utility, instead focusing on its usability. Table 7 shows a non-functional requirement for the proposed system.

Table 7: Non-Functional Requirement for The Proposed System

Requirement	Description
Operational	i. The system must be able to communicate with database. ii. The system must be able to establish a connection between fingerprint recognition and database. iii. The system must be able to establish a connection between QR code and database
Performance	i. The system should authenticate and verify customer by using fingerprint recognition. ii. The system should authenticate and verify customer by using QR code
Usability	i. The system's design graphic user interface (GUI) is simple and easy to use
Security	i. The fingerprint should be able to authenticate each of the customer. ii. The QR code should be able to authenticate each of the customer

3.4 Use Case Diagram

As shown in Figure 4, the system only requires two main users: an administrator and a customer. This use case explains how the customer and the administrator will interact with the system. As shown in the diagram, the customer must first log in to the system before using their fingerprint and QR code to verify their identity. Meanwhile, the administrator will examine the fingerprint to see if it matches. The administrator will then check the QR code, which is unique to each customer. The customer's basic personal information, such as name, phone number, and address, will be displayed via QR code.

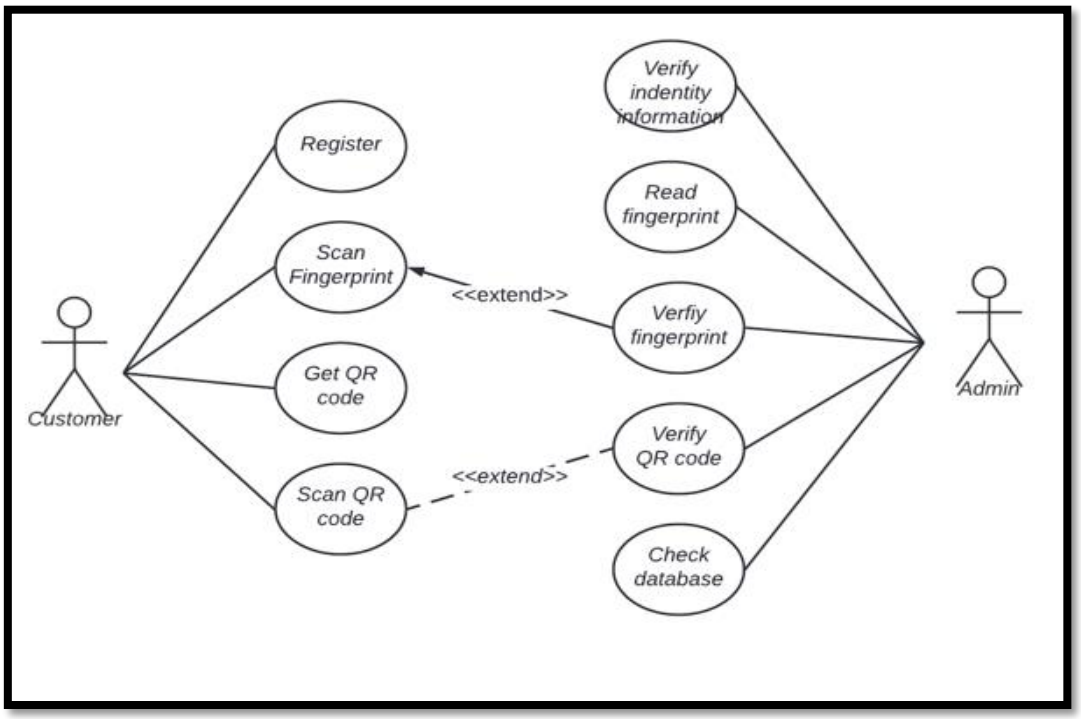

Figure 4: Use Case Diagram for the proposed system

3.5 Sequence Diagram

Figure 5 shows the process in general when the customer is the first timer to register at PSKJB. The customer will enter their personal information into the system with the help of the admin. After the customer registers their personal information, they are prompted to scan and capture their fingerprint. The fingerprint that has been scanned will be extracted and saved in the database. The fingerprint that has been scanned will be assigned with the customer's personal information that had been registered earlier. After being assigned, the customer's fingerprint will be verified before the customer returns to the registration page.

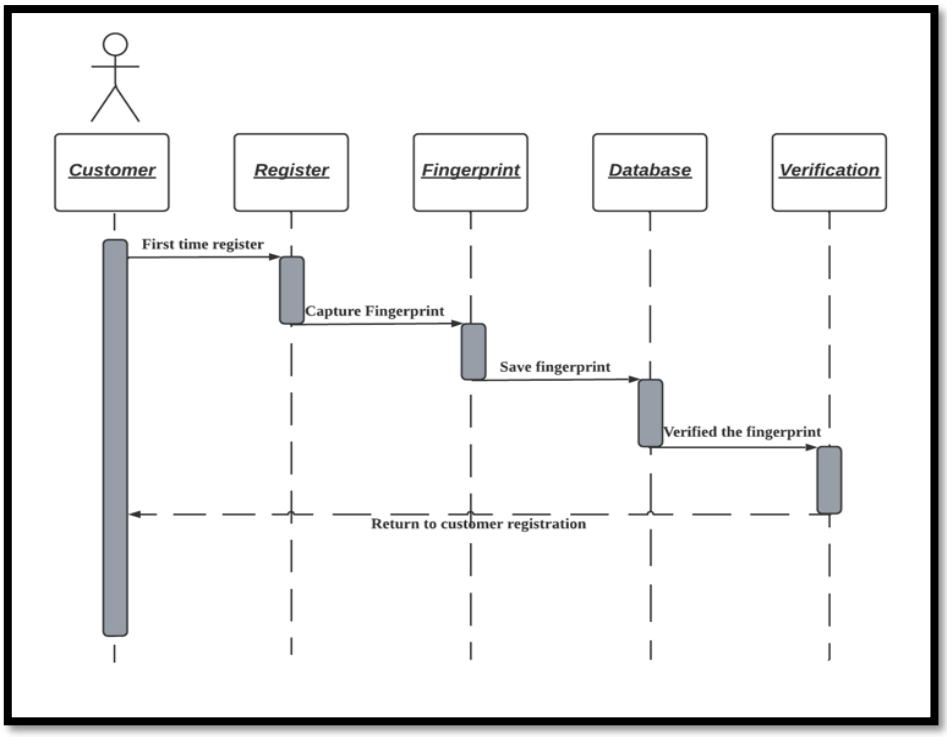

Figure 5: Sequence diagram for customer register fingerprint

Next, Figure 6 shows the process of how the QR code will be generated for the customer. The process is almost identical to the previous steps in the fingerprint scan process, but a little different. First, after capturing their fingerprint, the customer will go to the services page. The admin will insert the customer's information that is required, such as name, address, phone number, type of service, brand name, and model number. After all the important information has been inserted, the system will require the customer to verify their fingerprint again before being able to generate a QR code. The QR code will then be sent to the customer's email.

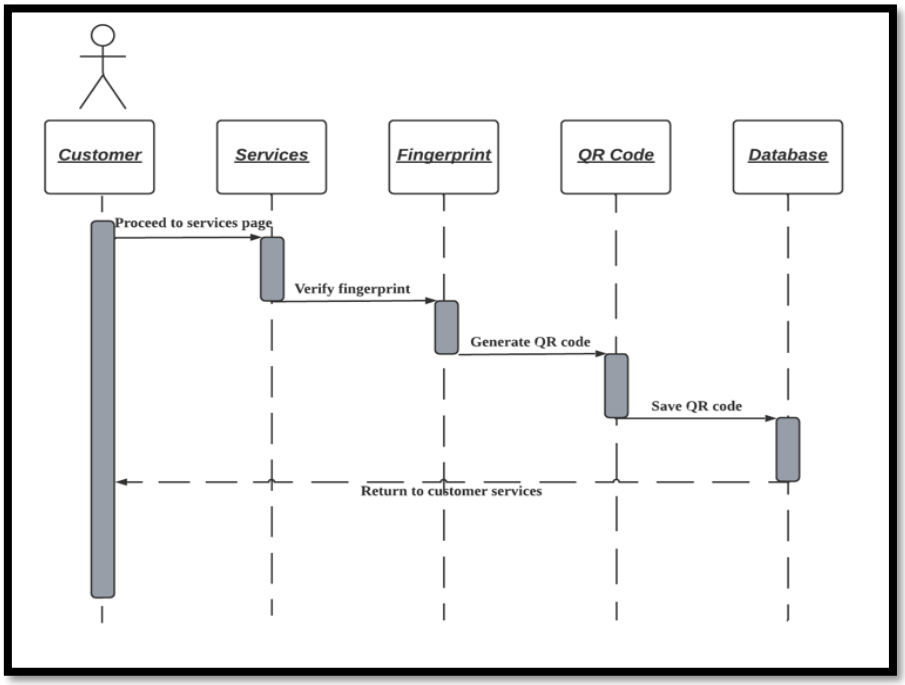

Figure 6: Sequence diagram of QR code that generated for customer

Finally, Figure 7 shows how the entire process of the system works. Firstly, the registered customer will go to the services page. The customer will enter their information such as service, brand name, and model number. The admin will set the status of the services manually, such as initiated, still in process, or finished. If the customer comes back again to take their laptop after finishing the service, the customer will go through to the two-authentication page where the customer needs to authenticate their fingerprint and scan the QR code that they received through. Next, the customer's fingerprint will be authenticated if it matches with any fingerprint samples in the database. Then, if the QR code scanned the same as the QR code that had been generate and sent to the customer's email, the customer considers as authenticated before they can proceed to take their laptop that had been sent to get service at PSKJB from the technician. If not, the customer needs to re-authenticate their information again.

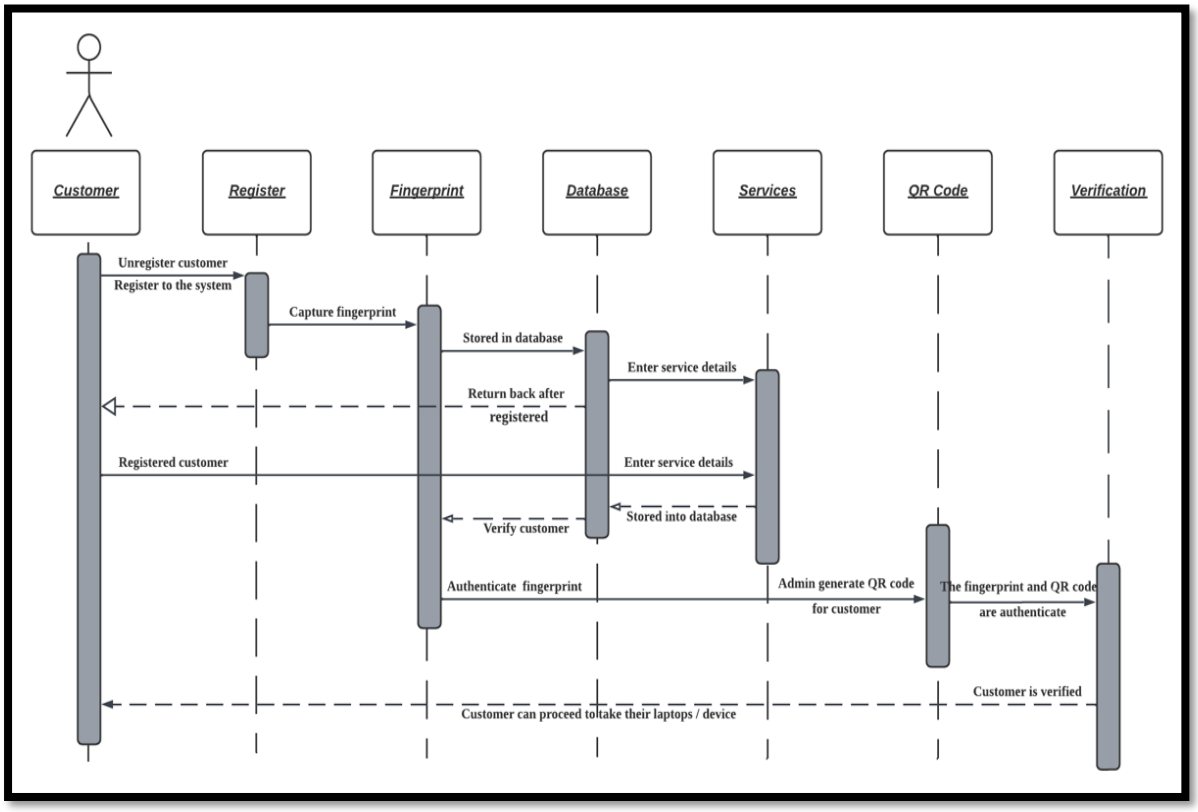

Figure 7: Sequence diagram of the propose system.

3.6 Activity Diagram

In the UML, the activity diagram is used to depict the system's dynamic features. The activity diagram is a more complex depiction that shows how information moves from one action to the next using a flow chart. Figure 8 shows the activity diagram of for the proposed system.

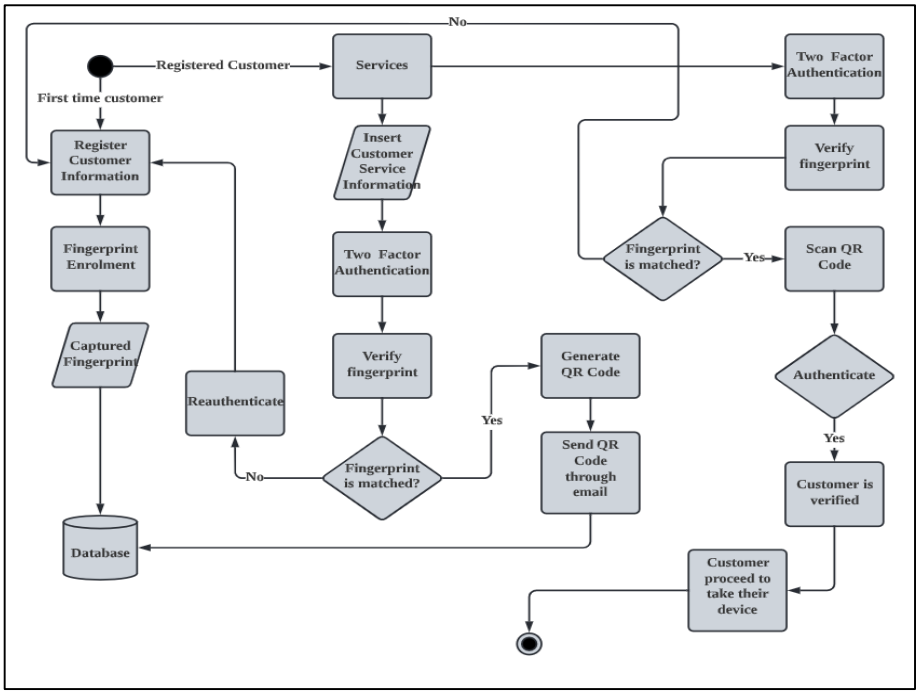

Figure 8: Activity Diagram of the proposed system

3.7 Class Diagram

In the UML, a class diagram is used to present the static behaviour of objects. The class diagram should be represented in analysis and design to describe the attributed and operations of a class and the constraints imposed on the proposed system. It is a rectangle with up to three sections that are used to represent it. The first sections display the class's name, while the second sections display the class's attributes, which represent the objects' attributes. The bottom one contains a list of the class's operations, which describes the class's behaviour. Figure 9 shows the class diagram of the system.

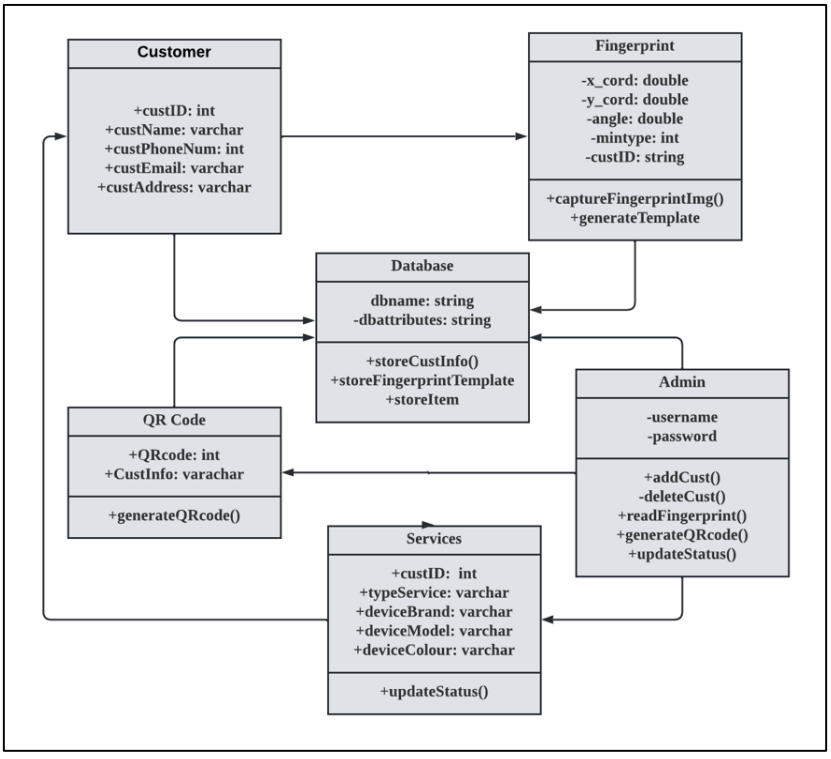

Figure 9: Class Diagram of the proposed system

3.8 Object Oriented Testing

The methodology for developing the Fingerprint and QR code-based system at PSKLJB was discussed in detail in this chapter, and the Object-Oriented Methodology Model was chosen. There are five phases in total, starting with the Requirements phase, which is combined with the Analysis phase. The Design phase is the second phase, which is followed by the Implementation phase, which is the third phase. Then there's the Testing phase, and finally, the Maintenance phase. The Object-Oriented model was chosen also because of the process of development would go along smoothly as it is easier to comprehend and learn.

4. System Implementation and Testing

The implementation phase of any system's development is critical because it ensures that the system is usable and relevant in real-world situations. System testing is used to see if the proposed system's operations and features are working properly and if there are any flaws.

4.1 System Development

The entire system was created in Visual Studio 2022 with the C# environment. The back-end database is Microsoft SQL Server Management Studio 18. C# was selected for this system is because the C# was built on the principles of object-oriented programming (OOP). It is fully integrated with Microsoft's.NET software framework, which allows for the creation of Windows desktop applications.

The Figure 10 shows the customer registration form. There are a few customers information details that needed to be register such as name, phone number, email address, address, and fingerprint template. The button capture is used to capture customer fingerprint during fingerprint enrolment process as shown in Figure 11.

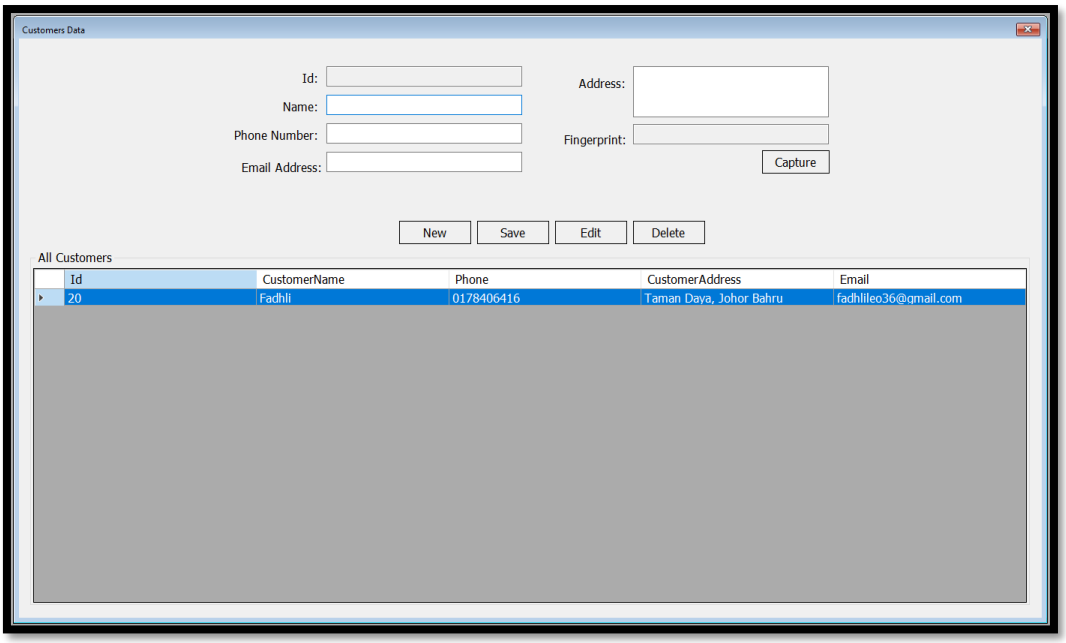

Figure 10: Customer registration form

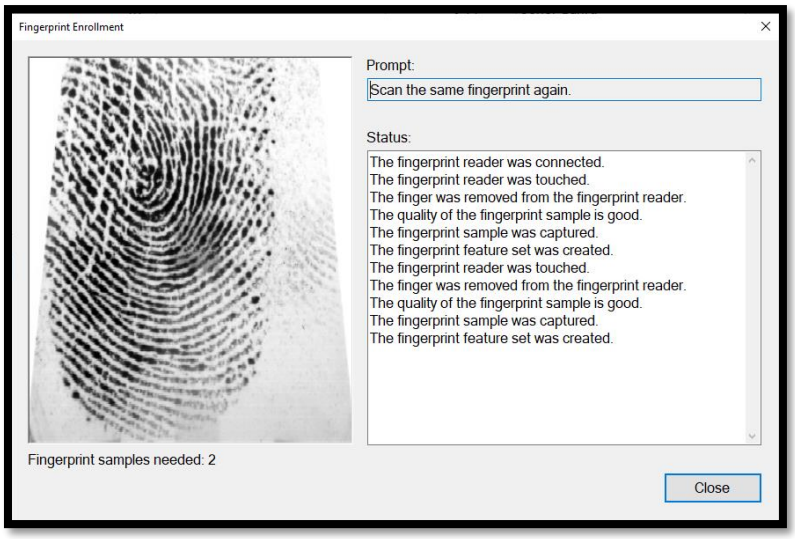

Figure 11: Fingerprint enrolment form

After customer successfully register their fingerprint, there are another form which is service data form as shown in Figure 12. This page is used by admin to insert customer details about their service type and device information. For example, is device brand, device model and device colour. Also, the admin can set the device service status whether it is initiated, in process or completed.

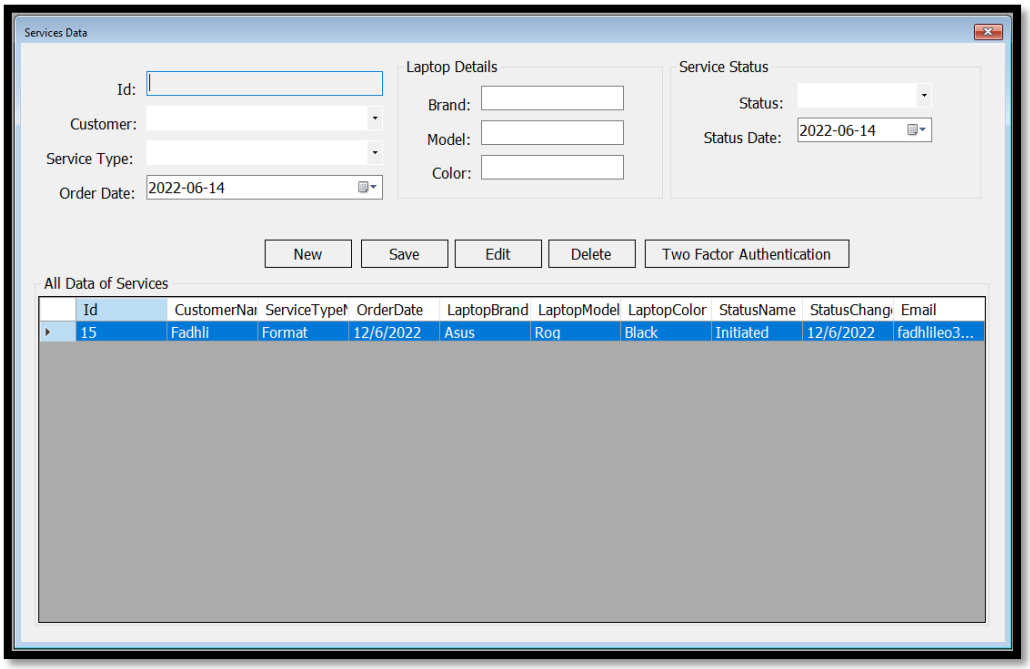

Figure 12: Service data form

Figure 13 shows the customer two-factor authentication form. This form is used twice. Before the admin can generate a QR code for the first-time customer, they must verify their fingerprint that was captured during the enrolment process. The generated QR code will be sent through the customer's email. So, the next time the customer comes again to the shop to take their laptop, they just need to verify their fingerprint and scan their QR code from the email to the scanner. If the customer's fingerprint and QR code have been authenticated, the authenticated label will turn green. Also, if the label is still in red, that means the customer is not authenticated. In the Figure 14 show the example of the customer is trying to scan the QR code to the QR code scanner.

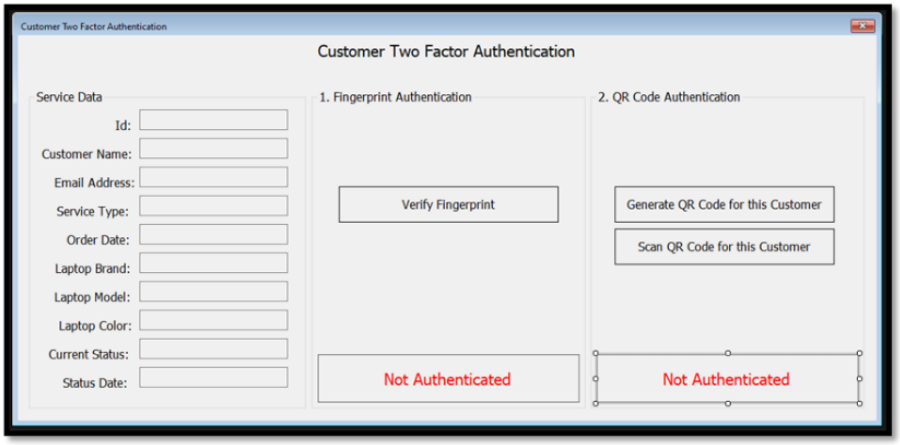

Figure 13: The customer two-factor authentication form

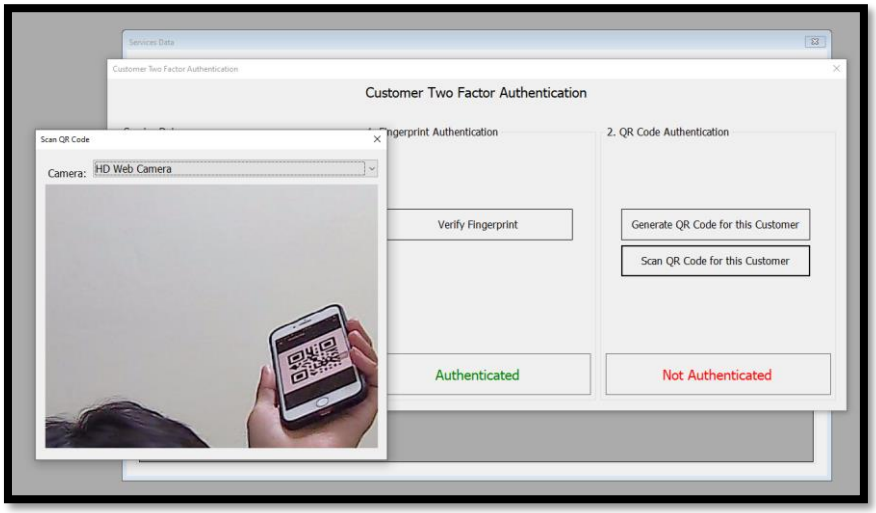

Figure 14: Scan QR code

Lastly in the Figure 15 show the services type form. In this form, the admin can add, delete, or edit the type of services that their premise provided.

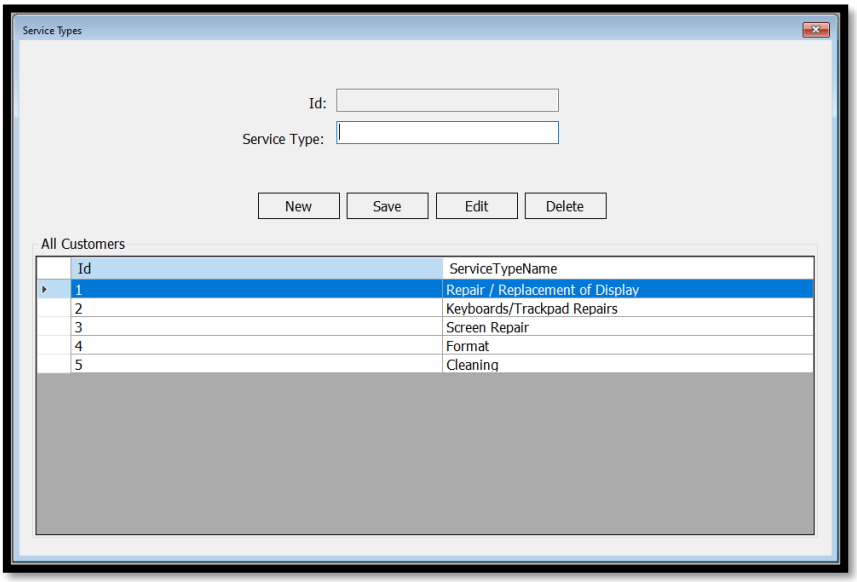

Figure 15: The type of services form

4.2 System Testing

The testing phase is critical in the system development process because it determines whether all the functionality of the produced system is fully functional after the implementation phase. This ensures that no defects will appear during system use and that the system will run smoothly and without errors. Table 8 shows the test plan category of the system. Next, Table 9, Table 10 and Table 11 show the result of the test plan for each module.

Table 8: Test Plan Category of the proposed system

Test Category	Descriptions
1	Test the functionality of register, adding, deleting, updating the customer profile.
2	Test the functionality of register, login, and fingerprint authentication. The system must be able to register, login and check the fingerprint verification.
3	Test the functionality of the system that able to generate QR code and check the QR code verification.

Table 9: Test Category 1 of the proposed system

Test Category	Descriptions	Expected Result	Pass/Fail
1	Register – Add new customer	New customer is added	Pass
1	Register – Delete customer	Customer is deleted	Pass
1	Register - Update customer	Customer is updated	Pass

Table 10: Test Category 2 of the proposed system

Test Category	Descriptions	Expected Result	Pass/Fail
2	Login – Customer does not insert a valid username	A message appears: Invalid username	Fail
2	Login – Customer does not insert a valid password	A message appears: Invalid password	Fail
2	Customers scan their fingerprint into the fingerprint scanner	System manages to register the customer	Pass
2	Customer login the system by scanning their fingerprint	System verifies the fingerprint by labelling it with the customer's information	Fail

Table 11: Test Category 3 of the proposed system

Test Category	Descriptions	Expected Result	Pass/Fail
3	The QR code is generate for customer	QR code is successfully generated for the customer	Pass
3	Customers scan their QR code and	QR code is verified by the admin	Pass

4.3 User Accepting Testing Form

A form is used to determine results of testing the user acceptability with the system. The form is used as a guide to assist the test case within the system. The user acceptance form is to evaluate the test case within the proposed system. The score of the test used is Likert scale from 1 to 5 with 1 being strongly disagree and 5 for strongly agree as in Table 12.

Table 12: User acceptance of the proposed system

System Testing							
No	Acceptance Requirements	Test Scale 1 – Strongly disagree 5 – Strongly agree					
		1	2	3	4	5	
1	Admin can access the system					/	
2	The system can be functioning properly from start to end					/	
3	Admin can successfully login into the system				/		
4	Admin can successfully register customer					/	
5	Admin can successfully verify the customer					/	
6	Admin can successfully check the service status					/	
7	System can detect fingerprint from image captured by fingerprint scanner					/	
8	System can generate a QR code for each customer					/	

5. Conclusion

As a result of the implementation of fingerprint and QR code-based authentication as a customer authentication system at Pusat Servis Komputer JB, time was saved while the customer was securely authenticated. The use of fingerprint authentication techniques in the real world has the potential to be accurate to the point of having low false rejection rates (FRR) and false acceptance rates (FAR) (FAR). Although this system has suffered several setbacks as a result of an unauthorised customer attempting to impersonate other people, there is still room for further improvements that would improve the accuracy and efficiency of the multifactor authentication system using fingerprints and QR codes. A few changes and enhancements are planned to increase the system's functionality and usefulness in order to provide the best user experience possible.

Acknowledgment

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

References

[1] "What is user authentication?" https://www.techtarget.com/searchsecurity/definition/user-authentication.

[2] "What is Customer Management System? - LeadSquared." https://www.leadsquared.com/what-is-customer-management-system/ (accessed Dec. 29, 2021).

[3] M. Ansar and M. Fatima, "Biometric encryption in Cloud Computing: A systematic Review," *Biometric encryption in Cloud Computing: A systematic Review*, vol. 18, no. 8, pp. 125–131, 2018.

[4] "What Are Finger Scanners and How Do They Work?" https://www.lifewire.com/understanding-finger-scanners-4150464 (accessed Dec. 29, 2021).

[5] "How QR Codes Work and Their History - QR Code Generator." https://www.qr-code-generator.com/blog/how-qr-codes-work-and-their-history

[6] "What is Biometrics? - Biometrics Institute." https://www.biometricsinstitute.org/what-is-biometrics

[7] "Biometric Authentication Methods. Fingerprints, facial recognition, hand… | by Anh T. Dang | Towards Data Science." https://towardsdatascience.com/biometric-authentication-methods-61c96666883a

[8] J. Tian and Y. Peng, "Research of the Matlab application in the fingerprint identification system," in *Proceedings of 2012 International Conference on Image Analysis and Signal Processing, IASP 2012*, 2012, pp. 118–122. doi: 10.1109/IASP.2012.6425005.

[9] J. A. Lewis, "How Does Facial Recognition Work?" *Csis.org*. [Online]. Available: https://www.csis.org/analysis/how-does-facial-recognition-work.

[10] J. Daugman, "How Iris Recognition Works," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 21–30, Jan. 2004, doi: 10.1109/TCSVT.2003.818350.

[11] W. H. Abdulla, D. Chow, and G. Sin, "Cross-words reference template for DTW-based speech recognition systems," in *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, 2003, vol. 4, pp. 1576–1579. doi: 10.1109/tencon.2003.1273186.

[12] M. NarayanMohanty and R. Sikka, "oReview On Fingerprint-based Identification System," *Materials Today: Proceedings*, Apr. 2021, doi: 10.1016/j.matpr.2021.03.414.

[13] S. Tadvi and M. Kolte, "A Hybrid System for Fingerprint Identification," Researchgate.net, May-2010. [Online]. Available: https://www.researchgate.net/publication/49618605_A_Hybrid_System_for_Fingerprint_Identification.

[14] A. E. Amin, A. E. Amin, and A. F. Elgamal, "Performance Improvement for Fingerprint Recognition System Using Shape and Orientation Descriptors Optimization Text Summary View Project Multi-Agent Supervisory System View Project Performance Improvement For Fingerprint Recognition System Using Shape And Orientation Descriptors," *International Journal of Advanced Research in Computer Science*, vol. 5, no. 8, [Online]. Available: www.ijarcs.info

[15] B. Nagpal, M. Kumar, P. Pandey, S. Vij, and Vaishali, "Minutiae vs. Correlation: Analysis of Fingerprint Recognition Methods in Biometric Security System," vol. 5, no. 1, pp. 1–5, Oct. 2015, [Online]. Available: https://www.ijeat.org/wp-content/uploads/papers/v5i1/A4305105115.pdf

[16] Y. He, J. Tian, X. Luo, and T. Zhang, "Image enhancement and minutiae matching in fingerprint verification." [Online]. Available: www.elsevier.com/locate/patrec

[17] M. Fukuda, S. Hama, and T. Aoki, "Biometric Authentication Device, Biometric Authentication Method, and Computer Program for Biometric Authentication," Researchgate.net, Oct-2013. [Online]. Available: https://www.researchgate.net/publication/302677892_Biometric_authentication_device_biometric_authentication_method_and_computer_program_for_biometric_authentication.

[18] Yukihiro Abiko, "Biometric Authentication Device, Biometric Authentication Method and Computer Program for Biometric Authentication," US 8, 983, 143, B2, May 2015 [Online]. Available:

https://www.researchgate.net/publication/302861132_Biometric_authentication_device_biometric_authentication_system_biometric_authentication_method_and_recording_medium

[19] K. Kumar, B. Kumar, D. Kumar, and R. Shah, "Fingerprint Recognition using Minutiae Extraction." [Online]. Available: https://www.researchgate.net/publication/335109828

[20] F. Suthar, "Fingerprint Recognition in Biometric Security Systems", doi: 10.13140/RG.2.2.11683.17441.

[21] S. Tiwari, "An Introduction to QR Code Technology," in *Proceedings - 2016 15th International Conference on Information Technology, ICIT 2016*, Jun. 2017, pp. 39–44. doi: 10.1109/ICIT.2016.38.

[22] Y. Gon Kim and M. Seog Jun, "A Design of User Authentication System Using QR Code Identifying Method," Ieee.org, Nov-2011. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6316569.

[23] Z. Gao, G. Zhai, and C. Hu, "The Invisible QR code," in *MM 2015 - Proceedings of the 2015 ACM Multimedia Conference*, Oct. 2015, pp. 1047–1050. doi: 10.1145/2733373.2806398.