Multi Account Embedded System with Enhanced Security

Devika[1], Vaishnavi[2], Ankitha[3], Chandana [4]

[1]*Proffessor, Department of TCE, K S Institute of Technology, Bangalore, Karnataka, India*
[2]*IV year student, Department of TCE, K S Institute of Technology, Bangalore, Karnataka, India*
[3] *IV year student, Department of TCE, K S Institute of Technology, Bangalore, Karnataka, India*
[4]*IV year student, Department of TCE, K S Institute of Technology, Bangalore, Karnataka, India*

---***---

Abstract - *Automated Teller Machine (ATM) services are more popular because of their flexibility and easiness for banking systems. People are widely using their ATM cards for immediate money transfer, cash withdrawal, shopping etc. On most modern ATMs, the ATM card used by the customer for each bank account which is a plastic ATM card with a magnetic stripe or a plastic smart card with a chip. However, password PIN which is the main authentication for ATM transactions represent the weakest link in the computer security chain. In the proposed Multi Account Embedded ATM card, we embed more than one bank account into a single ATM card so that the customer can carry out the financial transactions for multiple bank accounts. The user need not carry multiple ATM cards and remember multiple passwords. To provide high security we introduced fingerprint based customer authentication. It reduces the cost of inter banking transactions as interfacing different bank databases is a resource consuming thing.*

***Key Words*: ATM(AutomateTellerMachine), PIN(personal Identification Number), Multibanking, Security, Biometric Authentication.**

1. INTRODUCTION

An ATM (Automated Teller Machine) is a machine that enables bank account holders to complete transaction at any time without human intervention. In an ATM system customer authenticate themselves by using a plastic card on which magnetic stripe is mounted known as ATM card. The magnetic stripe carry details related to customer. Sometimes it happens that data on magnetic can be easily destroyed by strong magnetic fields. About PINs (Personal Identification Number), each account has distinct PINs in traditional ATM system occasionally we forget PINs or chance to get confused or losing PIN to someone other. So the ATM card have number of drawbacks like breaking card, losing card, stolen card, losing PIN, forgot PINs, etc. due to such issues there are maximum chances of frauds. ATM system provides users 24 x 7 services for performing straightforward transactions, but as the use of ATM increasing in the same ratio fraudulent attacks [1] on the ATM system are also increasing day by day.

This call for the biometric systems to be integrated in traditional ATM. In Biometric authentication fingerprint based system is becoming highly popular worldwide. In [7] The uniqueness of fingerprint of every individual makes the fingerprint recognition as the most secure system.

This prevents the illegal access to the bank account of a customer. It acts as a latch which opens only if correct key i.e. authorized fingerprint is found. Biometric authentication has been proved its accuracy because the skin on our hands and feet show a stream arrangement of hills on every tip of the finger which is exclusive and abiding.

2. LITERATURE SURVEY

ATM can be described as Any Time Money. We can get money at any time 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.

A survey, as a comparative case study is given in Table I. It deliberates the Biometric techniques in enhancing the security for ATM transaction and other system.

The customer inserts a plastic card with magnetic strip that contains his or her account number. The customer then verifies his or her identity by entering a passcode (i.e.) personal identification number (PIN) of four digits.

User can manage his/her multiple accounts in various banks with the help of this single card.

Since more than one bank accounts are being added, the existing PIN security is not sufficient enough.

The entry of a correct PIN is inadequate to authenticate to the bank system. This is because an additional level has been incorporate for the authentication process which requires the customer to enter a valid code which will be sent to the customer‟s pre-registered mobile device via SMS gateway.

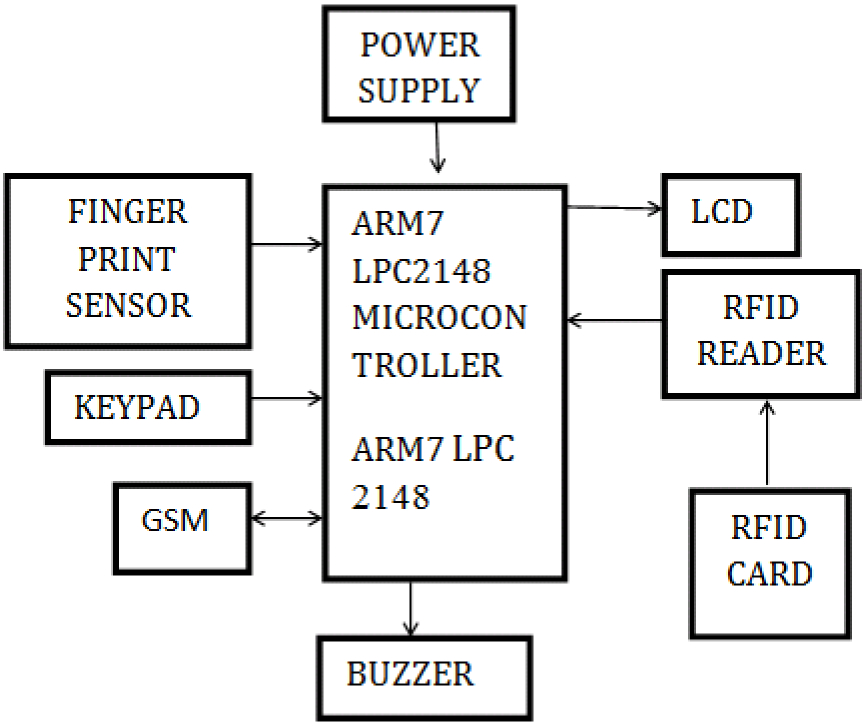
The proposed system can provide a practical and workable solution that addresses the requirements of the regulatory authority of the banks.

User has to maintain various atm cards for different banks.

In this research paper, a greater demand for fast and accurate user identification, authentication and authorization is considered. Therefore, a secure layer of Electronic Transaction mechanism is proposed to developed cardholder identification, authentication, authorization and security clearances. It could provide Better risk/ fraud management. It could enhance trust and confidence which could result more usability of ATM. The above approach made in this paper isn't feasible in context of time and availability of particular mobile network.

3. PROPOSED SYSTEM

Designing a system which is replacing the traditional ATM transaction system by the biometric based fingerprint identification technique and GSM based authenticate transaction. For the purpose of identification, customer fingerprint is required for authentication process. Everyone has unique fingerprint. Thus human fingerprint is replacing the traditional ATM cards and PIN. After successful authentication it gives all the distinct account list of customer and gives permit to perform transactions on the accounts. During transaction process a control transferred to the GSM module to execute an authentication transaction from the bank side.



Methodology

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 forward 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, 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.

To implement the proposed security for ATM terminals with the use of fingerprint recognition, we use the different hardware and software platforms. Fig .1 shows the major system modules and their interconnections.it consist of ARM7 (LPC2148), finger print module GSM module, RFID reader and tags ALCD display.

4. CONCLUSION

In the proposed card-less multi-banking Transaction ATM system, replaces the traditional ATM system. It has advantages such as saves manufacturing cost of cards and overcomes drawbacks of the traditional system like carrying multiple cards, losing of card, losing PINs, remembering multiple PINs, fraud calls related to ATM card, etc. and provides high security by using authentication like fingerprint and OTP system; therefore making it easy to use multiple bank account transaction in a single touch.

REFERENCES

[1] H. Lasisi , A.A. Ajisafe, "Development biometric based fingerprint Authentications Systems in automated teller", IEEE 2nd International Conference on Advances in Computation Tools for Engineering Applications, 2012.

[2] Gokul.R, Godwin Rose Samuel.W, Arul.M, Sankari.C, "Multi Account Embedded ATM Card" International Journal of Scientific & Engineering Research, April-2013.

[3] Harshal M. Bajad1Sandeep E. Deshmukh, Pradnya R.Chaugule3Mayur S. Tambade4, "Universal ATM Card System", International Journal of Engineering Research & Technology (IJERT), October – 2012.

[4] Ronald Petrlic University of Paderborn, "Integrity Protection for Automated Teller Machines", International Joint Conference of IEEE

[5] Ugochukwu Onwudebelu, Olumide Longe, Sanjo Fasola, Ndidi C. Obi and Olumuyiwa B. Alaba , "Real Time SMSBased Hashing .
Scheme for Securing Financial Transactions on ATM Systems", 3rd IEEE International Conference on Adaptive Science and Technology (ICAST 2011).

[6] Algorithm and Performance Evaluation by Lin Hong, Student Member, IEEE, Yifei Wan, and Anil Jain, Fellow, IEEE IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 20, No. 8, August 1998 Fingerprint Image Enhancement.

[7] PENNAM Krishnamurthy, Mr. M. Maddhusudhan Redddy. International Journal of Electronics Communication and Computer Engineering Volume 3, Issue (1) NCRTCST, ISSN 2249 –071X Implementation of ATM Security by Using Fingerprint recognition and GSM.

[8] Youjung Ko, Insuk Hong, Hyunsoon Shin, Yoonjoong Kim"Development of HMM-based Snoring Recognition System for Web Services" 2016 IEEE.

[9] Ashutosh Gupta, Prerna Medhi, Sujata Pandey, Pradeep Kumar, Saket Kumar, H.P.Singh "An Efficient Multistage Security System for User Authentication" International Conference on Electrical,of stripe electronics, and Optimization electronics, and Optimization Techniques (ICEEOT) – 2016.

[10] Shweta Sankhwar,Dhirendra Pandey proposed "A safeguard against ATM fraud".2016 IEEE 6th International Conference on Advanced Computing.