A THIRD GENERATION DESIGN   FOR SECURED ATM TRANSACTION USING SIM CARD

A.Chandhanaa , Durga.S

Adhiyamaan college of engineering, Hosur, Dept., Of CSE

chandhanaa95@gmail.com,durga.hosur@gmail.com

ABSTRACT- The use of mobile handheld devices is expanding rapidly both within the business and individual context. These devices are now essential tools that offer competitive business advantages in today's growing world of ubiquitous computing environment. The technology advancement has made it possible to embed more facilities in mobile phones. While they provide benefits, they also pose new risks on security either by the information they contain or information that they can access remotely. Secure cash transaction is of serious concern in growing use of cash cards and internet transactions. The main objective of this project is to create a new generation of ATM machine in which transaction can be made without ATM cards. Because in existing system the user should carry the ATM card without fail. In this system ATM machine can be operated by using SIM in the mobile phone. When the SIM is inserted in the reader unit of the ATM machine it transfers the mobile number information to the server. In server the related information of the mobile number (i.e) the users account details, their photos etc. are collected. The Face recognition module and Fingerprint recognition module present in the ATM machine compares the image and fingerprint ridges of the consumers with the existing one in the server. Only when the image and fingerprint matches, it asks for the PIN number and further processing starts. Otherwise the process is terminated. So, by using this system the need of ATM card is completely eliminated. We can operate the ATM machine with SIM itself. This paper will introduce the concept of physical browsing and development of a system that will allow users to use their mobile phones to securely withdraw cash from ATM machines. The paper presents the new generation of ATM machine for M-Cash withdrawal application, relevant technologies and security issues. By using this system malfunctions can be avoided and the transaction will be much secured.

1. INTRODUCTION

Automated teller machine is a mechanical device that has its roots embedded in the accounts and records of a banking institution. 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. 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 and face recognition. Using valid PIN, fingerprint and image of the 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 and image of the person are not changeable, so card holder may changes his/her PIN code while maintaining one's 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. To achieve various functionality and make good use of mobile devices so that people can keep them and utilized their potentials.

2. 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. 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 +9used 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. There has been a growing use of Radio Frequency Identification Tags (RFID) in different business environments. A typical example includes supermarkets, airline industry and the majority of supply chains. The main advantage of RFID to businesses is being the effectiveness of identifying System that transmits the identity (in the form of a unique serial number) of an object wirelessly, using radio waves

luggage/product; providing good customer service; cost reduction and flexibility. In this paper this technology has been used in a new application called Secure M-Cash Withdrawal, a system whereby a mobile phone is equipped with RFID tags and NFC. The mobile will interact with an ATM machine which is equipped with RFID reader and writer and a banking system. The process of interaction will be utilized using the physical browsing phenomenon. The main purpose of interacting via mobile device is to improve the security of transactions as well as eliminating the need to use cash/credit cards.
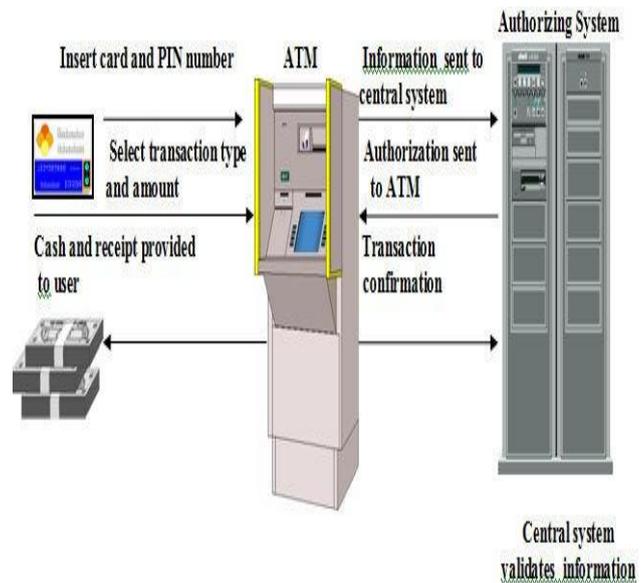

Fig. 1: Existing banking transactions system

3. ATM TECHNOLOGIES, STANDARDS AND SERVICES

ATM technologies, standards, and services are being applied in a wide range of networking environments, as described briefly below (Fig. 2)
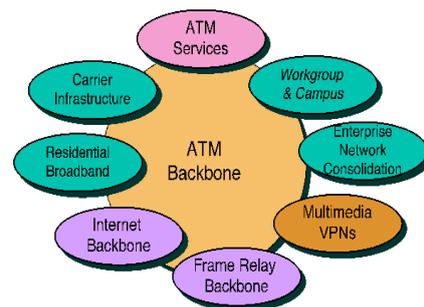

Fig.2: ATM Technologies, Standards and Services

❖ ATM services— Service providers globally are introducing or already offering ATM services to their business users.

❖ ATM workgroup and campus networks— Enterprise users are deploying ATM campus networks based on the ATM LANE standards. Workgroup ATM is more of a niche market with the wide acceptance of switched-Ethernet desktop technologies.

❖ ATM enterprise network consolidation — A new class of product has evolved as an ATM multimedia network-consolidation vehicle. It is called an ATM enterprise network switch (ENS). A full-featured ATM ENS offers a broad range of in-building (e.g., voice, video, LAN, and ATM) and wide-area interfaces (e.g., leased line, circuit switched, frame relay, and ATM at narrowband and broadband speeds) and supports ATM switching, voice networking, frame-relay SVCs, and integrated multiprotocol routing.

❖ Multimedia virtual private networks and managed services — Service providers are building on their ATM networks to offer a broad range of services. Examples include managed ATM, LAN, voice and video services (these being provided on a per-application basis, typically including customer-located equipment and offered on an end-to-end basis), and full-service virtual private-networking capabilities (these including integrated multimedia access and network management).

❖ Frame-relay backbones — Frame-relay service providers are deploying ATM backbones to meet the rapid growth of their frame-relay services to use as a networking infrastructure for a range of data services and to enable frame relay to ATM service interworking services.

❖ Internet backbones — Internet service providers are likewise deploying ATM backbones to meet the rapid growth of their frame-relay services, to use as a networking infrastructure for a range of data services, and to enable Internet class-of-service offerings and virtual private intranet services.

❖ Residential broadband networks — ATM is the networking infrastructure of choice for carriers establishing residential broadband services, driven by the need for highly scalable solutions.

❖ Carrier infrastructures for the telephone and private-line networks — Some carriers have identified opportunities to make more-effective use of their SONET/SDH fiber infrastructures by building an ATM infrastructure to carry their telephony and private-line traffic.

4. PROPOSED ATM BANKING SYSTEM

Biometric authentication has become more and more popular in the banking and finance sector. 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 face recognition and fingerprint security system, in order to meet its customer's needs who many of them have savings account and need to have access to their money during non-banking hours. Operated using only a SIM 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 and image of the original user. 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. In banking system Biometrics holds the promise of fast, easy-to-use, accurate, reliable, and less expensive authentication for a variety of applications. 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 and 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. 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.
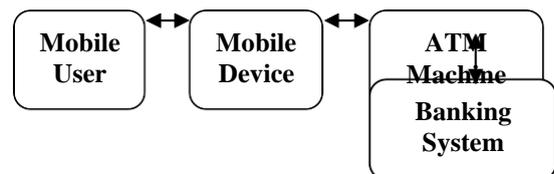

Fig. 3: Proposed ATM system

5. ARCHITECTURE

The overall architecture of this third generation ATM transaction using SIM card is described below:
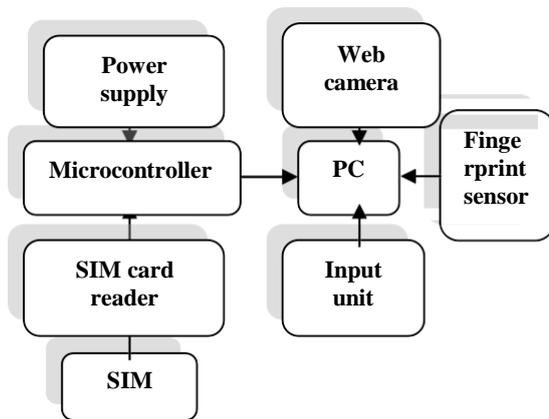

Fig.4:Architecture of third generation ATM

User's SIM card is inserted into the SIM slot unit. SIM card reader device scans SIM number through GSM Modem. GSM Modem is a data oriented GSM transceiver system that uses a network provider to connect and transfer data. GSM modem has on board RS-232 converter that you can use to connect the modem directly to a PC serial port. Using a windows accessory program HyperTerminal, you can immediately begin test driving your GSM Modem. The GSM Modem will work with just about any popular microcontroller.

Microcontroller with a built-in UART; this will save you from having to write bit banging codes that only for advanced programmers to consider. If your microcontroller works on 3.3V supply,
interfacing will be a breeze. Interfacing to a 5V microcontroller will require some
more work. The RX pin of the GSM Module is designed to accept 3.3V logic level only, forcing a 5V logic input may damage the GSM Modem. To
prevent this, a resistive divider must be added on the TX pin of your 5V microcontroller circuit. The GSM SIM card reader unit scans the mobile number, Which data given to the Teller machine for further processing. At the same time, web camera captures the images and comparing with the existing user's image using digital signal processing. And further it requires fingerprint for the access of money from ATM machine. Atmel Company's AT77CI04B be used as a fingerprint recognition. It has a 500dpi resolution, anti-press, anti-static, anti-corrosion. If an image, finger print & PIN number are same then further processing continued. Otherwise the process gets terminated.

6. SECURITY CONSIDERATION

The Secure M-Application deals with information transfer and financial transactions. Hence, the security elements considered during the design and implementation stage consist of making sure that the RFID and NFC used are in compliance with the ISO 14443 standards. WLAN technologies are equipped with the latest encryption protocol

standard. WEP and WPA address these issues by providing password protection for access control and encryption for privacy. The wireless security protocol 802.11w which is to be introduced in April 2008 has promised to provide facilities that will prevent denial of service attacks and make use of the AES encryption standards. These protocols (WEP and WPA), only deal with access control and privacy issues. That is determining who is allowed to enter your network and hiding information from hackers who may try to intercept information during transmission. However because the Secure M-application is more susceptible to security threats, the design incorporates other security measures such as making use of Biometric data, as a further authentication layer. It can utilize any of the fourteen different types of biometrics that fall within two categories namely: those that measure behaviour and those that measure physical traits. Any of the Biometric information within these types can be used in identifying users, by making use of individual anatomy or physiology, that is either deeply ingrained into the skin, or other behavioural characteristics, or it can be a combination of the two. Hence, the data will be used as a unique personal attribute for security and authentication purposes. Since the focus of this paper is not on analyzing biometrics as a means of authentication, details on the use of biometric can be found in and using biometric data to generated encryption and decryption keys. Both authentication factors are needed to match the stored once before allowing access to transactions else authentication will be automatically denied. This process will be able to reduce the effects of brute force attack, as millions of combinations need to be tried before gaining access and as only 3 tries are allowed this should prevent such attacks from occurring. Also it is important to point out that a single sign-on process will improve the reliability of identity management and access control. Having this application as the security measure, the Secure M-Cash Withdrawal will be able to provide an excellent wireless identity management that will remove the current risk of identity theft and meet the required security standard of implementing the secure M-cash withdrawal and other M-applications.

7. USE OF ATM:

The following uses can be made by using both ATM card as well as SIM card

➢ **Cash Withdrawal and Balance Enquiry**
In spite of a number of innovative services being made available at many ATMs, cash withdrawal stills remains the most accessed service at ATMs. However, the migration of routine bank transactions like cash withdrawals and balance enquiries from teller counters to ATMs significantly raises the potential for savings in employee costs and greater employee focus on value-added revenue-enhancing activities such as selling other financial products and advisory services to customers.

➢ **Cash /Cheque Deposit**
Again, due to the strong cash culture in India, cash deposits are most likely higher than in other markets, especially cash deposits made by commercial

customers such as retail shopkeepers and those whose work involves substantial travelling. A high cash withdrawal rate results in higher ATM servicing costs due to frequent cash replenishment requirements. Recent developments in ATM technology have made it possible to recycle cash in ATMs. Currency notes received as cash deposits are counted; soiled notes separated and deposited cash dispensed to fulfil withdrawal transactions. However, regulatory concerns relating to identification of counterfeit notes and its depositors need to be addressed first. ATM with Cheque deposit facility is not picking up in India, like other countries. One of the reasons is the delay in collection of the cheque deposited in ATMs. Cheque deposited in ATMs is to be collected and deposited in the designated branch for collection. Another reason is the introduction of cheque deposit Kiosks by various Banks especially Private sector ones. These are kept at each some important locations/branches where customers can deposit their cheques which are collected at intervals which may be difficult in ATMs.

> **Bill   Payments**
Most utilities have inadequate infrastructure for receiving bill payments resulting in long queues at collection centres. Hence, bill payment at ATMs has achieved noticeable acceptance by bank customers. Most banks provide this service through bi-lateral arrangements with bill-payment service providers. ATM users register their water, electricity and telephone utility accounts with banks, check their dues at ATMs, approve bill payments that are debited to their bank accounts and receive printed receipts for the transactions. This service has the effect of improving customer satisfaction for both the bank as well as the bill-payment service providers. Some Banks' ATMs even accept charitable contributions to Temples.

> **Sale   of   Paper   Based   Products**
ATMs are ideally suited to sell paper-based products and services such as tickets, wireless phone recharge cards, financial products, etc. The screen interface allows browsing and customization, access to bank accounts facilitate payments and printing capabilities produce the actual product/service. A number of banks including ICICI Bank, SBI and PNB have ATMs at Mumbai's local railway stations to dispense season tickets to commuters. Own-bank customers pay no extra charge while other bank customers pay a fee of Rs. 50 for this extremely useful service of anytime ticket purchase. Railway season tickets represent a high-volume mass-appeal product. As technical standards get established and product/service sellers become aware of the ATM sales channel, niche-appeal high-margin products like entertainment tickets will join the fray.

8. CONCLUSION

This paper presents the new idea that can be used as a means of interaction between mobile phone, ATM machine and a Banking application for the purpose of withdrawing cash. The proposed design ; the secure M-cash withdrawal allows the use of mobile phones as a tool of interaction and provide flexibility through a robust identity management architecture. The Secure M-cash has examined the possibility of making use of similar approaches/techniques (RFID and NFC) for other applications and already there are some applications that have adapted this strategy. The Secure M-Cash Withdrawal has been defined, it will form as a foundation for future work within this area, which includes implementing a PC based simulation of the architecture and implementing the system. 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 & face recognition module. 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 E-banking system. The prototype of the developed application has been found promising on the account of its sensitivity to the recognition of the customer's 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] Välkkynen, P. Korhonen, I., Plomp, J., Tuomisto, T., Cluitmans, L., Ailisto, H. and Seppä, H. ‒A user interaction paradigm for physical browsing and near-object control based on tags‖: in *Proc. Physical Interaction Workshop on Real World User Interfaces*, (2003), 31-34. Authorized licensed use limited to: Bharat University. Downloaded on October 10, 2009 at 08:53 from IEEE Xplore. Restrictions apply.

[2] *Lauri Pohjanheimo, Heikki Keränen and Heikki Ailisto,* ‒Implementing TouchMe Paradigm with a Mobile Phone‖, ACM International Conference Proceeding Series; Vol. 121.

[3] Keränen, H., Pohjanheimo, L., Ailisto, H. (2005) Tag Manager: a Mobile Phone Platform for Physical Selection Services in International conference on Pervasive Services (ICPS 2005). Santorini, Greece. pp 405-412.

[4] Synchronized Multimedia Integration Language (SMIL 2.0), W3C Recommendation 07 August 2001 http://www.w3.org/TR/smil20/ .

[5] Java 2 Platform, Micro Edition (J2ME). http://java.sun.com/j2me/ .

[6] M. Johns and G. Marsden ‒*Mobile Interaction Design*‖, Wiley and Sons Ltd 2006, pg s178-182.

[7] ‒Openwave *Phone Simulator*‖ http://developer.openwave.com/dvl/tools_and_sdk/phone_simulator/ .

[8] European ATM Security Team, ―*European ATM Security Team*‖, Diebold, Incorporated 2006, http://www.diebold.com/rd/whitepapers/atmfraud&security.pdf

[9] A. Jain, R. Bolle, and S. Pankati, ‒*Biometrics: personal identification in networked society*‖, Kluwer Academic Publishers, 1998.

[10] J. Chirillo and S. Blaul, ‒*Implementing Biometric Security*‖, Wiley & Sons, 2003.

[11] S. Hoque, M.C. Fairhurst, F. Deravi, W.G.J. Howells, ‒*On the Feasibility of Generating Biometric Encryption Keys*‖ IEE Electronics Letters, 41(6), 309-311, 2005.

[12] Cellan-Jones, R., *London starts digital cash trial* in Technology correspondent, BBC News Online, http://news.bbc.co.uk/1/hi/technology/7117213.stm.2007: UK.

[13] Blythe, P.T. *Improving public transport ticketing through smart cards*. in Proceedings of the Institution of Civil Engineers: Municipal Engineer. 2004.

[14] New Barclaycard is touch-and-pay in BBC News,http://news.bbc.co.uk/go/pr/fr/-/1/hi/business/6945991.stm.2007.