Smart Card for Banking with Highly Enhanced Security System

A.Salma[1], C.Sarada Devi[2], V. Saranya[3]
[1,2,3] Student (B.E[ECE], University College of Engineering Arni, India)

ABSTRACT **:** Banking Transactions with ATM depends on authorization of a financial transaction by the card issuer or other authorizing institution via the communication network. At present every customer has an individual ATM card for each and every bank in which they maintain an account. Hence handling the ATM cards with confidentiality of their passwords play a major role here. To overcome this difficulty or complexity, embedding all their bank accounts of the users in a single ATM smart card in such a way that, the users can swipe the card and can select the bank from which they are interested to carry out transactions. Hence, a combination of multiple security compliments is mandatory to provide a high level of protection against fraud and other threats. As a result, the paper proposes framework for user identification and authentication in Automatic Teller Machine (ATMs) using Personal Identification Number (PIN) and Fingerprint identification. In addition with a GSM based security system for ATM machine is provided to prevent theft of money and other illegal activities in ATM machine. The security system automatically will send information to the nearby police station in such situations.

Keywords *- Automatic Teller Machines [ATM], biometrics, fingerprint, Global System for Mobile Communication [GSM, Personal Identification Number.*

1. INTRODUCTION

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 or human teller.

In most modern ATMs, the customer identifies him or herself by inserting a plastic card with magnetic strip or plastic Smart card with a chip that contains his or her account number [2]. The customer then verifies his or her identity by entering a pass code (i.e.) personal Identification number (PIN) of four digits. The use of the password or PIN schemes was introduced in the early days of multi-user (timesharing) machines and its use has continued into today's highly networked and distributed systems [2]. The system does not further identify the user if the password or PIN is incorrectly entered because the password or PIN is meant to be known only to the authorized user. This allows anybody related or unrelated to the user who knows the user's password or PIN to make illegal access or withdrawal. 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 transaction fee.

Personal identification based on biometrics has been receiving extensive attention in public security and information security domains [3]. The biometrics identification uses physiological characteristics of humans and distinguishes one from another. These characteristics are face, facial thermo grams, fingerprint, iris, retina, hand geometry etc. The Identification and authentication is a process for verifying a user identity. Identification is concerned with how the user provides his or her unique identity to the system [3]. The identity must be unique so that the system can distinguish one user from another. Authentication, on the other hand, is the process of associating an individual with his/her unique identity, which is the manner he/she establishes the validity of his/her claimed identity.

Authentication consists of three methods:

- Something you are (e.g., biological characteristics)
- Something you possess (e.g., a token or a card)
- Something you know (e.g., password or PIN)

The use of biological characteristics such as fingerprint has always been a better identification method rather PIN. The easiest biological characteristic to capture and process is fingerprint [5]. Among all the biometric techniques, fingerprint based identification is the oldest method which has been successfully used in numerous application. In this paper we propose a radically new set of banking transaction protocols with new architectural design [4]. We believe that the implementation of this model will make banking transactions more user friendly, more inexpensive and more secure.

2. FINGERPRINTS

Fingerprints basically consist of ridges (raised skin) and furrows (lowered skin) that twist to form a distinct pattern as shown in Fig 1. When an inked imprint of a finger is made, the impression created is of the ridges while the furrows are the un-inked areas between the ridges.

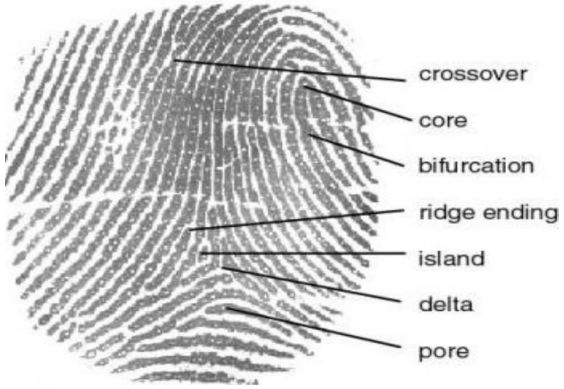

Fig 2.1 Fingerprint image

Although the manner in which the ridges flow is distinctive, other characteristics of the fingerprint called 'minutiae' are what is most unique to the Individual [1].

2.1 FINGER PRINT AUTHENTICATION

Here the methodology of the project involves the use of a fingerprint biometric device incorporated to an existing ATM screen with the aid of an existing pin code system. The software development kit (SDK) helps to model the various stages of the authentication (fingerprint and pin) on the ATM screen [3]. 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.

The card and fingerprint reader are installed on the ATM which has been already designed using C programming language; it also has the capability to operate on a network while the ATM server is up [1].

The ability to identify a customer based on fingerprint is incorporated in the ATM by changing the software and programming on the software development kit (SDK). User screens are created to guide the client through the process of entering the fingerprint and receiving notification of fingerprint acceptance or denial [1].

The Biometric system is implemented with a C programming language. Here it is designed with a C language to initialize client program, identification, fingerprint and normal transactions. The C language is written to initialize an existing pin code system which operates on the biometric system. The program is fully designed into the system through software changes on the software development kit. The application solicits the capture of the user's fingerprint and PIN number; the biometric system activates the sensor; the sensor captures the fingerprint, encrypts it and sends it to the biometric system [1]. The biometric system de-encrypts and processes the fingerprint, using the PIN, compares the captured fingerprint to the stored templates for the database user, and notifies the application of the results of the validation process and hence, provides appropriate transaction authorization or denial.

3. EXISTING SYSTEM

In existing ATM system all ATM machines are connected to their respective bank servers and all bank servers are connected to a single interface i.e. National Finance Switch (NFS) [3]. 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.

3.1 Disadvantages:

- User has to carry more than one ATM card for more number of bank accounts and also user has to remember password for each ATM card.
- User has to pay extra charges when transactions are done from different bank's ATM other than ATM card after fee transactions over.
- Do not have finger print recognition and theft detection in ATM.

4. PROPOSED SYSTEM

Universal ATM implementation requires minor change in present banking network. The routing algorithm and protocol needs to be changed [4]. The idea behind this universal ATM card is that the customers can use a single ATM card to operate different bank accounts instead of having individual card for each bank account and maintaining their pin's, carrying the cards safely which is a tedious process at present scenario. The technology behind the product of the service is that adding all the user bank accounts to a universal ATM card. In this the user swipes his/her smart card in the ATM machine, then it request for authentication in the server side [4]. After the user is authenticated with his fingerprint, then it displays the list of all banks that the user is having account. Now the user can select the bank from which he/she is willing to perform transaction. After selecting the bank the request is sent to the corresponding bank through a network and links it with the banks server for accessing the database of the user or customer so that the transaction is

processed. In case of theft, if the ATM machine is broken or damaged, the door of ATM center is locked automatically and buzzer is activated to alert the security.

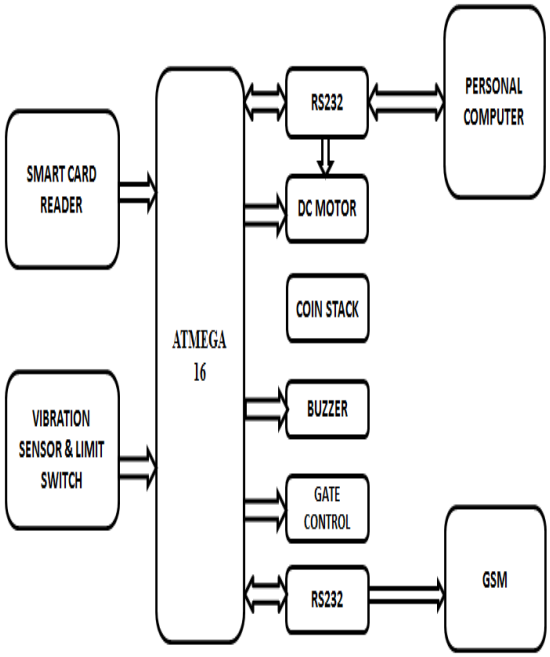

Fig 4.1 Block Diagram

ATMEGA16 is used in this project. If the user swipes the smart card with the help of Smartcard reader it will read the Radio frequency of that smartcard and send to the microcontroller. The microcontroller and the personal computer will connect through RS232. Then the personal computer will ask for fingerprint authentication. It will access the user fingerprint and then it will ask the user to give pin password. If both the fingerprint and pin password matched with the database which is already stored in a microcontroller of that particular database, then it will shows some list of banks where the account holder has account. With the help of vending machine using solenoid relay the user can withdraw the cash. If a thief tries to break the ATM the vibration sensor which senses some voltage due to vibration and it will make a alert using the buzzer. The limit switch will have two modes normally closed and normally opened. Actually it will be in normally opened condition which is connected with the vending machine. If a thief tries to break the ATM machine it will become normally closed and make the buzzer to alert.

Fig 4.2 Prototype model

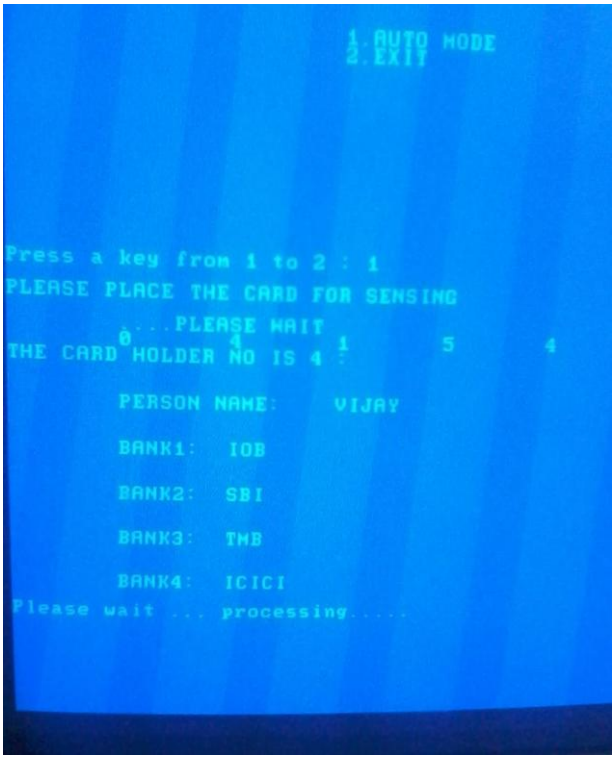

Fig 4.3 Display of multiple Account details

With the help of GSM module which is connected to RS232 it will send information to nearby police station and the door of an ATM machine will be automatically closed with the help of DC motor.

Figure 4.2 shows the prototype model of smart card for banking with highly enhanced security system,

which we have implemented. Fig 4.3 shows multiple account details of the user.GSM module is also added to this system to send instant password to the user number after user swipes his ATM card.

5.GSM

Global System for Mobile Communication (GSM) is the most popular standard for mobile phones in the world. This has also meant that data communication was built into the system using the 3rd Generation Partnership Project (3GPP). GSM also pioneered a low-cost alternative to voice calls, the Short message service. GSM is a digital mobile telephone system that is widely used in Europe and other parts of the world.

GSM uses a variation of Time Division Multiple Access (TDMA) and GSM is the most widely used of the three digital wireless telephone technologies (TDMA, GSM, and CDMA). GSM digitizers and compresses data then sends it down a channel with two other streams of user data, each in its own time slot. It operates at either 900 MHz or 1,800 MHz frequency band. GSM is the default wireless telephone standard in Europe. GSM has over one billion users worldwide and is available in 190 countries.

5.1.Technical details:

GSM is a cellular network, which means that Mobile phones connect to it by searching for cells in the immediate vicinity. GSM networks operate in four different frequency ranges. Most GSM networks operate in the 900 MHz or 1800MHz bands. Some countries in the Americans (including Canada and the United States) use the 850 MHz and 1900 MHz bands because the 900 and 1800 MHz frequency bands were already allocated. The rarer 400 and 450 MHz frequency bands are assigned in some countries, notably Scandinavia, where these frequencies were previously used for first-generation systems.

The Future of GSM together with other technologies is part of an evolution of wireless mobile telecommunication that includes High-Speed Circuit-Switched Data (DSCSD), General Packet Radio System (GPRS), Enhanced Data rate for GSM Evolution (EDGE), and Universal Mobile Telecommunications Service (UMTS).

6. FUTURE ENHANCEMENT

Since more than one bank accounts are being added, the existing PIN security and finger print authentication is not sufficient enough, so we can also embed a biometric scan like face recognition and vein authentication in the smart card i.e. multicomponent card. So that the user holds the card such that the face and vein rests on the biometric scan reader while he/she swipes the card and the image is authenticated at the real time. No one other than the user can use the card

7. 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 and reduces the complexity of managing more than one ATM card and their respective passwords. In this project Fingerprint provides a more viable method of identifying users' sufficient security level for the ATM system. The use of human characteristics in this prototype development tackles a lot of security implementation issues in identification and authentication of ATM.

The Implementation of ATM security by using fingerprint recognition and GSM MODEM took advantages of the stability and reliability of fingerprint characteristics. Additional, the system also contains the original verifying methods which are inputting owner's password and which is send by the controller. The security features were enhanced largely for the stability and reliability of owner recognition. The whole system is built on the technology of embedded system which makes the system more safe, reliable and easy to implement. Hence, the vulnerabilities of the ATM fraud will be reduced in future.

7.1 ADVANTAGES

The advantages of proposed system

- More user friendly than present system.
- Reduces transaction cost.
- Make banking system more inclusive.
- User can perform transactions for all his bank Accounts using single ATM card.
- Enhanced security system.
- Sending theft information to the nearby Police station.

REFERENCES

1. H. Lasisi and A.A. Ajisafe, "Development of stripe biometric based fingerprint Authentications Systems in automated teller", *IEEE 2nd International Conference on Advances in Computation Tools for Engineering Applications, 2012.*

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

3. Harshal M. Bajad1Sandeep E. Deshmukh2Pradnya R. Chaugule3Mayur S. Tambade4 , " Universal ATM Card System ", *International Journal of Engineering Research & Technology (IJERT) , October – 2012.*

4. Ronald Petrlic University of Paderborn, "Integrity Protection for Automated Teller Machines" , *International Joint Conference of IEEE 2011.*

5. Ugochukwu Onwudebelu, Olumide Longe, Sanjo Fasola, Ndidi C. Obi and Olumuyiwa B. Alaba , "Real Time SMS-Based Hashing Scheme for Securing Financial Transactions on ATM Systems", *3rd IEEE International Conference on Adaptive Science and Technology (ICAST 2011).*