Volume 4, Issue 3, March 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Overview of ATM Security Using Biometric Technology

Jaspreet Kaur
Computer Science and Engineering
SGGSWU, Fatehgarh Sahib, Punjab India

Sheenam Malhotra
Computer Science and Engineering
SGGSWU, Fatehgarh Sahib, Punjab,India

ABSTRACT-- ATM i.e. Automated Teller Machine is most commonly used commercial application by people for their money transactions. Over the last thirty years people are largely using and have been depend on automated teller machine(ATM). Today ATM transactions are not much secure so there is need of security in ATM transactions. Security of customer account is not guaranteed by the PIN (Personal Identification Number). As PIN can be share with others. The fingerprints of every person are unique and cannot be shared with others. This paper combines the biometric recognition technology with PIN to identify the customer more accurately. The nominee fingerprints and family member fingerprints are used to access the ATM machine in case of emergency when actual card holder unable to do the transactions. Most of times the recognition of fingerprints and passwords are restricted to 3.This proposal will solve the security problem and enhance the ATM security.

Keywords-- ATM system, Security, Finger Print Recognition, Biometric Verification, PIN.

I. INTRODUCTION

An automated teller machine was first introduced in 1960 by City Bank of New York on trial basis. The concept of this machine was for customer to pay useful (utility) bills and get a receipt without a teller **[1].**

Traditional banking systems are undergoing advancements very fastly for example the self service banking system has got great extent popularization with 24 hours high quality service for customer **[2].**The banking operation system provides the cash to customer through Automated Teller Machine at anywhere anytime. ATM is a computerized telecommunication device that enables the clients to perform the financial transactions like deposit, transfers, balance enquiries, mini statement and withdrawal etc without any need for a cashier or human clerk**.** There are two types of ATM: first one is a simple one which is used for cash withdrawal and to receive a receipt of account balance and second one is complex which is used for deposits and money transfer. The first one ATM is most widely and frequently used by people **[3].** Now a days, crimes at ATMs have been extensively increasing. In ATM, identification of people is done with the help of PIN number which is confidential. In such cases there is possibility of hacking passwords and personal information is more and some time it is difficult to remember the PIN number. The security of customer account is not guaranteed by PIN. Suppose by mistake if the card of customer is lost and the password stolen, then the criminal draw all the money in the shortest time. Many people are unlikely to memorize the PIN. So there is need of security in ATM transactions. The PIN is the 4 digit number given to all ATM card holders. The PIN numbers are different from each others. The password is only way to identify the customer when they have the card and correct password. Once the password and ATM card is stolen by the culprit they can take all money from the account in the shortest time.

To enhance the security level the **Padmapriya V et.al** introduced new technology which use the fingerprint recognition system and nominee for the main user and GSM technology. Biometric technologies are a secure means of authentication because biometric data of every person are unique, cannot be shared, cannot be copied and cannot be lost. The fingerprint based identification is one of the most mature and well proven techniques. So the author uses the fingerprint for person identification. The fingerprints of the card holder and nominee will be stored in the database of the bank. When the card holder or nominee wants to access the ATM machine they will have to enter the PIN and enroll the fingerprint. The fingerprint is checked by the bankers and matched with the stored database of the card holder. To enhance the security and authentication of the customer account, the concept of biometric feature such as fingerprint of customer is used along with the PIN is proposed since biometric fingerprints of every person is unique and unchangeable and it will provide more authentication than the PIN[6].

II. Literature Survey:-

EXISTING ATM SYSTEM

ATM is most widely used by people for transactions such as cash withdrawal, money transfers, balance inquiry, mini statements etc. The banking systems provide the PIN number to ATM card holder which has account in bank. The PIN (Personal Identification Number) is important to ATM and the only way to provide the security to ATM. A PIN is a 4 digit number which is generated by bank. PIN is easily remembered and is also changeable by user. As the PIN strength is decreased but there are chances of tracking the codes. The PINs are 4 digit numbers and has range from 0000-9999 resulting in 10000 possible numbers. An attacker would need to guess an average of 5000 times to get the correct PIN. The number of entering the password is restricted to 3 only. In the existing system firstly the user inserts his card and the

PIN number. If the PIN number is correct, then the system allows the user to perform the transactions. If the PIN is not correct then system will again ask to user for PIN and it allows maximum of three times to enter the PIN **[3].**

Duvey Anurag Anand et.al also proposed a system which provides security to the ATM transactions that uses the Dyna-pass (Dynamic Password). In this system the user accesses his account using debit card through ATM machine with the help of PIN. Then ATM machine reads this card and check the PIN with bank server through dedicated network. Bank server now connects to SMS center with any password called the Dynamic Password i.e. Dynamic Password. Then using mobile phone network SMS center send the password to Base Transceiver System (BTS). BTS then send it to user's cell phone. Now finally users get this dynamic password and enter this password to ATM machine. Then ATM machine again confirms this dynamic password with bank server and then responds to Banking Institute [7].

In this paper the **Duvey Anurag Anand et.al** also proposed third party authentication in which three or four persons registers with their mobile numbers through debit card. In case of emergency these registered people can do transactions when the actual user is unable to do transactions. User can fix their limit also for per day transactions [7].

The **Duvey Anurag Anand** also proposed biometric based ATM transaction system which is based on biometric data i.e. fingerprint recognition, iris recognition, face recognition etc. In this system biometric data is used along with PIN number and if biometric data of user is matched with stored biometric data then user will allow to do the transactions otherwise exit from the system[7].

BIOMETRIC IN ATM

Biometrics comes from the Greek language and is derived from words bio (life) and metric (to measure). Biometric are automated methods of recognizing a person based on physiological or behavioral characteristics of a person. Physiological information means)- information related to humans shape of body like fingerprint recognition ,face recognition, iris recognition, hand geometry, DNA, palm print etc. Behavioral information includes information related to the behavior of the person like signature and voice. Biometric technologies are a secure means of authentication because biometric data of every person is unique cannot be shared, cannot be copied and cannot be lost. With the help of biometric data it is possible to identify the person more accurately. Biometric recognition system is widely used for various applications which are as under:-

1. Commercial applications such as building access, computer system, ATM etc.
2. Government applications such as personal id, driver license, passport etc.
3. Forensic applications such as criminal investigation, terrorist identifications etc**[8].**

When developing recognition system which is based on biometric feature there are some points which must be considered as follows:**[8].**

1. Universality:- Every human being has those characteristics.
2. Distinctiveness:-Every two persons have different fingerprint impressions.
3. Permanence:- The biometric characteristics of every human does not change over a time.
4. Collect ability:- The biometric characteristics can be easily collected and measured.

In this paper **Ravi Kumar et.al** proposed the concept of fingerprint recognition along with the PIN in ATM to make the ATM and ATM transactions more secure. Fingerprints of every person are unique and can't be changed through the whole life. Using fingerprints the users will be more relieved that their account can't be accessed by others and it will maintain the security level **[3].** Every account has two passwords that is PIN Number and fingerprints of card holder. The nominee fingerprints and family member fingerprints are also used in case of emergency when actual card holder are unable to do the transactions. The money transactions are limited for the nominee i.e. they will not be able to withdraw more than certain amount on the same day. This system will provide the more security to banks as well as ATM terminals.

Patterns

The three basic patterns of fingerprint ridges are the arch, loop and whorl.

- *Arch:* The ridges enter from one side of the finger, rise in the center form an arc, and then exit the other side of the finger.
- *Loop:* The ridges enter from one side of a finger, form a curve and then exit on that same side.
- *Whorl:* Ridges forms circularly around a central point on the finger or field that is defined as the tangential vector of the fingerprint ridges curves is disclosed**[4].**

PROBLEMS IN ATM

Types of ATM Frauds:-

1. *Skimming Attack:-* This is the most popular act in ATM transactions. In this skimmer (card swipe device) reads the information on ATM card. These devices resemble with hand held credit card scanner. When it is removing from the ATM, skimmer allows the download of personal data belonging to everyone who used it to swipe an ATM card. A single skimmer can continue to use information from more than 200 ATM cards before being reused.
2. *Card Trapping:-* In this a device is placed directly over or into the ATM card reader slot. In this case a card is physically captured by the trapping device inside the ATM. When the user leaves the ATM without their card, the card is retrieved by the thieves.
3. *Pin Cracking:-* This is a harmful function that is used to allow customer to select their PIN's online. In this an attacker discovers the PIN codes. For example those entered by customers while withdrawing cash from an

ATM providing they have access to the online PIN verification facility. A bank insider could use an existing hardware security module to know the encrypted PIN codes.

4. *Phishing Attack:-* Phishing scams are designed to the user to provide the card number and PIN for their bank card. In this an attacker uses e-mail representing them as a bank and claiming that user account information is incomplete or that the user needs to update their account information to prevent the account from closed. The user is asked to click on a fraud link and follow the directions provided. The link is fraudulent. The site directs the user to input sensitive information such as card numbers and PIN's. The information is collected by the thieves and used to create the duplicate cards.
5. *ATM Malware:-* This attack required an insider such as an ATM technician who has a key to the machine to place the malware on the ATM. After this the attacker could insert a control card into machine card reader that act as the malware and give them control of machine through a custom interface and the ATM's keypad. Malware captures magnetic stripe data and PIN codes from the private memory space of transaction processing application installed on a ATM.
6. *ATM Hacking:-* In this attacker use sophisticated programming technique to break into website which reside on a financial institution network. They can access bank's system to locate the ATM database and collect card information which used later to make a clone card. Most of ATM hackings are due to the use of non-secure ATM machines.
7. *Physical Attack:-* ATM physical attacks are attempted on the safe inside the ATM through mechanical mean with intention of breaking the safe to collect the cash money. Robbery can also be done when ATM are being serviced **[1].**

III. CONCLUSION

ATM provides financial services to people in many countries. Existing ATM's machines are based on PIN (Personal Identification Number) which is not highly secure as a means of authentication. So there is need of privacy or security. Fingerprint Biometric feature is used for providing such security. Fingerprint scanning gain acceptance as a reliable identification and verification process. The system takes advantage of using biometric database of individual as a password along with PIN (Personal Identification Number).The security features are enhanced largely for the stability and reliability of customer recognition.

REFERENCES

1. Mohammed Lawan Ahmed "*Use Of Biometrics to tackle ATM fraud,*" International Conference on Business and Economics Research, IACSIT Press, Kuala Lumpur, Malaysia, Vol. 1, pp.: 331-335, 2011.

2. Yang Yun, Mi Jia "*ATM terminal design is based on fingerprint recognition,*" IEEE, 2nd International Conference on Computer Engineering and Technology, pp.: 92-95, 2010.

3. RaviKumar Sowmya, Vaidyanathan Sandhya, Thamotharan B. "*A new business model for ATM transactions security using fingerprint recognition,*" International Journal of Engineering and Technology(IJET), ISSN: 0975-4024, Vol. 5, pp.: 2041-2047, Issue No. 3, Jun-Jul 2013.

4. Devi CHSN Sirisha, Patil Maya "*Security System For ATM Terminal By Using Biometric Technology and GSM*," Global Journal of Advanced Engineering Technologies (GJAET), ISSN: 2277-6370, Vol. 11, pp.: 124-127, Issue No. 3, Year 2012.

5. Indi Trupti S, Raut Suhas D"*Person Identification based On Multi-biometric Characterstics,* " IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology(ICECCN), pp.: 45-52, Tirunelveli, 25-28 March 2013.

6. Padmapriya V, Prakasam S. "*Enhancing ATM Security Using Fingerprint and GSM Technology,*" International Journal of Computer Application (IJCA), ISSN: 0975-8887, Vol. 80, pp: 43-46, Issue No. 16, October 2013.

7. Duvey Anurag Anand, Goyal Dinesh, Hemrajani Dr. Naveen " *A Reliable ATM Protocol and Comparative Analysis on Various Parameters with other ATM Protocols*," International Jouranl of Communication and Computer Technologies (IJCCT), ISSN: 2278-9723, Vol. 01, pp.: 192-197, Issue No. 56, 06 Aug 2013.

8. Sudiro Sunny Arief, VOINE Michel PANDA, Kusuma Tb. Maulana "*Simple Fingerprint Minuitiae Extraction Algorithm Using Crossing Number On Valley Structure*," IEEE, pp.:41-44, 2007.