Enhancing ATM Security using Fingerprint and GSM Technology

V.Padmapriya
Research Scholar
SCSVMV University
Enathur, kanchipuram

S.Prakasam, Ph.D
Asst. professor
Department of CSA, SCSVMV University
Enathur, kanchipuram

ABSTRACT
There is need for improve security in ATM transactions. Due to tremendous increase in the number criminals and their activities, the ATM has become insecure. ATM systems today use no more than an access card and PIN for identity verification. The Personal Verification Number(PIN) not only give good security. The fingerprint is unique and cannot duplicate by others. This paper combine the pin verification and fingerprint recognition technology for identification. With fingerprint recognition technology and pin verification we embedded the GSM modem connected to the microcontroller generates the 4 digit one time password and it send to the main user mobile number when the user (main user or nominee user) enroll the fingerprint. The fingerprint of the nominee and the card holder are collected and stored in the database. Every fingerprint which enrolls is check by the db. The 4digit one time password should be entered by pressing the keys on the touch screen. After enter all the correct information customer can begin the further transaction. We also proposed nominees fingerprint identification process while actual card holder unable to do the transactions. The biometric features cannot be replicated, this proposal will go a long way to solve the problem of account safety.

Keywords: ATM, Fingerprint, GSM, magnetic strip card

1. INTRODUCTION

Rapid development of banking technology has changed the way banking activities are dealt with. One banking technology that has impacted positively and negatively to banking activities and transactions is the advent of automated teller machine (ATM). It is a computerized machine designed to dispense cash to bank customers without need of human interaction. Today the ATM users are increase in numbers. They use the ATM cards for banking transactions like deposits, transfers, balance enquiry, mini statement, withdrawal, fast cash, etc [1].

The ATM machine has card Reader and keys as input devices and display screen, cash dispenser, receipt printer, speaker as output devices. ATMs are connecting to a host processor, which is a common gateway through which various ATM networks become available to users. Various banks, independent service providers owned this host processor.

Account information of user is stored on the magnetic strip present at the back side of the ATM card. When we enter the card in the card reader, the card reader captures the account Information and the information is used for the transaction purpose. And we have to insert the pin by keys. The pin is the 4 digit number given to all ATM card holders. ATM card holders pin are different from each others. The number is verifying by the bank and allows the customers to access their account. The password is only identity so anyone can access the account when they have the card and correct password. Once the card and the password is stolen by the culprit they can take more money from the account in shortest period, it may bring huge financial losses to the users [2].

To increase security level we are introducing new technology which works the technology fingerprint recognition system and nominee for the main user and GSM technology. Physical characteristics include fingerprint, hand or palm geometry, retina, iris and face while popular behavioral characteristics are signature and voice. Biometrics technologies are a secure means of authentication because biometrics data are unique, cannot be shared, cannot be copied and cannot be lost. The fingerprint based identification is one of the most mature and proven technique [3]. So we use the fingerprint for the identification purpose. The fingerprint of the card and nominee will be stored in the db of the bank when the cardholder or the nominee tries to access the account; they will have to enter the pin and need to enroll the fingerprint. The finger print is check by the bankers, if it is in the data base the 4 digit code is send to the user by the GSM technology (Global system for mobile communication).

The GSM technology is cellular network which means that mobile phone connect to it by searching for cells in the immediate vicinity [2]. The GSM modem connected to the microcontroller generates the 4 digit code to the main user mobile number [1]. The user can access the account after he/she enter one time password. After they can begin the transactions. We made the transactions what we want like deposits or withdrawal, etc. After complete our transaction we can get the card.

2. RELATED WORKS
ATM can be described as Any Time Money. We can get money at anytime anywhere only through ATM machines. To do the secure transactions we need biometric authentication. Biometric authentication is a growing and controversial field. Today biometric laws and regulations are in process and biometric industry standards are being tested. Automatic recognition based on “who you are as opposed to “what you know” (pin) or “what you have” (ID card).

2.1 Comparative table

Table 1 comparative table

Title and author	Method	Strength	Limitation
Fingerprint recognition using minutia score matching by Ravi J K.B.Raja, Venugopal K.R. 2009	Minutia score matching method	Fingerprint thinning is used.	-
Fingerprint validation and outlier detection using minutiae approach in network security by Prathima Devi sirivella, Mrs. D. Raga vamsi 2004.	User verification based on the elliptical curve.	This approach gives better results in real time applications from database type of attacks.	Future improvement in the terms of efficiency and accuracy or improve the hardware to capture the image
Implementation of the security by using fingerprint recognition and GSM by Pennam Krishna murthy & Maddhusudhan red 2008.	1.Finger print recognition. 2.Remoteau thentication 3.Message alarming. 4.Gobor and direction filter algorithm.	GSM modem is connected s3c2440 chip is embedded with the technologie s of fingerprint recognition.	Gobor and direction filter algorithm is used but it slow in dealing with high capacity requirement.
Designing a biometric strategy(fingerprint) measure for enhancing ATM security in Indian E-Banking system-2011 by Sri Shimal Das smt.Jhunnu D	Tools UML &VB 6.0/passw ord and fingerprint recognitio n	Fingerprin t is used as a biometric template & nominees are used.	Missed to explain about what failure cause.

2.2 Discussion

Implementation of the security by using fingerprint recognition and GSM. By Pennam Krishna murthy & Maddhusudhan reddy using fingerprint recognition method, remote authentication, message alarming and Gobar and direction filter algorithm, it is more safe and reliable and easy to use but it is slow when dealing with high capacity requirements.

The United Kingdom recently launched identity card scheme which has been analyzed by Shaikh and Rabaiotti(2009). They approach the scheme from the perspective of high volume public deployment and describe a trade-off triangle model. They have found that there is a trade-off between several characteristics, i.e., accuracy, privacy and scalability in biometric based identity management system, where emphasis on one undermines the other (Shaikh and Rabaiotti2009).

Fingerprint recognition using minutia score matching by Ravi J K.B.Raja, Venugopal K.R. using the minutia score matching method and gives the better FMR value compare to the existing. Fingerprint validation and outlier detection using minutia approach in network security by Devi sirivella, Mrs.D.Raagavamsi gives the better result in real time applications from database type of attacks.

Recently Govt. of India started a biometric based ID card i.e., 'unique identification authority of India', it provides a unique identity to person residing in India[1].

3. PROPOSED SYSTEM

The ATMs are networked and connected to a centralized computer (Switch), which controls the ATMs. The use of biometric identification is possible at an ATM. The information can be stored at a bank branch or Network Provider. The typical ATM has two input devices (a card reader and keypad) and four output devices (display screen, cash dispenser, receipt printer, and speaker). Invisible to the client is a communications mechanism that links the ATM directly to an ATM host network. The ATM functions much like a PC, it comes with an operating system (usually OS/2) and application software for the user interface and communications.

While most ATMs use magnetic strip cards and personal identification numbers (PINs) to identify account holders, other systems may use smart cards with fingerprint validation. The ATM forwards information read from the client's card and the client's request to a host processor, which routes the request to the concerned financial institution. If the cardholder is requesting cash, the host processor signals from the customer's bank account to the host processor's account.

Once the funds have been transferred, the ATM receives an approval code authorizing it to dispense cash. This communication, verification, and authorization can be delivered in several ways. Leased line, dial-up or wireless data links may be used to connect to a host system, depending on the cost and reliability of the infrastructure. The host systems can reside at a client's institution or be part of infrastructure. The host systems can reside at a client's institution or be part of an EFT network. The EFT network supports the fingerprint authentication. Point-of-sale services that use biometric solutions are also possible.

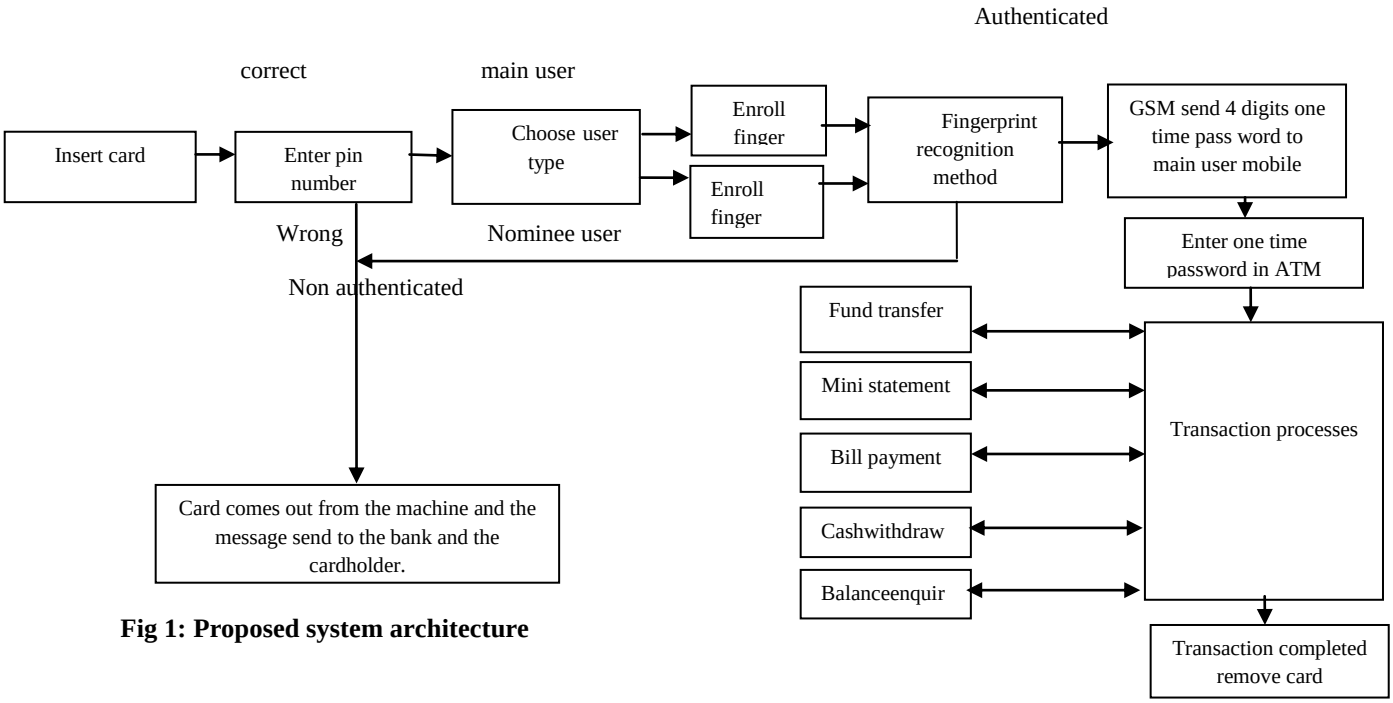

Fig 1: Proposed system architecture

With the fingerprint reorganization method we also embedded the GSM technique. That the GSM modem connects to microcontroller. That will send the 4 digit code to the user(when the card insert by the main user or nominee the 4digit number only send to the main user only for the knowledge of the main user). After enter the 4digir number the transaction will begin. The user may do the transactions like fund transfer, cash withdrawal, mini statement, bill payment, balance enquiry. After all the transactions done the card will comes out from the machine. So the system is so safe and secure, and it avoid the security problems what we face in the previous works.

3.2 Functionality of the Architecture

This system consists of 3 validation functions. First it validates the pin number second fingerprint. At last it validates the one time password which is send by GSM modem to the main user mobile number. The functionality of the system will explain by the below steps.

Step 1: insert the card

Step 2: Enter card's password. Correct password means step-4 follows false means step-3 follows

Step 3: The card comes out from the machine and the message send to banker.

Step 4: choose user type. Main user means step-5 follows. Nominee means Step-10 follows.

Step 5: Enroll the finger print. The user finger print already saved in the database. If authentication failure means next step follows. If success means step-7 follows.

Step 6: The card comes out from the machine and the message send to banker.

Step 7: With the help of GSM four digit one time pass word is send to main user mobile number.

Step 8: We need to type the 4 digit one time password on ATM machine

Step 9: Then the transaction begins after completion of transaction the card will come out.

Step 10: If second type user means the nominee must enroll the finger print then step-7, step-8, step-9 follows.

4. ADVANTAGES OF PROPOSED WORK

1. The GSM technology is cellular network, which means that mobile phones connect to it by searching for cells in the in the immediate vicinity it will make the authentication fast.

2. The fingerprint recognition will make the system so secure.

3. The nominee user also used so instead of the main user the nominee will access the account in case of emergency.

4. The one time password send by GSM modem to the main user changes every time so it provide good security.

5. Other advantage of the system validation functions. Pin validation, fingerprint validation and one time password are made it is one of advantage of the system.

The below mention bar chart is according to the data collected from 35professors, 25students, 35bank employs, 25 government employs and we have also discussed with middle literate(30) people to understand the effectiveness of the proposed system. As per the survey we have got positive report from these people.

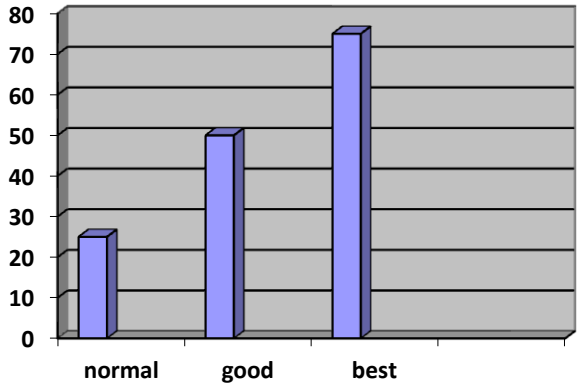

Fig 2: effectiveness of proposed work

The above bar chart shows the effectiveness of the proposed system.

5. CONCLUSION

Automatic Teller Machines have become a mature technology which provides financial services to an increasing segment of the population in many countries. Biometrics, and in particular fingerprint scanning, continues to gain acceptance as a reliable form of securing access through identification and verification processes. This paper identifies a high level model for the modification of existing ATM systems using both security protocols as PIN & Biometric fingerprint strategy and GSM technology. We have been able to develop a fingerprint mechanism as a biometric measure to enhance the security features of the ATM for effective banking. The prototype of the developed application has been found promising on the account of its sensitivity to the recognition of the cardholders and nominees‟ 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 and nominee, access to the bank account, and the nominee user also will do the transaction so it is more comfortable in case of emergency.

6. FUTURE DIRECTIONS

1. These are so many fingerprint recognition models are available practice with new fingerprint recognition method.

2. Try this with two or more nominees.

3. Use the minutia approach for avoiding the database type attacks.

7. REFERENCES

[1] Implementation ATM security by using fingerprint recognition and GSM by Pennam Krishna murthy & Maddhusudhan reddy

[2] Designing a biometric strategy(fingerprint) measure for enhancing ATM security in Indian E-Banking system-2011 by Sri Shimal Das smt.Jhunnu Deddarma

[3] A method to improve the security level of ATM banking systems using AES algorithm, N.Selvaraj & G.Sekar, international journal of computer applications(0975-8887)volume 3- no.6.,june 2010.

[4] Fingerprint recognition using minutia score matching by Ravi J K.B.Raja, Venugopal K.R

[5] Fingerprint validation and outlier detection using minutiae approach in network security by Prathima Devi sirivella, Mrs. D. Raga vamsi.

[6] Lin Hong, Wan Yifei, Anil Jain. Fingerprint image enhancement: algorithm and performance evaluation[J]. IEEE Transactions on pattern Analysis and Machine intelligence. 1998,20(8):777-789.

[7] Gu J,Zhou J Zhang D.A combination model for orientation field of fingerprints. Pattern Recognition, 2004,37:543-553.

[8] Cheng J,Tian J. fingerprint enhancement with dyadic scle –space. Pattern Recognition Letters,2004,25(11):1273-1284.

[9] Diniz,E(1998) Web Banking in USA. Journal of international Banking and commerce,3,(2).

[10] A UID NUMBERING SCHEME,Hemant Kanakia, Srikanth Nadhamuni and Sanjay Sarma,May 2020

[11] E-banking Functionality and Outcome of Customers Satisfaction An Empirical Investigation feb 2011 by Dr.Ala'Eddin Mohd Khalaf Ahmad and Dr.Hasan Ali Azu'bi.

[12] Journal of Internet Banking and Commerce, December, 2012 vo17,no3(http://www.arraydev.com/commerce/jibc/)

[13] Facial Verification Technology Use in ATM TransactionsAru, Okereke, Eze, Ihekweaba Gozie

[14] ATM security Using Fingerprint Biometric Identifier: An investigate Study 2012 by Moses Okechukwu Onyesolu, Ignatius Majesty Ezeani

[15] Towars Designing a Biometric Measure for Enhancing ATM security in Nigeria E-banking System by Ididapo, Akinyemi, Zacheous, Omogbadegun, and olufam M.Oyelami.