BIOMETRIC AUTHENTICATION BASED ATM MACHINE

Bose Arok.J

Abstract

Security measures at banks can play a critical, contributory role in preventing attacks on customers. These measures are of paramount importance when considering vulnerabilities and causation in civil litigation. Banks must meet certain standards in order to ensure a safe and secure banking environment for their customers. This paper focuses on vulnerabilities and the increasing wave of criminal activities occurring at Automated Teller Machines(ATMs). where quick cash is the prime target for criminals rather than at banks themselves. A biometric measure as a means of enhancing the security has emerged from the discourse. A general iris recognition system is used for the security.

Keywords: Security, ATM, Biometric, Crime

I. INTRODUCTION

Automated teller machine is a mechanical device that has its roots embedded in the accounts and records of a banking institution. It is a machine that allows the banks customers carry out banking Transactions like, deposits, transfers, balance enquiries and withdrawal most of the Modern ATM's uses plastic magnetic card (ATM Card) to identify Account Details. This magnetic tape will have unique card number and security information embedded. It is possible to hack the account data and security information & Pin Number. This issue can be resolved by using Bio-metric Authentication for user/customer. This will resolve most of the security related issues minimize from the hackers to hack them. Security measures at banks can play a critical, contributory role in preventing attacks on customers. These measures are of paramount importance when considering vulnerabilities and causation in civil litigation and banks must meet certain standards in order to ensure a safe and secure banking environment for their customers. Basically, the ATM scam involves thieves putting a thin, clear, rigid plastic sleeve into the ATM card slot. When you insert your card, the machine can't read the strip, so it keeps asking you to re-enter your PIN number. Meanwhile, someone behind you watches as you tap In your number. Eventually you give up, thinking the machine has swallowed your card and you walk away. The thieves then remove the plastic sleeve complete with card, and empty your Account. The way to avoid this is to run your finger along the card slot before you put your card in. The sleeve has a couple of tiny prongs that the thieves need to get the sleeve out of the slot, and you'll be able to feel them. The primary focus of this work is on developing a biometric strategy (Fingerprint) to enhance the security features of the ATM for effective banking transaction. The iris of the eye has a unique pattern, from eye to eye and person to person.

II. METHODOLOGY

The security feature for enhancing the ATM was designed using the client/server approach. There will be a link between the customer's identification information, customer's accounts and records in the bank (server). The network is designed to support a large number of users and uses dedicated server to accomplish this. The reason for choosing Client/Server model for this application is

because it provides adequate security for the resources required for a critical application such as Banking. Similarly, a descriptive conceptual approach which includes Unified Modeling language (UML) tools such as Use Case models, class diagrams etc is adapted. Microsoft Access 2003 as a database software is employed to create database to store cardholder's information. The work is implemented using Visual Basic 6.0 software tool, used to design the user interfaces and/or cardholder interaction with the ATM Machine. Since iris is small in size and dark in color, it is difficult to acquire good image. Also all the subsequent steps depend on it. A Panasonic camera has been used to take eye snaps while trying to maintain appropriate settings such as lighting, distance to the camera and resolution of the image. The image is then changed from RGB to gray level for further processing. finger print of the user Since the finger print is unique for everyone no one can imitate the user for malpractices After verification of the finger print the User can communicate with the ATM Machine for Money Transaction.

III.MOTIVATION

The Motivation of the project is to Secure the Money From Strangers The money theft is totally dropped from the ATM Machine It is very useful for users to secure the money from the stranger This technology can be very useful for the customers since they are not using the current ATM's with safe. The people's authentication can be decided using the finger print of the user Since the finger print is unique for everyone no one can imitate the user for malpractices After verification of the finger print the User can communicate with the ATM Machine for Money Transaction.

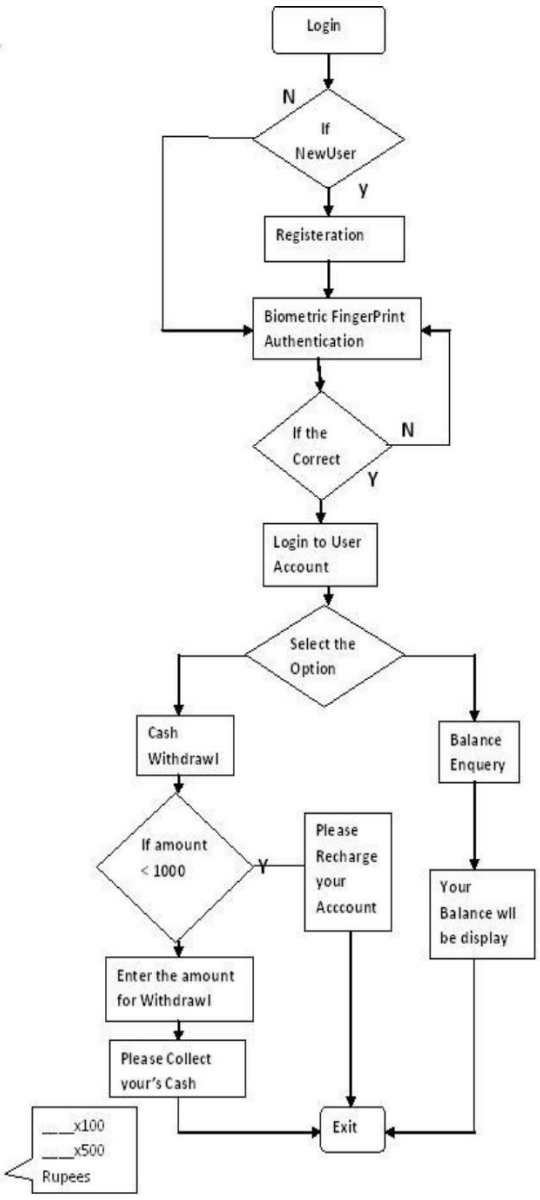
IV.BIOMETRIC SYSTEM SECURITY

Although biometric systems can be used for reliable user authentication, a biometric system itself is vulnerable to a number of threats. The goal of this project is to identify the vulnerabilities of a biometric system and provide solutions to counter these threats. Biometric cryptosystems combine biometrics and cryptography effectively to improve the security and privacy of biometric systems. A critical issue in biometric systems is protecting the template of a user which is typically stored in a database or a smart card. Cryptographic constructions such as fuzzy vault can be used for template protection and secure biometric matching. Iris recognition as a biometric technology has great advantages such as variability, stability and security. Thus it will have a variety of applications.

V. SYSTEM DESIGN AND IMPLEMENTATION

This research is being carried out for the sole purpose of designing a three factor authentication metrics, that is, the ATM ID number, the PIN number and the Biometric feature (fingerprint). It is expected that the customer should possess an ATM card, to know and remember his/her PIN number and to enroll his/her fingerprint into the fingerprint device/reader adapter into the system. The ATM card accepts our credit/debit card and the PIN number to dispense cash. Biometric ATM's are the latest inventions to help us avoid fraud and duplication. If somebody steals our card and also knows our PIN they can easily withdraw cash from our account. In case of biometric ATM's they cannot use. These cannot be duplicated and hence they are very safe and secure for transaction. But they are very costly when compared to traditional ATM machines and hence they are not very widely used now. A retinal scan has an error rate of 1 in 10,000,000, compared to fingerprint identification error being sometimes as high as 1 in 500.

VI.DESCRIPTION



From the System Flow Diagram,

The User Login to the User account (If New user mean) they want to Register for Money Transaction. Biometric Finger Print Device is used for Login to the User Account. If new User mean Register, otherwise Login to the user account. The Biometric Authentication is used for entering the user into the account. They allow to access two process (Balance Enquiry/Cash Withdrawal).In the balance Enquiry option the user can able to saw the Balance Money. In the cash withdrawal option, if the total amount is below thousand rupees mean the Cash withdrawal is not be allow. Otherwise, Enter the amount for cash thousand rupees mean the Cash withdrawal is not be allow. Otherwise, Enter the amount for cash withdrawal. The amount for withdrawal is displayed on the screen.

Please collect your cash

500x_

100x_____Rupees

VII CONCLUSION

We have been able to develop a fingerprint mechanism as a biometric measure to enhance the security features of the ATM for effective banking transaction for Banks in Nigeria. The prototype of the developed application has been found promising on the account of its sensitivity to the recognition of the customers' finger print as contained in the database. This system when fully deployed will definitely reduce the rate of fraudulent activities on the ATM machines such that only the registered owner of a card access to the bank account