**FINGERPRINT-BASED AUTOMATIC TELLER MACHINE**

**­­­­**

TONNY OCHIENG' LANG'O

COM/B/01-02167/2016

# A project report submitted in partial fulfillment of the requirements for the award of the degree of Bachelor of Science in Computer Science of Masinde Muliro University of Science and Technology.

# September, 2015

# 

**DECLARATION AND CERTIFICATION**

This project report is my original work prepared with no other than the indicated sources and support and has not been presented elsewhere for any other award. Signature……………………… Date……………………...

Jusper Ondulo

COM/B/01-02167/2016

**CERTIFICATION**

The undersigned certify that they have supervised and coordinated and hereby recommend for acceptance of Masinde Muliro University of Science and Technology a project report entitled Fingerprint-based automatic teller machine.

Signed…………………………… Date……………………..

[Supervisor name]

Department of Computer Science

Masinde Muliro University of Science and Technology

Signed…………………………… Date……………………..

Mr. Jusper Ondulo

Coordinator Computer Science Project II

Department of Computer Science

Masinde Muliro University of Science and Technology

Acknowledgement

This project would not have been successful without a myriad of people who were always there to give me support.

Thank you to the Almighty God for giving me life and strength to be able to accomplish my project.

Thank you to my parents for all the financial, mental and physical support that they provided to me without which I would have lost all hope.

Thank you to my friends who gave me all the ideas to help me accomplish my project. Their ideas were great.

Dedication.

I dedicate this project to my friends.

Table of Contents

[Declaration 2](#_Toc531524855)

[Abstract. 4](#_Toc531524856)

[INTRODUCTION 5](#_Toc531524857)

[Background information 5](#_Toc531524858)

[Problem Statement 5](#_Toc531524859)

[Main Aim of the Project. 5](#_Toc531524860)

[Objectives 6](#_Toc531524861)

[General objectives. 6](#_Toc531524862)

[Specific objectives. 6](#_Toc531524863)

[Limitations. 6](#_Toc531524864)

[Scope. 6](#_Toc531524865)

[Benefits and beneficiaries of the Project. 7](#_Toc531524866)

[Project Justification. 7](#_Toc531524867)

[LITERATURE REVIEW 8](#_Toc531524868)

[METHODOLOGY. 9](#_Toc531524869)

[Introduction. 9](#_Toc531524870)

[Methodologies used 9](#_Toc531524871)

[1. Documents and Records reviews. 9](#_Toc531524872)

[2. Interview 9](#_Toc531524873)

[System requirements 10](#_Toc531524874)

[BUDGET AND SCHEDULE 11](#_Toc531524875)

[Budget 11](#_Toc531524876)

[Schedule 11](#_Toc531524877)

[SUMMARY, RECOMMENDATIONS AND CONCLUSIONS. 12](#_Toc531524878)

[Summary. 12](#_Toc531524879)

[Recommendations. 12](#_Toc531524880)

[Conclusions 12](#_Toc531524881)

[REFERENCES. 13](#_Toc531524882)

# Abstract.

The main purpose of this system is to make online transaction more secure and user-friendly. Now days Biometric technology is increasing rapidly. Biometric is used for personal identification. Here we are using Fingerprint scanning biometric to provide access to ATM machine. Data of a fingerprint is stored in database using the enrollment process through the Bank. Bank provide authentication to the customer that can be access while performing transaction process. If fingerprint match is found in data base then transaction take place. After verification if fingerprint does not match transaction will be canceled. Using fingerprint based ATM system user can make secure transaction.

# 

# INTRODUCTION

## Background information

Of all the biometrics, fingerprint recognition is one of the most dependable and promising personal identification technology. Fingerprints play an important role in biometric system. In biometrics technology, fingerprint authentication has been in use for the longest time and bears more advantages than any other biometric technologies. Fingerprints are the most widely used biometric feature for an individual identification and verification.

This project implements a fingerprint verification of ATM (Automatic Teller Machine) security system using the biometric with hybridization. The fingerprint trait is chosen, because of its characteristics like availability, reliability and high accuracy. The fingerprint based biometric system can be implemented easily to secure the ATM machine. In this system the working of these ATM machine is when the customer places his finger on the fingerprint module when he needs to access the ATM to withdraw the cash then the machine processes the fingerprint of the user. With the help of biometrics, it verifies and identifies the fingerprint and gives accurate result that if it is valid or not. In this way we can try to control the criminal activity of ATM and secure it.

The present scenario to operate an ATM, customers are typically identified by inserting a plastic ATM card (or some other acceptable payment card) into the ATM, with authentication being by the customer entering a personal identification number (PIN), which must match the PIN stored in the chip on the card (if the card is so equipped), or in the issuing financial institution's database.

To initiate the application, the fingerprint of the person is entered and it is stored into database as a template. To login into application user has to scan his/her fingerprint, if it matches with the pre-stored template then the person has to enter the unique id which is given to him to access his ATM. An unauthorized person tries to login then the user will be alarmed with the help of a buzzer which is linked with the controller. An authorized user is given 3 chances to re-enter the id if he/she forgets. In order to avoid criminal activities like man-in-the-middle attacks, biometric authentication system is implemented.

Fingerprint based ATM system is one of the secure system. In this system, we are implementing ATM system based fingerprint authentication.

## Problem Statement

The invention of ATM has brought lots of benefits to bank users as it has provided easy access to money from their accounts. By using the ATM card provided by the bank, one is able to access his/her account 24/7.  Customers are typically identified by inserting a plastic [ATM card](https://en.wikipedia.org/wiki/ATM_card" \o "ATM card) (or some other acceptable payment card) into the ATM, with authentication being by the customer entering a [personal identification number](https://en.wikipedia.org/wiki/Personal_identification_number" \o "Personal identification number) (PIN), which must match the PIN stored in the chip on the card (if the card is so equipped), or in the issuing financial institution's database.

Use of the ATM card has experience lots of security threats and caused lose of customers’ money through card fraud. Cards are easily lost or stolen from the card holders. An attacker can use the lost card and a guessed PIN to access a customer’s account. A later variant of this approach is to trap the card inside of the ATM's card reader with a device often referred to as a [Lebanese loop](https://en.wikipedia.org/wiki/Lebanese_loop" \o "Lebanese loop). When the customer gets frustrated by not getting the card back and walks away from the machine, the criminal is able to remove the card and withdraw cash from the customer's account, using the card and its PIN.Another simple form of fraud involves attempting to get the customer's bank to issue a new card and its PIN and stealing them from their mail.By contrast, a newer high-tech method of operating, sometimes called card skimming or card cloning, involves the installation of a magnetic card reader over the real ATM's card slot and the use of a wireless surveillance camera or a modified digital camera or a false PIN keypad to observe the user's PIN. Card data is then cloned into a duplicate card and the criminal attempts a standard cash withdrawal. The availability of low-cost commodity wireless cameras, keypads, card readers, and card writers has made it a relatively simple form of fraud, with comparatively low risk to the fraudsters.

This project intends to come up with a solution to this huddles through the use of a customers fingerprint. Fingerprint Based ATM is a desktop application where fingerprint of the user is used as a authentication. The finger print minutiae features are different for each human being so the user can be identified uniquely. Instead of using ATM card Fingerprint based ATM is safer and secure. There is no worry of losing ATM card and no need to carry ATM card in your wallet. You just have to use your fingerprint in order to do any banking transaction. The user has to login using his fingerprint and he has to enter the pin code in order to do further transaction. The user can withdraw money from his account. In order to withdraw money user has to enter the amount he want to withdraw and has to mention from which account he want to withdraw (i.e. saving account, current account) .The user must have appropriate balance in his ATM account to do transaction. User can view the balance available in his respective account.

## Main Aim of the Project.

## The main aim of this project is to provide fingerprint as authorized identity and to design a more secure ATM system .

### General objective.

To design and implement a program that will use fingerprint to authorize identity of a bank customer who want to transact through an ATM.

### Specific objectives.

1. To design a system that will use fingerprints to authorize customers.
2. To implement a system that will use fingerprints to identify customers.
3. To design a database to customers records.

## Limitations.

Some of the problems that may hinder the project from performing according to specification include:

1. As this technology is so sensitive , cheap components in its construction can result in an authorized person being denied access because of a bit of sweat on the finger or an inconveniently placed cut , If the valid customers are not allowed their approved access to the ATM to perform transactions , the results can be quite stressful
2. Using fingerprint scanner does not take into consideration when a person physically changes. A person’s finger changes sizes or form/pattern over time and the fingerprint scanner does not take this into consideration. When this changes occur, an individual can have difficulty identifying themselves and gaining access. The fingerprint scanner can have problems in capturing an accurate fingerprint image as well. E.g In the manual labour industry since employees are usually working with their hands, their fingers may get rough or scratched which could lead to a miss-reading.
3. Using the fingerprint scanner can lead to false rejections.A biometric device does not always read an individuals fingerprint accurately, and could therefore refuse access to a user. In certain cases, a user may have not placed their fingerprint in the right spot or placed the left finger instead of the right and visa versa. When this happens the software will falsely rejects the user’s fingerprint. If a user does not place their correct finger in the right spot the fingerprint scanner may not read the employee's identification properly and the software will reject him/he
4. Since fingerprint recognition software only reads one section of a person's finger—it is prone to error. Manually repositioning fingers to get the right reading can be time-consuming. Also the the process of comparing fingerprints is a bit slow compared to comparing data from magnetic cards. This make the system to run slowly compared to the previous card-based ATM.
5. . For some people it is very intrusive, because is still related to criminal identification.
6. It can make mistakes with the dryness or dirty of the finger’s skin, as well as with the age (is not appropriate with children, because the size of their fingerprint changes quickly).
7. Crooks can find ways to deceive and outsmart fingerprint machines, such as finding a target’s fingerprints on another surface like a drinking glass and using these prints to access the device, or even cutting off someone's finger for the print. The software will not be able to recognize that a valid person is not currently at the system performing a transaction. Hacker can correctly guess the password of his/her target using either brute force attack or dictionary on the target data from other sources. By having both the fingerprint and the correct PIN the attacker will be able to masquerade as the valid user and transact using the ATM.

## Scope.

The project suggests to design and develop a system that will register bank users by scanning their fingerprints and the use the data to authorize one when accessing the account to withdraw cash.A bank employee will be able to register a customer into the bank’s database. Among the data captured will be the customer’s fingerprint data and will be stored into the banks database. The customer will be able to register for one or more accounts using the same fingerprint data. The authorized bank employee will also be able to view customer’s details for verification purposes only. The employee will not be able to edit a customer’s data.

The project also involve designing and implementing an interface to enable the customer to access his/her account to check balance and withdraw money. The interface will allow a customer to use the ATM machine by first placing his finger at Biometric scanner which will scan his fingerprint feature and compare that extracted feature with stored feature from the database, if feature matches then the person is allowed for transaction otherwise it not process. The customer will have to provide a PIN for verification purposes. The system will the match if the password is correct.

## Benefits of the project.

1. Reliable: The system will be reliable in that no two people will be matched to the same fingerprint. Using of fingerprint makes it possible to use the ATM 24/7 whenever one requires to use it. One will always transact by being able to use his/her fingerprint without the fear of losing it or forgetting it at inaccessible place.
2. Easy to use: The system is easy to use for people from every class of the society. It involves only placing a finger to be scanned and inserting a correct PIN. It removes the need to have intense training of it users. Instead of having to learn and remember which side to insert a card as in the case with card-based ATM, the user need only to place his/her finger on the scanner.
3. Extra Secure: The system eliminates cloning of card by using fingerprint of which no current technology can clone. This provide a unique feature of identifying customers. Also The human fingerprint contains unique whorls and ridges that would be difficult for the average crook to duplicate. According to Forbes magazine, requiring a unique fingerprint only can speed up a secure transaction or registration process compared to a complex series of verification of emails, passwords, encrypted data and more. This together with a 4 character PIN increases the security of the system.
4. No need to further invest on the Cards Cost. The card-based ATM require that a banking institution provide plastic card to their customers for use at the ATM. When the card is lost or stolen, the customer would have to purchase a new ATM card as a replacement. These costs are cut when using the fingerprint-based ATM. The customer will always have his fingerprint and therefore no need to purchase cards.
5. No excuses for RF/Magnetic Cards forgetness. Many people have the problem of forgeting to carry their cards or even don’t remember where they place them when they used it last. This prevent them from using an ATM thus costing the banking institution a lot of money since the customers are charged when they use an ATM. This also inconveniences the customers since they waste lots of time trying to find the card or going back to get it.

## The beneficiaries of this project.

1. Bank customers: The customer of the bank will benefit immensely in that the need to carry the ATM card will be lifted from him. This will solve the problem of forgetting it or the card being stolen and inconveniencing him/her from using the ATM. The customer will therefore be able to use the ATM any time he/she needs to. There will no losing or forgetting the authorization requirements since one will always be in position of his/her fingerprint. Also, the customer will be saved from having to purchase the ATM card to be allowed to use the ATM. By using his/her fingerprint the customer can withdraw money and check balance from his/her account at an ATM. The problem of storing the ATM cards properly is also solved and therefore the customer does not need to worry so much about the safety of the authorization documents.
2. Banking institutions: The confidence of customers with the bank will increase as cases of card fraud will be no more. This will increase the number of users who open an account with the bank. Also, profits will increase to the banking institutions that use fingerprint based ATM since customers are given the priviledge of using the ATM at any time. The excuse of having forgotten the ATM and therefore one cannot use the ATM is solved.
3. The government : The government will see a drop in the number of criminal cases at the ATM. This is because fingerprint provide high security and hackers will find it hard to clone the fingerprint data of the bank customers.

## Project Justification.

The purpose of this project is to implement a system that can use fingerprint biometric technology to identify customers of a bank at an ATM point before performing any operation. While the use of fingerprint as a biometric identification of people has been widely used in other areas that make use of biometric technology such as in security to identify criminals at a crime scene and in the workplace to allow certain people access to resources, it is rarely used at the ATM to authorize access to customers. The ATM use a plastic card which is affected by card fraud leading to lose of money.

Lost ATM card lead to huge amount of loses if they fell into wrong hands.Although incidences of credit card fraud are limited to about 0.1% of all card transactions, they have resulted in huge financial losses as the fraudulent transactions have been large value transactions.  Also, 0.04% (4 out of every 10,000) of all monthly active accounts were fraudulent. Even with tremendous volume and value increase in credit card transactions since then, these proportions have stayed the same or have decreased due to sophisticated [fraud detection](https://en.wikipedia.org/wiki/Fraud_detection" \o "Fraud detection) and prevention systems. Today's fraud detection systems are designed to prevent one-twelfth of one percent of all transactions processed which still translates into billions of dollars in losses (Hassibi PhD, Khosrow 2000). Biometric authentication using fingerprint identification is seen by many as the solution to most of the theft and fraud cases being reported in the use of ATM systems and ATM cards. Biometric-based authentication offers several advantages over other authentication methods, as there has been a significant surge in the use of biometric for user authentication in recent years (S. Oko and J. Oruh, 2012). Majority of peoples chose fingerprint identification as the preferred biometric identification solution to ATM card theft and fraud (Onyesolu and Ezeani 2012).

In this proposed biometric-based ATM authentication system biometric authentication on ATM systems is implemented to prove that it is practicable and could be implemented in production environments. The need of using a card is eliminated and replaced by use of fingerprint which solves the problem of smart-card loss, card theft, card cloning and card clocking by Lebanese loop. Fingerprint identification is an exceptionally flexible and versatile method of human identification. Fingerprint are unique for every living person and therefore provide a very reliable of authorization. Using this characteristic, the project aims at enrolling bank customers into their system and recognizing at the ATM point using the fingerprint.

# LITERATURE REVIEW

## Introduction.

This chapter aimed to be a review of the literature relevant to this subject of study focusing on the use of biometric on ATM to authorize customers. The biometric that we focus on is fingerprint to see how it has been suggested by other people or already been utilized. Existing cases of attempts to achieve this kind of implementation are analyzed with reference to work that has already been published. In this chapter, the achievements of existing similar systems were discussed together with the challenges those systems face, the similarities there had to the proposed system and the advantages the proposed system had over them hence that’s why it should be the system of choice

## Review

This project aims at implementing an ATM that will have biometric authentication techniques to verify the owner of ATM card at the time of transaction. To provide such type of facility we have studied different research papers and found some vital information.

For the system we use fingerprint bio-metrics scanner that capture the fingerprint and then follow certain algorithm for fingerprint matching. Most finger-scan technologies are based on minutiae. 80 percent of finger-scan technologies are based on minutiae matching but that pattern matching is a leading alternative (Samir Nanavati, Michael Thieme, and Raj Nanavati, 2002). This technology bases its feature extraction and template generation on a series of ridges, as opposed to discrete points. The use of multiple ridges reduces dependence on minutiae points, which tend to be affected by wear and tear (Julian Ashbourn, 2002). The downside of pattern matching is that it is more sensitive to the placement of the finger during verification and the created template is several times larger in byte size.

Finger-scan technology is proven and capable of high levels of accuracy. There is a long history of fingerprint identification, classification and analysis. This along with the distinctive features of fingerprints has set the finger-scan apart from other biometric technologies. There are physiological characteristics more distinctive than the fingerprint (the iris and retina, for example) but automated identification technology capable of leveraging these characteristics have been developed only over the past few years. The technology has grown smaller, more capable and with many solutions available. Devices slightly thicker than a coin and an inch square in size are able to capture and process images. Additionally, some may see the large number of finger-scan solutions available today as a disadvantage; many see it as an advantage by ensuring marketplace competition which has resulted in a number of robust solutions for desktop, laptop, physical access, and point-of-sale environments. Biometric data are separate and distinct from personal information. Biometric templates cannot be reverse-engineered to recreate personal information and they cannot be stolen and used to access personal information (Edmund Spinella, 2003).

**ATM Card Fraud**

Crime at ATM has become a notion wide issue that faces not only customer but also bank operators and the financial crime case rises repeatedly.

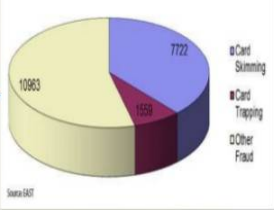


Figure 1: Pie chart of ATM card frauds

|  |  |  |  |
| --- | --- | --- | --- |
| ATM Fraud’s | Card Skimming | Card Trapping | Other Fraud |
| Fraud ration | 7722 | 1559 | 10963 |
| Overall fraud ratio | 20244 | 20244 | 20244 |

Table 1: Sample table to estimate card fraud ratio

Criminal steal customers card, after stealing the card criminal use detail of card by illegal means. The fraud include like card Skimming and card Trapping and many more way included in ATM fraud. Above table and Pie chart gives the approximate Ratio of ATM card related Fraud. We can Say that card Skimming is most common type of Fraud. Card skimming involves the installation of a magnetic card reader over the real ATM's card slot and the use of a wireless surveillance camera or a modified digital camera or a false PIN keypad to observe the user's PIN. Card data is then cloned into a duplicate card and the criminal attempts a standard cash withdrawal. The availability of low-cost commodity wireless cameras, keypads, card readers, and card writers has made it a relatively simple form of fraud, with comparatively low risk to the fraudsters(snopes.com 2016).

Once a customer card is lost and the password is stolen, the user's account is able to hack. When customer's credit card get stolen there may be a chance that unauthorized user can often come with the correct personal code to choose easily guessed pins and password that can be birthdays, phone number and social security numbers.

A later variant of the above approach is to trap the card inside of the ATM's card reader with a device often referred to as a [Lebanese loop](https://en.wikipedia.org/wiki/Lebanese_loop" \o "Lebanese loop). When the customer gets frustrated by not getting the card back and walks away from the machine, the criminal is able to remove the card and withdraw cash from the customer's account, using the card and its PIN. This type of fraud has spread globally. Although somewhat replaced in terms of volume by skimming incidents, a re-emergence of card trapping has been noticed in regions such as Europe, where EMV chip and PIN cards have increased in circulation(Atmsecurity.com, 2009).

Another simple form of fraud involves attempting to get the customer's bank to issue a new card and its PIN and stealing them from their mail(the original, 2008).

**Comparison**

|  |  |  |
| --- | --- | --- |
| Factor | Fingerprint -based ATM | Card-based ATM |
| Risk | Hands can become disfigured over time. Though this happens slowly and the fingerprint data can be stored afresh. | Card can be lost or even stolen. Stolen cards can be used to commit fraud. Cloning of the card is also possible. |
| Remembering | Use of fingerprint save one from having to remember to carry any authentication material to an ATM. | One has to remember to carry the ATM because one won’t be able to access the ATM without it. |
| Cost | Requires the acquisition of one fingerprint scanner for every ATM. | Requires the bank institution to provide a card to every customer who need to use the ATM. Lost ATM cards also cost to replace is mostly discouraged |
| Reliable | Its reliable since one is expected to always have his/hand when trying to access the ATM | One may not have his/her ATM card when he/she want to access an ATM. |

# METHODOLOGY.

## Introduction.

This chapter provides a general description of the methods that were used to collect data from the field, the tools that were used to analyze and the tools that were used to implement the proposed solution. This chapter will focused on data collection, data analysis and processing, sampling procedure, tools for implementation, time plan and budget allocation.

## Software Development Process

The software development process used to design and implement this project is the agile software development. Under this software development process, iterative and incremental methodologies were used.

Iterative development enabled the feature code to be designed, developed and tested in repeated cycles. With each iteration, additional features were designed, developed and tested until there was a fully functional software application that could be deployed.

Using incremental development, the software development was split into smaller segments that build upon each other. Working iteratively allowed going through a cycle to evaluate with each iteration, and determine what changes are needed to produce a satisfactory end product.

### Reasons for choosing Agile

Agile software development process provided a flexible, fast, lean, responsive, and consistent way of developing the software. In Agile development, testing is integrated during the cycle, this made it possible for regular checkups to see that the product was working during the development and make changes if needed. This ensured high quality end-product. Defination and elaboration of requirements was just in time so that the knowledge of the product features were as relevant as possible.

Incorporating continuous integration and daily testing into the development process, allowed addressing of issues while they were still fresh.It allowed software to be developed in incremental, rapid cycles. This resulted in small incremental releases with each release building on previous functionality. Each release was thoroughly tested to ensure software quality was maintained.

Agile methodology helped to reduce risks in that it virtually eliminate the chances of absolute project failure. Changes to the project are added incrementally and tested if they can cause the project to fail.

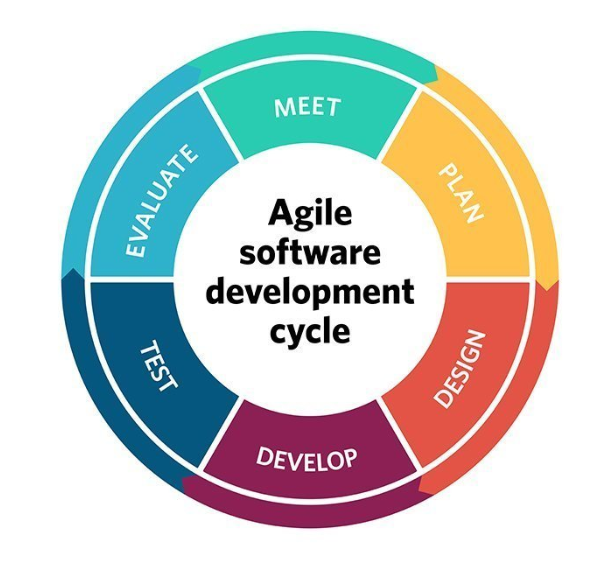


Figure 2: Agile software development cycle

## Data collection methods

Secondary and primary data sources were used during data collection. The secondary sources that were of significant help included newspapers, the internet, and literature from the library books and magazines which will increase knowledge about the field of study.Research documents from the internet came in handy to explain the concepts of biometric means of identification.They helped to explain how previous biometric implementation were done and their shortcomings.

Face to face interviews were setup to gather information from bank users and employees such as what affected their use of the bank ATM. A sample of these groups of people were asked similar questions at ATM point where they came to use the ATM or in the banking halls as they were waiting for services then the data was analyzed from those samples. The data collected was voice recorded for accuracy.

Observation is the other approach that was used to gather information. An ATM point observed and recordings of data collected were presented for analysis.

Social media also came in handy during data collection. Particularly Facebook and twitter to pose questions to social media users such as if they are content with the current ATM system of using plastic card and if it would be more efficient to have biometric methods.

## Techniques for Data Analysis and Design

Use case diagrams to demonstrate the system and user interactions.

Entity–Relationship Diagrams (ERDs) to show the relationship between entities.

Data flow diagrams, flowcharts and context diagrams to indicate flow of data in the system and the different processes.

## System requirements

The following segment describe both hardware and software requirements that will be used in the project.

* Hardware requirements

Intel Quad core laptop (2.1 GHz)

* Software Requirements.

1. Windows 7 Operating System
2. A Java IDE.
3. MySQL server.

# System design.

## Introduction.

The aim of this chapter was to provide a detailed description of the proposed system’s architecture, interface, components, subsystems as well as the hardware, software and network architectures. This process of definition is divided into three distinct parts:

1. Process design.
2. Database design
3. User interface design

**Proposed Plan.**

The proposed system is a desktop application with a 3-tier architecture.

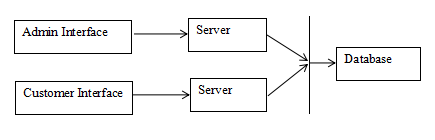


Figure 3 : Architecture of the system

Basically we can explain complete Fingerprint base ATM system in two phases:

1. Enrolment Phase
2. Authentication phase

**Database.**

The proposed system use a single database for both the admin and the customer. It has five tables that are queried by the server. Attributes of the different entities in the database include:

Admin: (username, password)

Details: (id \_number(PK), first\_name, last\_name)

Accounts: (id\_number, account \_number, balance)

Fingerprints: (id\_number, print)

Passwords: (id\_number, password )

Logs: (action\_time, action)

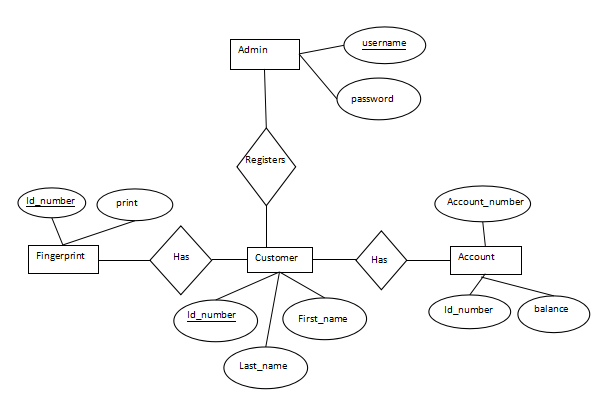


Figure 4 : Entity-Relationship diagram for the proposed system

Database Tables:

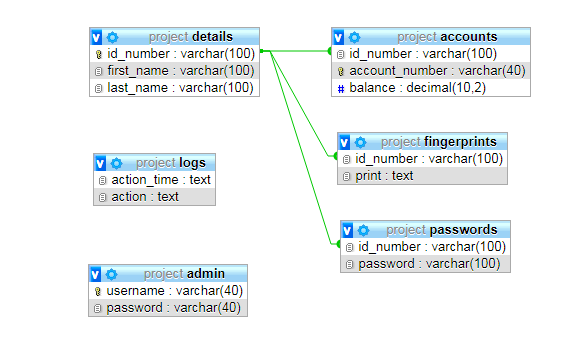


Figure 5 : Logical design for the database

1. Details

This table holds the personal information of all the customers. It holds first name, last name and the id number of a customer. The id number act as the index key of the database.

1. Accounts

It holds the account details of every customer. This includes the account number of a customer and the balance in that account. The id number has an ON DELETE and ON UPDATE foreign key with a reference to the details table.

1. Fingerprints

It holds the fingerprint data of each and every customer. The id number has an ON DELETE and ON UPDATE foreign key with a reference to the details table.

1. Passwords

This table hold the PINs of the customer. The id number has an ON DELETE and ON UPDATE foreign key with a reference to the details table.

1. Logs.

This table hold the logs of the actions on the database. The description of the action is logged together with the time of action into this table using triggers on each table.

1. Admin.

This table hold the details of all the admins authorized to view and edit the data in the database. The password of the admin and his/her username are used to verify the admin on request.

Interface Design

The proposed system has 3 different point of user interface i.e bank employee, server and customer interface.

1. Bank employee Interface

This interface allow the bank employee to interact with the system. It allow the employee to log into the system, add a new customer, add an account to a customer and search for customer details.

To use the system the employee has to login first with correct username and password.

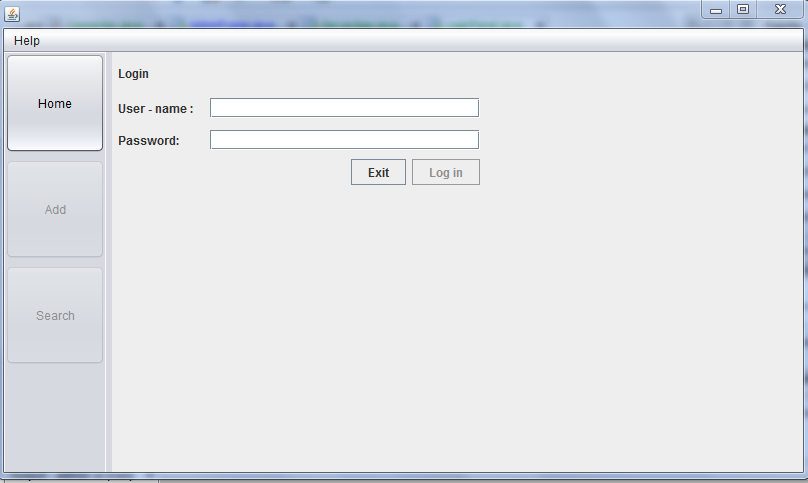


Figure 6 : Admin login interface

After log in, the bank employee can add a new customer into the database and search for data of existing customer from the database. The flow chart for adding a new customer is as follows:-

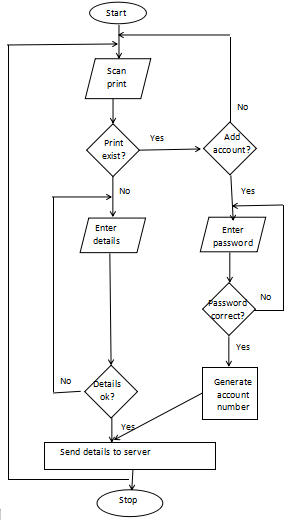


Figure 7 : Flow chart for adding a customer

The search area provide the employee the ability to search for existing customer data. By entering the id number of the customer, the system provide the data about the customer from the database.

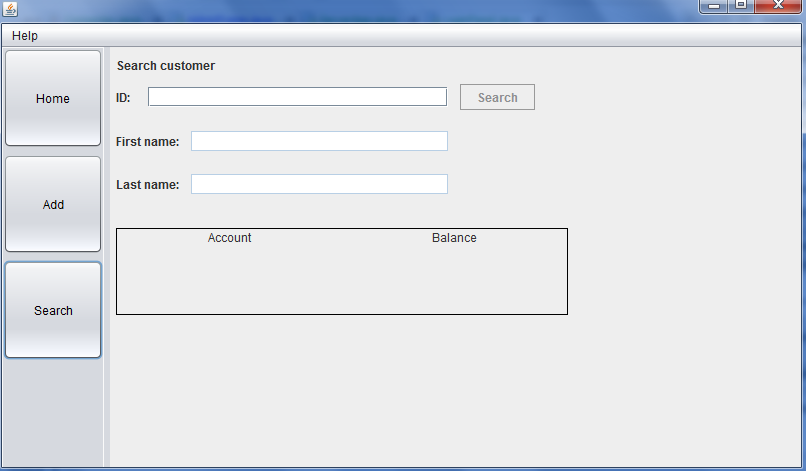


Figure 8 : Searching interface

Customer interface.

Using this interface, the user can make transaction by using their fingers. User can place finger on the Biometric scanner and user’s finger scan can be matched through database, where all authenticated user’s fingerprints are stored .If User wants to do transaction they simply place their finger on biometric scanner and then he/she will be asked to enter his/her PIN.

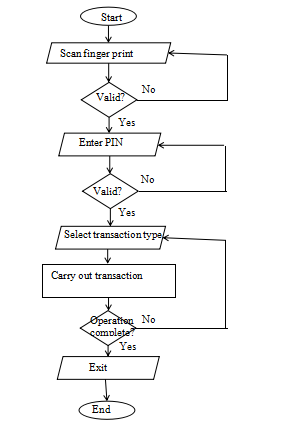


Figure 9 : Authentication phase flow chart diagram

Server interface.

The server interface provide the ability to run the server. The server receives requests from client applications and process them by retrieving data from the database.

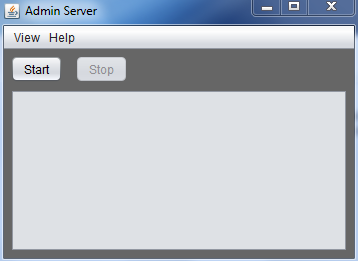


Figure 10 : Server interface

# BUDGET AND SCHEDULE

## Budget

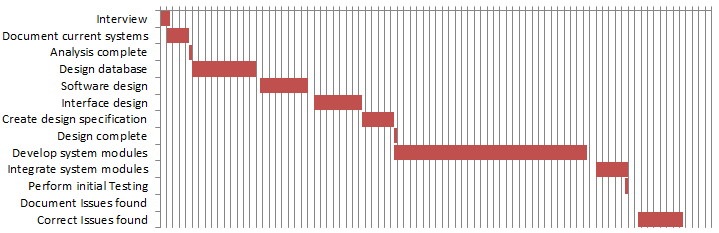
|  |  |
| --- | --- |
| Item | Cost |
| Computer | 20,000 |
| Java IDE | 0 |
| MySQL Server | 0 |
| OS | 0 |

## Schedule

Table 2: schedule table

|  |  |  |  |
| --- | --- | --- | --- |
| Interview | 10/7/2018 | 5 | 10/11/2018 |
| Document current systems | 10/11/2018 | 7 | 10/17/2018 |
| Analysis complete | 10/18/2018 | 1 | 10/12/2018 |
| Design database | 10/19/2018 | 20 | 10/13/2018 |
| Software design | 11/9/2018 | 15 | 10/14/2018 |
| Interface design | 11/26/2018 | 15 | 10/15/2018 |
| Create design specification | 12/11/2018 | 10 | 10/16/2018 |
| Design complete | 12/21/2018 | 1 | 10/17/2018 |
| Develop system modules | 12/21/2018 | 60 | 10/18/2018 |
| Integrate system modules | 2/22/2019 | 10 | 10/19/2018 |
| Perform initial Testing | 3/3/2019 | 1 | 10/20/2018 |
| Document Issues found | 3/3/2018 | 5 | 10/21/2018 |
| Correct Issues found | 3/7/2019 | 14 | 10/22/2018 |

Figure 11: schedule Gantt diagram



# SUMMARY, RECOMMENDATIONS AND CONCLUSIONS.

## Summary.

To summarize, the project allows a person to record information about his/her family. Other members of the family who join later may add more information about this family. One can also view and learn about his/her relations with other members. A member can describe another member and allow other to know about him/her. Members of the family can also advice each other member on the way of life. Information about the family hierarchy will be easily available.

## Recommendations.

Any person who wants to record his/her family genealogy is advised to use this application. It will make it easy for other people to access the information. The information will also be easy to update.

## Conclusions

Family is important and should always be close and be readily accessed. Bringing family together is so important and information about each other can make each member to appreciate each other.

# REFERENCES.

["Archived copy"](https://web.archive.org/web/20080724213440/http://venus.soci.niu.edu/~cudigest/phracks/phrack-08). Archived from [the original](http://venus.soci.niu.edu/~cudigest/phracks/phrack-08) on 24 July 2008. Retrieved 13 March 2008.

 snopes (29 March 2016). ["Skimming with ATM Cameras : snopes.com"](http://www.snopes.com/crime/warnings/atmcamera.asp). snopes.

Samir Nanavati, Michael Thieme, and Raj Nanavati, “Biometrics: Identity Verification in a Networked World”, John Wiley & Sons, 2002.

Julian Ashbourn, “Biometrics: Advanced Identity Verification”, Springer-Verlag, London, 2002.

Hassibi PhD, Khosrow (2000). [Chapter 9 on "Detecting Payment Card Fraud with Neural Networks in book "Business Applications of Neural Networks"](https://www.amazon.com/Business-Applications-Neural-Networks-State-Of-The-Art/dp/9810240899/ref=sr_1_1?ie=UTF8&qid=1365701642&sr=8-1&keywords=Business+Applications+of+Neural+Networks). Singapore-New Jersey-London-Hong Kong: World Scientific. pp. 141–158.