JOMO KENYATTA UNIVERSITY

OF

AGRICULTURE AND TECHNOLOGY

College of Pure and applied Sciences

School of Computing and Information Technology

Department of Information Technology

**IMPLEMENTING BIOMETRICS FOR AN ONLINE SACCO SYSTEM**

RICHARD FELIX ODHIAMBO

SCT222-0164/2018

Project Proposal Submitted to the School of Computing and Information Technology in Partial fulfillment of the Requirements for the award of the Bachelor of Science in Business Computing of Jomo Kenyatta University of Agriculture and Technology.

JULY, 2022

## DECLARATION

This research is my original work in partial fulfillment of Bachelor of Science in Business Computing and has not been presented or submitted to any institution.

Richard Felix Odhiambo

……………………………… ………………………..

Signature Date

This proposal has been submitted for examination with my approval as university supervisor

Dr. Dennis Kaburu

……………………………… ………………………..

Signature Date

## ACKNOWLEDGEMENT

I am over whelmed in all humbleness and gratefulness to acknowledge all those who have helped me to put these ideas, well above the level of simplicity and into something concrete. I would like to express my special thanks of gratitude to my Supervisor Dr. Dennis Kaburu for his time, support and dedication in guiding me during the whole process.

Any attempt at any level can 't be satisfactorily completed without the support and guidance of my parents and friends. I would like to thank UNITED AMANI SACCO Staff and members who helped me a lot in gathering diﬀerent information, collecting data and guiding me from time to time in making this project, despite of their busy schedules, they gave me diﬀerent ideas in making this project unique.

## DEDICATION

I dedicate this work to United Amani Sacco members who have supported and encouraged me all the way.

I also dedicate this to my parents for their loyal and everlasting support.

## ABSTRACT

The proposed system is to be implemented to UNITED AMANI SACCO. In this establishment, the Sacco members had to go to the physical location to get statements of their monthly contributions, loan details and recent transactions. The objective of the system is to enable members to use an online website to log in and get all these information securely from hackers. The system will target the over 500 members of the Sacco. Data collection was done through interviews of various members concerning the ease and convenience of getting their information. After analysis, findings show all members preferred a more convenient way of getting their information provided it the security of it was assured.

Justification of a proper web-based system is that ensuring security of member information will guarantee more users and boost confidence of using these systems.

Agile methodology will be used during the entire process to continuously test while developing the system.

TABLE OF CONTENTS

Contents

[DECLARATION I](#_Toc101945826)

[ACKNOWLEDGEMENT II](#_Toc101945827)

[DEDICATION III](#_Toc101945828)

[ABSTRACT IV](#_Toc101945829)

[CHAPTER ONE 1](#_Toc101945830)

[INTRODUCTION 1](#_Toc101945831)

[1.1 BACKGROUND INFORMATION 1](#_Toc101945832)

[1.2 INTRODUCTION TO AREA OF RESEARCH 1](#_Toc101945833)

[1.3 PROBLEM STATEMENT 2](#_Toc101945834)

[1.4 PROPOSED SOLUTION 2](#_Toc101945835)

[1.5 OBJECTIVES 2](#_Toc101945836)

[1.5.1 GENERAL OBJECTIVES 2](#_Toc101945837)

[1.5.2 SPECIFIC OBJECTIVES 2](#_Toc101945838)

[1.6 RESEARCH QUESTIONS 3](#_Toc101945839)

[1.7 JUSTIFICATION 3](#_Toc101945840)

[1.8 SCOPE OF STUDY 3](#_Toc101945841)

[1.9 SYSTEM METHODOLOGY 3](#_Toc101945842)

[PROJECT REQUIREMENTS 4](#_Toc101945843)

[GANTT CHART 7](#_Toc101945844)

[CHAPTER 2 8](#_Toc101945845)

[LITERATURE REVIEW 8](#_Toc101945846)

[2.1 INTRODUCTION 8](#_Toc101945847)

[2.2 CONCEPTUAL FRAMEWORK 11](#_Toc101945848)

[2.3 CRITIQUE 12](#_Toc101945849)

[2.4 SUMMARY 12](#_Toc101945850)

[CHAPTER 3 13](#_Toc101945851)

[SYSTEM ANALYSIS AND DESIGN 13](#_Toc101945852)

[3.1 INTRODUCTION 13](#_Toc101945853)

[3.2 SYSTEM DEVELOPMENT METHODOLOGY 13](#_Toc101945854)

[3.3 FEASIBILITY STUDY 14](#_Toc101945855)

[3.4 REQUIREMENTS ELICITATION 15](#_Toc101945856)

[3.5 DATA ANALYSIS 17](#_Toc101945857)

[3.6 SYSTEM SPECIFICATIONS 19](#_Toc101945858)

[3.7 ANALYSIS MODEL (PHYSICAL AND LOGICAL DESIGN) 21](#_Toc101945859)

[ER-DIAGRAM 25](#_Toc101945860)

[CHAPTER 4 30](#_Toc101945861)

[SYSTEM ANALYSIS, DESIGN AND IMPLEMENTATION 30](#_Toc101945862)

[4.1 INTRODUCTION 30](#_Toc101945863)

[4.2 SYSTEM CODE GENERATION 30](#_Toc101945864)

[4.3 SYSTEM SCREENSHOTS 39](#_Toc101945865)

[4.4 TESTING 41](#_Toc101945866)

[4.5 LIMITATIONS 42](#_Toc101945867)

[4.6 CONCLUSION 43](#_Toc101945868)

[4.7 RECOMMENDATION 43](#_Toc101945869)

[4.8 REFERENCES 43](#_Toc101945870)

[*Bibliography* 43](#_Toc101945871)

LIST OF TABLES

[Table 1 Budget 5](#_Toc88160584)

[Table 2 Schedule 6](#_Toc88160585)

LIST OF FIGURES

[Figure 1 SDLC lifecycle 4](#_Toc101865311)

[Figure 1.2 Gantt Chart 7](#_Toc101865312)

[Figure 3 User Authentication Algorithm 9](#_Toc101865313)

[Figure 4 User Authorization Algorithm 10](#_Toc101865314)

[Figure 5 Data Access Algorithm 11](#_Toc101865315)

[Figure 6 Agile Methodology 14](#_Toc101865316)

[Figure 7 Members who would use the new system 18](#_Toc101865317)

[Figure 8 Members with smart devices 19](#_Toc101865318)

[Figure 9 Members who have been victims of fraud 19](#_Toc101865319)

[Figure 10 Data flow diagram 22](#_Toc101865320)

[Figure 11 Use Case Diagram 23](#_Toc101865321)

[Figure 12 Activity Diagram 24](#_Toc101865322)

[Figure 13 Sequence Diagram 25](#_Toc101865323)

[Figure 14 Member login page 39](#_Toc101865324)

[Figure 15 Fund transfer 39](#_Toc101865325)

[Figure 16 User dashboard 40](#_Toc101865326)

[Figure 17 Registering new members(staff) 40](#_Toc101865327)

LIST OF ABBREVIATION

SSL Secure Sockets Layer

TLS Transport Layer Security

SEDK symmetric encryption/decryption key

SSH Secure Shell

DEFINATION OF TERMS

Doxing: act of revealing identifying information about someone online, such as their real name, home address, workplace, phone, financial, and other personal information.

Broken access control: vulnerabilities that exist when a user can in fact access some resource or perform some action that they are not supposed to be able to access.

Cryptographic Failures: includes not using encryption at all

SQL injection: attack that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed.

Insecure design: designing a system without security in mind.

Security Misconfiguration: security controls that are inaccurately configured or left insecure, putting your systems and data at risk.

Server-Side Request Forgery: type of exploit where an attacker abuses the functionality of a server causing it to access or manipulate information in the realm of that server that would otherwise not be directly accessible to the attacker.

# CHAPTER ONE

## INTRODUCTION

## 1.1 BACKGROUND INFORMATION

With the current technology, there has been very many ways of being online. But with all these ways, new concerns of online security come to light. One common way of being online is by the use of websites where users can log in to social platforms or even in banking platforms where their sensitive information is at risk

UNITED AMANI SACCO is a Sacco located in Nakuru that offers banking services. They recently sought services for the creation of their website mainly for displaying their information to aspiring new members. Analytics showed that not many people visited the website despite the Sacco boasting over 500 members. It was noticed that members were uncomfortable always calling or visiting the premises to get information about their sensitive account information.

Banking and digital money lending services require secure online platforms that can enable users to log in to get all their information. UNITED AMANI SACCO has gained some members that need such services while they are assured of their personal data security.

## 1.2 INTRODUCTION TO AREA OF RESEARCH

The research area of this project focuses on the use of various current technologies to secure information of the members. According to OWASP (Open Web Application Security Project), as of 2021, the top 10 web application security risks hackers have used are:

Broken access control, Cryptographic Failures, SQL injection, Insecure design, Security Misconfiguration, Vulnerable and Outdated Components, Identification and Authentication Failures, Software and Data Integrity Failures, Security Logging and Monitoring Failures, Server-Side Request Forgery.

In light of all these security risks that are being exploited, new technologies have also been put in place to safeguard current systems. Such technologies include SSL/TLS Encryption, Phone number and Email verification, digital certificates, IP blockers, Two factor authentication and also SSH keys for file transfer.

## 1.3 PROBLEM STATEMENT

UNITED AMANI SACCO is using a system way of providing members with their information where a member has to make a formal request by calling, emailing, messaging or going physically to the premises. The staff who send this information get access to information that should be private. Impersonation occurs when relatives of the member or unknown people call the premises and ask for this information since the staff do not have a proper way of verifying the members. Some members who leave far or moved to other places are inconvenienced when they need to go to the premises to get their information. During evenings and holidays, the staff members are not around to send the information to all those who require it.

There is clearly a need to tackle these problems for the members to enjoy while reassuring them of the highest level of security of their information.

## 1.4 PROPOSED SOLUTION

From the problems stated, adoption of an online web-based system will be able to solve them. The members will be able to login, transact, view loan details, view recent transactions and buy monthly statements. The system will be able to prevent all the top 10 web security attacks while providing members with the platform to retrieve their information.

## 1.5 OBJECTIVES

### 1.5.1 GENERAL OBJECTIVES

To develop a fully functional online hosted website that will allow sacco members to access their information in a very secure manner conveniently.

### 1.5.2 SPECIFIC OBJECTIVES

1. To collect data from members about what information they prefer to access on an online platform and the way they would like it presented to them.
2. To analyze all the collected data extensively to determine how the next approach will be.
3. To research the methods used by hackers to cause web security vulnerabilities and how these security issues can be solved
4. To design a system that can display all relevant information to the right members at any part of the world
5. To design a system that solve all the top 10 security issues and all others.
6. To test the designed system and ensure it solves all the addressed security issues.
7. To implement the system for the members to use.

## 1.6 RESEARCH QUESTIONS

1. How can information being sent to and from a website be encrypted and secured?
2. How can various methods of online security threats be detected and protected against?
3. How can members access information relevant to them through internet?
4. How can the gaps in security be exploited?
5. How can the gaps in security be addressed by this system?

## 1.7 JUSTIFICATION

Many modern banking services and Saccos provide portals for members to gain access to their data with security in mind and hence UAS need to keep up with the technologies in place to provide such services.

The system will enable members to save on time and costs of travelling to the premises. It will also ensure they can get access to their information at any time they require it. The system will also eliminate impersonation of members.

The system will ensure security of all information hence giving members a peace of mind.

## 1.8 SCOPE OF STUDY

This is a web-based system that will enable Sacco Members to login and access their information securely. The system will provide a secure platform for members to access their relevant information securely from anywhere on the globe.

## 1.9 SYSTEM METHODOLOGY

I will use Agile Methodology in the development of this system. Agile Methodology will promote continuous iteration of development and testing throughout the software development lifecycle of the project. The Agile methodology is a way to manage a project by breaking it up into several phases. It involves constant collaboration with stakeholders and continuous improvement at every stage hence will allow the development of the system while consulting with the members.

The system development will follow this Software Development Life Cycle:

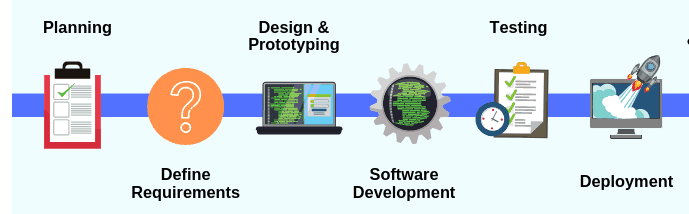


Figure 1 SDLC lifecycle

### PROJECT REQUIREMENTS

Hardware Requirements

1. A personal computer with the following minimum specifications
   1. 2.5 GHz processing speed
   2. 4 GB RAM
   3. 500 GB Hard disk space
2. Wifi Adapter

Software Requirement

1. Browser most preferably Chrome
2. Sublime text

Other requirements

1. A website domain: <http://www.unitedamanisacco.com/>
2. A web-hosting service: Truehost

#### BUDGET

Table 1.1 Budget

|  |  |  |
| --- | --- | --- |
| ITEMS | QUANTITY | AMOUNT(KSH) |
| DOMAIN | 1 | 1000 |
| HOSTING SERVICES | 1 | 1500 |
| Internet |  | 3000 |
| TOTAL |  | 5500 |

#### SCHEDULE

Table 1.2 Schedule

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ACTIVITY |  | DURATION  (WEEKS) | EXPECTED  STARTING  MONTH | EXPECTED  ENDING  MONTH | DELIVARABLES |
| Project Identification |  | 4 | June | June | Problem statement |
| Proposal Writing |  | 8 | June | July | Research proposal document |
| Data Collection |  | 2 | - | - | Raw data |
| Data  Analysis |  | 1 | - | - | Organized data |
| System Design |  | 1 | - | - |  |
| System Coding |  | 3 | - | - |  |
| System Testing |  | 2 | - | - | Working system |
| System  Implementation |  | 1 | - | - | Working online system |
| Final documentation |  | 2 | - | - | Project report |

### GANTT CHART

Figure 1.2 Gantt Chart

# CHAPTER 2

## LITERATURE REVIEW

## 2.1 INTRODUCTION

Until now the web continues to grow both in terms of the number of users and in terms of the technology used. Along with that there has also been an increase in attacks on the web. The attacks on the web cannot be separated from the vulnerabilities that exist on the web. Therefore, we need to look for any vulnerabilities that exist on the web. To make a web-based information system eﬃcient, the access to its re-sources of diﬀerent users will be matched with their pre-assigned rights. Also, different rights are assigned to authorized persons in the information systems intended for updating and modiﬁcation of separate parts of the information stored.

Dimitar Pilev (Pilev, 2014) came up with the following summarized details from his research for web-based information system security: Provision of the application security is of particular importance for the web-based information systems. For this, mechanisms will be used for providing each one of the three security levels which every information system should have – user authentication, user authorization and data access (Burtescu, 2006).

**User Authentication**

A user name, a password and a customer certificate are entered as input data into the user authentication algorithm. Before being processed, the data sent to the system undergo filtering. Filtering is essential in curbing SQL injections (Dougherty, 2012).Only data which format is in compliance with the system requirements are processed in this way. The following algorithm was proposed for User Authentication

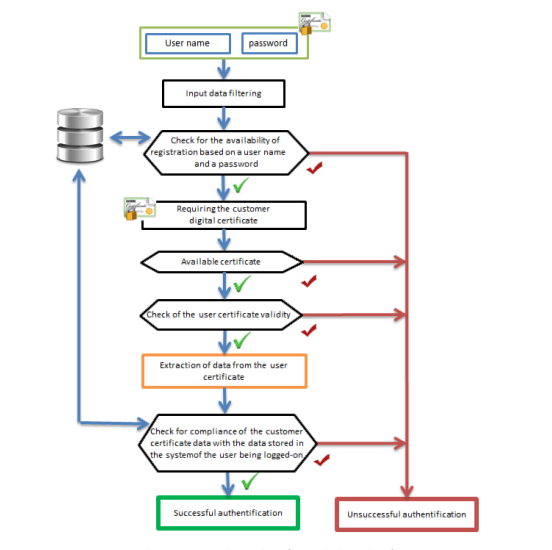


Figure 3 User Authentication Algorithm

**User Authorization**

From journal titled “Issues and Challenges in Web Service”, (S. Tanwar, 2012) it described that one of the issues about web service implementation is un-authorized access.

Each request sent by a user being logged-on to the system is processed by the authorization algorithm. The check for access rights granted takes into consideration the information stored in the database, as well as the information from the user session. The requests sent to the IS are filtered so as to provide system protection against attacks on the part of users authenticated successfully.

The following algorithm was proposed for User Authorization:

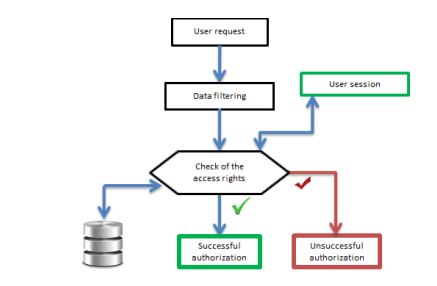


Figure 4 User Authorization Algorithm

**Data Access**

Only successfully authenticated and authorized users should be able to gain the relevant information to them. In doing so, records or logs should be but in place to show the operations executed by each individual user especially in a system with more than one administrators for easier accountability.

The following algorithm was proposed for Granting data access:

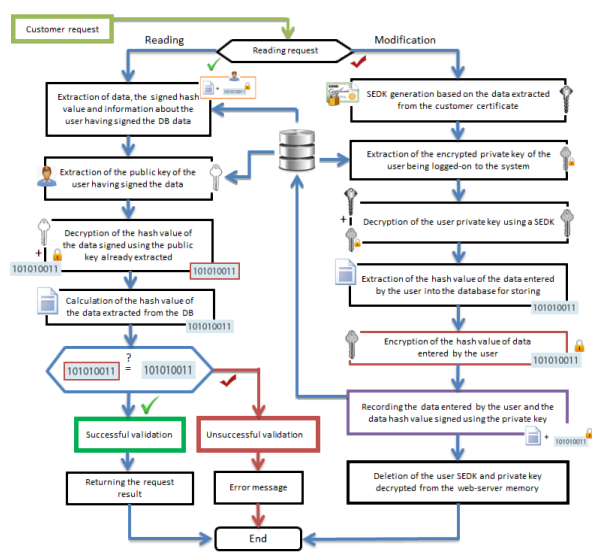


Figure 5 Data Access Algorithm

## 2.2 CONCEPTUAL FRAMEWORK

Lack of proper security measures in a web-based system will lead to various forms of attacks or vulnerabilities on a system. When attacks happen or vulnerabilities are exploited, sensitive data and information will be lost or revealed to the wrong people for exploitation. Security is a must for any online system to protect member information and privacy.

## 2.3 CRITIQUE

This existing system of making calls or going to the organization’s premise physically to get your information is unviable for this current age of technology. The current issues faced are involved are

Lack of confidentiality: any staff member currently at the premises is the one to print out or send your information. In doing this, any staff member can view your information.

Impersonation: as it has happened before, some relatives of the Member call the make calls through the member’s phone and ask for the information. Since the staff can not recognize the voices or even know every member, they end up sending sensitive information

Unavailability of staff: during holidays and at night, the staff are not present to receive calls from members

Time wasting: calling or going to the premises are very time consuming.

## 2.4 SUMMARY

The proposed web-based system will solve the above issues as well as taking the Sacco to the current standards of technology. Every member will be authenticated and get access to the correct data that they should view while the security of this information is heavily adhered to. This will enable members to use public Wi-Fi to retrieve their information without the risk of the data being compromised.

# CHAPTER 3

## SYSTEM ANALYSIS AND DESIGN

### 3.1 INTRODUCTION

### 3.2 SYSTEM DEVELOPMENT METHODOLOGY

#### 3.2.1 AGILE METHODOLOGY

Agile methodology starts by defining the users and documenting a vision statement on a scope of problems, opportunities, and values to be addressed. This methodology entails constant collaboration with users and continuous improvement at every stage. With this methodology, user acceptance can be tested at every stage to ensure that the system meets all the requirements

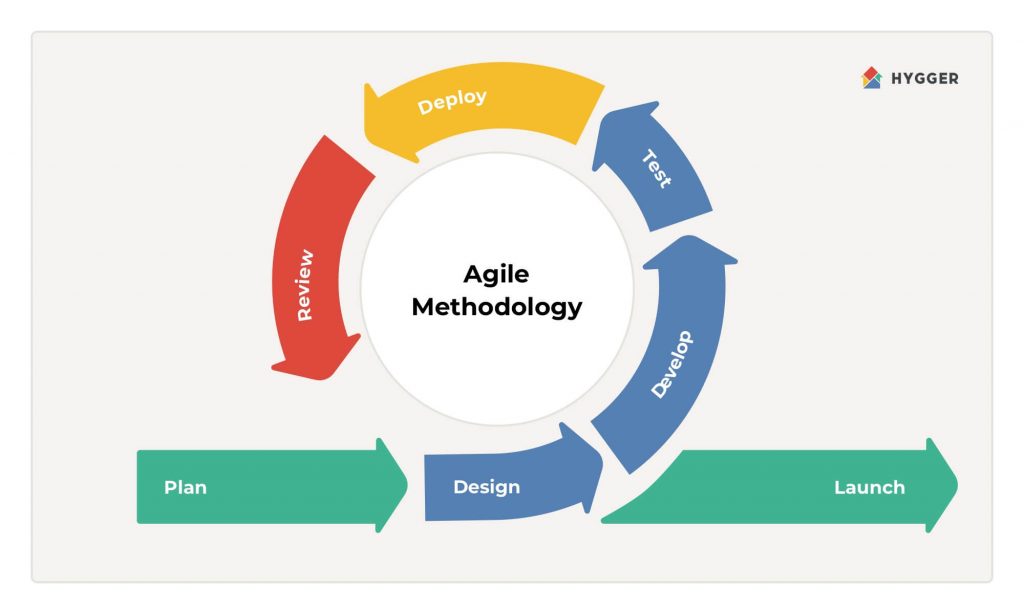


Figure 6 Agile Methodology

Plan: The planning involves performing the feasibility study to determine cost and resources required for implementing the analyzed requirements.

Design: in this phase, all the requirements and details of the overall application are outlined. They are outlined alongside specific aspects such as how the user and system interfaces will be, all the network requirements and also which type of databases will be used.

Develop: from the design, the system will be coded and built so that it will cover all the specifications that were formulated as well as according to the design that was agreed upon.

Test: The developed system can now be tested to ensure that no issues arise during its execution and the errors that are observed can be mended. The system should also be tested to ensure that it meets the quality of the standards that were laid on during the design stage

Deploy: In this phase, the system will be made available for use by the users.

### 3.3 FEASIBILITY STUDY

Feasibility study is an analysis that considers all of a project's relevant factors to determine the viability of the project. This study is mainly performed to ascertain whether a project can be performed depending on the available resources. With this study, we can determine whether the system and the project are worthwhile for the business while considering several factors that affect the business

These factors include operational, economic, technical and schedule factors or studies.

#### 3.3.1 Operational feasibility

Operational Feasibility involves measuring how well a proposed system solves the stated problems. It also examines how the requirements that were stated are satisfied by the system

In order to perform a comprehensive feasibility study, questions that can be used include:

1. Will the system perform all the requirements stated?
2. Will the system secure the user from fraud and any other attacks?

#### 3.3.2 Technical Feasibility

This study entails looking at the current technical resources and equipment available. This project does not require heavy or a lot of hardware and software requirements for its development hence showing that it is feasible in technical aspect.

Some questions that can be used to ascertain the current level of technical resources include:

1. Does the current equipment available support the system?
2. Is the software licensed and available for use?

#### 3.3.3 Economic Feasibility

Economic feasibility involves looking into the cost of resources which include financial resources that will be required in the development of the project. From the hardware and software requirements, the price comes up to 5500 Kenya shillings shows that this project is economically feasible.

The questions used to determine its economic feasibility include:

1. Will the system be cost effective?
2. What is the total expected cost?

### 3.4 REQUIREMENTS ELICITATION

This refers to the process of collecting the requirements of the system from all concerned parties. The data collection techniques used in this entire process are:

#### 3.4.1 Interviews

I was able to interview the staff and some members of the Sacco. I took survey of the members on the issues they encounter when trying to gain access to their data. I also interviewed the staff on the process of registering new members and on their knowledge of storing data to databases as opposed to excel files.

The questions that the members were asked include:

1. Have you ever been a victim of fraud on banking systems?
2. Do you require your Sacco information past working hours?
3. Would you like to perform your banking operations without human intervention?
4. Would you like to use a system to perform all your operations at the comfort of your home?
5. Do you currently own a smartphone or a smart device that can access the internet?

The questions that the staff members were asked include:

1. Will enabling the members to perform their operations reduce the queue time at the organization?
2. Do you have experience of using databases as opposed to excel sheets?

### 3.5 DATA ANALYSIS

Pie chart

Figure 7 Members who would use the new system

Column graph

Figure 8 Members with smart devices

Bar graph

Figure 9 Members who have been victims of fraud

### 3.6 SYSTEM SPECIFICATIONS

#### 3.6.1 Functional requirements

Functional requirements define the functions that must be implemented so that users can be able to use the system to accomplish their tasks. Some functional requirements that should be met include:

Users

1. The system should enable members to login and access their information
2. The system should enable members to pay their monthly contribution
3. Users should be able to buy their monthly statements
4. Users should be able to deposit and withdraw money
5. Users should be able to transfer funds to other accounts
6. Users should be able to view their beneficiaries
7. Users should be able to apply for loans
8. The system should be able to check the eligibility of each member for a loan and the maximum amount they can be given
9. The system should notify a user about late payments

Staff

1. The system should enable the staff to verify new members after the required information is provided by them
2. The staff should be able to deposit, withdraw or transfer funds for the users
3. The staff should be able to resolve issues that may arise on the system on the user’s side

Admin

1. The system should enable the admin to view the logs of all operations performed by the staff or the users
2. The admin should be able to gain access to the backend of the system to perform more complex operations
3. Create staff accounts

3.6.2 Non-functional requirements

These requirements define how a system should perform.

1. Security: The system is centered around the security of the users. The security features that will be implemented include
   1. Encrypting of the data
   2. Keeping records of attempted and failed logins to determine any risk of an account
   3. Keeping logs of all activities performed by the users
   4. Authentication and authorization of users
   5. Biometric verification of users
   6. Phone number verification
2. Performance: the system should perform all its operation efficiently in terms of speed and time.
3. Availability: The system should always be available at any time of day.
4. Usability: the system should be easy to use for any member without the need for extensive training or much effort from the user.
5. Accuracy: the system should perform the biometric verification to the highest accuracy to completely limit the number of frauds.

### 3.7 ANALYSIS MODEL (PHYSICAL AND LOGICAL DESIGN)

#### 3.7.1 Data flow diagram

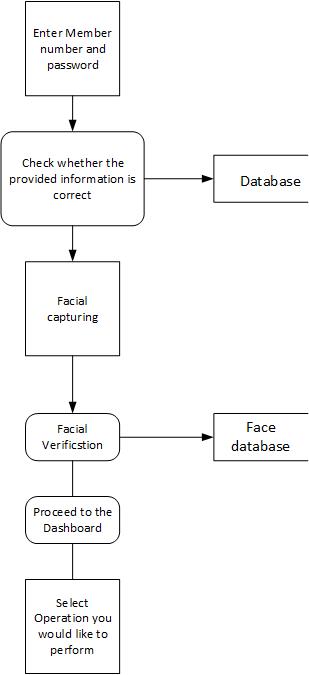


Figure 10 Data flow diagram

#### 3.7.2 Logical design

Use case diagram

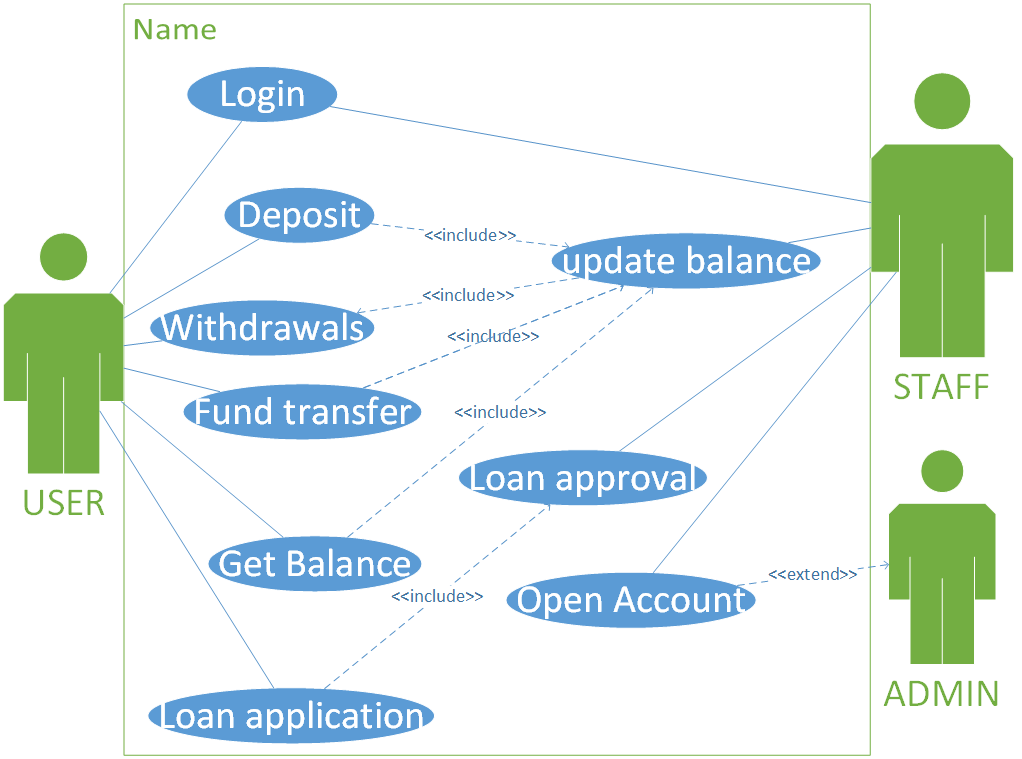


Figure 11 Use Case Diagram

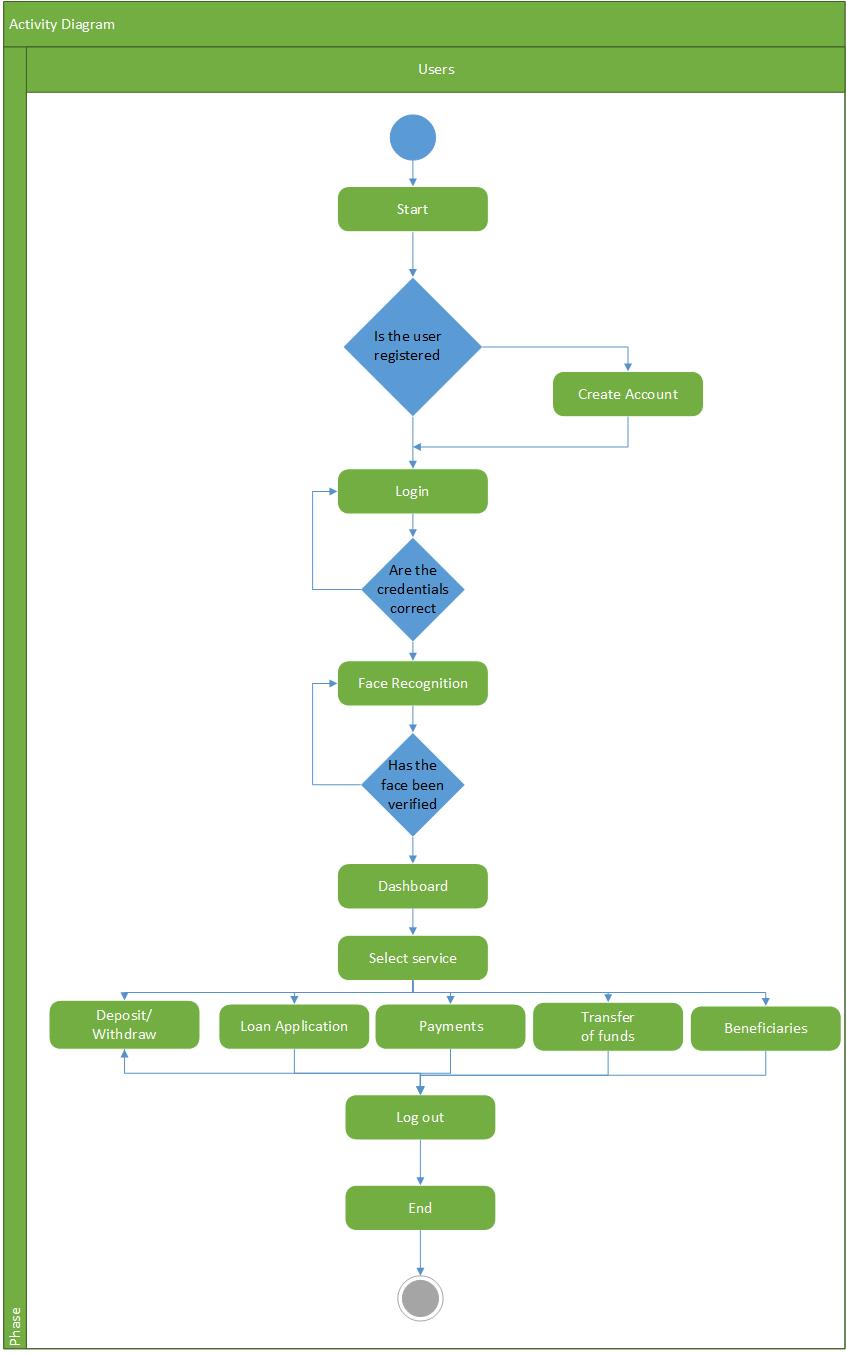


Figure 12 Activity Diagram

Sequence Diagram

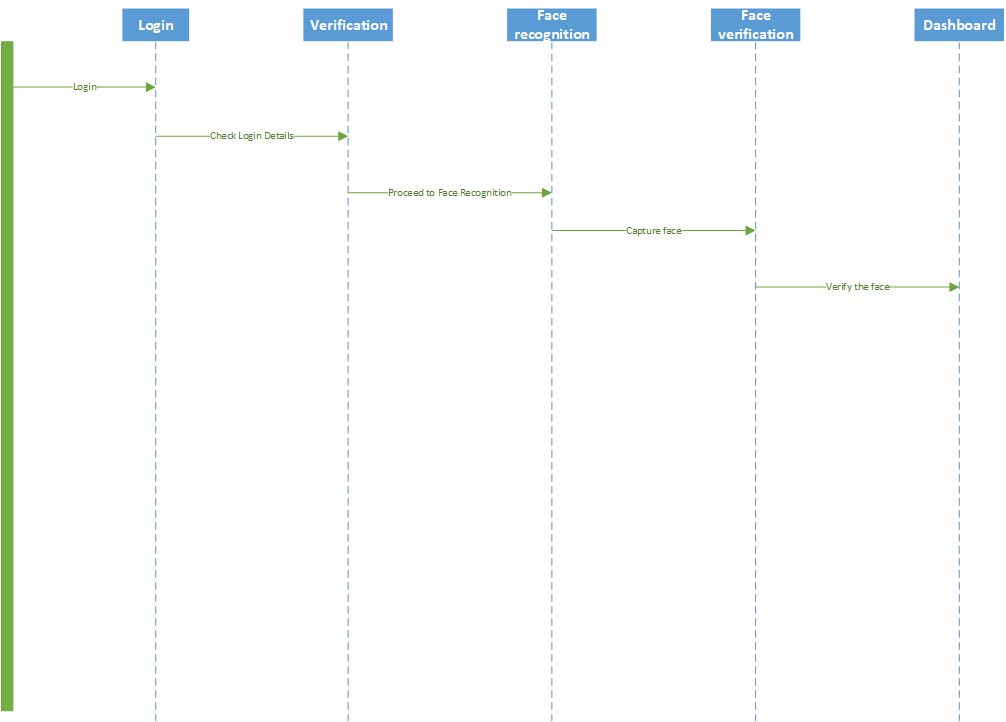


Figure 13 Sequence Diagram

### ER-DIAGRAM



#### 3.7.3 Physical design

Table 1 Member table

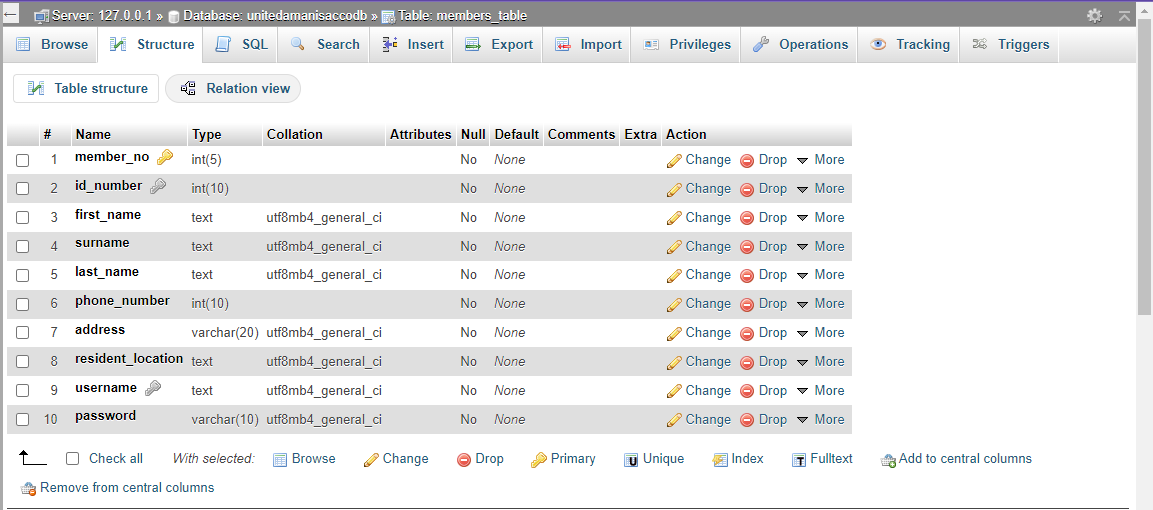


Table.0.1 Staff table

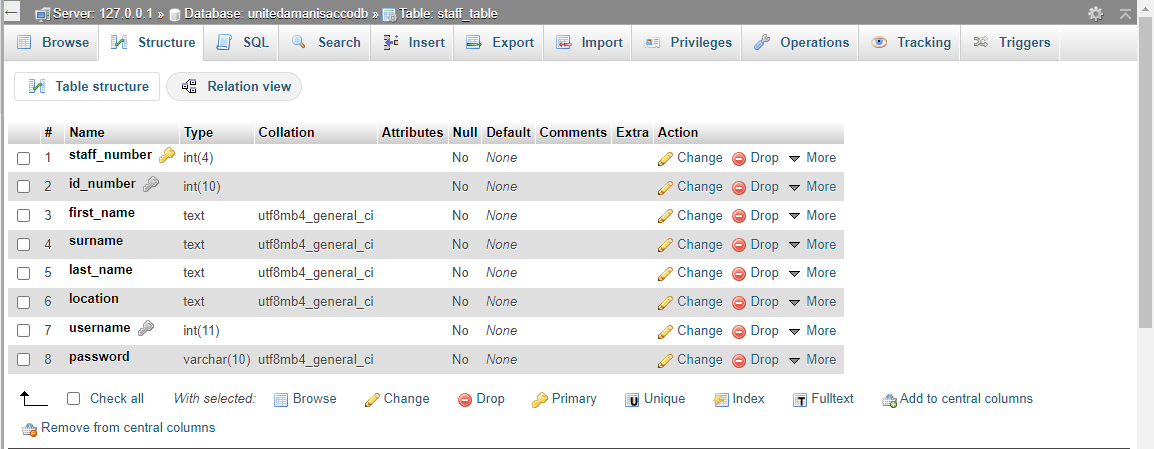


Table.3 Transaction Table

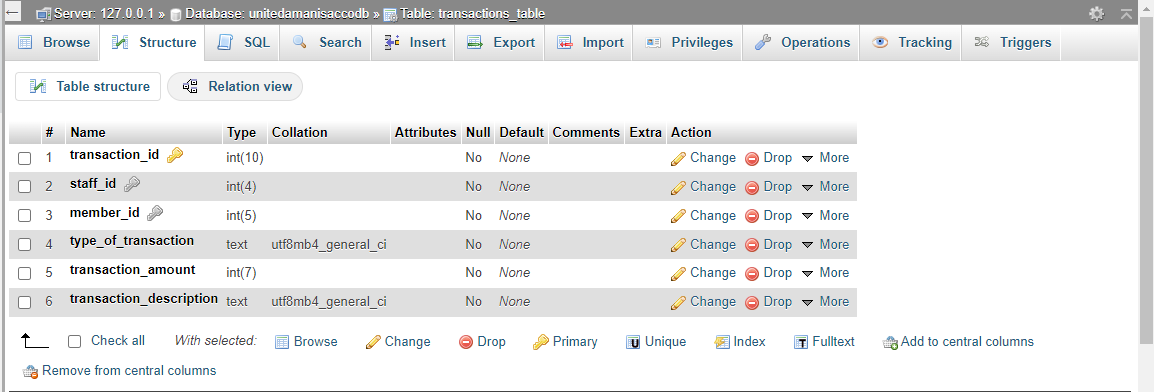


Table 4 Accounts table

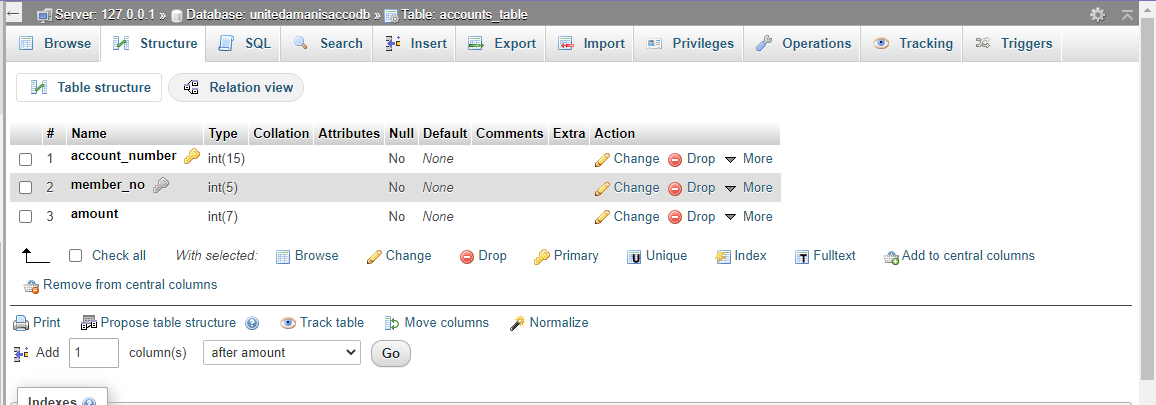


Table5 Logs table

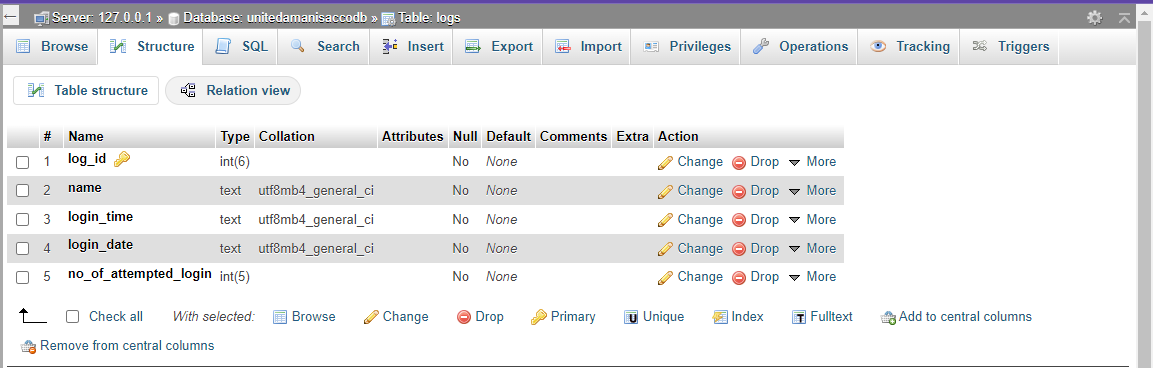
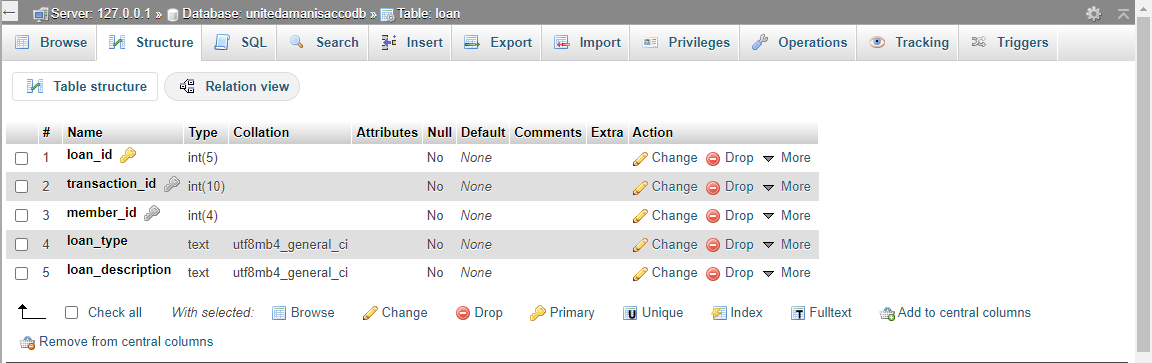


Table 6 Loan table



# CHAPTER 4

## SYSTEM ANALYSIS, DESIGN AND IMPLEMENTATION

### 4.1 INTRODUCTION

This chapter reports the findings and results obtained from the research conducted. It covers the coding, the designs of the system and its implementation.

### 4.2 SYSTEM CODE GENERATION

|  |  |
| --- | --- |
| Accounts.php | <!DOCTYPE html>  <html>  <?php include('includes/header.php') ?>  <?php  $member\_number = $\_POST['member\_number'];  $id\_number = $\_POST['id\_number'];  $f\_name = $\_POST['f\_name'];  $surname = $\_POST['surname'];  $l\_name = $\_POST['l\_name'];  $phone = $\_POST['phone\_number'];  $address = $\_POST['address'];  $resident\_location = $\_POST['resident\_location'];  $username = $\_POST['username'];  $password = $\_POST['password'];  $new\_account = $\_POST['account'];  $amount = $\_POST['amount'];  $staff = "Peter";  $staff\_id = "1";  include('includes/config.php');  session\_start();  $userid = $\_SESSION['userid'];    $hash = password\_hash($password,  PASSWORD\_DEFAULT);  // Check connection  if($link === false){  die("ERROR: Could not connect. " . mysqli\_connect\_error());  }    $sql = "INSERT INTO members\_table(member\_no,id\_number,first\_name, surname,last\_name,phone\_number,address,resident\_location,username,password) VALUES('$member\_number','$id\_number','$f\_name' ,'$surname','$l\_name','$phone','$address','$resident\_location','$username','$hash')";  if ($link->query($sql) === TRUE) {  } else {  echo "Error: " . $sql . "<br>" . $link->error;  }  $link->close();  $sql1 = "INSERT INTO accounts\_table(account\_number,member\_no,amount)VALUES('$new\_account','$member\_number','$amount')";  if ($link1->query($sql1) === TRUE) {  echo "You have successfuly registered the member";  } else {  echo "Error: " . $sql1 . "<br>" . $link1->error;  }  $link1->close();  $sql2 = "INSERT INTO transactions\_table(staff\_id,type\_of\_transaction,transaction\_description, transaction\_amount) VALUES('$staff\_id','Account','Created Account for $member\_number ' ,'$amount')";  if ($link2->query($sql2) === TRUE) {  } else {  echo "Error: " . $sql2 . "<br>" . $link2->error;  }  $link2->close();  ?>  <?php  include('includes/footer.php')  ?>  </body>  </html> |
| Recog index.html | const verifybutton = document.getElementById('verify')  const imageview = document.getElementById('imgPreview')  const passedimage=localStorage.getItem("photo")  var membername="";  const trimmedname=[];  Promise.all([  faceapi.nets.faceRecognitionNet.loadFromUri('/Face Recognition Security/recog models'),  faceapi.nets.faceLandmark68Net.loadFromUri('/Face Recognition Security/recog models'),  faceapi.nets.ssdMobilenetv1.loadFromUri('/Face Recognition Security/recog models')  ]).then(start)  async function start() {  const container = document.createElement('div')  container.style.position = 'relative'  document.body.append(container)  const labeledFaceDescriptors = await loadLabeledImages()  const faceMatcher = new faceapi.FaceMatcher(labeledFaceDescriptors, 0.6)  let image  let canvas  document.getElementById("verify").disabled = false;  document.getElementById("loadingdiv").style.display = "none";  var url = localStorage.getItem("photo");  /\*fetch(url)  .then(res => res.blob())  .then(blob => console.log(blob))  \*/  verifybutton.addEventListener('click', async () => {  if (image) image.remove()  if (canvas) canvas.remove()  const imagepic= localStorage.getItem("photo");  document.querySelector("#imgPreview").setAttribute("src",imagepic)  image = await faceapi.fetchImage(url);  /\*container.append(image)\*/ //Stopping it from creating an image  canvas = faceapi.createCanvasFromMedia(image)  /\*container.append(canvas)\*/ //Stopping it from creating an image  const displaySize = { width: image.width, height: image.height }  faceapi.matchDimensions(canvas, displaySize)  const detections = await faceapi.detectAllFaces(image).withFaceLandmarks().withFaceDescriptors()  const resizedDetections = faceapi.resizeResults(detections, displaySize)  const results = resizedDetections.map(d => faceMatcher.findBestMatch(d.descriptor))  const results2 = detections.map(fd => faceMatcher.findBestMatch(fd.descriptor))  var membername = localStorage.getItem("membername");  results2.forEach((bestMatch, i) => {  const text = bestMatch.toString()  const name= text.trim();  const trimmedname=name.slice(0, -6)  })  results2.forEach((bestMatch, i) => {  const text = bestMatch.toString()  const nametrim= text.trim();  const nameslice=nametrim.slice(0, -6);  console.log("namesliced"+nameslice)  trimmedname.push(nameslice);  /\*localStorage.setItem("verifiedname",nameslice)\*/  })  membername=localStorage.getItem("membername");  console.log("trimmedname"+trimmedname[0].trim());  console.log("membername"+membername.trim());  /\*const trimmedname= localStorage.getItem("verifiedname");\*/  if (trimmedname[0].trim()===membername){  console.log("You have Been verified successfully")  window.location.href = "user dashboard.php"  }else{  console.log("Sorry we could not verify you")  }  /\* results.forEach((result, i) => {  const box = resizedDetections[i].detection.box  const drawBox = new faceapi.draw.DrawBox(box, { label: result.toString() })  drawBox.draw(canvas)  })\*/  })  }  function loadLabeledImages() {  const labels = [document.getElementById("helper").getAttribute("data-name")]  return Promise.all(  labels.map(async label => {  const descriptions = []  for (let i = 1; i <= 2; i++) {  const img = await faceapi.fetchImage(`face images/${label}/${i}.jpg`)  const detections = await faceapi.detectSingleFace(img).withFaceLandmarks().withFaceDescriptor()  descriptions.push(detections.descriptor)  }  return new faceapi.LabeledFaceDescriptors(label, descriptions)  })  )  }  function verifyperson(membername,trimmedname){  if (membername.trim() === trimmedname[0]) {  console.log("Verified successfully")  /\*console.log(membername.trim()+trimmedname)\*/  } else if (trimmedname[0]=== "") {  console.log("Sorry you could not be Verified")  console.log(membername.trim()+trimmedname[0])  } else{  greeting = "Good evening";  }  } |
| View benefeciaries.php | <!DOCTYPE html>  <html>  <?php  include('includes/config.php');  session\_start();  $userid = $\_SESSION['userid'];  include('includes/registeredheader.php');    // Check connection  if($link === false){  die("ERROR: Could not connect. " . mysqli\_connect\_error());  }    $sql = "SELECT beneficiary\_no, father\_id, mother\_id, first\_name,surname,last\_name,amount FROM beneficiaries WHERE father\_id= '$userid' OR mother\_id= '$userid'";  if($result = mysqli\_query($link, $sql)){  if(mysqli\_num\_rows($result) > 0){  echo "<table width=100% style=table-layout:fixed;>";  echo " <tr>  <th>  First Name  </th>  <th>  Surname  </th>  <th>  Last Name  </th>  <th>  Amount  </th>  </tr>";  while($row = mysqli\_fetch\_array($result)){  $first\_name= $row['first\_name'];  $surname= $row['surname'];  $last\_name= $row['last\_name'];  $amount= $row['amount'];  echo " <tr>  <th>  $first\_name  </th>  <th>  $surname  </th>  <th>  $last\_name  </th>  <th>  $amount  </th>  </tr>";    }  echo "</table>";  mysqli\_free\_result($result);  } else{  echo "You Currently dont have any beneficiaries under your account";  }  }  mysqli\_close($link);  ?>  <?php  include('includes/footer.php')  ?>  </body>  </html> |

### 4.3 SYSTEM SCREENSHOTS

Member login page

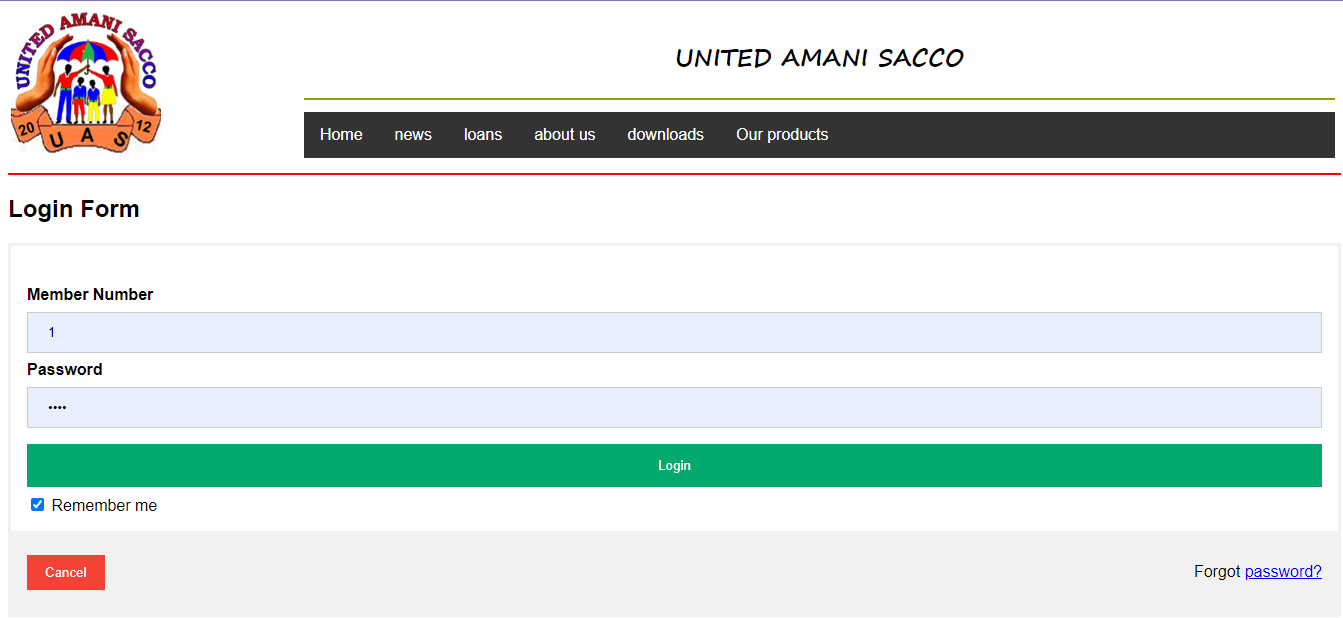


Figure 14 Member login page

Fund transfer

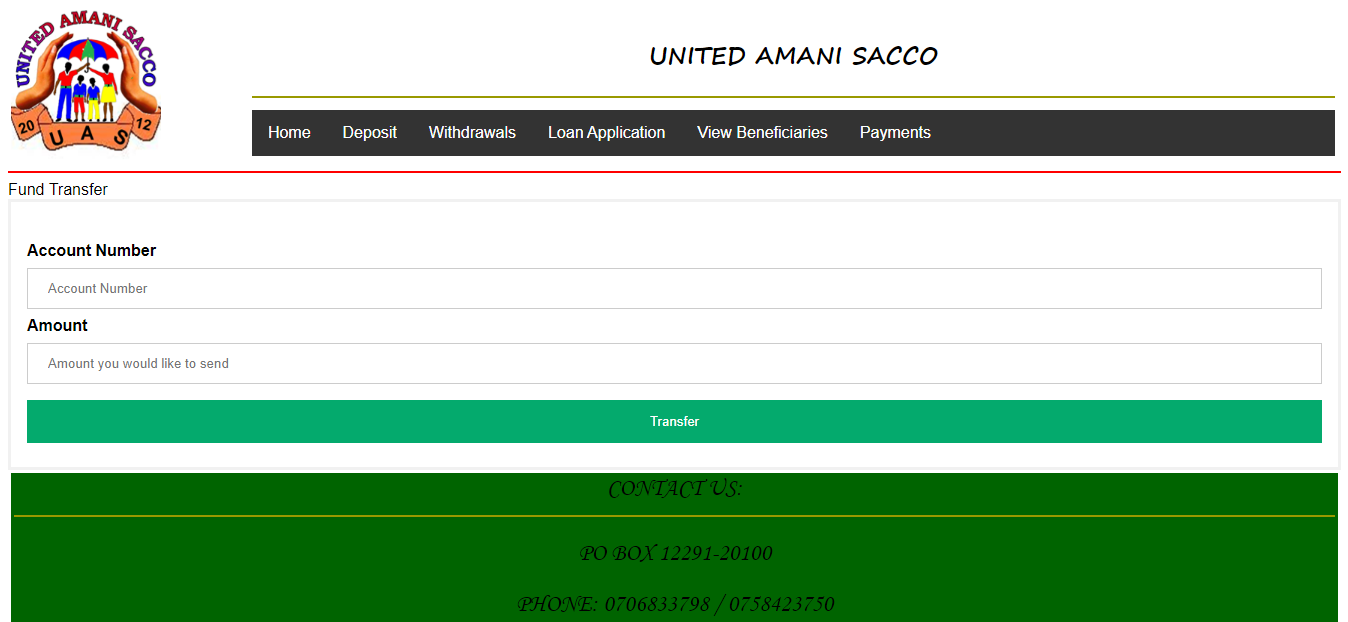


Figure 15 Fund transfer

User dashboard

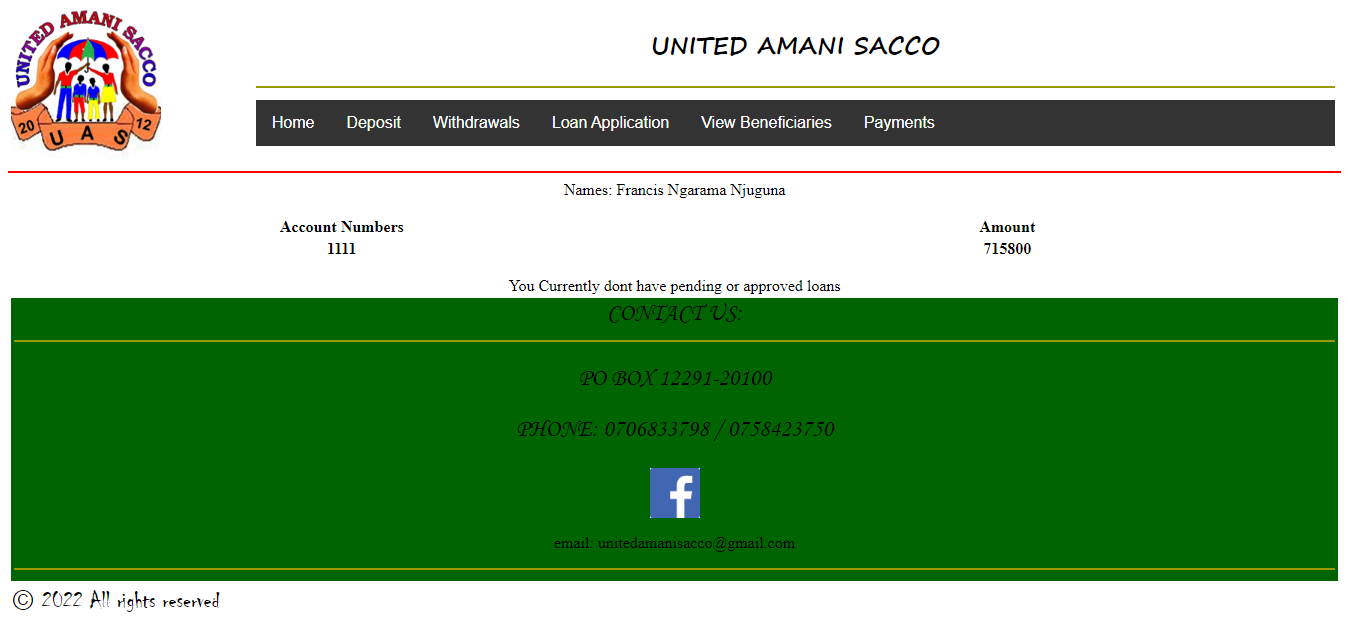


Figure 16 User dashboard

Registering new members(staff)

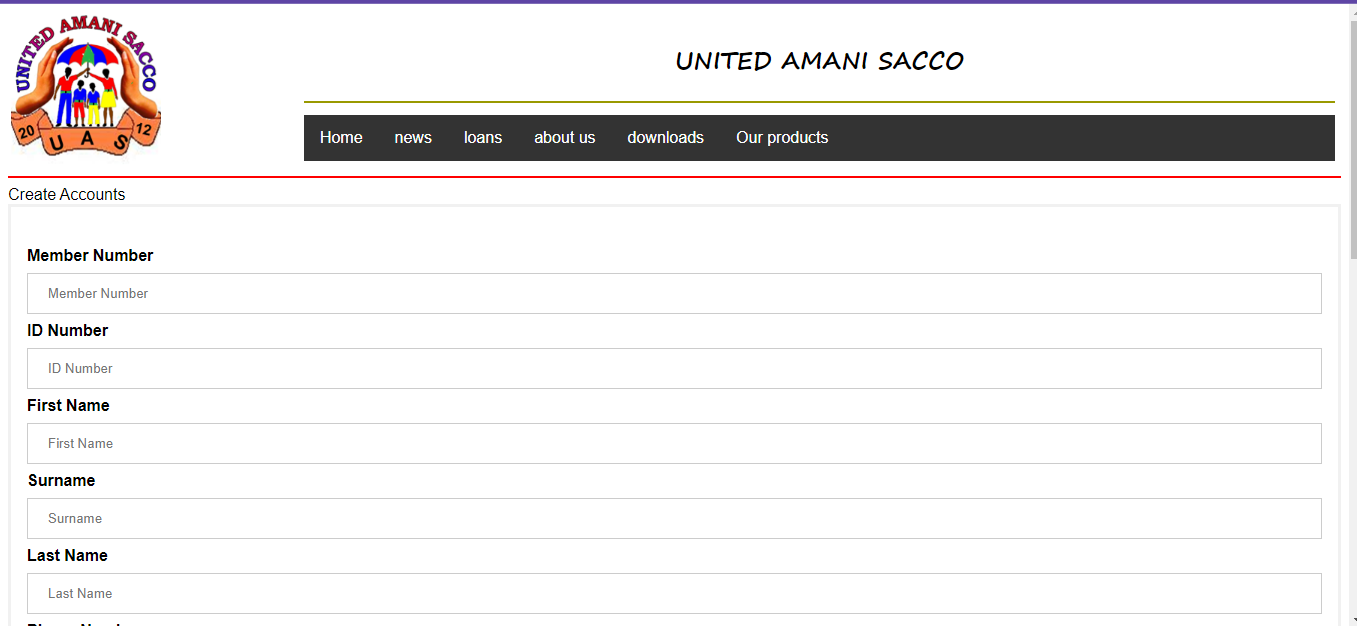


Figure 17 Registering new members(staff)

### 4.4 TESTING

#### 4.4.1 UNIT TESTING

Unit testing involves the testing of each unit or an individual component of the software application. The purpose is to validate that each unit of the software code performs as expected. It assures to identify and fix the bugs at the early stage of SDLC.

|  |  |  |
| --- | --- | --- |
| Unit Test Case | Input/Action | Expected Result |
| Test Case: The face is recognized and an image taken | Taking an image | The image taken is passed to the verification module |
| Verifying image | The image | When successfully verified, open the user dashboard |

#### 4.4.2 Integration Testing

It is a type of software testing in which the different units, modules or components of a software application are tested as a combined entity

Integration testing involves integrating the various modules of an application and then testing their behavior as a combined, or integrated, unit. Verifying if the individual units are communicating with each other properly and working as intended is essential.

The aim of integration testing is to test the interfaces between the modules and expose any defects that may arise when these components are integrated and need to interact with each other.

#### 4.4.3 System Testing

System Testing is a type of software testing that is performed on a complete integrated system to evaluate the compliance of the system with the corresponding requirements. System testing detects defects within both the integrated units and the whole system. The result of system testing is the observed behavior of a component or a system when it is tested.

### 4.5 LIMITATIONS

The system cannot differentiate between an image taken from other sources and an image taken directly from the camera.

### 4.6 CONCLUSION

The system enables the members to perform all the operations that they normally do at the premises. The security is heavily enforced through encryption of the data and most importantly the passwords. The face recognition module acts as a two-factor authentication system to further improve the security of the user’s data.

### 4.7 RECOMMENDATION

The system can be updated to cover other aspects that were not covered depending on the necessities of the users.

### 4.8 REFERENCES

# Bibliography

Anon., 2021. *OWASP Top Ten.* [Online]   
Available at: https://owasp.org/www-project-top-ten/

Burtescu, E., 2006. *database security - attacks and control methods, Department of Accounting and Management Informatics.* Pitesti, Romania: s.n.

Dougherty, C., 2012. *Practical Identification of SQL Injection Vulnerabilities.* s.l.:USCERT.

J. Lopez, S. M. F. S. K. a. A. P., 2008. *Securing Information and Communications Systems: Principles, Technologies, and Applications,.* 1st ed ed. s.l.:Artech House.

Pilev, D., 2014. *International Electronic Journal of Pure and Applied Mathematics,* 8(4), pp. 1-11.

S. Tanwar, 2012. “Issues and challenges in web services,”. *International Journal of Advanced Research in IT and Engineering,* vol. 1(2).