****

**MERU UNIVERSITY OF SCIENCE AND TECHNOLOGY**

**BACHELOR OF SCIENCE IN COMPUTER SECURUTY AND FORENSICS**

**DEPARTMENT OF COMPUTER SCIENCE**

**SIGNATURE VERIFICATION IN A BANK SYSTEM**

|  |  |
| --- | --- |
| **STUDENT REGISTRATION NUMBER** | **STUDENT NAME** |
| CT206/101972/20 | Diphlex Ochieng |
| CT206/104336/20 | Japheth Kasinya |
| CT206/104339/20 | Paul Muia |
| CT206/104351/20 | Laban Kiptoo |
| CT206/104355/20 | Brian Kipkoech Too |

A Research group project submitted in partial fulfillment of the requirements of the Bachelor of Science in Computer Security and Forensics.

September,2022

**DECLARATION**

This group research project is our original work prepared with the indicated sources and support and has not been presented elsewhere for a similar or different assignment.

|  |  |  |  |
| --- | --- | --- | --- |
| Student reg no | Student name | Signature | Date |
| CT206/101972/20 | Diphlex Ochieng |  |  |
| CT206/104336/20 | Japheth Kasinya |  |  |
| CT206/104339/20 | Paul Muia |  |  |
| CT206/104351/20 | Laban Kiptoo |  |  |
| CT206/104355/20 | Brian Too |  |  |

Contents

[CHAPTER ONE 1](#_Toc116981478)

[INTODUCTION 1](#_Toc116981479)

[1.1 Background of study 1](#_Toc116981480)

[1.2 Motivation for study 3](#_Toc116981481)

[1.3 Problem statement 3](#_Toc116981482)

[1.4 Research objectives 3](#_Toc116981483)

[1.4.1 General Objectives 3](#_Toc116981484)

[1.4.2 Specific Objectives 3](#_Toc116981485)

[1.5 Significance of the study 4](#_Toc116981486)

[1.6 Scope of the study 4](#_Toc116981487)

[1.7 Assumptions in the study 4](#_Toc116981488)

[1.8 Limitations of study 4](#_Toc116981489)

[CHAPTER TWO 6](#_Toc116981490)

[LITERATURE REVIEW 6](#_Toc116981491)

[2.1 Overview 6](#_Toc116981492)

[2.2 Function of the existing system. 6](#_Toc116981493)

[2.3 Components of the existing signature verification system. 6](#_Toc116981494)

[2.4 Challenges of the existing signature verification system. 6](#_Toc116981495)

[2.5 Related work 7](#_Toc116981496)

[2.6 Summary 7](#_Toc116981497)

[CHAPTER THREE 8](#_Toc116981498)

[METHODOLOGY 8](#_Toc116981499)

[3.0 Overview 8](#_Toc116981500)

[3.1 Research Design 8](#_Toc116981501)

[3.3 Population and Sampling 9](#_Toc116981502)

[3.4 Data collection instrumentation 9](#_Toc116981503)

[3.5 Development tools and materials 11](#_Toc116981504)

[3.6 System development methodology 11](#_Toc116981505)

[3.7 Data processing and analysis 11](#_Toc116981506)

[3.8 Ethical consideration 12](#_Toc116981507)

[3.9 Summary 12](#_Toc116981508)

[CHAPTER FOUR 13](#_Toc116981509)

[SYSTEM ANALYSIS 13](#_Toc116981510)

[4.0 Overview 13](#_Toc116981511)

[4.1 Feasibility study 13](#_Toc116981512)

[4.2. Overall description of the current banking system. 14](#_Toc116981513)

[4.2.1. Banking system use-case diagram. 15](#_Toc116981514)

[4.2.2. Banking system class diagram. 16](#_Toc116981515)

[4.2.3. Banking system sequence diagram. 17](#_Toc116981516)

[4.2.4 Banking system data flow diagram. 18](#_Toc116981517)

[4.2.5 Banking system activity diagram. 19](#_Toc116981518)

[4.3 Requirement gathering 20](#_Toc116981519)

[4.3.1. Functional requirements. 20](#_Toc116981520)

[4.3.1.1. Register 20](#_Toc116981521)

[4.3.1.2 Report generation. 20](#_Toc116981522)

[4.3.1.3 Verification. 20](#_Toc116981523)

[4.3.2. Non-functional requirements. 21](#_Toc116981524)

[4.3.2.1 Security 21](#_Toc116981525)

[4.4 Summary. 21](#_Toc116981526)

[CHAPTER FIVE 22](#_Toc116981527)

[SYSTEM DESIGN 22](#_Toc116981528)

[5.0. OVERVIEW 22](#_Toc116981529)

[5.1 Logical design of signature verification in a bank 22](#_Toc116981530)

[22](#_Toc116981531)

[22](#_Toc116981532)

[22](#_Toc116981533)

[22](#_Toc116981534)

[22](#_Toc116981535)

[22](#_Toc116981536)

[22](#_Toc116981537)

[22](#_Toc116981538)

[22](#_Toc116981539)

[22](#_Toc116981540)

[22](#_Toc116981541)

[22](#_Toc116981542)

[5.2 Physical design 23](#_Toc116981543)

[5.2.1 Welcome page 23](#_Toc116981544)

[5.2.2 Password reset 24](#_Toc116981545)

[5.2.3 Login page 25](#_Toc116981546)

[5.2.4 Loan request 26](#_Toc116981547)

[Figure 5.4: Showing Loan Request Form 26](#_Toc116981548)

[5.2.5 Account form. 26](#_Toc116981549)

[5.2.6 Bank attendant form 27](#_Toc116981550)

[Figure 5.6: Showing Bank Attendant Form 27](#_Toc116981551)

[5.2.7 Bank form. 27](#_Toc116981552)

[5.2.8 Customer registration form. 28](#_Toc116981553)

[Figure 5.8: Showing Customer Registration Form 28](#_Toc116981554)

[5.3 Database design of the signature verification in a bank system 28](#_Toc116981555)

[5.3.1 Account table 28](#_Toc116981556)

[5.3.2 Bank table 29](#_Toc116981557)

[Figure 5.1.0: Showing Bank Table. 29](#_Toc116981558)

[5.3.3 Bank Attendant table 29](#_Toc116981559)

[Figure 5.1.1: Showing Bank Attendant Table 29](#_Toc116981560)

[5.3.4 Customer Table 29](#_Toc116981561)

[5.3.5 Loan table 30](#_Toc116981562)

[5.3.6 Database logical design 30](#_Toc116981563)

[5.4. Summary 31](#_Toc116981564)

[CHAPTER SIX 32](#_Toc116981565)

[SYSTEM IMPLEMENTATION 32](#_Toc116981566)

[6.0 Overview 32](#_Toc116981567)

[6.1 Implemented Features 32](#_Toc116981568)

[6.1.1 Registration Feature 32](#_Toc116981569)

[6.1.2 Customer Login Feature 33](#_Toc116981570)

[6.1.3 Loan Feature 35](#_Toc116981571)

[6.1.4 Signature Verification Feature 36](#_Toc116981572)

[6.2 System Testing 36](#_Toc116981573)

[6.2.1 Customer Registration 37](#_Toc116981574)

[6.2.2 Password verification 37](#_Toc116981575)

[6.2.3 Customer login 38](#_Toc116981576)

[6.2.4 Loan Request 39](#_Toc116981577)

[6.3 System Changeover 39](#_Toc116981578)

[6.4 Documentation 40](#_Toc116981579)

[6.5 Summary 41](#_Toc116981580)

[CHAPTER SEVEN 42](#_Toc116981581)

[FINDINGS, CONCLUSION AND RECOMMENDATIONS. 42](#_Toc116981582)

[7.0 Findings. 42](#_Toc116981583)

[7.1 Conclusion 43](#_Toc116981584)

[7.2 Recommendations 43](#_Toc116981585)

[REFERENCES 45](#_Toc116981586)

# CHAPTER ONE

# INTODUCTION

## Background of study

Signature verification has been in use since long ago to authenticate documents. In the early ages documents were been verified by affixing signatures to documents and this signatures were handwritten. Intricate seals were applied to clay cuneiform tablets by the Sumerians to authenticate writings. In the late 1670’s an act to prevent fraud was enacted by England which required participating parties to sign their documents. Around 1980 studies on signature verification were published which were later followed by numerous studies, attempting various feature extraction and matching techniques (Diaz,2018) .

The cheapest and easiest way to authenticate a person is via signature. A signer is identified through a signature on the document. Every document processing platform requires a signature verification system, Aguilar(2004). Signature verification of an account holder is done manually, which has brought rise to automation of signature verification.

The manual signature verification technique was introduced. It involved comparing an already signed document with a newly presented document. Features of both signatures were crosschecked, if they matched then the signature would be deemed genuine and therefore would be verified. If the signature in the already signed document did not match with the new signature, then the new signature would be deemed fake therefore would not be verified. The traditional signature verification technique that was used had several limitations including signature forgery which hinders the effectiveness of the manual signature verification technique. This problem made researchers come up with an electronic system like Nagel and Rosenfeld IEEE T. Comp which was an offline system and also Liu and Herbst online system which were less prone to forgery compared to the manual verification technique, Sharif(2020). These systems involved training the computer on how to distinguish between genuine signatures and forged ones. Once forged signatures have been detected, they would be flagged-off and deemed fake therefore they would not be verified.

This however has been met with several challenges such as these systems being high capital intensive and required a lot of time to develop. They were also not very user friendly. Therefore there was need for the development of a much more effective system which is less costly, user friendly and requires less time to develop, Diaz(2018).

## Motivation for study

Traditional signature verification systems are prone to forgery. This has motivated several researchers towards developing better and viable solutions which are less prone to faking and forgery which in turn would improve the signature verification process.

## Problem statement

The proposed system that is to be developed would have two main features. One would be to verify genuine signatures and allow a user to apply a loan while the other feature would be to detect and flag-off forged signatures therefore deny the user a loan. Currently, manual verification is used as well as other electronic verification techniques, Khan(2020). However, these verification methods are prone to several challenges. Manual verification technique is susceptible to forgery which allows verification of forged signatures and mismatching of signatures. The other already developed have a challenge of being too costly and not as effective as they should be.

## Research objectives

## 1.4.1 General Objectives

The aim of this project is to develop a signature verification system that is intended to allow user signature verification in a bank which in turn would be used to determine whether a user is eligible to apply for a loan or not.

## 1.4.2 Specific Objectives

The purpose of this project is to develop a system that should be able:

1. To allow a customer open an account.
2. To allow a customer apply for a bank loan.
3. To allow the system verify the customer signature.
4. To enable the system generate a monthly report on the type of customers with the highest number of mismatched signatures.

## Significance of the study

The proposed system will help the organization to only verify genuine signatures and flag-off faked ones. The system will therefore address the issue of verification of forged signatures.

The proposed system is also intended to help the researchers pass their course and attain their Bachelor’s degree.

## Scope of the study

The main focus of this project is on signature verification where the system will be able to verify genuine signatures, detect and flag-off forged signatures.

## Assumptions in the study

The following assumptions were made regarding this research study:

1. The devices used will have enough capability to handle the proposed system and allow it to run successfully
2. The user’s signature will remain the same at all times
3. All user signatures are completely different from each other.

## Limitations of study

1. The proposed system will not be effective in the event that a user forgets or changes their signature
2. The proposed system will not be able to immediately verify new users whose signatures have not been updated in the system.

# CHAPTER TWO

# LITERATURE REVIEW

## Overview

In this section; functions, components, features and challenges of the signature verification systems are discussed.

## Function of the existing system.

According to Diaz (2018) developed a signature verification system whose function was to verify an individual’s identity by only training the system with only one signature specimen.

According to Aguillar (2004) the developed system verified user signatures offline based on integration of both Global and Local information.

In Faisal(2020) the developed system implemented a novel signature verification technique which implemented Genetic Algorithm selection technique.

## Components of the existing signature verification system.

The existing systems involved training the system using signature specimens which were later used in verification of signatures. Technologies such as integration of both Global and Local information and also Genetic algorithm were used in order to develop systems that could successfully verify signatures.

## Challenges of the existing signature verification system.

* Several signature specimens were required to provide sufficient accurate verification of an individual’s identity.
* Users have difficulty in assigning speed to their signature therefore users could not perceive the level of difficulty of the signature.
* In hand held signature verification devices, Fernandez(2007) small input areas and poor ergonomics in mobile devices increase variability during the signing Poor ergonomics and small input areas in mobile devices are key factors that increase the variability during the signing process and verification process.
* Inter and intra-variability in skilled forgeries hinders the system from achieving good verification performance.

## Related work

In Diaz (2018) the system developed only focused on training the system with a single signature specimen whereas in Faisal(2020) developed a system that implemented Genetic Algorithm selection technique.

Sharif (2020) offline signature verification system used a novel technique that involved fusion of geometric features and Gray Level Co-occurrences Matrix (GLCM) while Tekerek (2021) developed an offline handwritten signature verification system that used Cycle-GAN as a data argumentation method.

## Summary

This chapter represented functions, components and challenges of the signature verification system. Comparisons of related works were also made to determine the drawbacks addressed by each one of them.

# CHAPTER THREE

# METHODOLOGY

## 3.0 Overview

This chapter deals with research design methodology used in the research on the signature verification in a bank system. It provides information on the participants, data collection and the analysis of the data as well as the conclusions drawn and the ethical issues that were followed in the process.

## 3.1 Research Design

According to Abbott (2013), Research design is a plan that provides the underlying structure to integrate all elements of a quantitative study so that the results are credible, free from bias and maximally generalizable. Research design provides the glue that holds the research together. The research design determines how the participants were selected, what variables were included and how they are manipulated, how data was collected and analyzed, and how extraneous variability was controlled so that the overall research problem can be addressed. Regardless of the sophistication of the statistics, the researcher conclusions could be worthless if an inappropriate research design was used. This study utilized a quantitative approach, in this approach the researcher’s focuses on quantifying the data into numerical values and it adopted a descriptive survey design.

## 3.3 Population and Sampling

Study population is that population from which it was used to generalize the results of the study. The population of the study consists two banks; Equity and KCB bank, Meru branches.

According to Hamed (2016), Sampling is a technique of choosing a sub-group from a targeted population. It is a process of selecting a number of individuals for a research in such a way that the individuals selected represent the entire population from which it was selected from. Probability sampling was used in this study. This technique was best suited for this study since it was easy to carry out and included all respondents with characteristics to be included in the study. Stratified sampling became suitable for this study.

## 3.4 Data collection instrumentation

Data collection is the process of gathering and measuring information on targeted variables in an established system which then enables one to answer relevant questions and evaluate outcome Collin (2020).

There several methods of data collection .For this research, questionnaires were used to obtain information from bank attendants and customers. A sample of the questionnaire is attached on the appendix.

## 3.5 Development tools and materials

The following tools were used to develop the system:

* Laptop (EliteBook g1, 4GBRAM/500GB internal memory)
* Python programming language
* HTML, CSS, JAVASCRIPT
* Word processing 2016

## 3.6 System development methodology

SDL is a methodology for designing, building and maintaining information and industrial system Bassil (2012).

For this research, waterfall model was used because:

* It is easy and simple to understand, utilize and implement
* It is rigid therefore easy to manage
* Phases do not overlap

## 3.7 Data processing and analysis

In order to process data that was obtained from the questionnaires, the questionnaires were grouped according to the questions that were related.

Responses from the questionnaires were then analyzed and comparison was made between responses from customers and bank attendants. It was noted that most banks verify their customers’ signature manually. Also when a customer is opening a new account, their identification card number, full names and signature were required. When requesting for a loan, a customer signature was required in order to authenticate the loan transaction. From the above findings, it was discovered that signature verification in most banks was not a priority which proved to cause problems as stated by some customers in the questionnaire

## 3.8 Ethical consideration

The researchers obtained an informed consent from the relevant authorities in order to be permitted to conduct the research.

The data collected will only be used for purposes none other than for research and research only.

## 3.9 Summary

The above chapter discussed; data collection, data processing and analysis. The SDLC methodology as well as ethical consideration was also discussed.

# CHAPTER FOUR

# SYSTEM ANALYSIS

## 4.0 Overview

This chapter covers feasibility study done by the researchers to make the project viable; social feasibility was used to show how the signature verification system in a bank was socially accepted, economic feasibility to show the cost of the project. Feasibility report was documented and attached as an appendix. Overall description of the current system such as data flow diagrams is also covered. Requirements necessary for gathering information; functional requirements (the ones that can be shown), non-functional requirements (cannot be shown) and summary appear in this chapter.

## 4.1 Feasibility study

According to (Shah 2012) feasibility study is a preliminary exploration of a proposed project or undertaking to determine its merits and viability. It aims to provide an independent assessment that examines all aspects of a proposed project, including technical, economic, financial, legal and environmental considerations. This information then helps researchers whether or not to proceed with the project. The feasibility study results can also be used to create a realistic project plan and budget. While conducting the feasibility study, it was found out that technically the organization has enough computers to run the proposed system. However, software upgrades and random access memory (RAM) will also need to be upgraded. The current system will take four and a half months to develop. Legally the current system meets all the legal and contractual laws of the country. It was also discovered that the proposed system meets the economic feasibility since the cost that would be incurred to develop the proposed system would be minimal and can be handled by the organization. The proposed system is likely to change the work environment of the organization since some staff may need to be trained, replaced and a qualified system administrator be hired.

## 4.2. Overall description of the current banking system.

The current banking system is manual. When a customer wants to open a bank account, the customer visits the bank and manually submits their names, identification number, Kenya revenue authority (KRA) pin, passport and copies of their national identification card and KRA pin. The bank attendant then enters the customer details into the system for registration of the new customer. The customer then signs a declaration and registration forms to approve their membership. The attendant then activates the new customer account and the customer deposits some amount of money into the account to complete the activation.

Once the bank account is active, the customer can then start saving money into the account. After using the account for a minimum of six months the customer is allowed to request for a loan. The loan is awarded based on the customer's savings where a customer can be given a loan of up to three times their savings. Once the customer has met the minimum requirements to apply for a loan, the customer can visit the bank and pick a loan form. In the loan form, the customer fills in their name, identification number, loan amount, loan terms and signs off the loan form. The customer is also required to gather at least two signatures of guarantors to make him or her eligible for the loan. After receiving the loan form, the bank attendant checks and manually verifies the details in the loan form to determine whether the member can be awarded the loan or not. The bank attendant generates loan reports from the system which are then handed over to the bank manager. The overall view of the banking system is represented using use-case diagrams, class diagrams, sequence diagram, dataflow diagram and activity diagram are detailed in the sections below.

## 4.2.1. Banking system use-case diagram.

A use-case diagram is a graphical depiction of a user's possible interactions with a system ("use-case diagram," 2021). Figure 4.1 below shows the use-case diagram for the current banking system.

Customer Cash dispenser

Manager Bank attendant

Figure 4.1: The current banking system Use-Case diagram.

## 4.2.2. Banking system class diagram.

In ("class diagrams," 2009) a class diagram is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among objects. It is important for translating the models into programming code. Figure 4.2 shows the use class diagram for the current banking system.

Name

ID NO

Bank Attendant

Bank

Name

Code

1 m

Add customer ()

Remove customer ()

Verify loan ()

m

Verify signature ()

Acc\_number

Balance

Customer

Cust\_id

Name

Card number

Pin

Phone

Signature

Loan

Account

m

Loan no

Amount

Type

1 1 1 m

Deposit ()

Withdraw ()

Get balance ()

Verify loan ()

Verify signature ()

Figure 4.2: The current banking system class diagram.

## 4.2.3. Banking system sequence diagram.

According to ("unified modelling language,"2011) a sequence diagram shows process interactions arranged in time sequence in the field of software engineering. It depicts the processes involved and the sequence of messages exchanged between the processes needed to carry out the functionality.

Figure 4.3 shows the sequence diagram for the current banking system.

**Customer Bank Attendant Manager**

1. Open account 1. Request loan
2. Deposit cash 2. Issue report
3. Issue receipt
4. Withdraw cash
5. Dispense cash
6. Check balance
7. Show balance
8. Request loan
9. Award loan

Figure 4.3: The current banking system sequence diagram.

## 4.2.4 Banking system data flow diagram.

A data-flow diagram is a way of representing a flow of data through a process or a system. ("data flow diagram,"1990). Figure 4.4 shows the Data flow diagram for the current banking system

Customer

Bank system

Manager

Open account

Deposit cash Request report

Check balance Issue report

Show balance

Request loan

Issue loan

Figure 4.4: The current banking system data-flow diagram.

## 4.2.5 Banking system activity diagram.

According to (Rumbaugh,1999) activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. Figure 4.5 shows the activity diagram for the current banking system.

Request loan

Current balance

Open account

Award loan

Is eligible

Withdraw

Deposit

Y

Update balance

Deny loan

N

Figure 4.5: The current banking system activity diagram

## 4.3 Requirement gathering

According to(Boogaard,2022) Requirements gathering is the process of determining what your projects need to achieve and what needs to be created to make that happen.

## 4.3.1. Functional requirements.

Functional requirement defines a function of a system or its component, where a function is described as a specification of behavior between inputs and outputs.

## 4.3.1.1. Register

The bank attendant is provided with a platform to register a new customer. The attendant is required to enter the customer name, Identification number, phone number, Kenya Revenue Authority Pin and collect customer password. The system saves the information and confirm customer registration.

## 4.3.1.2 Report generation.

The system can generate reports according to the court information provided by the bank attendant. The following reports are generated by the system:

A monthly report showing the number of loans awarded. The attendant is required to query the database using customer identification number and loan number.

A monthly report of newly registered customers. This is initiated by the bank attendant by using the customer identification number. The report illustrates the details of all newly registered customers.

## 4.3.1.3 Verification.

The system is expected to verify a loan awarded to a customer. This is based on customer savings and the transactions the user has been making. The system is also expected to calculate the actual loan amount to be awarded to a customer.

## 4.3.2. Non-functional requirements.

According to (Rowel,1997) a non-functional requirement is a requirement that specifies criteria that can be used to judge the operation of a system, rather than specific behaviors. The non-functional requirements will serve as constraints or restrictions to the bank signature verification system across the different backlogs. The non-functional requirements will also ensure effectiveness and usability of the entire system. In usability, it ensures the system functions the way it is supposed to, while effectiveness ensures the system gives correct output when given some input values.

## 4.3.2.1 Security

Security is the protection from or resilience against potential harm caused by others by restricting the freedom of others to act (Buzan,1998). The bank signature verification system requires a customer to identify himself or herself using a login username and password. The Metrix for measuring the security of the system is the number of attempts made to access the bank with the correct or wrong login attempt. This helps the manager to know the eligibility of the system to verify customer.

## 4.4 Summary.

This chapter entails feasibility study and how it affected the current system, the overall description of the current banking system. It also covers use-case diagram, class diagram, sequence diagram, dataflow diagram and activity diagram. It also entails requirement gathering.

## CHAPTER FIVE

## SYSTEM DESIGN

## 5.0. Overview

This chapter contains logical designing of the signature verification in a bank system using entity relation diagrams which show the relations of entities in the system. Physical designing of the system whereby snapshots of how it was developed are shown. How the database was designed and summary also appear in the chapter.

## 5.1 Logical design of signature verification in a bank

The ER diagram below explains the relationships between different entities.

Has

Award to

Loan

Verifies

Bank attendant

## 

Bank

## 

## 

## 

## 

## 

## 

## 

## 

Operator

## 

Account

Customer

## 

## 

Figure 5.0: The current banking system relation between entities diagram.

## 5.2 Physical design

## 5.2.1 Welcome page

When a user enters the open Rotse Bank app, this will appear. The customer will be required to enter customer name, national identification card, phone number and password. In case he/she has forgotten password, the customer will click password reset button and follow procedure to reset password

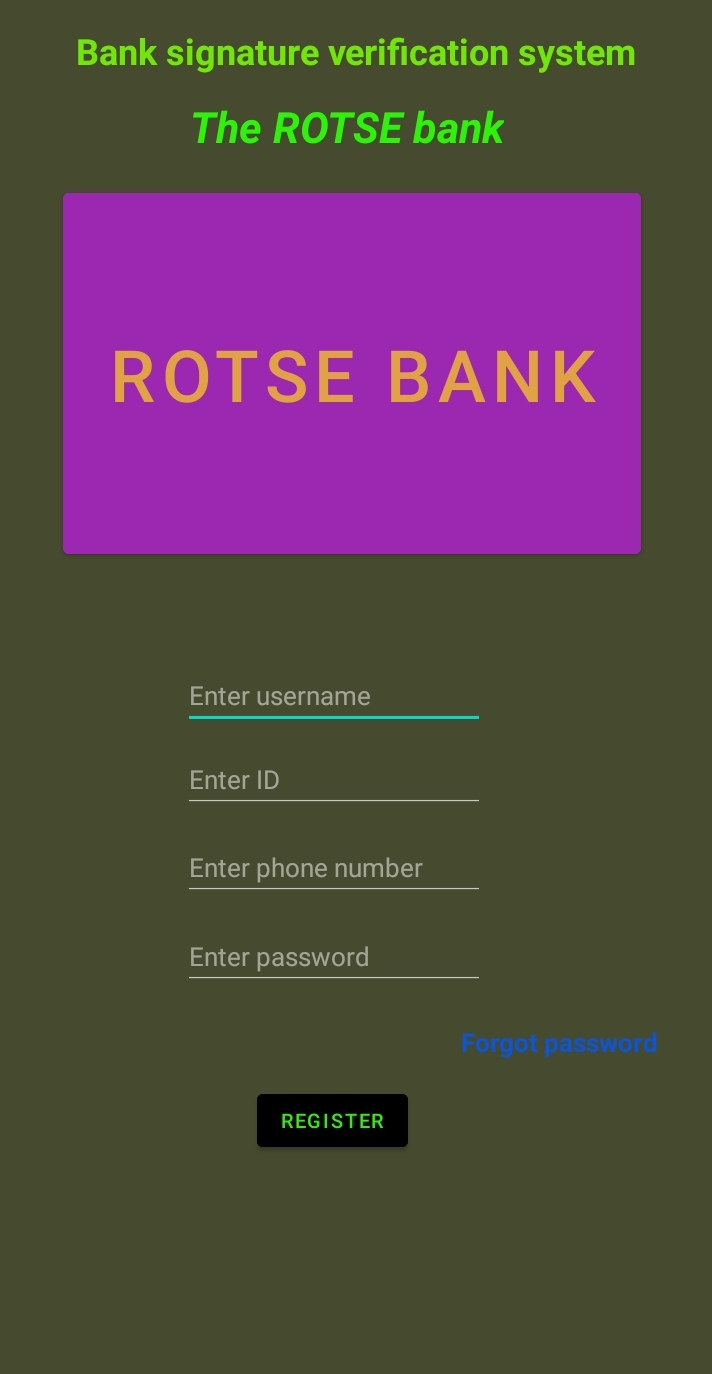


Figure 5.1: Showing the Welcome Interface.

## 5.2.2 Password reset

Customer will be required to enter to enter phone number, national identification number and if the details will be verified then a password reset code will be sent and he/she will be required to ether it in the box that will ask for verification code

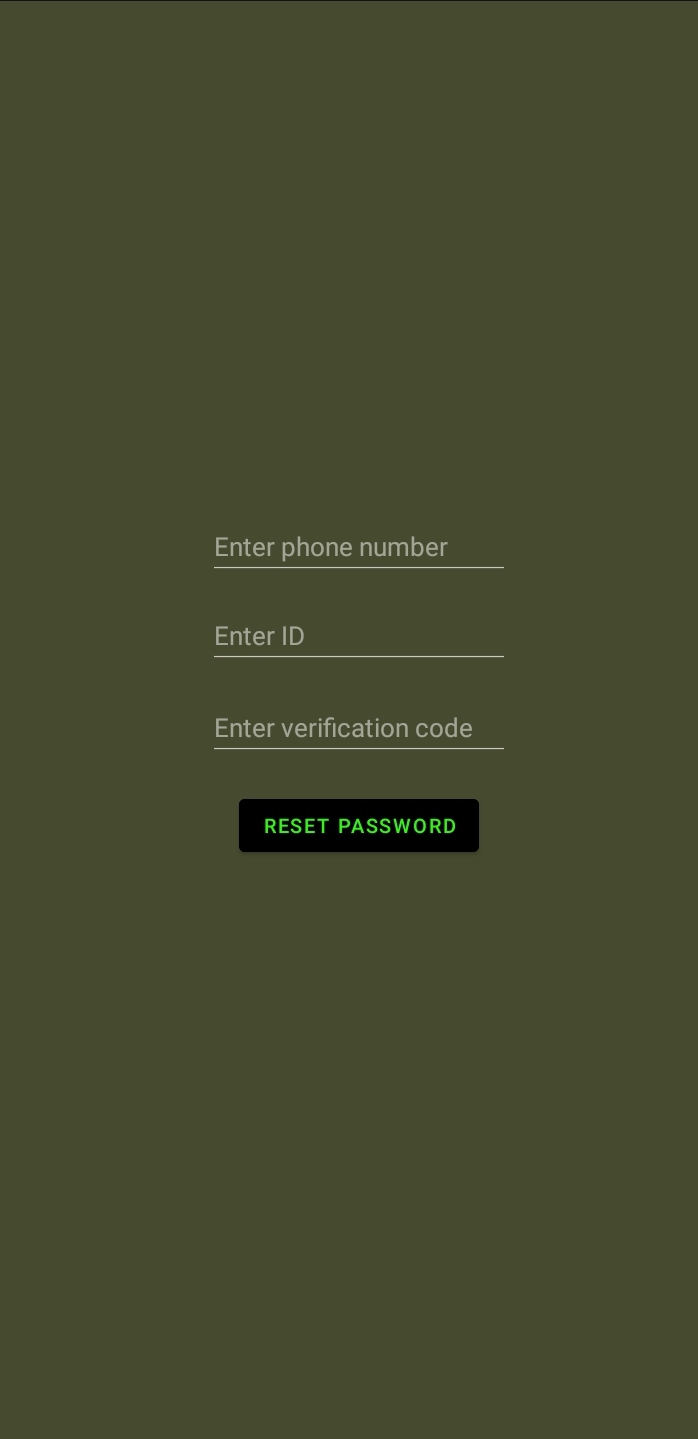


Figure 5.2: Showing Password Reset Interface

## 5.2.3 Login page

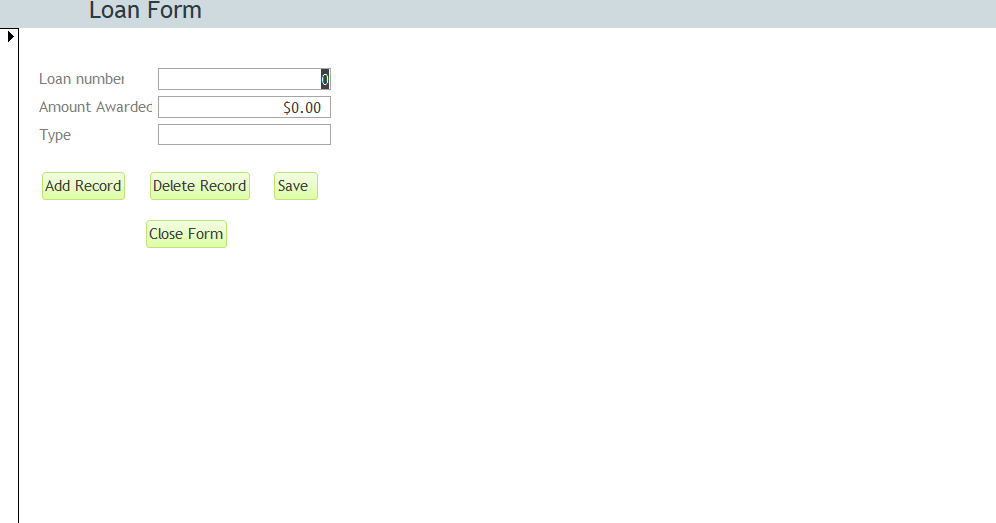
When customer credentials are verified a page that displays two options will appear. The customer will then choose one of the options according to the needs



Figure5.3: Showing Loan Request Interface

## 5.2.4 Loan request

This page will appear when a customer clicks on Request loan button



## Figure 5.4: Showing Loan Request Form

## 5.2.5 Account form.

On this interface the bank attendant is required to enter the customer’s account number and update their balance.

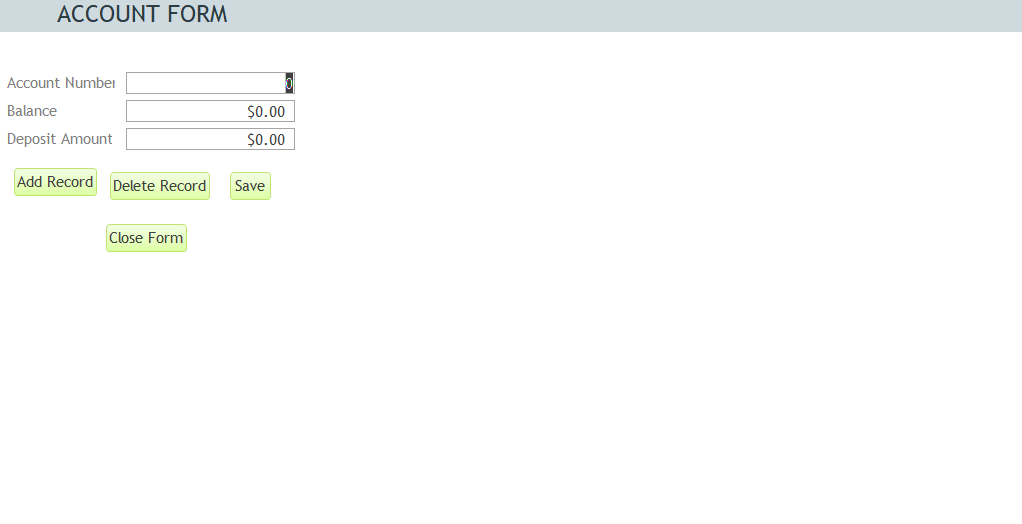
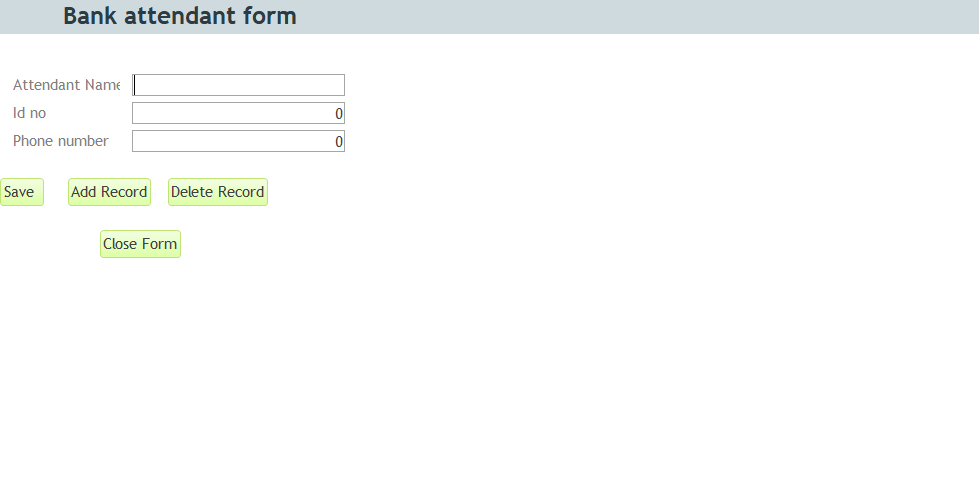


Figure 5.5: Showing Account Form

## 5.2.6 Bank attendant form

This interface allows the manager to enter details of bank attendance.

****

## Figure 5.6: Showing Bank Attendant Form

## 5.2.7 Bank form.

This interface allows the bank manager to enter bank details which include the bank code and the name.

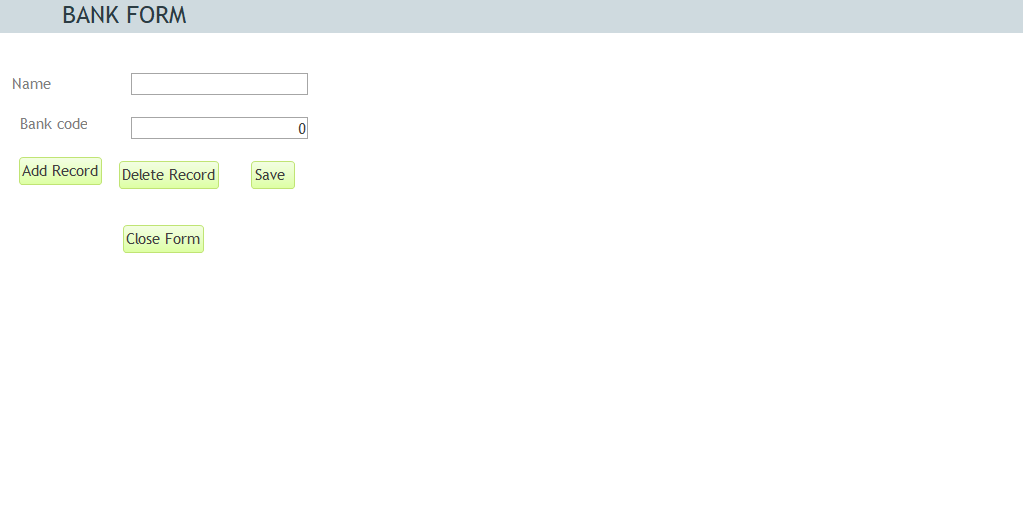


Figure 5.7: Showing Bank Form

## 5.2.8 Customer registration form.

This interface is accessible by both the customer and the bank attendant. This form is used to add and save customer details. The pin entered should be a four- digit number and should be kept secret

## Figure 5.8: Showing Customer Registration Form

## 5.3 Database design of the signature verification in a bank system

The following are the tables in the signature verification system in a bank.

## 5.3.1 Account table

The account table include the account number, deposit and balance. The account number is the primary key.

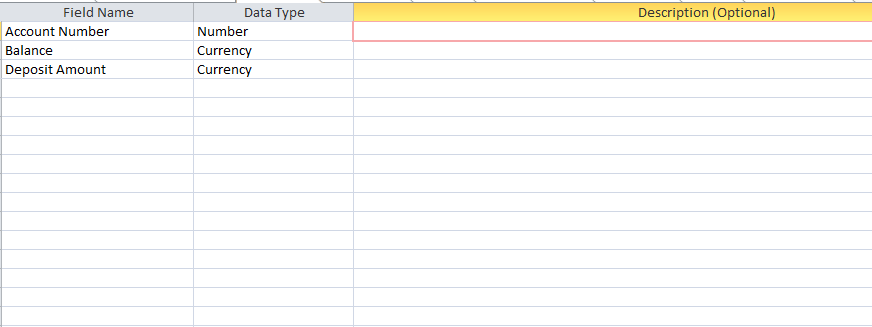
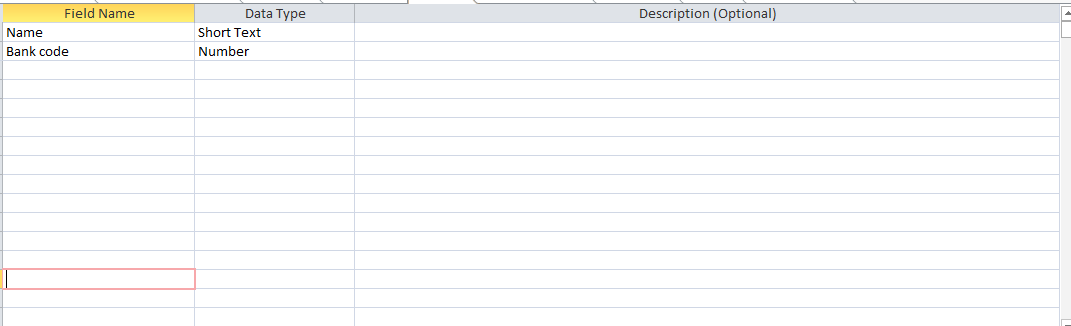


Figure 5.9: Showing Account Table

## 5.3.2 Bank table

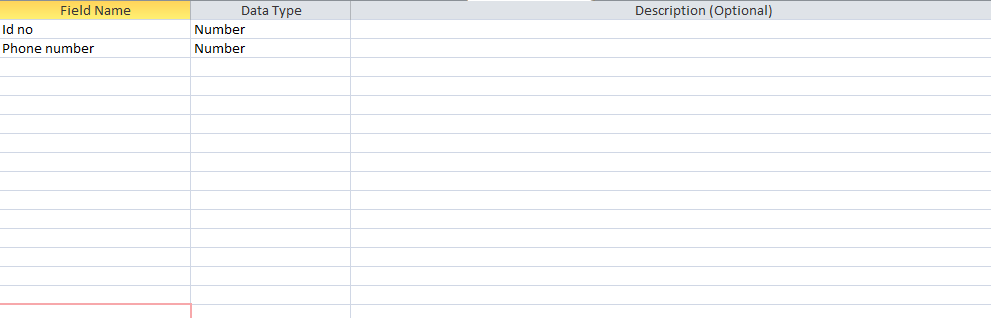
This containsthe bank name and bank code (primary key)

****

## Figure 5.1.0: Showing Bank Table.

## 5.3.3 Bank Attendant table

The bank attendant table includes the name, identification number and phone number.

****

## Figure 5.1.1: Showing Bank Attendant Table

## 5.3.4 Customer Table

The customer table contains the following; customer id, customer name, pin and phone number.

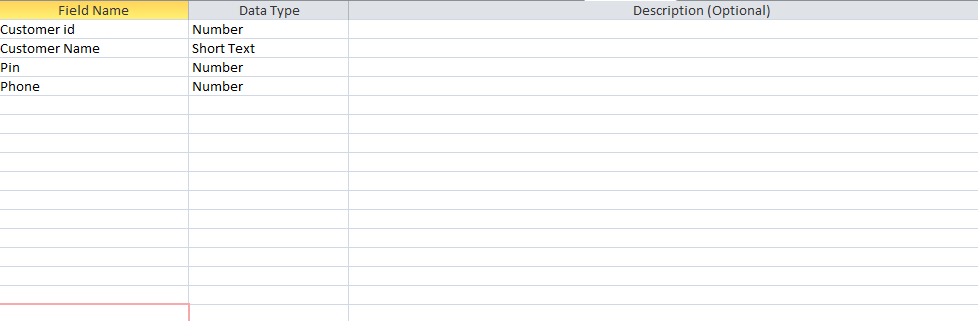
****

Figure 5.1.2: Showing Customer Table.

## 5.3.5 Loan table

This table has loan number as the primary key. Other details include loan type and loan amount.

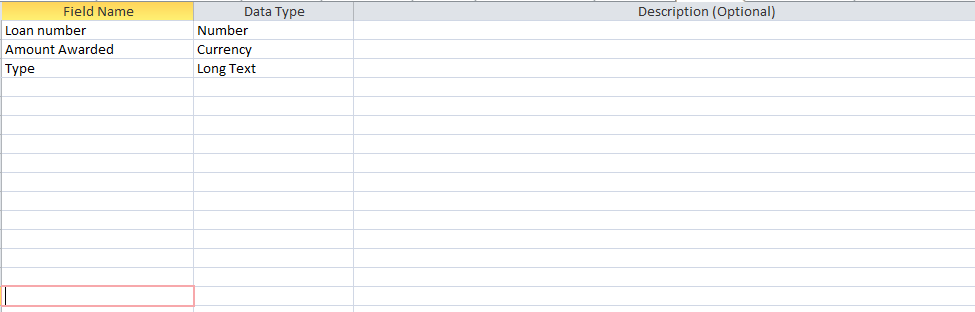
****

Figure 5.1.3: Showing Loan Table

## 5.3.6 Database logical design

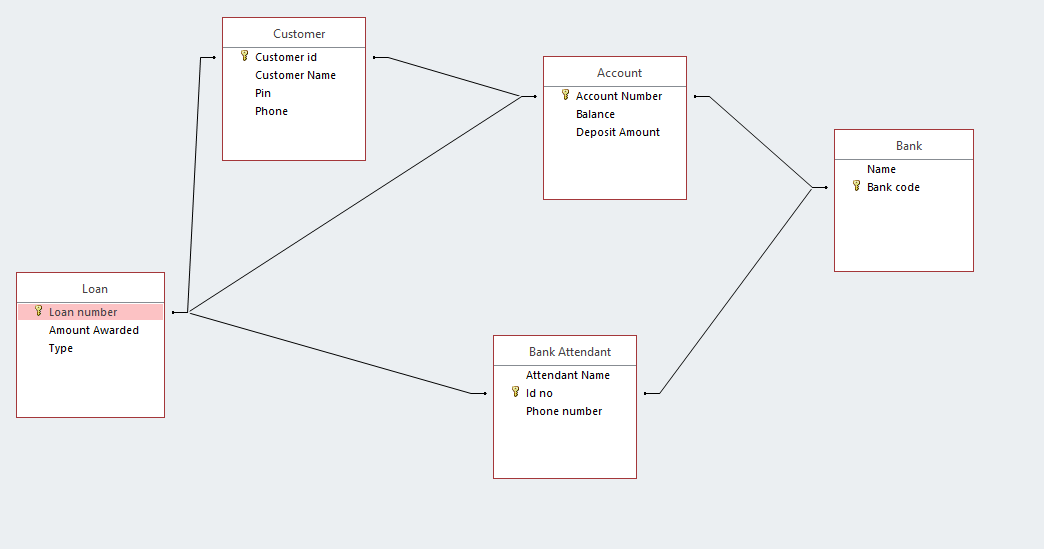


Figure 5.1.4: Showing Database Logical Design.

## 5.4. Summary

This chapter entails logical design of the proposed signature verification banking system. It also entails application pages which helps the user to interact with system more easily. It also entails forms, tables and the relationship diagrams in the database that keeps records of the customer details.

# CHAPTER SIX

# SYSTEM IMPLEMENTATION

## 6.0 Overview

This chapter entails detailed explanation of the developed system. Implemented features have been explained as well as the system testing carried out on various units of the system explained. The system changeover method applied is also explained in this chapter. Documentation of the system is highlighted; both internal and external documentations are briefly explained.

## 6.1 Implemented Features

## 6.1.1 Registration Feature

The registration feature allows the customer to input their full names, National identity number and enter their password twice. The system ensures that the two passwords entered by the customer match and that the password contains a combination of letters, characters and a special character before proceeding to register the customer otherwise the customer would not be registered. The system also ensures that the all the text boxes are filled by the customer in order to complete the registration process. The system does not allow a customer to be registered twice. Figure 6.1 below shows a view of the code syntax of the registration feature.

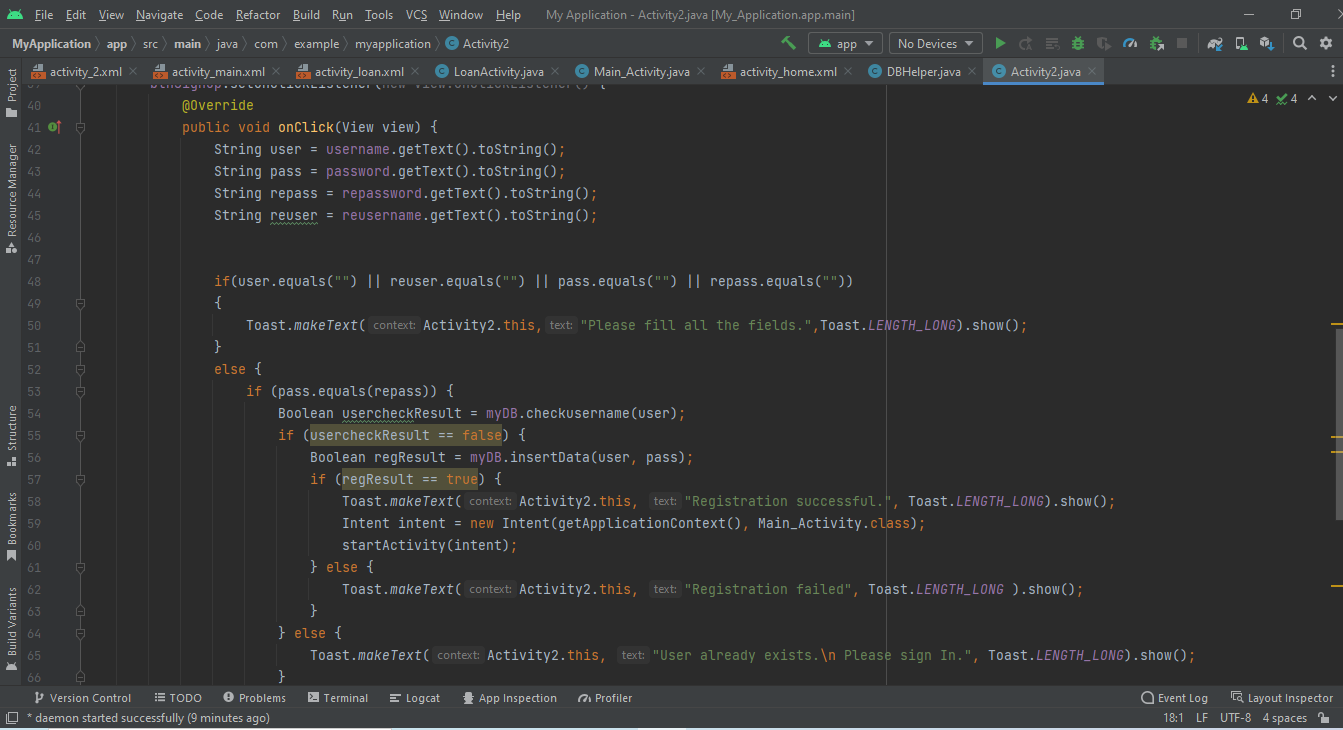


Figure: 6.1 Showing code syntax for registration feature.

## 6.1.2 Customer Login Feature

The login feature allows only already registered customers to login into the system. A user must enter their name and password which are then verified by the system to ensure that the details entered by the customer are the same details stored in the system’s database. The figure below shows the code syntax of the customer login feature.

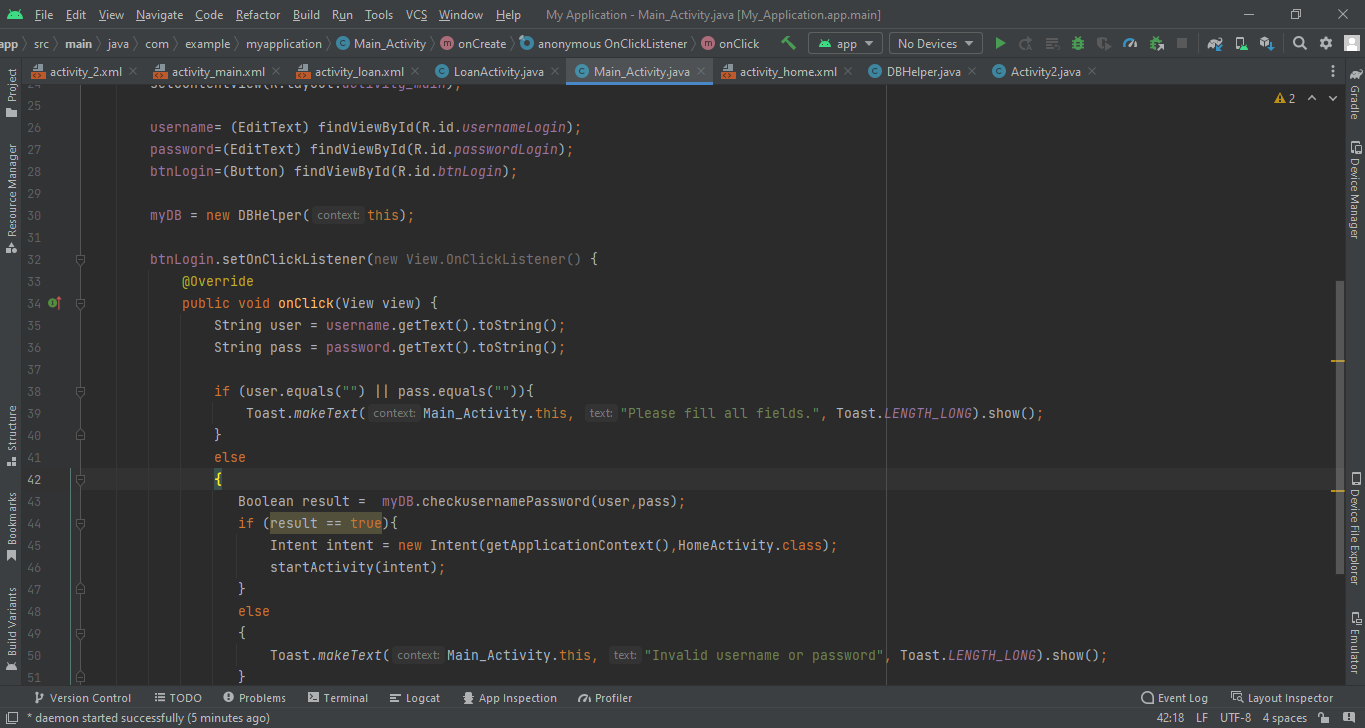


Figure: 6.2 Showing code syntax for customer login feature.

## 6.1.3 Loan Feature

The loan feature outlines the loan types that a customer is eligible for. The types of loan are specified together with the loan amounts and repayment period. The system allows the customer to select the loan amount of their choice and then key in their name and password to verify the loan requested for. Below is the code syntax for the loan feature.

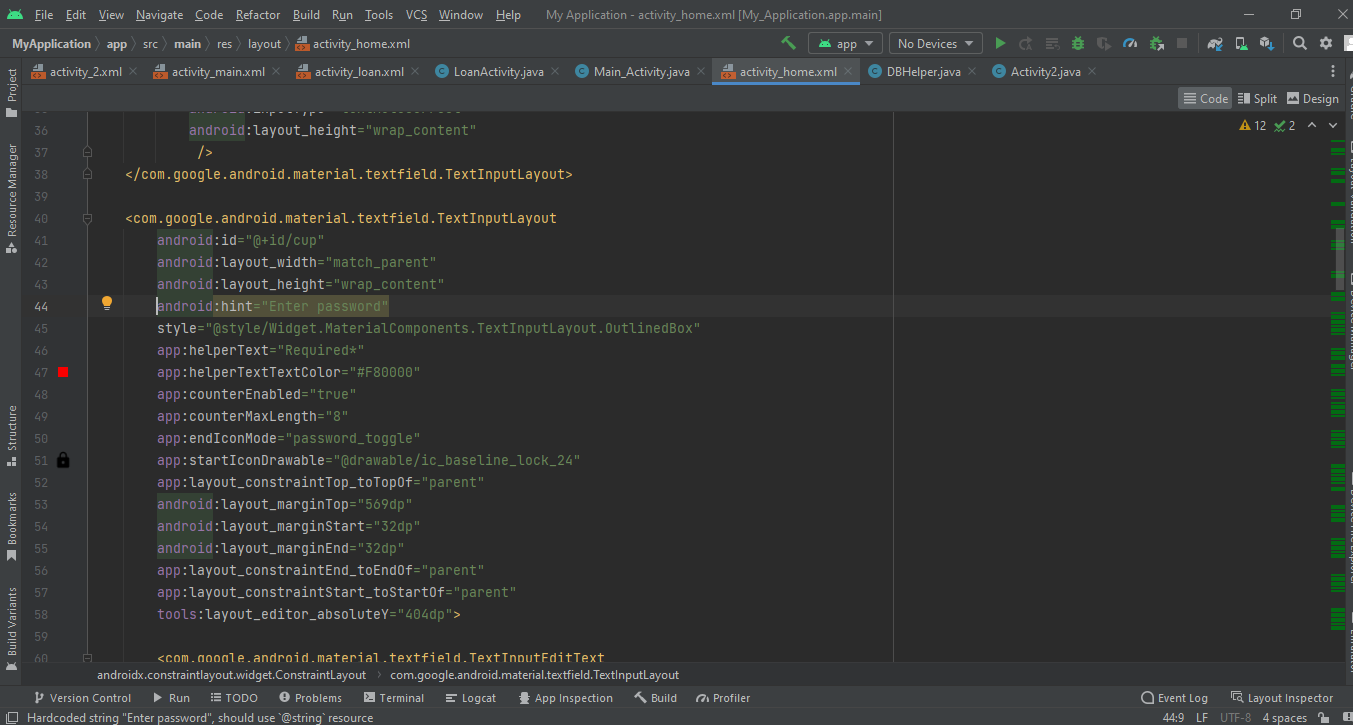


Figure:6.3 Showing code syntax for loan request feature

## 6.1.4 Signature Verification Feature

The signature verification feature allows a customer to insert their signature into the system. After the system recognizes the customers signature, it can then be used to verify the user when applying for the loan. The figure below shows the code syntax for the signature verification feature.

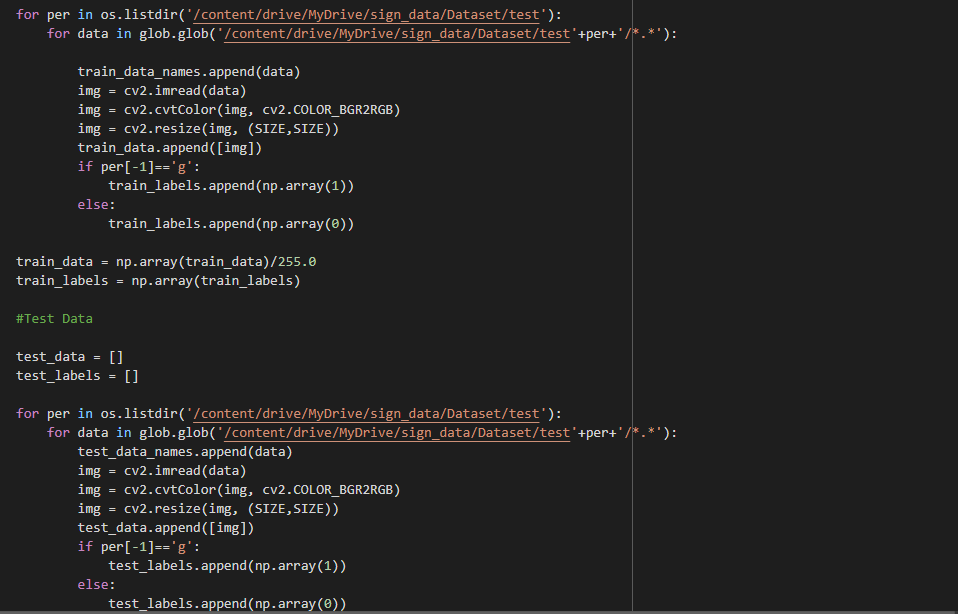


Figure:6.4 code syntax for signature verification feature.

## 6.2 System Testing

According to Rex (2002) system testing refers to testing conducted on a complete integrated system to ensure that the system meets its specified objectives.

System testing is important since it assures the quality of the system developed and satisfies the user needs. The features to be tested and their respective results are highlighted below.

## 6.2.1 Customer Registration

The system should allow a user to register only once into the system. This feature was tested on the system’s ability to allow a user to input their details, submit the data and the system to store the details in the database. The system was also tested to ensure that a customer does not register twice into the system.

Table 6.1 Test results for customer registration feature

|  |  |  |  |
| --- | --- | --- | --- |
| **Test Field** | **Test Data** | **Test Results** |  |
|  |  | **Data validation** | **Data Stored into database** |
| Name | Paul  Laban  Diphlex | Pass | Pass |
| ID Number | 38345689  37895673  39054321 | Pass | Pass |

## 6.2.2 Password verification

The system allows a customer to enter their password twice while registering into the system. The two passwords must match for the customer to be registered into the system. This feature was tested on its ability to function as expected. The table below shows the results.

Table 6.2 Test results for password verification feature

|  |  |  |  |
| --- | --- | --- | --- |
| **Test Data** |  | **Test Type** | **Test Result** |
| **Password 1** | **Password 2** |  |  |
| Brayoo12 | Brayoo12 | Test whether password 1 and password 2 match | Pass |
| Laban13 | Paul123 | Check whether the system registers a user who has entered different passwords. | Pass |

## 

## 6.2.3 Customer login

The system has an interface to allow registered customers to login into the system with their names and passwords already saved in the systems database. This feature was tested to ensure that it functions as expected and data validation.

Table 6.3 Test results for customer login feature

|  |  |  |  |
| --- | --- | --- | --- |
| **Test Data** |  | **Test Type** | **Test Result** |
| **Username** | **Password** |  |  |
| Japheth | 1542 | Test strength of password. Password should be a combination of characters and numbers rather than just numbers | Pass |
| 52445 | Brayoo12 | Test validity of a customer’s username which should be a combination of characters rather than numbers | Pass |

## 6.2.4 Loan Request

The system allows a customer to login and request for a loan. Once a user identifies their desired loan, the customer selects it and enters their username and password to complete the loan request. The system was tested to ensure that it meets this functionality.

Table 6.4 Test results for loan request feature

|  |  |  |  |
| --- | --- | --- | --- |
| **Test Field** | **Test Data** | **Test Results** |  |
|  |  | **Data Validation** | **Data storage into the database** |
| Loan type | Super loan | Pass | Pass |
| Payment Period | 3 years | Pass | Pass |

## 6.3 System Changeover

System changeover refers to the process of transitioning from one system to another, Rex (2002). There are four changeover techniques that can be implemented;

Direct changeover- According to Rex (2002), Direct changeover is where the old system is abandoned and the new system is implemented immediately.

Parallel changeover- This is a changeover method where both the new system and the old system are running side by side while their performance is being compared and after sometime the one that is more optimal is picked and fully adopted Spacey (2017)

Phased changeover- In this changeover technique, on part of the overall system that needs changing is being changed, Spacey (2017)

Pilot Changeover- This involves implementing the complete new system at a selected location of an organization for example in a branch, Gunner (2020)

Parallel changeover was used for this system where the old system and the new system are running concurrently while the performance of both systems are analyzed and compared. After sometime, the analyzed results are checked and the most optimum system between the two is picked.

## 6.4 Documentation

System documentation refers to a write up that provides an overview of the system and helps engineers and stakeholders understand the underlying technology, Altex (2020)

According to Tom (2009) Internal documentation refers to documentation where various parts of the code within the source code operate as comments. The figure below shows the code syntax which entails comments.

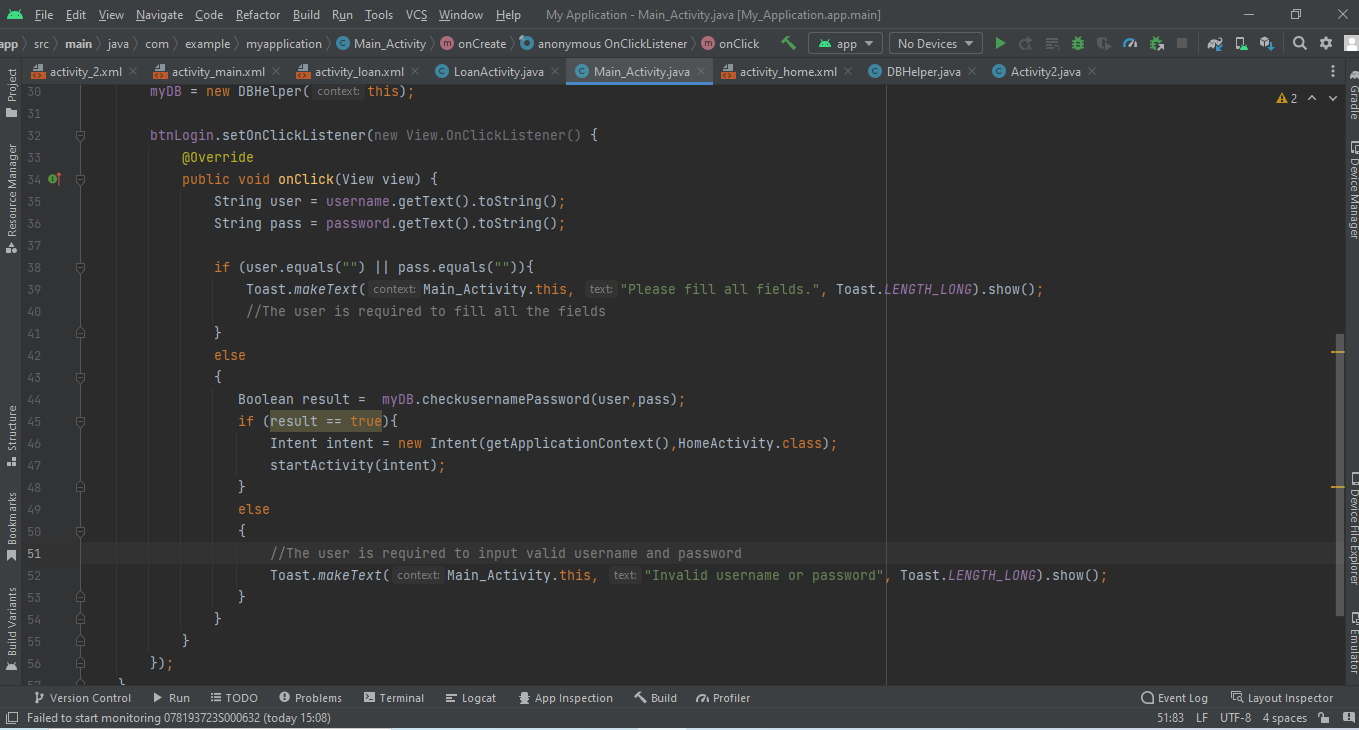


Figure: 6.5 Showing code syntax containing comments.

External documentation consists of user guides and sometimes includes a detailed description of the design and implementation features of the system, Tom (2009). The developer external documentation explains the language used to code, meanings to certain jargon and outlines the code functionalities.

The user external documentation explains to the user how to register into the system, log into the system and request for a loan. It also explains to the user how to troubleshoot the system in case the system fails to login. The user manual is attached as an appendix.

## 6.5 Summary

This chapter entails an explanation of the implemented features, system testing, system changeover and system documentation.

# CHAPTER SEVEN

# FINDINGS, CONCLUSION AND RECOMMENDATIONS.

## 7.0 Findings.

Banks worldwide are striving to provide reliable banking services to their customers. Several banks have reported cases of fraud and money laundering whereby the bank incurs huge losses while money is lost to malicious individuals. This has caused several banks to lose their customers trust to the extent where some banks have to shut due to lack of funds. This in turn has made several banks to invest in its security. Banking systems nowadays have robust systems which are less prone to security breaches.

In response to these challenges, banks are employing stricter measures to curb security breaches. Nowadays banks emphasize on security at the customer’s level where a customer’s interaction with the bank system is guaranteed to be secure. In mobile devices, small input areas and poor ergonomics have caused an increase in the variabilities during the verification and customer sign in processes. Some banks have opted for bank systems that use signature verification to authenticate customers and also bank attendants into its system.

The researchers found out that these signature verified systems were prone to several challenges. These include forgeries of signatures by malicious individuals who may use these forged signatures to maliciously acquire money from legitimate customer’s bank accounts. This could potentially have long term serious consequences on customer loyalty, experience and profitability from core products. It could also cause serious financial crisis on the bank.

The researchers also found out that as banks make improvements on the security of their systems, so too is there an increase in the number of breaches which have proven to be much more fatal compared to security breaches which were reported approximately five years ago. Therefore, the future success of a bank will be decided by its ability to harness emerging technologies in order to deliver great customer experience and improved loyalty while at the same time empowering its employees and improving operational efficiencies. Innovations in the banking fields is a stepping stone for banking systems to transform their operations and business models.

## 7.1 Conclusion

Before introduction of modern computing, signature verification was done manually, whereby a bank attendant would manually check a customer’s signatures and compare it with the customer’s previous signatures. The manual process of signature verification was prone to human errors and forgeries. Nowadays each bank is striving to provide the best customer services by guaranteeing security of customer’s money. The computerized signature verification automates signature verification in the above system thus reducing time wastage, human errors as well as signature forgeries that are brought about by manual signature verification.

To many individuals, automated signature verification seems very expensive and complicated. From the researcher’s point of view computerized signature verification in a bank system has much more advantages compared to manual signature verification. Adding on to this, the computerized signature verification in the bank system is much more secure and less prone to security breaches. If this system is impressed by all banks, customer loyalty and money security will be guaranteed. Therefore, with these several advantages with minimal drawbacks such as additional cost the researchers hope that banks and other financial institutions will adopt this automated signature verification and in turn enjoy its several benefits.

## 7.2 Recommendations

The researchers recommend the following about the system:

* The researchers recommend that the customers and bank attendant and of ROTSE bank be trained on how to use the system
* Other researchers can use this project report as a background for conducting future studies of signature verification in a bank or in any other organization.
* Modifications should be made to the system so as to make it more affordable so as to encourage consumers to using this system.
* Further research on this system needs to be done in order to identify and eliminate some of the weaknesses identified in the bank system.
* There is need for system upgrade as user’s requirements change in order to meet the user’s needs.
* The system must be protected from unauthorized access to avoid misuse and damage of system components.
* While registering into the system, users need to carefully choose their passwords and avoid using their names, year of birth or any other weak passwords so as to secure their accounts.
* More research needs to be done on this field to improve functionality of the system.
* To avoid data loss due to deliberate or accidental errors as well as hardware or software malfunctions, backups should be done frequently

## REFERENCES

1. M. Diaz, A. Fischer, M. A. Ferrer and R. Plamondon,(2018) "Dynamic Signature Verification System Based on One Real Signature," Transactions on Cybernetics, vol. 48, no. 1, pp. 228-239, Jan. 2018, doi: 10.1109/TCYB.2016.2630419.
2. Signature verification MSU-CSE(2013) retrieved from <http://www.cse.msu.edu/~cse802/Papers/802_Signature_Verification>
3. Signature recognition (2022) *Biometrics Research Group* retrieved from <https://www.biometricupdate.com/201601/explainer-signature-recognition>
4. Fierrez-Aguilar, J., Alonso-Hermira, N., Moreno-Marquez, G., & Ortega-Garcia, J. (2004, May). An off-line signature verification system based on fusion of local and global information. In *International workshop on biometric authentication* (pp. 295-306). Springer, Berlin, Heidelberg.
5. Sharif, M., Khan, M. A., Faisal, M., Yasmin, M., & Fernandes, S. L. (2020). A framework for offline signature verification system: Best features selection approach. *Pattern Recognition Letters*, *139*, 50-59.
6. Martinez-Diaz, M., Fierrez, J., Galbally, J., Alonso-Fernandez, F., & Ortega-Garcia, J. (2007, November). Signature verification on handheld devices. In *Proc. MADRINET Workshop, Salamanca, Spain* (pp. 87-95).
7. Batool, F.E., Attique, M., Sharif, M. *et al.* Offline signature verification system: a novel technique of fusion of GLCM and geometric features using SVM. *Multimed Tools Appl* (2020). <https://doi.org/10.1007/s11042-020-08851-4>
8. Yapıcı, M.M., Tekerek, A. & Topaloğlu, N. Deep learning-based data augmentation method and signature verification system for offline handwritten signature. *Pattern Anal Applic* **24**, 165–179 (2021). <https://doi.org/10.1007/s10044-020-00912-6>
9. Collin, E.M. (2020). Easy earned money.com”Data collection: The complete guide”
10. Youssef Bassil- arXiv preprint arXiv : 1205.6904,2012-arXiv.org
11. Hamed Taherdoost. How to choose a sampling technique for research (April 10,2016),2016
12. ML Abbott, J Mckinney-2013-books.goggle.com
13. Visual Paradigm Community Circle.(2021,April 22).In Wikipedia.https://en.m.wikipedia.org/wiki/Use\_case\_diagram.
14. Class diagrams. (2009,Dec). In Wikipedia.https://en.m.wikipedia.org/wiki/Class\_diagram#:~:text=In%20software%20engineering%2C%20a%20class,and%20the%20relationships%20among%20objects.
15. Unified modelling language (2011) . In Wikipedia. https://en.m.wikipedia.org/wiki/Sequence\_diagram#:~:text=A%20sequence%20diagram%20or%20system,to%20carry%20out%20the%20functionality.
16. Data flow diagram (1990). In Wikipedia. https://en.m.wikipedia.org/wiki/Data-flow\_diagram#:~:text=A%20data%2Dflow%20diagram%20is,decision%20rules%20and%20no%20loops.
17. J. Rumbaugh, I. Jacobson, and G. Booch. The Unified Modeling Language Reference Manual. Addison-Wesley, 1999.
18. Kat Boogaard. What you need to know about requirements gathering,2022.
19. Fulton R, Vandermolen R (2017). "Chapter 4: Requirements - Writing Requirements". Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254. CRC Press. pp. 89–93. ISBN 9781351831420. Retrieved 15 June 2018.
20. Requirements Engineering A good practice guide, Ramos Rowel and Kurts Alfeche, John Wiley and Sons, 1997.
21. Barry Buzan, Ole Waever, and Jaap de Wilde,Security: A new Framework for analysis (Boulder: Lynne Rienner publishers,1998)
22. Black, Rex (2002). *Managing the Testing Process* (2nd ed.). Wiley Publishing
23. 2. John, spacey (2017) five examples of direct changeover
24. 3. Gunner (2020) pilot changeover, the pilot changeover method involves. University of phoenix.
25. 4. Altex (2020) technical documentation in software development: types, best practices and tools
26. 5. Tom (2009) internal documentation. em.m.wikipedia.org/wiki/ internal documentation

|  |
| --- |
| **BANKING INFORMATION QUESTIONNAIRE** |
| BANK ATTENDANT |
| 1. What is the process of verifying a customer? 2. How does a customer open up an account?      1. What is the procedure or a customer to apply or a loan? 2. How are monthly loan records generated? |
| CUSTOMER |
| 1. Do you have an account? If yes, what was the opening procedure?   …………………………………………………………………………………………………………………………………………………………………………………………………………………………..   1. Have you ever acquired a loan? If yes, what was the procedure?   …………………………………………………………………………………………………………………………………………………………………………………………………………….   1. Have you ever had issues with your account?   ……………………………………………………………………………………………………………………………………………………………………………………………………………………………….. |

**Appendix 1: Questionnaire**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Activities | WK1 | WK2 | WK3 | WK4 | WK5 | WK6 | WK7 | WK8 | WK9 | WK10 | WK11 | WK12 | WK13 |
| Title identification |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Reading background study |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Problem formulation |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Coining the objectives |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Writing Chapter One |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Writing Chapter  Two and Three |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Writing Chapter  Four and Five |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Writing Chapter  Six and Seven |  |  |  |  |  |  |  |  |  |  |  |  |  |

**Appendix 2: Budget**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Items** | **Description** | **Unit Cost**  **(ksh)** | **Quantity** | **Total cost** |
| **Documentation and Literature** |  |  |  |  |
| Internet services | Telcom bundles | 400 | 4 | 1600 |
| Printing, Scanning, Photocopying and Binding | Each chapter | 70 | 14 | 1500 |
| Air Time | Safaricom Airtime | 200 | 5 | 1000 |
| **Data Collection** |  |  |  |  |
| Data collection | Distribution of Questionnaires | 50 | 10 | 500 |
| **Implementation** |  |  |  |  |
| Software requirements | Android Studio  Anaconda | 0 | 0 | 0 |
| **Total** |  |  |  | 4600 |

**Appendix 3: Budget**