AN IMPROVED FRAMEWORK FOR ELECTRONIC BANKING SECURITY

OLADIPO OLATUNDE ISAAC

15010301020

BEING A PROJECT SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE AND MATHEMATICS, COLLEGE OF BASIC AND APPLIED SCIENCES

IN FUFILLMENT OF THE REQUIREMENTS FOR THE
AWARD OF DEGREE OF BACHELOR OF SCIENCE
MOUNTAIN TOP UNIVERSITY, IBAFO,
OGUN STATE, NIGERIA

2020

Certification

This is to certify that this project, **AN IMPROVED FRAMEWORK FOR ELECTRONIC BANKING SECURITY** was carried out and submitted by **OLADIPO OLATUNDE ISAAC**(Matriculation Number: 15010301020) in fulfillment of the requirements for the degree of **BACHELOR OF SCIENCE (Computer Science)**, is hereby accepted

_____________________________ (Signature and Date)
Dr. F. A.KASALI
Supervisor

_______________________________ (Signature and Date)
Dr. I. O.AKINYEMI
Head of Department

Accepted as fulfillment of the requirement for the degree of BACHELOR OF SCIENCE (Computer science)

______________________________ (Signature and Date)
Prof. A. I. AKINWANDE
Dean, College of Basic and Applied Science

Dedication

This project work is dedicated to the giver of life and wisdom: The God Almighty

Acknowledgement

I owe my profound gratitude to God Almighty who gave the wisdom, knowledge, understanding, resources, health and divine assistance to me from the beginning to the completion of this work. His undyning love, grace and mercies saw me through the challenges encounterd during the course of this project.

My hearfelt thanks also to;

My supervisor Dr. F.A. Kasali, lecturer like mother, sister, colleague, friend, the mother of all who specially took interest in my project work and taking the time out of no time to attend to me and guided me all along to the successful completion of this work right from day one.

The Head of Department, Computer Science and Mathematics Dr. I.O. Akinyemi, for his efforts, constant encouragement, guidance and support of all the academic staff;Dr. F.A. Kasali, Dr. Adewole, Dr. Adamu O. B, Dr. Okunoye O. B, Dr. Ojesanmi O. A, Dr. Peter A. I. and non-academic staff of the Department of Computer Science and Mathematics.

My parents Mrand Mrs. Oladipo. I will always be thankful to you to them of inestimable value who sacrificed wealth, pleasure and great moments of their lives for the sake of my success and also to my wonderful aunty and grama Mrs Toyin Ayodele and Mrs Florence Oladipo for their prayers, support and encouragement.

Mymentors, Mr. O.J. Osaghae d’oracle himself, Mr. A. Akindeji for there guidance, teachings and contributions that have brought out positive values in me, and making my stay worthwhile. The anointed man of Heaven too, my lecturer Late Dr. M. O. Oyetunji., for the fatherly love, teachings, encouragement, word of God and advice. I say a big thank you and may your gentle soul rest in perfect peace of God sir.

My pastors, Pst Olumide Adeshina , Pst Olumide Tanimowo for all the prayers, advice, word of God and fatherly love. God bless you all.

I acknowledge the constant support of Multi-Grace Venture who had contributed to my academic achievement financially and morally, right from the begining up till now. I pray God would continue to increase your knowledge ma.

My friends, Olusegun Timilehin, Oluwatofunmi, Deborah Matthewfor the word of advice,assistance, encouragement and selfless efforts in ensuring the achievement of this work, various brain storming sessions, prayer and provision of tips and helpful materials for this project work. God bless you deeply.

Mountain Top University colleagues, I sincerely appreciate for their help in one way or the other and support during the period of working on this project. I say God bless you all

TABLE OF CONTENTS

LIST OF FIGURES

Figure **Page**

ABSTRACT

Security is a huge factor in the design of e-banking applications and systems. The current means of authentication which involve the use of some form of username and password Unique Identification Number (PIN) or a Personal Identification Number tends to high vulnerability and attacks. Hence, the focus of this study was to design an enhanced ATM using a multimodal biometrics system.

In order to achieve its aim and objectives, an extensive study was done to identify current frameworks developed to improve the security of ATMs. This project work was built and implemented on WAMP.

The improved framework for electronic banking system created helped to provide a more secure to authenticate users. The framework provided a more efficient way to carry out banking operations.

The improved framework for electronic banking system proved very useful in authenticating users and protecting the user’s identity compared to the traditional method of Account Identification Numbers (PIN) and passwords. It was recommended that the framework be improved upon to increase the scope and productivity of the system.

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND TO THE STUDY

Due to internet technological advances such as online commerce and safe information sharing, electronic banking has grown and advanced steadily over the last ten to fifteen (10-15) years. E-banking allows people from almost anywhere in the world to connect via the Internet with their banking accounts. The electronic banking system faces many new technologies: consumer demand for service anytime, anywhere, product time-to-market imperatives, and highly complicated back-office integration issues. This interface enables clients to access their bank accounts, review recent transactions and request a current statement, transfer cash, reorder checks, display current bank rates and product details.

The deployment of banking services and products directly to customers over electronic and communication networks can be described as e-banking (Singh & Malhortra, 2009). Automatic delivery of modern and traditional banking products and services directly to clients via electronic, automated communication networks (Chai, 2015). Automated Teller Machines (ATMs), direct dial-up services, private and public networks, the Internet, televisions, handheld computers, and telephones are used in these electronic and networking networks. Among these innovations, the growing penetration of personal computers, the comparatively easier access to the Internet and, in particular, the broader distribution of mobile phones have brought e-banking to the notice of the majority of banks.

The term 'Biometrics' has also recently used as a guide to the new area of technologies dedicated to the identification of people based on their biological features, such as retinal scans, iris detection, fingerprints, deoxyribonucleic acid (DNA), facial recognition, hand geometry, recognition of signatures, etc. Biometrics is used for identification and management of entryA wide range of apps in today's world require unique and reliable methods of authentication to verify a person's identity person requesting their service. Some examples of such applications are safe access to homes, operating networks, smartphones, cellular phones, account records, memory such as Universal Serial Bus (USB) sticks, and many more (Jain & Ross, 2015).

Two forms of biometric details are:

Biometrics Physiological: This will identify your fingerprint, word, deoxyribonucleic acid (DNA), side geometry, face recognition, etc.

Behaviouralbiometrics: These are connected to the actions of an individual, such as typing speed, gait, etc.It is very difficult to replicate, exchange and spread biometric characteristics such as universality, distinctiveness, measurability, permanence, performance, acceptability, circumvention and, most significantly, the individuality that cannot be missed or forgotten. An person must be physically present, using biometric information, to use his/her biometric information for authentication purposes. This form of authentication will allow customers to log into the bank server remotely to access their account using their bank ID and biometrics (Greeta, Swati, &Aaradhana, 2012). The goal of this study is therefore to develop and enforce an improved ATM using a multimodal biometrics system to optimize the availability, security and addition of user data confidentiality.

1.2 STATEMENT OF THE PROBLEM

The first thing that comes to mind when talking about e-banking is protection, In the use of Automated Teller Machines (ATM) in particular.Computer technology developers working on e-banking applications will pay more attention to the fact that security and authentication issues when working on e-banking applications than they do when working on other types of applications.

The rate of change in cyber security measures these days seems to be equivalent to the rate at which loopholes and backdoors are discovered. It seems the black hats are becoming more unrelenting.

For most e-banking applications, authentication mechanisms containing some type of username and a static Password or Number for Personal Identification are used. Over time, different types of attacks such as phishing (Identity Theft) have proved resistant to this method of authentication. Alternative and theoretically more reliable technologies must be implemented for security assurance not to slip below thresholds that are appropriate for applications such as e-banking. Security/authentication remains the big e-banking problem, therefore.

1.3 AIM AND OBJECTIVES

This research aims to design and implement an improved ATM using biometrics. The objectives of this study are to:

i. Study existing ATM authentication techniques.
ii. Design an interface that will demonstrate the application of multimodal biometrics for authentication purposes.

1.4 THE PROJECT SCOPE

The e-banking application system that will be used in this study is the ATM (Automated Teller Machine) and this will be programmed to use a fingerprint scanner and a voice recognition system and this, in turn, will grant such user access to his/her account information and allow them to do any transaction after authentication has been done.

1.5 SIGNIFICANCE OF STUDY

This project is expected to identify issues regarding security in e-banking, especially in recent times when most banking operations are carried out online. This study is expected to proffer a foolproof solution to existing security issues in e-banking specific, the use of ATMs. It serves as a bridge between two areas in computing: E-banking and Biometrics as it applies the latter to the former. It is expected that the outcome of this work would be an adaptable framework for existing and newly developing e-banking systems and other systems in which authentication is a key issue.

1.6 RESEARCH METHODOLOGIES

For the first objective to be achieved, an extensive study of literature will be done to identify current frameworks that have been developed to improve the security of ATMs. A current and widely acceptable one will be adapted and improved on.

To achieve the second objective, a multimodal biometrics system that uses both fingerprint and voice trait would be used to enhance the improved framework and consequently implemented using WAMP.

1.7 DEFINITION OF TERMS

ATM: An electronic teller machine is an automated teller machine (ATM) or cash point (British English). telephone system that allows financial institution customers are expected to carry out financial transactions at any time and without the need for human contact with bank employees, such as withdrawals of money, deposits, money transfers or information about accounts inquiries. (Wikipedia,2020).

E-banking: A banking system in which the client makes transactions through the Internet electronically.

WAMP: It is a variant LAMP for Windows-based systems that is mainly constructed as a package kit (Apache, MySQL PHP and). That is the mainly used for internal testing and web development, but can also be used to support websites that are live. (Christensson, P., 2013).

DNA: The molecule that comprises organisms' genetic code is abbreviated as deoxyribonucleic acid. This includes animals, fungi, protists, archaea, and bacteria. In every cell, DNA is in the body and tells cells what proteins to make. (Wikipedia,2020).

USB: A Universal Serial Bus (USB) is a standard interface allowing communication between computers and a host controller, a personal computer, for example, (PC). (Techopedia,2020)

Biometrics: That can be used to show who the person is, pointing to specific details about someone's anatomy, such as the colour variations of their eyes.

Fingerprint Scanners: They are biometric authentication solutions. They are used in other surveillance applications and to open doors.

Voice Recognition: Human voice machine analysis, especially to translate words and phrases or recognize an individual voice.

ID: As a card or bracelet containing official or authorized identity documents, a means of identification.

Virtual Top-Up (VTU): Digital Top Up is a profiteering venture where you can use your mobile device to market services as a retailer to earn a profit.

Access Products: Products which require consumers, generally from remote locations, to access traditional payment instruments electronically.

Chip Card: It is also referred to as an IC card (Integrated Circuit). A card that contains one or more computer chips or integrated circuits used for the validation of personal identity numbers, the acceptance of transactions, the verification of account balances, and the storage of personal information for identification, the collection of data, or the processing of special uses. (Jones 2019)

Interchange of electronic data (EDI): In machine-readable mode, the sharing of knowledge between organizations.

Electronic Money: A monetary value calculated in units of currency deposited in electronic form on an electronic computer in the hands of the user. Via purchasing or conversion, this electronic value may be bought and kept on the computer until decreased.

Mobile Banking: This is a product that helps a bank's customers to use resources as they go.

Clients can make their transactions everywhere, such as account balance, transaction enquiries, stop checks and service orders for other customers, balance requests, account verification, bill payment, the electronic transfer of money, account balances, alerts and records, mobile customer care, account transfer, etc.

POS (Point of Sale) Machine: The payment system that enables credit/debit cardholders to make purchases at sales/purchase locations is a point-of-sale machine.

Smart Card: A card with an embedded computer chip on which it is possible to store and process financial, health, educational, protection and all other kinds of records.

Transaction Alert: When necessary information is to be shared, the warning system also acts as a notification system to reach out to consumers.

Interact: It is a Canadian interbank network for the exchange of electronic financial transactions connecting financial institutions and other businesses.

IVR(interactive voice response): Telephony technology in which someone connects to a device using a touch-tone phone or gathers information from or uploads data to a database.

CHAPTER TWO

LITERATURE REVIEW

2.1 HISTORY OF E-BANKING SYSTEM

E-business has been continuously growing as a new industry during the last decade. In recent years, It's the banking sector that has been leading this movement, and now all banking transactions made via internet apps are often referred to as e-banking. E-banking developments have proliferated in recent years, and the proliferation of a large variety of products has led to rising consumer adoption among these technologies are direct deposit, computer finance, stored value cards and debit cards (Servon&Kaestner, 2008). Customers are drawn to these technologies due to convenience, increasing ease of use and, in some cases, cost savings (Hogarth & Anguelov, 2004).). At a remarkable rate, e-banking has grown. E-banking grew eightfold from 1995 to 2003 (Hogarth & Anguelov, 2004). Online banking use increased 47 percent from late 2002 to early 2005,strong proof that e-banking correlates with better financial management for households.

All companies in particular the small and medium-sized businesses, regardless of their geographical areas, are all e-banking beneficiaries. This covers all forms of commercial transactions carried out on an electronic medium, mainly through the internet.

E-banking brings businesses to consumers without regard to their geographical position. It enables businesses to establish new business connections from various global business partnerships, evaluate new goods and services, and perform market analysis and other inquiries at a minimum expense, both financially and otherwise. (Adrian & Shin, 2008). To achieve some comparative benefits over their larger rivals, smaller community banks, among others, are more interested in using e-banking.

Online banking gives banks a modern and more effective electronic delivery mechanism, in addition to previous e-banking delivery services, Automatic Teller Machines (ATMs) and telephone transaction processing centres (Costanzo, 2000). Although ATMs were first launched in the early 1980s and originally sought to minimize operational costs, in the 1990s, telephone call centres were formed to perform basic transactions and offer remote customer services. E-banking has been an improvement for the banking industry from past electronic distribution systems to open new market possibilities (Ebling, 2001).

For the last two decades, a modern service channel focused on the evolution in information technology has been selected by the banking industry to respond to developments in consumer tastes and needs, increasing non-bank competitiveness, changes in demographic and social patterns, and financial service sector government deregulation (Byers &Lederer, 2001).

Banks have recognised the importance of differentiating themselves across new service delivery networks from other financial institutions in the quest for sustainable strategic advantages in the technological financial services sector (Daniel, 1999).

To enhance their goods and services, banks have historically been at the vanguard for harnessing technologies. Over the years, computer and telecommunication networks have been used to provide a broad spectrum of value-added goods and services. The selection of services and products provided by numerous banks varies greatly in terms of content as well as complexity. In terms of the convenience and expense of purchases, e-banking offers tremendous advantages to customers (Liu, 2008).

The growth in e-banking, as the variety of interface options available for accessing online banking solutions has expanded, has led to a steady increase in the number of customers interacting to a greater extent than before through remote channels. Banks who have opted to maintain large branch networks are re-aligning the positions of workers in these branches in a world of growing internet competition and shifting towards a relationship-driven sales culture (Durkin, 2007).

E-banking has intensified bank-to - bank rivalry, allowed banks to access new markets and thereby extend their geographical scope. Some also see e-banking as a possibility to jump into advanced stages Countries with under-developed financial institutions structures.

Via wireless networking technologies, which are evolving more quickly than conventional 'fixed' communication networks, consumers in such countries, it is possible to access services more effectively from banks outside one's own country (Gao &Owolabi, 2008).

2.2DEFINITIONS OF ELECTRONIC BANKING

Electronic banking is characterized as the application of computer technology to banking, particularly the banking aspects of payment (deposit transfer). It is also a banking mechanism with an electronic communications network that allows credit and debit transfers of funds between member institutions of the clearing system to be performed electronically on the same day (Anyanwaokoro, 1999).Electronic banking is described by the As a type of banking in which funds are exchanged, the exchange of electronic signals between financial institutions rather than money, cheques or other negotiable instruments (Clive, 2007).

Electronic banking is characterized as a mechanism in which, without the use of paper cheques, funds are transferred between various accounts using computerized online/real-time systems (Omotayo, 2007).Electronic sales networks provide a larger variety of consumers with options for easier delivery of banking services (Kaleem, 2008). The newest distribution platform for financial services is e-banking. Among scholars, the concept of e-banking differs in part because e-banking applies to many types of services via which customers of a bank can request data and conduct most retail banking facilities through device, television or cell phone (Mols, 1998).

A range of the platforms below can also be described as e-banking:

- Internet (or online banking.
- Telephone Banking

Television-based banking

- Mobile telephone banking

PC banking (or banking offline)

The majority of customers who start online banking do so because they have to pay for it. bills frequently, and would like to do it with minimum effort. Besides that, people use internet banking to keep an eye on their money matters, view their account balance and check to receive payments from other parties. E-banking technologies can be classified as either ‘passive’ or ‘active’. Passive technologies such as direct deposit do not require behavioral changes on the part of the consumer. These innovations are therefore more easily spread to the mainstream.

Perhaps the most user engagement is expected by e-banking, as it allows the customer to retain and communicate frequently with additional devices such as a computer and internet connectivity (Hogarth, Kolodinsky, &Hilgert, 2004).

2.2.1 BENEFITS OF E-BANKING TO CUSTOMERS

- **Convenience:** You can perform your banking activities whenever you want by banking online. Online banking is a 24-hour operation, so the hours of the branch are no longer tied to you. On top of that, you don't need to wait in the inevitable lines and take the time to take the opportunity to drive to the branch, allowing you more time to do what you want.

- **Mobility:** As long as you have an Internet connection, online banking can be carried out from anywhere.
- **No Fees:** With all these extra expenses, fees can be minimized and are often non-existent because an online bank does not have to think about locating an actual bank location. Those checking and savings accounts provided by fully online banks typically have no fees whatsoever.
- **Higher Interest Rates:** Again, higher interest rates are also provided for their accounts due to a lack of costs related to operating an online bank. You will normally need to bank with an entirely online account for higher interest rates.
- **Online Statements:** The majority of online banks aim to be as paper-free as they can. Online, most statements and communications are carried out, minimizing the amount of paper used and sent to you. Again, this would help to lower the online bank's costs. As a bonus, this makes online banking a great choice for the environment.
- **Direct Deposit:** You should pay for it to be directly deposited into your bank account for any incoming money, such as your paycheck, by the company sending the money. As you don't have to take the time to make that happen. deposit the check, this is a double advantage, plus the money goes into your account quicker, allowing you to gain interest even faster.
- **Automatic Bill Paying:** You can simplify the payment of your monthly bills with automated bill payments. You need to set this up, of course, but in the long run, it will be worth it. Next, you should not ever skip a payment of your bills being paid automatically. Plus, you can hold your account for a little longer by not having to think about the time taken to send in your deposit, gaining you a little more interest, and you also save on postage. Finally, you can do away with using checks and you also save on paper used, making this a much greener way of banking.
- **Real-Time Account Information:** As you can access your accounts at any time, you can get up-to-date, real-time information about the money in your accounts. This will help you to manage your money better and reap the most from the bank's various accounts, interest rates and services.
- **Transfers:** Transfers can be achieved almost instantly. between accounts of same financial institution online. There is not just no lock on the money being on the money passed around but whenever you want and from anywhere, you can also do it. You save time when you fly to the nearest branch, too. Even transferring to other financial

institutions is easier, and safer as you don’t have to carry the money around with you. You can even now email money to and from other people with INTERAC email money transfer.

2.3DIFFERENT ELECTRONIC BANKING TYPES

The words' PC banking,' online banking,' internet banking,' telephone banking,' or 'mobile banking' refer to a variety of forms in which clients can reach their accounts without needing to be present at a branch of a bank physically. E-banking is possible to view as a concept that electronically encompasses all these aspects of the banking business (Leow & Bee, 1999).

2.4 RECENT TRENDS AND DEVELOPMENTS IN E-BANKING

2.4.1Tele-banking

Tele-banking service is provided by phone. It is important to call a certain telephone number to reach an account, though there are many service choices. The launch of online telebanking systems has now made it possible to conduct a variety of banking-related services, including financial transfers, from the comfort of consumers selected anywhere in the globe and at any moment, of day and night. Through dialling the customer can access his account from anywhere, the provided telebanking number from a landline or a smart phone, and entire banking can be achieved via the Interactive Voice Response (IVR) method. by following the user-friendly menu. Customer calls they're not going to to fail with ample numbers of hunting lines made available. The device is multilingual, providing the following facilities;

- Automatic voice-out balance for the default account.
- Balance Request and Transaction Request in all.
- Investigation of all term deposit accounts.
- Account Statement via fax, e-mail or daily mail.
- Application for cheque books.
- Stop payment, which is instant and online.
- The automated and instantaneous transfer of funds to CBS.
- Bill Payments for electricity.
- Term deposit renewal, which is automatic and immediate.
- Voice from the last 5 transactions.

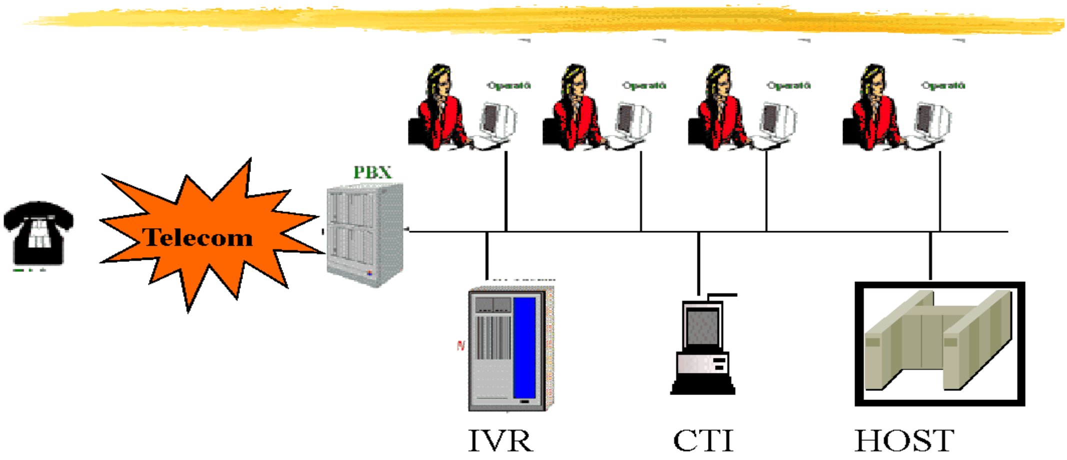


Figure 2.1 Telephone Banking Infrastructure (Lan, 2011)

2.4.2 PC-banking

Growing understanding of the value of computer literacy has contributed to a worldwide rise in the use of the personal computers.

The term 'PC-banking 'is used for banking business transacted from a customer's PC, i.e. customers can be using their home or personal computers at their office to access their purchasing accounts by connecting and dialing by password into the banks' intranet proprietary computing system.

2.4.3 Internet banking

Digital banking will liberate both bankers and consumers from the need to continue their online banking transactions using proprietary applications.

The behaviour of consumers is quickly changing. The financial service is today distinguished by individuality, time-and-place freedom and versatility. These facts raise immense obstacles for suppliers of financial services. Often the internet is now considered a 'strategic tool' for them to fulfill the demand and creative market needs of ever-changing consumers.

2.4.4 Mobile banking

Wireless internet banking applications, often called m-banking, are a more recent e-banking approach development. Thus, a modern support (service for mobile data) is allowed with the merging of internet and mobile phones and the first such wireless internet commercial a transaction was conducted by the banking industry (Barnes, 2003).

2.5 (ATM) AUTOMATED TELLER MACHINES

An unattended electronic computer attached to a data system and associated facilities in a public place and enabled by a client of a bank to access cash withdrawals and other financial services. It is called a cash register, automatic teller or machine for a money machine.

An automated teller machine (ATM) is an electronic computerized telecommunications device that enables a financial institution's clients to use a safe touch mechanism to directly access their bank accounts, order or make cash deposits (or cash advances using a credit card) and check their account balances without the need for a human bank teller (or cashier)

In most modern ATMs, by inserting a plastic card with a magnetic stripe or a plastic smartcard with a chip containing his or her account number, the customer identifies himself. The client Then, inserting a pass code, often known as a PIN (Personal Identification Number) with four or more digits, verifies their identity then, inserting a pass code, often known as a PIN (Personal Identification Number) with four or more digits, verifies their identity. The client, on good entry of the PIN

If the number is wrongly inserted a few times in a row (usually three attempts per insertion of a card), any ATMs may try to preserve the card as a security measure to prevent an unwanted individual from discovering the PIN through guesswork. If the card issuing bank is not the ATM owner, caught cards are often discarded as it is not possible to correctly search the names of non-customers.

The ATM helps individuals to withdraw and deposit money using computers from their bank accounts. It is assumed that it is a blend of a few different innovations. The first automatic banking system only collected cheques and deposits and was founded in 1960 by Luther Simjian, an American inventor and businessman. John Shepherd-Barron, a Scottish engineer, developed an ATM that used toxic ink-printed paper vouchers so that the system could decipher them in 1967. Finally, in 1969, in the United States, Donald Wetzel produced the first ATM that used plastic cards identical to those we have today (Luther Simjian, 1960, 1967, 1969).

An automated teller machine (ATM) is an electronic banking outlet that makes it possible for customers to finish simple transactions without the help representative or teller of a division.Someone with a credit card or a debit card will use most ATMs. The first ATM arrived in London in 1967, and in less than 50 years, ATMs have exploded across the globe, ensuring a presence in every large country and even small island nations such as Kiribati and the Federated States of Micronesia (Kagan, 2018).

ATM Ownership

Credit Unions and banks own ATMs in many instances. However, ATMs can often be bought or rented by individuals and corporations, on their own or by an ATM concession. The benefits model is focused while ATMs are owned by individuals or small businesses such as restaurants or gas stations, charging fees for the machine's customers. With this purpose, banks often own ATMs, but besides, the convenience of an ATM is service banks use to draw customers. ATMs often remove some of the pressure of customer service of bank tellers, saving money on labour expenses for banks.

ATM Fees

Account-holders may use their bank's ATMs at no discount, although typically a minor fee is paid to access funds from a unit owned by a rival bank. As of 2017, $4.69 was the total charge cash withdrawal from an out-of-network environment ATM. The lowest ATM average fees were $4.07 in Dallas, while the highest average fees appeared to be $5.19 in Pittsburgh.

In the ATM ecosystem, ATM fees are split between different parties or partners. The three key parties in any ATM firm are the ATM owner, the venue owner and the ATM processor. The ATM's owner is the one who purchases the machine and places it in a certain position or area. The owner of the place is the person that you have called and arranged to locate your ATM machine. Finally, the ATM processor is the entity that prepares the paperwork or documentation that helps to run the ATM. The three parties are the ones that are going to divide the sum paid by all.

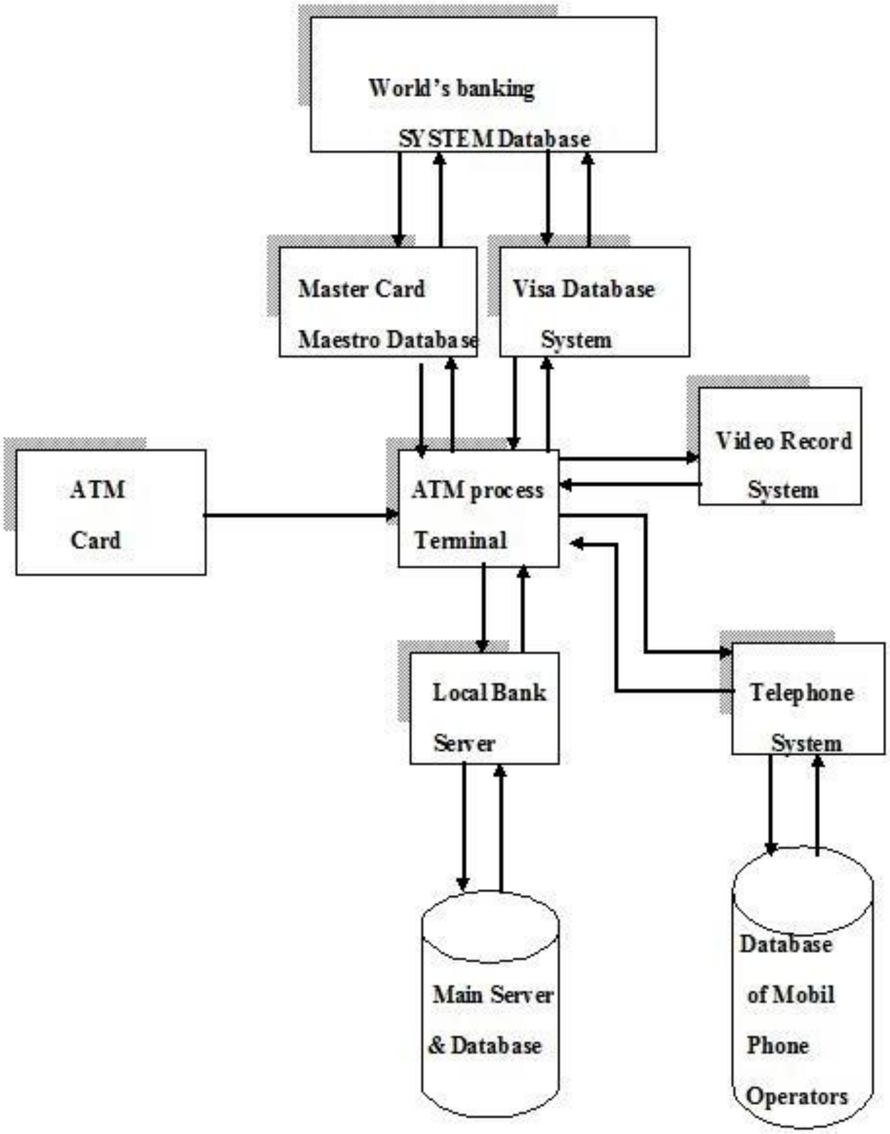


Figure 2.2 Architecture of a simple ATM Machine (Christohe, 2007)

2.5.1 USES IN NIGERIA FROM ATM

1. **Shopping**

As many online business owners now incorporate payment solutions into their websites, online shopping has been made quick and convenient. You can conveniently purchase goods and things online with certain ATMs; you can use it to pay at certain retail shops. The bank's terms and conditions can apply, so you should ensure that before you start a transaction, you read their terms and conditions.

2. Recharging Airtime on Mobile Phones and Devices

You will improve airtime on your cell phones and computers with an ATM computer. Usually, this is achieved in two ways;

- By the previous credit balance by the number you ordered, Virtual Top Up-In Virtual Top Up (VTU), you get phone credits topped up automatically. This is available for all network customers of MTN, Zain and Glo.

3. Quick Teller Option

You can buy airtime, make purchases electronically and shop online with a swift teller.

4. Buying and Transferring Airtime to Others

Airtime can be bought and passed via an ATM system to your family member, parent or acquaintance. If you own an account with the bank that operates the ATM system, this is typically simple and feasible.

5. Cash Withdrawal

This is the very using an ATM system that everybody is conscious of. 24/7 Cash Withdrawal from your account is given by ATMs.

6. Printing of Mini Statement of Your Account

You will print out the last eight transactions on your account using an ATM. Usually, this is necessary If you want to have a collect accurate statements of the last few bank transfers made in your account.

7. Intra Bank Transfer

An intra-bank payment is the transfer of money from your deposit to another account of the same bank via an ATM computer. The service for Intra Bank Money Transfer is normally free. For example, if you are the first holder of a bank account, you will use an ATM to move money from your first bank account with a different bank account. There's no fee for this kind of trade.

8. Inter Bank transfer

Using an ATM, you can even transfer money from an account in your bank to a bank account separate bank account; this is called interbank transfer. Bank fees can apply.

9. Send or Transfer Money to Your Family Members, Relatives or Friends

You will give or pass money to a family of yours members, relatives and friends using an ATM system. The system for doing things is sometimes uncovered, in addition to the ATM computer terminals. It is simple and clear. Any ordinary reader who can read words from the computer can do it.

10. Check Account Balance

You can run an account balance inquiry using an ATM unit. This is for all country-wide account holders (both savings and current). By dialling a basic ussd code on a cell phone, but these days it is relatively easier; your account balance will be transmitted to you.

11. Check-Account-Number

You may also use the ATM system to ask for your bank account number. Visit every ATM terminal close you if you losing a bank account number and you are in danger of having it. However, you can also dial a code to collect your checking number of the account on your phone from your bank, much like dialling a code on the phone to receive your account balance.

12. Payment for DSTV, Electricity Bill and Other Utility Bills

The use of ATMs to make bill payments is one big using an ATM system that people do not know. You will pay for utility services, such as electricity bills, DSTV & HITV billing charges and postpaid GSM bills, using an ATM terminal. With a fast teller option on ATMs, there's more you can do than that.

13. Airlines: Payment for Pre-Booked Aero Air Tickets and Others

You should pay for yourself, the pre-booking of Aero Air Fares and other airlines using an ATM system. You will simply pre-book an airline from an ATM near you in a case in which you are choked up with time to board air tickets from Air Travelers' Agents.

14. Card-Based Cash Deposit

With your Verve or Naira MasterCard wallet, cash deposits based on cards can be made. Only the debit card, though, can be deposited into the linking account(s). All ATMs do not serve this purpose.

15. Cardless Cash Deposit

You will deposit cash into account in the cardless cash deposit without the use of a mark debit card. Again, this function is fulfilled by not all ATM computers.

2.5.2. ISSUES RELATED TO THE USE OF IN NIGERIA ATM

Several major challenges and issues are facing the e-banking industry today.

1. **Automated Teller Machine Fraud**

In an article, Emeka (2007) states that as the number of ATM cardholders continues to grow daily as a result of the e-payment acceptance of Nigerian banks and the deployment of more than three thousand ATMs cash points across the nation, the activities of card fraudsters seem to be on the rise. As a result of fraudsters who are said to be on the prowl, many Nigerian banks, especially United Bank for Africa, have cautioned ATM card users nationwide against revealing their ATM card data to a second party. In a paper entitled 'ATM Fraud and Security,' Diebold (2002) reported some ATM fraud. The strategies below have been highlighted.

2. **Card Theft**

Criminals also used several card trapping systems made of slim mechanical devices, frequently encased in a clear plastic film, embedded into the throat of the card reader, in an attempt to procure genuine cards. Hooks are connected to the probes that keep the card from being returned after the purchase to the customer. As the ATM terminal user expresses concern about the caught card, the suspect will provide help, usually close to the ATM, indicating that the user enters the PIN again, so what he or she is or is can access the entry and recognize the PIN. The thief would then use a probe (fishing device) to retrieve the card after the customer leaves the area, thinking their card to have been caught by the ATM. The thief will quickly remove money from the unsuspecting user's account after having seen the customer's PIN and now having the card in hand.

3. Skimming Devices

Another way to view the credit records of a customer is to skim the information off the wallet. Skimming is the method of secretly accessing card track data that is most widely used. 'Skimmers' are machines that thieves use to intercept the data contained in the card's magnetic strip.

4.PIN Fraud: This can take the following forms:

i. **Shoulder Surfing:**The act of direct observation is Shoulder Surfing, seeing what number the person taps on the keypad. Usually, when the ATM customer enters their PIN, the robber places in near but not explicitly connected to the ATM, to himself watch covertly. Often, easily obtained miniature video cameras can be mounted discreetly On the fascia, or on the anywhere near the PIN pad to capture the PIN entry detail.

ii. **Utilizing a Fake PIN Pad Overlay:** Over the original keypad, a fake PIN pad is mounted. The PIN data is collected by this overlay and the information is retained in its memory. After that, the false PIN pad is erased and registered PINs are downloaded. In appearance and scale, fake PIN pads can be virtually the same as the original. A 'thin' overlay, which is invisible to the user, is an alternative form of overlay that is more difficult to spot. The approach used in connection with card data fraud provides the perpetrator with the details required to enter the account of an innocent customer.

iii. **PIN Interception:** The information is collected in electronic format using an electronic data recorder after the PIN is entered. It is necessary to catch the PIN either inside the terminal or when the PIN is sent for online PIN search to the host device. The suspect will need access to the contact cable of the PIN pad inside the terminal, which can be accomplished more conveniently at off-premise sites, to catch the PIN centrally.

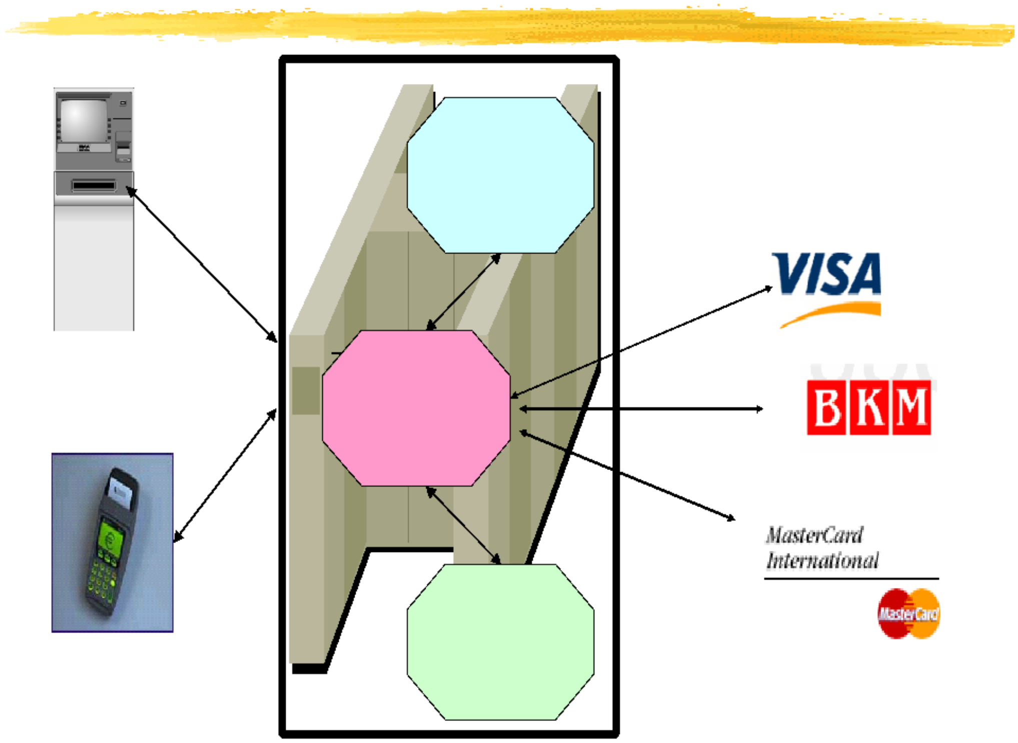


Figure 2.3 ATM and POS Application Architecture

2.6 APPLICABILITY OF BIOMETRICS IN E-BANKING FOR AUTHENTICATION

The use of biometrics for e-banking (such usage of passwords including or personal identification numbers) is becoming easy and substantially more reliable than existing conventional methods. This is because biometrics connect the case to a single party (someone other than the registered recipient may use a password or token), it is easy (nothing to bring or remember), precise (it allows for positive authentication), it can provide an audit trail and it is becoming socially appropriate and inexpensive.

2.6.1 What is Biometrics?

Biometrics is characterized as the human body's specific physiological or behavioural features and traits (Jain & Ross, 2015). To classify each person, certain features and traits are used. Biometrics is used as a strategy of authentication and access control in computer science. Among populations that are under observation, sometimes it is used to classify persons.

The identifiable, observable features used to mark and describe persons are biometric identifiers. Biometric signatures are also classified as aspects of physiology versus behavior.

Biometrics is the recognition or authentication, based on physiological or behavioral features, of the identity of another (Brey, 2007). For example, an individual can be defined by characteristics such as fingerprints, hand geometry, signature, retina or voice (Venkatraman&Delpachitra, 2008). For organizations such as financial institutions, it may be a secure means of regulation of access and personal authentication, but there are a large number of safety risks in the application of biometric technologies, such as the following: variations in lighting and picture angles in facial recognition affect data reliability; masking a digit to prevent a match in fingerprint technology can affect data reliability; the failure to conduct liveliness tests in iris/retina scanning opens the opportunity to print iris patterns on contact lenses, and because of variable trait data, signature recognition may endanger data consistency and reliability (Venkatraman & Delpachitra, 2008).

Retina, iris, fingerprint, facial recognition, vein lines, deoxyribonucleic acid (DNA), etc. are physiological biometrics. Either registration or authentication is used by them. Behavioral biometrics, including but not restricted to to: typing rhythm, speech recognition, gait and signature, are related to a person's behavior. The word behavior metrics has been coined by some scholars to describe the above class of biometrics. For authentication, they are used. More common forms of access control also include token-based authentication Systems, like a driver's license or a driver's license, a visa, and systems for knowledge-based authentication, such as a password or a number for personal identification. Identity authentication is more accurate than token and knowledge-based approaches because individuals have unique biometric signatures, but the compilation of biometric identifiers poses privacy questions about the actual use of this information. For biometric protection systems, there are seven fundamental criteria: individuality, universality, permanence, collectability, efficiency, acceptability, and circumvention.

Uniqueness is regarded as the priority criterion for biometric data, as mentioned above. It will show how the biometric device will identify each user individually and uniquely within groups of users. For example, everyone’s DNA is unique and it's difficult to reproduce.

Universality is the secondary standard for protection in biometrics. This parameter implies criteria that cannot be repeated for features of each person in the world. For starters, retinal and iris are features that would fulfill these criteria. Thirdly, for a particular attribute or trait that is registered in the device database and needs to be constant for a certain period, a permanence parameter is required. This parameter would often be determined by the user's age. Collectability is accompanied by the permanence parameter. To check their identity, the collectability parameter includes the selection of each attribute and characteristic by the device.

The output is the next system metric that outlines how well the protection system performs. The accuracy and robustness of the biometric protection device are primary considerations. The efficiency of the biometric protection system will be determined by these factors. Fields, where biometric technologies are suitable, would be selected by the acceptability parameter. Finally, circumvention can evaluate how quickly each user-provided function and trait will lead to failure during the verification process.

2.6.2 Advantages of Using Biometric

Using biometrics for identifying human beings in E-banking offers some unique advantages given as follows:

- Biometrics usage can be made for recognize you as you are.
- Tokens may be misplaced, broken, duplicated, or left at home, such as smart cards, magnetic stripe cards, picture ID cards, physical keys, etc.

- It is easy to lose, exchange, or watch passwords. Also, today's fast-paced modern world suggests that people are asked to recall a multitude of computer accounts, bank ATMs, email accounts, cell phones, websites, and so forth, including passwords and personal identifying numbers (PINs).
- For several applications, biometrics holds the promise of quick, easy-to-use, precise, secure, and less costly authentication.
- Another main factor is how a device is "user friendly." The method, such as getting a This is a picture taken by a video camera, talking to a microphone, or touching a fingerprint scanner, should be fast and simple.
- Dealing with several layers of authentication or several authentication instances will become less of a hassle for consumers as biometric solutions evolve and fall into wide-scale commercial use.

2.6.3 BIOMETRIC AUTHENTICATION

Biometric instruments are comprised of a reader or scanner, software that translates the information obtained into digital form, and a database that preserves biometric data for compatibility with previous documents. The program defines individual points of data as match points when translating the biometric input. Using an algorithm, the match points are translated into a value that can be correlated in the database with biometric data. Both biometric authentications require that a licensed or registered biometric sample (biometric template or identifier) be matched to a newly collected biometric sample (such as a login fingerprint).

To be included in the scheme, by gathering a raw biometric, individuals must first register their form of identity with the system. This technique is known as enrollment and consists of three different stages: capture, service, and enrollment.

- Capture: The Biometric sensor system captures a raw biometric device.
- Process: Features that are individual-specific and differentiate individuals from each other are derived from the raw biometric and translated into a "template" biometric.
- Enrol: The processed prototype is stored on a disk storage unit or on a compact device smart card, for example, in an acceptable storage medium such as a database, whereby subsequent comparisons can be readily made.

- Once Enrolment is complete, the machine will authenticate people using the saved template. Authentication is the mechanism by which the person who authenticates with the system relative to the recorded (enrolled) biometric prototype collects a new biometric sample. Two forms of authentication are available: verification and identity.

The process identifying a person from their biometric features is done by registration. Identification asks the question, **"Who are you?"**Verification entails comparing the collected against the biometric sample stored enrolled template and allows consumer to assert a particular identification argument, such as a unique key for the user name. The question **"Are you who you think you**" are is asked by the authentication.

Using the parameters below the quality of a device in conducting verification is calculated.

Effective schemes would have high values of the real good and the real negative, with high values of False negatives and false positives in a bad system. The description of each metric is as follows:

- TP: correctly allow access to an authorized user
- TN: correctly deny access to an unauthorized user
- FP: incorrectly allow access to an unauthorized user
- FN: incorrectly deny access to an authorized user

A diagram illustrating the process of Enrollment and Authentication is shown below:

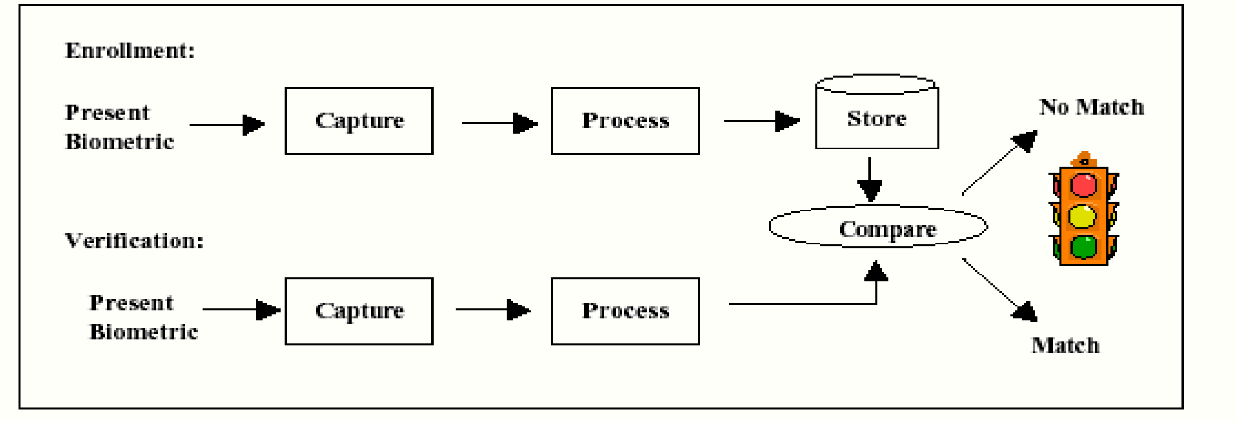


Figure 2.4 Biometric Authentication

2.6.4 EXAMPLES OF BIOMETRICS IN BANKING

Bank of America: Authentication of Fingerprints, Iris-Scanning and App Linking

Several years back, smartphone applications from Bank of America launched fingerprint and Touch ID authentication and a pilot of iris scanning followed in short order. The financial institution recently announced the inclusion of a new App Linking feature. This capability is available in all smartphone applications (Bank of America, Merrill Lynch, Merrill Edge, and U.S. Trust) that come under the umbrella of Bank of America. Users authenticate once using a fingerprint scan or facial recognition, and can then use a button without having to re-authenticate to switch between these apps.

Barclays: Finger Vein Reader Technology

Barclays partnered up with tech giant Hitachi to deliver Finger Vein reader technology to its corporate banking clients, close to fingerprint technology. Instead of inserting codes and PINs, company clients merely put a finger inside a small laptop scanner to approve transactions. The importance of technology lies in the distinctive vein patterns found on each digit, which are formed in the womb and remain relatively unchanged throughout life. For a creative authentication experience, the Biometric Reader at Barclays blends advanced safety with user-friendly security interface.

Citi: Voice Authentication

In 2016, to verify the identity of consumers calling their call centres, Citi launched speech biometrics. Speech verification uses biometrics to check the identity of consumers as they clarify a query on the phone to a customer service agent. It analyzes distinctive features in the vocal pattern of an individual and cross-checks them to validate their identity against a pre-recorded voice print. Voice verification takes out the tedious method of checking the identification of a client via ID numbers and personal information, reducing consumer friction, and empowering members to quicker deliver practical assistance. It takes less than a minute for a client More than one million consumers within one year of its publication, voice authentication was used in the Asia Pacific region in order to set up a voice print.

The Scottish Royal Bank and NatWest: Biometrics Payments Card

A Payment Cards pilot with biometric fingerprint technology was revealed in 2019 by Royal Bank (RBS) of Scotland.The experiment is being conducted with around 200 NatWest clients of the bank and will take place in the UK. The fingerprint acts as a replacement for PIN entry that used to check is transactions over £ 30, making it safer and easier for customers to finish their purchases. This new growth was followed by a long line of biometrics advancement as RBS and NatWest became the first U.K. Banks make Touch ID fingerprint recognition on their mobile banking apps.

Wells Fargo: Eye-print Authentication

The CEO Mobile ® solution from Wells Fargo enables commercial consumers to view bank account balances, make deposits, and accept payments all from the comfort of their mobile devices. Advanced security technologies are also integrated into the solution, including encryption, secondary authentication, and token creation. The use of an antenna eye-print biometrics mechanism is an added security capability. By scanning their eyes on their mobile devices with the flash, this feature helps users to sign in. Via eye-print authentication, the need to have a password or token is eliminated, making the sign-in method easier and cleaner.

2.7 RELATED WORK OF STUDY

Ramrakhyani, et al (2017) made use of biometric fingerprint scanning to provide access to ATMs. Fingerprint data is collected in a database using the bank's enrollment process. Banks supply the client with authentication that can be obtained as the transaction process is carried out. In the database, if a fingerprint match is detected, then transactions take place. After authentication, the transaction will be cancelled if the fingerprint does not fit. Safe purchases can be made by using fingerprint-based ATM users.

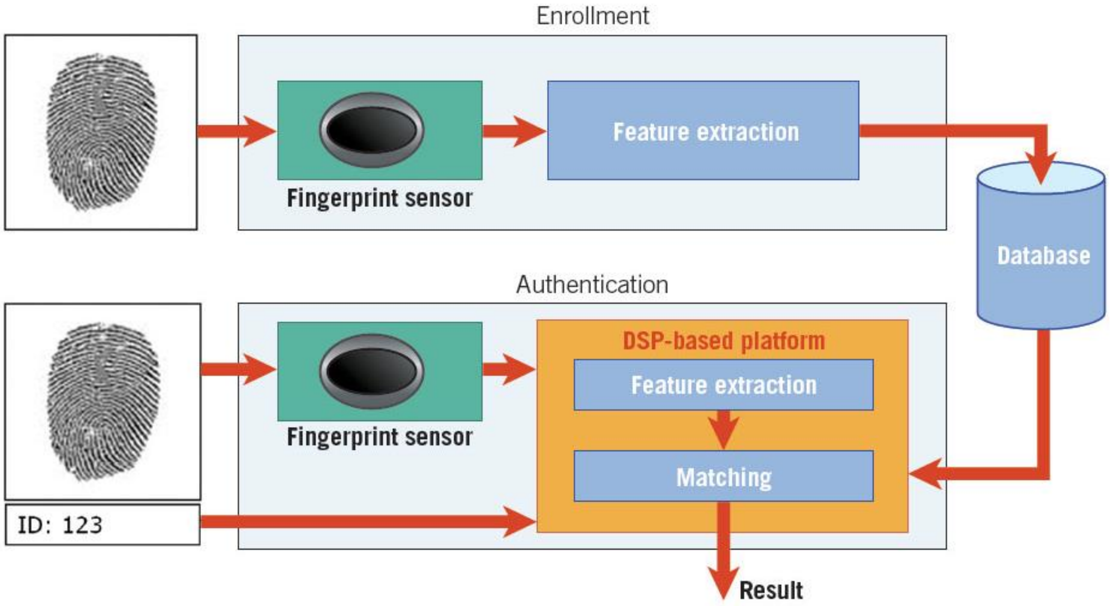


Figure 2.5: Fingerprint Scanning

An embedded fingerprint recognition device the ATM is used for authentication was developed by Daula et al (2012). Their device uses GSM modems for user authentication. During account opening, the scheme allowed banking institutions to collect biometric fingerprints and the The number of cellular mobile) customers. The bank's customer places his/her fingerprints on the fingerprint reader mounted to the ATM unit on the ATM system console. Then the machine on the ATM matches The fingerprints on the markers fingerprints previously captured. A 4-digit code is produced and sent to the customer's cell phone if the fingerprints are known to be a match. On the ATM, these 4 digits are then entered. Utilization of an ATM card would not require this device. The machine is safe because The identity of an individual cardholder who attempts to make a transaction through the ATM is safely checked and authenticated.

In their analysis, Onyesolu and Ezeani (2012) found that most of their respondents selected fingerprint recognition as the preferred biometric identification solution for the theft and fraud of ATM cards. As the proposed biometric-based ATM authentication mechanism, developed and developed by the authors in Oko and Oruh (2012), assessed, as a result of their methodology and analysis, that biometric authentication on ATM systems was feasible and could be applied in production environments.

An study was performed to introduce a method of authentication of crypto-bio in ATM banking systems also carried out (Biswas, 2012). Their method was focused entirely on the use of retinal pictures.

In their report, Venkatraman&Delpachitra (2008) concluded that there is little literature on their application in the banking sector, while biometrics have been successfully applied in areas such as border management and criminology. Their research identified 4 key categories of problems crucial to the viable implementation in New Zealand of biometric-based authentication. Technological, management, legal and ethical, and monetary considerations are identified as well.

A study For the development of crypto-bio authentication method in ATM banking systems (Biswas & B, 2012) was also performed. Their method was focused entirely on the use of retinal pictures.

A Scheme of biometric authentication for ATMs was introduced (Hossain & N, 2013), and their system used an Advanced The Instead of the Encryption Standard (AES) processor Encryption Standard for Triple Data (3DES). The research concluded that the ATM transaction was made safer with the use of biometric AES processors and fingerprints authentication.

(Oudu & T, 2010) introduces a modern approach to creating fingerprint images from traditional models and discusses the degree to which their built images are equivalent to the original ones. The majority of so-called biometric cryptosystems seek to merge cryptographic systems with biometric recognition systems to strengthen security in common key management systems. systems. Therefore, these systems generate cryptographic keys, denoted Biometric Keys, based on biometric knowledge.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 INTRODUCTION

The chapter introduces the materials that will be used to achieve the objectives stated in this study.

3.2 METHOD OF OBJECTIVE

To meet the first goal, comprehensive analyses of existing works will be carried out to clarify and illustrate new methods used in ATM authentication. Besides, the following technologies will be used to design an architecture which will illustrate the application of multimodal biometrics for authentication purposes:

3.3 MySQL

This will be the search engine that will be used to house all the data that will be used in the framework for e-banking. It will include details such as the name of the mark customer, account number, pin, face picture, etc. All information will be collected from this archive and stored during authentication and transfers.

3.3.1 Microsoft Visual Studio

The integrated programming system that will be used for this project will be Microsoft's visual studio. It would be used to write all the code related to the functionalities of the interface architecture and backend.

3.3.2 Wamp Server

As the backend driver, the Wamp server will be used to provide both authentication and transaction-related processing. To have the required resources, it will communicate with the database and the application.

To WAMP. WAMP is a variant LAMP for Windows-based systems which is mostly built as a package kit (PHP, Apache, and MySQL). WAMP stands for "Windows, Apache, PHP and MySQL." It is mostly used for internal testing and web creation, but it can also be used for support live websites.

The term WAMP applies to a collection of free (open source) programs widely found in Web server environments, paired with Microsoft Windows. Four main elements of a Web server are provided to developers by the WAMP stack: an operating system, database, Web server, and Web scripting tools.

WampServer is a Windows server for Software development framework This allows Apache2, PHP, MySQL, and MariaDB to be used to build complex Web applications. The best thing is that WampServer is available, in both 32-bit and 64-bit versions for free (under the GPML license). WampServer does not support Windows XP, SP3 or 2003 Windows Server.

3.3.2.1 What is WAMP used for?

WAMP (Windows Apache MySQL PHP) is a package used on the local Windows framework for PHP developers to build their web projects. It comes with Apache Server, MySQL Database, PHPMyAdmin, and PHP to build an acceptable development environment.

3.3.2.2 How does the WAMP server work?

WampServer is a Windows software development tool that makes it possible for you to use Apache2, PHP, and MySQL to build complex Web applications. WampServer downloads everything you need automatically to build Web apps intuitively. Without even accessing the configuration files, you should be able to tune the server. 16, Sep 2015

WampServer refers to an operating system for Microsoft Windows software stack, developed by Romain Bourdon, consisting of an Apache web server, SSL help OpenSSL, a MySQL database, and a PHP programming language.

3.3.2.3 How Modify the default browser to it open localhost in wampserver?

Changing the norm tray icon in the browser:

- In Windows Explorer, open C:\wamp (or anywhere wampserver is installed)

In the text editor, open wampmanager.conf

- Find the main] segment
- Consider the line below:

"Navigator = "C:\Internet Explorer\Program Files\IEXPLORE.EXE

- Substitute it with:

"Navigator = "C:\Mozilla Firefox\firefox.exe\Program Files\

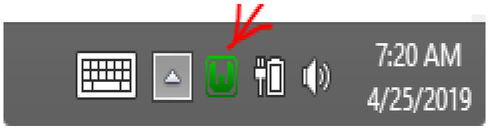
- Save a file
- Start the tray icon again

(2012: Evan. Bovie)

3.3.2.4 How to know if a server with a WAMP is running?

If WAMP is running, there should be a green WAMP icon in the lower-right corner of your screen. If you have extra applications represented there, you may have to hit an up-icon to see them all.

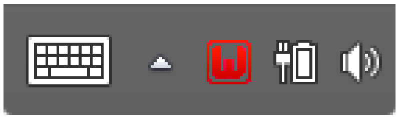
For me, it looks like this:



Green = All services running (Apache HTTP Server, MySQL)

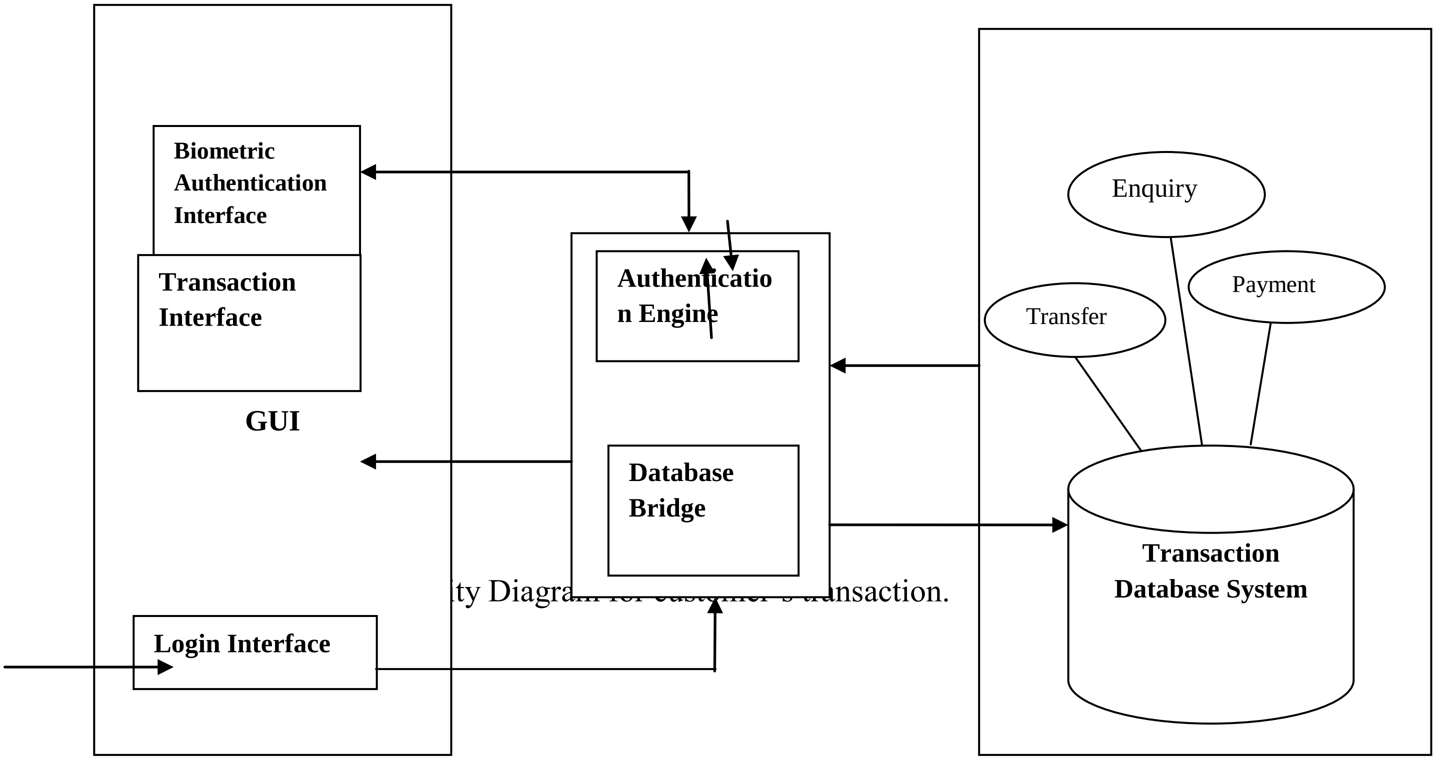
Orange = One of the two services are running.

Red = No services running



(Josh Greig, 2017)

3.1 FLOWCHART PROCESS



ity Diagram for customer's transaction.

The figure above is the flow process of the proposed e-banking system. The figure consists of a graphical user interface, which consists of a login interface, a transaction interface and a multimodal biometrics authentication interface.

3.4 Multimodal Biometrics Authentication Interface

This is the part of the system that will deal with biometric authentication. It would take fingerprints and voice of users intending to login and send it to the server for authentication.

3.4.1 Transaction Interface

This is the part of the system that will deal with accepting transaction instruction from users and sending them to the server for processing.

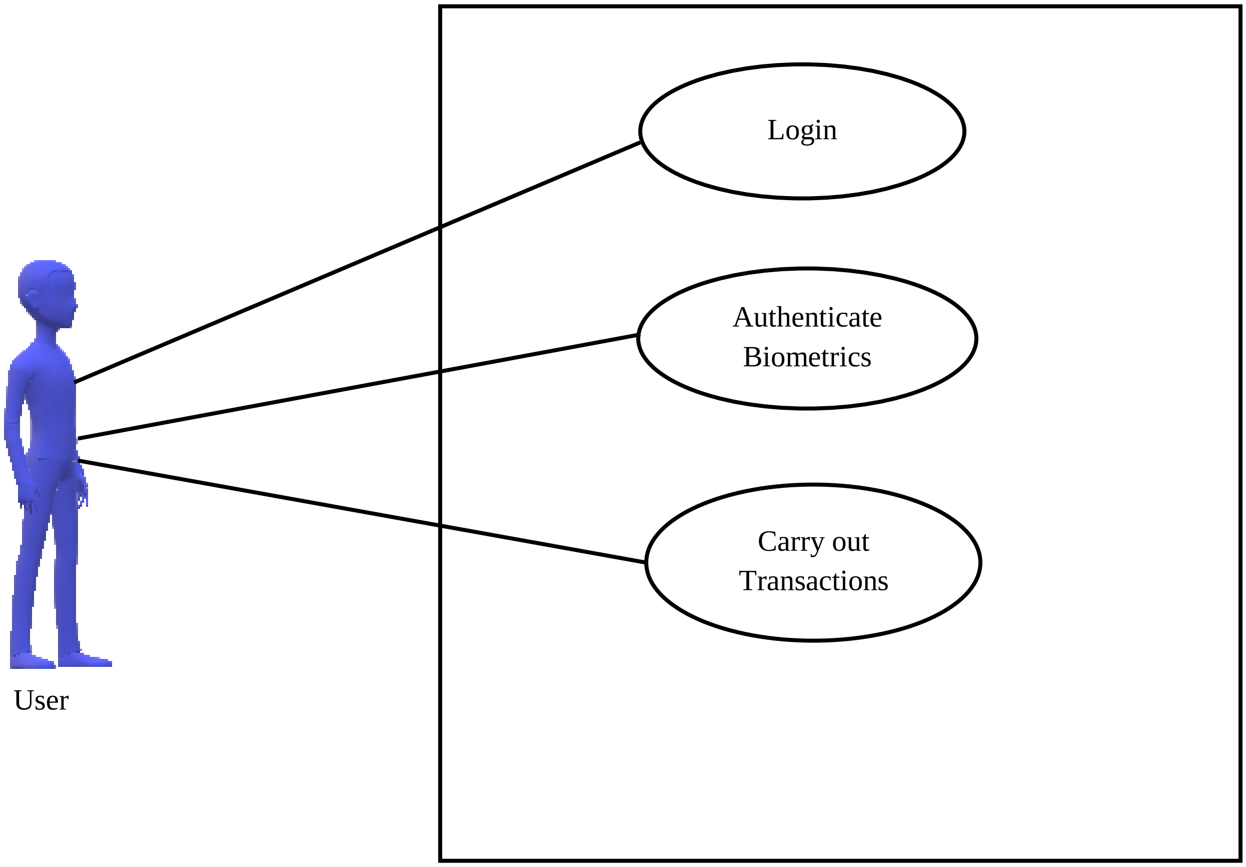
3.4.2 Login interface

This is the part of the system that will deal with accepting account number and pin from users intending to login.

3.4.3 Transaction Database system

This will be the search engine that will be used in the ATM program to store all the data that is to be used. Details such as customer name, account number, pin, fingerprint image, user voice, and so on, will be included. All information will be collected from this archive and stored during authentication and transfers.

3.5 Use Case Diagram



CHAPTER FOUR

IMPLEMENTATION OF THE PROPOSED SYSTEM

4.1 IMPLEMENTATION

The implementation phase of a project covers the period from the acceptance of the tested design to its operation supported by the appropriate user and operation manual.The hardware and software specification required is in line with the requirement of the version ofMICROSOFT VISUAL STUDIO used for the implementation of this project (VISUAL STUDIO 2010)

4.2 Hardware specification

A system with the following hardware specification is supported:

- At least a Pentium III processor
- Minimum of 512MB RAM
- At least a 60GB Hard disk
- RGB webcam.

4.3 Software Specification

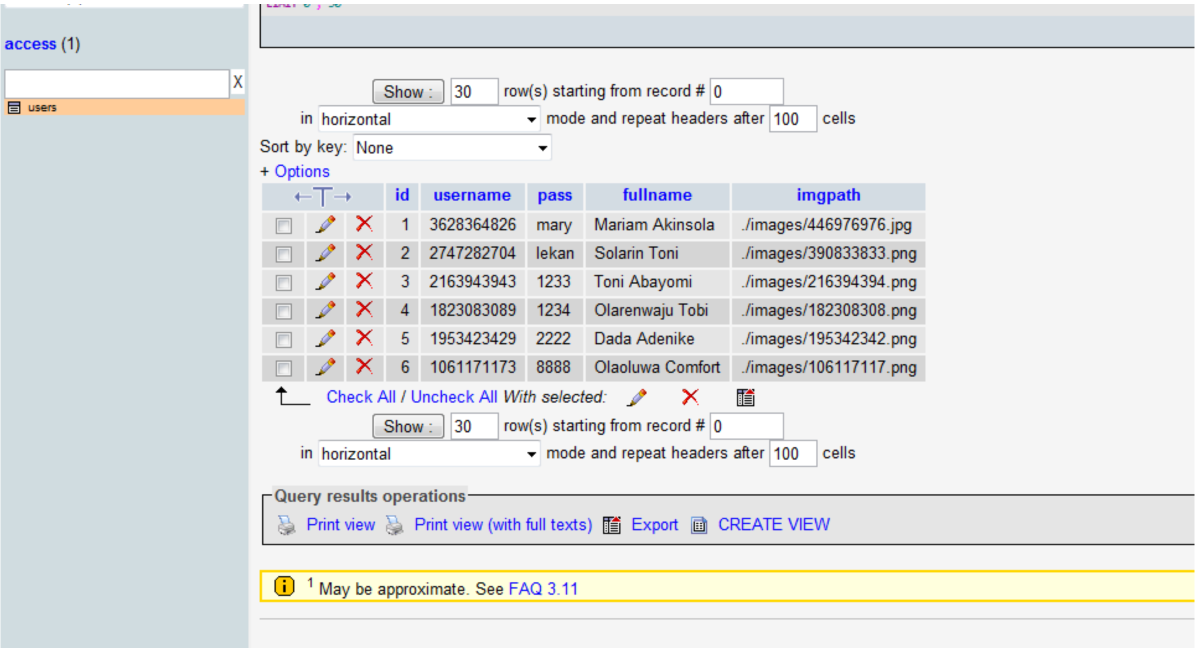
- At least Windows XP operating system.
- Digital Studio 2010 by Microsoft
- At least Microsoft .NET Framework 3.5

4.4 Choice of Programming Language

The programming language used in this project is C#. This programming language was used because it is an object-oriented programming language.

4.5 DATABASE

The database used was MySQL, a relational database was built containing one table for the bank accounts of the registered users.



Show : 30 row(s) starting from record # 0
in horizontal mode and repeat headers after 100 cells
Sort by key: None
+ Options

←T→			id	username	pass	fullname	imgpath
☐	✎	✕	1	3628364826	mary	Mariam Akinsola	./images/446976976.jpg
☐	✎	✕	2	2747282704	lekan	Solarin Toni	./images/390833833.png
☐	✎	✕	3	2163943943	1233	Toni Abayomi	./images/216394394.png
☐	✎	✕	4	1823083089	1234	Olarenwaju Tobi	./images/182308308.png
☐	✎	✕	5	1953423429	2222	Dada Adenike	./images/195342342.png
☐	✎	✕	6	1061171173	8888	Olaoluwa Comfort	./images/106117117.png

Check All / Uncheck All *With selected:*

Show : 30 row(s) starting from record # 0
in horizontal mode and repeat headers after 100 cells

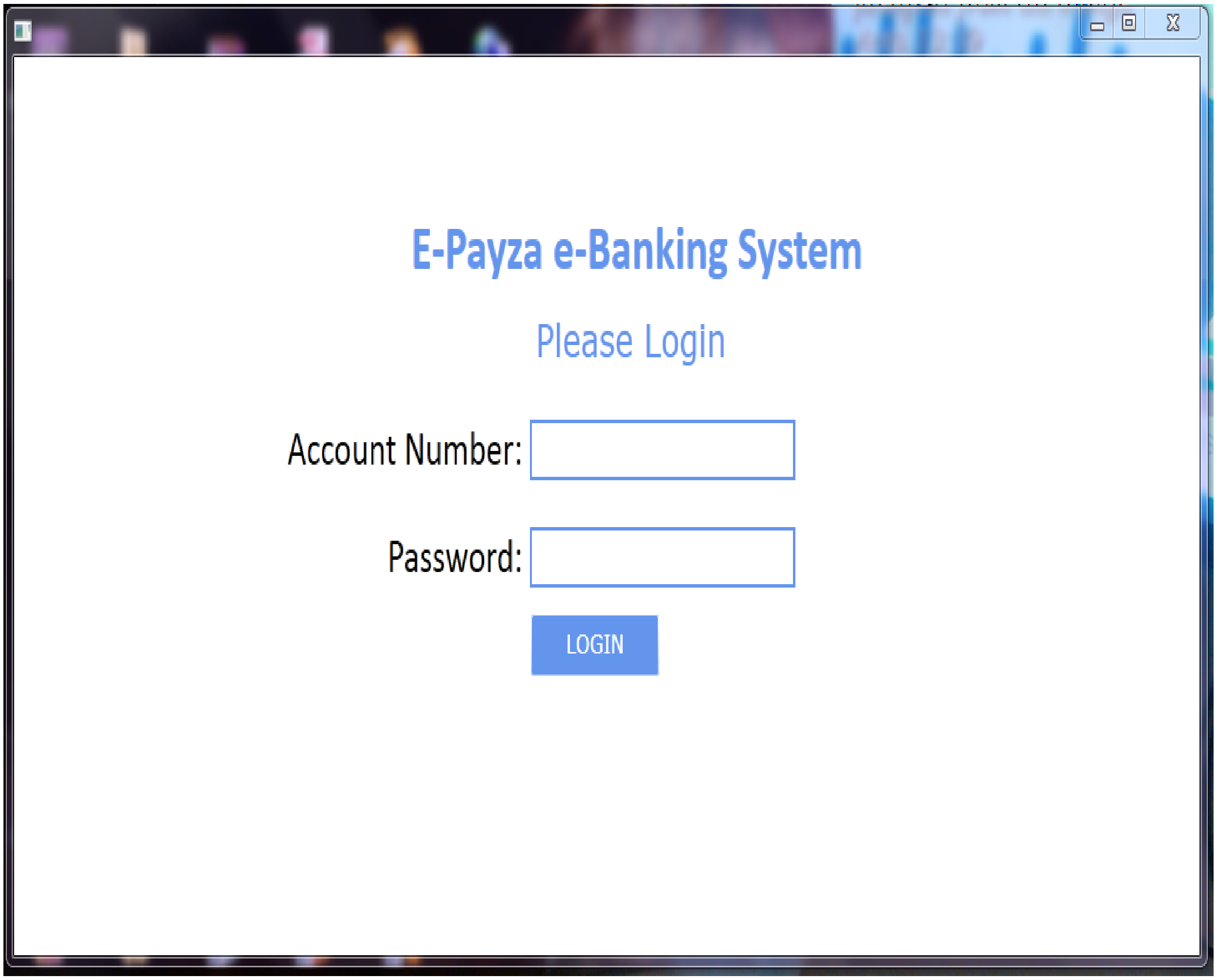
[1] May be approximate. See FAQ 3.11

Figure 4.1. The Database Containing Account Details

The above screenshot is of the MySQL database that contains user details including the account number, password, full name and the path to their image stored in the database. It also contains an ID field used to define individually each user during program flow.

4.6 GRAPHICAL INTERFACE

Login interface



E-Payza e-Banking System

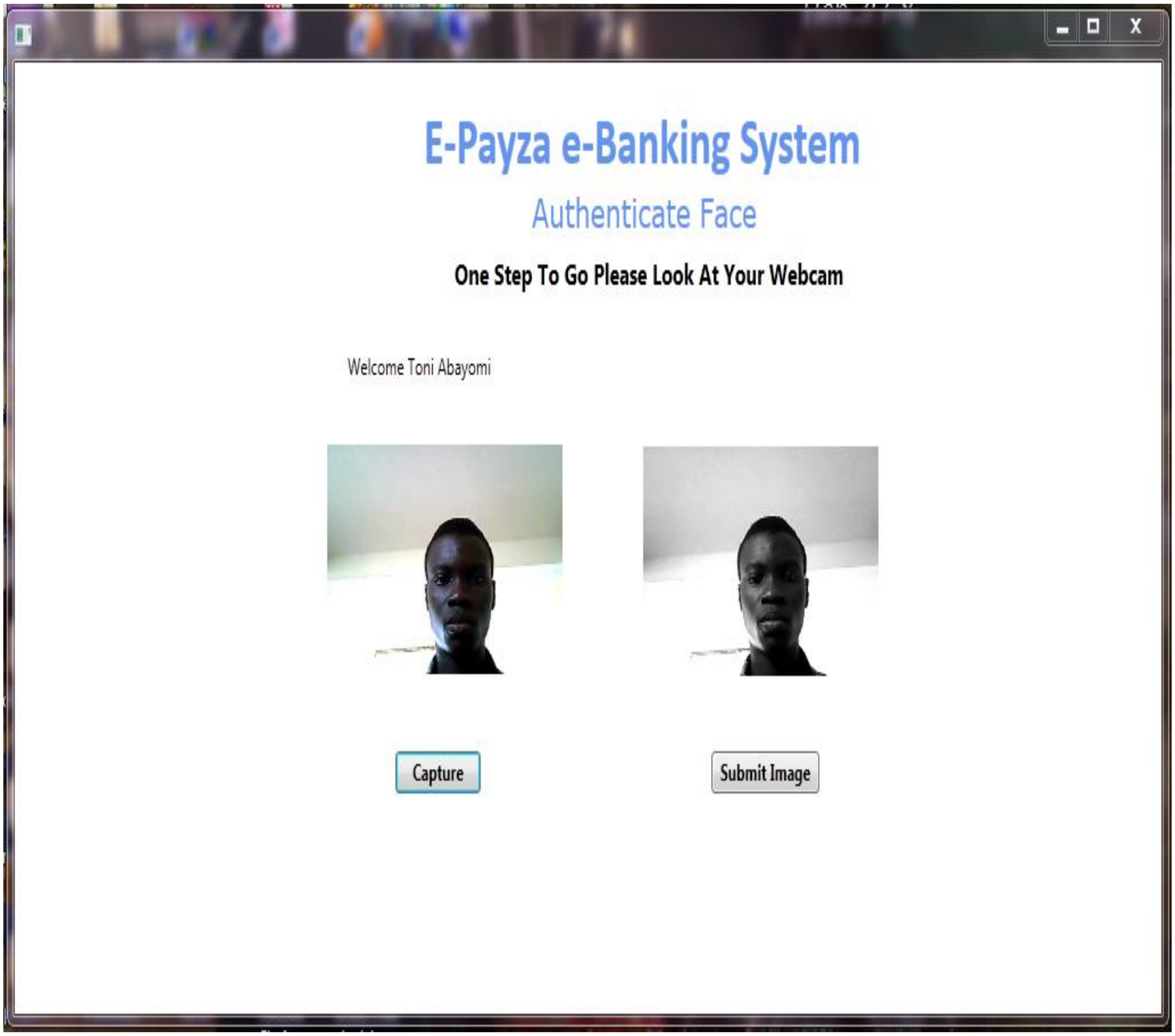
Please Login

Account Number:

Password:

Figure 4.2; The login screenshot Interface

The above interface is where registered users will authenticate themselves by providing their account number and password. The account balance is a number special account number that is ten-digit number that is automatically and uniquely generated by the system upon registration completion.



E-Payza e-Banking System

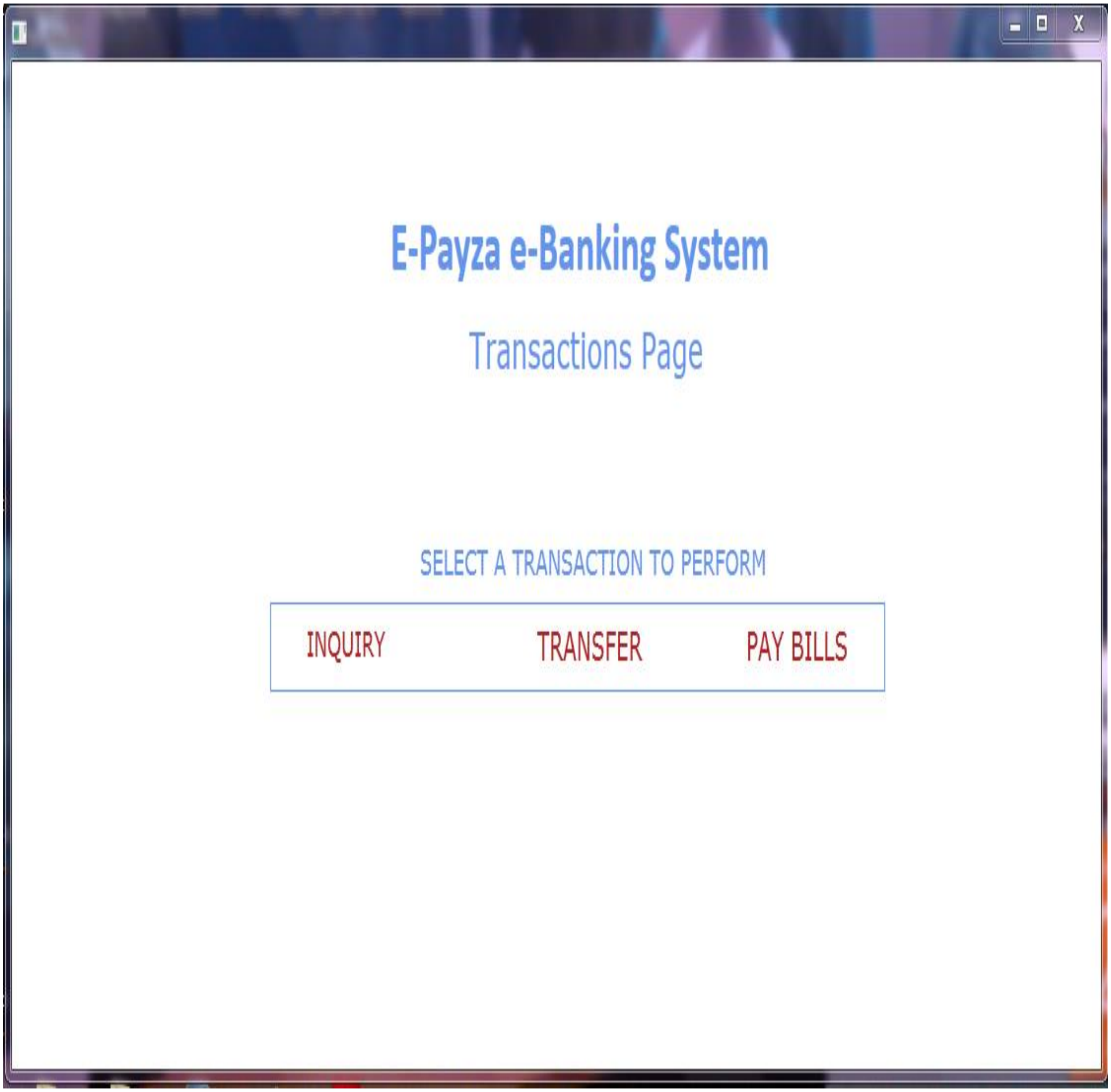
Authenticate Face

One Step To Go Please Look At Your Webcam

Welcome Toni Abayomi

Figure 4.3; The Fingerprint Authentication Interface

On the page, the already authorized user is put through one final test to confirm that he/she is indeed the authentic owner of that account. The application automatically activates the fingerprint scanner and the user is required to thumbprint and submits it. The software then processes the submitted image and compares it to the already processed database image if the recognition level meets a specific threshold the user is authenticated and taken to the transaction page, if not the user is blocked and that session is cancelled.



E-Payza e-Banking System

Transactions Page

SELECT A TRANSACTION TO PERFORM

Fig 4.4; Screenshot the Transaction Interface

Once successful authentication by face the user is deemed bonafide and granted access to his control panel page (transaction page) from where he can perform various actions with his bank account. Transactions like balance inquiry, secure transfer of money and paying bills of registered merchants. The registered merchants could be governmental companies like PHCN or privately held corporations like DSTV.

CHAPTER FIVE

5.1 CONCLUSION

This project has met the objective for which it was designed. This shows that e-banking technology has empowered customers and businesses with the information needed to make better investment decisions. Around the same time, technology allows banks to sell new goods, to work more effectively, to improve efficiency, to grow globally and to succeed internationally.

E-banking has become a critical survival tool and is transforming the banking industry around the world profoundly. Today, the mouse click delivers banking services to consumers at a much lower cost and empowers them with incredible flexibility to choose suppliers for their financial service needs. Given the dynamic and dynamic nature of the economy, no nation today has a preference as to whether to adopt e-banking. The technical takeover of banking has created an information era and commoditized banking services. Banks have come to understand that sustainability in the modern e-economy while continuing to sustain their existing networks, depends on offering any or all their financial services on the Internet.

Biometric access control and authentication are of high importance in this technological age where the level of security awareness is increasing daily, especially in electronic banking. Compared to standard schemes such as keys, personal identifying numbers (PIN), credit cards etc., biometric fingerprint authentication systems offer several usability advantages. Specifically, users will never lose their fingerprints, and it is impossible to steal or fake a fingerprint due to its uniqueness. The internal bit strength of a fingerprint is relatively strong compared to conventional passwords. Finger scanners are becoming smaller, less costly and more precise. They can be used in gadgets without the scale, price and power usage being spruced up. Identity theft and unauthorized access to people's accounts can be reduced by the use of this technology. The definition, design, construction and execution of the project showed that the use of biometric fingerprints to ensure protection is not only limited to e-banking, but also in all other areas of human life.

5.2 LIMITATIONS

The limitations I encountered while undergoing this research work were the integration of Java, web technology used during the developmental process, hardware limitation (Getting a sensitive scanner), and interfacing software with the hardware.

5.3 RECOMMENDATION

With the high level of various biometric security technologies available in the world today, the following recommendations should be noted.

Firstly, knowledge of biometrics should be taught as a core course in higher schools.

Also knowledge and real-life application of good but simple algorithms, programming language and cryptography should be taken seriously not only by students inside the field of computing but all other fields as well since the use of biometric technology encompasses all areas of life for security and access control.

I also recommend that with better, cost-effective and more efficient design, this project can be implemented where applicable within the university system e.g. in the cafeteria, instead of the traditional issuing of Identification cards by students, a simple fingerprint biometric system will be more efficient and faster.

Finally, financial Institutions, Security outfits (Police stations, prisons military zones etc), corporate organizations in Nigeria that are yet to embrace this technology should be educated about it and more awareness should be done on the advantage that fingerprint biometrics has over all other biometric traits.

REFERENCES

Adrian, T., & Shin, S. H. (2008). Liquidity, monetary policy and financial cycles. *Current issues in economics and finance*.

Alison Arthur and Bethany Frank. (2019, May 8). Examples of Biometrics in Banking. pp. https://www.alacriti.com/biometrics-in-banking.

Anyanwaokoro, M. (1999). *Theory and Policy of Money and Banking.* Enugu: Hosanna Publications.

Biswas, S., & B, A. (2012). A Structure of Safe ATM Banking focused on Biometric Authentication. International Journal Software and Computer Science Advanced Study *Engineering*.

Brey, P. (2007). Ethical aspects of information security and privacy.

Byers, R., &Lederer, P. J. (2001). Retail bank services strategy: a model of traditional, electronic, and mixed distribution choices. *Management Information Systems Journal*, 56-133.

Chai, L. G. (2015). E-Banking in Malaysia: Opportunity and Challenges. *Journal of Internet Banking and Commerce*.

Christensson, P. (2013, May 23). *WAMP Definition*. Retrieved 2020, Oct 13, from https://techterms.com

CHRISTOHE, N. J. F. (2007, October 21). Architectural Diagram of an ATM System. Blogger. Retrieved 18:03, October 17, 2020, from http://csacsenavet.blogspot.com/2007/10/assignment-2-architectural-diagram-of.html

Clive, W. (2007). *Academics Dictionary of Banking.* New Delhi: Arrangement Academic New Delhi.

Daniel, E. (1999). Electronic banking provision in the UK and Ireland. Bank International Journal *Marketing*, 72-82.

Daula, S., Murthy D. S., Pulla G. (2012). An Embedded ATM Protection Design using Fingerprint Recognition and ARM Processor GSM.

Durkin, M. (2007). On The role of bank employees in online customer service purchase.

Marketing Intelligence & Planning Journal, 82-97.

Evan.bovie. (2012, Jully 2).

F. S. Hossain, A. N. (2013). ATM Banking System Biometric Authentication Scheme Using an Energy Efficient AES Processor. Journal of Information and Computer Science International *(IJICS)*.

Gao, P., &Owolabi, O. (2008). Nigeria's market embrace of internet banking. Foreign Electronic Journal *finance*.

Greeta, S. N., Swati, S. J., &Aaradhana, A. D. (2012). A futuristic enhanced security strategy, M-Banking Security. IJCSI Computer Science International Journal *Issues*.

Hogarth, J., &Anguelov, C. (2004). Are families who use e-banking better financial managers? *Journal of financial counseling and planning*.

Hogarth, M. J., Kolodinsky, J., &Hilgert, A. M. (2004). US customers' embrace of electronic banking innovations. International bank marketing journal. F. S., Hossain, & N, A. (2013) (2013). ATM Banking System Biometric Authentication Scheme Using an Energy Efficient AES Processor. International Knowledge and Computer Science Journal. Jain, A. K., & Ross, A. (2015). Multibiometric Systems, Communications of the ACM. In A. K. Jain, & A. Ross, *Multibiometric Systems, Communications of the ACM* (pp. 34-40).

Jeanne M. Hogarth, J. M. (2004). *emeraldinsight.*

Jones. A. (March 6, 2019). All about EMV Contactless. Global Payments Integrated. Retrieved 11:35, October 17, 2020, from https://www.globalpaymentsintegrated.com/en-us/blog/2019/03/06/the-next-big-thing-in-payment-processing-emv-contactless

Kagan, J. (2018). *Automated Teller Machine (ATM).* Investopedia.

KAGAN, J. (2018, Aug 3). *investopedia*. Retrieved from https://www.investopedia.com/terms/a/atm.asp

Keng, C. (2018, May 10). *Forbes*. Retrieved from https://www.forbes.com/sites/cameronkeng/2018/05/10/starting-a-passive-atm-business/#7608a7607b1e

Lan, A. (2011, September 15). E - BANKING. SlideServe. https://www.slideserve.com/Albert_Lan/e-banking-banking-internet

Leow, H., & Bee, H. (1999). New distribution channels in banking services. *Bankers Journal Malaysia*, 45-56.

Liu, C.-C. (2008). The relationship between digital capital of internet banking and business performance. *Foreign Electronic Journal finance*.

Luther Simjian, J. S.-B. (1960,1967,1969). *softschools.com*. Retrieved from http://www.softschools.com/inventions/history/automated_teller_machines_history/15/

Mols, N. (1998). PC banking's behavioral implications. Bank Marketing International Journal, 195-201.

O. Oudu, N. T. (2010). "Tokenless Cancelable Biometrics Scheme for Protecting Iris Codes". *Proc. 20th Intl Conf. Pattern Recognition (ICPR)*.

Omotayo, G. (2007). A Dictionary of Finance. *International Journal of Electronic Publications finance*, 18-30.

ONWUKA, E. (2015, june 23). *naijaonlinebiz*. Retrieved from https://www.naijaonlinebiz.com/15-top-uses-of-automated-teller-machine-atm/

Oudu, O., & T, N. (2010). Tokenless Cancelable Biometrics Scheme for Protecting Iris Codes. *Proc. 20th Intl Conf. Pattern Recognition (ICPR)*.

Ramadan, E. (2016). ATM and POS Application Architecture.

Ramrakhyani, E. A. (2017). Fingerprint Based ATM System: Survey. *International journal of creative science, innovation and engineering study technology*.

S. Venkatraman, I. D. (2008). A Case Study," Information Management & Computer Security.

S.Oko, J. O. (2012). Enhanced ATM Security System using Biometrics.

Servon, J. L., &Kaestner, R. (2008). Consumer financial literacy and the impact of online banking on the financial behavior of lower income bank customers. *The journal of consumer affairs*.

Singh, B., &Malhortra, P. (2009). Adoption of Internet banking: An empirical investigation of Indian Banking Sector. *Journal of Internet Banking and Commerce*.

SnehaRamrakhyani, M. M. (2017, November). Fingerprint Based ATM System: Surve. *ijirset*, 6.

Sonal. (Dec, 10 29).

Van Hoeck. (2001).

Venkatraman, S., &Delpachitra, I. (2008). Biometrics in banking security: A case study. *Information management and computer security*.

Wikipedia contributors. (October 4, 2020). Automated teller machine. In *Wikipedia, The Free Encyclopedia*. Retrieved 22:31, October 13, 2020, from https://en.wikipedia.org/w/index.php?title=Automated_teller_machine&oldid=981756400

Wikipedia Contributors. (2020, September 27). DNA. *Wikipedia, The Free Encyclopedia*. Retrieved, October 13, 2020 from https://simple.wikipedia.org/w/index.php?title=DNA&oldid=7124521.

APPENDIX
PROGRAMMING LISTING

```
using System;
usingSystem.Collections.Generic;
usingSystem.Linq;
usingSystem.Text;
usingSystem.Windows;
usingSystem.Windows.Controls;
usingSystem.Windows.Data;
usingSystem.Windows.Documents;
usingSystem.Windows.Input;
usingSystem.Windows.Media;
usingSystem.Windows.Media.Imaging;
usingSystem.Windows.Navigation;
usingSystem.Windows.Shapes;
usingSystem.Windows.Forms;
usingSystem.Drawing;
usingWebCam_Capture;
usingMySql.Data.MySqlClient;
usingAForge;
usingAForge.Math;
usingAForge.Imaging;
usingAForge.Imaging.Filters;

namespace BBACS
{
///<summary>
/// logic of Interaction for Authenticate.xaml
///</summary>
publicpartialclassAuthenticate: Page
    {
public Authenticate()
        {
InitializeComponent();
        }

publicList<string> Values;
publicList<string> Values1;
publicList<string> Values2;
```

```
publicList<string> Values3;
publicSystem.Windows.Forms.PictureBoxmypic;
publicSystem.Windows.Forms.PictureBox mypic2;
publicint rand;
publicstring sub;

privatevoidauthenticate_Loaded(object sender, RoutedEventArgs e)
        {
Uri r = NavigationService.Source;
string path = r.ToString();
int full = path.Length;
sub = path.Substring(18, full - 18);
//System.Windows.MessageBox.Show(sub);

stringconnectionstring = "SERVER = localhost; DATABASE = access; UID = root; PASSWORD =
'';";
MySqlConnection connect = newMySqlConnection(connectionstring);

try
            {
connect.Open();
            }
catch (Exception ex)
            {
System.Windows.MessageBox.Show("Registration Failed Unable to Connect To Our Database.
Try Again!" + ex.Message);
            }


stringcmdtext = "SELECT * FROM `users` WHERE id = '"+ sub +"';";
MySqlCommandcmd = newMySqlCommand(cmdtext, connect);

try
            {
MySqlDataReader reader = cmd.ExecuteReader();
                Values = newList<string>();
                Values1 = newList<string>();
                Values2 = newList<string>();
                Values3 = newList<string>();
while (reader.Read())
                {
Values.Add(reader["fullname"].ToString());
Values3.Add(reader["imgpath"].ToString());
                }

            }
catch (Exception ex)
            {
System.Windows.MessageBox.Show(ex.Message);
            }

welcome.Content = "Welcome "+ Values[0];

Bitmap bit = newBitmap(Values3[0]);


            mypic2 = newPictureBox();
            mypic2.SizeMode = PictureBoxSizeMode.StretchImage;
snaphost.Child = mypic2;

//mypic2.Image = bit;
mypic = newPictureBox();
mypic.SizeMode = PictureBoxSizeMode.StretchImage;
myhost.Child = mypic;

WebCamCapture camera = newWebCamCapture();
camera.Start(0);
camera.ImageCaptured += newWebCamCapture.WebCamEventHandler(Cam_ImageCaptured);

        }


publicvoidCam_ImageCaptured(object source, WebcamEventArgs e)
        {
mypic.Image = e.WebCamImage;
        }

privatevoid button1_Click(object sender, RoutedEventArgs e)
        {
Random r = newRandom();
rand = r.Next(10, 10000);
Bitmap bee = newBitmap(mypic.Image);
AForge.Imaging.Filters.GrayscaleRMY gray = newAForge.Imaging.Filters.GrayscaleRMY();
bee = gray.Apply(bee);
bee.Save("./images/temp/" + rand.ToString() + ".png");
            mypic2.Image = bee;

rec.IsEnabled = true;
        }

privatevoidrec_Click(object sender, RoutedEventArgs e)
        {
NavigationService.Navigate(newUri("Transact.xaml?" + sub, UriKind.Relative));
        }

    }
}


using System;
usingSystem.Collections.Generic;
usingSystem.Linq;
usingSystem.Text;
usingSystem.Windows;
usingSystem.Windows.Controls;
usingSystem.Windows.Data;
usingSystem.Windows.Documents;
usingSystem.Windows.Input;
usingSystem.Windows.Media;
usingSystem.Windows.Media.Imaging;
usingSystem.Windows.Navigation;
usingSystem.Windows.Shapes;
usingSystem.Windows.Forms;
usingWebCam_Capture;
usingMySql.Data.MySqlClient;
using System.Drawing.Drawing2D;
usingSystem.Drawing;
usingSystem.Drawing.Imaging;

namespace Access
{
```

```
///<summary>
/// Interaction logic for MainWindow.xaml
///</summary>
publicpartialclassMainWindow :Page
    {
publicMainWindow()
        {
InitializeComponent();
        }

publicList<string> Values;
privatevoidlogin_Click(object sender, RoutedEventArgs e)
        {
if (user.Text == "" || pass.Text == "")
            {
System.Windows.MessageBox.Show("All Fields Must Be Completed!");
            }
else
            {

stringconnectionstring = "SERVER = localhost; DATABASE = access; UID = root; PASSWORD =
'';";
MySqlConnection connect = newMySqlConnection(connectionstring);

try
                {
connect.Open();
                }
catch (Exception ex)
                {
System.Windows.MessageBox.Show("Registration Failed Unable To Connect To Our Database.
Try Again!" + ex.Message);
                }

stringcmdtext = "SELECT id FROM `users` WHERE username = '" + user.Text + "' AND pass =
'" + pass.Text + "';";
MySqlCommandcmd = newMySqlCommand(cmdtext, connect);


try
                {
MySqlDataReader reader = cmd.ExecuteReader();
                    Values = newList<string>();
while (reader.Read())
                    {
Values.Add(reader["id"].ToString());
                    }

string[] list = Values.ToArray();
if (list.Length == 0)
                    {
invalid.Visibility = Visibility.Visible;
                    }
else
                    {
// /BBACS;component/bin/Debug/images/352738738.png
intlen = list.Length;
System.Windows.MessageBox.Show("Login Successful!!");
NavigationService.Navigate(newUri("Authenticate.xaml?" + list[0], UriKind.Relative));
                    }
                }
catch (Exception ex)
                {
System.Windows.MessageBox.Show(ex.Message);
                }
            }
        }
    }
}
```