**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 all my friends.

Table of Contents

[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. i](#_Toc16873)

[September, 2015 i](#_Toc10413)

[Abstract. vi](#_Toc29711)

[INTRODUCTION 1](#_Toc5133)

[Background information 1](#_Toc27158)

[Problem Statement 2](#_Toc20642)

[Main Aim of the Project. 3](#_Toc761)

[The main aim of this project is to provide fingerprint as authorized identity and to design a more secure ATM system . 3](#_Toc6709)

[General objective. 3](#_Toc26925)

[Specific objectives. 3](#_Toc8174)

[Research questions 3](#_Toc11167)

[Limitations. 3](#_Toc26598)

[Scope. 5](#_Toc1907)

[Benefits of the project. 5](#_Toc5203)

[The beneficiaries of this project. 6](#_Toc12552)

[Project Justification. 7](#_Toc16153)

[LITERATURE REVIEW 9](#_Toc7627)

[Introduction. 9](#_Toc1720)

[Review 9](#_Toc7638)

[METHODOLOGY. 21](#_Toc32764)

[Introduction. 21](#_Toc19324)

[Target users of the product 21](#_Toc6615)

[Target population. 21](#_Toc18470)

[Sample population. 23](#_Toc11589)

[Methods of data collection. 25](#_Toc14643)

[System requirements 27](#_Toc310)

[Software Development Process 28](#_Toc19640)

[Reasons for choosing Agile 29](#_Toc2758)

[Techniques for Data Analysis and Design 29](#_Toc3404)

[System design. 31](#_Toc13400)

[Introduction. 31](#_Toc17744)

[System Implementation 38](#_Toc2626)

[DISCUSSIONS 45](#_Toc30029)

[SUMMARY, RECOMMENDATIONS AND CONCLUSIONS. 47](#_Toc25140)

[Summary. 47](#_Toc15963)

[Recommendations. 47](#_Toc31360)

[Conclusions 47](#_Toc26803)

[REFERENCES. 48](#_Toc14566)

# 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. Other biometric used currently include face-recognition, iris pattern matching etc. 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.

## Research questions

## 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 form 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.

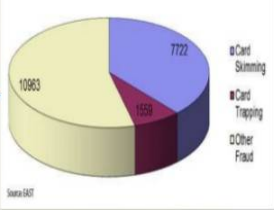


Figure 1: Pie chart of ATM card frauds

|  |  |  |  |
| --- | --- | --- | --- |
| 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 with current system.**

|  |  |  |
| --- | --- | --- |
| 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. |

**Other biometric technologies Available**

Currently their exist different biometric technologies that can be used to authorize people. These technologies have advantages and disadvantages and strengths over each other. Choosing one biometric over the others requires careful consideration, specifications, needs and requirements. Available techniques include:-

1. **Facial recognition**

This is a technology capable of [identifying](https://en.wikipedia.org/wiki/Identification_of_human_individuals" \o "Identification of human individuals) or [verifying](https://en.wikipedia.org/wiki/Authentication" \o "Authentication) a person from a [digital image](https://en.wikipedia.org/wiki/Digital_image" \o "Digital image) or a [video frame](https://en.wikipedia.org/wiki/Film_frame" \o "Film frame) from a [video](https://en.wikipedia.org/wiki/Video" \o "Video) source  by comparing selected [facial features](https://en.wikipedia.org/wiki/Face" \o "Face) from given image with faces within a [database](https://en.wikipedia.org/wiki/Database_management_system" \o "Database management system). One key advantage of a facial recognition system that it is able to person mass identification as it does not require the cooperation of the test subject to work. Properly designed systems installed in airports, multiplexes, and other public places can identify individuals among the crowd, without passers-by even being aware of the system.

However, as compared to other biometric techniques, face recognition may not be most reliable and efficient. Quality measures are very important in facial recognition systems as large degrees of variations are possible in face images. Factors such as illumination, expression, pose and noise during face capture can affect the performance of facial recognition systems.

1. **Voice Recognition**

This technique involve the use of human voice to identify a person. A person’s voice is prerecorded and is used later as an authorization feature.

Voice recognition provide low accuracy and an illness such as a cold can change a person’s voice, making absolute identification difficult or impossible. This makes it an unreliable mechanism when compared to fingerprint mechanism. Voice recognition is also affected by background noise making it impossible to authorize a person. They require a quite environment unlike fingerprint which can be used anywhere.

1. **Iris recognition**

Iris recognition is an automated method of [biometric](https://en.wikipedia.org/wiki/Biometrics" \o "Biometrics) identification that uses mathematical pattern-recognition techniques on video images of one or both of the [irises](https://en.wikipedia.org/wiki/Iris_(anatomy)" \o "Iris (anatomy)) of an individual's [eyes](https://en.wikipedia.org/wiki/Human_eye" \o "Human eye), whose complex patterns are unique, stable, and can be seen from some distance.

Many commercial iris scanners can be easily fooled by a high quality image of an iris or face in place of the real thing ([Swati Khandelwa](https://thehackernews.com/p/authors.html)l, 2015). The scanners are often tough to adjust and can become bothersome for multiple people of different heights to use in succession. The accuracy of scanners can be affected by changes in lighting. Iris scanners are significantly more expensive than fingerprint scanners.

Iris recognition has been found to have a lot of limitations that affect its use. Pupil dilation , for example, is found to affect the accuracy of iris recognition, especially if the amount of dilation is different at enrollment than at verification. Wearing contact lenses, especially cosmetic lenses designed to change the color and appearance of the eye, can also decrease recognition rates.

1. **Retinal scanning**

A retinal scan is a [biometric](https://en.wikipedia.org/wiki/Biometric" \o "Biometric) technique that uses unique patterns on a person's [retina](https://en.wikipedia.org/wiki/Retina" \o "Retina) blood vessels.

Using the retinal scanning for authorization, measurement accuracy can be affected by a disease such as [cataracts](https://en.wikipedia.org/wiki/Cataracts" \o "Cataracts). Measurement accuracy can also be affected by severe [astigmatism](https://en.wikipedia.org/wiki/Astigmatism" \o "Astigmatism). Scanning procedure is perceived by some as invasive. Retina scanning requires being very close to an eye piece, as is done by looking through a microscope. Also, an infrared light is shot in the eye, so it is quite invasive and annoying to carry it out on a regular basis. Not very user friendly as its use require intensive training. High equipment cost compared to the fingerprint scanners. Leads to eye problems that can be identified by CT Scan.. Cheap equipment have been found to damage your eyes on regular usage

**Comparison of some biometric systems**

The following sections compare the current available technologies using factors that influence their use.

The following table compares some of the biometric systems used lately, from the point of view of accuracy, cost, devices required and social acceptability.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Biometric Technology | Accuracy | Cost | Devices required | Social acceptability |
| DNA | High | High | Test equipment | Low |
| Iris Recognition | High | High | Camera | Medium-low |
| Retinal Scan | High | High | Camera | Low |
| Facial recognition | Medium-low | Medium | Camera | High |
| Voice recognition | Medium | Medium | Microphone, telephone | High |
| Hand geometry | Medium-low | Low | Scanner | High |
| Fingerprint | High | Medium | Scanner | Medium |
| Signature recognition | Low | Medium | Optical pen, touch panel. | High |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Eye-iris | Eye-retina | Fingerprint | Hand’s geometry | Writing signature | voice |
| Reliability | Very high | Very high | High | High | High | High |
| Easiness of the use | Average | Low | High | High | High | High |
| Attack’s precaution | Very high | Very high | High | High | Average | Average |
| Acceptance | Average | Average | Average | High | Very high | high |
| Stability | High | High | High | Average | Average | Average |
| Identification and authentication | Both | Both | Both | Authentication | Both | Authentication |
| standards |  |  | ANSI/NIST |  |  | SVAP |
| Interference | Glasses | Irritations | Dirtiness, injury, roughness | Arthritis , rheumatism | Changeable or easy signature | Noise , cold |
| Use | Nuclear installations, medical services, penitentiary centers | Nuclear installations, medical services, penitentiary centers | Police, industrial | General | Industrial | Remote access in banks or databases |
| Current price |  |  |  |  |  |  |

Different biometric recognition methods offer different set of features, advantages and disadvantages. Cost is also an important factor to consider while choosing a biometric recognition system. For high security applications, multi-factor authentication or multi-modal biometric implementation can be considered, while low security applications can be implemented with single biometric modality. Multi-modal biometric applications may hike up the investment required multi-fold, so there has to be a balance of everything and a thorough return on investment study may be required before taking up multi-modal biometric recognition. Fingerprinting is the most popular modality among all biometric recognition methods. Being inexpensive, easy to implement and use, it has most penetration in authentication and access control applications as well as consumer electronics like mobile phones and portable devices. Fingerprint scanners make use of sensors to scan a pattern. These sensors come equipped with different techniques to read and produce image of the fingerprint pattern.

**Biometric in the market**

In recent years, biometric identification systems and fingerprint recognition systems in particular have been widely adopted by both government as well as private outfits. Governments across the nations have been using this technology for the purposes like civil identity, law enforcement, border control, access control, employee identification, attendance, etc. Business setups have been using it to save time by streamlining various processes like employee identification, physical and logical access control, user authentication, safeguarding cloud communication, etc. Biometric systems have been embraced by organizations of all sizes and shapes regardless their industry type and vertical. Availability of fingerprint sensors in affordable mobile devices and government national ID programs have particularly brought biometrics to common man and have increased awareness as well as acceptance. Biometric systems are also getting more and more inexpensive due to widespread implementation and increasing rate of adoption.

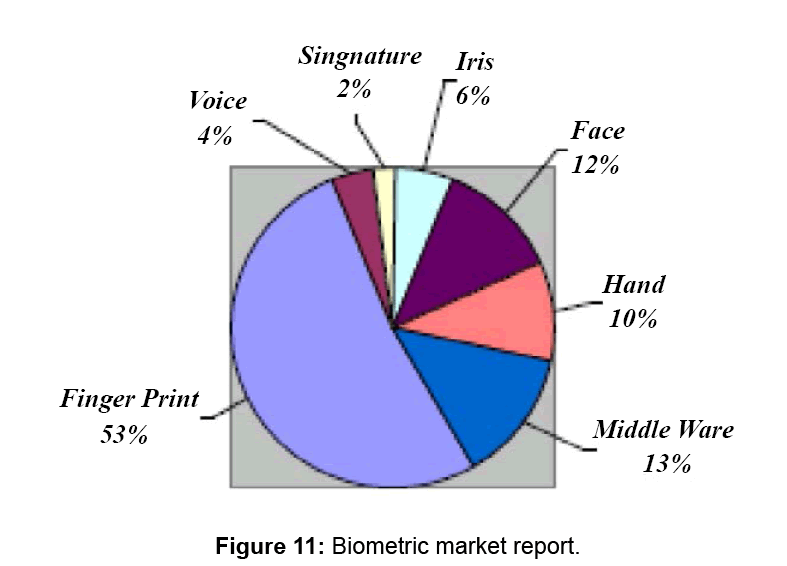


Image 1 : Biometric market share

Mass production cuts down prices, and that is what exactly happening with biometric recognition systems right now. Increasing numbers of implementation made mass production of biometric systems imperative and slashed prices. A biometric system’s price may depend on factors like brand, certifications, waterproofing, type of sensor, etc. A small USB fingerprint scanner can cost as little as $50 and a sophisticated ten finger scanner with live finger detection ability can cost $2500 as well. Increasing production and completion are expected to lower the prices further. Average selling price of global mobile fingerprint sensor volumes is estimated to be dropped to $2 per unit in 2020 which was as high as $5.5 in 2014.



Image 2 : Global Fingerprint sensor volume vs. ASP from year 2014 to 2020 (Source: Carnegie Research)

Increasing adoption has helped bring down cost of biometric devices. Factors like economy of scale, increasing production and electronic components getting cheaper, have helped biometric systems to become affordable for small business and even for individual applications. Slashing prices are particularly evident in case of fingerprint scanners. Fingerprint recognition systems, which were earlier used only in high security facilities or restricted areas, are now commonly seen everywhere. Let it be office doors, server rooms, schools, banks, POS, etc., fingerprint scanners have made their way to everyday life. Due to mass production, building blocks of biometric systems are getting cheaper and new entrants are offering very competitive prices. Technological enhancements and introduction of new hardware also slash prices of previous iterations.

**Common types of sensors used in fingerprint scanners**

1. **Optical sensors**

Optical sensors capture the image of fingerprints with a specialized digital camera setup. This is the most common type of fingerprint sensors, which are widely available at cheap prices. Optical sensors pose shortcomings like quality of scan is impacted with dirty fingers and they are easier to be tricked than other types of sensors.



Image 3 : Optical fingerprint scanner

1. **Capacitive scanners**

Capacitive scanners make use of pixel array of capacitors instead of visible light, to produce image of fingerprints. Capacitive scanners are hard to forge because they cannot be fooled with fingerprint images. They are more expensive than optical sensors.



Image 4 : Zvetco p5000 capacitive fingerprint scanner

1. **Ultrasound/ultrasonic sensors**

Ultrasonic scanners use very high frequency sound wave to read pattern of fingerprints. Ultrasonic sound waves reflected form the fingertip surface are measured by the sensor and fingerprint pattern image is produced. Performance of ultrasonic sensors stay unaffected by dirtiness of finger surface as it doesn’t capture image like optical sensors.

1. **Thermal line sensors**

These sensors read a fingerprint pattern by measuring temperature variation in fingertip ridges and valleys. It requires finger to be moved over a linearly arranged narrow array of thermal sensors. They are small in size and require finger movement to measure fingerprint patterns.

# 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. The different methods of data collection that were employed are also explained in details.

This chapter also deliberates on the population expected to be affected when this project is implemented. The various ways of how the data was gotten is explained herein.

## Target users of the product

This project was developed to solve fraud problems in the banking sector. The use of cards as a means of authorization is expected to be replaced by use of the fingerprints. Biometric fingerprint scanners placed at the ATM points will be used to scan users fingerprints anytime they want to transact using the ATM.

The bank users will have to be first registered at the bank. The process of registration will include: taking user details such as first name, last name and id number and then scanning the fingerprint of the user. The fingerprint data will be stored in a database and later retrieved when the user tries to authorize himself/herself at the ATM point.

## Target population.

Kenya has many banks. In 2017, this number stood at 42. Currently there are 28 domestic and 14 foreign commercial banks with branches, agencies, and other outlets throughout the country; one mortgage finance company; eight representative offices of foreign banks; eleven licensed deposit taking microfinance institutions; 49 insurance companies; the Post Office Savings Bank with a large network of branches around the country; 79 foreign exchange (forex) bureaus; three licensed credit reference bureaus, 14 money remittance providers and about 200 deposit-taking licensed savings and credit cooperative organizations (SACCOs) with a membership of over 3 million Kenyans. However, the banking sector is essentially dominated by seven tier 1 commercial banks, namely Equity Bank, Kenya Commercial Bank, Barclays Bank of Kenya, Diamond Trust Bank, Cooperative Bank, Central Bank of Africa and Standard Chartered. In addition, smaller banks have emerged and experienced tremendous growth in recent years.

Kenyan Banks have realised tremendous grow in the last five years and have expanded to the east African region. The banking industry in Kenya has also involved itself in automation, moving from the traditional banking to better meet the growing complex needs of their customer and globalization challenges.

There has been increased competition from local banks as well as international banks, some of which are new players in the country. This has served the Kenyan economy well as the customers and shareholder are the ones who have benefited the most.

The target population of this project come from the massive customers of the banks in Kenya. The following table show the Assets and Market share of commercial Banks

|  |  |  |
| --- | --- | --- |
| **Bank** | **Assets (Million K shs.)**  **Weighting:0.33** | **Market share** |
| Kenya Commercial Bank Ltd | 304,112 | 13.1% |
| Equity Bank Ltd | 215,829 | 9.3% |
| Cooperative Bank Ltd | 199,663 | 8.6% |
| Standard Chartered Bank (K) Ltd | 195,493 | 8.4% |
| Barclays Bank of Kenya Ltd | 185,102 | 7.9% |
| CFC Stanbic Bank Ltd | 133,378 | 5.7% |
| **Sub-total** | **1,233,577** | **52.94%** |
| NIC Bank Ltd | 101,772 | 4.4% |
| Diamond Trust Bank Ltd | 94,512 | 4.1% |
| Commercial Bank of Africa (Ltd) | 100,456 | 4.3% |
| I&M Bank Ltd | 91,520 | 3.9% |
| Citibank N.A. | 69,580 | 3.0% |
| National Bank of Kenya Ltd | 67,155 | 2.9% |
| Baroda Bank Ltd | 46,138 | 2.0% |
| Chase Bank Ltd | 49,105 | 2.1% |
| Bank of Africa Ltd | 48,958 | 2.1% |
| Prime Bank Ltd | 43,463 | 1.9% |
| Housing Finance Company of Kenya Ltd | 40,686 | 1.7% |
| Imperial Bank Ltd | 34,590 | 1.5% |
| Family Bank Ltd | 30,985 | 1.3% |
| Bank of India | 24,877 | 1.1% |
| Ecobank Kenya Ltd | 31,771 | 1.4% |
| **Sub-Total** | **875,566** | **37.6%** |
|  |  |  |
| African Banking Corporation Ltd | 19,071 | 0.8% |
| Fina Bank Ltd | 17,150 | 0.7% |
| Consolidated Bank of Kenya Ltd | 18,001 | 0.8% |
| Gulf African Bank Ltd | 13,562 | 0.6% |
| Giro Commercial Bank Ltd | 12,280 | 0.5% |
| Equatorial Commercial Bank Ltd | 14,109 | 0.6% |
| Fidelity Bank Ltd | 11,772 | 0.5% |
| Guardian Bank Ltd | 11,745 | 0.5% |
| Victoria Commercial Bank Ltd | 10,323 | 0.4% |
| Development Bank of Kenya Ltd | 13,417 | 0.6% |
| Habib A.G. Zurich | 9,702 | 0.4% |
| K-Rep Bank Ltd | 9,546 | 0.4% |
| Trans-National Bank Ltd | 8,801 | 0.4% |
| First Community Bank Ltd | 9,959 | 0.4% |
| Paramount Universal Bank Ltd | 7,255 | 0.3% |
| Habib Bank Ltd | 7,014 | 0.3% |
| Oriental Commercial Bank Ltd | 6,220 | 0.3% |
| Credit Bank Ltd | 6,407 | 0.3% |
| Jamii Bora Bank Ltd | 3,480 | 0.1% |
| Middle East Bank (K) Ltd | 5,870 | 0.3% |
| UBA Bank Kenya Ltd | 2,924 | 0.1% |
| Dubai Bank Ltd | 2,584 | 0.1% |
| Charterhouse Bank Ltd | 0 | 0.0% |
| **Sub-Total** | **221,192** | **9.5%** |
| **Grand-Total** | **2,330,335** | **100%** |

Source: Banks Published Financial Statements. December 2012

## Sample population.

It has been observed that ATM points gets rather busy during the weekends, month-ends and mid-month periods as it is when people want to spend money. Weekends people withdraw money to go shopping, attend and arrange parties, refill their food-stock. Most people withdraw money during mid and end-months because it is generally the payday. This causes the ATM points to experience high traffic compared to the other days.

The following table show the traffic at an KCB ATM point located at JKUAT Main gate, Juja, Kiambu county. The data was collected on August 1 2019 - August 31 2019. The data was collected mainly through observation of the ATM users and asking them questions. The guard at the ATM also provided information about the general traffic at the ATM. The data collected can be summarized in the table below:

|  |  |
| --- | --- |
| Day | No. of customers |
| 1 | 77 |
| 2 | 70 |
| 3 | 72 |
| 4 | 66 |
| 5 | 67 |
| 6 | 60 |
| 7 | 61 |
| 8 | 55 |
| 9 | 50 |
| 10 | 50 |
| 11 | 49 |
| 12 | 53 |
| 13 | 68 |
| 14 | 68 |
| 15 | 66 |
| 16 | 71 |
| 17 | 77 |
| 18 | 80 |
| 19 | 67 |
| 20 | 50 |
| 21 | 51 |
| 22 | 45 |
| 23 | 44 |
| 24 | 40 |
| 25 | 49 |
| 26 | 50 |
| 27 | 49 |
| 28 | 66 |
| 29 | 65 |
| 30 | 63 |
| 31 | 69 |
| **Total** | 1868 |
| **Average per day** | 61 |
| **Average per hour** | 2 |

## Methods of data collection.

1. **Secondary data sources.**

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 increased knowledge about the field of study.

Information from this sources helped to understand better the problems facing the current technology employed in the ATM. They provided data on the fraud cases that face the magnetic card technology.

Published research documents from the internet came in handy to explain the concepts of biometric as a useful means of identification.They helped to explain how previous biometric implementation were done and their shortcomings. The documents also explained how to extract useful features of a fingerprint that uniquely differentiated people and how these features could be stored securely in a database. The links to the research documents are provided below:

1. <https://www.ijirset.com/upload/2017/november/77_Fingerprint%20Based%20Atm%20System.pdf>
2. <http://www.bis.org/events/cbcd06e.pdf>
3. https://web.archive.org/web/20161223062608/https://www.rbrlondon.com/about/G20\_Press\_Release\_091015.pdf
4. <http://www.ijeijournal.com/papers/Vol.3-Iss.11/D030112228.pdf>
5. https://web.archive.org/web/20190211183232/http://www.tmgejournal.com/pdfs/vol9-no1/Drivers-and-Barriers-of-Adoption.pdf
6. <https://www.ijcsmc.com/docs/papers/April2014/V3I4201409.pdf>
7. <https://lra.le.ac.uk/bitstream/2381/8163/1/ATM_v7_wtables.pdf>
8. <https://www.emvco.com/wp-content/plugins/pmpro-customizations/oy-getfile.php?u=/wp-content/uploads/documents/EMV_v4.3_Book_2_Security_and_Key_Management_20120607061923900.pdf>
9. <http://www.chipandpin.co.uk/reflib/Consumer_digi-guide_Post_14_Feb_FINAL.PDF>
10. <http://www.clpex.com/Information/Pioneers/galton-1892-fingerprints-lowres.pdf>
11. [https://web.archive.org/web/20061013094924/http://www.clpex.com/Information/Pioneers/henry-classification.pdf](https://web.archive.org/web/20061013094924/http:/www.clpex.com/Information/Pioneers/henry-classification.pdf)
12. <http://www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf>
13. **Observation.**

Observation involved watching, at a distance, people being registered at the bank. Customer information was keyed into the computer and the customer was asked to come up with a four digit key to be used as password. This information would then be used to process the ATM cards.

An ATM point was observed and recordings of data collected were presented for analysis. This enabled one to understand the amount of traffic expected on the system.

The guard at the ATM was also helpful in observing how customers were having trouble with the smart cards.

1. **Questionnaires.**

Questionnaire papers that asked people for data were prepared and provided to the project stakeholders to fill. The questionnaire was given to the customer at the bank and at the ATM point.

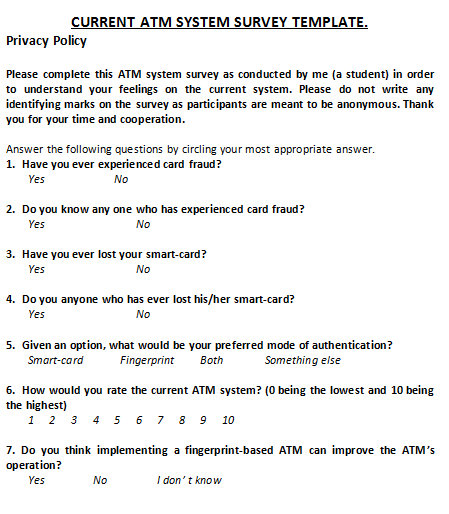


Image 5 : questionnaire used

## System requirements

System requirements are the configuration that a system must have in order for a hardware or software application to run smoothly and efficiently. Failure to meet these requirements can result in installation problems or performance problems. The former may prevent a device or application from getting installed, whereas the latter may cause a product to malfunction or perform below expectation or even to hang or crash

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

The hardware requirement of the system will be as follows:

|  |  |  |  |
| --- | --- | --- | --- |
|  | ATM client application | Bank teller application | Server application |
| OS | Windows 7 or later | Windows 7 or later | Windows 7 or later |
| Processor | Intel Quad core (2.1 GHz) | Intel Quad core(2.1 GHz) | Intel Quad core (2.1 GHz) |
| Memory size | 255Mb | 1Gb | 100Gb |
| Network | Broadband internet connection | Broadband internet connection | Broadband internet connection |
| RAM | 254Mb | 1Gb | 1Gb |
| Peripheral | Fingerprint scanner | Fingerprint scanner |  |

The software requirement of the system will be as follows:

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

## 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.

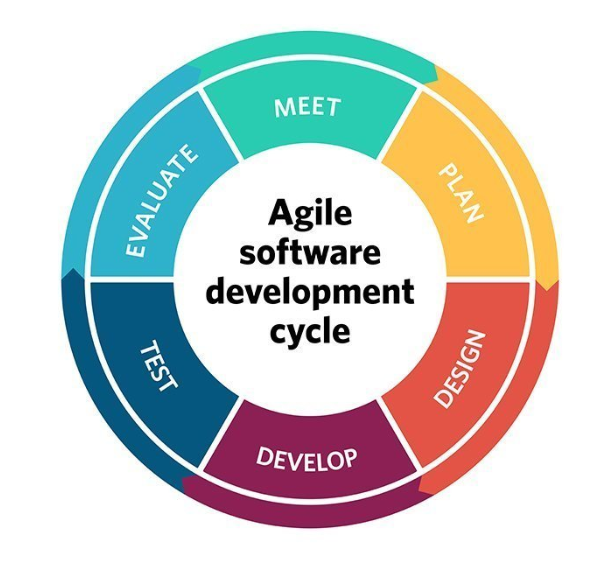


Figure 2: Agile software development cycle

## 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 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.

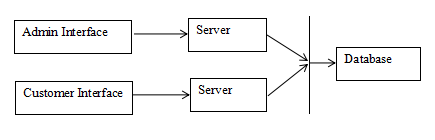


Figure 3 : Architecture of the system

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)

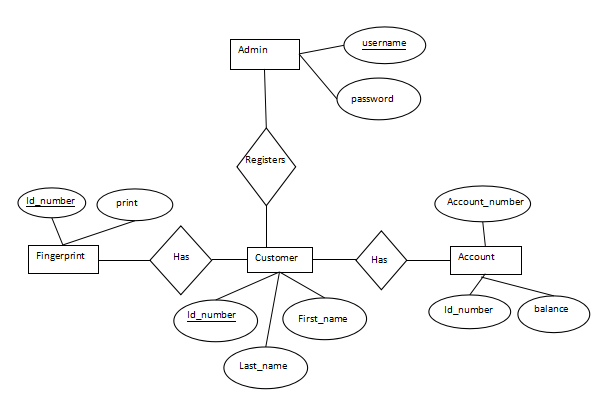


Figure 4 : Entity-Relationship diagram for the proposed system

Database Tables:

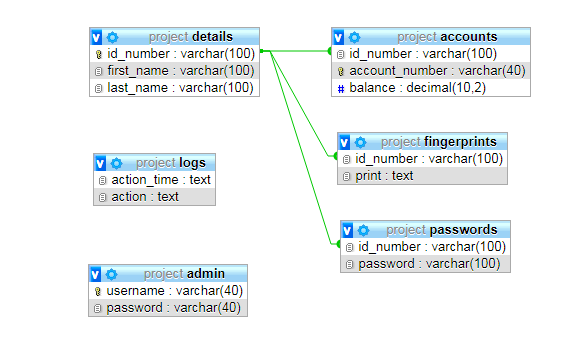


Figure 5 : Logical design for the database

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.

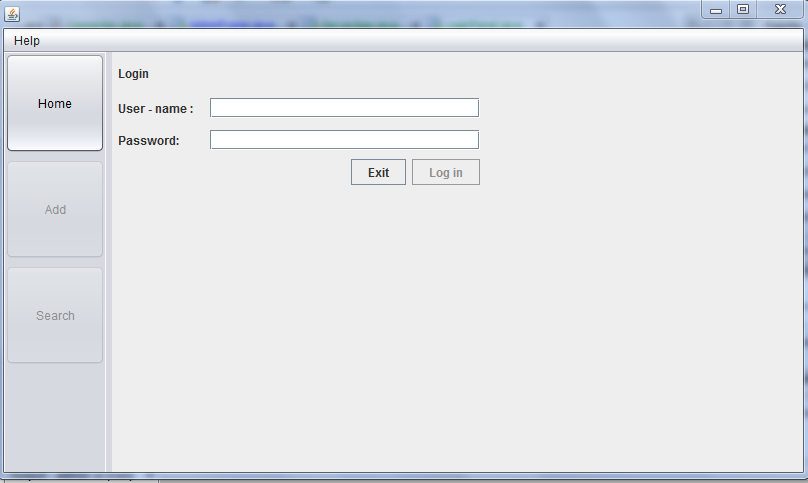


Figure 6 : Admin login interface

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:-

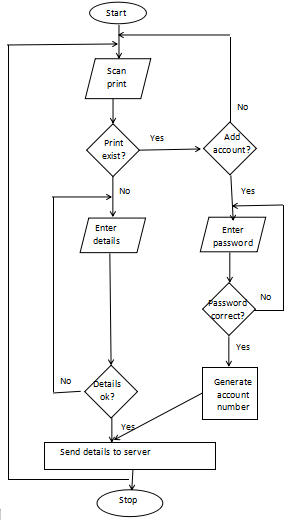


Figure 7 : Flow chart for adding a customer

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.

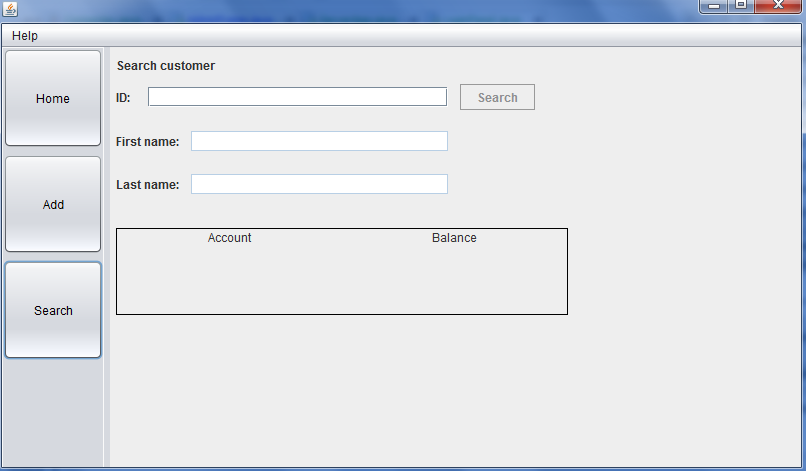


Figure 8 : Searching interface

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.

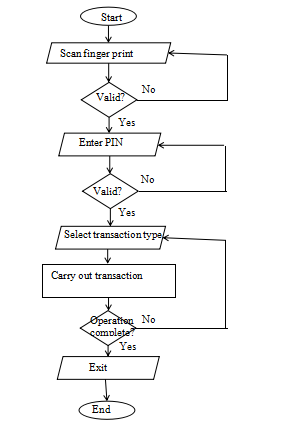


Figure 9 : Authentication phase flow chart diagram

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.

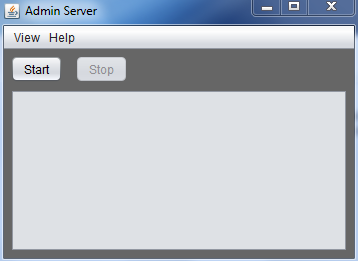


Figure 10 : Server interface

# System Implementation

Introduction

In the implementation of the project is explained. The chapter describes the implementation of the project and how the project transited from design to final product. All the technologies used for each module are stated and explained, where each technology was used and why the technology the technology was used.

Coding language.

The programming language used to code the project was Java. Java language was chosen due to its advantageous features and its immense libraries. The most important features of java include:-

1. Simple - Java is easy to learn and its syntax is quite simple, clean and easy to understand.The confusing and ambiguous concepts of C++ are either left out in Java or they have been re-implemented in a cleaner way.
2. Platform independent - Unlike other programming languages such as C, C++ etc which are compiled into platform specific machines. Java is guaranteed to be write-once, run-anywhere language. On compilation Java program is compiled into bytecode. This bytecode is platform independent and can be run on any machine, plus this bytecode format also provide security. Any machine with Java Runtime Environment can run Java Programs

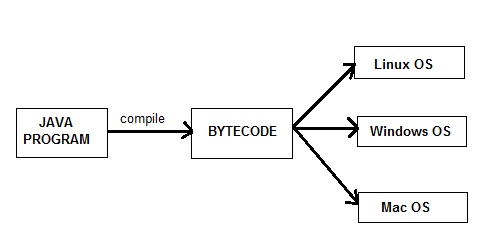


Image 6 : Java program compilation

1. Object-oriented - Java is a fully object-oriented programming language. It has all OOP features such as [abstraction](https://www.codejava.net/java-core/the-java-language/what-is-abstraction-in-java-the-why-and-the-truth" \t "https://www.codejava.net/java-core/_blank), [encapsulation](https://www.codejava.net/java-core/the-java-language/what-is-encapsulation-in-java-the-what-why-and-how" \t "https://www.codejava.net/java-core/_blank), [inheritance](https://www.codejava.net/java-core/the-java-language/what-is-inheritance-in-java-the-what-why-and-how" \t "https://www.codejava.net/java-core/_blank) and [polymorphism](https://www.codejava.net/java-core/the-java-language/what-is-polymorphism-in-java-the-what-how-and-why" \t "https://www.codejava.net/java-core/_blank). object-oriented design is a programming technique that focuses on the data (= objects) and on the interfaces to that object
2. Secured - The Java platform is designed with security features built into the language and runtime system such as static type-checking at compile time and runtime checking (security manager), which let you creating applications that can’t be invaded from outside
3. Robust - Java is intended for writing programs that must be reliable in a variety of ways. Java puts a lot of emphasis on early checking for possible problems, later dynamic (runtime) checking, and eliminating situations that are error-prone. . . The single biggest difference between Java and C/C++ is that Java has a pointer model that eliminates the possibility of overwriting memory and corrupting data.
4. Architecture neutral - The compiler generates an architecture-neutral object file format—the compiled code is executable on many processors, given the presence of the Java runtime system. The Java compiler does this by generating bytecode instructions which have nothing to do with a particular computer architecture. Rather, they are designed to be both easy to interpret on any machine and easily translated into native machine code on the fly.
5. High performance - While the performance of interpreted bytecodes is usually more than adequate, there are situations where higher performance is required. The bytecodes can be translated on the fly (at runtime) into machine code for the particular CPU the application is running on. With the use of Just-In-Time compilers, Java enables high performance. r, the just-in-time compilers have become so good that they are competitive with traditional compilers and, in some cases, even outperform them because they have more information available. For example, a just-in-time compiler can monitor which code is executed frequently and optimize just that code for speed. A more sophisticated optimization is the elimination (or “inlining”) of function calls. The just-in-time compiler knows which classes have been loaded. It can use inlining when, based upon the currently loaded collection of classes, a particular function is never overridden, and it can undo that optimization later if necessar
6. Multi-threaded - With Java's multithreaded feature it is possible to write programs that can perform many tasks simultaneously. This design feature allows multiple fingerprints to be matched at the same time thus saving time.
7. Distributed - Java has an extensive library of routines for coping with TCP/IP protocols like HTTP and FTP. Java applications can open and access objects across the Net via URLs with the same ease as when accessing a local file system. This feature allowing sending of client and server application data to and fro across a network.
8. Dynamic - In a number of ways, Java is a more dynamic language than C or C++. It was designed to adapt to an evolving environment. Libraries can freely add new methods and instance variables without any effect on their clients. In Java, finding out runtime type information is straightforward. This is an important feature in the situations where code needs to be added to a running program.

Database.

Customer data was stored for later retrieval and use during the authentication phase. During registration of a customer, the teller application receives the data entered by the teller and sends it to the server on command. Upon receiving the data, the server application process the data before sending it to the database for storage.

The project used MySQL database for information storage. MySQL is a free-to-use, open-source database that facilitates effective management of databases by connecting them to the software. It is a stable, reliable and powerful solution with advanced features like the following:

1.    Data Security - MySQL is globally renowned for being the most secure and reliable database management system used in popular web applications like WordPress, Drupal, Joomla, Facebook and Twitter. The data security and support for transactional processing that accompany the recent version of MySQL, can greatly benefit a business that involves frequent money transfers.

2.    On-Demand Scalability - MySQL offers unmatched scalability to facilitate the management of deeply embedded apps using a smaller footprint even in massive warehouses that stack terabytes of data. On-demand flexibility is the star feature of MySQL. This open source solution allows complete customization to eCommerce businesses with unique database server requirements.

3.    High Performance - MySQL features a distinct storage-engine framework that facilitates system administrators to configure the MySQL database server for a flawless performance. MySQL is designed to meet the most demanding applications while ensuring optimum speed, full-text indexes and unique memory caches for enhanced performance.

4.    Round-the-clock Uptime - MySQL comes with the assurance of 24X7 uptime and offers a wide range of high availability solutions like specialized cluster servers and master/slave replication configurations.

5.    Comprehensive Transactional Support - MySQL tops the list of robust transactional database engines available on the market. With features like complete atomic, consistent, isolated, durable transaction support, multi-version transaction support, and unrestricted row-level locking, it is the go-to solution for full data integrity. It guarantees instant deadlock identification through server-enforced referential integrity.

6.    Complete Workflow Control - With the average download and installation time being less than 30 minutes, MySQL means usability from day one. Whether the platform is Linux, Microsoft, Macintosh or UNIX, MySQL is a comprehensive solution with self-management features that automate everything from space expansion and configuration to data design and database administration.

7.    Reduced Total Cost of Ownership - Using MySQL as the database allow significant cost savings on the projects. The dependability and ease of management that accompany MySQL save troubleshooting time which is otherwise wasted in fixing downtime issues and performance problems.

8.    The Flexibility of Open Source - All the fears and worries that arise in an open source solution can be brought to an end with My SQL’s round-the-clock support and enterprise indemnification. The secure processing and trusted software of MySQL combine to provide effective transactions for large volume projects. It makes maintenance, debugging and upgrades fast and easy while enhancing the end-user experience.

Connecting to the database

To connect the java program code with the MySQL database. MySQL provides connectivity for client applications developed in the Java programming language with MySQL Connector/J, a driver that implements the [Java Database Connectivity (JDBC) API](https://www.oracle.com/technetwork/java/javase/jdbc/) and also [MySQL X DevAPI](https://dev.mysql.com/doc/x-devapi-userguide/en/).

MySQL Connector/J 8.0 is a JDBC Type 4 driver that is compatible with the [JDBC 4.2](https://docs.oracle.com/javase/8/docs/technotes/guides/jdbc/) specification. The Type 4 designation means that the driver is a pure Java implementation of the MySQL protocol and does not rely on the MySQL client libraries.

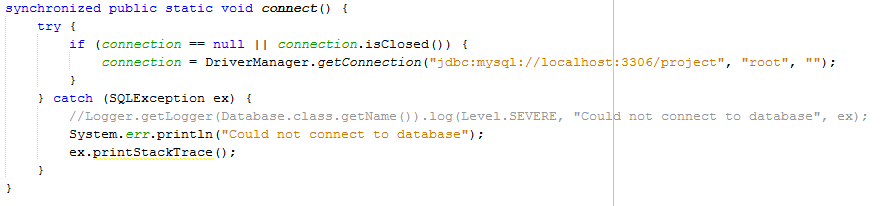


Image 7 : Server code to connect to database

Network

The customer application and the bank teller application connect to the server application using a network. The different applications use sockets technology to communicate having been allocated each a unique port number.

Sockets provide the communication mechanism between two computers using TCP. A client program creates a socket on its end of the communication and attempts to connect that socket to a server.

When the connection is made, the server creates a socket object on its end of the communication. The client and the server can now communicate by writing to and reading from the socket.

Connection of server and client application

The java.net.Socket class represents a socket, and the java.net.ServerSocket class provides a mechanism for the server program to listen for clients and establish connections with them.

The following steps occur when establishing a TCP connection between two computers using sockets −

The server instantiates a ServerSocket object, denoting which port number communication is to occur on.

The server invokes the accept() method of the ServerSocket class. This method waits until a client connects to the server on the given port.

After the server is waiting, a client instantiates a Socket object, specifying the server name and the port number to connect to.

The constructor of the Socket class attempts to connect the client to the specified server and the port number. If communication is established, the client now has a Socket object capable of communicating with the server.

On the server side, the accept() method returns a reference to a new socket on the server that is connected to the client's socket.

After the connections are established, communication can occur using I/O streams. Each socket has both an OutputStream and an InputStream. The client's OutputStream is connected to the server's InputStream, and the client's InputStream is connected to the server's OutputStream.

TCP is a two-way communication protocol, hence data can be sent across both streams at the same time.

To connect to the server application, the following call is made on the client side program:

Socket socket = new Socket(“127.0.0.1”, 8888)

First argument – IP address of Server. ( 127.0.0.1  is the IP address of localhost, where code will run on single stand-alone machine).

Second argument – TCP Port. (The number representing which application to run on a server.)

To communicate over a socket connection, streams are used to both input and output the data. The socket connection is closed explicitly once the message to server is sent.

The server code run on an independent thread waiting for connections from the clients which are passed to another thread after being received. This ensure that the server can process more that one socket connection. The thread processing the sockets reads data from the socket and processes them, send a reply across the socket again and closes the socket.

The following figure show the code that wait for socket connections:

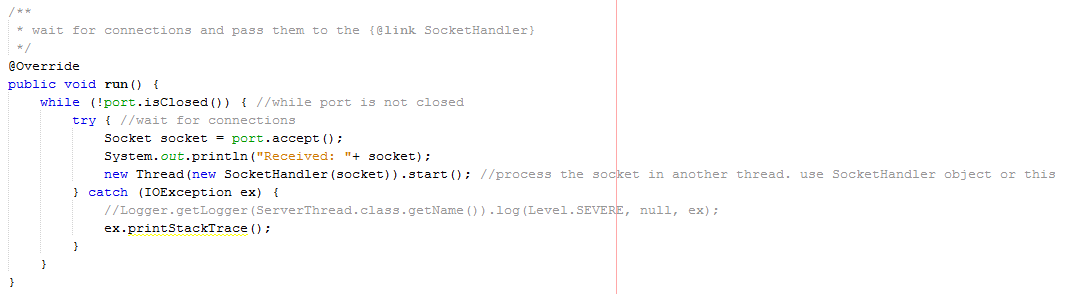


Image 8 : Waiting for connections

Fingerprint matching

The fingerprint template captured by the scanner is first serialized to JSON string. Serialized template can be stored in a database or sent over network. It can be deserialized to the original template to allow matching. Serialized template excludes search structures that FingerprintTemplate keeps to speed up matching. Serialized template is therefore much smaller than in-memory FingerprintTemplate.

Serialization of the fingerprint templates is done at the client side application and the string version sent to the database for storage or matching.

# DISCUSSIONS

Introduction

This chapter explains the findings of the research done prior to project implementation objective by objective. For each objective, the findings are stated and explained, implication of the findings and whether the objective was met or no. Prior to the start of the project, objectives were set for the project to meet. This chapter details the objective and how they have been met.

Objectives

These project objectives describe the intended project’s outcomes: intended and direct, short- and medium-term effects on the target group. The project objective lie within the scope of the project. These objectives are meaningful steps towards a business goals that are accomplished by this project. They communicate the project purpose, direction, value and progress. The following are the objectives accomplished by this project:-

1. Reduce cases of card fraud.
2. Provide efficient alternative form of authorization.
3. Provide easy to use user interface.
4. Store user bio-data in a secure and easily retrievable manner.

Findings

This sub-section explains the findings of trying to accomplish the objectives of the project during its implementation. The objectives that were required to be accomplished are listed with the explanation of how they were accomplished.

1. Reduce cases of card fraud.

This project was developed to counter the rampant cases of card fraud common with the use of ATM cards. This objective was accomplished since the use of fingerprint remove the risk of lost, theft or forgery.

ATM cards can be easily lost or forgotten making it not possible for one to use the ATM. This is disadvantageous to both the bank customer and the banking institution. The lost ATM card can be used to commit fraud when it gets into the wrong hands. The use of fingerprints was found to curb these cases in that fingerprint cannot be lost or duplicated. Human fingerprints are detailed, nearly unique, difficult to alter, and durable over the life of an individual, making them suitable as long-term markers of human identity.

Using fingerprint unique features, we can curb the card fraud activities evident in the card technology. These will reduce money lost to the fraudsters. Fingerprint from before birth and except for resulting in permanantscars,,remain unchanged till death. Each one is known to have unique,immutable fingerprints. Hence fingerprint recognition is most powerful techniques used in field of biometrics.

Each fingerprint is made of a series of RIDGES and FURROWS on the surface of finger. Another feature of a fingerprint are MINUTIAE points. MINUTIAE points are local ridge characteristics. That occur at either a ridge bifurcation or ridge ending. The uniqueness of a fingerprint tcanbe determine by the pattern of ridges and furrows as well as minutiae points.

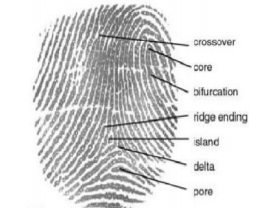


Image 9 : Human finger print

1. Provide efficient alternative form of authorization.

Using the current ATM technology 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. The cards have a [magnetic stripe](https://en.wikipedia.org/wiki/Magnetic_stripe" \o "Magnetic stripe) or a plastic [smart card](https://en.wikipedia.org/wiki/Smart_card" \o "Smart card) with a [chip](https://en.wikipedia.org/wiki/Integrated_circuit" \o "Integrated circuit) that contains a unique card number and some security information such as an expiration date or [CVVC](https://en.wikipedia.org/wiki/Card_Verification_Value_Code" \o "Card Verification Value Code) (CVV).

The use of fingerprint has been observed to be more efficient compared to the current ATM card technology. Efficiency(as herein used) is the (often measurable) ability to avoid wasting materials, energy, efforts, money, and time in doing something or in producing a desired result. In a more general sense, it is the ability to do things well, successfully, and without waste(Longman Dictionary of Contemporary English). In more mathematical or scientific terms, it is a measure of the extent to which input is well used for an intended task or function (output). The efficiency of the project outcome comprises the capability of the application of effort to authenticate the bank customers with a minimum amount or quantity of waste, expense, or unnecessary effort.( [Sickles, R., & Zelenyuk, 2019)](https://assets.cambridge.org/97811070/36161/frontmatter/9781107036161_frontmatter.pdf)

This project aims at introducing fingerprint as a new form of authorization at the bank. The use of fingerprint is efficient in that one is always in possession and therefore can not be lost or forgotten to cause inconvenience. Fingerprints have been used in many sectors for identification of people. These sectors include Forensic laboratories, crime scene investigations, detection of drug use and police force databases. In all these sectors it has been seen that the use of fingerprint is highly efficient in that:-

1. It is highly accurate. No two people have the same fingerprint and therefore no one can be falsely authorized.
2. It is the most economical technique. Every person has a fingerprint and therefore the bank do not have to manufacture them fore their customers. Also the cost of replacing lost smart cards is solved by the use of fingerprints as a form of authorization.
3. It is easy to use. The use of fingerprint authentication only involves placing ones finger on the biometric scanner.
4. Easy to use user interface.

The project aims was to develop an application that was user friendly to the user. This was achieved by developing an application that was neat and user friendly. By use of GUI to design the application, the application become more natural, easy and intuitive to use and communicate with the user. The use of GUI bring a lot of advantages to the application eg making computer operation more intuitive, and thus easier to learn and use, providing users with immediate, visual feedback about the effect of each action, GUI allows multiple programs and/or instances to be displayed simultaneously , Users do not need to know any programming languages etc.

A good interface makes it easy for users to tell the computer what they want to do, for the computer to request information from the users, and for the computer to present understandable information. Clear communication between the user and the computer is the working premise of good UI design.

Good interfaces are:  
1. Clear - A clear interface helps prevent user errors, makes important information obvious, and contributes to ease of learning and use.

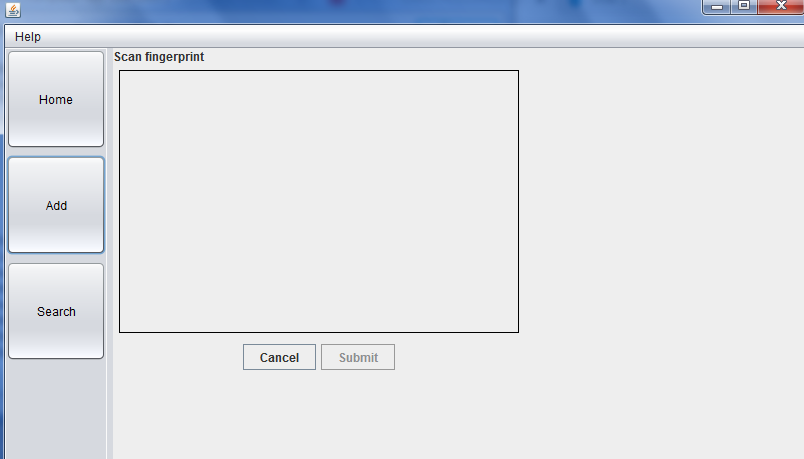


Image 10 : Scanning a finger print

2. Consistent - A consistent interface allows users to apply previously learned knowledge to new tasks. Effective applications are both consistent within themselves and consistent with one another.  
3. Simple - The best interface designs are simple. Simple designs are easy to learn and to use and give the interface a consistent look. A good design requires a good balance between maximizing functionality and maintaining simplicity through progressive disclosure of information.  
4. User-Controlled The user, not the computer, initiates and controls all actions.  
5. Direct - Users must see the visible cause-and-effect relationship between the actions they take and the objects on the screen. This allows users to feel that they are in charge of the computer's activities.  
6. Forgiving - Users make mistakes. User actions should be reversible. A good interface facilitates exploration and trial and error learning.   
7. Provide feedback - Keep the user informed and provide immediate feedback. Also, ensure that feedback is appropriate to the task.

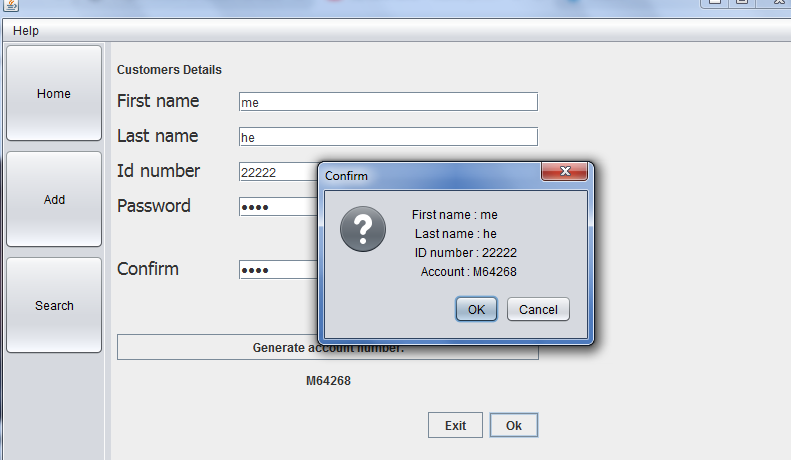


Image 11 : user confirming action

8. Aesthetic - Every visual element that appears on the screen potentially competes for the user's attention. Provide an environment that is pleasant to work in and contributes to the user's understanding of the information presented.

1. Store user bio-data in a secure and easily retrievable manner.

The bio - data used in the project are user fingerprint. The fingerprints are acquired during user registration at the bank through scanning. The fingerprint data and other user data are then sent to the server and stored in a database. Before storage the fingerprints are encrypted using SHA -512 encryption technique. This ensures that data stored in the database is not comprehensible to human in case the database confidentiality is sabotaged. Other user information stored are also encrypted.

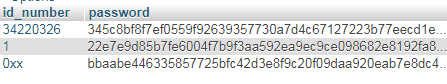


Image 12 : User encrypted passwords

SHA-2 (Secure Hash Algorithm 2) is a set of [cryptographic hash functions](https://en.wikipedia.org/wiki/Cryptographic_hash_function" \o "Cryptographic hash function) designed by the United States [National Security Agency](https://en.wikipedia.org/wiki/National_Security_Agency" \o "National Security Agency) (NSA) (Wouter Penard, Tim van Werkhoven, 2016). They are built using the [Merkle–Damgård structure](https://en.wikipedia.org/wiki/Merkle%E2%80%93Damg%C3%A5rd_construction" \o "Merkle–Damgård construction), from a [one-way compression function](https://en.wikipedia.org/wiki/One-way_compression_function" \o "One-way compression function) itself built using the [Davies–Meyer structure](https://en.wikipedia.org/wiki/One-way_compression_function" \l "Davies%E2%80%93Meyer" \o "One-way compression function) from a (classified) specialized block cipher. The SHA-2 family consists of six hash functions with [digests](https://en.wikipedia.org/wiki/Cryptographic_hash_function" \l "message_digest" \o "Cryptographic hash function) (hash values) that are 224, 256, 384 or 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256. Currently, the best public attacks break [preimage resistanc](https://en.wikipedia.org/wiki/Preimage_attack" \o ")e for 57 out of 80 rounds of SHA-512 (Dmitry Khovratovich, Christian Rechberger & Alexandra Savelieva, 2011).

The use of SHA-512 encryption scheme to secure user data ensure that only authorized parties can access it and those who are not authorized cannot. User administrators who have access to database should not be able to retrieve customers’ confidential data. Encrypting the data before storage ensure that the admin can not make out what the user data

1. Fast processing of user authentication.

Fast processing of user authentication was hindered by the fact that matching of customer fingerprint takes time. Fingerprint present a lot of data which are required to be matched and check if two fingerprint match. The slowness can be further be influenced by a not powerful computer. Using a highly powerful computer is recommended for fingerprint matching.

To improve the speed of matching, the process has been moved to the server program. Assuming that the server will be a more powerful computer compared to client.

Also the matching of a fingerprint against the fingerprints stored in the database is done by separate threads. Using threads, one fingerprint can be matched to multiple fingerprints from the database at the same time. This reduces the time taken to get a matching fingerprint from a database containing a lot of fingerprint data. Also use of multithreading make it possible to share resources such as the memory and make the program more responsive as one fingerprint matching may be slow while the other are continuing.

1. Efficient transfer of data across the Network.

The project aimed at creating an application that sends data across the network efficiently to prevent data loss or alteration. .This was achieved through encoding of data before being sent then decoding it on the receiving end. Since [encoding](https://www.medianova.com/encoding-platform/" \t "https://www.medianova.com/en-blog/2015/09/21/_blank) removes redundancies from data, the size of the data sent will be a lot smaller. This results in faster input speed.

The purpose of encoding is to transform data so that it can be properly (and safely) consumed by a different type of system, e.g. binary data being sent over email, or viewing special characters on a web page. The goal is not to keep information secret, but rather to ensure that it’s able to be properly consumed.

Encoding transforms data into another format using a scheme that is publicly available so that it can easily be reversed. It does not require a key as the only thing required to decode it is the algorithm that was used to encode it.

Encoding and decoding of data was done using the Base64 model encoding scheme. , Base64 is a group of [binary-to-text encoding](https://en.wikipedia.org/wiki/Binary-to-text_encoding" \o "Binary-to-text encoding) schemes that represent [binary data](https://en.wikipedia.org/wiki/Binary_data" \o "Binary data) in an [ASCII](https://en.wikipedia.org/wiki/ASCII" \o "ASCII) string format by translating it into a [radix](https://en.wikipedia.org/wiki/Radix" \o "Radix)-64 representation. Base64 is designed to carry data stored in binary formats across channels that only reliably support text content. Given below is The Base64 index table

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Index | Binary | Char |  | Index | Binary | Char |  | Index | Binary | Char |  | Index | Binary | Char |
| 0 | 000000 | A | 16 | 010000 | Q | 32 | 100000 | g | 48 | 110000 | w |
| 1 | 000001 | B | 17 | 010001 | R | 33 | 100001 | h | 49 | 110001 | x |
| 2 | 000010 | C | 18 | 010010 | S | 34 | 100010 | i | 50 | 110010 | y |
| 3 | 000011 | D | 19 | 010011 | T | 35 | 100011 | j | 51 | 110011 | z |
| 4 | 000100 | E | 20 | 010100 | U | 36 | 100100 | k | 52 | 110100 | 0 |
| 5 | 000101 | F | 21 | 010101 | V | 37 | 100101 | l | 53 | 110101 | 1 |
| 6 | 000110 | G | 22 | 010110 | W | 38 | 100110 | m | 54 | 110110 | 2 |
| 7 | 000111 | H | 23 | 010111 | X | 39 | 100111 | n | 55 | 110111 | 3 |
| 8 | 001000 | I | 24 | 011000 | Y | 40 | 101000 | o | 56 | 111000 | 4 |
| 9 | 001001 | J | 25 | 011001 | Z | 41 | 101001 | p | 57 | 111001 | 5 |
| 10 | 001010 | K | 26 | 011010 | a | 42 | 101010 | q | 58 | 111010 | 6 |
| 11 | 001011 | L | 27 | 011011 | b | 43 | 101011 | r | 59 | 111011 | 7 |
| 12 | 001100 | M | 28 | 011100 | c | 44 | 101100 | s | 60 | 111100 | 8 |
| 13 | 001101 | N | 29 | 011101 | d | 45 | 101101 | t | 61 | 111101 | 9 |
| 14 | 001110 | O | 30 | 011110 | e | 46 | 101110 | u | 62 | 111110 | + |
| 15 | 001111 | P | 31 | 011111 | f | 47 | 101111 | v | 63 | 111111 | / |
| padding | | = |  |  |  |  |  |  |  |  |  |  |  |  |

# SUMMARY, RECOMMENDATIONS AND CONCLUSIONS.

## Summary.

The project comes up with a system that is able to register bank users and then validate them at the ATM using their fingerprint. Fingerprints was chosen mainly because of its uniqueness among all people. Also , fingerprint technology is easy to use and would thus require less training. This documentation presents these and many other reason for the use of fingerprints as the means of bank customers authorization.

The documentation also explains how the current ATM systems work and how these project is aiming to improve it. The shortcomings of the current system are highlighted and how the proposed system aims at solving them.

Other biometric forms of authorization are explained in the documentation. The documentation explore the different areas that need to be factored when considering to use a biometric technology. These factors include cost, ease of use, cultural perception, stability, accuracy, devices required, reliability, attacks precaution etc. The reason as to why fingerprint was preferred to the other forms are also explained.

The implementation of the system is also explained with focus on the technology use and the area the technology was used. Reason for using the technology to implement the system are outlined and the explained. The methodology used for implementation is given.

The system designs are outlined herein detailing how all the different parts of the system were designed. The flowchart diagrams used to design the system are provided. The documentation also record the tables used for creating the database and their purpose in storing the data.

The security aspects of the system are also discussed. The documentation discus how the security of the system are implemented. The encryption process is explained together with the different that were used. The different schemes that are currently available are explored and their strengths noted. The documentation explain encryption scheme that is implemented on the system and the reasons for its consideration.

## Recommendations.

Banking institutions are recommended to consider implementing the system to be as the new technology for the ATM. It is high time to reduce the rampant cases of card fraud facing the smart card technology

## Conclusions

# 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.

Dmitry Khovratovich, Christian Rechberger & Alexandra Savelieva (2011). ["Bicliques for Preimages: Attacks on Skein-512 and the SHA-2 family"](http://eprint.iacr.org/2011/286.pdf) (PDF). IACR Cryptology ePrint Archive. 2011:286.