

# DAB AND GSM BASED SECURED AUTHENTICATION IN ATM

Hepzibah Shanny Mol. D<sup>#1</sup> and Esther Benita. S<sup>\*2</sup>

<sup>#</sup> 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. Among all the biometrics, fingerprint based identification is one of the most proven and mature technique. At the time of transaction fingerprint image is acquired at ATM terminals using high resolution fingerprint scanner. These acquired fingerprint image is compared with the cardholder's fingerprint. Matching and Mismatching triggers confirmation call to the cardholder's number which allows the cardholder to accept/deny the transaction. Our aim is to design and implement a high security ATM system based on BIOMETRICS (fingerprint), PASSWORD and GSM technology.

**Index Terms**— Fingerprint Recognition, GSM SIM800, AT89S52.

## I. INTRODUCTION

Biometrics is method that recognize a person uniquely based on physiological or behavioral characteristic. Biometric-based solutions are able to provide for confidential financial transactions. The different biometric features used are fingerprints, face, palm print, handwriting, iris, retina, voice and vein. Fingerprinting or finger-scanning technologies are the most established technique of the biometric sciences and utilize unique features of the fingerprint to identify or verify the individuals 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 those we choose fingerprint because in other biometric cases there are slight recognition problems. For example iris scanner has complication while scanning eyes with lens. All fingerprints have unique characteristics and patterns. A normal fingerprint unique mark design is made up of lines and spaces. The ridges are the lines and the valleys are the spaces between the ridges. It is through the pattern of these ridges and valleys that a unique mark design is matched for verification and authorization. These unique mark design traits are termed "minutiae" and comparisons are made based on these traits. 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 deals with automated method of identifying a person or verifying the person identity based on the behavioral or physiological characteristic, and thus they are used for authentication 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 or mismatched to the prepared prints then GSM call was generated automatically and then send to registered mobile number. If the cardholder presses 1 then the person in ATM proceeds the normal process to take the amount if the card holder press 0 the transaction will denied. The authorized person can able to deny the transaction.

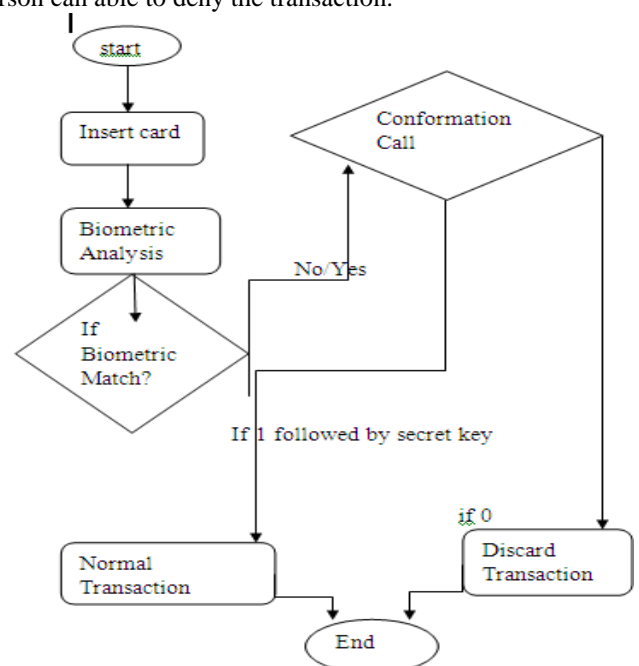


Fig 1. The overall flow chart of software

**A. 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

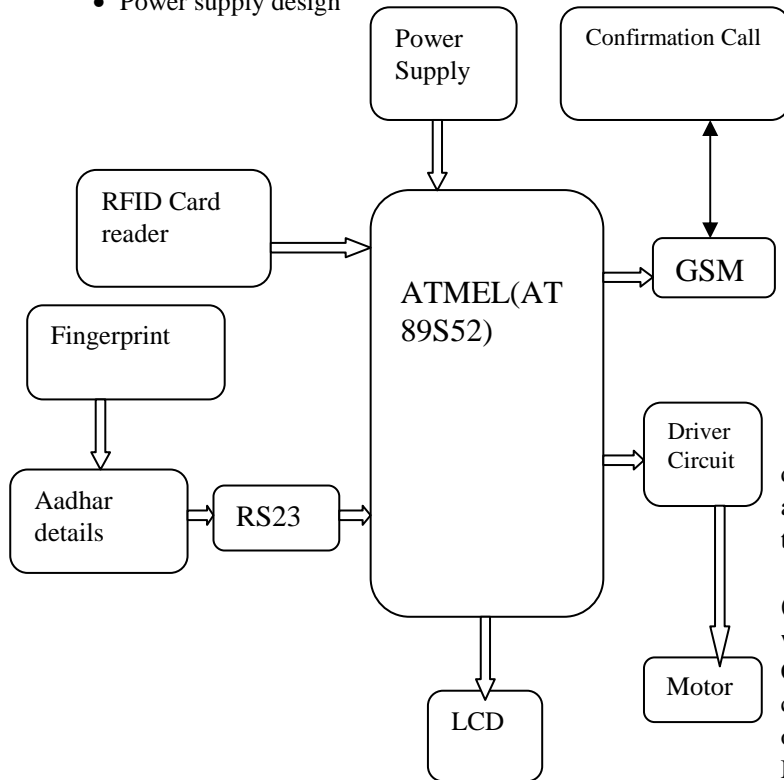


Fig 2. Block diagram of the proposed system

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 place to withdrawal the amount. If the fingerprint does not matches a conformation call will we send to the registered mobile number of the cardholder. If the cardholder press 1 the person who is in the ATM can take the amount through normal process, if the cardholder press 0 the transaction will denied.

**1) MICROCONTROLLER CIRCUIT → ATMELE (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.

**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.

**a) 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.
- Professional optical innovation, exact module manufacturing techniques.
- Good image processing capacities, can successfully capture image up to resolution 500 dpi.

**3) GSM**

GSM(Global System for Mobile communication) is a digital cellular technology used for transmitting data services and mobile voice. GSM is a digital mobile telephony system that is broadly used in Europe and different parts of the world.

GSM uses a variety of Time Division Multiple Access (TDMA) and is the most broadly used of the three digital wireless telephone advancements (TDMA,GSM and CDMA).GSM packs data and digitizes then sends it down a channel with two other streams of user data and each in its own time slot and it operates at either the 900MHz or 1800 MHz frequency band.

**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 orders 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 the web can be figured it out. Also, the module underpins driving on and resetting by means of programming.

**4) RFID CARD READER**

In most general applications aloof labels are generally the most practical. These are made in a wide variety of sizes and materials: there are durable plastic tags for discouraging retail robbery, skinny labels for use inside "keen" paper names, modest following labels which are inserted beneath an animal’s skin and credit card sized tags for access control.

**Technical Specifications:**

Distance:	Up to 6m (with mounted antenna)
Frequency:	125 KHz / 13.56 MHz / 915 MHz / 2.45 GHz Read/Write
Dimensions	Varies, as small as 0.8mm diameter

Weight: 6-54g  
Memory: Up to 16 Kbits  
Data durability: 10 Years

#### IV. PROGRAMMING LANGUAGE

##### A. EMBEDDED C LANGUAGE:

ATMEL microcontroller provides a development environment. The newer Atmel studio and the AVR studio. A typical Atmel sketch consists of two functions that are compiled and linked with a code stub main() into an executable cyclic executive code:

- Setup (): a function that runs once at the start of a code and that can initialize settings.
- Loop (): a function called repeatedly until the board powers off.

#### V. WORKING PRINCIPLES

Fingerprint verification of ATM security system using biometric along with GSM technology. The fingerprint trait is chosen, because of its availability, reliability and high accuracy. The fingerprint biometric can be easily implemented in ATM machine to provide security. Fingerprints and the mobile numbers are collected from the customer while opening the account in the bank. If fingerprint is matched or not matched GSM call was generated automatically and then send to registered mobile number. If the cardholder presses 1 then the person in ATM proceeds the normal process to take the amount if the card holder press 0 the transaction will denied. The authorized person can able to deny the transaction.

#### VI. CONCLUSION

Our system has high security implementations such as BIOMETRICS (fingerprint), Secret PIN number and Confirmation call 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 Reddy, "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 Descriptor-Based Fingerprint Minutiae Matching", the Journal of the Pattern Recognition Letters, vol. 29, pp. 286-294, (2008).