ISSN No:-2456-2165

Design of an Online Banking Authentication System, Implementing Mobile-OTP with QR-Code

[1]Chukwu, E. G
Federal University of Technology
Ikot-Abasi, Akwa-Ibom State

[2]Nwazuo E. K.
Rhema University
Aba, Abia State

[3]Oden P. J.
University of Nigeria
Nsukka, Enugu State

[4]Onwuasoanya U. K
Rhema University
Aba, Abia State

Abstract:- Financial institutions will keep working to make it possible for clients to move money, pay bills, and access critical information online. The internet banking landscape has changed substantially in recent years. Online banking has been targeted by thieves and cybercriminals looking to steal client data during this time. Fraudsters today frequently employ well-known attacks like phishing and pharming to get client data and gain access to online banking accounts. As a result, financial institutions are now quite concerned about the authentication of customers using online banking services. This study unequivocally shows that internet banking requires stronger authentication. It discusses the key security issues, criminal behavior, and development of robust authentication that are driving.

I. INTRODUCTION

With traditional signature mechanisms, the user who signs the document has complete control over how it is signed. With electronic signatures, however, the user is always dependent on an untrustworthy client. Despite the fact that secure revolving payments are employed, the user is usually unable to claim that the knowledge displayed on the screen truly matches the knowledge signed by the revolving payment. This shortcoming is common to any type of electronic transaction that requires some type of signature by the user. Examples include online banking and electronic signatures of contracts. The most significant drawback is that data on the client can be carelessly altered by malicious code. As a countermeasure, financial institutions are focusing on One Time Password (OTP) and have introduced OTP co-confirmation canters as one of the user confirmation measures; OTP is anonymous, immutable, and scalable, and can prevent knowledge leakage.

A. Background of Study

Online banking gives you complete control over your bank account using a computer or mobile device connected to the Internet. This operation includes transferring funds, depositing checks, and paying bills electronically. Traditional banks with branches generally allow you to access your account via the Internet. However, online banks and access providers primarily offer mobile access. You never see a banker in person, but you can access your account at any time with a mobile device or computer.

Online banking is one of the most daunting tasks the average Internet user performs. Most traditional banks now offer "secure" online banking. Banks offer the apparent "100% Online Security Guarantee," but in small print and usually with the condition that the user meets certain security requirements.

In the first quarter of 2009, the number of users of the National Banking System steadily increased: the average number of daily transactions exceeded 26.41 million and the number of transactions exceeded 26.9 trillion won. However, banks have been reluctant to reimburse users who have been victims of online frauds such as phishing and pharming; the first hacking incident in Korea in 2005 prompted the FSS (Korea Financial Supervisory Service) to announce comprehensive measures. One of the most notable measures taken by financial institutions is the use of one-time passwords (OTPs) as a method of user verification and the establishment of a common OTP verification center.

Currently, online financial transactions use security cards and public key certificates as a method of user verification, but recently one-time passwords have been introduced. A one-time password is a password that can only be used once, requiring the user to authenticate with a new password key each time. This ensures security even if a hacker exploits the password on the network or the user loses the password. OTPs are also anonymous, portable, and scalable, preventing information leakage. Types of devices used to generate OTPs include smart cards, USB keys, and fingerprint authentication. Our online banking authentication system uses "mobile OTP," one of the OTP-generating devices that offer the same security as existing OTPs, but with the convenience of mobile functionality and semi-permanent use. This not only reduces deployment costs but also facilitates the download of deployment disciples in the case of financial deployments. In addition, users do not need to pay any additional fees, except for the initial download cost.

On the other hand, the use of electronic banking is gradually increasing in daily life. Currently, online banking requires the use of a security card from the respective bank. However, current security card-based services are not suited to the modern mobile environment because it is impossible to know when and where online banking transactions will take place. In an emergency, it is impossible to perform online banking without a security card. To overcome these weaknesses and shortcomings of security cards, we proposed an authentication system that uses two-dimensional barcodes (2D barcodes) instead of security cards. Barcodes are a fast, easy, accurate, and automatic data collection method. Barcodes can track products efficiently and accurately at speeds not possible with manual data entry.

This paper proposes an authentication system for online banking that can provide higher security and convenience by using mobile OTP with QR codes, one of the 2D barcodes used in current international and national standards. The bank generates a QR code from the login information entered by the user, and the user uses his/her cell phone to read or scan the barcode. The cell phone then generates an OTP code from the login information and the user's hashed password. The user then enters the generated OTP code to complete the login process.

To achieve the above objectives we have introduced OTP (One Time Password) and QR code (2D barcode). We have described our new scheme and an analysis of the proposed authentication system. Additionally, we ended this paper with a concluding section.

B. Problem Statement

As fast web frameworks are created and individuals gain access to information, even budgetary businesses are occupied with web domains. In the field of pc organization, hacking is a specialized effort to control the normal behavior of system-related and associated frameworks. Today's online banking frameworks are exposed to hacking threats and their consequences and cannot be overlooked (Onu et. al, 2015). In the past, personal information has been disclosed through sophisticated techniques such as phishing and pharming to steal customers' login names and passwords. Therefore, mechanisms to protect customer information have become more fundamental and important. In this study, we proposed an alternative online banking authentication system that uses mobile OTP mixed with QR codes, a variant of two-dimensional standardized identifiers.

C. Research Aims and Objectives

The main objective of this study is to design and implement an online banking authentication system using a combination of mobile OTPs and QR codes, and to achieve it through one objective: to propose a new online banking authentication system that uses a combination of mobile OTP and QR codes as a variant of 2D barcodes.

Importance of this research

- The objective of this research is to develop a system that can manage user authentication and ensure proper security when connecting to an online bank
- This research is important for both the bank and the customer because it reduces the risk of unauthorized access to the customer's bank account
- It would be important for students, especially computer science students, as a reference for designing their projects
- Professors who teach systems analysis and design can also use it as a guide when teaching their students
- Presenters of workshops and conference papers could benefit, especially those who present or have presented work related to the design and implementation of authentication systems.

D. Scope of the Study

This study focuses on the design and implementation of an online banking authentication system using Mobile-OTP with QR-Code.

This system will not be developed to integrate all the features of online banking but will focus only on the features mentioned above. This system will not be responsible for any data loss in case its environment (network/installed system) is destroyed.

II. REVIEW OF RELATED LITERATURE

This chapter provides an overview of the literature review on online banking authentication systems using mobile OTPs with QR codes and other papers detailing their implications. It also describes the theoretical development of online banking and its authentication systems, integrating previous research and complementing existing systems.

A. Theoretical Developments

Internet banking emerged in the 1980s in the form of telephone banking and came into existence when it was used in homes (Muniruddeen, 2007). During this period, banks and financial companies in Europe and the United States began to work on the concept of "home banking." Since computers and the Internet were not yet widespread, the focus shifted to telephone banking (Sarel and Marmorstein, 2003; Gregory, et al. 2022). The first online banking applications appeared in the United States, and prominent banks such as Citibank and Wells Fargo began offering the service to their customers in 2001 (Gefen, Pearson, and Straub, 2008).

B. History of Online Banking

Banking has advanced significantly from the days of routine trips to the teller window. Customers can now deposit checks into their checking or savings accounts by taking a photo of them with their smartphone, or they can sign up to receive text message alerts from banks. Online banking was first developed in the 1980s, when it was much less common and practiced differently than it is now.

ISSN No:-2456-2165

In 1981, the first iteration of what is now known as internet banking was introduced. Four major banks—Citibank, Chase Manhattan, Chemical Bank, and Manufacturers Hanover—offered home banking to their customers in New York for the first time in the country and were the first to test this cutting-edge business strategy of providing remote services. The first online banking service in the UK was made available to consumers by Bank of Scotland under the name Homelink. To pay bills and transfer money, people had to have a phone or television connection to the Internet. In October 1994, Stamford Federal Credit Union became the first financial organization in the United States to offer Internet banking services to all of its members. This was the beginning of online banking as we know it today.

Online banking grew in popularity in the e-commerce sector over time as it continued to develop. Online banking appeared to gain traction among customers as major banks started to offer online goods and services. In the United States, more than 80% of banks offered online banking services in 2006, making it a popular practice. Online and mobile banking are expanding faster than the Internet, according to a 2010 report by financial services technology company Fiserv on customer billing and payment trends. Since its beginning, Bank of Internet USA has been a pioneer in mobile banking programs for well-known mobile devices, mobile check deposit, Popmoney for money transfers by SMS or email, and EMV chip technology. Online banking has continued to advance with technical innovation and ease.

Despite its slow adoption in the early days of online banking, online banking is proving to be here to stay: whereas in the 1980s you had to use a landline to pay bills, today you can transfer funds, pay bills, and deposit checks with the click of a mouse or the use of a mobile device. Payments, check deposits, online banking features, and services have evolved considerably since the early days of online banking. As technology continues to advance, online banking will become easier and more integrated into the average consumer's lifestyle.

C. Authentication for Online Banking

Effective authentication systems are necessary to meet the requirements of protecting customer information, preventing money laundering and terrorist financing, reducing fraud, combating identity theft, and promoting the enforceability of electronic contracts and transactions. In an online banking environment, the risk of dealing with unauthorized or misidentified persons can result in financial loss and reputational damage through fraud, disclosure of customer information, data corruption, or breach of contract. There are a variety of technologies and methodologies that financial institutions can use to authenticate customers. These methods include the use of passwords, personal identification numbers (PINs), digital certificates using public key infrastructure (PKI), physical devices such as smart cards, one-time passwords (OTPs), QR codes, USB plug-ins, and other types of "tokens," transaction profile scripts, biometric authentication and other uses.

The level of protection against risk offered by each of these technologies varies. The choice and use of authentication technology and methods should be dictated by the results of the financial institution's risk assessment process.

Multi-factor authentication schemes are more difficult to compromise than one-factor authentication schemes. Therefore, properly designed and implemented multi-factor authentication methods are more reliable and have a stronger deterrent effect against fraud. For example, the use of an ID/password is a one-factor authentication (i.e., something the user knows), whereas ATM transactions require multi-factor authentication that combines something the user has (i.e., a card) and something the user knows (i.e., a PIN). Multi-factor authentication methods may also include "out-of-band" checks to mitigate risk. The success of a particular authentication method is not merely dependent on the technology. It also depends on appropriate policies, procedures, and controls. An effective authentication method must be acceptable to customers, provide reliable performance, be scalable to accommodate growth, and be interoperable with existing systems and future projects.

D. OTP (One-Time Password)

A randomly generated password, the OTP is only good for one use. A gadget that can produce the OTP using an algorithm and cryptographic key is given to the user. The authentication server uses the same technique and key on the server side to validate the password's validity. For example, OTPs can be generated using a variety of software and devices, including PDAs, cell phones, and specialized hardware tokens. A PIN to unlock the OTP generator and the OTP smart card itself, which you own, are the two factors of two-factor authentication used by the most secure smart card OTP generators to ensure tamper protection.

The three processes necessary to generate OTP are shown in Figure 1. These include gathering external data, such as the time for synchronous OTPs and the challenge for asynchronous OTPs; using an encryption scheme with a shared secret key between the device and the authentication server; and, finally, formatting the OTP to specify its size (usually 6 to 8 digits).

Prior to recently, OTP solutions relied on patented, proprietary algorithms based on time and events. In 2005, the top businesses in the industry established OATH-HOTP as an open standard. The supply of numerous OTP-generating devices and authentication servers from various suppliers is made possible by this open standard. Standard algorithms like SHA-1 and HMAC are used by the HOTP algorithm, which is based on a secret key and counter that are shared by the client and server and uses a shared secret key and counter.

Because OTP does not require the installation of smart card readers, drivers, or PC software, it has advantages over PKI.

ISSN No:-2456-2165

Installing smart card readers, drivers, or PC software is not necessary. However, OTP just offers identification and authentication in terms of functionality, but PKI also offers further encryption and signature. Because OTP is password-based authentication, it is also susceptible to man-in-the-middle attacks like phishing scams. Since there is no mutual authentication between the PC and the ISP server, hackers can use fake websites to intercept the OTP and pretend to be the user on the actual website.

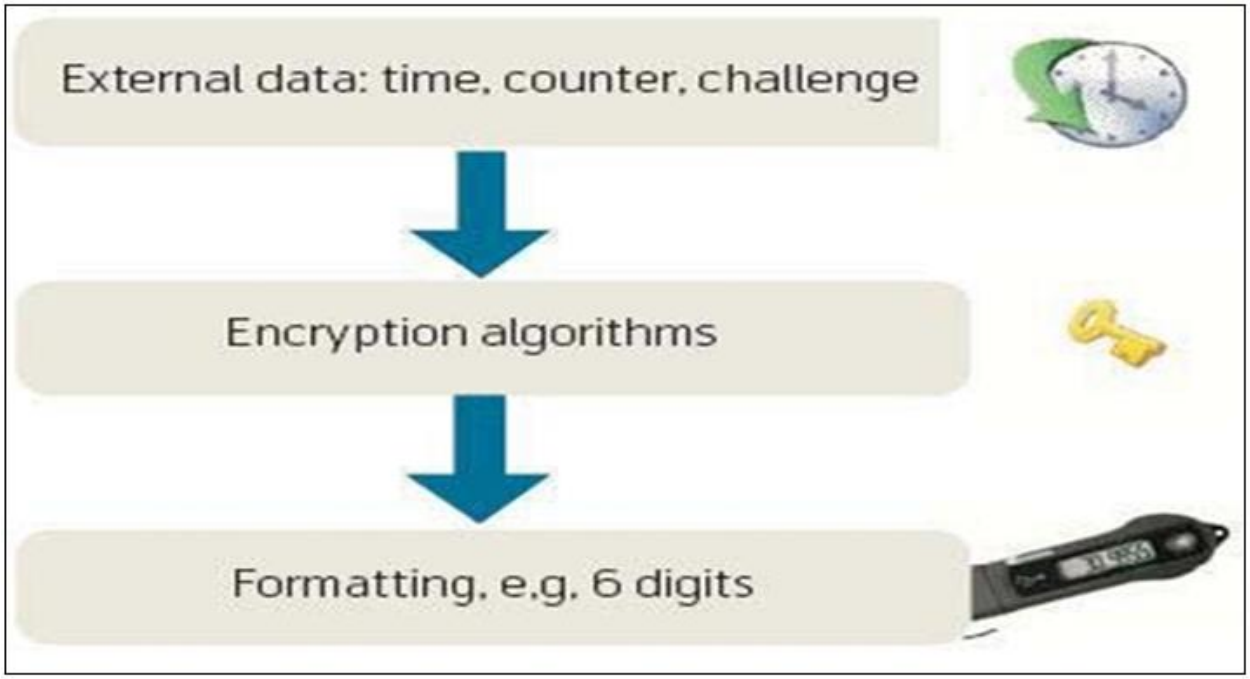

Fig 1 The Generation of One-Time Passwords

E. QR-Code (Two-Dimensional Barcode)

The ISO DataMatrix uses both open standards and proprietary two-dimensional barcodes, including Somacodes, Spotcodes, Rohs'visualcodes, ColorCode, Cybercode, MobileTag, VeriCode, ShotCode, eZcodes PDF417 (Portable Data File), and MaxiCode. (ISO/IEC 16022:2000) and QR-code (ISO/IEC 18004:2000) are well-known 2D barcode media, and there is no license fee for using DataMatrix or QR-code. No license fee is charged for the use of DataMatrix and QR-code.

Studies comparing these citations explain the superiority of encoding, but QR-code is more common in Asia and especially popular in Japan.

Fig 2 The Development of QR-Code

ISSN No:-2456-2165

The Japanese company Denso Wave invented the two-dimensional barcode known as the QR code in 1994. Originally employed for inventory control in the production of automobile parts, this kind of barcode is now widely used across a number of industries. The acronym "QR" stands for "Quick Response," which expresses the developer's goal to enable rapid decoding of the code's contents.

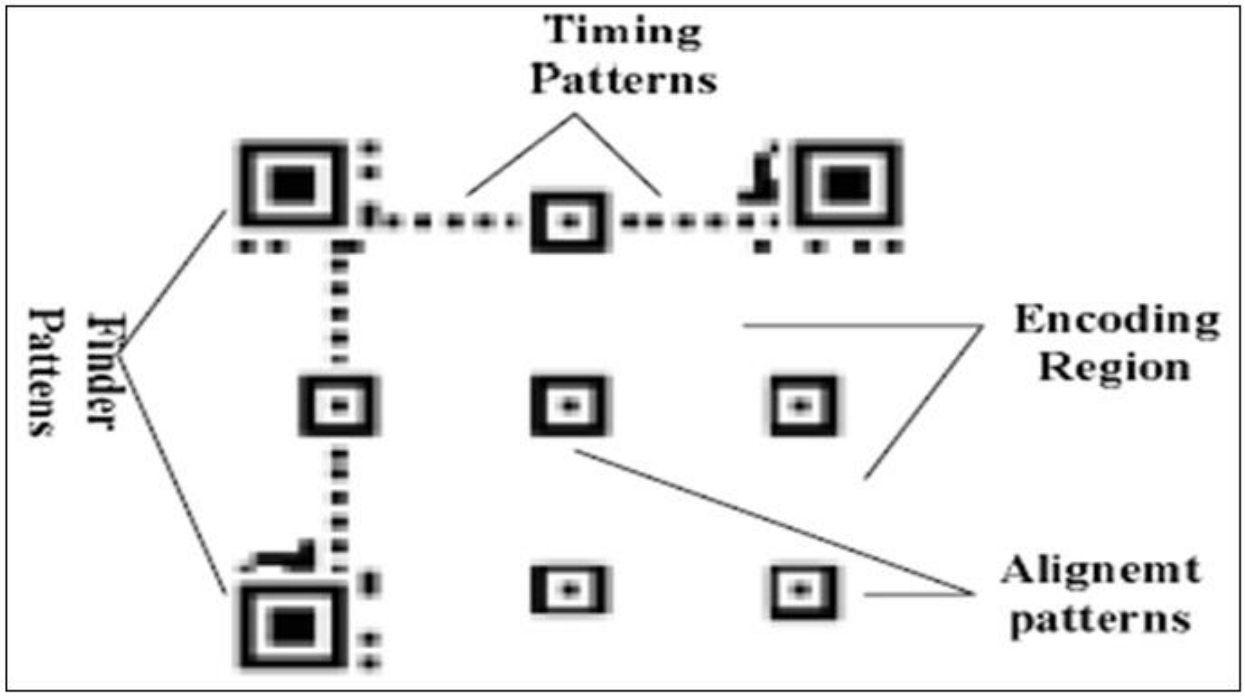

Fig 3 The Structure of QR-Code

Each QR Code symbol consists of an encoding area and a functional pattern as shown in Figure 2. Functional patterns include registration patterns, separation patterns, synchronization patterns, and alignment patterns. Search patterns located at the three edges of the symbol are intended to make it easy to identify the position, size, and tilt of the symbol.

QR Code is a matrix code that was developed and published with the main goal of being a symbol that can be easily interpreted by a scanner. While conventional barcodes contain data in only one direction (usually vertical), QR codes contain information in both vertical and horizontal directions. Compared to 1D barcodes, QR codes contain 7,089 numeric characters, 4,296 alphanumeric characters, 2,953 binary (8-bit) bytes, and 1,817 kanji and kana The QR Code can hold a very large amount of information: 7,089 numeric characters, 4,296 alphanumeric characters, 2,953 binary (8-bit) bytes, and 1,817 kanji and kana characters. Furthermore, QR Code has an error correction function. Even if a large portion of the code is distorted or damaged, the data can be recovered.

Items are labeled and estimated according to the QR Code standard so that the internal code may be read. Five steps are involved in barcode recognition: (1) edge detection, (2) shape detection, (3) identification of the control bar, (4) use of the control bar to determine the barcode's orientation, size, and bit density, and (5) calculation of the barcode's value.

For camera phones and PDAs that do not have a QR code reader, additional tools are available to decode the QR code by simply placing the device in front of the QR code. This operation is done automatically in the stream, and the user does not need to take a picture of the QR code. Good examples of free tools using this technique are the Quick-Mark reader and the 1-nigma reader, which are available for a wide range of models and devices. Quick-mark offers an additional feature to QR codes, allowing partial or total encryption of the code. This option encodes binary data (e.g., images) in the form of QR Code strings that can be scanned by the user to recover the original content.

This option encodes binary data (e.g., images) in the form of a string of QR codes that can be scanned by the user to recover the original content. If the end user only needs to scan the code and view the resulting message, the above software is sufficient. However, for developers who need to manage QR codes, several SDKs (Software Development Kits) have been released and some are already commercially available. For example, the Microsoft Windows Live Barcode project, OpenNetCF, QRCode Library for .NET Compact Framework, and Google ZXing (Zebra Crossing) project will be available soon. Twit88 offers open source projects related to QR codes.

ISSN No:-2456-2165

III. SYSTEM ANALYSIS

A. Proposed Authentication System

One of the most crucial components of the authentication system needs is security. When a user is authenticated by a server utilizing data supplied by their mobile device, this procedure must be secure to ensure that only authorized users can be served. Security and convenience are both crucial, and any shortcoming of an authentication system may eventually cause its use to be discontinued. The authentication method must therefore be user-friendly and offer the highest level of security.

Because of this, one crucial strategy suggested in this article is the usage of mobile OTPs, which at the moment create QR codes instead of protecting bank cards. The user must be identified in order to scan the QR code on a mobile device, and the OTP code is created by the bank using the user's login information and the cell phone's authentication application. By inputting the produced OTP code on the screen, the user completes the connection. The suggested approach makes the security of communication between the user's computer and the certifying authority an assumption.

Additionally, existing online banking authentication systems can be used to issue and register the user's certificate and digital signature, simplifying the authentication process.

- The user logs in using his/her login information to initiate login authentication
- The server sends the entered login information (LI) to the certification authority (CA) and at the same time converts the information displayed on the screen into a QR code with a random number value (RN`)
- The certification authority (CA) generates a QR code from the received login information (LI).
- The user converts the QR code on the screen with a mobile terminal: First, the user reads the random number value (RN) displayed on the screen with a mobile terminal (smartphone) and confirms the random number value (RN`). If the random number value is correct, the user proceeds to the next step to check the converted connection information. If the information is correct, the user generates an OTP code to the mobile device. If the information does not match, the connection is canceled.
- When the user executes the generated QR code, the mobile device scans the QR code and generates an OTP, and the generated OTP is also shared with the certification authority (CA).
- When the user enters the OTP code generated from the mobile device on the screen, the server (bank) sends the OTP to the certification authority (CA) and receives the OTP from the user.
- The certification authority (CA) compares the OTP code (OTP1) received, generates an OTP code (OTP2), and sends it to the server (bank) for approval of the OTP code
- Upon receiving the OTP authorization from the certification authority (CA), the server (bank) checks the entered OTP code against the user's consistent value and the user's digital signature. If the OTP value is not approved, the connection is canceled.

B. Assumptions

The proposed authentication system is based on the following assumptions

- The user and the certification authority (CA) share hashed login information (LI) to the user's online banking account through a secure process
- The user can use an authentication application, such as Google Authenticator, to recognize and decode a QR code on their mobile device
- Assume that communications are protected by SSL/TLS exchange between the user (PC), the certification authority (CA), and the service provider (bank)
- The user must download and use the mobile OTP program (algorithm) provided by the certification authority (CA) or service provider (bank)
- The OTP algorithm is generated between the user and the certification authority (CA) synchronized by the time-event coupling method.

C. System Architecture

System architecture is a conceptual model that defines the structure, behavior, and views of the system. The system architecture used in the proposed project is a three-tier architecture

D. Presentation Layer

The presentation layer of the proposed project is the front-end layer, also known as the user interface. The presentation layer is built on HTML5, Bootstrap, JavaScript, and Tailwind, a CSS framework for a fast workflow.

E. Application Layer

The application layer of the proposed project consists of the functional logic that drives the core functionality of the application. It is written in PHP Laravel using the Jetstream API.

F. Data Layer

The data layer consists of the database system, the database layer, and the data access layer. The database used for the proposed system is the MYSQL database. The application layer accesses the data through API calls.

IV. SYSTEMS DESIGN

A. Design Methodology

An method to software engineering called object-oriented analysis and design (OOAD) models a system as a collection of interconnected objects. Each object in the model represents a relevant entity. These models can be represented using a variety of notations, including unified modeling languages.

ISSN No:-2456-2165

In object-oriented analysis, the most important objective is to identify objects and describe them appropriately. Since objects must be given responsibilities, and responsibilities are the functions that the objects perform, the following design work becomes easier once these objects have been effectively identified (Onu et al, 2015). The result of object-oriented analysis is a description of what the system needs to do functionally in the form of a conceptual model (James et. al., 2016). This model is typically presented in the form of a set of use cases.

B. Unified Modeling Language

For the purpose of creating conceptual software diagrams, the Unified Modeling Language (UML) is a graphical notation. It can also be characterized as a general-purpose visual modeling language used to specify, depict, and create software system documentation. Instead than defining a set procedure, the UML definition is meant to be helpful as a component of an interactive development process. A system's static structure and dynamic behavior are both detailed in UML (James et. al., 2016).

In order to understand and manage dependencies, a complex system is divided into manageable components in software using the organizational framework provided by UML for grouping models into packages.

C. Use Case Diagrams

A use case diagram, in its most basic form, depicts the relationship between the user and the many use cases in which the user is involved. It also shows how the user interacts with the system. Figure 4 depicts the use case diagram for the suggested system.

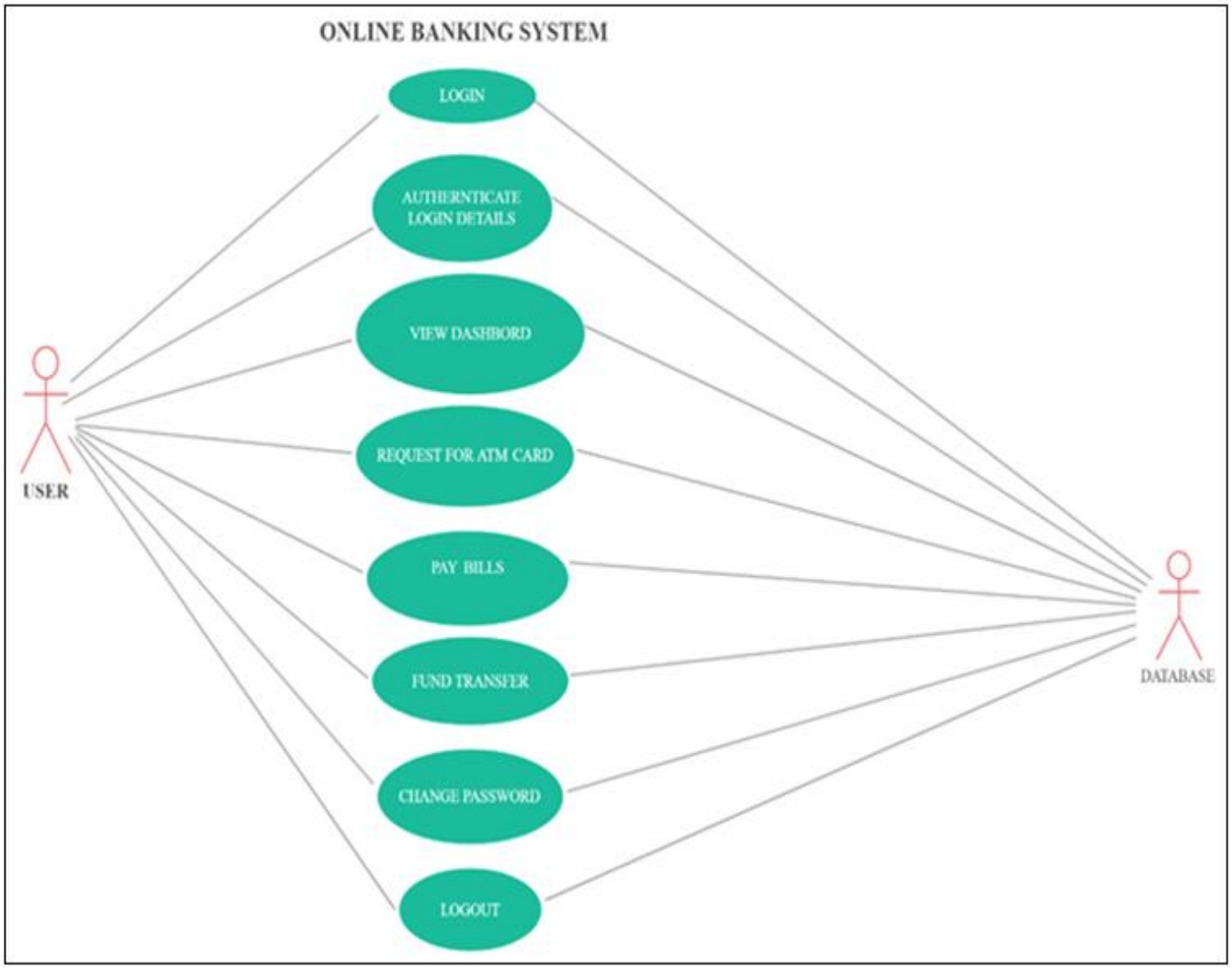

Fig 4 The Use Case Diagram of the Proposed System

ISSN No:-2456-2165

The Flowchart of the Proposed System

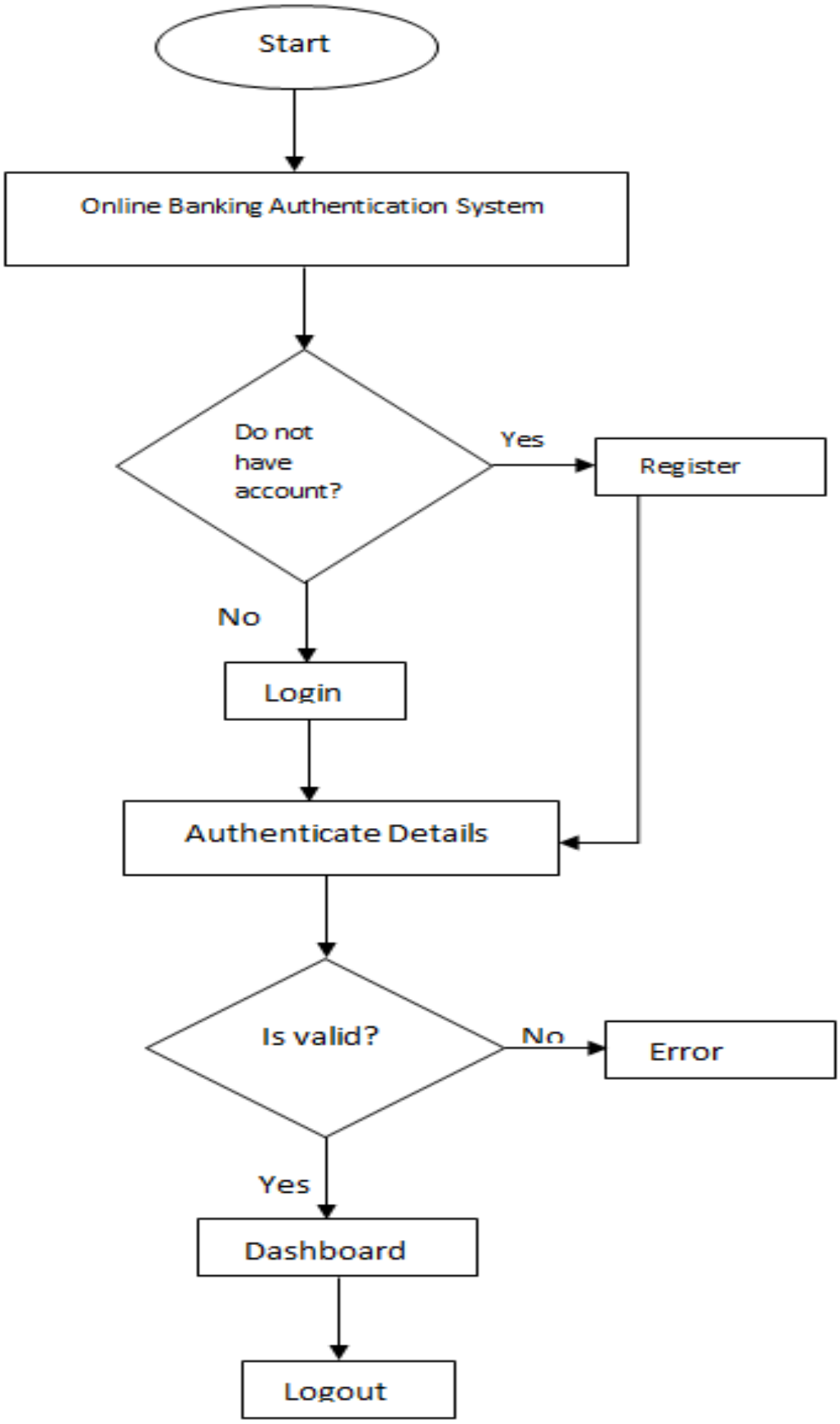

Fig 5 The Flowchart of the Proposed Online Banking Authentication System

ISSN No:-2456-2165

D. Database Design

The database used in developing this web application is the structured query language (MYSQL). The following tables were used in developing this web application.

Table 1 The Users Table

FIELD NAME	FIELD TYE	FIELD LENGTH	DESCRIPTION
ID	Bigint	25	Primary key
Name	Varchar	15	
E-mail	Varchar	20	Secondary key
E-mail_Verified_At	Timestamp		
Password	Varchar	20	
Two_Factor_Secret	Text		
Two_Factor_Recovery_Codes	Text		
Remember_Token	Varchar	150	
Created_at	Timestamp		
updated_at	Timestamp		

Table 2 The Personal Access Token Table

FIELD NAME	FIELD TYE	FIELD LENGTH	DESCRIPTION
Id	Bigint	20	Primary key
Tokenable_Type	Varchar	255	Secondary key
Tokenable_Id	Bigint	20	Secondary key
Name	Varchar	15	
Token	Varchar	64	Secondary key
Abilities	Text		
Last_Used_At	Timestamp		
Created_At	Timestamp		
Updated_At	Timestamp		

Table 3 The Sessions Table

FIELD NAME	FIELD TYE	FIELD LENGTH	DESCRIPTION
Id	Varchar	225	Primary key
User_Id	Bigint	20	Secondary key
Ip_Address	Varchar	45	
User_Agent	Text		
Payload	Text		
Last_Activity	Int	11	Secondary key

Table 4 The Password Resets Table

FIELD NAME	FIELD TYE	FIELD LENGTH	DESCRIPTION
Email	Varchar	20	Secondary key
Token	Varchar	225	
Created_At	Timestamp		

V. SYSTEM IMPLEMENTATION

This chapter identifies the overall picture of the system analyzed in the previous chapter and describes its requirements, the choice of the programming language used to conduct this study, and the development environment. The chapter also presents screenshots of the implemented online banking authentication system.

A. Choosing a Development Environment

The project was implemented using web application programming languages: hypertext preprocessor (PHP) with the Laravel framework, hypertext markup language (HTML), and relational database MySQL for storing user information.

Web technologies were used in the construction of this project for the following reasons

- Very flexible
- Easy integration and compatibility
- Efficient performance
- Cost-effective
- Good compatibility with the most common database

B. System Platform

The solution was developed using the Microsoft Windows operating system (Windows 10) and HP personal computers (PCs).

ISSN No:-2456-2165

C. Integrated Development Environment

The integrated development environment used to implement this software application is Microsoft visual studio code and Xamp.

D. Implementation Architecture

The implementation architecture shows the different components of the research work and their links. A diagram of the implementation architecture, including the following elements, is shown below.

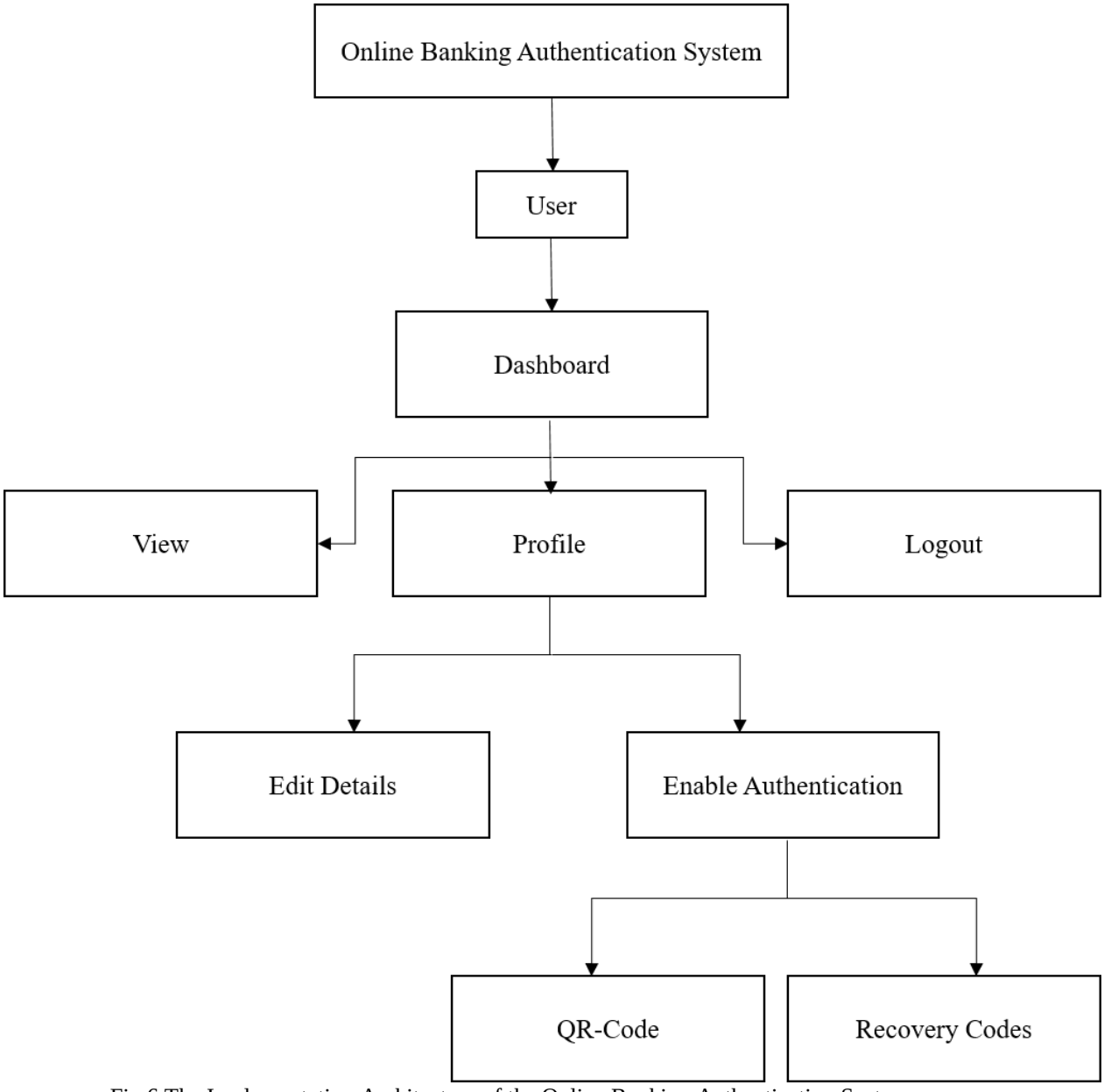

Fig 6 The Implementation Architecture of the Online Banking Authentication System

E. Software Testing

Software testing was conducted at each stage of development to ensure that the software was bug-free. After implementation, the software was evaluated by a number of users to obtain feedback for improvement. The software was also tested on localhost using Xampp, which acts as a local server that renders the web application in conjunction with the MySQL database. The software showed no signs of bugs.

Below are screenshots of the web application, from the home page to the registration, to the user interface of the client module, to the administration module.

ISSN No:-2456-2165

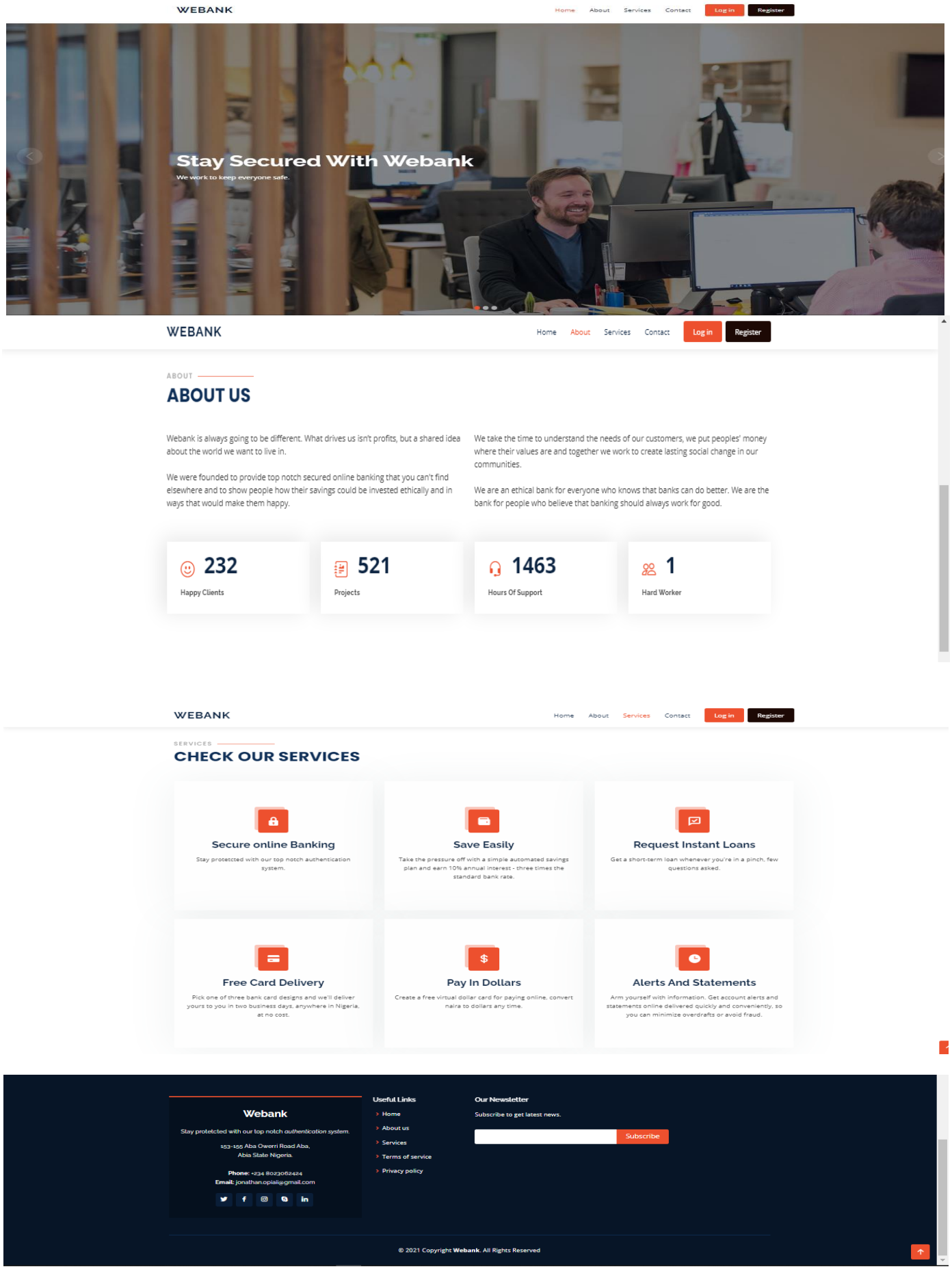

Fig 7 The Landing Page of the Online Banking Authentication System

ISSN No:-2456-2165

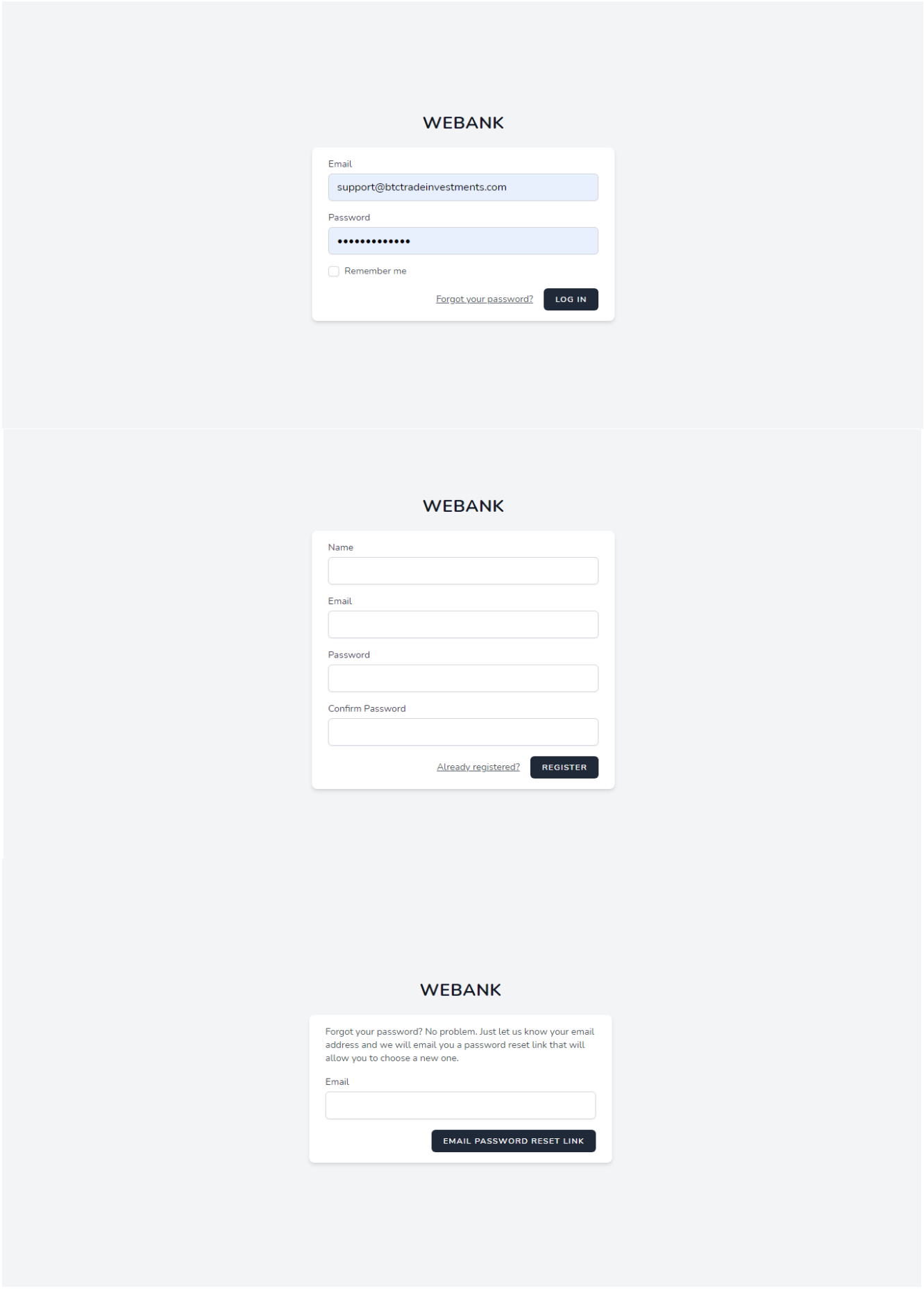

Fig 8 The Login, Registration and Reset Password Page of the Online Banking Authentication System

ISSN No:-2456-2165

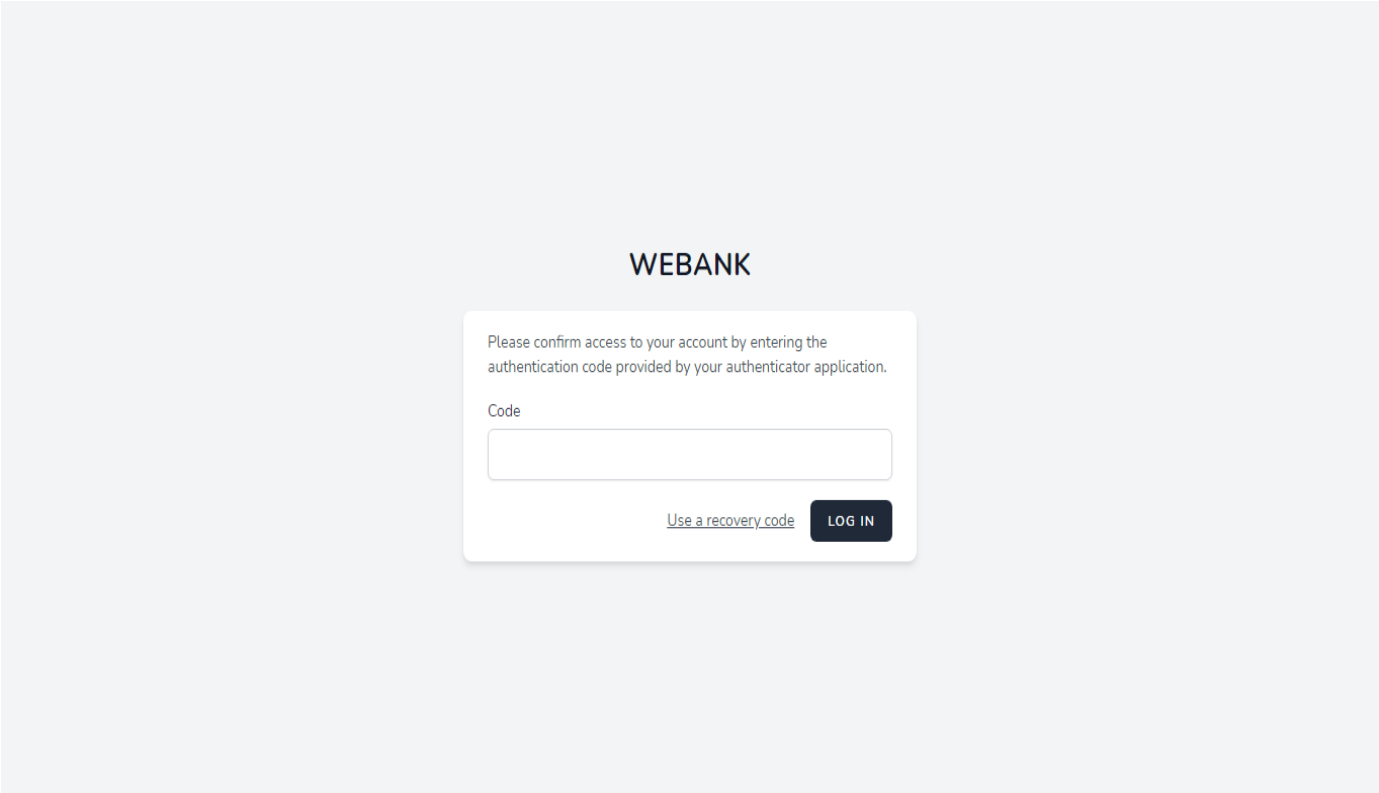

Fig 9 The Authentication Page of the Online Banking Authentication System

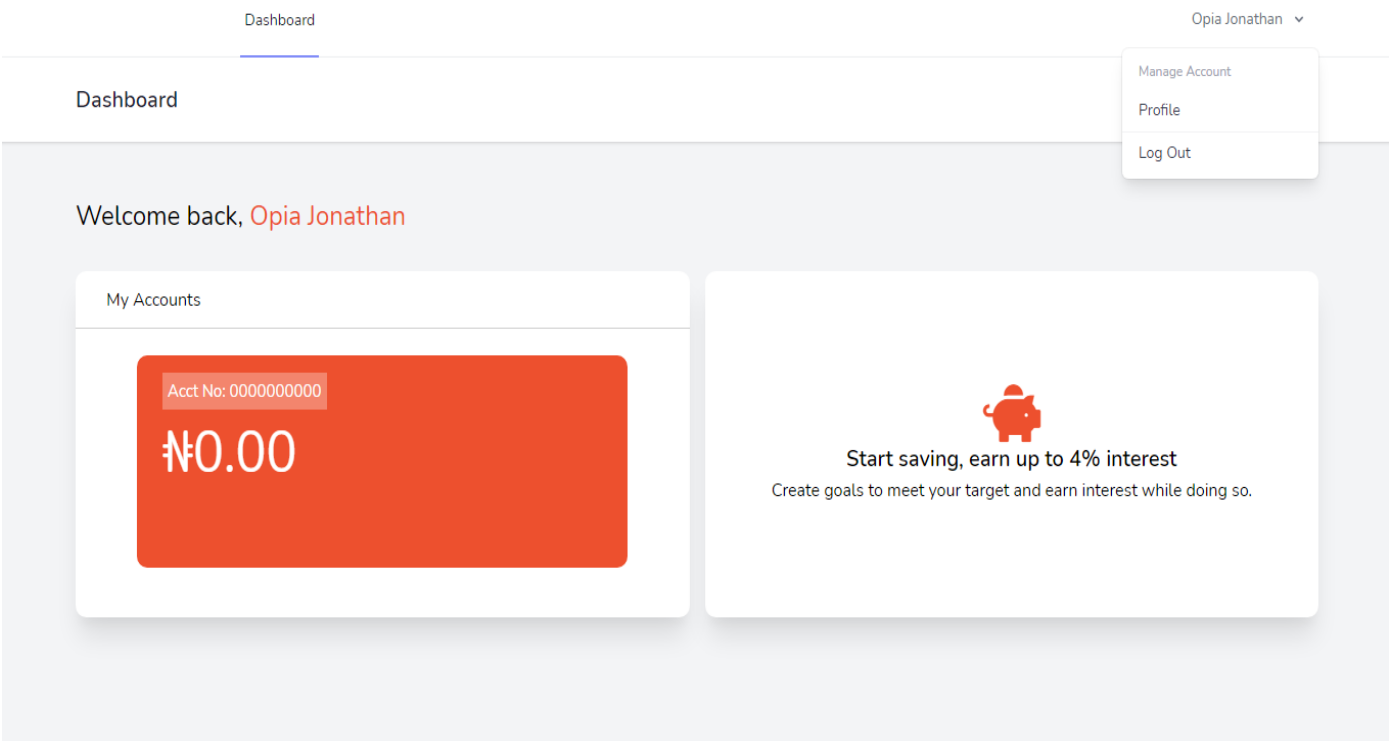

Fig 10 The Dashboard of the Online Banking Authentication System

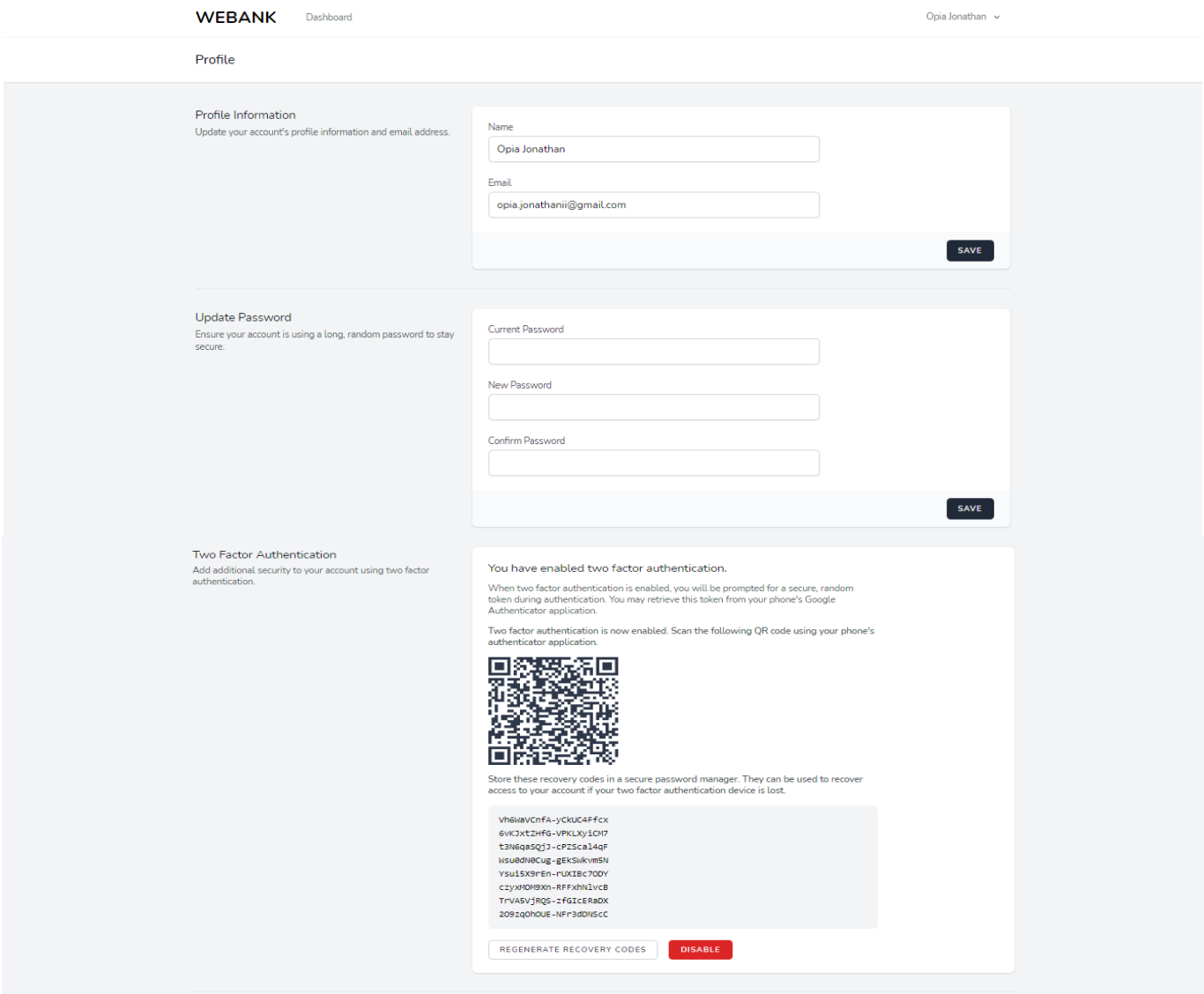

Fig 11 The Edit Profile and Enable Authentication page of the Online Banking Authentication System

VI. DISCUSSION OF RESULTS

This section provides an overview of the outcomes of the project.

A. Security Analysis

We assume that the communication is protected by an SSL/TLS tunnel between the users (PC), the Certificate Authority (CA), and the service provider (bank). As a result, our proposed system uses the camera of the mobile device to recognize the QR code and does not separate the communication between the user's PC and the mobile device, so a malicious user cannot analyze the content of the communication. In addition, the user and the certification authority (CA) share hashed login information (LI) in a secure process during initial registration. In the proposed system, the OTP value is changed every 30 seconds to prevent phishing attacks. After verifying the legitimacy of the service provider, the login information is converted. At the same time, the proposed system requires pre-input of login information via QR code and authentication with a public certificate in order to generate an OTP. Through this process, the system can confirm that the OTP user is a legitimate user and block the use of malicious users. In addition, the time value used to generate the OTP code cannot be arbitrarily changed since the transfer time requested by the user is used.

B. Responsive User Interface

It was an important requirement for this system that the application responds to any screen. To achieve this, we developed the system's user interface using Bootstrap and Tailwind, a CSS front-end framework. This allowed the user interface to work on all types of screens, including smartphones, tablets, laptops, and desktops. It also responds to device proximity. The application interface automatically adapts to the size of the device, whether it is held horizontally or vertically; Bootstrap and Tailwind CSS also have the ability to reorganize page elements to fit the screen. To compare the results of using an automated system versus standing in line, 10 people simulated a queue management system, and another 10 people simulated using a web application. The results showed that the 10 people using the web application completed their orders in less than 3 minutes per person, while those in line took 15 minutes longer.

ISSN No:-2456-2165

C. User Guide

- To use the software application, the user must follow these instructions
- Register with the web application and access the user dashboard interface
- Upon successful registration, proceed to the Profile page.
- On the Profile page, enable authentication.
- Once authentication is enabled, scan the QR code with Google authenticator and save the recovery code in a safe place.

VII. CONCLUSION

In this paper, we have designed an online banking authentication system that protects the online banking login process via a web application. This system reduces unauthorized access to a user's account. The ultimate goal of developing this system is to improve the security of online banking, and this approach will undoubtedly have a positive impact on the security of users' accounts and increase their trust in banks.

Although the use of electronic banking services is gradually increasing in daily life, existing online banking services require the use of the respective bank's security card, which is not compatible with the modern mobile environment where one never knows when and where online banking services will be used In the event of an emergency, the security card must be used to access online banking services. In an emergency, online banking cannot be used without a security card. To eliminate the discomfort of security cards, an online banking authentication system using 2D barcodes instead of security cards has been proposed.

The bank must generate a QR code using the user's login information, recognize the user by reading the code with a cell phone, generate an OTP code using the QR code, and finally authenticate the user by entering the generated OTP code on the screen.

This paper proposes a new authentication system for online banking that is more secure and convenient by using QR codes and mobile OTP, one of the 2D barcodes used in current international and national standards.

In electronic financial services, the importance of security and ease of use are like two sides of a coin: what appears on one side determines its supply. Therefore, it is necessary to seek security features that satisfy all of the ease-of-use and security requirements of electronic financial services.

RECOMMENDATIONS

Since this research work focuses only on login authentication, it can be extended to all aspects of electronic banking that require authentication, such as "transaction authentication".

REFERENCES

[1]. *Gefen*, Pearson & *Straub*, 2003. An Exploratory Study into the Adoption of Internet Banking in a Developing Country: Malaysia, *Journal of Internet Commerce*, May 2008, vol. 16, no.3-13

[2]. FU Onu, PU Osisikankwu, CE Madubuike, G James, Impacts of Object Oriented Programming on Web Application Development. International Journal of Computer Applications Technology and Research Volume 4– Issue 9, 706 - 710, 2015, ISSN: 2319–8656.

[3]. Muniruddeen L., An Examination of Individual's Perceived Security and Privacy of the Internet in Malaysia and the Influence of This on Their Intention to Use E-Commerce: Using An Extension of the Technology Acceptance Model, *Journal of Internet Banking and Commerce*, December 2007, vol. 12, no.3 http://www.arraydev.com/commerce/jibc/

[4]. *Sarel*, D., & *Marmorstein*, H. (*2003*). Marketing Online *Banking* Services: The Voice of the Customer. Journal *of Financial Services Marketing*, 8, 106-118.

[5]. James, Gabriel Gregory, Okpako Abugor Ejaita & Inam, I. A. Development of Water Billing System: A Case Study of Akwa Ibom State Water Company Limited, Eket Branch. The International Journal of Science & Technoledge. Vol 4 Issue 7 July, 2016 (ISSN 2321 – 919X), www.theijst.com.

[6]. Gregory Gabriel James, Abugor Ejaita Okpako, C. Ituma, J.E. Asuquo. Development of Hybrid Intelligent based Information Retreival Technique. International Journal of Computer Applications (0975 – 8887) Volume 184– No.34, October 2022.