International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 07 | July 2020 www.irjet.net p-ISSN: 2395-0072

Secured Money Transaction using Multi Account Embedded ATM Card

Sumukh R Pobbathi[1], Sujan Bharadwaj[2], Srikanth A[3], Smt.Sujaya.B.L[4]

[1,2,3]Department of Electronics and Communication, BNM Institute of Technology, Bangalore
[4]Assistant Professor, Dept. of Electronics and Communication Engineering, BNM Institute of Technology, Bangalore

---

Abstract - *The need of cash can only be satisfied after you are carrying money with you. That also increases the chance of getting robbed. This research focuses on the way to enhance security of transactions in ATM system employing a multi-factor authentication system (PIN and Facial Recognition). This research proposed a highly secured cash machine using an optimized Advanced Encryption Standard (AES) algorithm. This research proposes two levels of security. Firstly, we consider the protection level at the client side by providing biometric identification scheme together with a password of 4-digit long. Identification is achieved by considering the biometric identification of the client. Secondly, we ensure a secured communication link between the client machines to the bank server using an optimized energy efficient AES processor. The matched face ID is that the data for encryption process and 4-digit long password is that the symmetric key for the encryption process. The biometric and cryptography techniques are used together for private identity authentication to enhance the protection level.*

Key Words: **ATM, PIN, Advanced Encryption Standard, Biometric Identification, Cryptographic Techniques.**

1. INTRODUCTION

In latest ATMs, the customer identifies him or herself by inserting a plastic card with magnetic strip or plastic smart with a chip that contains his or her account number. The customer then verifies his or her identity by entering a pass code of 4 digits. If the amount is entered incorrect several times consecutively, most ATMs will retain the card as a security precaution to stop an unauthorized user from discovering the PIN by guess work. Moreover there's a limitation in transaction for the other bank customers in using the ATM of another bank crossing the limit they need to pay transaction fees.

At present every customer has a personal ATM card for each and every bank within which he or she maintains account. So handling the cards, their passwords play a significant role here. So to beat these difficulties we embedded all the accounts of the user in a single ATM smart card, so that the user can swipe the card and select the bank from which he or she have an interest to carry out transaction.

2. Motivation

In existing ATM system all ATM machines are connected to their respective bank servers and every bank servers is connected to one interface i.e. National Finance Switch. When user swipes his ATM card at respective bank's ATM machine, then that ATM machine directly links to its bank server for validation of ATM card. If the ATM card is belonging to the same bank then transaction proceeds else connects to the respective bank's server via NFS for further transaction. More over there's a limitation in transaction for the other bank customers in using the ATM of another bank crossing the limit they need to pay transaction fees. This project aims at designing system with enhanced security, multi account transactions using same card together with exemption of transaction charges.

3. Problem Statement

At present situation as each person has more than one bank account, user has to carry more than one ATM card and also remember password for each ATM card. The customer should also pay transaction charges when using card in ATM of different bank. There is also no OTP system in the present technology. The present ATM has no facial recognition and theft alarm.

4. Objectives

To build a system with enhancement in security aspect of present ATM system, each time the customer can change the password at beginning of transaction, thereby increasing the security. We use an RFID card stored with every account linked with the customer which reduces the complexity of carrying or managing more than one ATM card and their passwords. Once the customer swipes the card, he gets a display of all the banks linked to him, after the bank is selected a request is sent to the corresponding bank through network and links it with the bank server to access the database of the user so that the transaction is processed.

Each time the card is used anyone else other than the account holder, it has to be authorized by the account holder through SMS. This reduces fraud providing better security to customer. In our system the transaction charges are also waived off.

5. Proposed System

5.1 Block Diagram

The idea behind this universal ATM card is that the customers can use a single ATM card to operate different bank accounts. The LPC2148 microcontroller is the heart of the system. It is used to process the data between each component of the system. The GSM module is used for communication between customer and the bank. A facial recognition module is used for the authentication of user. LCD display and keypad is used as the human machine interface and a RFID reader for the card identification.

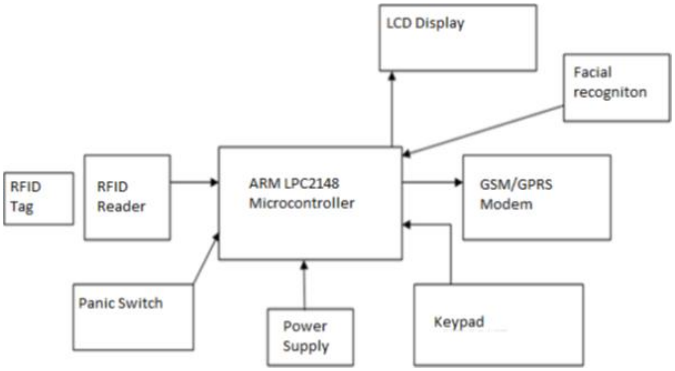
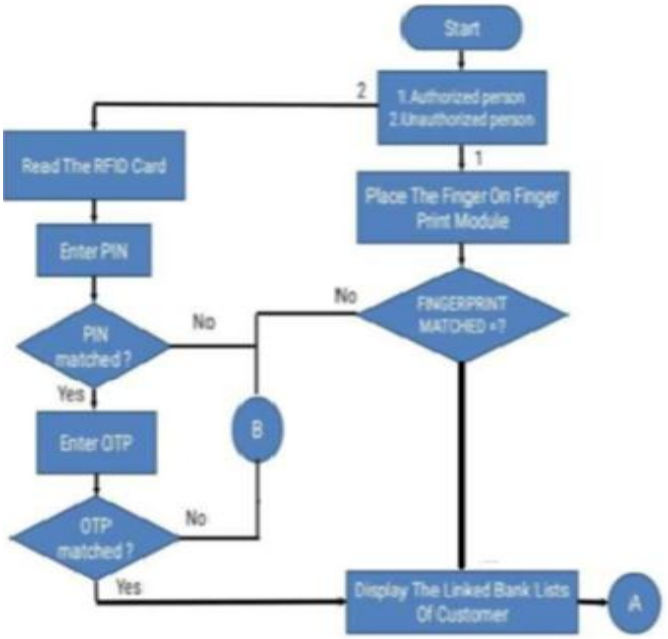


Fig-1: Block Diagram

5.2 UML Diagram

The proposed system has two different procedures, which procedure to be executed is decided by the facial recognition module. First case is when the card is being used by the owner itself. The other case is when card is being used by an unauthorised person. The flow diagram for both the cases is shown below.



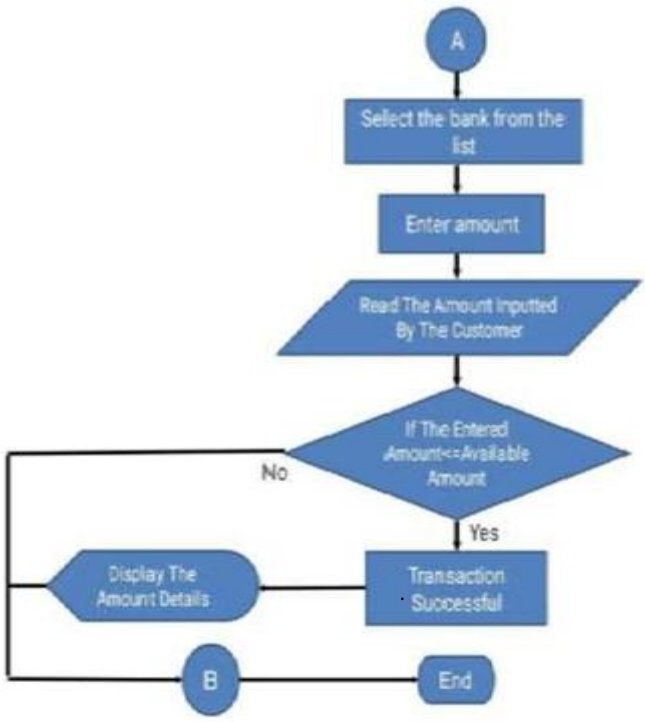


Fig-2: UML Diagram of System

6. Hardware Requirements

6.1 LPC2148

The LPC2148 is a 32bit ARM7 family based microcontroller with ISP and IAP feature using on-chip boot loader software. On-chip static RAM is 8 kB-40 kB, on-chip flash memory is 32 kB-512 kB, the wide interface is 128 bit. It takes 400 milliseconds time for erasing the data in full chip and 1 millisecond time for 256 bytes of programming. It has 2 kB of endpoint RAM and USB 2.0 full speed device controller. Furthermore, this microcontroller offers 8kB on-chip RAM nearby to USB with DMA. One or two 10-bit ADCs offer 6 or 14 analogs inputs with low conversion time as 2.44 µs/ channel. The modes for power-conserving mainly comprise idle & power down.

Fig-3: ARM LPC2148

6.2 RFID Reader RC522

This low cost MFRC522 based RFID Reader Module is simple to use and can be employed in a good range of applications. The MFRC522 is a highly integrated reader/writer IC for contactless communication at 13.56 MHz. It requires supply voltage of three and consumes current of 13-26mA. The read range is approximately 3cm with supplied card and fob. Its dimensions are 60mm × 39mm.

Fig-4: RFID Reader

6.3 GSM Module (SIM 800)

SIM800 is a complete Quad-band GSM/GPRS solution during a SMT type which may be embedded within the customer applications. SIM800 support Quad-band 900/1800MHz, it can transmit voice, SMS and data information with low power consumption. With tiny size of 24*24*3 mm, it can fit into slim and compact demands of customer design. It is interfaced such some way that it sends an SMS tuned in to the customer after the transaction is completed indicating the updated balance.

Fig-5: SIM800 GSM Module

6.4 Max232

MAX232 is an integrated circuit (embedded in a single chip) designed by Maxim Integrated Products and act as a Voltage Logic Converter i.e. it is used to convert TTL Logic level (Microcontrollers' COM Port) into TIA/EIA-232-F level (Laptop Serial Port RS-232) and the other way around. It is used for the communication between Microcontroller and PC or laptop. 9 Pin Serial Port on our Laptop works on RS232 Voltage Logic while our Microcontroller's Serial Port i.e. Tx, RX pins work on TTL Logic. Suppose you are working on PIC16F877A Microcontroller and you want to connect to Serial Pin of your Laptop, then you have to place MAX232 in between.

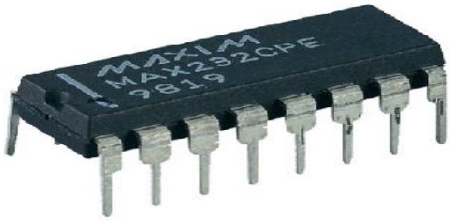


Fig-6: MAX232 IC

7. Expiremental Results

The demonstration of the system can be given as two cases. These cases are decided by the facial recognition module. If the face matches with the face data stored in card, system will ask for the fingerprint followed by pin and then the amount to withdraw. After the transaction is completed, a message will be sent to the registered number about the amount withdrawn and available balance in the account.

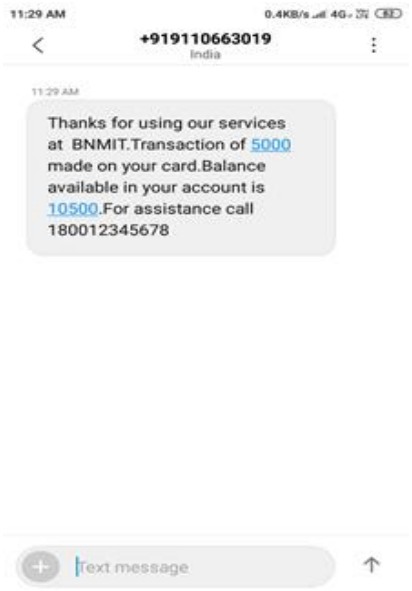


Fig-7: Message received on registered Mobile Number

The second case is for the unauthorised user that is when the face does not match with face data on the card. In this case the customer is alarmed with a message and the customer has to reply with YES if we wants the transaction to be continued. After this the user in ATM has to enter PIN after

this, customer has to send a OTP from his number and ask the user in ATM to enter the same. If they are matched, user can enter the amount to withdraw and complete the transaction.

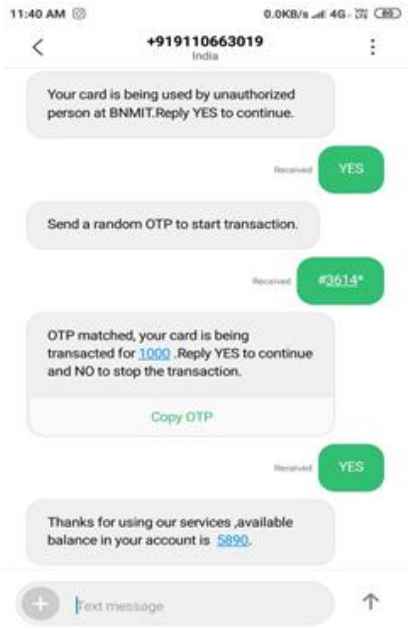


Fig-8: Messages received when card is used by unauthorized person

Any mismatch either in PIN or OTP will terminate the transaction with a alert message to the customer.

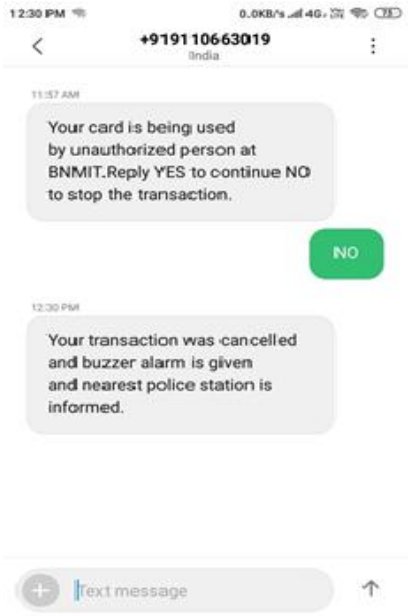


Fig-9: Customer terminating transaction when misused

8. CONCLUSION

Thus the user can manage his/her multiple accounts in various banks with the help of this single smart card which provides easy access. This feature reduces the complexity of managing more than one ATM card and their passwords. The transaction charges levied on the users/ customers for transactions done in ATMs other than their respective banks are waived off. Production cost of ATM cards can also be reduced.

REFERENCES

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

[2] "Smart card based Identity Card and Survey"-White Paper JKCSH (Jan Kremer Consulting Services)

[3] Fingerprint Verification Using Smart Cards for Access Control Systems, Raul Sanchez-Reilllo, IEEE AESS Systems Magazine, September 2002

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