Dactylogram Based Authentication Along with GSM in ATM

Esther Benita.S[1], Hephzibah Shinny Mol.D[2], Mohana.K[3]
UG Scholars, Department of Computer Science and Engineering
K. Ramakrishnan College of Technology,
Trichy-621112, India

Abstract*:- *The main objective of this system consists of two states of the arts- Portable dab based authentication along with GSM. Fingerprint based identification is the most proven and mature technique while comparing all the biometrics. While performing transaction image of the fingerprint is acquired at ATM terminals using fingerprint scanner which should be high resolution. These acquired fingerprint image is compared with the cardholder's fingerprint. Matching allows the customer to continue the normal ATM transaction. Mismatch triggers confirmation SMS to the cardholder's number which allows the cardholder to accept/deny the transaction. To achieve high security system it can be implemented based on BIOMETRICS (fingerprint) and GSM technology.

Keywords:* *Fingerprint Recognition, GSM SIM800, AT89S52.

I. INTRODUCTION

Biometrics is method that recognizes persons uniquely based on their physiological or behavioral characteristic. Biometrics is used for confidential information such as financial transactions. The different biometric features used are fingerprints, face, palmprint, style of writing, iris, retina, voice and vein. Fingerprinting or finger-scanning technologies are the most commonly used technique of the biometrics. The fingerprint is as a unique feature to identify or verify the individual's identity. Finger-scan technology is the most commonly conveyed biometric technology, used in a wide range of logical access and physical access applications. Among all of those fingerprint was chosen because in other biometric cases there are slight recognition problems. For example iris scanner has complication while scanning eyes with lens. All fingers in a human have unique patterns which are commonly known as fingerprint. A fingerprint is a mark design formed of lines and spaces which is unique. The lines are the ridges. The spaces between the valleys are the ridges. The unique mark design (pattern of ridges and valleys) is used for authorization. These unique mark design traits are known as "minutiae". On average, a normal live scan produces 40 "minutiae".

II. EXISTING SYSTEM

In modern ATMs, the customer is identified by inserting a plastic card with magnetic strip. The information stored in the magnetic strip is compared with the database and verified by entering a pass code known as PIN (personal identification number) of four digits. A personal identification number is sent to its user in a letter. The darkened paper flap prevents the number from being read by holding the unopened envelope to the light. This PIN number may vary from four to twelve digits. Most commonly four digit PIN number is used. IBM 3624 method, IBM3624+ offset method and VISA method is used for PIN number validation.

III. PROPOSED SYSTEM

The Proposed system will be developed by using fingerprint and GSM technology for authentication of the system. Biometrics is used to identify a person or else to verify the identity of the person based on the behavioral or physiological characteristic. Because of this they are used to authorize persons in many of the online transactions. Fingerprint is the biometric chosen for implementation, as fingerprint is highly reliable and easily available compared to other biometrics. Finger prints of the users are stored first and then verified while using. If fingerprint is matched to the prepared prints then access was accepted and normal procedure takes place. If the fingerprint does not matched to the prepared prints GSM call was generated automatically and then send to registered mobile number. If the cardholder presses *0 then the person in ATM proceeds the normal process to take the amount if the card holder press *1 the transaction will denied. The authorized person can able to deny the transaction.

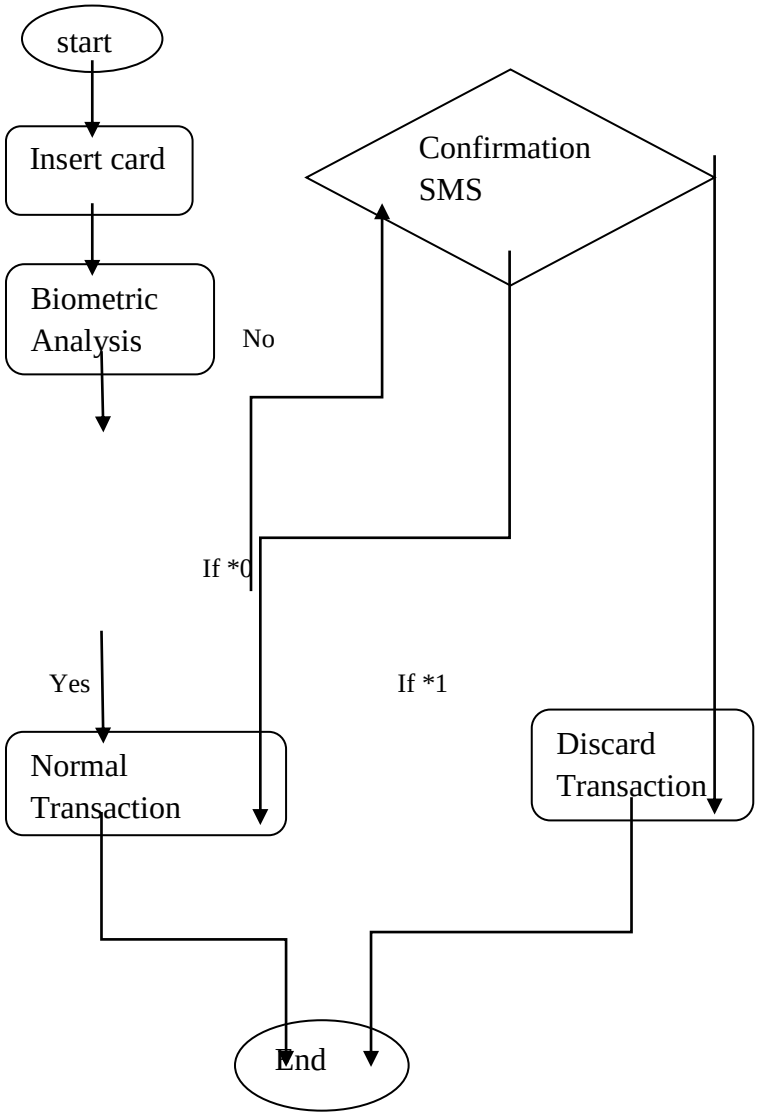

Fig 1. The overall flow chart of software

3.1 HARDWARE DESIGN

The main objective of this project is to provide the security to your bank account. To do this we are using Fingerprint module, GSM module and keypad.

The hardware components are:

- Microcontroller circuit
- Driver circuit
- Gear motor
- Fingerprint
- Power supply design

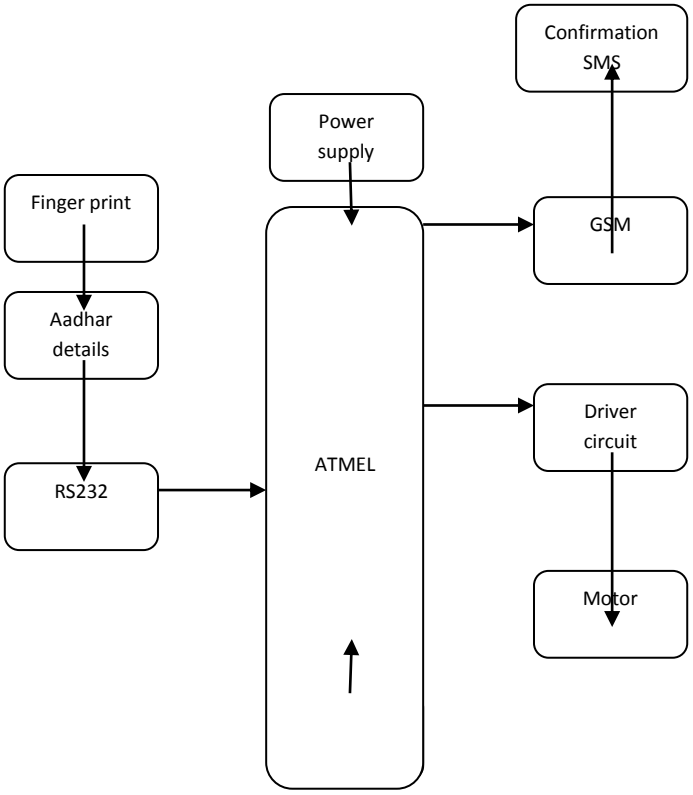

Fig 2. Block diagram of the proposed system

First of all the cardholder must register his/her fingerprint using fingerprint module.

At the time of withdrawing the amount the cardholder has to keep his fingerprint, if the fingerprint matches the normal process takes places to withdrawal the amount. If the fingerprint does not matches a conformation SMS will we send to the registered mobile number of the cardholder. If the cardholder press *0 the person who is in the ATM can take the amount through normal process, if the cardholder press *1 the transaction will be denied.

3.1.1MICROCONTOLLER CIRCUIT→ATMEL (AT89S52)

The AT89S52 is a low- power and high-performance CMOS 8-bit microcontroller with 8K bytes of in-system programmable flash memory. The device is manufactured using Atmel's high thickness non-unpredictable memory technology and is compatible with Industry-standard 80C51 instruction set and printout. On-chip flash allows the program memory to be reprogrammed in-system or by a traditional non-unpredictable memory programmer. This is highly effective and cost effective controller. This powerful microcontroller is suitable for many embedded control applications.

3.1.2 FINGERPRINT MODULE

The fingerprint sensor module with TTL UART interface for direct connections to microcontroller UART or to PC through MAX232/USB-Serial adaptor. The user can store the fingerprint data in the module and can configure it in 1: N or 1:1 mode for identifying the person. The fingerprint module can directly interface with 3v3 or %v Microcontroller. A level converter like MAX323 is required for interfacing with PC serial port.

Features:

- Coordinated image gathering and algorithm chip together, All-in-one.
- Fingerprint sensor can conduct secondary development, can be embedded into a variety of end products.

- Low cost, low power consumption, compact, magnificent execution.

3.1.3 GSM

GSM SIM800

Raspberry PI SIM800 GSM/GPRS Add-on V2.0 is modified for Raspberry Pi fuse based on SIM800 quad-band GSM/GPRS/BT module. AT commands can be sent via the serial port on Raspberry Pi, thus functions such as sending and receiving messages and dialing and answering calls, and surfing on line can be realized. Moreover, the module supports powering-on and resetting via software.

IV. WORKING PRINCIPLES

Fingerprints and the mobile numbers are collected from the customer while opening the account in the bank. If fingerprint is matched to the trained prints then access was accepted and normal procedure takes place. If the fingerprint does not matched to the trained prints then an SMS was generated automatically and then send to registered mobile number. If the cardholder presses *0 then the person in ATM proceeds the normal process to take the amount if the card holder press *1 the transaction will denied. The authorized person can able to deny the transaction.

V. CONCLUSION

Our system has high security implementations such as BIOMETRICS (fingerprint), Secret PIN number and Confirmation SMS which allows the cardholder to accept/deny the transaction. But in all existing system it only allows the cardholder to accept the transaction. Thus our system is highly secured when compared to other systems.

REFERENCES

[1] Ambavarapu Bhavana, M.Jasmine ”Fingerprint based authentication system using ARM7”, International Journal of Science and Research, Impact factor(2015):6.391.

[2] Joshpinmary.S,Manikandan.M, Sangavi.S, Aarthi.R “Implementation of real time embedded security system for ATM using enhanced Finger Vein Recognition”, International Journal of Advanced Research in Management, Architecture, Technology and Engineering”, Vol. 2, Issue 3, March 2016.

[3] Mr. Mahesh A. Patil, Mr.Sachin P.Wanere, Mr.Rupesh P.Maighane, Mr.Aashay R.Tiwari,” ATM Transaction Using Biometric Fingerprint Technology”, International Journal of Electronics, Communication & Soft Computing Science and Engineering ISSN:2277-9477, Volume2,Issue 6 22.

[4] Sri Shimal Das, Smt. Jhunu Debbarma, “Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian E-Banking System”, International Journal of Information and Communication Technology Research, Volume 1 No. 5, September 2011.

[5] Pramila D. Kamble, Dr.Bharti W. Gawali, “Fingerprint Verification of ATM Security System by Using Biometric and Hybridization”, International Journal of Scientific and Research Publications, Volume 2, Issue 11, November2012 ISSN 2250-3153.

[6] Namit Gupta, Anu Sharma, “REVIEW OF BIOMETRIC TECHNOLOGIES USED FOR ATM SECURITY”, International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 2, August 2013.

[7] V.Ramya1, B. Palaniappan, V.Sumathi, “Gsm Based Embedded System For Remote Laboratory Safety Monitoring And Alerting”, International Journal of Distributed and Parallel Systems (IJDPS).

[8] D. Vinod kumar, Prof.M R K Murthy, “Fingerprint Based ATM Security by using ARM7”, IOSR Journal of Electronics and Communication Engineering (IOSRJECE) ISSN : 2278-2834.

[9] Mary Lourde R and Dushyant Khosla, ”Fingerprint Identification in Biometric Security Systems” ,International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010.

[10] Pennam Krishnamurthy, Mr. M. Maddhusudhan Redddy, ”Implementation of ATM Security by Using Fingerprint recognition and GSM”, International Journal of Electronics Communication and Computer Engineering Volume 3, Issue (1) NCRTCST, ISSN 2249 –071X,(2012).

[11] Ravi. J, K. B. Raja, Venugopal. K. R, ”Fingerprint Recognition Using Minutia Score Matching”, International Journal of Engineering Science and Technology Vol.1(2), 2009,35-42.(2012).

[12] Xifeng Tong, Songbo Liu, Jianhua Huang, and Xianglong Tang, “Local Relative Location Error Descriptior-Based Fingerprint Minutiae Matching”, the Journal of the Pattern Recognition Letters, vol. 29, pp. 286-294, (2008).