Multi Account Embedded ATM with fingerprint Sensor

Prof. Sangamesh Gama[1],Reshma P N, Shalini M S[2], Rajeshwari M[3]

Assistant Professor, Department of Information Science & Engineering, Atria Institute of Technology, Bangalore, India.[1]
Student, Department of Information Science & Engineering, Atria Institute of Technology, Bangalore, India.[2,3]

---***---

Abstract - Automated TellerMachine (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. To provide high security we introduced fingerprint based customer authentication. The main objective of this project is to develop a single smart card ATM (Automated Teller Machine) for multiple bank accounts. It reduces the cost of inter banking transactions as interfacing different bank databases is a resource consuming thing.In this security system the non-authorized persons can enter by using this smart card (RFID) and GSM Module based OTP (One Time Password) and keypads. User module is the interactive module through which the user can log into the system and perform the transactions of the user's choice. Though the proposed system provides the user a level higher convenience, efficient and user friendly.

Key Words: **IOT,Automated Teller Machine(ATM),RFID**

1.INTRODUCTION

An Automated Teller Machine (ATM) allows customers to perform banking transactions anywhere and at any time without the need of human teller. By using a debit or ATM card at an ATM, individuals can withdraw cash from current or savings accounts, make a deposit or transfer money from one account to another or perform other functions. You can also get cash advances using a credit card at an ATM. Individuals should be aware that many banks charge transaction fees – generally ranging from Rs.50- 150 per transaction for using another bank's ATM.

The ATM is online with the bank, that is, each transaction will be authorized by the bank on- demand and directly debited from the account's owner. The ATM works as follows. First, the client will insert his/her client card in the ATM and then the ATM will ask for a Personal Identification Number (PIN) , if the number is entered incorrectly several times in a row, most ATMs will retain the card as a security precaution to prevent an unauthorized user from working out the PIN by pure guesswork. Once the correct PIN is given, the

ATM will ask for the amount of money to be withdrawn. If the amount is available and if the client has enough money on his credit then the said amount of money will be paid. Whether the amount of money is payable or not, i.e. the ATM has enough cash but could be the case the ATM has no change for that amount, will be also checked. Once the money is offered to the client a countdown is started, i.e. the client has a determined amount of time to pick up the money. If this time-out is over, the money will be collected by the ATM and the transaction will be rolled back.

The class Card input has the methods for reading the code of the client's card and for ejecting the card from the ATM. The class Card_ input will interact through the Controller with the class Terminal, where the methods Req. PIN and Req. amount are defined, in order to get the PIN of the user and to verify if the given PIN is correct or not. The class Card will have the information of the cardholder, that is, the Card number, PIN, and Account number. The Controller will interact with Bank using the information of the cardholder in order to get the authorization to pay (or not) the requested amount. The bank interface will send the request to the Accounting class, which belongs to the Bank package, in order to call the Debit method of the accounting class[3]. The Accounting class has the methods Rollback, Authorization and Debit which directly interact with the Accounts class. Rollback is for roll back a transaction (for the case anything is wrong) and should leave the account and the teller machine in the original state; Authorization will authorize or not an operation and Debit will extract the requested amount of mo ney from the account in the case the operation is authorized.

ATMs are generally reliable, but if they do go wrong customers will be left without cash until the following morning or whenever they can get to the bank during opening hours. Of course not all errors are to the detriment of customers; there have been cases of machines giving out money without debiting the account or giving out a higher denomination of note by mistake.

There are also many "phantom withdrawals" from ATMs, which banks often claim are the result of fraud by customers. Phantom withdrawals are considered to be a problem generated by dishonest insiders by most other observers

2. LITERATURE SURVEY

This Paper gives an overview of basics of smart card and its application and how it is used in various sectors. It also deals with security algorithm during encryption and decryption of data's. This Paper tells us that why smartcard is preferred for banking system than other type cards.

A Smart card is type of chip card embedded with computer chip that stores and transacts data between users. It was introduced in Europe nearly three decades ago to pay phone bills. Smart cards greatly convenience and security of any transaction. The card is made from PVC, Polyester or Polycarbonate. The card layer are printed first and then laminated in a large press. The next step in construction is the blanking or die cutting. The card consists of several layers to prevent from card damage. Secure Internet Banking Application

This paper tells about how authentication can be kept safe during malicious software attacks. Here short-time passwords and one on certificate are used to protect the authentication. There two types of common attack during internet banking authentication are,1.Offline credential stealing attacks2.Online channel-breaking attacks

Here short lived passwords are generated using offline card reader and smart card to manage the authentication. Hence the transaction can be done without any malicious attacks.

Tools used for Implementation are SSL/TLS server certificate and, Private Key.

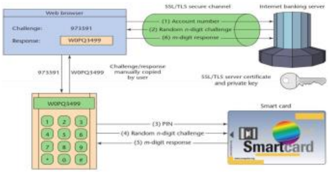
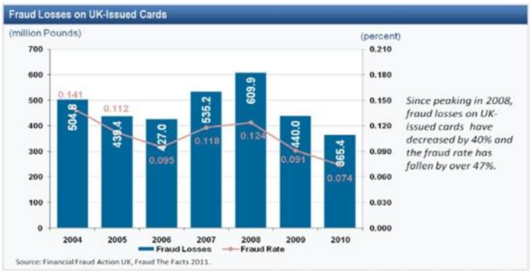


Figure 2.1: Secure internet banking

Chip-and-PIN: Success and challenges in reducing Fraud from Federal Reserve Bank of Atlanta Traditional Payment cards have evolved in much of the world and now rely on the EMV (Euro pay, MasterCard and Visa) global standard using chip technology. Transaction conducted with EMV chip –embedded cards (smart cards) that uses PIN verification are more secure than transaction conducted using magnetic strip technology.

Chart 1: Fraud Losses on UK-Issued Cards



Source: Financial Fraud Action UK, Fraud The Facts 2011.

Figure 2.2: Chart on Fraud Losses on UK-Issued Cards

EMV cards are used globally in which united stated stand apart in experience, chip-and-PIN cards have successfully reduced fraud on face-to-face transactions. However, these cards have less impact on overall fraud levels as fraudsters have shifted their focus to non-chip transactions. Tools Used for Implementation are Session keys-Generated every time when a secure channel is initialized, C-MAC-For securing Messaging and, ALGSCP-Algorithm for identifying the secure channel protocol

3.METHODOLOGY

3.1OVERVIEW OF ARM MICROCONTROLLER

General Description:

The LPC2141/42/44/46/48 microcontrollers are based on a 16-bit/32-bit ARM7TDMI-S CPU with real-time emulation and embedded trace support, that combine microcontroller with embedded high speed flash memory ranging from 32 kB to 512 kB. A 128-bit wide memory interface and a unique accelerator architecture enable 32-bit code execution at the maximum clock rate. For critical code size applications, the alternative 16-bit Thumb mode reduces code by more than 30 % with minimal performance penalty.

Due to their tiny size and low power consumption, LPC2141/42/44/46/48 are ideal for applications where miniaturization is a key requirement, such as access control and point-of-sale. Serial communications interfaces ranging from a USB 2.0 Full-speed device, multiple UARTs, SPI, SSP to I2C-bus and on-chip SRAM of 8 kB up to 40 kB, make these devices very well suited for communication gateways and protocol converters, soft modems, voice recognition and low end imaging, providing both large buffer size and high processing power. Various 32-bit timers, single or dual 10-bit. ADC(s), 10-bit DAC, PWM channels and 45 fast GPIO lines with up to nine edge or level sensitive external interrupt pins make these microcontrollers suitable for industrial control and medical systems.

Features:

B. Features

16-bit/32-bit ARM7TDMI-S microcontroller in a
tiny LQFP64 package. 8 kB to 40 kB of on-chip static RAM and 32 kB to 512 kB of on-chip flash memory. 128-bit wide interface/accelerator enables high-speed 60 MHz operation. In-System Programming/In-Application Programming (ISP/IAP) via on-chip boot loader software. Single flash sector or full chip erase in 400 ms and programming of 256 bytes in 1 ms. Embedded ICE RT and Embedded Trace interfaces offer real-time debugging with the on-chip Real Monitor software and high-speed tracing of instruction execution. USB 2.0 Full-speed compliant device controller with 2 kB of endpoint RAM. In addition, the LPC2146/48 provides 8 kB of on-chip RAM accessible to USB
by DMA. One or two (LPC2141/42 vs. LPC2144/46/48) 10-bit ADCs provide a total of 6/14 analog inputs, with conversion times as low as 2.44 μs per channel. Single 10-bit DAC provides variable analog output (LPC2142/44/46/48 only). Two 32-bit timers/external event counters (with four captures and four compares channels each), PWM unit (six outputs) and watchdog. Low power Real-Time Clock (RTC) with independent power and 32 kHz clock input. Multiple serial interfaces including two UARTs (16C550), two Fast I2C-bus (400 Kbit/s), SPI and SSP with buffering and variable data length capabilities. Vectored Interrupt Controller (VIC) with configurable priorities and vector addresses. Up to 45 of 5 V tolerant fast general purpose I/O pins in a tiny LQFP64 package. Up to 21 external interrupt pins available.
60 MHz maximum CPU clock available from programmable on-chip PLL with Settling time of
100 μs.
On-chip integrated oscillator operates with an external crystal from 1 MHz to 25 MHz Power saving modes include Idle and Power-down. Individual enable/disable of peripheral functions as well as peripheral clock scaling for additional power optimization.
Processor wake-up from Power-down mode via
external interrupt or BOD. Single power supply chip with POR and BOD
circuits:
CPU operating voltage range of 3.0 V to 3.6 V (3.3

V ± 10 %) with 5 V tolerant I/O pads.Embedded ICE RT and Embedded Trace interfaces offer real-time debugging with the on-chip Real Monitor software and high-speed tracing of instruction

*3.2 **RFID Concept***

The RFID technology is a means of gathering data about a certain item without the need of touching or seeing the data carrier, through the use of inductive coupling or electromagnetic waves. One important feature enabling RFID for tracking objects is its capability to provide unique identification. One possible approach to item identification is the EPC (Electronic Product Code), providing a standardized number in the EPC global Network, with an Object Name Service (ONS) providing the adequate Internet addresses to access or update instance-specific data.

3.3GSM (GLOBAL SYSTEM FOR MOBILE COMMUNICATION)

DEFINITION:

Global System for Mobile (GSM) is a second generation cellular standard developed to cater voice services and data delivery using digital modulation.

TECHNICAL DETAILS:

Global System for Mobile communications is the most popular standard for mobile phones in the world. Its promoter, the GSM Association, estimate that 82% of the global mobile market uses the standard. GSM is used by over 2 billion people across more than 212 countries and territories. Its ubiquity makes international roaming very common between mobile phone operators, enabling subscribers to use their phones in many parts of the world.

3.3 SUBSCRIBER IDENTITY MODULE (SIM)

One of the key features of GSM is the Subscriber Identity Module (SIM), commonly known as a SIM card.

The SIM is a detachable smart card containing the user's subscription information and phonebook. This allows the user to retain his or her information after switching handsets. Alternatively, the user can also change operators while retaining the handset simply by changing the SIM. Some operators will block this by allowing the phone to use only a single SIM, or only a SIM issued by them; this practice is known as SIM locking, and is illegal in some countries.

3.4 Liquid Crystal Display:

In recent years the LCD is finding widespread use replacing LEDs this is due to following reasons:

1) The declining prices of LCDs.
2) The ability to display numbers, characters and graphics. This is in contrast to LEDs, which are limited to numbers and few characters.
3) Incorporation of a refreshing controller in to LCD, there by relieving the CPU of the task of refreshing the LCD. In contrast LCD must be refreshed by CPU to keep displaying the data.

Figure 3.4: LCD display

3.5 FINGERPRINT READER:

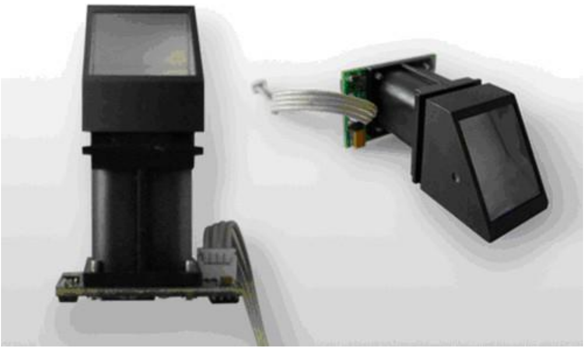


Figure 3.5: Fingerprint Reader

Specification of Finger Print reader:

- DC power: 3.6V-6V.
- Current working rate: 100mA-150mA.
- Time taken to acquire: <0.5sec.
- Average searching time: <0.8sec.
- Working environment Temp -10°C-+40°C.
- Matching mode: 1:1 and 1:n matching.

Operation Principle OF Fingerprint Reader:

1. Fingerprint processing includes two parts: fingerprint enrollment
2. fingerprint matching (the matching can be 1:1 or 1:N).

When enrolling, user needs to enter the finger two times. The system will process the two time finger images, generate a template of the finger based on processing results and store the template. When matching, user enters the finger through optical sensor and system will generate a template of the finger and compare it with templates of the finger library. For 1:1 matching, system will compare the live finger with specific template designated in the Module; for 1:N matching, or searching, system will search the whole finger library for the matching finger. In both circumstances, system will return the matching result, success or failure.

Fingerprint-processing Instructions:

- **To collect finger image GenImg**

  Detecting finger and store the detected finger image in Img_Buffer while returning successful confirmation code. If there is no finger, returned confirmation code would be "can't detect finger".

- **Upload image UpImage**

  To upload the image in Img_Buffer to upper computer.

- **Download the image DownImage**

To download image from upper computer to Img_Buffer.

- **To generate character file from image Img2Tz**

To generate character file from the original finger image in Img_Buffer and store the file in CharBuffer1 or CharBuffer2.

- **To generate Template**

To combine information of character files from CharBuffer1 and CharBuffer2 and generate a template which is store back in both CharBuffer1 and CharBuffer2.

- **To store template**

To store the template of specified buffer (Buffer1/Buffer2) at the designated location of Flash library.

- **To read template from Flash library**

To load template at the specified location of Flash library to template buffer CharBuffer1/CharBuffer2

- **To delete template**

To delete a segment (N) of templates of Flash library started from the specified location.

- **To empty finger library**

To delete all the templates in the Flash library.

- **To search finger library**

To search the whole finger library for the template that matches the one in CharBuffer1 or CharBuffer2. When found, PageID will be returned.

3.7 Flowchart

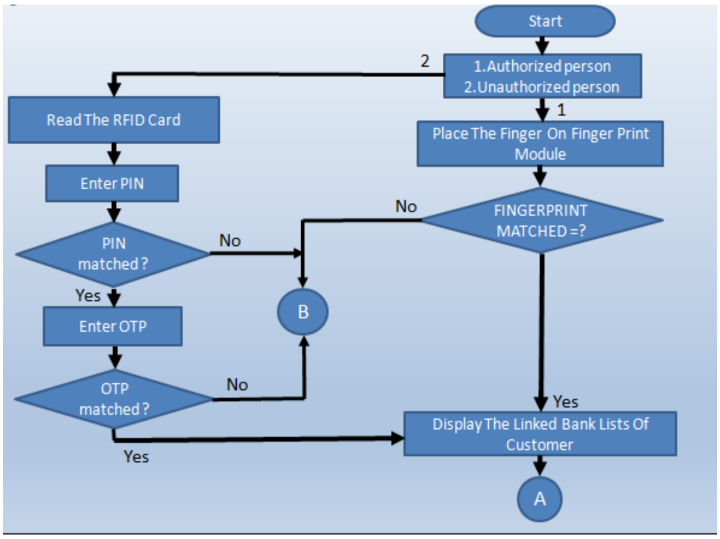


Figure 3.6.2: Flowchart of Multiaccount ATM system

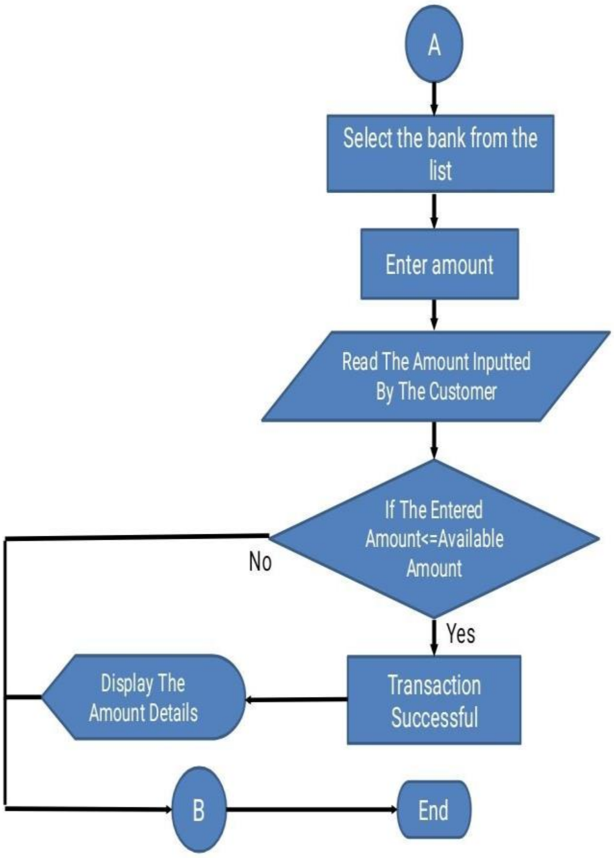

A
Select the bank from the list
Enter amount
Read The Amount Inputted By The Customer
If The Entered Amount<=Available Amount
No
Yes
Display The Amount Details
Transaction Successful
B
End

Figure 3.6.3 : Block diagram of Multi account ATM system

- Wireless scanning of atm cards.
- Authentication using password and fingerprint.
- Sending password request sms to user when fingerprint recognition failed.

- Waiting for reply from user.
- If no reply comes transaction is blocked.
- If there is a password reply fingerprint scanner turns on and gives input to microcontroller.
- If fingerprint matches go for bank selection.
- If it mismatches otp request will be sent to the user.
- Asks for otp entry.
- Comparison of entered and sent otp.
- If both are matching go for transaction.
- Send a confirmation message to user.
- Comparison of entered and sent otp.
- If both are matching go for transaction.
- Send a confirmation message to user.

4 IMPLEMENTATION

3.6 Architectural Diagram

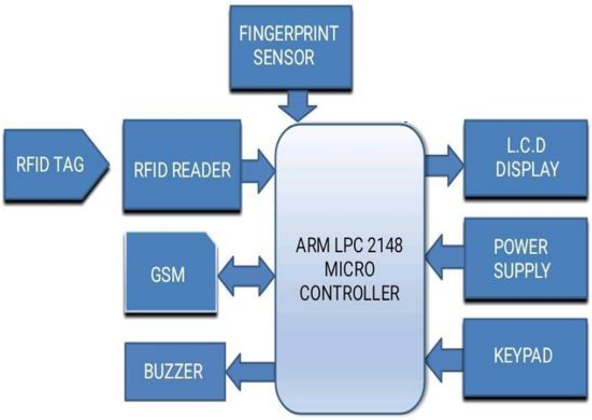


Figure 3.6.1: Block diagram of Multi account ATM system

5 APPLICATION, ADVANTAGES & DISADVANTAGES

APPLICATION OF PROJECT:

- Security purpose
- Voter verification at polling booth
- At airport
- Defense

ADVANTAGES OF PROJECT:

- Provides very food security to ATM users.
- Use of RFID allows only authorized users to use ATM facility.
- Alerts card holders during theft through GSM modem.
- Low cost and secure transaction is possible.
- There is not possible to duplicate the RFID card.
- Advantages of smart card over magnetic cards

FEATURE	SMART CARD	MAGNETIC CARD
Reduction in fraud		x
Accuracy		x
Positive identification		x x
Security		

Table 5: Advantage of smart card over magnetic card

DISADVANTAGES OF PROJECT:

- If network fails, then it is not possible to transact.
- It requires more time during transaction.

6 CONCLUSION

The system we are using for handling multiple accounts here is more efficient than existing system. This Reduces transaction cost of handling multiple accounts of a single user. This make banking system more efficient than the existing system. Using this the users can perform transactions for all his bank Accounts using single smart ATM card with Enhanced security system such as OTP (one time password) and face recognition. Thus the user can manage his multiple accounts in various banks with the help of this single smart card which provides access and reduces the complex of managing more than one ATM card and passwords. This also leads to reduce cost of transaction charges that were on the customers for making transaction and decrease in their production of smart cards for each every account the user has. By implementing this ATM fraud i.e. skimming etc., can be avoided.

7 FUTURE SCOPE:

This project can be implemented for office security also.

- Also to colleges, hospitals and also in parking system.
- Future research will help to do away with PINs completely and dwarf ATM card authorization by introducing palm and finger vein authentication which is fast, accurate and difficult to fake.

Since more than one bank accounts being added, the existing PIN security are not sufficient enough, so we can use a biometric scan in the smart card i.e. multi component card So that the user holds the card such that the face recognition on the biometric scan reader while he swipes the registered card and the image is authenticated at the real time. No one other than the user and their family can use the card. Only if the face matches the user can enter his PIN number otherwise the transaction will not be allowed until the user is authenticated

8 REFERENCE

[1] “Smart Card & Security Basics” - CardLogix, paper no.:710030 www.cardlogix.com

[2] “Smart card based Identity Card And Survey”-White Paper JKCSH (Jan Kremer Consulting Services).

[3] Chip-and-PIN: Success and challenges in reducing Fraud from Federal Reserve Bank of Atlanta”-Douglas King, Jan 2012.

[4] “Examining Smart-Card Security under the Threat of Power Analysis Attacks”- Thomas S.Messaerges member IEEE, Ezzat A.Dabbish member IEEE, and Robert H.Sloan senior member IEEE vol.51, No. 5, MAY 2002.

[5] “Secure Internet Banking Application”-Alain Hiltgen, Thorsten Kramp.

[6] Fingerprint Verification Using Smart Cards for Access Contol Systems, Raul Sanchez-Reillo, IEEE AESS Systems Magazine , September 2002 [7] “Benefits Of Smart cards versus Magnetic Stripe Cards for Healthcare Application”-Smart card Alliance 2011.

[7] Katakam Swathi, Prof.M.Sudhakar “Multi Account Embedded ATM Card with Enhanced Security” IOSR Journal of Electronics and Communication Engineering IOSR Journal of Electronics and Communication Engineering, Volume 10, Issue 3, Ver. I (May - Jun.2015)

[8] Tahaseen Taj I S, Dr Suresh M B“AN EMBEDDED APPROACH: FOR HANDLING MULTIPLE ACCOUNTS WITH SMART ATM CARD” International Conference on Computer Science, Electronics & Electrical Engineering-2015

[9] Nair Vinu Uthaman, Pratiksha Shetty, Rashmi, Mr.Balapradeep K N “MAASC Multiple Account Access using Single ATM Card” International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 6, June 2014

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