DEVELOPMENT OF A MORE SECURED BANKING TRANSACTION AUTHENTICATION APPLICATION

Thesis Submitted in Partial Fulfillment of the Requirement For the Degree of

B.Sc.

In Computer Science

By

DANKWARA ADAMU SANI BU/19C/IT/3777

To

The Department of Computer Science Baze University, Abuja

[OCTOBER, 2022]

# DECLARATION

This is to certify that this Thesis entitled [**DEVELOPMENT OF A MORE SECURED BANKING TRANSACTION AUTHENTICATION APPLICATION** , which is submitted by

[DANKWARA ADAMU SANI] in partial fulfillment of the requirement for the award of degree for B.Sc. in Information Technology to the Department of Computer Science, Baze University Abuja, Nigeria, comprises of only my original work and due acknowledgement has been made in the text to all other materials used.

Date: [18TH OCTOBER,2022] Name of Student: [DANKWARA ADAMU SANI]

**APPROVED BY** …………………

# HOD

Dept. of Computer Science

# CERTIFICATION

This is to certify that this Thesis entitled [**DEVELOPMENT OF A MORE SECURED BANKING TRANSACTION AUTHENTICATION APPLICATION**], which is submitted by

[**ADAMU SANI DANKWARA**] in partial fulfillment of the requirement for the award of degree for B.Sc. in Information Technology to the Department of Computer Science, Baze University Abuja, Nigeria is a record of the candidate’s own work carried out by the candidate under my/our supervision. The matter embodied in this thesis is original and has not been submitted for the award of any other degree.

Date:18TH OCTOBER,2022 Supervisor: Mr Gilbert George

# APPROVAL

This is to certify that the research work, Dental Management System and the subsequent preparation by [DANKWARA ADAMU SANI] with [BU/19C/IT/4538] has been approved by the Department of Computer Science, Faculty of Computing and Applied Science, Baze University, Abuja, Nigeria.

By

Mr. Gilbert George Date

1st Supervisor

[Full name] Date

2nd Supervisor

Dr. C. V Uppin Date

Head of Department of Computer Science

Prof . Peter Ogedebben Date

Dean, Faculty of Computing and Applied Science

Prof. CHOJI Davou Nyap Date

External Examiner

# DEDICATION

I dedicated this study to Almighty Allah from the beginning of this program to the end. I also pray for my parents for their guide and support. I am also proud to have you as a parent Alhaji Sani Dankwara for his spiritual and financial support.

ABSTRACT

Over the years, the issue of banking fraud has become a very huge problem in the banking system of today. The percentage of banking fraud has risen greatly day-by-day by the cyber criminals coming up with different strategies such as cloning SMS and hacking into the database of unencrypted banking system. The major aim of the project is to great a more secured banking system for username to use flexibly without an thought of been hacked at an point. In this case AES(Advanced Encrypted Standard) would be deployed in the aspect of encryption of the OTP in the banking web app. The OTP would be involve in login feature and all other transaction that would take place.

# TABLE OF CONTENTS

[CHAPTER 1: INTRODUCTION](#_bookmark0) 2

* 1. [OVERVIEW](#_bookmark1) 2
  2. [BACKGROUND AND MOTIVATION](#_bookmark2) 2
  3. [STATEMENT OF THE PROBLEM](#_bookmark3) 3
  4. [AIM AND OBJECTIVES](#_bookmark4) 3
  5. [SIGNIFICANCE OF THE PROJECT](#_bookmark5) 4
  6. [PROJECT RISKS ASSESSMENT](#_bookmark6) 5
  7. [SCOPE/PROJECT ORGANIZATION](#_bookmark7) 5

[CHAPTER 2: LITERATURE REVIEW](#_bookmark8) 6

* 1. [INTRODUCTION](#_bookmark9) 6
  2. [HISTORICAL OVERVIEW](#_bookmark10) 6
  3. [RELATED WORK](#_bookmark11) 7
  4. [SUMMARY](#_bookmark12) 9

[CHAPTER 3: REQUIREMENTS, ANALYSIS, AND DESIGN](#_bookmark13) 10

* 1. [OVERVIEW](#_bookmark14) 10
  2. [PROPOSED MODEL](#_bookmark15) 10
  3. [METHODOLOGY 31](#_bookmark15)
  4. [TOOLS AND TECHNIQUES](#_bookmark15) 19
  5. [ETHICAL CONSIDERATION](#_bookmark15) 21
  6. [REQUIREMENT ANALYSIS](#_bookmark16) 21
  7. [SYSTEM DESIGN](#_bookmark17) 23

|  |  |
| --- | --- |
| [*3.7.1 Application Architecture*](#_bookmark18) | *24* |
| [*3.7.2 Use Case*](#_bookmark19) | [*1*](#_bookmark19)*7* |
| [*3.7.3 Data Design*](#_bookmark20) | *28* |
| [*3.7.4 Activity Diagrams*](#_bookmark21) | *29* |
| [*3.7.5 Dataflow Diagram*](#_bookmark22) | *30* |
| [*3.7.6 Control Flow Diagram*](#_bookmark23) | *31* |
| [*3.7.8 User Interface Design*](#_bookmark24) | *33* |
| [*3.8 Summary*](#_bookmark25) | *34* |

[**CHAPTER 4: IMPLEMENTATION AND TESTING**](#_bookmark26) **35**

* 1. [OVERVIEW](#_bookmark27) 35
  2. [MAIN FEATURES](#_bookmark28) 35
  3. [IMPLEMENTATION PROBLEMS](#_bookmark29) 36
  4. [OVERCOMING IMPLEMENTATION PROBLEMS](#_bookmark30) 37
  5. [TESTING](#_bookmark31) 38
     1. [*Tests Plans (for Unit Testing, Integration Testing, and System Testing)*](#_bookmark32) *38*
  6. [USE GUIDE](#_bookmark33) 41
  7. [SUMMARY](#_bookmark34) 48

# [CHAPTER 5:CONCLUSION AND RECOMMENDATION](#_bookmark35) 49

* 1. [OVERVIEW](#_bookmark36) 49
  2. [OBJECTIVE ASSESSMENT](#_bookmark37) 49
  3. [LIMITATIONS AND CHALLENGES](#_bookmark38) 50
  4. [FUTURE ENHANCEMENTS](#_bookmark39) 50
  5. [RECOMMENDATIONS](#_bookmark40) 51
  6. [SUMMARY](#_bookmark41) 52

# [REFERENCES](#_bookmark42) 53

# [APPENDICES](#_bookmark43) 54

# LIST OF TABLES

TABLE 1 RISK ASSESSMENT 5

TABLE 2 WATER FALL MODEL PHASES 15

TABLE 3 SPIRAL MODEL PHASES 17

TABLE 4 OTP CODE GENERATOR 20

TABLE 5 HARDWARE REQUIREMENT 21

TABLE 6 SOFTWARE REQUIREMENT 22

TABLE 7 FUNCTIONAL REQUIREMENT 22

TABLE 8 NON FUNCTIONAL REQUIREMENT 23

TABLE 9 UNIT TESTING 37

TABLE 10 INTEGRATION TESTING 38

TABLE 11 TEST TRACEABILITY MATIX 39

# LIST OF FIGURES

FIGURE 1 PROPSOSED 10

FIGURE 2 METHODOLOGY USEDL 12 FIGURE 3.WATER FALL 14

FIGURE 4 SPIRAL MODEL 16

FIGURE 5 ACCOUNT OPENING DIAGRAM. 24 FIGURE.6 PAYMENT PROCESS DIAGRAM. 26 FIGURE 7 TRANSFER PROCESS DIAGRAM. 26

FIGURE 8 USE CASE DIAGRAM. 27

FIGURE 9 DATA DESIGN 28

FIGURE 10 ACTIVITY DIAGRAM FOR SYSTEM USERS. 29 FIGURE 11 DATA FLOW DIAGRAM 30

FIGURE 12 CONTROL FLOW DIAGRAM 31

FIGURE 13 ENTITY RELATIONSHIP DIAGRAM 32

FIGURE 14 GUI 33

FIGURE 15 LANDING PAGE 41

FIGURE 16 ACCOUNT CREATIONG PAGE 42

FIGURE 17 LOGIN INTERFACE 43

FIGURE 18 FORGOTTEN PASSWORD 43

FIGURE 19 CUSTOMER USER INTERFACE 44

FIGURE 20 OTP REQUEST 45

FIGURE 21 SEARCH PAYMENT GATEWAY 46 FIGURE 22CUSTOMER ACCOUNT DETAILS 47 FIGURE 23 STATEMENT OF ACCOUNT 47

FIGURE 24 ACCOUNT DELETING 48

FIGURE 25 TRANSFER PAYMENT GATEWAY 49

FIGURE 26 DOWNLOAD OF STATEMENT 49 FIGURE 27 STATEMENT OF ACCOUNT DOWNLOAD

# CHAPTER 1: INTRODUCTION

# Overview

Banking application as we all know has become a major impact in our society today. Users of most banking application have come to notice the problem of remote authentication fraud.

Basically when we talk about remote authentication fraud, we are referring to having access to a person financial account without the proper permission and carrying out illegal activities with might include stealing from the victims account due to access of information of the owner being intercepted, Christopher et al (2006).

Remote authentication comes in various ways which most us are familiar with, such as receiving calls from people pretending to be your bank customer-care and requesting for information regarding your customer account. another way authentication fraud takes place is interception of individual OTP which is sent from their various bank to grant some transaction being carried out on various accounts which might be login code to their mobile bank application or code to perform a transaction. Remote authentication fraud has been an ignored issue over the years and due to that, it has brought about so much insecure in the banking system application with a rapid rate of authentication fraud on a daily basis. The sole purpose of this project is to provide a more secured authentication system against any type or form of authentication fraud. As we all know, security cannot never be 100% in any system. This project seeks to reduce the level of remote authentication fraud, (Mahdi, A. and Zhila A., 2008). Nevertheless, we will work hand in hand with other related researches relating to remote authentication fraud and make use of some concept if needed.

# Background and Motivation

Following the COVID-19 pandemic, an increase in remote authentication fraud has been notice according to new research reveals that 2020 was a time for significant increases to fraud with a number of types of credit. Between 2019 and 2020, there were notable increases in fraud in the areas of car

loans, mortgage lending, personal loans and lines of credit, according to a 2021 report from Javelin Strategy & Research.

Heightening the need for greater attention to authentication fraud, the COVID-pandemic increased demand for more consumers to enroll in online or mobile (digital) accounts to make remote payments. In fact, average U.S. consumer e-commerce spending was 36% of total spending in December 2020, up from just 26% in March 2020.As we can see so many people have an enroll into mobile or online banking which means that new ways to intercept the system are coming up so this really motivated me to look into it and to put my idea into use it might not solve the whole problem of authentication but my main goal is to provide a platform for consumer or user to be able to carry out transaction with a rest of mine without any thought of theft due to how the system is going to be very secured and only the customer would have access through the use of hybrid cryptography and under that, we will be use the asymmetric encryption which consist of public and private key to encrypt details of the user in other words, only the user using his private key can decrypt a message sent to him

# Statement of the Problem

While there are many authentication methods to prevent remote fraud, these methods provide different levels of protection and may function independently of each other. Because of the changing nature of fraud, the effectiveness of some methods is declining. These methods are being replaced with stronger, but not widely adopted, alternatives across the payments industry. The sophisticated attacks to the payment system expose flaws in current authentication practices and create a need to develop more complex defense strategies. Remote authentication fraud already has some any method put in place to tackle different aspect of fraud. As this program is concern, we are looking into aspect of securing the already secured authentication system in place such as the multi-layered and multi-factor authentication system. This above concept are really strong when it comes to securing authentication system. Nevertheless, the problem in hand is, to find a way to restrict fraudster from intercepting any information of a user that is been sent either from his financial industry or payment system redirecting him to his bank. For more clarity, we are trying to find a way of stopping fraud relating to one-time password or OTP. Basically the problem we have in hand to give a solution is remote authentication fraud all of kind and with the help of the hybrid cryptography we tend to make this goal of ours going through. Under the study of security we are familiar with the major goal of security which are confidentiality, integrity and available. From research and some case studies, it has been conclude that security cannot be balance, in the sense that increasing one lowers the other but in this case, we

are adopting a system that security would be at it full capacity and only an authorized user can gain access after providing the valid information and then being able to decrypt the encrypted information sent so authorization can take place

# Aim and Objectives

This study is focusing on basically on a more secured authorization fraud and in other to do so, we are going to implement the following strategies in achieving in the goal which is creating a more secured platform for the daily transaction of user without any act of interception from an unauthorized user. In every system a method is stated and research to make sure it fit the problem that is meant to be solved. In this study we have decided to use the hybrid cryptography due its various strategic algorithm which are very hard to intercept because of the level of complex it comes with. Under the hybrid cryptography we are selecting the concept of symmetric encryption to toughen up the system that is already in place. The aim as I mentioned earlier is to develop a most authentic and secured,

Platform for day-to-day transaction. After we get to implement this algorithm by the end this program, we should be able to get achieve our goal with the AES(Advance Encryption Standard) algorithm, documentation and implementation from the research made and tools of design, requirement and implement.

# Significance of the Project

First of all, every project/project has a significance which is the reason why that project can to be and the problem for it to tackle. In case of this study, the significance of this project is generally based on security of daily transaction made on either bank platform or any payment system platform Gupta, P.

K. (2008). Security is a very broad study on its own but for the scope of this project, we are dealing with the securing of authentication system of financial industry in general. This is not only secure but also enhancing some features already in place to protect the current system from an act of remote authentication. After some time of study and research it was noticed that the security system of financial industry is a bit behind from another sections. It has come to public awareness that financial industry can’t protect the information of their various customer due the lack of solid secure authentication system in place. Nevertheless the system currently in use are not bad themselves. As nice system are been launched to use all this criminal are also discovery new ways to catch with the new system in place.

# Project Risks Assessment RISKS

|  |  |
| --- | --- |
| Inability to carry out research due to loss of hardware/software resources | Be aware of and observe school IT security procedures  Secure Android mobile phone when not in use. |
| Loss of work due to equipment failure /loss | Weekly data backup to H drive |
| Software availability (Unavailability of API’s) | Alternative API’s will be checked for. Software  requirements will be identified in good time for possible contentious software |
| Late delivery of hardware  component | Hardware requirements will be identified in good  time to be able to order them in good time |

Table 1: Risk Assessment

# Scope/Project Organization

The scope of this project is to develop a more secured authentication platform/application which has enhance features of the component of a more secured system. During this scope it is also necessary to have a good tool to carry the design, functional requirement and implementation Gupta, P. K. (2008). Furthermore, this project has other minor goal to be achieved before remote authentication fraud can take place. Some of these goals are to research previous related studies under concept of authentication fraud and make use of some of the technique and methods they implemented and also to notice areas that needs adjustment to improve the current system in place. As I mention early, the scope of this project is to develop a well secured system with a strong authentication platform against authentication fraud.

The remaining parts of this project which is chapter 2 consist of review of related literature for the techniques and technology used in the implementation and development of a more secured banking transaction authentication application using hybrid cryptograph, the historical overview, related work and summary. Chapter 3 describes the methodology applied during implementation and development of a more secured banking transaction authentication application using hybrid cryptography. Chapter

4 describes the design and testing of the implemented application while. Chapter 5 describes the concluding part of the project, discussion and recommendations for the implemented project.

# CHAPTER 2: LITERATURE REVIEW

# Introduction

Authentication is basically a method of identify a user or an individual in the sense that it identify the user as who they said they are and that the account holder of a particular account is the user as he said he. Authentication has been a major aspect in every concept of security system Kannabira & Narayan (2005). When we talk of banking authentication it simply means the method use in banking system to protect prevent and preserve data of customer from been tampered with and use to carry out various transaction without the acknowledgement of the holder of that particular account. In the process of every authentication system they are built on very strong algorithm which prevent various types of attack. For the sake of this project which has an aim of enhancing the current online banking system to solve the problem of authentication fraud we are going to be using the hybrid cryptography and under that we will apply the RSA and MD5 algorithm simultaneously as we move on ahead. In every system we cannot fully have a protected system because all the goal of security system cannot be achieved at once as one is progress another must be decreasing but are major aim and object is to add more encryption to the system already in place to make it less volatile and harder for hackers and scammers to gain access.

# Historical Overview

Over the years and due to previous incidence of Covid pandemic, a large amount of customers moved online and as a result that fraudsters have been taking advantage of the high population of the online banking system to commit remote authentication fraud. As a result that, banking community have come to a conclusion of advancing the authentication system already in place to makes sure that system is encrypted in both database of the banking system and mobile account of different holders. Furthermore, different programmer around the world have been able to come up with various method of authentication to prevent and act of fraud on the banking. From the various research I have made and gone through such as the article like “strategies for fighting remote authentication fraud” by the author Elizabeth.J, (2021)and some many more who have given their thought and ideas out to the general public on method they have examine, tested and used to enhanced the banking system already in place. This project is main focusing on majorly two aspect of the authentication system to apply on the banking system currently function. As we all bank user know, the current system uses either your SMS or EMAIL to send a code of numeric value known as the OTP of any act of authentication to allow authorization access. Multiple cases have been report of a case whereby a customer either lose his Sim card attach to his bank and his OTP get compromised and fraudster take advantage an carry

out fraud on that account. All this possible to the absence of a good encryption system put in place to encrypt every stages involve in the banking system, Kannabira and Narayan (2007).

# Related Work

* + 1. **Enhancing online banking authentication using hybrid cryptographic method**

Security of Electronic payment is a crucial factor today, as many clients choose to do transactions online instead of going to banks in person. Electronic transactions over an insecure Internet communication channel get harder to secure as Internet traffic increases. Here, well designed data encoding methods, secure transactional methods, and a dependable third party that maintains the database electronically are the key security components. Only employing conventional encryption techniques in a reliable and secure route of communication can data security be kept up to date? The most dangerous hazard in this situation, though, is the theft of client data for any nefarious reason, such serious internet attacks. For electronic transactions via wireless networks, the suggested encryption approach ensures adequate security. This report clearly illustrates the requirement for stronger verification in online banking. It highlights the significant safety concerns, unlawful activity, and expansion of online channels led by customers and financial institutions that are driving the demand for well-built verification. This study offers a comprehensive analysis of the different authentication options available on the market, as well as a set of guidelines for picking and implementing superior authentication that are based on the knowledge and comprehension of industry professionals and customers.

* + 1. **A Review of SMS Security Using Hybrid Cryptography and Use in Mobile Money System** Mobile technology has spread faster throughout the developing world in the last dozen years than any other technology in history. Mobile money is the most recent phenomenon spawned by mobile technology. SMS (short message service) is a popular and simple communication technology for mobile phone devices. Because this service was not originally intended to transmit encrypted data, security was not a priority during its development. Nonetheless, it is still used today to exchange sensitive information between communicating parties, such as Mobile Money. Confidentiality, integrity, authentication, and non-repudiation are the most important security services provided to secure SMS .In this review, a secured short message service (SMS) is analyzed, which is a peer-to- peer hybrid cryptography that provides security services. Mobile technology has spread faster throughout the developing world in the last dozen years than any other technology in history. Mobile money is the most recent phenomenon spawned by mobile technology. SMS (short message service) is a popular and simple communication technology for mobile phone devices. Because this service

was not originally intended to transmit encrypted data, security was not a priority during its development. Nonetheless, it is still used today to exchange sensitive information between communicating parties, such as Mobile Money. Confidentiality, integrity, authentication, and non- repudiation are the most important security services provided to secure SMS .In this review, a secured short message service (SMS) is analyzed, which is a peer-to-peer hybrid cryptography that provides security services. It employs symmetric (AESRijndael) and asymmetric (NTRU) techniques to create more resilient functionality, and because of its vulnerability, it is advised that the usage of the hashing algorithm SHA-1 be replaced with HMAC-SHA256. The protocol is designed to be used in the short messaging service for mobile money communication channels.A Review of SMS Security Using Hybrid

Cryptography and Use in Mobile Money System. American Journal of Computer Science and Engineering. Vol. 2, No. 6, 2015, pp. 53-62.

# Geofencing based Banking Authentication System: A Fraud Mitigation Technique

In the current digital era, banking authentication and online electronic payment systems are crucial to everyone's daily lives. To maintain the security of their clients' money, banks employ multiple layers of verification. Fraud is caused by security weaknesses in electronic payment systems, ATMs, and websites that save cardholder data or information. Other than a card and PIN, there is no other authentication option available for POS and ATM transactions. Researchers pursued a variety of approaches, including biometric techniques that are currently challenging to execute. The user cannot be authorized in an ATM or POS machine in any other way. The user will utilize his phone as an authentication tool in our proposed system, and we will regularly log his location. Due to geofencing, he will only be able to conduct transactions while his phone and ATM/POS are in the same place. This will make it easier to track illegal access and create an alert event anytime someone tries to log in. If there is fraud, it will help the investigative team.

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 6, Article No. 3 (October 1, 2020)

# E-Banking Fraud Detection: A Short Review

Customers are more satisfied with the quality of the services they receive when they use e-banking, and banks benefit from a competitive edge over other market participants. However, due to the fraudulent activity of fraudsters, e-banking security has drawn attention; up to this point, a lack of appropriate e-banking security has discouraged many consumers from using the service. An overview of the security concerns relating to online banking is given in this article. The challenges

and traits of e-banking fraud have also been duplicated. This study also looked at several fraud and attack detection techniques, as well as certain security precautions for e-banking services. Based on the opinions of experts, this study ranked the different e-banking security strategies and models. The research revealed that "Transaction Monitoring" was the model that worked the best, while "Virtual Keyboards," "Browser Protection," and "Device Identification" were the models that performed the worst. The first portion of this essay addressed the subject of interest, while the second section included background knowledge on e-banking. The third portion of the article contained the literature review, and the last section contained the study's conclusion.

International Journal of Innovation, Creativity and Change. [www.ijicc.net](http://www.ijicc.net/) Volume 6, Issue 8, 2019

# Enhanced Authentication in Online Banking

This research ranked the major e-banking security strategies and models based on professional judgment. The results showed that "Transaction Monitoring" was the model that worked the best, while "Virtual Keyboards," "Browser Protection," and "Device Identification" were the models that performed the worst. The first portion of this essay explained the subject at hand, while the second section gave an overview of e-banking. The literature review was located in the third portion of the essay, while the conclusion was located in the last section. This report clearly illustrates the requirement for stronger verification in online banking. It describes the primary security issues and criminal activity driving the demand for enhanced authentication, as well as the expansion of the internet channel pushed by customers and financial institutions. This research makes complicated alternatives easier to understand when adopting improved authentication in the online banking environment and acts as a reference for doing so. Based on the expertise and experience of customers and industry professionals, it offers a thorough analysis of the many authentication options available as well as a set of recommendations for choosing and implementing advanced authentication.

# Summary

Internet banking has become more widely used in recent decades to maintain and improve the equipped and administrative performance of the banking industry. Banks should have the best backup and emergency plans in place, as well as the best safety measures and practices. Customers of an online bank can manage their accounts using their own electronic devices as long as they have access to the Internet. Internet banking has caused a complete revolution in the banking industry. Improving security is not something that should be done only once. A frequent and continuing procedure is

needed that overlooks the entire working and classified threats and opening. Modern implementations of providing security using techniques such as authentication and cryptography tend to use a combination of cryptographic algorithms to confirm the identity of the user and secure data communication over the network.

In conclusion study is majorly focusing on enhancement of the banking system authentication to advanced one with the use of hybrid cryptography algorithm/method.

# CHAPTER 3: REQUIREMENTS, ANALYSIS, AND DESIGN

# Overview

In this chapter, the architecture of the whole project is analyzed. System analysis is the process of collecting and interpreting facts, identifying the problems and decomposition of a system into its component. System analysis is conducted for the purpose of studying a system or its parts in order to identify its objectives. It is a problem-solving technique that improves the system and ensures that all the components of the system work efficiently to accomplish their purpose. Design is a method of studying a system by examining its component parts and their interactions. Before implementation began, the system was analyzed and designed.

# Proposed Model

In this section, we will discuss proposed method which combines two different hiding techniques, which are Cryptography. In this proposed method first, the message is encrypted by use AES algorithm. After that, we use the modified LSB technique to embed the encrypted information in image. So, this technique combines the features of cryptography and provides a high level of security. It is better than either of the technique used separately. There will be an agreement between the sender and the receiver about the key for the concealment algorithm as well as the key for the encryption algorithm or these keys may be exchanged by a secure communication method. Our method starts by encryption first then hide encrypted data.

Encryption

Decryption

Start Application

OTP

Email

Figure 1: Proposed Model

Before applying the cryptography, initially we convert our input to Base-64. And we save the obtained text in a text file. Then we proceed to cryptography.

# Sender Side

The Sender side consists of cryptographic and steganography stages. This method starts with cryptographic then steganography.

# Cryptography Stage:

In encryption stage, we use AES (Advanced Encrypted Standard) algorithm. This technique takes two prime numbers. The Encryption can be done using the Plain Text and with “e” values which was generated using the two prime numbers. Then we will get a cipher text, which is communicated to the receiving end for decryption. This encrypted data will be used in steganography stage.

Input= Message + Two Prime Numbers. Output= Encrypted Message.

# Receiver side

Receiver side consists of steganography and cryptography stages. In receiver side we will first extract embedded data then decrypt it.

# Steganography Stage:

In the receiver side, we start with steganography then cryptography. We will use the same steps which are used in sender side.

Input= Stego-Image+ Secret Key. Output= Encrypted Message. (OTP)

# Cryptography Stage:

In cryptography stage, we use the data which is extracted from stego file and use RSA. We will use the same steps which are used in sender side. The Decryption can be done using the Encrypted message, receiver’s private key and sender’s public key.

Input= Encrypted Message + 2 Prime Numbers. Output= Plain Text.

Now the Plain Text is in the form of Base-64. After getting the plain text apply Base-64 conversion to change the Plain-text to given input, which can be Text, Image, Video, and Audio.

# Methodology

This section describes the methodology applied during the development of more secured banking transaction authentication application using hybrid cryptography. Methodology is a model which projects managers employ for their design, planning, implementation and achievement of their [project objectives.

The methodology used for this project is the time-based one-time password (TOTP) secret key/seed is static just like the HOTP, but the moving factor in TOTP is time-based (hence the name). The TOTP algorithm populates an OTP using a time counter – instead of a running counter – as the second input. The time counter is calculated by dividing the current UNIX time by the time step value. A time step is a pre-set lifetime of an OTP, and in this case, is the amount of time that each password remains valid (typically for 30 or 60 seconds, but can be up to 120 seconds). The secret key/seed and the time step are fed into a cryptographic hash function that outputs an OTP. If the password isn’t used within that allotted time step, it becomes invalid, and a new OTP request must be made.



# Figure 2: Methodology Used

**Advantages**

# TOTP is more secure

TOTP tend to be more secure because they are only valid for a specific period. The extra criteria required to be met greatly increase the security.

# TOTP Offers Flexibility with Various Token Options

A TOTP authenticator can be embedded in both dedicated hardware tokens as well as implemented in software, typically as a mobile application such as Google Authenticator. By implementing it in software (also known as a software token) you avoid the costs associated with hardware manufacturing, distribution, inventory, and maintenance.

# Internet Connection is not necessary

TOTP codes can be generated and accepted offline if the devices have the same secret key/seed and are in sync. This allows them to individually create TOTP codes and compare them against each other.

Some models was adopted in regards to the development of the banking app after which the integration of the security feature was later added in line with the objectives of the project. The Model adopted includes:

1. Waterfall model
2. Spiral model
3. V model
4. Agile model

# WATERFALL MODEL

The waterfall model is utilized for projects with clearly defined objectives to be reached because it is designed or set up in a way that stresses sequential operation. The paradigm moves progressively downward through the stages of software implementation, as its name suggests. The steps in this paradigm must be performed one after the other before moving on to the next. The waterfall approach is best suited for projects that do not anticipate unanticipated changes mid-development since it prohibits going back to previously accomplished phases. The fact that the software cannot be seen or tested until the very end of development also increases the risk and unpredictability of the project. Testing is frequently hurried, and fixing errors can be expensive.

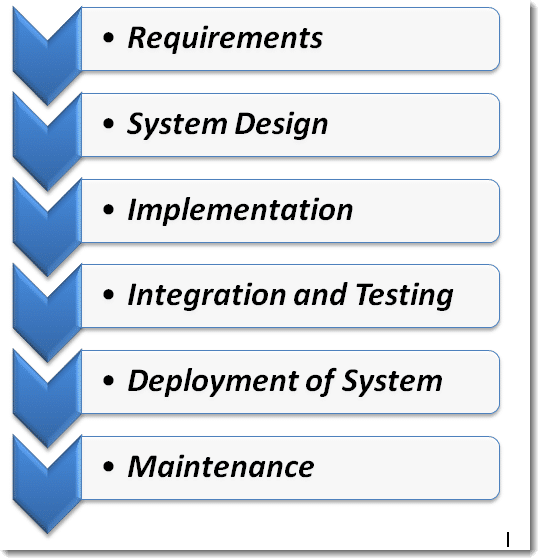


Figure 3: Water Fall **Waterfall Model Phases** Activities during phase

|  |  |
| --- | --- |
| Requirement | Understanding what needs to be designed, as well as its goal, function, and other details, comes first. The specifications for the input, output, or finished product are examined and noted  here. |
| System Design | This phase studies the need specifications from the first phase and prepares the system design. System design aids in determining the overall system architecture as well as the hardware and system requirements. In the current phase, the  software code is being created. |
| Implementation | The system is initially built in little programs known as units that are integrated into the following phase with feedback from the system design. Unit testing is the process of developing and  evaluating each unit for functionality. |
| Integration and Testing | Following the testing of each unit created during the implementation phase, the entire system is merged. Constant software testing is required to check for bugs and mistakes in the developed program. Testing is carried out to ensure that the  client has no issues installing the software. |

|  |  |
| --- | --- |
| Deployment System | Once the product has undergone functional and non-functional  testing, it is either installed in the customer environment or made available for purchase. |
| Maintenance | After installation, this step entails modifying the system or a specific component to change characteristics or boost performance. These changes result from either customer- initiated change requests or flaws found when the system is being used in real life. The developed software is regularly  maintained and supported for the client. |

Table 2: Water Fall Model Phases

In the following situations, waterfall is advised:

* projects with tightly defined specifications that don't allow for alterations during the development process;
* The primary obstacle is not financial but rather development-related;
* when the consumer has no intention of actively contributing to the development process but will instead judge the final product;
* There are no confusing requirements and the technology is clear;
* An exact vision of the finished result exists.

# ADVANTAGES OF WATERFALL MODEL

* The Waterfall Model is a controllable approach that is excellent for the lifecycle management of smaller projects where the needs are understood and decided upon up front. It is clear and simple
* suitable for smaller projects with clearly specified needs
* Before finishing each stage, they should conduct quality assurance tests (Verification and Validation).
* With minimal client involvement, the project is entirely dependent on the project team.
* Any modifications to software are made while it is being developed.

# DISADVANTAGES OF WATERFALL MODEL

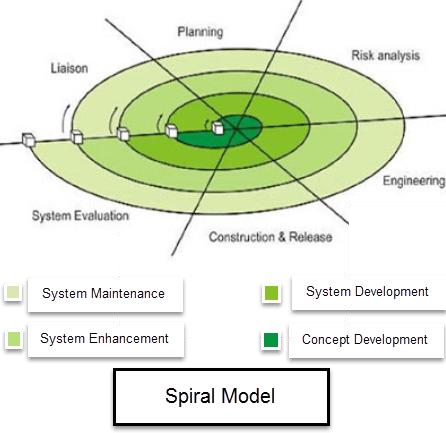
* Error can only be corrected during this phase.
* For complicated projects where requirements change frequently, it is not ideal.
* The testing phase begins quite late in the development process.
* It is not possible to incorporate client comments into the ongoing development phase.

# SPIRAL MODEL

A risk-driven model of the software development process is the spiral model. It combines an iterative model with a waterfall paradigm. The Spiral Model aids in the adoption of software development components from several process models for the software project based on distinctive risk patterns, enabling an effective development process.

In software engineering, each spiral-shaped phase starts with a design goal and concludes with the client reviewing the progress. Barry Boehm initially mentioned the spiral model for software engineering in his work from 1986. (According to Matthew martin, July 9, 2022).

# SPIRAL MODEL PHASES



**Figure 4: Spiral Model** By Mattew Martin (2022)

# WHEN TO USE SPIRAL MODEL

* + When a project is vast in software engineering, a spiral model is utilized
  + spiral technique is employed when frequent releases are necessary
  + when building a prototype is appropriate
  + When evaluating costs and risks is crucial; Spiral approach is beneficial for projects with moderate to high risk
  + when committing to a long-term project is impractical due to shifting economic considerations;

# ADVANTAGES OF SPIRAL MODEL

* + Later on, further features or modifications can be made.
  + The small-scale construction of the prototype makes cost assessment simple.
  + Regular or ongoing development aids in risk management.
  + With spiral development, features are developed quickly and methodically.
  + There is always room for client comments.

# DISADVANTAGES OF SPIRAL MODEL

* + Risk of failing to adhere to the plan or budget
  + Only large projects benefit from spiral development, which also necessitates proficiency in risk assessment.
  + The spiral model protocol must be closely adhered to for it to operate smoothly.
  + Because there are intermediary steps, documentation is more.
  + For smaller projects, spiral software development is not recommended because it could be very expensive.

# MODEL

The abbreviation for the software development lifecycle is SDLC. The pros and disadvantages of the V model are as follows. Organizations use this framework to produce high-quality software in a methodical and economical manner.

The SDLC methodology is used by software development teams of all sizes to create dependable and efficient software. These companies adhere to development standards that include waterfall, fast, lean, and other comparable techniques.

One of the most widely utilized software development methodologies nowadays is the V model. The V model's theoretical underpinnings have validated the use of testing from the very beginning of software development. A verification and validation model is another name for the V model.

Users must first comprehend the function of verification and validation in software development in order to adhere to the V model.

* + Verification: Verification is a technique for passive analysis. Without running the code, testing is done using techniques like inspection, reviews, and walk-throughs.
  + Validation: Testing is done using the code as part of the validation process, which can include both functional and non-functional testing systems. Validation is a dynamic analysis technique.

# ADVANTAGES OF V-MODEL

* + Simple Application**:** The V model's framework is quite simple. The setting is very user- friendly and offers small-scale developers a strong foundation for software development. The software development industry uses the design environment because it is rather simple.
  + Time saver: The V model is straightforward to use, and because trial tasks like designing, planning, and development happen before coding the program, it eliminates the need for engineers to take a break during their busy days. As a trade-off for better success rates, swift designing and a well-integrated system increase the likelihood of success.
  + Proactive error-tracking: The V Model environment includes a proactive error tracking technique that enables engineers to quickly and effectively address bugs and other system issues so that software can be developed within the allotted time limit.
  + No downward data flow: The V Model design framework is extremely complex, thus there are no gaps in it. It prohibits downhill or unidirectional data transfer while the aforementioned software is being developed.
  + Simple design: The V Model has a very straightforward design. The architecture of the V model is simplistic but incredibly effective since its creators want it to be easy to understand.

# DISADVANTAGES OF V-MODEL

* + Very rigid**:** The V Model exhibits great rigidity. It was created to make the construction of extremely complex applications simpler. When it comes to utilization, the V Model is comparatively rigid. Although the execution and methods are rather complex when compared to other design environments or models, the structure may appear straightforward.
  + The V model has a limited range of flexibility. It isn't simple, and it takes new coders some time to get used to it. Although the architecture is simple to understand, there is not much design flexibility. Overall, it is unsuitable for usage during the creation of object-oriented programs. Because the model's design does not permit extremely complex calculations, it is utterly unsuitable for application.
  + There is no initial software prototype made because the V Model software is developed during the implementation phase. It is inappropriate for usage to construct complex or professional software that needs a precise, robust, and sound execution design due to the lack of prototype direction.

# TOOLS AND TECHNIQUES:

**TOOLS**

**Drawio**: Is a free and open source cross-platform graph drawing software. Its interface can be used to create diagrams such as flowcharts, wireframes, UML diagram, organizational charts and network diagrams.

**Figma**: is a prototyping tools which is primarily web based, with additional office features enabled by desktop applications for windows. The mobile app allow viewing and interacting with Figma prototypes in real time mobile devices. The feature set of Figma focuses on use in user interface and user experience design with emphasis on real time collaboration.

**Visual studio**: Visual Studio is an IDE made by Microsoft and used for different types of software development such as computer programs, websites, web apps, web services, and mobile apps. It contains completion tools, compilers, and other features to facilitate the software development process. The Visual Studio IDE (integrated development environment) is a software program for developers to write and edit their code. Its user interface is used for software development to edit, debug and build code. Visual Studio includes a code editor supporting IntelliSense (the code completion component) as well as code refactoring. The integrated debugger works both as a source- level debugger and a machine-level debugger.

The technique used to achieve the statement of problem above is discussed in this section.

The password generated is created using the current time and it also factors in a secret key. An example of this OTP generation is the Time Based OTP Algorithm (TOTP) described as follows:

1. Backend server generates the secret key
2. The server shares secret key with the service generating the OTP
3. A hash based message authentication code (HMAC) is generated using the obtained secret key and time. This is done using the cryptographic SHA-1 algorithm.

Since both the server and the device requesting the OTP, have access to time, which is obviously dynamic, it is taken as a parameter in the algorithm. Here, the UNIX timestamp is considered which is independent of time zone i.e. time is calculated in seconds starting from January First

1970. Let us consider “0215a7d8c15b492e21116482b6d34fc4e1a9f6ba” as the generated string from the HMAC-SHA1 algorithm.

The code generated is 20 bytes long and is thus truncated to the desired length suitable for the user to enter. Here dynamic truncation is used. For the 20-byte code “0215a7d8c15b492e21116482b6d34fc4e1a9f6ba”, each character occupies 4 bits. The entire string is taken as 20 individual one byte sting.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 02 | 15 | A7 | D8 | C1 | 5B | 49 | 2E | 21 | 11 | 64 | 82 | B6 | D3 | 4F | C4 | E1 | A9 | F6 | BA |

Table 4: OTP Code Generator technique

1. We look at the last character, here a. The decimal value of which is taken to determine the offset from which to begin truncation. Starting from the offset value, 10 the next 31 bits are read to obtain the string “6482b6d3″. The last thing left to do, is to take our hexadecimal numerical value, and convert it to decimal, which gives 1686288083.

All we need now are the last desired length of OTP digits of the obtained decimal string, zero- padded if necessary. This is easily accomplished by taking the decimal string, modulo 10 ^ number of digits required in OTP. We end up with “288083” as our TOTP code.

1. A counter is used to keep track of the time elapsed and generate a new code after a set interval of time

OTP generated is delivered to user by the methods described above.

# Ethical Consideration

No profession or industry has maintained higher standards of conduct nor provided greater public service than the banking industry. Banks have traditionally recognized their duty to act in a manner of public trust and confidence which is one of their utmost priority. The relational context between the bank and customer during transfer or receiving of fund via digital means remained relatively problematized. Rather than assuming an anonymous interface between the banking industry and the customer or client, with specific ethical issues related to it. These consideration work to maintain scientific integrity, enhance the project validity and to protect the rights of the party involved in the

development. Some of the ethical consideration that were considered during the development of this project are:

* Confidentiality
* Result communication
* Anonymity

# Requirement Analysis

Requirement specification is a collection of requirement that are to be imposed on the design and verification of the product. The specification also contains other related information necessary for the design, OTP verification and maintenance of the banking App.

System specification of the banking are sub divided into two: the hard ware specification and the software specification. Below gives a tabular breakdown of the two system specification.

Table 5: Hardware requirement

|  |  |  |
| --- | --- | --- |
| **S/N** | **Hardware** | **Minimum System**  **Requirement** |
| 1 | Processor | 2.4GHz processor speed |
| 2 | Memory | 2GB RAM |
| 3 | Disk space | 500 GB |

This are requirements specification for a software system, is a description of the behavior of a system to be developed and may include a set of use cases that describe interactions the users will have with the software.

This are requirements specification for a software system, is a description of the behavior of a system to be developed and may include a set of use cases that describe interactions the users will have with the software. The software requirements specification document enlists enough and necessary requirements that are required for the project development. To derive the requirements, we need to have clear and thorough understanding of the products to be developed or being developed. The software specification used for this project are listed in the table below.

Table 6: Software Requirement

|  |  |  |
| --- | --- | --- |
| **S/N** | **Software** | **Minimum System**  **Requirement** |

|  |  |  |
| --- | --- | --- |
| 1 | Operating system | Windows 7,Windows 8,  windows 10, MAC OS and Linux |
| 2 | Database management | SQL Database |
| 3 | Runtime environment | Visual Studio Code |

Below is the detailed explanation of the functional requirement specification and the nonfunctional requirement.

* + 1. Functional Requirement Specification:

The functional requirements specification describes what the banking app must be able to do. It describes a software system or its component. Below is the functional requirement table

Table 7: Functional Requirement Specification

|  |  |  |
| --- | --- | --- |
| **Req No.** | **Description** | **Type** |
| R-101 | The website shall be Mobile friendly. Easy navigation  using mobile phones is guaranteed | Functional |
| R-102 | Standardize OTP (One Time Password) generation is  embedded in the system. | Functional |
| R-103 | Automated transfer of the OTP to the registered Email  address. | Functional |
| R-104 | Minimum steps to access the OTP | Functional |

* + 1. Non Functional Requirement Specification: Table 8: Nonfunctional Requirement Specification

|  |  |  |
| --- | --- | --- |
| **Req No.** | **Description** | **Type** |
| R-101 | System should provide a user friendly user interface and tooltips to enhance itself and be effective  responsive. | Performance |
| R-102 | The system is equipped with Security features to avoid  external injections or hacking. | Performance |
| R-103 | In the case of maintenance, the system will be maintained in order to derive the maximum satisfaction  of the system | Performance |
| R-104 | Ability to handle increase loads efficiently without a  break in the system efficiency. | Performance |

|  |  |  |
| --- | --- | --- |
| R-105 | The system will be highly reliable and it generates all the updates information in correct order. Data validation and verification is done at every stage of  activity. | Performance |

# System Design

Every system or website development must include a good system design. The system design involves the process of designing the element of a system such as the architecture, modules and components. The different interfaces of the component and the data that flows through that system are also part of the system design.

The diagram basically shows how the actors (Customer, Cashier and Admin) interact with the main system and between each other based on their roles. User stories are defined for each actor, which lists the exact activity done with the system. Finally, there is Use cases which are defined processes/functions for actors. Combining actors, user stories and use cases gives us a Use case diagram. The following are the listings of user stories and use cases for each actor.

User stories

* + 1. Customer:
       - Customer will get information about various account types with details.
       - Customers will be able to have options for different electronic cards and choose it
       - Customers should be able to do daily transactions like paying bills and getting OTP for every transactions made.
       - Customers will be able to view OTP in his or registered Email address
    2. Staff:
       - Staff will be able to verify and authenticate different date of customers and integrate it to the system which initially passed on by user.
       - Generate customers registrations
       - Authenticating and allowing each transaction done by customers with accountability
       - Tracking all the general activities of each end users with update alert and any required changes

# Application Architecture

* + - 1. Account opening sequence diagram

This shows how a general user gets his account opened, while it provides the details and further it is verified by the bank servers.

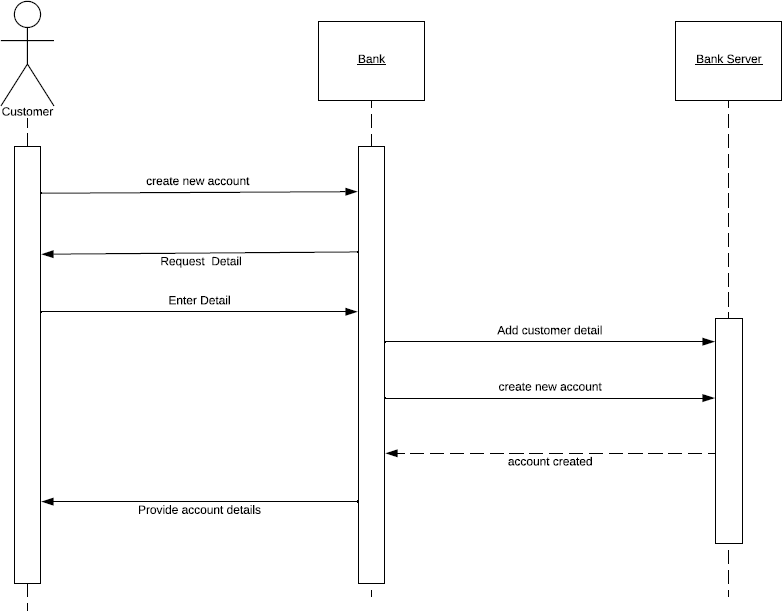


Figure 5: Account opening Diagram

* + - 1. Payment Process sequence Diagram

It shows how a user can do his daily life payments with the available balanceunder the authentication process of the bank.

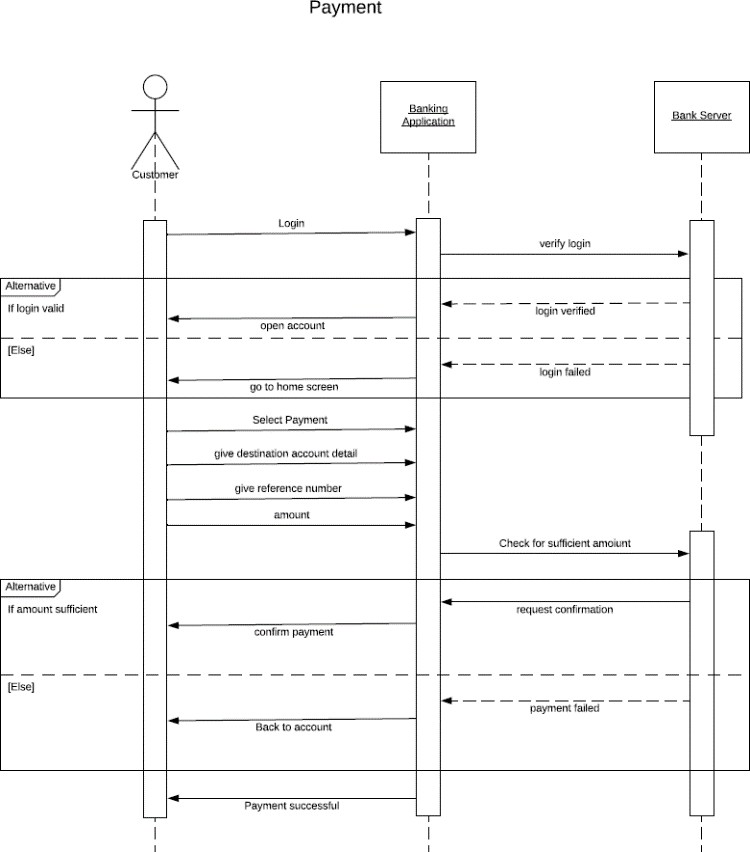
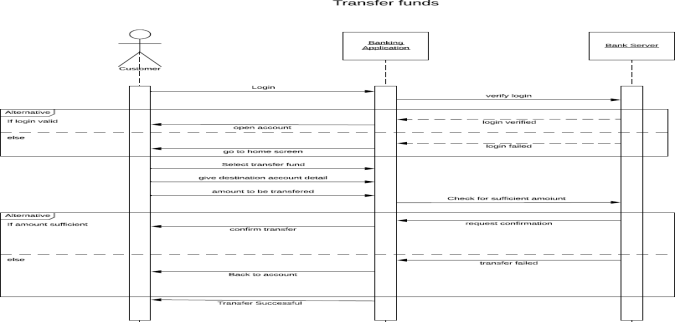


Figure 6: Payment Process Diagram

. 

* + - 1. Transfer Funds Sequence Diagram Figure 7: Transfer Process Diagram

# Use Case

A Use Case diagram depicts the interaction of users and systems. It depicts the system's functions from the user's point of view, as well as the various actions performed by the user as the actor.

* + - 1. Registration, authentication and verification

Each data of customers should be registered to generate a login system for each defined role with proper documentation. The data should be authenticated and certified by the admin for final integration to the system.

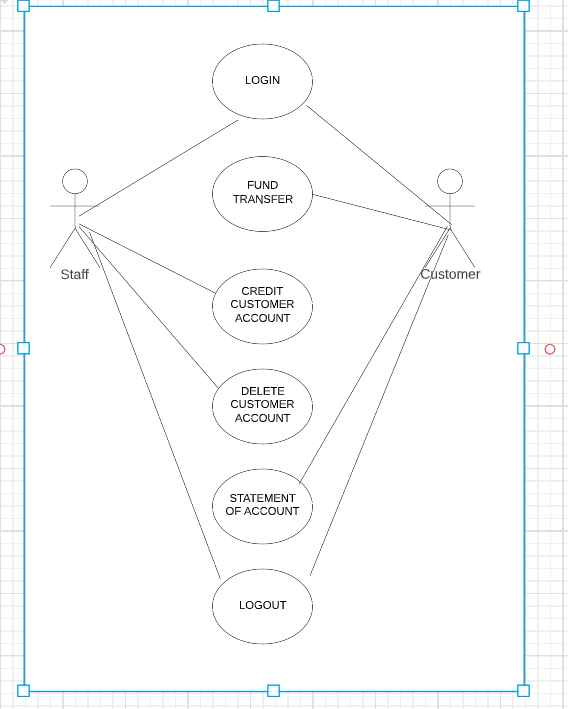
* + - 1. General and specific function associated with roles of each users:

Customers should be able to register itself and get login info for doing monetary transactions. A proper track of these transactions should be done by admin with its accountability.

* + - 1. Data storage and information processing:

All the interaction between admin, customers and cashier should be structurally stored by each of them based on the roles like online transactions of each customer. All the information should be processed with its authentication, accountability and final verification by admin before the storage process

# Figure 8: Use case diagram.



* + 1. **Data Design**

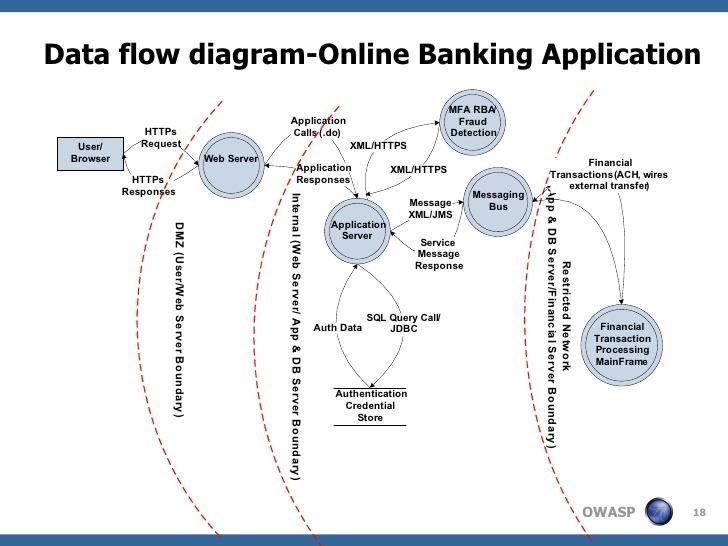


Figure 9: Data Design

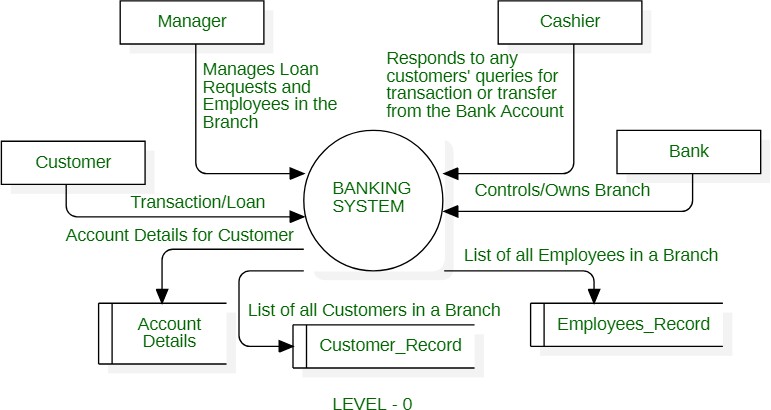
# Activity Diagrams

An activity diagram is a model that depicts the steps in the execution of a task or activity from a use case.

# activity diagram projectFigure

**10: Activity diagram for System users.**

# Dataflow Diagram



**Figure 11: Data flow diagram.**

In the above Data Flow Diagram, there is a Login Screen and this include username and password, users will supply this information for authentication on the server. If the authentication fails the user will see invalid username or password and be ask to try again (see Figure 3.6 below for more details about the authentication process).

# Control Flow Diagram

Control flow diagram for this implementation describes the flow of the process or review of the website. This control flow is design for each critical activity.

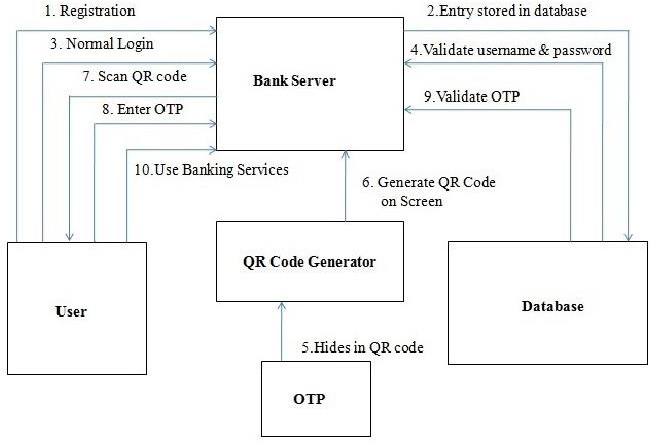


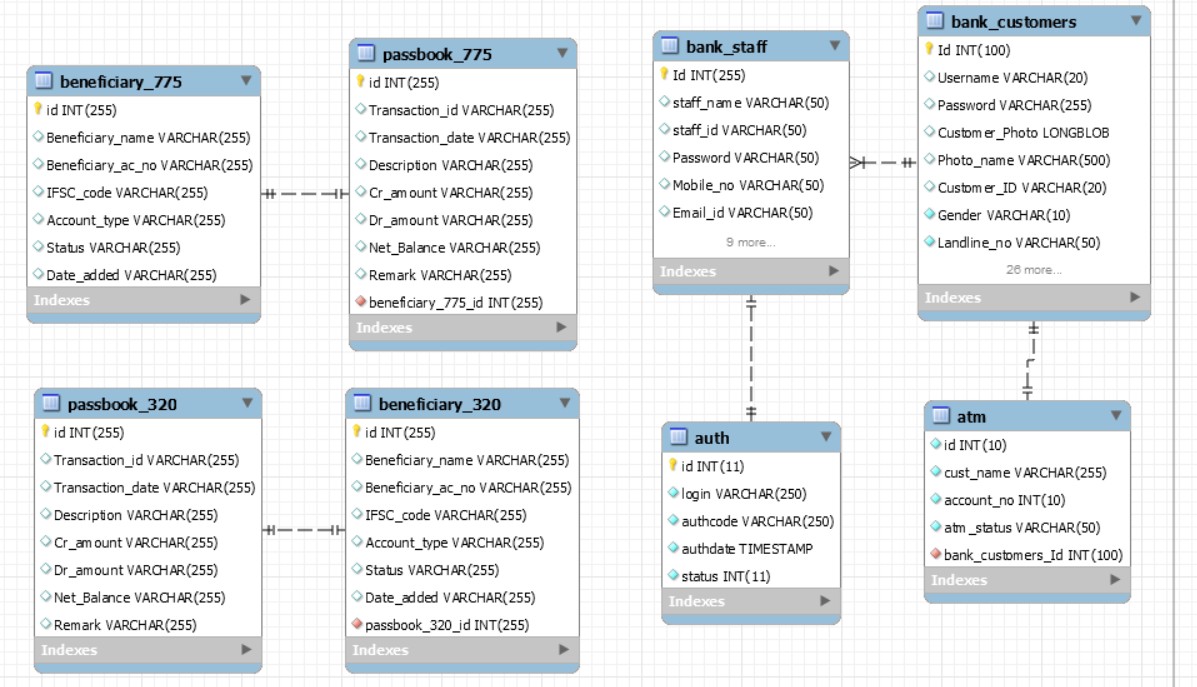
Figure 12: Control Flow Diagram

# Entity-Relationship Diagram (ERD)

It is a model that establishes relationships between people, objects, places,concepts or events within a system. It is very vital to project data modellingfor the database. It also helps in defining processes and develop relationaldatabase. Basically, it helps us to create a database model for our system including different entities revolving in our system.

There are five basic components for this diagram. They are listed below:

* Entities, these are concepts or objects that can have data stored about them. They are referred as tables used in database.
* Attributes, these are properties or characteristics of entities
* The relationships among and between those entities.
* Actions, that describes how entities share information in the database
* Connecting lines.

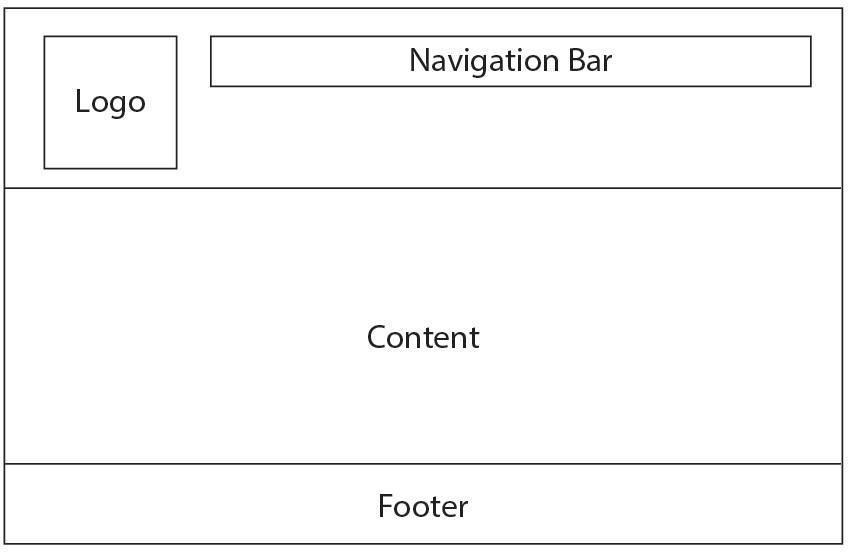
The following diagram represents the ER model of the banking system thatwe are developing.

# Figure 13: Entity Relationship Diagram

* + 1. **User Interface Design**

It is a type of user interface by which any user interacts with the system via visual indicator presentation. It is considered as use cantered design in softwareprogramming which basically means that it is an interface for a system graphicallydesign so that a user can access the services as accurately as possible. The users should understand what they are doing and what they are getting from thesystem as different type of user-friendly responses graphically.

Considering the level of technological knowledge of the stakeholders of the company and the requirements a simple and easily accessible GUI is developedfor this system. The GUI is developed using various tools and features available in windows form platform. There are different sections of GUI which are defined and graphically represented below.



# Figure 14: GUI.

* 1. **Summary**

This chapter has discussed the methodology that will be used in the design and implementation of this study. It also examines the functional requirements of the application as well as system design. The next chapter which is chapter four (4) will talk about Implementation and Testing.

# CHAPTER 4: IMPLEMENTATION AND TESTING

* 1. **Overview**

This chapter is the part that puts a planned system into action and examine in details the analysis and design of the implemented project. The present chapter discusses the implementation of the system, highlighting the testing exercise and describing some of the main components of the system's Graphical User Interface. It will give an output from programming language and other tools used to develop our system.

# Main Features

We can emphasize the vital aspects necessary when dealing with banking activities. Main features that was involved during the implementation of this projects are divided into three (3) sections.

1. Main Features for Admin
   * Admin can sign up quickly and easily: Simplified onboarding process for the admin
2. Main Features for Customers
   * Customers can sign up quickly and easily
   * Simplified onboarding process for the buyers.
   * Customers can easily process transactions with ease
   * Easy process, view and download of statement of account
   * Customers can check their bank balances
3. Authentication
   * System generated OTP for customers is embedded in the application using the cryptography algorithm.

# Implementation Problems

In every project implementation, several problems are encountered during the process. These problems could be encountered at the infancy stage, middle stage or during the completion stage of the project. Some problems that were encountered during the implementation of the development of a more secured banking transaction authentication application using hybrid Cryptography is listed below.

* + - Technical Design Issues
    - The right tech tracks
    - Tools and technique to be used
    - Performance and speed
    - Financial problems

# Overcoming Implementation Problems

What was done to overcome the implementation problem listed above is to break down the implementation process into batches. By so doing, the process will be addressed at each stage of the project. For example, the performance and speed of each stages differ depending on the complexity of the phase.

# Testing

The testing phase of any software development process is very crucial. The testing phase ensures that every part of the software works as expected. The best way to perform testing is to have inputs and expected out, then provide fill the input on the software and compare the result with the expected output. This helps in cross checking and identifying any possible errors in the system that has been design. Testing ensures that each functionality that has been added works according to

the software requirement. All errors are detected and remove at this stage of development. One great advantage of the testing is that it saves cost, because all problems that might arise in the future can be identify and fix in time. The first testing that was carried out is Functionality. The functionality tests a special type of system testing where all the functional requirement of the software is being tested to ensure that all component functions properly. Security testing is also carried out to check if the software is vulnerable to security threats. Compatibility test is carried out to see how the software can run in the suitable platforms it was designed to work on. Usability test was conducted to see if the software is easy to use and also user friendly.

Testing the functional requirements of more secured banking transaction authentication application using hybrid cryptography aims at verifying that the website features and operational behavior correspond to their specifications.

To achieve this aim, any failures due to the running environment should be avoided, or reduced to a minimum. Preliminary assumptions about the running environment will have to be made before test design and execution.

# Tests Plans (for Unit Testing, Integration Testing, and System Testing)

For a website to be termed good and reliable, it must have undergone series of test to make sure that every part and module of the website is working in accordance to the design by the developer. A test plan is a detailed document that outlines the test strategy, objectives, resources needed, schedule, and success criteria for testing a specific new feature or piece of software. Test plans that was conducted for secured banking transaction authentication application using hybrid cryptography are the Unit testing, Integration testing and the system testing.

* Unit testing is a testing technique using which individual modules are tested to determine if there are any issues by the developer himself. It is concerned with functional correctness of the standalone modules. Module that will be tested for the secured banking transaction authentication application using hybrid cryptography website is creation of an account.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **S/N** | **Test case**  **Name** | **Test Description** | **Sequence of Steps** | **Expected result** | **Remark** |
| 1. | Creation of an account | This test case test  the functionality for the creation of a | After a successful app  launch attempt, navigate to “Create an Account” | 1. The system  should show the user text field | Success |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | customer bank account. | Enter the required information needed. | and submit button. |  |

Table 9: Unit Testing

* Integration testing is done to test the modules/components when integrated to verify that they work as expected i.e. to test the modules which are working fine individually does not have issues when integrated. This test case tests the functionality for user registration, login and logout. These 3 different modules are integrated as one.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **S/N** | **Test case**  **Name** | **Test Description** | **Sequence of Steps** | **Expected result** | **Remark** |
| 1 | User Registration | This test case test the functionality for the user registration. | After a successful app launch attempt, navigate to “Create an Account”  1. Enter the required information needed.. | System should  display the  platform where user can input the necessary details. | Success |
| 2 | User Login | This test case test the functionality for the user login. | 2. After a successful registration, the system redirect user where login details will be entered. E.g. Username:aaroniliya [dikko@gmail.com](mailto:dikko@gmail.com) Password:12345678  @ | System should display 2 Text field. Text field for username and password. | Success |
| 3 | User logout | This test case test the functionality for the user Logout. | 3. User clicks on this link button to redirect user back to login  page. | System should redirect the user back to login page. | Success |

Table 10: Integration Testing

* System Testing is a level of testing that validates the complete and fully integrated website. The purpose of the system test is to evaluate the end to end system specification. System testing takes,

as its input, all of the integrated components that have passed integration testing.

# Test Suite

Test suites can identify gaps in a testing effort where the successful completion of one test case must occur before you begin the next test case. For instance, you cannot add new products to a shopping cart before you successfully log in to the application.

# Test Traceability Matrix

Testing traceability matrix is a document that traces and maps the relationship between two baseline documents. This includes one with the requirement specifications and another one with the test cases. The software testing matrix document plays a key role in convincing the client that all the requirements have been met and there are no loopholes that are left at the time of product delivery.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Req No.** | **Main requirement** | **Sub-requirement** | **Category** | **Description** | **Relationship** |
| R-101 | Registration | User Registration | Required | There will be a User/Customer registration in the  registration module. | Composition |
| R-102 | Service   * Login * Logout | .User Login  User Logout | Required  Required | User is expected to login successfully without any issue.  User is expected to logout from the system without  any issues | Composition |
| R-103 | Transfer | Fund Transfer | Expected | User should be able to transfer fund to another account at ease without  encountering any problem. | Association |
|  | | | |

Table 11: Test Traceability matrix

# Test Report Summary

Test cases are important document for future prospective. The three type of test (Unit testing, Integration testing and system testing) that was conducted on the website shows that the website

13

passes all the undergone test which gives assurance to related documentation for completeness, correctness, reliability and maintainability. It also includes assurance that the system meets the specification and the requirements for its intended use and performance.

All methods called from Unit testing, integrated testing ad system testing were tested. All the methods worked according to the specification for all sets of correct input parameters. Correct calls did not produce errors, incorrect calls produced the appropriate error codes and messages.

# Error Reports and Corrections

I n a so ft war e d e ve lo p me nt pr o je c t , er r o r s can be cr e ep ing a t an y s t ag e dur ing t he development. Due to its approach, dynamic testing can only as certain the presence of error in the program; the exact nature of the error is not usually decided by testing.

All errors gotten during the development of the development of a more secured banking transaction authentication application using hybrid cryptograph website are detected, and are thoroughly worked on so as to grant the assurance that the system meets the specification and the requirements for its intended use and performance.

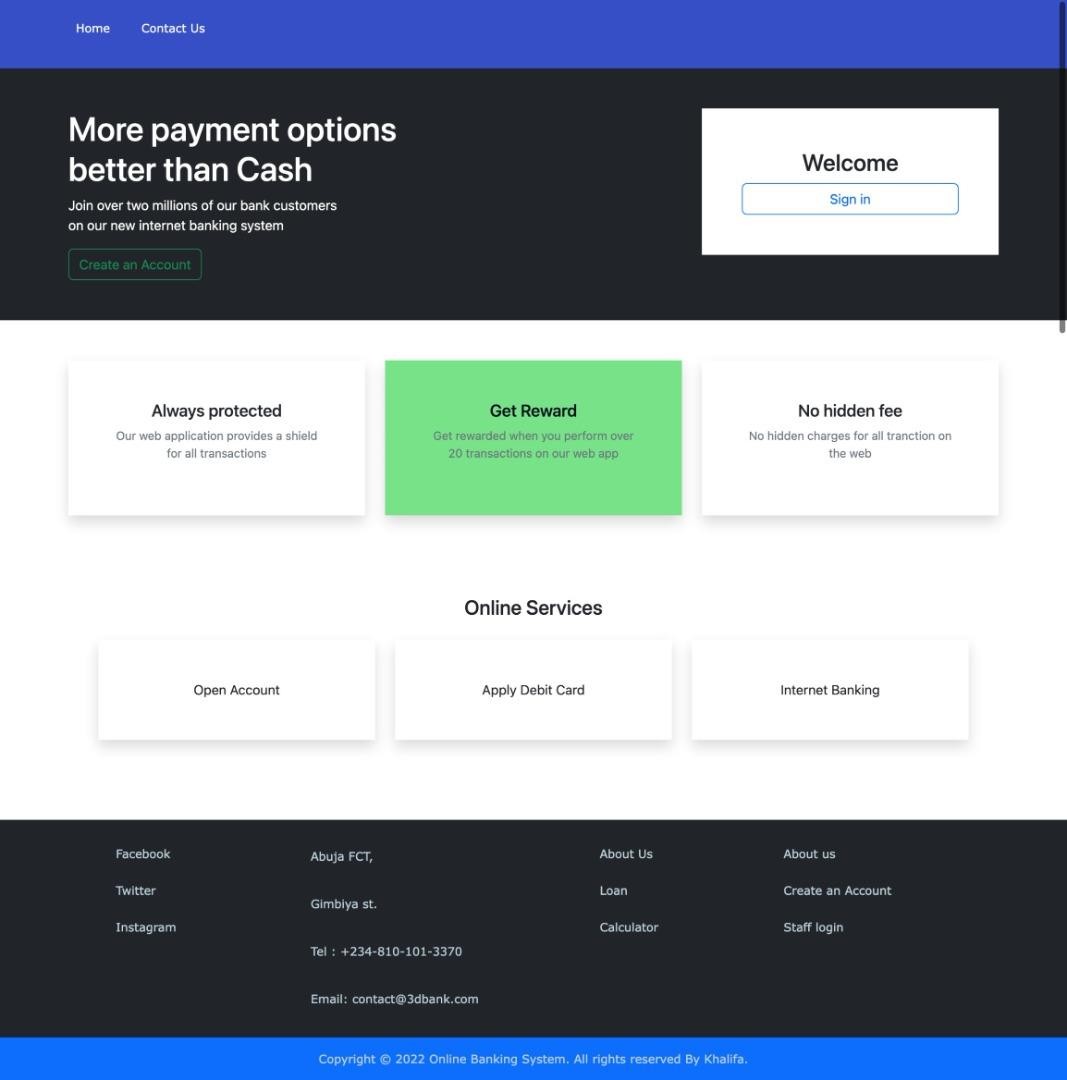
# Use Guide

User guide serves as a reference guide for working with the implemented Banking website. Users can make use of it to have in-depth knowledge about the functions of each link button, text field and dropdown menu. Below are screenshots that will assist user in using the implemented website.

# Landing page:

It is first interface that opens when we load the application. It consists of a Sign in section where users, cashiers and admin can login into the system. There are other divided sections such as Create

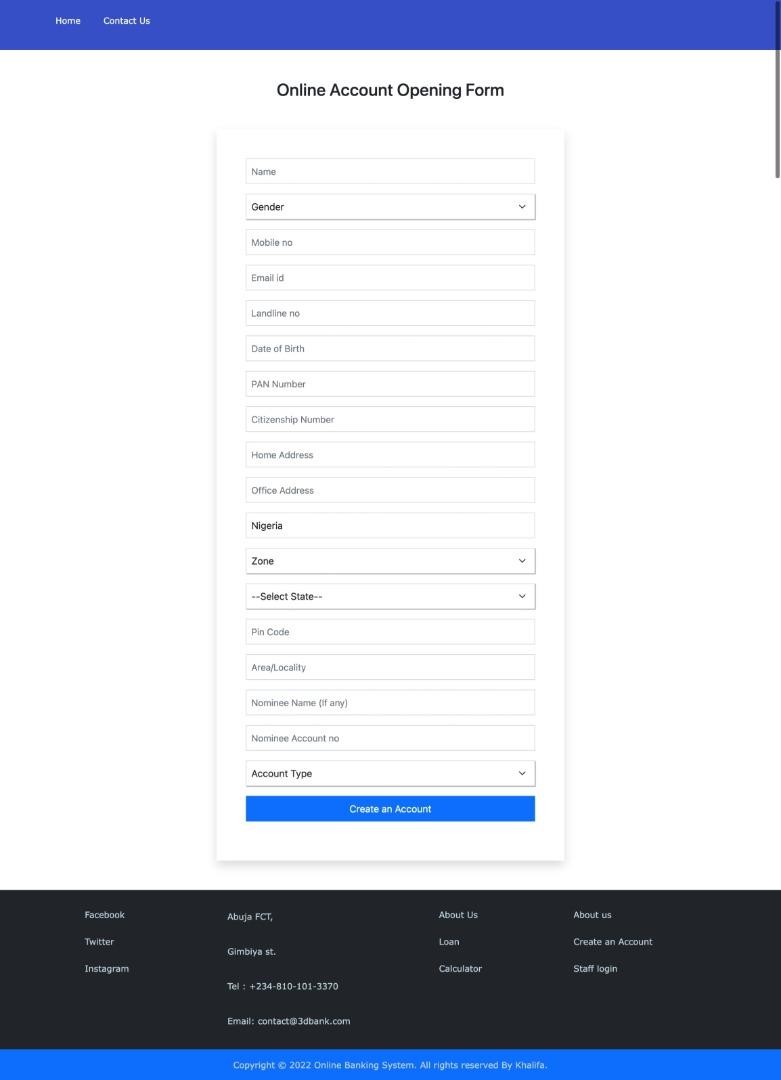
account, online services, get reward and as well no hidden fee.



# Figure 15: Landing Page

* + 1. **Create An Account:**

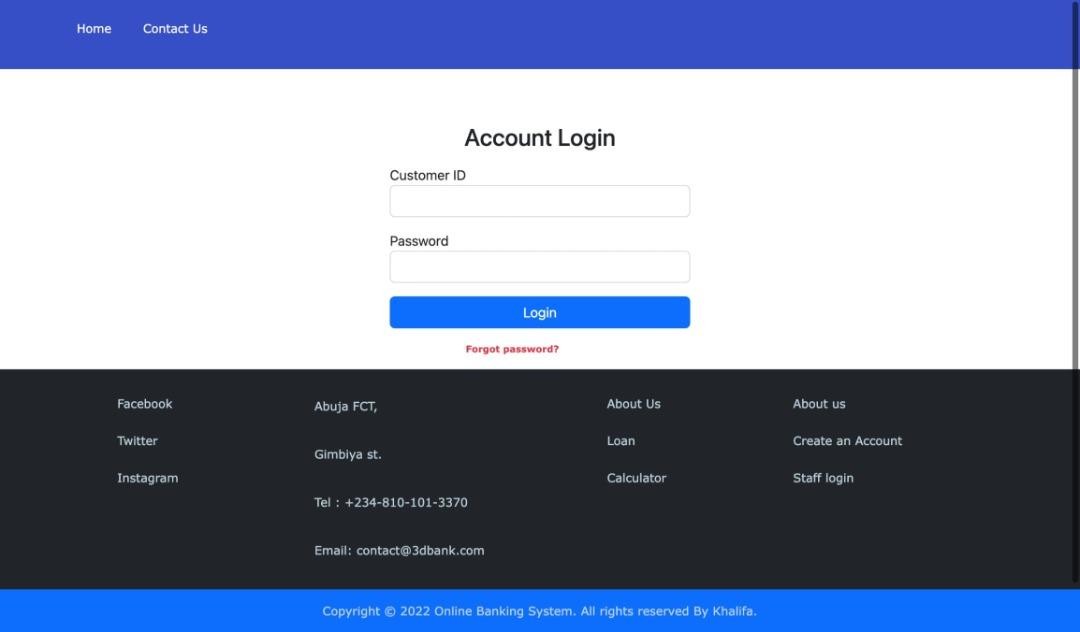
The interface allows to register as a user and open an account providing our personal details. Then we are allowed to login to the system.



# Figure 16: Account creation page

* + 1. **USERS LOGIN**

The login interface is an interface that appears a like a form which is required to be filled up by the users of the system which are customer user and customer user. Both customer users and customer users’ interfaces have different functionalities.



# Figure 17: Shows Login Interface

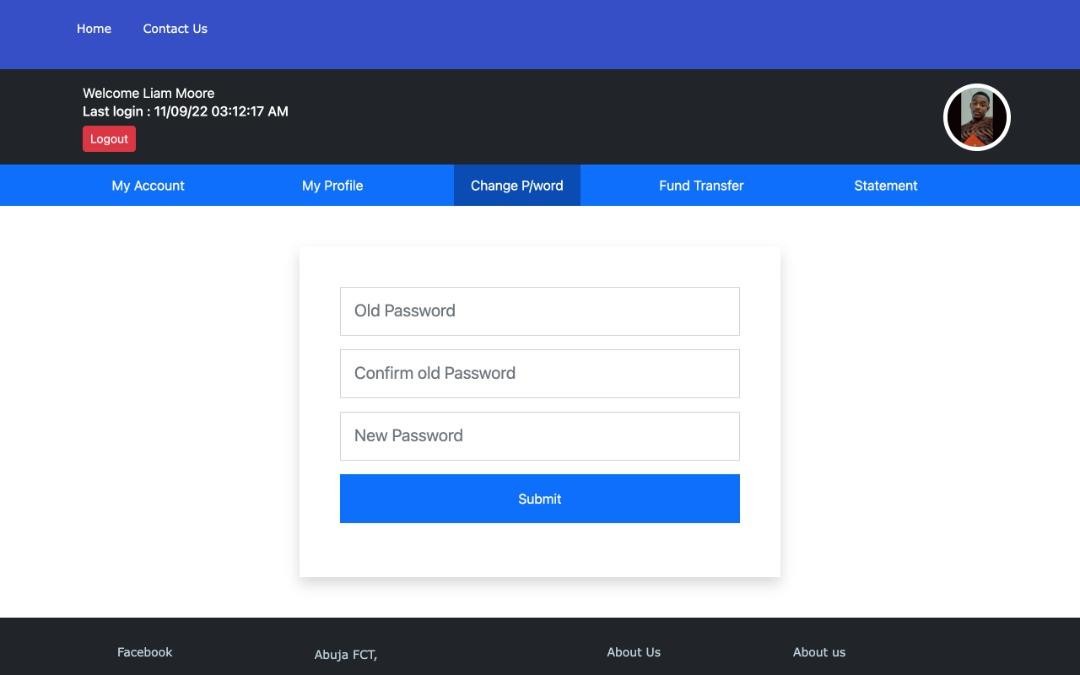
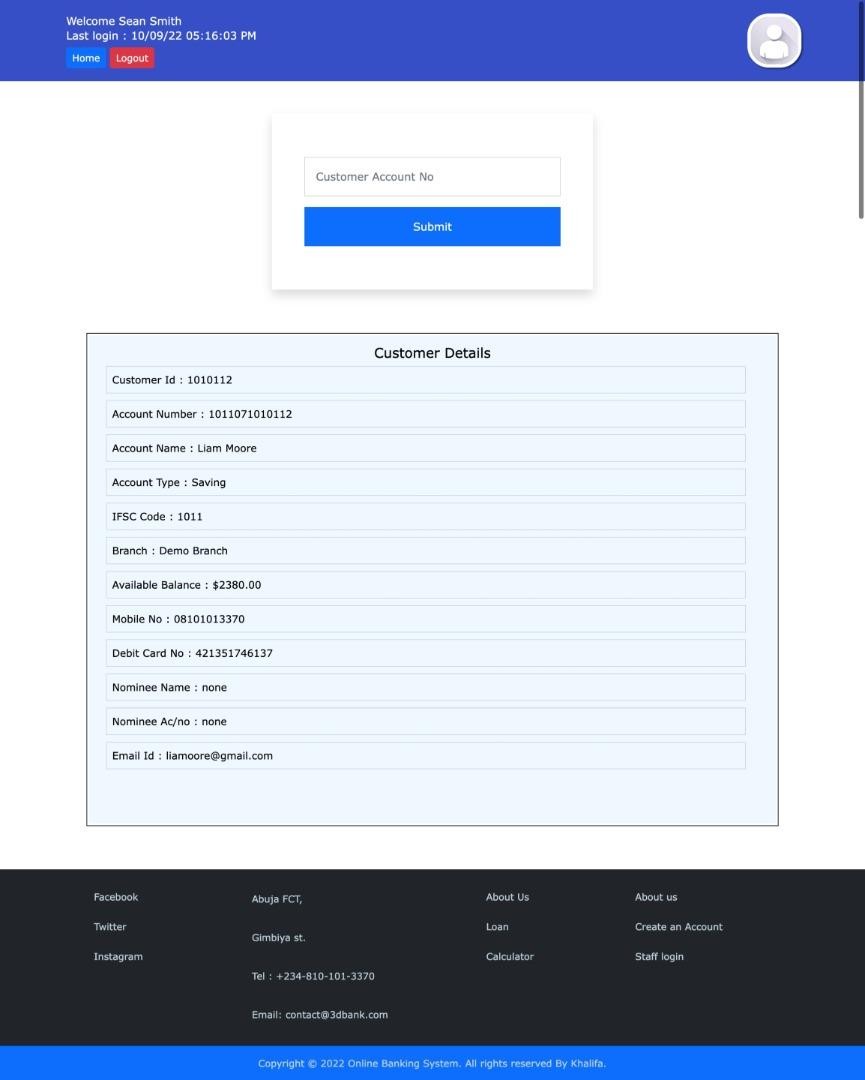
* + 1. **Forgotten Password**

Figure 18: Forgotten password

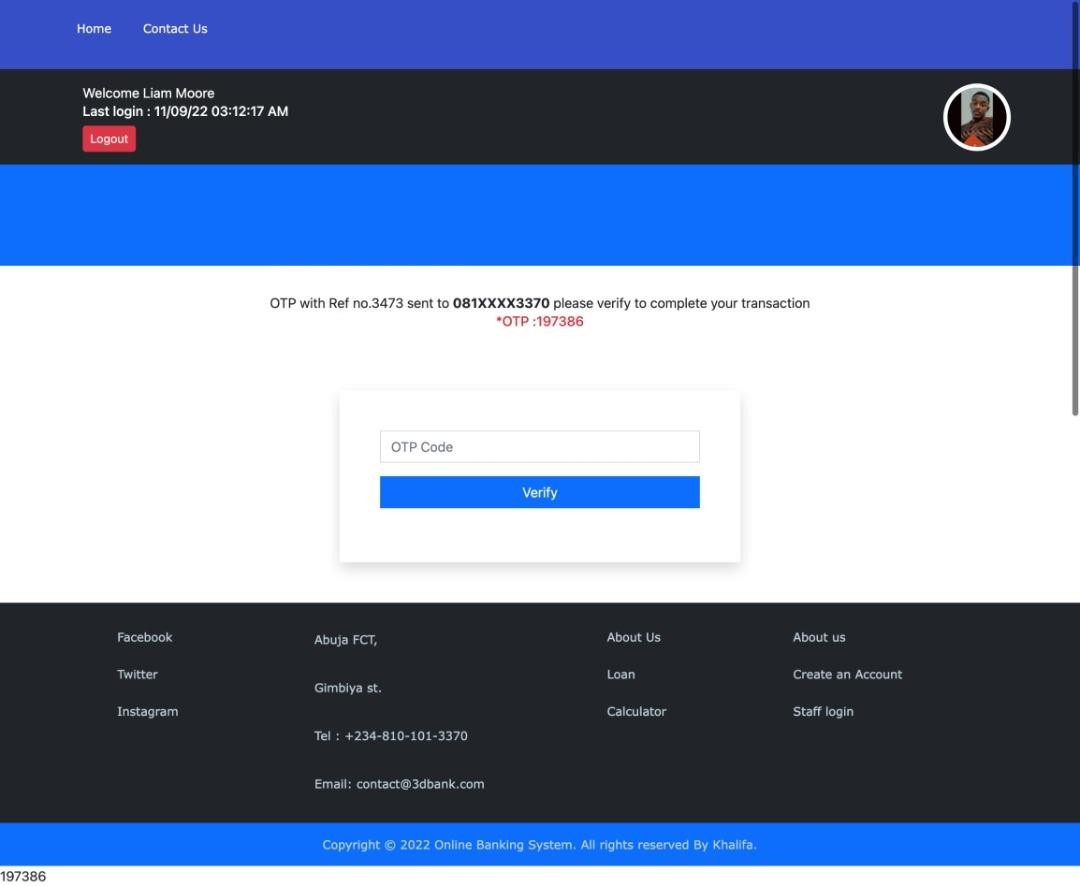
# Customers Details.

In this page, all user’s details such as name, Id, phone number, Email, can be edited by the user. All banking activities for customer user is displayed in their dashboard as seen above.



# Figure 19: Customer user Interface

* + 1. **TRANSACTION AUTHENTICATION AND ENCRYPTION METHODOLOGY**



# Figure 20: OTP Request edit Interface

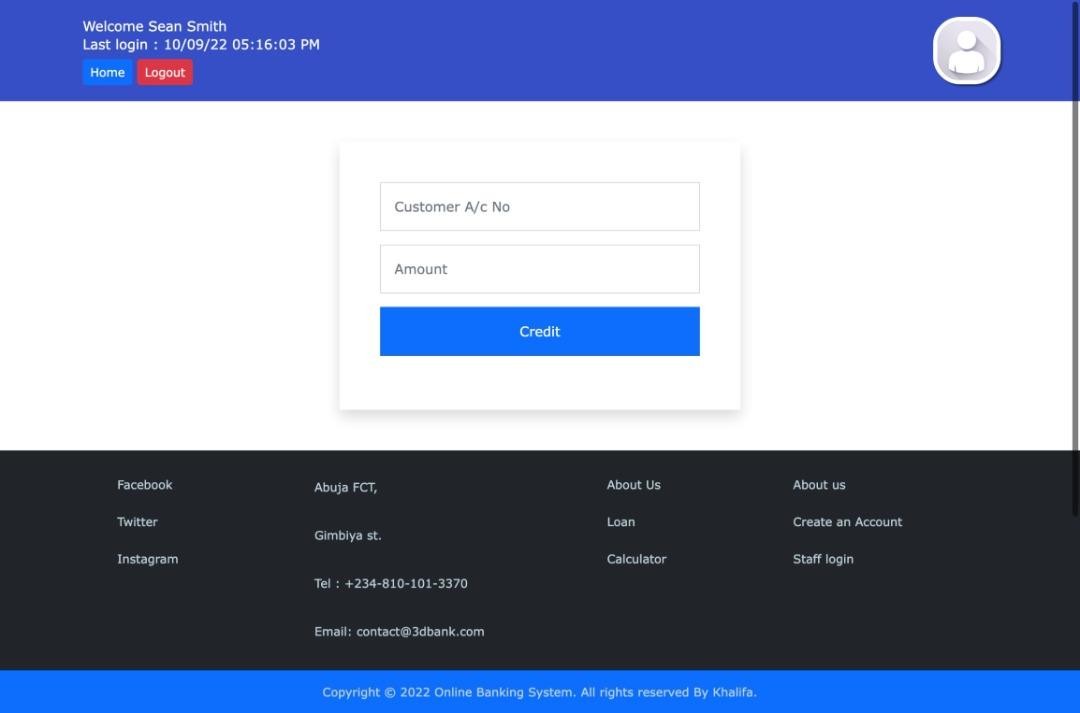
OTP means One Time Password: it’s a temporary, secure PIN-code sent to you via SMS or e-mail that is valid only for one session. All Citizens bnak uses OTPs during registration and account renewal, deposit or withdrawal to confirm your contact information.

If you cannot receive and confirm the OTP code, you will not be able to continue with your account registration. **So double-check when you are entering your contact details**!

* + - * **Phone number**: your phone number needs to be entered with the **correct country code.** Make sure you check it!
      * **E-mail address:** check for spelling mistakes and always use your **primary e-mail** account

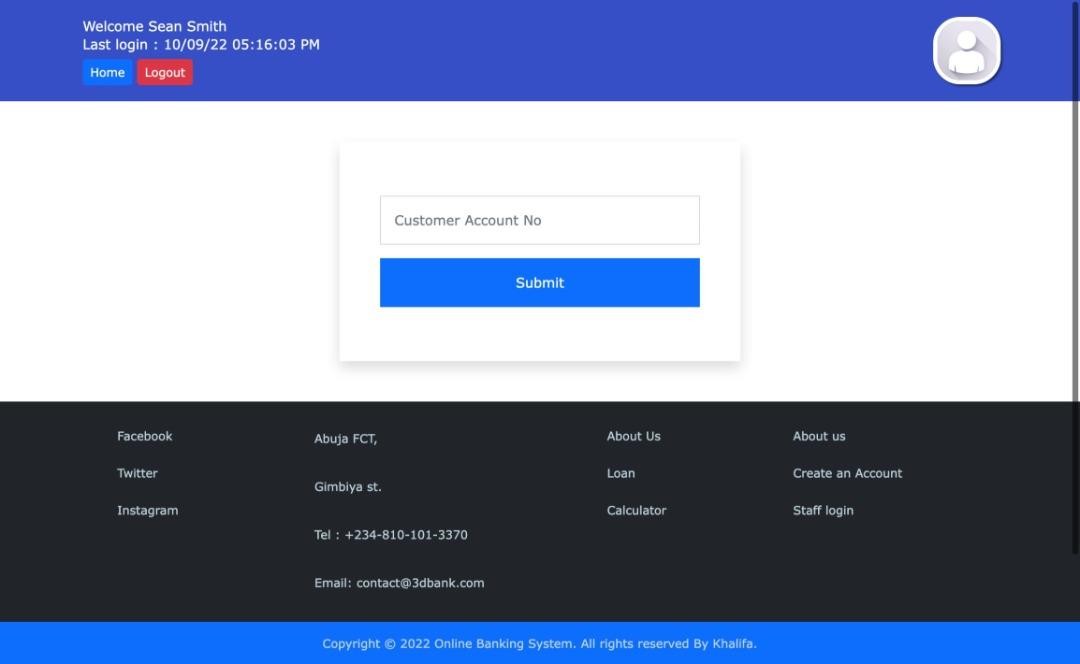
– one that you will still be using in years to come even if you change jobs, move abroad, change your surname etc.

# PAYMENT GATEWAY FOR SMOOTH BANKING TRANSACTION

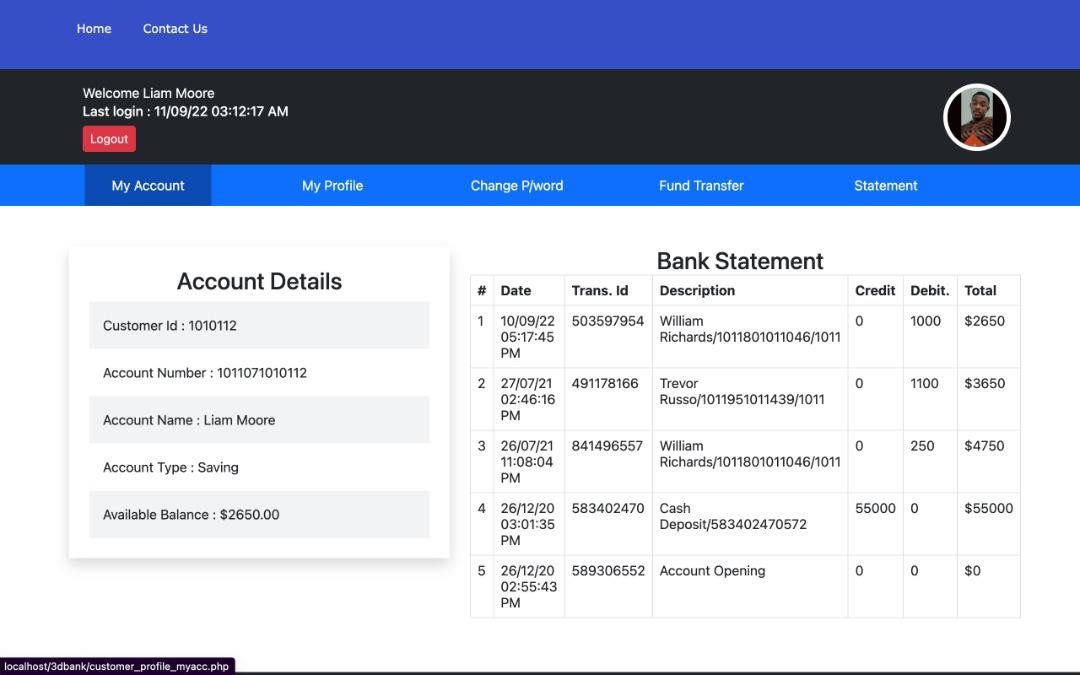


**Figure 21: Search Payment Gateway Interface**

In this page, customer user can be searched through Id or name by the customer user/nurse in the text box. Edit customer user, queue customer user, make appointment, notify customer user and generate Medical Report can all be searched using the search function.

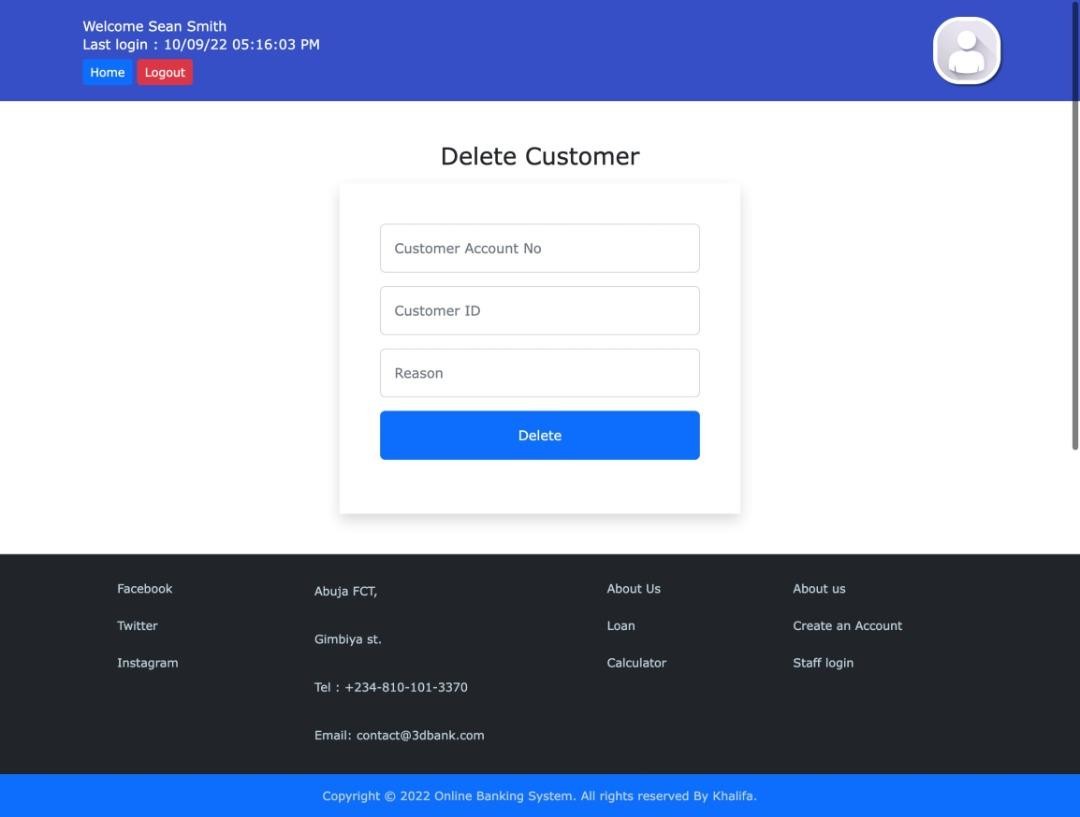


# Figure 22: Customer Account Details

* + 1. **Account Details:**

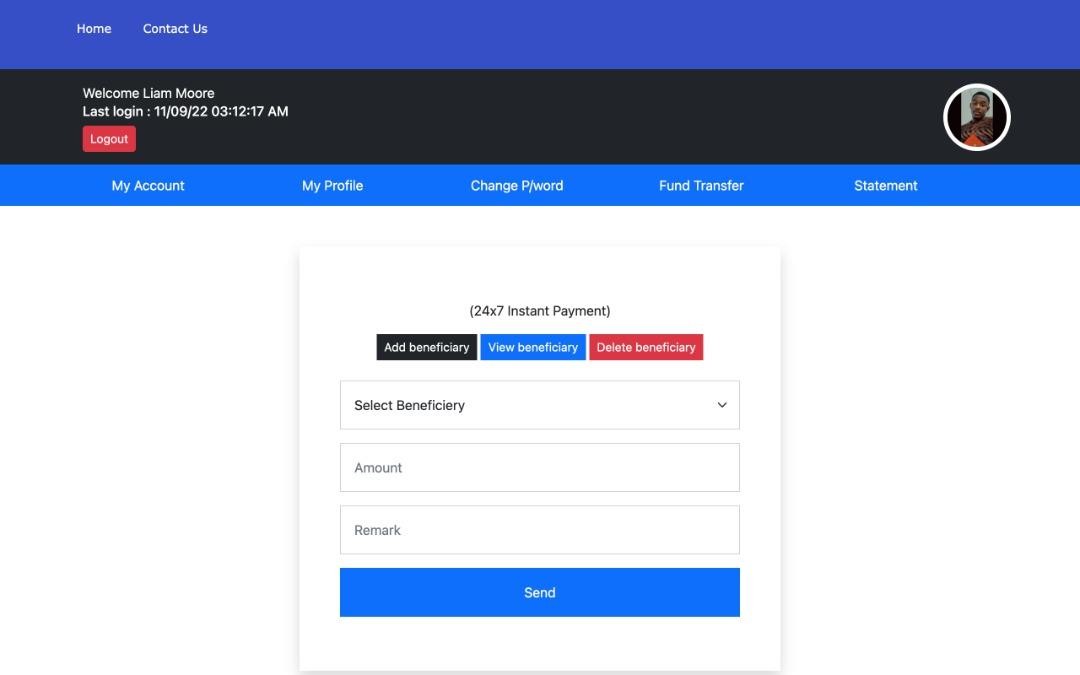
# Figure 23: Statement of Account

* + 1. **Delete Customer:**



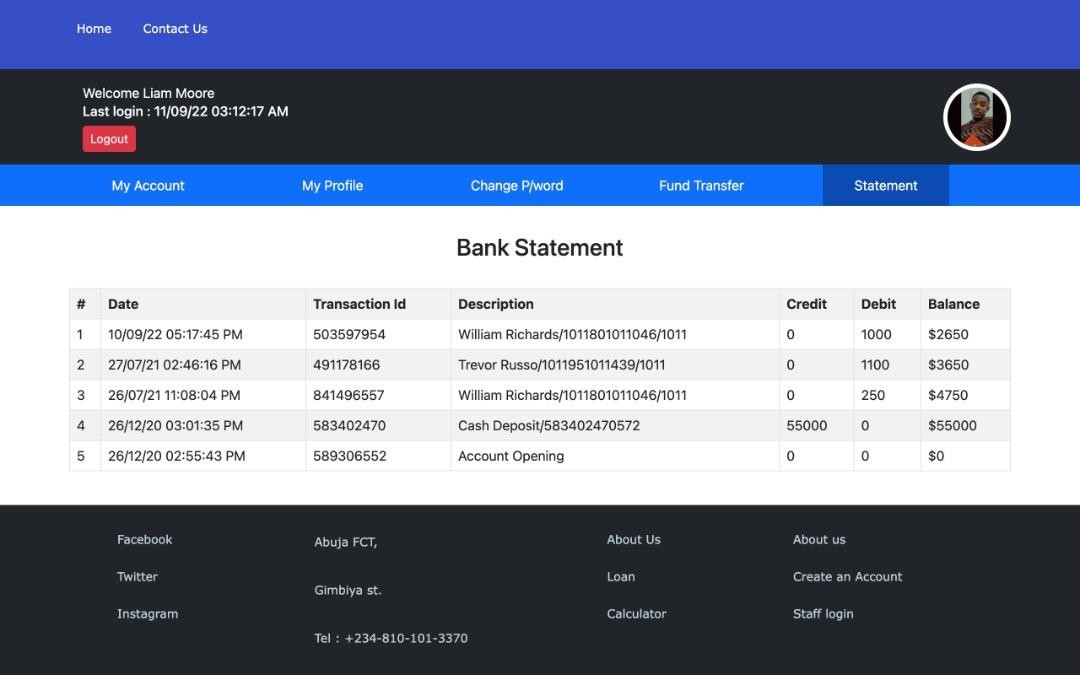
# Figure 24: Account Deleting

* + 1. **Instant Transfer payment Gateway**

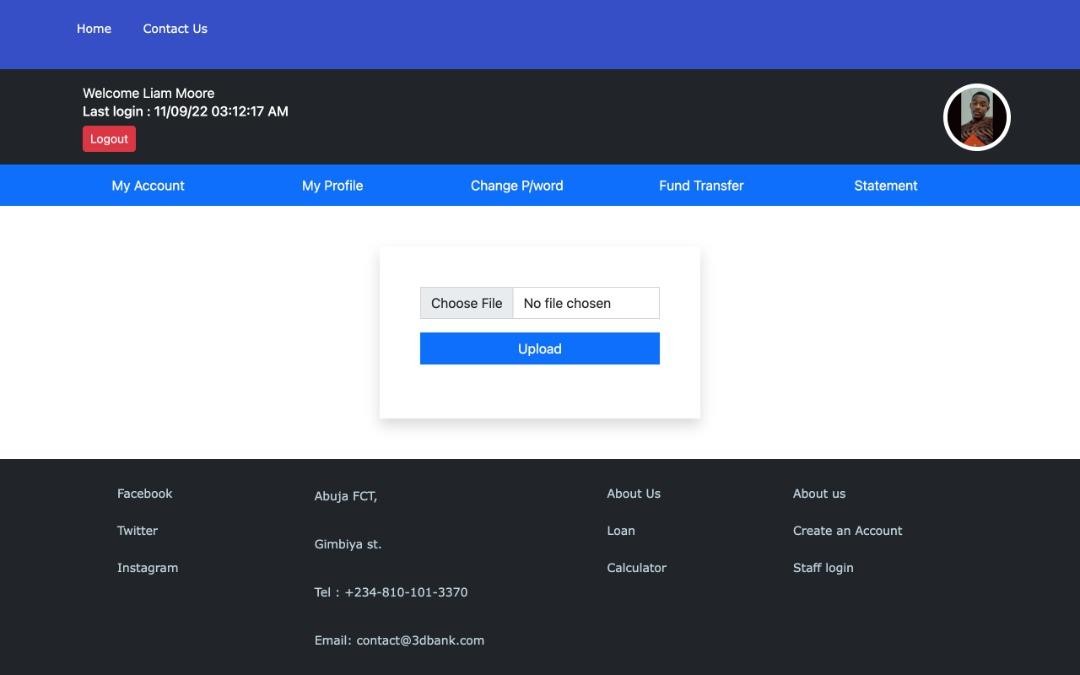


# Figure 25: Transfer Payment Gateway

* + 1. **Statement of account Generation:**



# Figure 26 Download of Statement of Account:



**Figure 27: Statement of Account Download**

# Summary

Implementation and implementation problems were discussed in this chapter, different types of application testing have also been discussed, some screenshots of the designed and developed application is also displayed in this chapter. Report and error reports has also been discussed. The next chapter which is chapter five is the final chapter of this project.

# CHAPTER FIVE

* 1. **Overview**

This chapter of this project is basically going to be focusing on conclusion of what has been able to be achieved over the period of time given to complete limitation that was undergone and the challenges faced as the project was progressing from one chapter to another till the end of the project.

# Objective Assessment

The aim and objectives of this project has been met and review about the implementation of the development of a more secured banking transaction authentication application using hybrid cryptograph has been done by selected Nigerians who are familiar with banking activities. Table below shows the score in percentage on how the implemented project has met with the aim and objectives.

|  |  |  |
| --- | --- | --- |
| S/N | Aim and Objectives | Score (%) |
| 1 | To develop a most authentic and secured means of transaction so as to eliminate fraudulent activities on  customers account | 90 |
| 2 | To use the hybrid cryptography algorithm due its  various strategic approach. | 95 |
| 3 | To develop and implement a user friendly platform | 97 |

# Limitations and Challenges

On the course of this project, many problems were encountered. Some of which includes lack of knowledge of adobe CS5. The problem was solved by leaning this programming language. Lack of adequate finance to run around for the project, this was solved by getting money from friends and family members. Unavailability of some research questions from text books and other sources, the solution was to interact with some Information Technology staff whom their practical experiences really helped in the project implementation.

There are some limitations for the current system to which solutions can be provided as a future development.

* + - The website is not accessible to everyone because it is currently on a local host server.
    - The system is not configured for multi user at this time.

# Future Enhancements

In the future development, the following can be done to improve or enhance the website functionalities of the website.

* + - The administrator of the website can be given more functionalities.
    - Third party proprietary software can be implemented for card validation check.
    - The concept of transaction can be used to achieve the uses of multi users not having access to the system at the same time.

# Recommendations

All Citizens Bank may have better improvement in the future since the current system is limited to few features, therefore more features can be added.

Another consideration is that the system needs large disk space in the future if it is running few years as system keeps growing with data.

# Summary

This project aim and objectives has been accomplished as discussed in the first chapter. All functional requirements stated has been implemented, though other important features like document handling and other automated processes were not implemented because of the time frame. This application was built properly meeting standard requirements for objective oriented programming, it is ready to deploy to live server for end user to use as an end product. Updates or few features will be included to better the performance of the application.

At the course of this project, I was able to develop software development skills in PHP, CSS and MySQL, I also learn a lot about sessions handling, development life cycle and many others.

# REFERENCES

Adeleke, A. (2003) Research Techniques. Concept Publications, Lagos.

Adetoro, S. A. (1997), Research Techniques for Projects, Proposals,Reports, Theses and Dissertations, Ahmadu Bello Univeristy Press LU. Zaria.

Ajayi, G. O., NITDA and ICT in Nigeria, (2013).

Akingbola, A. A (2006): “Electronic Payment Systems and Tele-banking Services in Nigeria”,

*Journal of Internet Banking and Commerce;* 11(3), 13-28

Ahasanul, H. (2009): “Issues of E-banking Transaction: An Empirical Investigation on Malaysian Customers Perception”, *Journal of Applied Sciences*, 2(6) 29-42

Andoh-Baidoo, F. K. & Osatuyi, B. (2013). *Examining Online Banking Initiative in Nigeria: A Value Network Approach*.

Al-Sukkar, H. (2005): “Toward a Model for the Acceptance of Internet Banking in Developing Countries”, *Information Technology for Development*, 11(4);.381-398

Archer, M.S. (2000), Homo economicus, Homo sociologicus and Homo sentiens, in M.S. Archer & Tritter, J.Q. (Ed.).*Rational Choice theory: Resisting colonization*, pp. 78-91. London: Routledge.

Asika, N. (2005), “*Research Methodology Process Approach”.* Mukugamu and Brother Enterprises.

Christopher, G. C., Mike, L. and Amy, W. (2006): “A Logit Analysis of Electronic Banking in New Zealand”, *International Journal of Bank Market*, 24: 360-383

Edet. O. (2008) Electronic banking Industries and Its effects. *International journal of investment and finance* 3(4), 10-16.

Gonzalez, M. E. (2008): “An Alternative Approach in Service Quality**:** An E-Banking Case Study”**,**

*Quality Manage,* 1(5); 41-48

Gupta, P. K. (2008): “Internet Banking in India: Consumer Concern and Bank Strategies”, *Global Journal of Business Research*, Vol. 2(1) 43-51

Ikechukwu, G. (2000). Enhancing the Performance of Banking Operations through Appropriate Information Technology in Nigeria Banking Industry, Ibadan: Spectrum Books.

Kannabira and Narayan (2005): “Deploying Internet Banking and E-Commerce: Case Study of a Private Sector Bank in India”, *Information Technology for Development;*11(4); 363-379.

Research Briefs on Informaiton & Communication Technology Evolution (ReBICTE), Vol. 6, Article No. 3 (October 1, 2020)

A Review of SMS Security Using Hybrid

Cryptography and Use in Mobile Money System. American Journal of Computer Science and Engineering. Vol. 2, No. 6, 2015, pp. 53-62.

Maholtra, P. and Singh, B. (2007): “Determinants of Internet Banking Adoption by Banks in India”, *Emerald Internet Research* 17(3); 323-339.

Madueme, I.S. (2009). Banking Efficiency and information Technology in Nigeria: An Empirical Investigation. *International Journal of Economics and Development* 8 (1&2). 23-45

Mohammed, S. K. Siba S. M. (2009): “Service Quality Evaluation in Internet Banking: An Empirical Study in India”, *International Journal of Indian Culture and Business Management*,2(1): 12-19

Mahdi, A. and Zhila A... (2008): “Islamic Banking Practice and Satisfaction: Empirical Evidence From Iran”, ACRM Journal of Business and Management Research, 3(2); 35-41

Oluyemi, S. A. (2010). *Development of Electronic Banking in Nigeria: The Associated Regulatory/Supervisory Challenges,* NDIC Quarterly, Vol II.

Osisioma, B. C. (2012). *Nigeria’s Transformation Agenda: the Management and Leadership Challenges,* presented on the occasion of 2012 NIM South-East Zonal Management Summit held at King David Hotels, Regina Caeli Road, Awka on 8th November, 2012.

Ovia, J. (2005): “Internet Banking: Practices and Potentials in Nigeria”*,* A paper presented at a

seminar organized by the Institute of Chartered Accountants of Nigeria (ICAN) Lagos Sheraton Hotel & Towers, Ikeja.

Oyesola S. (2007): “The Emergence of Internet Banking in Nigeria: An Appraisal”, *Information Technology Journal*;6 (4) 490-496.

Pandey, U. S. & Shukla, S. (2010). *E-Commerce and Mobile Commerce Technologies*, (S. Chand & Company Ltd, New Delhi, 2010), pp.159-161.

Saunders, M. et al.,(2009). *Research Methods for Business Students*, 5th Ed., (Pearson Education Limited, Essex, 2009), p.360.

Shavarts, A. (2002), Russian Mafia: The Explanatory power of Rational Choice theory’

*International Review of Modern Sociology* **30** (1), 66-106.

Sunday, O. & Arnold, P. E. (2012). *Accessing E-Banking Based on Resilient Transaction,*

Master\_Thesis\_E-banking\_updated.pdf> (03 April 2012), p.8.

International Journal of Innovation, Creativity and Change. [www.ijicc.net](http://www.ijicc.net/) Volume 6, Issue 8, 2019

Taro. (1976), *Analysis of Sample Size and Sample Population* in Research Methodology. Timothy, A. T. (2012), Electronic Banking Services and Customer Satisfaction in the Nigerian

Banking Industry *International Journal of Business and Management Tomorrow 2(3) 1 – 8*

website.informer.com (2014).

Christopher, G. C., Mike, L. and Amy, W. (2006).

[www.ffiec.gov/ffiecinfobase/booklets/e-banking/ebanking](http://www.ffiec.gov/ffiecinfobase/booklets/e-banking/ebanking) (06 January 2014).

[www.nibss-plc.com](http://www.nibss-plc.com/)> (10 February 2014).

APPENDICES

# Appendix - Questionnaire

Development of A More Secured Banking Transaction Authentication Application Using Hybrid Cryptograph Website Questionnaire For Research Purpose.

Kindly spare few minutes of your time to answer these questions by ticking your choice and writing where necessary.

Note: Please, do not write your Name, Phone Number or any personal information about yourself.

1. Please indicate your gender.

Male Female

1. Please indicate your age range 18-25

26-45

46 above

1. What is your first reaction to banking services within the cannabis industry?

Very positive Somewhat positive Neutral

Somewhat negative

Very negative

1. . How would you rate the quality of banking services you currently use?

Very high quality High quality

Neither high nor low quality Low quality

Very low quality

I don't use banking services

1. How innovative is the service?

Extremely innovative Very innovative Somewhat innovative Not so innovative

Not at all innovative

1. How often, if ever, do you currently use banking services?

Extremely often Very often Somewhat often Not so often



Never

31

1. If access to full business banking services were available today, how likely would you be to use the service?

Extremely likely Very likely Somewhat likely Not so likely

Not at all likely

1. When you think about banking, do you think of it as something you need or don’t need?

Definitely need Probably need Neutral

Probably don’t need

Definitely don’t need

1. When considering a new bank, what would be the top two things you would generally consider? (Check two boxes.)

Price Brand Innovation Quality Value

Other (specify)

1. How likely is it that you would recommend banking services to a friend or colleague? Not at all likely.

Extremely likely.

1. In your own words, what are the things you like most about your current bank?
2. In your own words, what are the things you like least about your current bank?

32

# Appendix – Source Codes

<?php ob\_start() ?>

<html>

<head>

<title>Registration Form</title>

<link rel="stylesheet" type="text/css" href="css/customer\_reg\_form.css"/>

<?php include'header.php'; ?>

</head>

<body>

<div class="container">

<h3 class="text-center my-5">Online Account Opening Form</h3>

<div class="row justify-content-center my-5">

<div class="col-md-6 shadow p-5">

<form method="post">

<div class="mb-3">

<input type="text" class="form-control rounded-0 p-2" name="name" placeholder="Name" required />

</div>

<div class="mb-3">

<select name ="gender" required class="form-select rounded-0 p-2">

<option class="" value="" disabled selected>Gender</option>

<option value="Male" required >Male</option>

<option value="Female">Female</option>

<option value="Others">Others</option>

</select>

</div>

<div class="mb-3">

<input type="text" class="form-control rounded-0 p-2" name="mobile" placeholder="Mobile no" required />

</div>

<div class="mb-3">

<input type="text" class="form-control rounded-0 p-2" name="email" placeholder="Email id" />

</div>

<div class="mb-3">

<input type="text" class="form-control rounded-0 p-2" name="landline" placeholder="Landline no" />

</div>

<div class="mb-3">

<input type="text" class="form-control rounded-0 p-2" name="dob" placeholder="Date of Birth" onfocus="(this.type='date')" required />

</div>

<div class="mb-3">

<input type="text" class="form-control rounded-0 p-2" name="pan\_no" placeholder="PAN Number" required />

</div>

<div class="mb-3">

<input type="text" class="form-control rounded-0 p-2" name="citizenship" placeholder="Citizenship Number" required />

</div>

<div class="mb-3">

<input class="form-control rounded-0 p-2" type="text" name="homeaddrs" placeholder="Home Address" required />

</div>

<div class="mb-3">

<input class="form-control rounded-0 p-2" type="text" name="officeaddrs" placeholder="Office Address" />

</div>

<div class="mb-3">

<input type="text" class="form-control rounded-0 p-2" name="country" placeholder="US" value="Nigeria" readonly="readonly"/>

</div>

<div class="mb-3">

<select name ="state" required class="form-select rounded-0 p-2">

<option class="default" value="" disabled selected>Zone</option>

<option value="North">North</option>

<option value="South">South</option>

<option value="East">East</option>

<option value="West">West</option>

</select>

</div>

<div class="mb-3">

<select name ="city" required class="form-select rounded-0 p-2">

<option class="default" value="" disabled selected>City</option>

<option disabled selected>--Select State--</option>

<option value="Abia">Abia</option>

<option value="Adamawa">Adamawa</option>

<option value="Akwa Ibom">Akwa Ibom</option>

<option value="Anambra">Anambra</option>

<option value="Bauchi">Bauchi</option>

<option value="Bayelsa">Bayelsa</option>

<option value="Benue">Benue</option>

<option value="Borno">Borno</option>

<option value="Cross River">Cross River</option>

<option value="Delta">Delta</option>

<option value="Ebonyi">Ebonyi</option>

<option value="Edo">Edo</option>

</div>

<div class="mb-3">

<input type="text" class="form-control rounded-0 p-2" name="pin" placeholder="Pin Code" required />

</div>

<option value="Ekiti">Ekiti</option>

<option value="Enugu">Enugu</option>

<option value="FCT">Federal Capital Territory</option>

<option value="Gombe">Gombe</option>

<option value="Imo">Imo</option>

<option value="Jigawa">Jigawa</option>

<option value="Kaduna">Kaduna</option>

<option value="Kano">Kano</option>

<option value="Katsina">Katsina</option>

<option value="Kebbi">Kebbi</option>

<option value="Kogi">Kogi</option>

<option value="Kwara">Kwara</option>

<option value="Lagos">Lagos</option>

<option value="Nasarawa">Nasarawa</option>

<option value="Niger">Niger</option>

<option value="Ogun">Ogun</option>

<option value="Ondo">Ondo</option>

<option value="Osun">Osun</option>

<option value="Oyo">Oyo</option>

<option value="Plateau">Plateau</option>

<option value="Rivers">Rivers</option>

<option value="Sokoto">Sokoto</option>

<option value="Taraba">Taraba</option>

<option value="Yobe">Yobe</option>

<option value="Zamfara">Zamfara</option>

</select>

<div class="mb-3">

<input type="text" class="form-control rounded-0 p-2" name="arealoc" placeholder="Area/Locality" required />

</div>

<div class="mb-3">

<input type="text" class="form-control rounded-0 p-2" name="nominee\_name" placeholder="Nominee Name (If any)" />

</div>

<div class="mb-3">

<input type="text" class="form-control rounded-0 p-2" name="nominee\_ac\_no" placeholder="Nominee Account no" />

</div>

<div class="mb-3">

<select name ="acctype" required class="form-select rounded-0 p-2">

<option class="default" value="" disabled selected>Account Type</option>

<option value="Saving">Saving</option>

<option value="Current">Current</option>

</select>

</div>

<div class="mb-3 d-grid">

<input type="submit" class="btn btn-primary btn-block rounded-0 p-2" name="submit" value="Create an Account">

</div>

</form>

</div>

</div>

</div>

<?php include'footer.php';?>

</body>

</html>

<?php

if(isset($\_POST['submit'])){

session\_start();

$\_SESSION['$cust\_acopening'] = TRUE;

$\_SESSION['cust\_name']=$\_POST['name'];

$\_SESSION['cust\_gender']=$\_POST['gender'];

$\_SESSION['cust\_mobile']=$\_POST['mobile'];

$\_SESSION['cust\_email']=$\_POST['email'];

$\_SESSION['cust\_landline']=$\_POST['landline'];

$\_SESSION['cust\_dob']=$\_POST['dob'];

$\_SESSION['cust\_pan=']=$\_POST['pan\_no'];

$\_SESSION['cust\_citizenship']=$\_POST['citizenship'];

$\_SESSION['cust\_homeaddrs']=$\_POST['homeaddrs'];

$\_SESSION['cust\_officeaddrs']=$\_POST['officeaddrs'];

$\_SESSION['cust\_country']=$\_POST['country'];

$\_SESSION['cust\_state']=$\_POST['state'];

$\_SESSION['cust\_city']=$\_POST['city'];

$\_SESSION['cust\_pin']=$\_POST['pin'];

$\_SESSION['arealoc']=$\_POST['arealoc'];

$\_SESSION['nominee\_name']=$\_POST['nominee\_name'];

$\_SESSION['nominee\_ac\_no']=$\_POST['nominee\_ac\_no'];

$\_SESSION['cust\_acctype']=$\_POST['acctype'];

header('location:cust\_regfrm\_confirm.php');

}

?>

42