Volume 1 No. 5, September 2011 ISSN-2223-4985
International Journal of Information and Communication Technology Research

http://www.esjournals.org

Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian E-Banking System

Sri Shimal Das, Smt. Jhunu Debbarma
Department of Computer Science & Engg. Tripura Institute of Technology, Narsingarh, Agartala – 799006

ABSTRACT

Biometrics based authentication is a potential candidate to replace password-based authentication. Among all the biometrics, fingerprint based identification is one of the most mature and proven technique. At the time of transaction fingerprint image is acquired at the ATM terminal using high resolution fingerprint scanner. Security measures at banks can play a critical, contributory role in preventing attacks on customers. These measures are of paramount importance when considering vulnerabilities and causation in civil litigation. Banks must meet certain standards in order to ensure a safe and secure banking environment for their customers. This paper focuses on vulnerabilities and the increasing wave of criminal activities occurring at Automated Teller Machines (ATMs) where quick cash is the prime target for criminals rather than at banks themselves. A biometric measure as a means of enhancing the security for banking system for both customer's & bankers also. We also proposed nominees fingerprint identification process while actual card holder unable to do the transactions.

Keywords: *Security, ATM, Biometric (Fingerprint), Crime, Verification, E-Banking, UML*

1. INTRODUCTION

Automated teller machine is a mechanical device that has its roots embedded in the accounts and records of a banking institution [3]. It is a machine that allows the bank customers to carry out banking transactions like, deposits, transfers, balance enquiries, mini statement, withdrawal and fast cash etc. Notwithstanding, we lived in a world where people no longer want to encounter long queues for any reason, they don't not want to wait for too long time before they are attended to and this has led to the increasing services being rendered by banks to further improve the convenience of banking through the means of electronic banking. On this note the advent of ATM is imperative, although with its own flaws. Crime at ATM's has become a nationwide issue that faces not only customers, but also bank operators [4]. Security measures at banks can play a critical, contributory role in preventing attacks on customers. These measures are of paramount importance when considering vulnerabilities and causation in civil litigation and banks must meet certain standards in order to ensure a safe and secure banking environment for their customers. Basically, the ATM scam involves thieves putting a thin, clear, rigid plastic sleeve into the ATM card slot. When you insert your card, the machine can't read the strip, so it keeps asking you to re-enter your PIN number. Meanwhile, someone behind you watches as you tap in your number. Eventually you give up, thinking the machine has swallowed your card and you walk away. The thieves then remove the plastic sleeve complete with card, and empty your account. The main fact that many of the customers have never used an ATM before and are completely unfamiliar with that concept therefore they are very unlikely to memorize and remember a PIN. Furthermore, there is a sense of mistrust with PINs. People may feel that it is unsafe because if they lose their card they worry that someone will find and somehow be able to determine their PIN and steal their money from the ATM. To keep it in mind we proposed a combined technique i.e. costumers insert their card & PIN, if costumers insert valid PIN then access is grant to another security approved process i.e. biometric fingerprint. Using valid PIN & biometric fingerprint costumer can access ATM transaction process i.e. deposits, transfers, balance enquiries, mini statement, Fast cash & withdrawal etc. By using fingerprint recognition customers are more comfortable with the idea of saving their money with the bank because they understand that if they lose their ATM card, no one can replicate their fingerprint and take their money. The way to avoid this is to run your finger along the card slot before you put your card in. The sleeve has a couple of tiny prongs that the thieves need to get the sleeve out of the slot, and you'll be able to feel them. The primary focus of this work is on developing a biometric strategy (Fingerprint) to enhance the security features of the ATM for effective banking transaction and more comfortable feature i.e. we proposed another option for nominee user because in case a card holder faces an accident, then the transactions process is not possible. To keep this drawback in mind we consider nominees fingerprint sample for second user to do the transaction while actual card holder unable to do the transactions. Actually PIN code are changeable but fingerprint are not changeable, so card holder may changes his/her PIN code while maintaining ones own secrecy and may permit his/her nominee with giving updated PIN code for transactions. We have considered the left & right thumb impression of an individual; it has been observed that there is no any match in these samples in any case. We have also observed that thumb impression samples have been taken in different angles & different forces. On study of these samples under the pattern matching algorithms as proposed it have shown at least up to 70% & more matching feature. The proposed algorithms have been

tuned to accept up to 70% matching tolerance. The rest of the paper arranged thus: section 2 presents Related works, section 3 presents Existing Banking ATM system in India, section 4 presents Biometric (fingerprint) strategy for Indian banking system, section 5 Represent Methodology, section 6 presents the Electronic banking system, section 7 presents Design and the general concept of the implementation, and section 8 presents Concludes the work.

2. RELATED WORKS

An embedded Crypto-Biometric authentication scheme for ATM banking systems is proposed in our paper. In this scheme, cryptography and biometric techniques are fused together for person authentication to ameliorate the security level [6]. The United Kingdom recently launched identity card scheme which has been analyzed by Shaikh and Rabaiotti (2009). They approach the scheme from the perspective of high volume public deployment and described a trade-off triangle model. They have found that there is a trade-off between several characteristics, i.e., accuracy, privacy and scalability in biometric based identity management system, where emphasis on one undermines the other (Shaikh and Rabaiotti 2009). The development and deployment phase of Belgium e-ID card has been discussed by Marein and Audenhove (2010). It has been argued that the pre-existence of national register was one of the factors that have helped in the development of the Belgium e- ID card. So far eight million cards have been provided to Belgium citizens mentioning the process was smooth and straightforward (Marein and Audenhove, 2010). A discussion on security and design of the Malaysian identity card, i.e., Mykad has been done by Raphael et al. (2003). Mykad integrates ID card, driving license, passport and ATM. As Mykad is used for various sensitive purposes, therefore, it is stated that its security features should be analyzed before it is deployed. It is important to consider the perceptions and response of end users while developing and analyzing biometric based identity management systems (Laurie et al., 2007). The commonly used biometrics are DNA, Face, Ear, Facial infrared thermo gram, Fingerprint, Gait, Hand and Finger geometry, Iris, Keystroke, Palm prints, Signature, Voice etc[5].A Physical Security, A Biometric Approach proposed by Ryan Hay SANS - GSEC Practical Track 1C November 12, 2003. Now a days Govt. of India also proposed varies Identity Card using Biometric based applications. Besides this we can also use this strategy in different field Govt. or non-Govt. in different applications. A Unique Identification is merely a string assigned to an entity that identifies the entity uniquely. We plan to assign a Unique ID to every person residing in India. Biometric identification system and checks would be used to ensure that each individual is as-signed one and only UID and the process of generating a new UID would ensure that duplicates are not issued as valid UID numbers [7]. Recently Govt. of India started a biometric based ID card i.e., 'Unique Identification Authority of India', it provides a unique identity to person residing in India.

3. EXISTING BANKING ATM SYSTEM IN INDIA

There is no doubt that rapid development of banking technology has changed the way in dealing with banking activities. One of the examples is automatic teller machine (ATM). Using ATM, a customer is able to conduct several banking activities such as cash withdrawal, money transfer, paying phone and electricity bills beyond official hours and physical interaction with bank staff. In short, ATM provides customers a quick and convenient way to access their bank accounts and to conduct financial transactions. Password or personal identification number (PIN) is one of important aspects in ATM security system which is commonly used to secure and protect financial information of customers from unauthorized access. The system compares the code against a stored list of authorized passwords and users. PIN typically in a form of four digit combination of numbers that entered through ATM panel. If the code is legitimate, the system allows access at the security level approved for the owner of the account fig. 1: shows the existing banking transactions system. In general, PIN is sufficient to protect against fraud and effectively eliminating most common attempts to gain unauthorized access. The four digit PIN is also easy to memorize and can be typed quickly with few errors and is quite difficult to be cracked if it is managed properly. The most recent cases show that the thefts have used sophisticated cracking programs to steal ATM holders' money very easily, some people who live in today's high tech society which are bombarded everyday by so many numbers such as social security number, computer password, credit card number and so on. Sometimes they are confusing, difficult to be recalled immediately which of course can lead to a serious problem. Sometimes it is written down on small piece of paper or on ATM card in order to anticipate such event. The strength of PIN as a security system is weakened since the likelihood of the code leaking to other people increased. A personal identification number (PIN) can be used in much the same as a password. It is numerical in format and like a password that should be kept secret. The most common use of the PIN is in automatic teller machines (ATM). "Most commonly PINs are 4-digit numbers in the range 0000-9999 resulting in 10,000 possible numbers, so that an attacker would need to guess an average of 5000 times to get the correct PIN." Biometrics is a rapidly evolving technology that is being widely used in forensics, such as criminal identification and prison security, and that has the potential to be used in a large range of civilian application areas. Biometrics can be used to prevent unauthorized access to ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks.

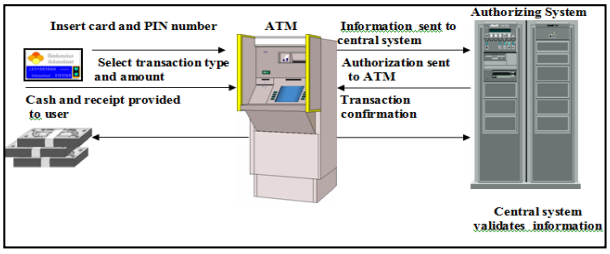

Fig. 1: Existing banking transactions system

4. PROPOSED BIOMETRIC (FINGERPRINT) STRATEGY FOR INDIAN BANKING SYSTEM

Biometric authentication has become more and more popular in the banking and finance sector [2]. The idea of fingerprint is not only for security but also to overcome the lack of customer understanding on ATM concept. We proposed ATM with biometric, a fingerprint security system, in order to meet its customers' needs who many of them have savings account and need to have access to their money during non-banking hours. Operated using only a smart card and a fingerprint scanner, the machines offer excellent security to card holders since there is very low possibility of fraud. If a customer loses the card, it is difficult for another person to use it because of the digital fingerprint. By using fingerprint recognition customers are more comfortable with the idea of saving their money with the bank because they understand that if they lose their ATM card, no one can replicate their fingerprint and take their money. Fingerprint authentication is the most popular method among biometric authentication, fingerprint based identification is one of the most mature and proven technique [1]. In banking system Biometrics holds the promise of fast, easy-to-use, accurate, reliable, and less expensive authentication for a variety of applications [5]. At the time of transaction customers enrolment their fingerprint to a high resolution fingerprint scanner. The fingerprint image is transmitted to the central server via secured channel. At the banking terminal the minutiae extraction and matching are performed to verify the presented fingerprint image belongs to the claimed user in bank database. The authentication is signed if the minutiae matching are successful. The proposed scheme is fast and more secure. Fig. : 2 Shows the whole procedures for proposed banking biometric application system in India. A basic biometric authentication system consists of five main components. These are: sensor, feature extractor, fingerprint/template database, and matcher and decision module. The function of the sensor is to scan the biometric trait of the user. The function of the feature extraction module is to extract the feature set from the scanned biometric trait. This feature set is then stored into the template database. The matcher modules takes two inputs, i.e. feature set from the template database and feature set of the user who wants to authenticate him and compares the similarity between the two sets. The last module, i.e., the verification module makes the decision about the matching of the two feature sets. Biometrics is a rapidly evolving technology that is being widely used in forensics, such as criminal identification and prison security, and that has the potential to be used in a large range of civilian application areas. Biometrics can be used to prevent unauthorized access to ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks.

5. METHODOLOGY

The security feature for enhancing the Indian banking ATM was designed using the client/server architecture. There will be a connection between the customer's identification information, customer's accounts and records in the bank (server). The network is designed to support a large number of users and uses dedicated server to accomplish this. The reason for choosing Client/Server model for this application is because it provides adequate security for the resources required for a critical application such as banking system. Similarly, a descriptive conceptual approach which includes Unified Modelling language (UML) tools such as Use case models, activity diagrams & sequence diagrams etc is adapted. The work is implemented using Visual Basic 6.0 software tool, used to design the user interfaces and/or cardholder interaction with the ATM Machine.

6. ELECTRONIC BANKING SYSTEM

Electronic banking is a new industry which allows people to interact with their banking accounts Via the Internet from virtually anywhere in the world. The electronic banking system addresses several emerging trends: customer demand for anytime, anywhere service, product time-to-market imperatives and increasingly complex back-office integration challenges. This system allows consumers to access their banking accounts, review most recent transactions, request a current statement, transfer funds, view current bank rates and product information and reorder checks. E-banking can be defined as the deployment of banking services and products over electronic and communication networks directly to customers [8]. It is the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels [9]. These electronic and communication networks include Automated Teller Machines (ATMs), direct dial-up connections, private and public networks, the Internet, televisions, mobile devices and telephones. Among these technologies, the increasing penetration of personal computers, relatively easier access to the Internet and particularly the wider diffusion of mobile phones has drawn the attention of most banks to e-banking. Significant differences exist among banks in terms of their e-banking capabilities. These differences can take two main dimensions. The first is the use of electronic

channels and the second is the sophistication of banking services delivered over an electronic channel.

Many established banks in developed countries began with ATMs and evolved through Personal Computer-banking, Telephone-banking, Internet-banking, TV-banking, and Mobile-banking. E-banking systems can vary significantly in their configuration depending on a number of factors. Financial institutions should choose their e-banking system configuration, including outsourcing relationships, based on four factors, therefore strategic objectives for E-Banking; scope, scale, and complexity of equipment, systems, and activities; technology expertise; and security and internal control requirements. In terms of e-banking services sophistication, this ranges from one way *information-push* services where customers receive information about the bank, its products and services to *information-download* where customers can download (or ask in case of telephone-banking) account information and forms to *full-transaction* services where customers can perform most banking transactions (such as transfer between accounts, bill payment, third party payment, card and loan applications, etc) electronically [10]. Recently some of the Indian banks provide new banking products (such as e-saving) that are only accessible electronically for their customer (example State Bank of India). Achieving these objectives tend to contribute strategic benefits in terms of better customer relationship management, increased customer base, and improved market image [4]. The electronic banking system brings the convenience of 24-hour, seven days a week, banking by offering home PCs tied directly to a bank's computers. In addition, electronic money also offers greater security than a paper-and-coin system. Users are able to make a backup copy of their funds and if the electronic money is stolen, the users can invalidate the serial number just as they now stop payment on a paper check. The banks will be able to offer their customers access to their services through the public Internet and parallel private network access, with security and privacy. Now a days in Tripura most of the bank provide internet banking facility & ATM facility for their customers. Some of the banks are S.B.I, U.B.I, Indian bank, Union Bank Of India, Bank Of Baroda, I.D.B.I., Syndicate bank, A.B.I, I.C.C.I etc, recently in Tripura, Tripura Gramin Bank also ready to provide internet banking facility, they already started ATM facility in branches in Tripura & probably last of November 2011 they will fully set up ATM facility all over India. Using this electronic banking technology customer's & banker's are happy & comfortable because customer need not require to interact with the bank, electrically full fill their requirement, it is not only saving time also provide banking facility 24 hours. Electronic banking is offering its customers with a wide range of services: Customers are able to interact with their banking accounts as well as make financial transactions from virtually anywhere without time restrictions. Therefore, any reliable e-Payment system should guarantee privacy, integrity, compatibility, efficiency, acceptability, convenience, mobility, anonymity and low financial risk [11].

7. PROPOSED SYSTEM DESIGN AND IMPLEMENTATION

This research is being carried out for the sole purpose of designing a three factor authentication metrics, that is, the ATM ID number, the PIN number and the Biometric feature (fingerprint) both card holder & nominee's. It is expected that the customer should possess an ATM card, to know and remember his/her PIN number and to enrol his/her fingerprint into the fingerprint device/reader adapter into the system. After which the fingerprint database compares the live sample provided by the customer with the template in the database, for identification proposed shows in figure 3. On confirmation that the information provided is true, that customer is granted access to the ATM system, for why proposed verification process shows in figure 4.

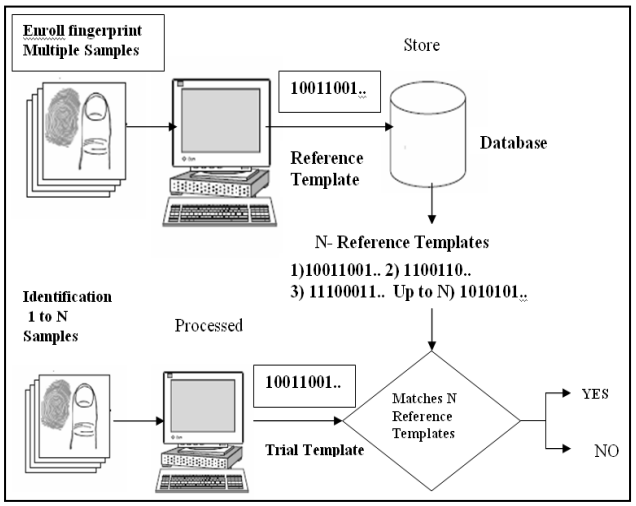

Fig. 3: Fingerprint Identification process

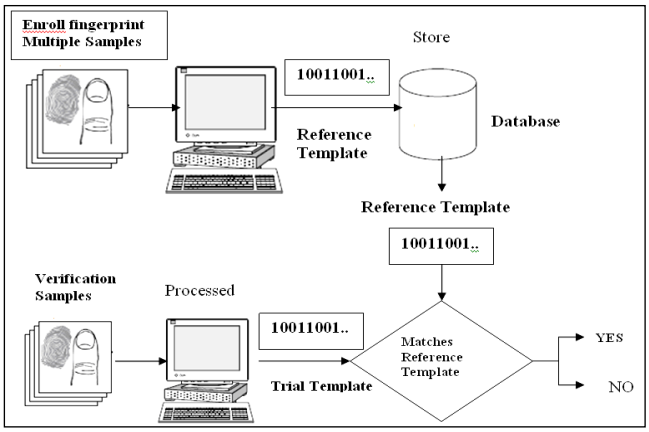

Fig. 4: Fingerprint Verification process

Similarly, we have also proposed customer's nominee concept for doing the transactions while actual customer is unable to do the transaction. For the design of this system Unified Modelling language tools (use case

models, activity diagram & sequence diagram) to represent how the user (bank customer) interacts with the proposed system are employed. Use cases are scenarios for understanding system requirements. A use-case model can be instrumental in project development, planning, and documentation of system requirements. A use case is an interaction between users and a system; it captures the goal of the users and the responsibility of the system to its users. It describes the uses of the system and shows the courses of events that can be performed as well as defining what happens in a system. In essence, the use case model tries to systematically identify uses of the system and provides an external view of a system or application; it is directed towards the users or the "actors" of the systems, not its implementers. In the design of the banking ATM application, the actor of the bank system is the bank customer. The bank customer must be able to deposit certain amount to and withdraw any amount from his or her accounts (provided he/she has up such amount in the account) using the bank application. Figure 5 show the use case diagram for our system design, where customers can perform transaction by inserting their ATM card and carry out the Approval Process by entering PIN Number and Confirm Fingerprint. After the approval, customer is requested type of transaction (deposit of money or withdrawal of money), and the transaction is carried out accordingly. At the completion of the transaction, the customer exit Application and remove his/her card.

A detail description of the system is shown in the activity diagram in figure 6. The business models of ATM transaction are highlights the card insertion, PIN validation, Fingerprint validation, transaction, withdrawal/deposit/fund transfer/fast cash/ mini statement etc.) & successfully removal of card after completion. Figure 7 shows the sequence diagram for use case withdrawal amount the following classes are identified: Bank client, ATM machine & Account. Here a simple valid transaction of withdraw Use case is taken to identify classes, without considering extension points such as overdraft, deficit &cross today's withdraw limit.

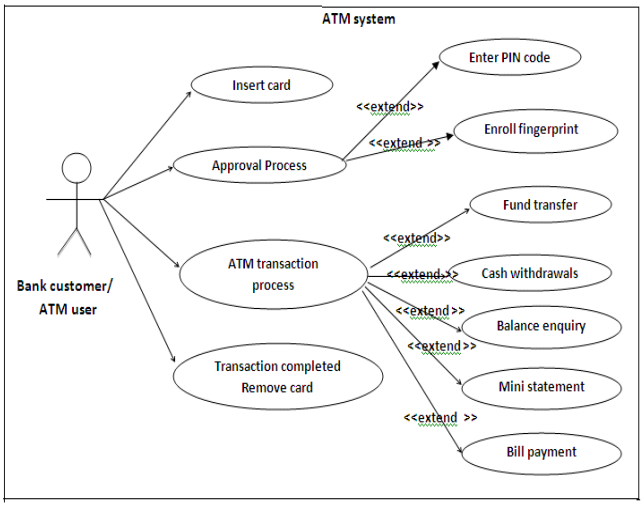

Fig. 5: Use case diagram for our system design

A detail description of the system is shown in the activity diagram in figure 6. The business models of ATM transaction are highlights the card insertion, PIN validation, Fingerprint validation, transaction, withdrawal/deposit/fund transfer/fast cash/ mini statement etc.) and successfully removal of card after completion. Figure 7 shows the sequence diagram for use case withdrawal amount the following classes are identified: Bank client, ATM machine & Account. Here a simple valid transaction of withdraw Use case is taken to identify classes, without considering extension points such as overdraft, deficit &cross today's withdraw limit.

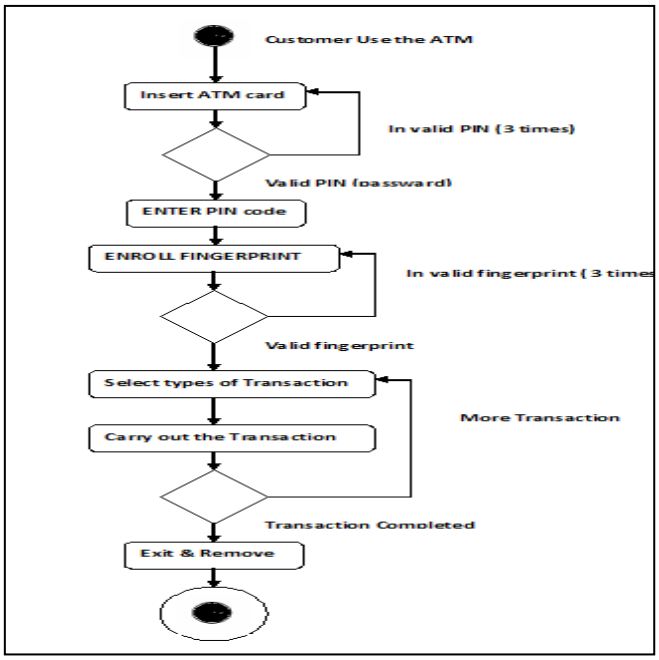

Fig.6: Activity diagram for Use case model

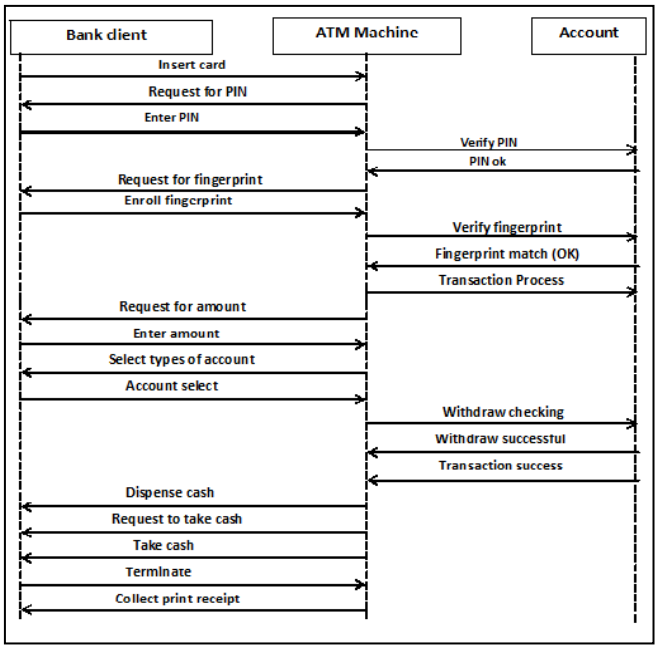

Fig. 7: Sequence diagram for Use case model

Besides this using Visual Basic 6.0 software tool, used to design the Customer/Card holder interfaces and/or cardholder interaction with the ATM Machine. Customer/Card holder Interface Design: A Customer/Card holder interface is a friendly means by which Customer/Card holder interfaces of a system can interact with the system to process inputs and obtain outputs. It is also a means of communication between the human user and the system through the use of input/output devices with supporting software tools. This particular ATM application is made up of 9 interfaces, which include; 1) ATM Login Interface -1 (PIN CODE Interface), 2) ATM Login Interface -2 (Enroll Fingerprint Interface), 3) Banking Transaction Type Interface, 4) Withdrawal Interface, 5) Deposit Interface, 6) Mini statement Interface 7) Fund Transfer Interface 8) Fast Cash Interface and 9) View statement of Account Interface etc.

Customer/Card holder Interface Design:

This interface is the very first interface the bank customer interacts with on the ATM machine. This interface prompts the customer to insert ATM card and proceeds with the entire authentication processes, that is, PIN number. If the user enters an invalid card number or PIN number, a dialogue box appears prompting an invalid PIN or invalid card number and the system returns enter a valid PIN number. A typical description of this is (see figure 8) figure. After validating the customer's PIN number, the customer is directed to the next phase of the authentication process via the authentication dialogue box for inputting the valid fingerprint i.e. Fingerprint Interface. This is the final interface the customer interacts with in the authentication process. It requests from the customer the enrolment of his/her fingerprint to be placed on a Fingerprint reader. The fingerprint reader accepts the fingerprint and seeks to match the live sample with the already enrolled templates in the banks database. The fingerprint of an individual is very peculiar to that individual since no two individuals can have the same fingerprint. The fingerprint reader captures the fingerprint features of an individual and search for a match of fingerprint brought up for identification among the stored fingerprints in the database. The fingerprints stored are kept along side the other ID's (Pin and Card Numbers) and the corresponding biometric templates are kept in the database. When the fingerprint is found correct, the customer is taken to the transaction phase where he/she will choose among the transactions, otherwise the customer is denied access and the system brings up a dialogue box for which the customer can choose Ok, and as soon as this done the system automatically log off the customer (see figure 9 & figure 10). After inserting valid PIN code & valid enrolment fingerprint customer can access banking transactions phase i.e. Fast cash, Withdrawal, Deposit, Mini statement, Fund Transfer, Balance enquiry etc. (see figure 11).

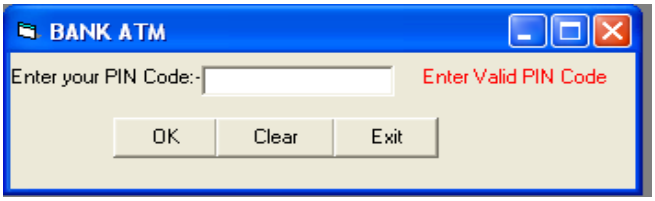

Fig. 8: ATM login Interface -1

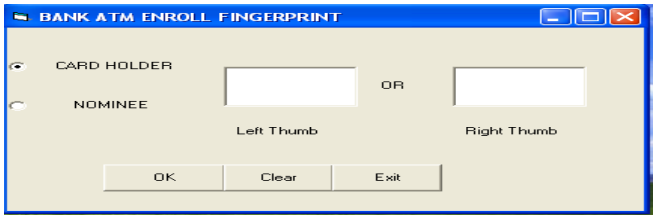

Fig. 9: ATM login Interface-2

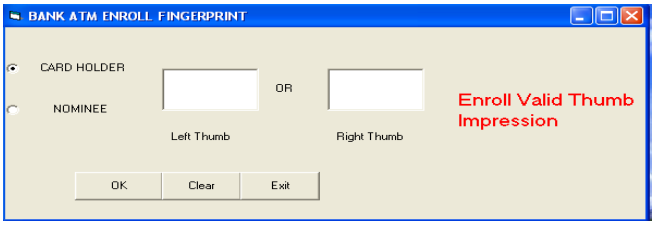

Fig. 10: Invalid Fingerprint

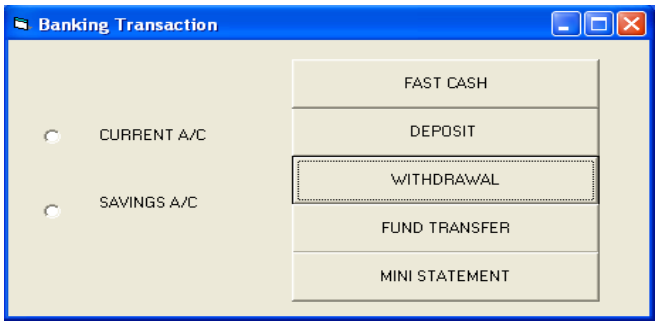

Fig11: Banking Transaction Interface

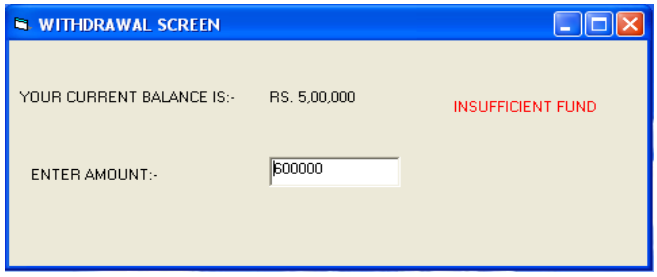

Fig. 12: ATM Withdrawal Interface

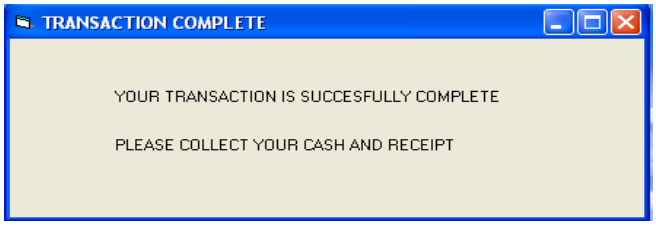

Fig. 13: ATM Transaction Closing Interface

This paper we only focus withdrawal Interface, This interface enables the customer withdraw money from his/her account. It shows the customers previous account balance for ensure, after inserting withdrawal amount it will check your previous balance if previous balance >= withdrawal amount then, a dialogue box pops up notifying the customer receive Cash & receipt else, a dialogue box pops up notifying the customer of his/her account has insufficient fund, the meaning is you can not withdraw money from your account if your previous balance less then the withdrawal amount (see figure 12). After the customer has completed all his/her withdrawals, a dialogue box pops up notifying the customer of his/her successful withdrawal transaction. The interface is shown figure 13.

8. CONCLUSION

Automatic Teller Machines have become a mature technology which provides financial services to an increasing segment of the population in many countries. Biometrics, and in particular fingerprint scanning, continues to gain acceptance as a reliable form of securing access through identification and verification processes. This paper identifies a high level model for the modification of existing ATM systems using both security protocols as PIN & Biometric fingerprint strategy. We have been able to develop a fingerprint mechanism as a biometric measure to enhance the security features of the ATM for effective banking transaction for Indian E-banking system. The prototype of the developed application has been found promising on the account of its sensitivity to the recognition of the customers' finger print as contained in the database. This system when fully deployed will definitely reduce the rate of fraudulent activities on the ATM machines such that only the registered owner of a card access to the bank account.

REFERENCES

[1] A Method to Improve the Security Level of ATM Banking Systems Using AES Algorithm, N.Selvaraju & G.Sekar, *International Journal of Computer Applications (0975 – 8887) Volume 3 – No.6, June 2010.*

[2] Biometric authentication in relation to payment systems and ATMs A new approach for biometric Verification using finger veins and the start of the proliferation of biometric incorporated ATMs by Gerik Alexander von Graevenitz.

[3] Wan, W.W.N.; Luk, C.L.; and Chow, C.W.C. (2005), Customers Adoption of Banking Channels in Hong K34rong, *International Journal of Bank Marketing*, Vol. 23, No. 3, pp. 255-272.

[4] Richard, B.and Alemayehu, M. (2006) Developing E-banking Capabilities in a Ghanaian Bank: Preliminary Lessons. *Journal of Internet Banking and Commerce*, August 2006, vol. 11, no.2. available online http://www.arraydev.com/commerce/jibc/)

[5] Recognition : Novel Approach for Library Patron Authentication ,Achintya K. Mandal & Subodh Gopal Nandi, West Bengal, India, online (*http://www.ibia.org*)

[6] A Method to Improve the Security Level of ATM Banking Systems Using AES Algorithm ,N.Selvaraju & G.Sekar, Sri Ramakrishna Institute of Technology, Coimbatore-641010, *International Journal of Computer Applications (0975 – 8887) Volume 3 – No.6, June 2010].*

[7] A UID NUMBERING SCHEME, Hemant Kanakia, Srikanth Nadhamuni and Sanjay Sarma, May, 2010.

[8] Singh, B. and Malhotra, P. (2004) Adoption of Internet banking: An empirical investigation of Indian banking Sector. *Journal of Internet Banking and Commerce*, 9 (2).

[9] Chai, L. G, (2005) E-Banking in Malaysia: Opportunity and Challenges, *Journal of Internet Banking and Commerce*, December 2005, vol. 10, no.3, available online – (http://www.arraydev.com/commerce/jibc/).

[10] Diniz, E. (1998) Web Banking in USA. *Journal of Internet Banking and Commerce*, 3, (2).

[11] Design of a secure unified e-payment system in Nigeria: A case study Charles K. Ayo1 and Wilfred Isioma Ukpere2*, African Journal of Business Management Vol. 4(9), pp. 1753-1760, 4 August, 2010, ISSN 1993-8233 ©2010 Academic Journals