IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 3, Ver. I (May - Jun.2015), PP 31-41
www.iosrjournals.org

Multi Account Embedded ATM Card with Enhanced Security

[(1)]Katakam Swathi, [(2)]Prof.M.Sudhakar
PG Student, Department of Electronics & Communication Engineering, C.M.R College of Engineering & Technology. Hyderabad, India.
Professor, Department of Electronics & Communication Engineering, C.M.R College of Engineering & Technology. Hyderabad, India.

Abstract: *Automated Teller Machine (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. On most modern ATMs, the ATM card used by the customer for each bank account which is a plastic ATM card with a magnetic stripe or a plastic smart card with a chip. However, password PIN which is the main authentication for ATM transactions represent the weakest link in the computer security chain. In the proposed Multi Account Embedded ATM card, we embed more than one bank account into a single ATM card so that the customer can carry out the financial transactions for multiple bank accounts. The user need not carry multiple ATM cards and remember multiple passwords. To provide high security we introduced fingerprint based customer authentication. It reduces the cost of interbanking transactions as interfacing different bank databases is a resource consuming thing.*

Keywords: *ATM, Banks, Fingerprint, Smart card, User authentication, NFS, PIN, Transaction.*

I. Introduction

ATM is an abbreviation of Automated Teller Machine. It was introduced in the year 1960s. ATM is an electronic telecommunication device that enables the customer of a financial institution to perform financial transactions without the need for a human cashier, clerk or bank teller. At first, the ATM was made to serve for the particular bank customers but later on the ATMs are connected to interbank network, to enable people to deposit, withdraw and transfer amount from the ATM machines not belonging to that particular bank i.e. a user can access any ATM machines to carry out transactions for any of his/her bank accounts [7].

ATMs relay on authorization of a financial transaction by the card issuer or other authorizing institution via the communication network. This is often performed through an ISO8583 messaging system. Many banks charge ATM usage fee from the customers for the transactions.

At present every customer has an individual ATM card for each and every bank in which he/she maintains account. Thus handling the cards and remembering their passwords is a difficult task for the customer.

In this paper to overcome these difficulties we embedded more than one bank account of the user in a single ATM smart card and the authentication of the customer is performed by biometric analysis and a single PIN. The customer inserts the card and can select the bank from which he/she interested to carry out the transaction after the authentication is successful [1].

Inter banking in India is provided by National Financial Switch (NFS). NFS is responsible for routing the transactions [2].

II. Existing System

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 for a human teller.

In modern ATMs, the customer identifies himself or herself by inserting a plastic card with a magnetic strip or a plastic smart card with an IC chip which contains Card Identification Number (CIN) and some information.

The main authentication for ATM transaction is the Personal Identification Number (PIN) of four digits that is used by the customer to access the ATM machine in order to make transactions. If the PIN entered by the user is incorrect then there is no further processing. Though the passwords are still the most prevalent method of authentication in security system, they represent the weakest link in the security chain. 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 the transaction fee [1].

III. Literature Survey

3.1 The ATM Machine

The idea of self service in retail banking developed through independent and simultaneous efforts in Japan, Sweden, the United Kingdom and the United States.

In the US patent record, Luther George Simjian has been credited with developing a "prior art device". Specifically his 132 patent (US3079603) was first field on 30 June 1960. City Bank of New York installed a machine called a Bankograph in 1961. This wasn't an ATM as we know it, though: rather than dispensing cash, it acted as an automated way to deposit cash and checks but removed after six months due to the lack of customer acceptance. In simultaneous independent efforts, Engineers in Japan, Sweden and Britain developed their own cash machines during the early 1960s. The first of these was put into use was by Barclays Bank in Enfield Town in North London, United Kingdom, on 27 June 1967. This machine was the first in the world and was used by English comedy actor Reg Varney, at that time so as to ensure maximum publicity for the machines that were to become main stream in the UK [7].

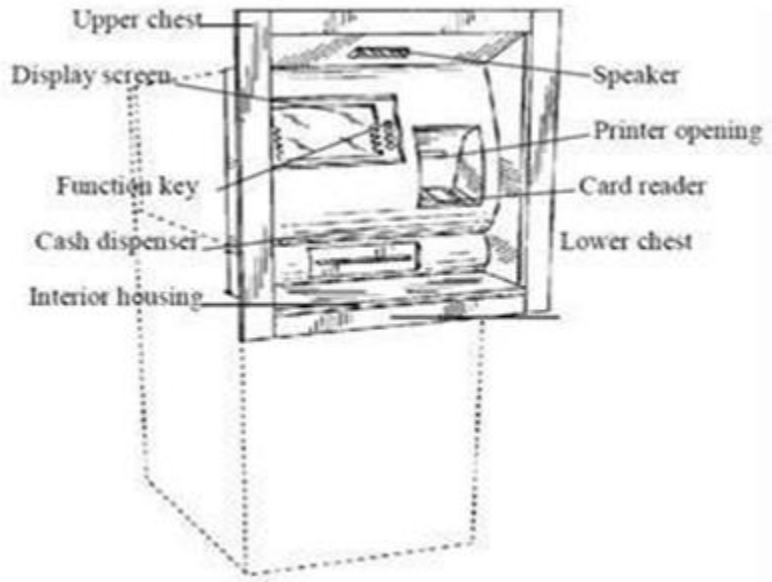


Figure 1: The ATM Machine showing different Parts

The machine comprises of enclosures that are made of metal steel. The chest portion often houses currency, deposits and the mechanisms that handle these items.

The chest portion also houses critical electric components that must be protected from tampering. It has an access door which is controlled by a suitable lock to prevent access to the interior by unauthorized personnel. The type of chest used varies with the type of ATM and the location where the machine is installed. Machines which operate in environment where they may be unattended for substantial period of time commonly have higher security chests and enclosures than machines which are installed in lobbies of buildings, stores or other places where guards or other people are usually present.

The enclosure also includes less security portion in addition to the chest portion; and they house items such as printers, screen displays, card readers and other items of less value or less susceptibility to tampering. Access to this less security area is controlled through locking mechanisms and only provides quick access to authorized persons for routine maintenance, such as changing paper rolls and printer ribbons [3].

3.2 Financial networks

Most ATMs are connected to interbank networks, enabling people to withdraw and deposit money for machines not belonging to the bank where they have their accounts or in the countries where their accounts are held (enabling cash withdrawals in local currency) [3].

ATMs relay on authorization of a financial transaction by the card issuer or other authorizing institution via the communication network. This is often performed through an ISO8583 messaging system [1].

Many banks charge ATM usage fee. In some cases, the fee charged solely to users who are not customers of the bank where the ATM installed; in other cases, they apply to all users.

ATMs are typically connected directly to their host or ATM controller via either ADSL or dial-up modem over a telephone line or directly via a leased line. Leased lines are preferable to plain old telephone services (POTS) lines because they require less time to establish a connection. Common lower-level layer

communication protocols used by ATMs to communicate back to bank include SNA over SDLC, TC500 over Asynchronous, X.25 and TCP/IP over Ethernet.

In addition to the methods employed for transaction security and secrecy, all communications traffic between the ATM and the transaction processor may also be encrypted via methods such as SSL [7].

3.3 Transaction network

Network transactions are routed through only one network switch. The switch can be either a regional network's or a national network's. Typically a network transaction is initiated by a cardholder of one member institution at an ATM of another member institution.

Reciprocal transactions occur when the cardholder uses an ATM of another institution and the card issuer and ATM owners use different regional networks but the networks have a reciprocal-sharing agreement.

National bridge transactions occur when the cardholder uses an ATM of another institution and the card issuer and ATM owners use different regional networks but the networks do not have a reciprocal sharing agreement.

Figure 2 shows the ATM transaction network. 6.

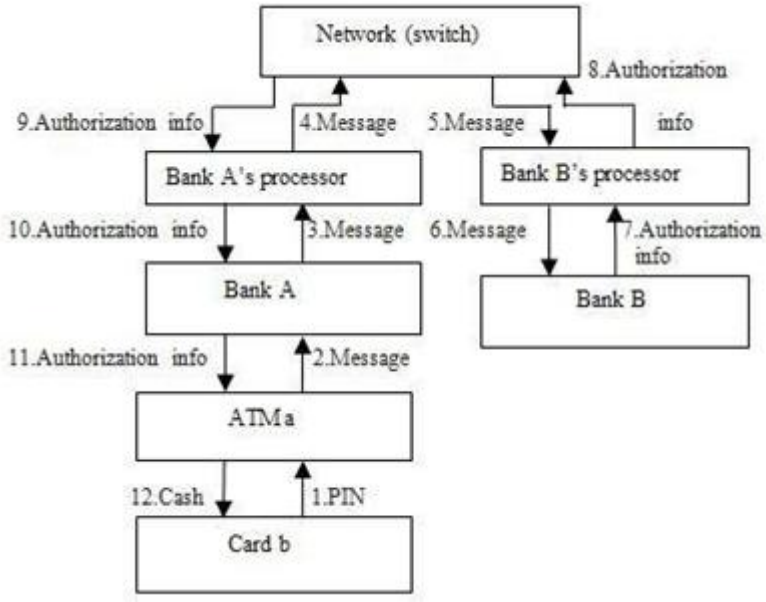


Figure 2: ATM Transaction network

1. A consumer uses AT card B, which is issued by Bank B, at ATM a, which is owned by Bank A and enters a PIN.
2. ATM a sends the transaction message to Bank A's host computer.
3. Bank A outsources transaction routing service from a third-party processor and routes the transaction to the network.
4. Bank A's processor sends the message to the ATM network that both Bank A and Bank B are members of the network.
5. The network forwards the message to Bank B's processor, which examines transaction authorization Bank B's processor then forwards the message to Bank B, the card issuer.
7. -11. Bank B authorizes the transaction and posts the debit to the cardholder's account. The decision is sent back to Bank B's processor, the network, Bank A's processor, Bank A and then the ATM a terminal. Consumer gets the cash [6].

3.4 ATM card

ATM card is a simple plastic card, just at the size of a credit card (54mm by 85.6mm by 0.76), with a microprocessor and memory embedded inside the card, which is seen as golden plates, contact pads, at one corner of the card. Figure 3 shows the card layout and dimensions. The plates are used to supply the necessary power and to communicate via direct electrical contact with the reader.

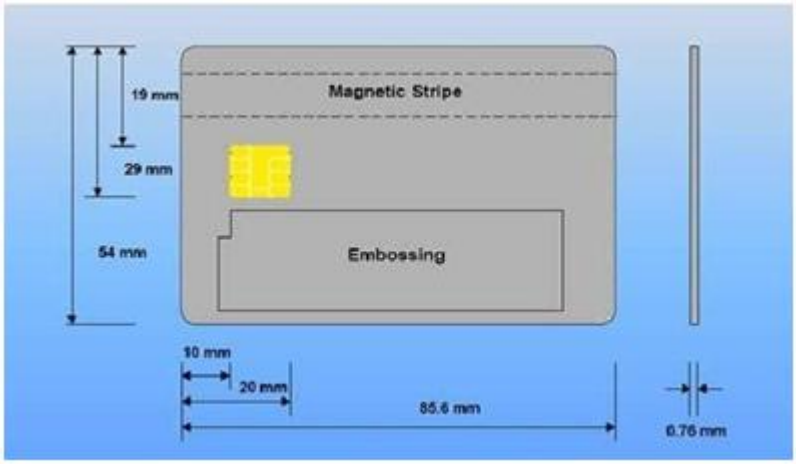


Figure 3: The Card Layout and Dimensions

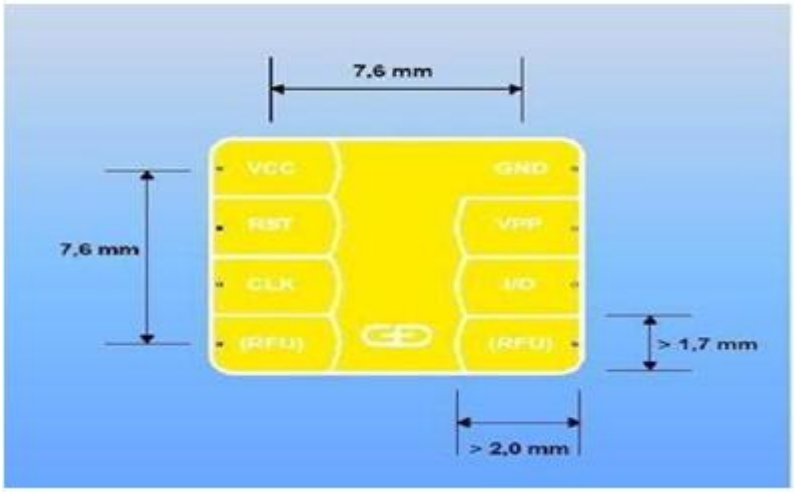


Figure 4: Contact Points and Pin Connections

When you insert the card into the reader, the contacts in the reader sit on the plates and the pin connections are according to the ISO7816 standards as seen in figure 4. The ATM card holds these data within different files, which is only visible to its program depending on the operating system of the card. These data files are arranged in a file system much like a Linux directory structure. The card capacity varies, depending on the architecture, from 16KB, 32KB and 64KB to 128KB; with 32KB capacity being currently the most popular [3].

3.5 Biometric Authentication

The term biometric comes from the word bio (life) and metric (measurement). Biometric equipment has the capability to measure, modify, compare, store, transmit and/or recognize a specific characteristic of a person with a high level of precision and trustworthiness. Biometric technology is based on the scientific fact that there are certain characteristics of living forms that are unique and not repetitive for each individual; these characteristics represent the only technically viable alternative to positively identify a person without the use of other forms of identification more susceptible to fraudulent behaviour. There are two major categories of biometric techniques: physiological (fingerprint verification, iris analysis, hand geometry-vein patterns, ear recognition, odour detection, DNA pattern analysis and sweat pores analysis) and behavioural (handwritten signature verification, key stroke analysis and speech analysis).

Transaction authentication represents a huge market as it includes transactions at an Automatic Teller Machine (ATM), electronic fund transfers, credit card and smart card transactions, transactions over the phone or on the internet etc. MasterCard estimates that smart credit card incorporating fingerprint verification could eliminate 80% of fraudulent cases.

Fingerprints are distinctive and persistent. Everyone has different fingerprints which do not change over a lifetime. Fingerprint solutions offer many advantages which address the human factors of authentication and it has the following distinct features:

a. One of a kind identifier: Fingerprints from each one of our ten fingers is distinctive, different from one another and from those of other persons.
b. Greater convenience: Users no longer has to remember multiple, long and complex, frequently changing passwords or carry multiple token keys.
c. Relatively equal security level for all users in a system-one account is not easier to break into than any other (such as easily guessed password or through social engineering).
d. Ensures the user is present at the point and tie of recognition and later cannot deny having accessed the system.
e. Cannot be shared, lost, stolen, copied, distributed or forgotten unlike passwords, PINs and smart cards. Fingerprints strongly link an identity to a physical human being making it difficult for attackers to forge.
f. Long history of successful use in identification tasks [3].

Ethernet is a family of computer networking technologies for local area networks (LANs). Ethernet was commercially introduced in 1980 and standardized in 1983 as IEEE802.3. Ethernet has largely replaced competing wired LAN technologies such as token ring, FDDI and ARCNET.

Systems communicating over Ethernet divide a stream of data into shorter pieces called frames. Each frame contains source and destination addresses and error-checking data so that damaged data can be detected and re transmitted. As per the OSI model, Ethernet provides services up to and including the data link layer. Since its commercial release, Ethernet has retained a good degree of compatibility. Features such as the 48-bit MAC address and Ethernet frame format have influenced other networking protocols.

Figure 5: An 8P8C modular connector (often called RJ45) commonly used on Cat 5 cables in Ethernet networks

Ethernet has evolved to include higher bandwidth, improved media access control methods and different physical media. The coaxial cable was replaced with point-to-point links connected by Ethernet repeaters or switches to reduce installation costs, increase reliability and improve management and troubleshooting.

Ethernet stations communicate by sending each other data packets: blocks of data individually sent and delivered. As 48-bit MAC address. The MAC addresses are used to specify both the destination and the source of each data packet. Ethernet establishes link level connections, which can be defined using both the destination and source addresses. On reception of a transmission, the receiver uses the destination address to determine whether the transmission is relevant to the station or should be ignored. Ethernet frames are said to be self-identifying, because of the frame type. Self-identifying frames make it possible to intermix multiple protocols together [8].

IV. Fingerprints

Fingerprints basically consist of ridges (raised skin) and furrows (lowered skin) that twist to form a distinct pattern as shown in figure. When an inked imprint of a finger is made, the impression created is of the ri dges while the furrows are the un-inked areas between the ridges. Although the manner in which the ridges flow is distinct, other characteristics of the fingerprint called “Minutiae” are most unique to the individual [4].

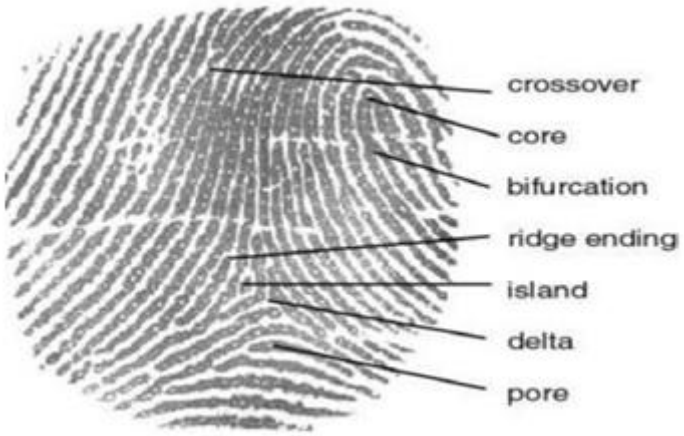


Figure 6: Fingerprint image

4.1 Fingerprint Authentication

Here the methodology of the project involves he use of a fingerprint biometric device incorporated to an existing
ATM screen with the aid of an existing pi n code system.
The software development kit helps to mo del the various stages of the authentication (fingerprint and pin) on the ATM screen. The integration of the two technologies 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 [5].

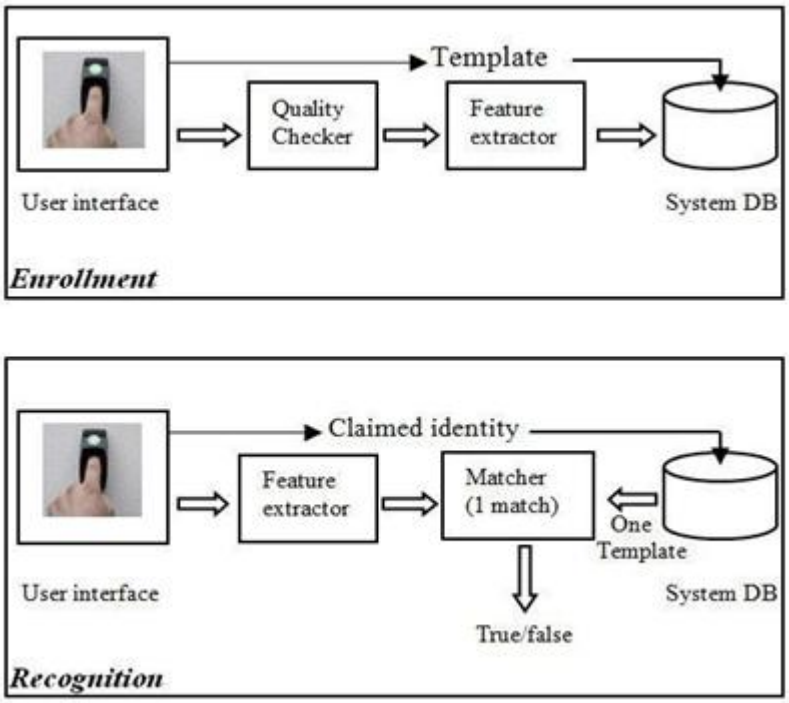


Figure 7: Process of Fingerprint authentication

The fingerprint reader captures the fingerprint image and extracts the unique features of the fin gerprint called template. This template is stored in system data base. When the authentication is to be performed, at that time the fingerprint reader reads the fingerprint of the user and extracts the unique features and this is compared with the previously stored template, which is in system data base [3].

V. Implementation

The idea behind this multi account embedded ATM card with enhanced security is that the customer can use a single ATM card to operate multiple bank accounts. Security is further enhanced by introducing fingerprint based authentication system.

The technology behind the product of the service is that adding all the user bank accounts to a multi account ATM card. In order to provide the access for the customer to all his/her bank account, first the fingerprint based authentication of the customer ne eds to be done. By introducing the biometric analysis (fingerprint authentication) we provide high sec urity for the customer because it is very difficult to fake [3].

The block diagram of the proposed system is as shown in the following figure. The parameters interfaced to ATM (ARM9 S3C2440A) are:

a. Fingerprint scanner (to read the fingerprint)
b. Smart card reader (to read th e smart card)
c. Ethernet (for communicatio n between ATM & bank server)
d. Ethernet to serial converters (to establish a compatible communication w ith 8052)
e. 8052 controllers (acts as ban k servers)

5.1 Block Diagram

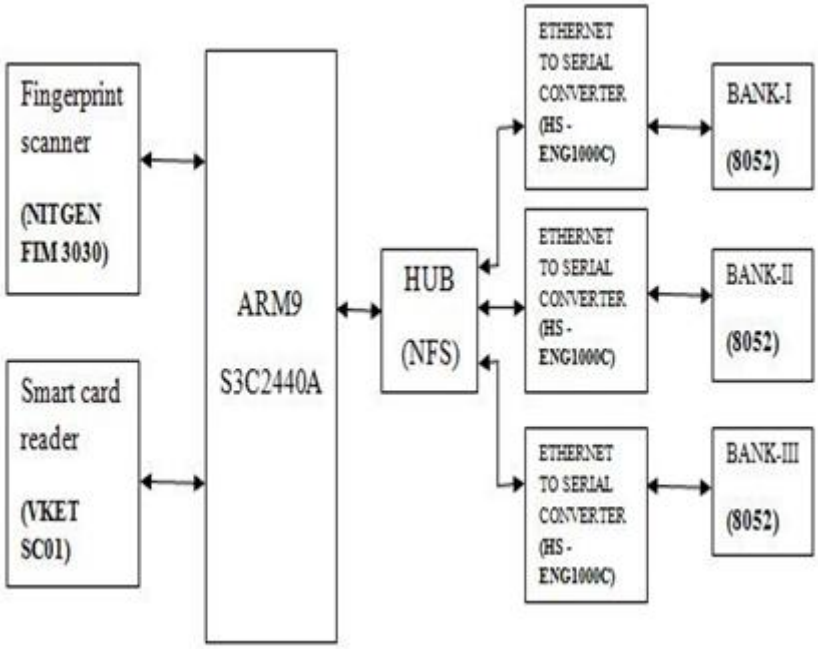


Figure 8: Block Diagram

Description: In this implementation, the ARM9 (S3C2440A) and smart card reader collectively represents an ATM machine. LCD (touch screen) screen is integrated on ARM9.

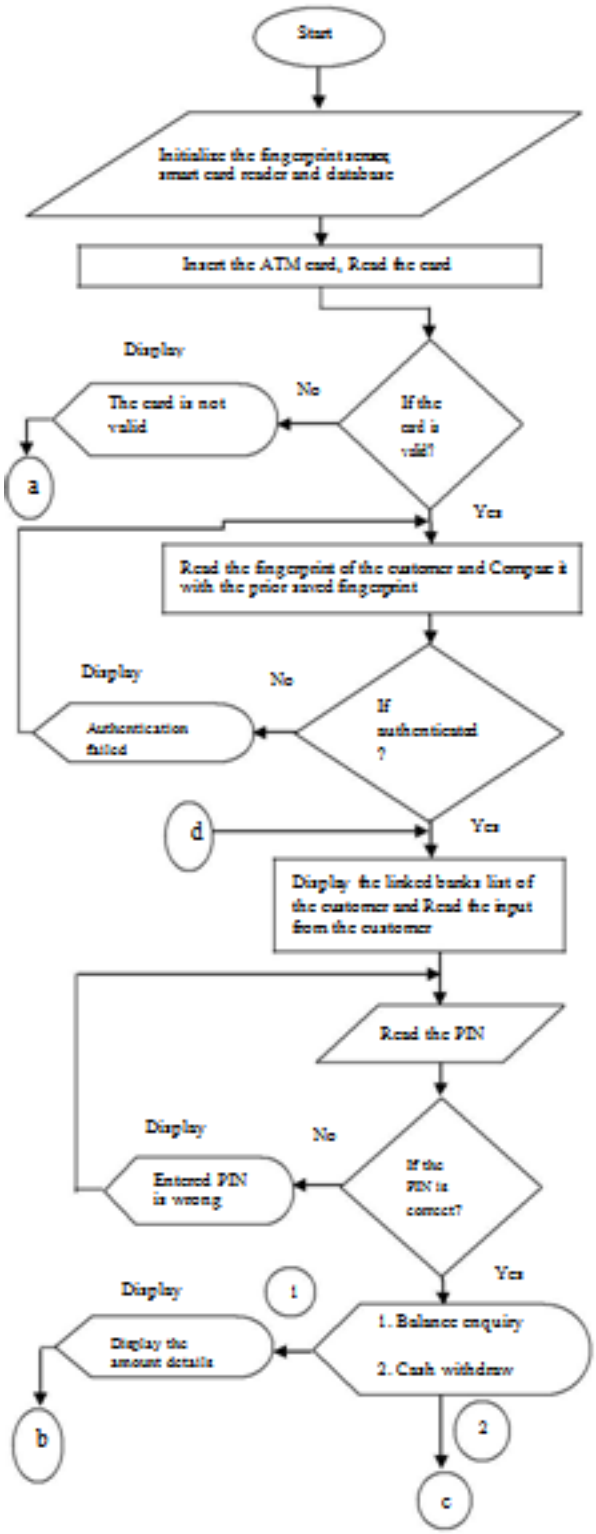
We are implementing a smart card as an ATM card with a small IC chip integrated on it. The ATM machine is interfaced with the fingerprint scanner to capture the fingerprint of the customer to be enrolled and/or authenticated. A minimum of three fingers were registered during the registration of the customer. The fingerprint sensor accepts the fingerprint image of the customer and extracts the unique features called as template of the fingerprint. This template undergoes comparison process with the template, which is earlier saved in the user's ATM card. A one-to-one comparison is done for authentication of the customer. If the fingerprint is matched correctly, then the ATM machine displays a message on the screen, indicating fingerprint validation of the customer. In this case the customer is allowed to continue with further transactions. If the fingerprint of the customer is not matched with the prior stored fingerprint, then the ATM displays a message for authentication failure. In this case the customer is not allowed to continue with further transactions.

After a successful verification of the customer, the list of banks that are registered and linked with the National Financial Switch are displayed on the screen. Here we are using HUB as NFS to route the transactions. The communication is carried over Ethernet between ATM and NFS. Between NFS and bank servers to establish a compatible communication for 8052, we are using Ethernet to serial converters. The customer is requested to select the bank of choice with which the customer intends to transact. On providing the bank of choice through touch screen, the corresponding bank server will be activated. Then the customer is asked to enter the PIN. The entered PIN is verified by controller by fetching the PIN from the respective bank server. After the PIN is authenticated, list of available services for the chosen bank account are displayed on the touch screen (LCD). Then according to the user input, the transaction is routed by the NFS. In this implementation the

respective bank data base corresponding to the customer, consisting of amount information is received by the controller through Ethernet by NFS.

In this project the bank servers are implemented using 8052 microcontrollers. The communication between the controller and the bank servers is carried out through Ethernet, but to establish a compatible communication for 8052, we are using Ethernet to serial converters. After the completion of transaction process the customer will get two options. One is

5.2 Flow chart



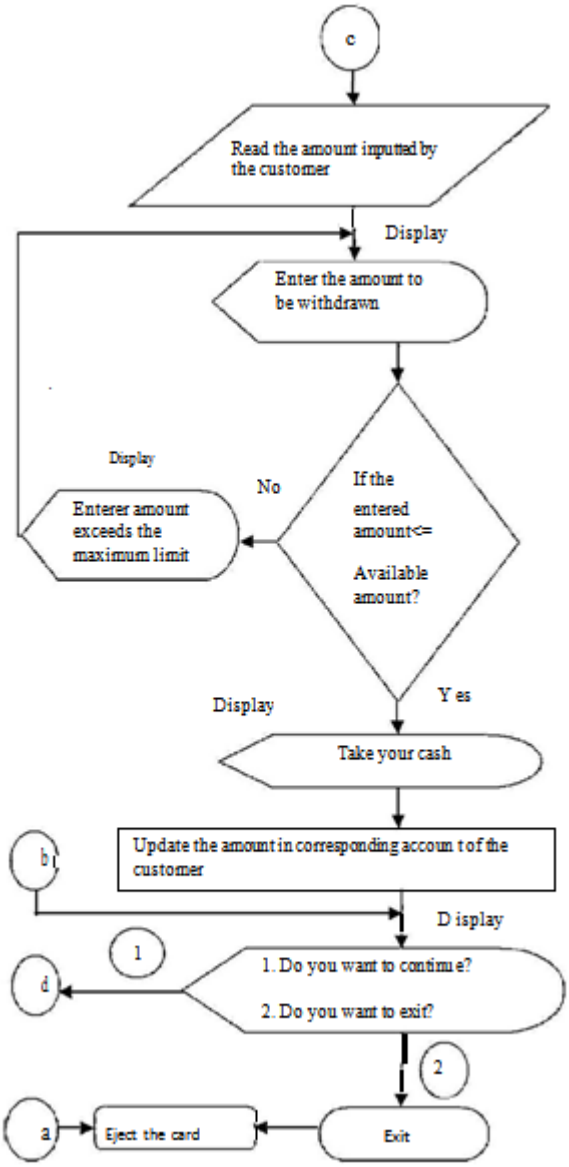


Figure 9: Flow chart

5.3 Features of multi account embedded A TM card with enhanced security system

1. More user friendly than the present system.
2. Reduces transaction cost.
3. Provides high security than the present syst em.
4. User can perform transactions for all his/her bank accounts using single ATM card and same PIN.
5. Interbank fund transfers are easily possible.

VI. Performance Evaluation

In order to evaluate the performance of the system three users were registered as genuine user s with different ATM cards. A minimum of three fingers were registered for each user. The three user's biometric templates were enrolled on the system to simulate storing it on their respective ATM cards.

Each user made three attempts on eve ry day for a period of three days each to access their account. Performance metrics such as False acceptance (FA), False rejection (FR), Correct accept (CA), Correct reject (CR) are observed.

Table 1 shows the performance metrics of the Multi Account Embedded ATM card.

	FA			FR			CA			CR		
	1	2	3	1	2	3	1	2	3	1	2	3
User-1	0	0	0	1	0	0	8	8	9	0	0	1
User-2	0	0	0	0	0	1	8	9	8	1	0	0
User-3	0	1	0	0	1	1	9	7	8	0	0	0

Table 1: Performance metrics of Multi acc ount embedded ATM card

FA is the number of imposter attempts that are falsely accepted.
FR is the number of customer attempts that are falsely rejected.
CA is the number of customer attem pts that are correctly accepted.
CR is the number of imposter attem pts that are correctly rejected.

From the above table we found that the accuracy of the proposed system is more than 91.35%. This could be further increased by enhancing the accuracy of the fingerprint module. Hence from the above conten t we conclude that the proposed system is providing high s ecurity compared with the existing system.

VII. Future enhancement

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.

VIII. Conclusion

This study is a venture into the e-banking system, especially

ATMs for easy, quick and multiple access to user's accounts with enhanced security. Users can access multiple accounts using a single ATM card to conduct different banking transactions. The system is also more convenient for users because they need not carry several bank ATM cards around and try to memorize many PINs.

References

[1]. Gokul.R, Godwin Rose Samuel.W, Arul.M, Sankari.C, "Multi account Embedded ATM card", "International Journal of Scientific and Engineering Research", Volume-4, Issue-4, April-2013.
[2]. Harshal M.Bajad, Sandeep E.Deshmukh, Pradnya R.Chaugule, Mayur S.Tambade, "Universal ATM Card System", "International Journal of Engineering Research and Technology", Volume-1, Isssue-8, October-2012.
[3]. Abayomi-Alli A., Omidiora E. O., Olabiyisi S.O., Ojo J.A., "Enhanced
[4]. E-Banking System with match-on-card fingerprint Authentication and Multi Account ATM Card", "International Journal of the Nigeria computer society", Volume-19 No.2, December-2012. A.Salma, C.Sarada Devi, V.Saranya, "Smart Card for Banking with highly Enhanced Security System", "SSRG-International Journal of Electronics and Communication Engineering", Volume-1, Issue-2, April-2014.
[5]. H. Lasisi and A.A. Ajisafe, "Development of stripe Biometric based fingerprint Authentication System in Automated Teller", IEEE 2nd "International Conference on Advances in Computational Tools for Engineering Applications", 2012.
[6]. Fumiko Hayashi, Richard Sullivan and Stuart E.Weiner, "A Guide to the ATM and Debit card Industry", 2003.
[7]. A Brief History of the ATM (http://mentalfloss.com/article/52714/brief-history-atm)
[8].] Ethernet (http://en.wikipedia.org/wiki/Ethernet)

Author Biography

Prof. M Sudhakar: He is graduated (B.Tech) from JNTU College of Engineering, Hyderabad in the year 1979, with the specialization of ECE. Later completed his post graduation (M.Tech) from Indian Institute of Technology, Madras in the year 1986 with the specialization of Instrumentation, Control & Guidance. He also did his PG Degree in Aeronautical Engineering
Bangalore in the year 1981. Presently pursuing his research in "Intelligent and Adaptive Control Systems, in JNTU Hyderabad. Completed R&D Project assigned by IAF on "Mathematical Modeling & Simulation of Aero Engine Control System_ at Aeronautical
Development Establishment, Bangalore and Gas Turbine Research Establishment, Bangalore for a period of 2 years.

K. Swathi (12H51D5512), received her B.Tech degree in Electronics & Communication Engineering from JNTU, Hyderabad, currently perceiving her M.Tech, Embedded Systems in CMR College of Engineering & Technology. Hyderabad.