



Smart Card With Fingerprint Identification And Highly Enhanced Security System

Athul Kalesh K, Athul Sanker V, Athira Ashok, Beema Nasrin ,ICET

ABSTRACT: This project proposes a smart atm card with a combination of multiple security compliments , mandatory to provide a high level of protection against fraud and other threats. As a result, the paper proposes framework for user identification and authentication in Automatic Teller Machine (ATMs) using Personal Identification Number (PIN) and Fingerprint identification. In addition with a GSM based security system for ATM machine is provided to prevent theft of money and other illegal activities in ATM machine. The security system automatically will send information to the nearby police station in such situations.

I.INTRODUCTION

An automated teller machine (ATM) or cash machine is an electronic device that allows a bank's customers to make cash withdrawals and check their account balances without the need of human teller. Many ATMs also allow people to deposit cash or cheques, transfer money between their bank accounts, top up their mobile phones prepaid or even buy postage stamps. In most modern ATMs, the customer identifies him or herself by inserting a plastic card with magnetic strip or plastic smart card with a chip that contains his or her account number. The customer then verifies his or her identity by entering a password (i.e.) personal identification number (PIN) of four digits.

If the number is entered incorrectly several times consecutively (usually three), most ATMs will retain the card as a security precaution to prevent an unauthorized user from discovering the PIN by guesswork and so on. Moreover there is a limitation in transaction for the other bank customers in using the ATM of some other bank crossing the limit they have to pay transaction fees. Now a days we often hear a lot of news related to

ATM robbery and thefts .So it is very important to improve the security system.

II. EXISTING SYSTEM

In the existing system, when the user enters the ATM system the user has to insert the respective card of the user's choice into the ATM system's card slot. The next immediate step the user has to do is enter the pin for that particular card. (Authentication purpose). There is a universal rule for ATM system, if the user enters the incorrect password the user will be provided with only three attempts to reenter the pin. In case the user fails to enter the right pin , that particular card will get blocked and for later use the user will have to consult the respective bank executives . Once the PIN is entered and is verified, the user has to select particular transactions to make as per as the user's needs.

The main problem in this system is that the user need to remember different passwords provided by the different banks if he has multiple bank accounts. User has to pay extra charges when transactions are done from different bank's ATM other than ATM card of respective bank after fee transactions are over.

III.PROPOSED DESIGN

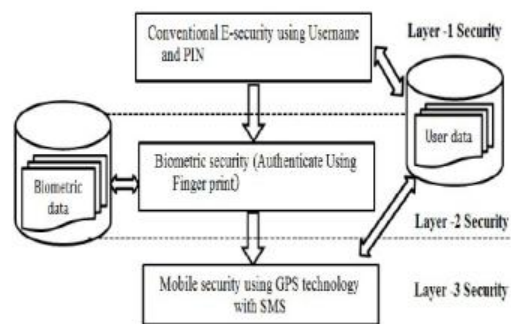


Figure.1 Flow chart for enhanced security system

IV.METHODOLOGY

The proposed design is a smart ATM card by which the customers can use a ATM card with a combination of multiple security complements. Implementation requires minor change in present banking network. The routing algorithm and protocol needs to be changed. In this the user swipes his/her smart card in the ATM machine, then it request for authentication in the server side. After the user is authenticated with his fingerprint, then it displays. The card and fingerprint reader are installed on the ATM which has been already designed using C programming language. Now the user can carry out transaction.

GSM module is also added to this system to send a message to the after swiping the ATM card. This method is used for deactivating fingerprint in case if the user has given the atm card to some other person. If the user replays to the message the access is granted. [2] proposed a system about Efficient Sensor Network for Vehicle Security. Today vehicle theft rate is very high, greater challenges are coming from thieves thus tracking/ alarming systems are being deployed with an increasingly popularity .As per as security is concerned today most of the vehicles are running on the LPG so it is necessary to monitor any leakage or level of LPG in order to provide safety to passenger. Also in this fast running world everybody is in hurry so it is required to provide fully automated maintenance system to make the journey of the passenger safe, comfortable and economical. To make the system more intelligent and advanced it is required to introduce some important developments that can help to promote not only the luxurious but also safety drive to the owner. The system "Efficient Sensor Network for Vehicle Security", introduces a new trend in automobile industry.

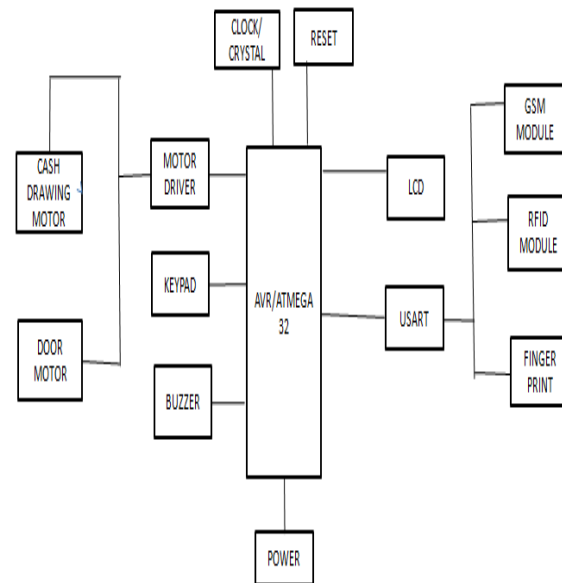


Figure.2 Block diagram of proposed system

A. ATMEGA 32

AVR is a family of microcontrollers developed by Atmel beginning in 1996. The ATMEGA 32 is a high performance, low power microchip 8 bit AVR RISC based microcontroller. Atmega 32 has less execution time, uses Von- Newman architecture and has 131 instructions that can be executed in one clock cycle. The ports PA,PB,PC,PD are four ports of Atmega 32. It has 32*8 general purpose working registers.

B. FINGER PRINT

Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human finger prints. Personal identification based on biometrics has been receiving extensive attention in public security and information security domains. The technology requires the incorporation of a card and fingerprint reader to the ATM and the interaction of the biometric system with the ATMs and the authorizing system.



C. USART

Here a Universal Synchronous/Asynchronous Receiver/ Transmitter (USART) is a type of serial interface device that can be programmed to communicate asynchronously or synchronously. We have to interface microcontroller to personal computer, most easiest way is using a serial port and MAX232. The MAX232 is an integrated circuit that typically is used to convert the RX/TX signals.

D. GSM

GSM is a cellular network, which means that Mobile phones connect to it by searching for cells in the immediate vicinity. GSM networks operate in four different frequency ranges. Most GSM networks operate in the 900 MHz or 1800MHz bands. Some countries in the Americas (including Canada and the United States) use the 850 MHz and 1900 MHz bands because the 900 and 1800 MHz frequency bands were already allocated.

case if the user has given the atm card to some other person. If the user replays to the message the access is granted.



Figure 3, LCD module displaying the request for finger print or personal identification number

V. RESULT

If the user swipes the smart card with the help of smartcard reader it will read the Radio frequency of that smartcard and send to the microcontroller. The microcontroller and the personal computer will connect through MAX232. Then the personal computer will ask for fingerprint authentication. It will access the user fingerprint and if the fingerprint and is matched with the database which is already stored in a microcontroller of that particular database. Now the user can type the amount to be withdrawn. With the help of vending machine and cash drawing motor the user can withdraw the cash. If a thief tries to break the ATM the vibration sensor which senses some voltage due to vibration and it will make a alert using the buzzer. With the help of GSM module which is connected to MAX 232 it will send information to nearby police station and the door of an ATM machine will be automatically closed with the help of DC motor.

GSM module is also added to this system to send a message to the after swiping the ATM card. This method is used for deactivating fingerprint in

VI. CONCLUSION

Thus the user can manage his/her multiple accounts in various banks with the help of this highly secure smart cards. In this project Fingerprint provides a more viable method of identifying users' sufficient security level for the ATM system. The Implementation of ATM security by using fingerprint recognition and GSM took advantages of the stability and reliability of fingerprint characteristics.

The use of human characteristics in this prototype development tackles a lot of security implementation issues in identification and authentication of ATM. The Implementation of ATM security by using fingerprint recognition and GSM MODEM took advantages of the stability and reliability of fingerprint characteristics. Additionally, the system also contains the original verifying methods which are inputting owner's password and which is sent by the controller. The security features were enhanced largely for the stability and reliability of owner recognition. The whole system is built on the technology of embedded system which makes the system more safe, reliable and easy to implement. Since more than one bank



accounts are being added, the existing PIN security and finger print authentication is not sufficient enough, so we can also embed a biometric scan like face recognition and vein authentication in the smart card . So that the user holds the card such that the face and vein rests on the biometric scan reader while he/she swipes the card and the image is authenticated at the real time. No one other than the user can use the card.

Hence, the vulnerabilities of the ATM fraud will be reduced in future.

REFERENCES

- [1] Gokul.R, Godwin Rose Samuel.W, Arul.M, Sankari.C, “MultiAccount Embedded ATM Card” *International Journal of Scientific & Engineering Research*, April-2013
- [2] Christo Ananth, I.Uma Sankari, A.Vidhya, M.Vickneshwari, P.Karthiga, “Efficient Sensor Network for Vehicle Security”, *International Journal of Advanced Scientific and Technical Research (IJST)*, Volume 2, Issue 4, March-April 2014, pp – 871-877
- [3] Ugochukwu Onwudebelu, Olumide Longe, Sanjo Fasola, Ndidi C. Obi and Olumuyiwa B. Alaba , “Real Time SMS-Based Hashing Scheme for Securing Financial Transactions on ATM Systems”, *3rd IEEE International Conference on Adaptive Science and Technology (ICAST 2011)*.

