Biometric Fingerprint ATM for More Secured ATM Transactions

Ansiya Mohammed Ali

***Abstract*— The transactions of money play an important role in the present society. ATMs and Credit cards are mainly used for transactions. ATM machine uses ATM Card and PIN (Personal Identification Number) as authentication mechanisms. Today intruders produce duplicate ATM card and make fraudulent transactions by fixing ATM Card scanners in ATM Machine to obtain encrypted data from ATM Card. So the authentication provided by card and PIN is not so secure. The fingerprints of customers can be used as a password instead traditional PIN to overcome this disadvantage. Fingerprints of each human being are unique and unchangeable. Hence it provides more security and authentication than the current systems.**

***Index Terms*— ATM, PIN, Biometric, Fingerprint**

I. INTRODUCTION

An Automated Teller Machine (ATM) is a computerized telecommunications device. It allows the clients of any financial institution to perform financial transactions like withdrawal, mini statement, transfers and deposit etc. without the need for a cashier. ATMs are of two types: first, a simple ATM for cash withdrawal and to receive a receipt on account's balance and second, a complex unit, for deposits and money transfer. Commonly people use the first type of ATM.

A customer uses an ATM card along with the PIN provided by the respective financial institution to perform a transaction. Crimes at ATMs are increasing day by day. The security provided by PIN for the customer's account is not guaranteed. The less educated people in rural area can't able to memorize and recognize PIN.

In this paper, the authentication of ATM using biometric fingerprint technology is used. Biometrics is the automatic identification of a person based on his physiological/ behavioral characteristics. The biometrics is of different types such as face recognition, fingerprint matching, iris recognition etc. Each and every human being has a unique biometric fingerprint. So it enhances the security and authentication of the customer's account than S PIN.

II. TYPES OF ATM FRAUDS

A. Skimming Attack

This is the most popular attack in ATM transaction. In this attack, the attacker uses a card swipe device called skimmer to read the information on ATM card. This device resemble a hand-held credit card scanner and are often fixed firmly in close nearness to or over top of an ATM's factory-installed card reader. When removed from the ATM, a skimmer allows the download of personal data belonging to everyone who used it to swipe an ATM card. A single skimmer can retain information from than 200 ATM cards before being re-used.

B. Card Trapping

This attack involves placing a device directly in to the ATM card reader slot. In this case, the trapping device inside the ATM physically captured the card. The card is retrieved by the thieves when the user leaves the ATM without their card. After trapping a card, the criminals have to withdraw the whole device in order to trap another one.

C. PIN Cracking

PIN cracking attack deals with how the processing system used by banks is open to abuse. This attack targets the translate function in switches - an abuse function that allow customers to select their PINs online. The flaws provide a means for an attacker to discover PIN codes. In order to reveal the encrypted PIN codes a bank insider could use an existing Hardware Security Module (HSM). This attack also allows an insider of a third-party switching provider could attack a bank outside of his territory. Unfortunately, proposals to counter such attacks are almost non-existent other than a few suggestions. For example, maintaining the secrecy (and integrity) of some data elements related to PIN processing (that are considered security insensitive according to current banking standards) such as the 'decimalization table' and 'PIN Verification Values (PVVs)/Offsets' has been emphasized.

D. Phishing Attack

Phishing scams are designed to persuade the user to provide their username and PIN of their bank account. Typically, an attacker sends a false email representing them as a bank and claiming that to prevent the user account being closed, the user have to update their account information. The user is then asked to click on a link and follow the directions provided. The link is absolutely fraudulent and it directs the user to a site set up by the attacker which exactly looks like the user's bank account. The information collected by the attacker is used to create fraudulent cards. Some variants of phishing attacks are Spear Phish attacks and Rock Phish attacks. Using the extracted information, the attacker can also go onto the online account of the victim and perform various online transactions such as withdrawal, transfer etc.

E. ATM Malware

Malware attack requires an insider such as an ATM technician. Using a key he places the malware on the ATM. Once the malware is placed, the attacker inserts a control card into the machine's card reader to activate the malware. The attackers can control the machine through a custom interface and the ATM's keypad. The malware captures magnetic stripe data and PIN codes from the private memory space of transaction-processing applications installed on a compromised ATM. The malware

Manuscript received January 30, 2015.

Ansiya Mohammed Ali, Computer Science& Engineering, M. G. University, Pathanamthitta, India, 8893485396,.

allows attacker to take over the ATM machine to steal data such as PINs and using it they can withdraw cash.

F. ATM Hacking

With the help of sophisticated programming techniques the websites which resides on a financial institution's network can be hacked by an attacker. Using this, he can access the bank's systems to locate the ATM database and hence collect card information which can be used later to create a clone card. Hacking is also commonly used to describe attacks against card processors and other components of the transaction processing network. Most of the ATM hackings are due to the use of non-secure ATM software.

G. Physical Attack

Physical ATM attacks focused on the safe inside the ATM. This attack tries to collect the cash inside the safe through mechanical or thermal means. Physical attacks are of different types such as ram raids, explosive attacks, cutting etc. When ATMs are being serviced, robbery can also take place. Staffs can be held up as they are carrying money to or from an ATM, or when the ATM safe is open and cash cartridge is replaced. A wide variety of physical and mechanical factors can affect attacks to the safe. Some of them are the following.

- The certification level of the safe (UL 291 Level 1 is recommended as a minimum for ATMs placed in unsecured, unmonitored locations).
- To detect physical attacks on the safe alarms and sensors are used
- Ink stain technologies may ruin bank notes.

III. Existing ATM System

ATMs are mainly used for transactions such as cash withdrawal, money transfer and payment of telephone bills and electricity bills. The working of the existing system is depicted in the below figure.

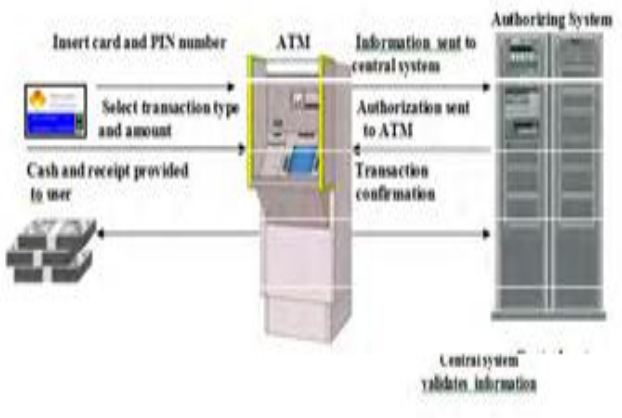

Figure 1- Existing ATM System

Personal Identification Number (PIN) provides security in current ATM system. PIN is a four digit number and is generated by the respective financial institution. A user can change his/ her PIN. But, today as the code tracking is increased, the PIN strength is decreased. n the existing system the user has to insert the card and the PIN number in the ATM system. The system allows for transaction only if the PIN is correct. Else, the system asks for PIN again and a maximum of three times is allowed.

IV. Proposed System

A. Why Fingerprint

Biometric characteristics are of different types such as fingerprint, hand geometry, retina, iris, ear, voice and face. Each of these characteristics has its own advantages and disadvantages. Hence the selection among the biometrics depends on the requirements and authentication of the application.

Fingerprint technology uses unique features of the fingerprint to identify or verify the identity of individuals. Among other biometric characteristics finger scan technology is most deployed. It is used in a wide variety of applications ranging from physical access and logical access. Each and every human have unique fingerprint characteristics and patterns. A Fingerprint pattern consists of lines and spaces. These lines are referred to as ridges and the spaces between these ridges are called valleys. For verification and authorization these ridges and valleys are matched. The unique fingerprint traits are referred as “minutiae” and comparisons are made on these traits. A typical live scan produces 40 “minutiae”. Some of the reasons for the selection are the following:

- Reliable: Fingerprints are reliable since every human being has a unique fingerprint. Not even twins have the same fingerprint.
- Universality: Majority of the population in the world have fingerprints. So fingerprint is universal in nature.
- Permanent: Fingerprints are permanent in nature. Over the course of time their characteristics do not change. They are formed in the fetal stage and it remains structurally unchanged.
- Storage: Small amount of storage is generally required for fingerprints.
- Accuracy: fingerprints are more accurate when compared to other biometrics.
- Inexpensive: The acquisition of fingerprints, its operations and maintenance are relatively inexpensive in nature.

Biometric characteristic	Universality	Unicity	Persistence	Colectability	Performance	Acceptability	Circumvention
Face	high	low	medium	high	low	high	low
Fingerprint	medium	high	high	medium	high	medium	high
Hand Geometry	medium	medium	medium	high	medium	medium	medium
Iris	high	high	high	medium	high	low	high
Retinal Scan	high	high	medium	low	high	low	high
Signature	low	low	low	high	low	high	low
Voice	medium	low	low	medium	low	high	low
Thermogram	high	high	low	high	medium	high	high

Table 1-Comparison of Biometrics Characteristics

B. Proposed System’s Strategy

Fingerprints can be used as passwords in ATM instead of the traditional PIN. Fingerprint recognition provides more accuracy and secrecy than PIN. Each and Every account maintains two passwords, i.e., two fingerprints. The account holder’s fingerprint is the primary one and the fingerprint of the nominee’s or a close family member is the reference fingerprint. The motive behind the introduction of two

passwords is to provide access to the account even if he/she is in an urgent situation and is in need of money, or when he/she has met with an accident, or has injuries on finger tips, and then the nominee can access the account. The nominee will be given a controlled access to the account. This proposed system is an advantage for both banks and customers in terms of security.

C. Procedure

The proposed system's steps are as follows.
STEP 1: Insertion of ATM Card by the user.
STEP 2: Input fingerprint on the scan pad (Primary or Reference print)
STEP 3: Fingerprint verification
STEP 4: If Valid
STEP 5: Execute Transaction
ELSE RETRY (GOTO STEP 2 Max.3 times)
STEP 6: Terminate

D. Design

With the help of UML tools the design is supported. It represents how the user interacts with the proposed system. The use case diagram of ATM system which is used only for cash withdrawals and report inquiries is depicted in the below figure.

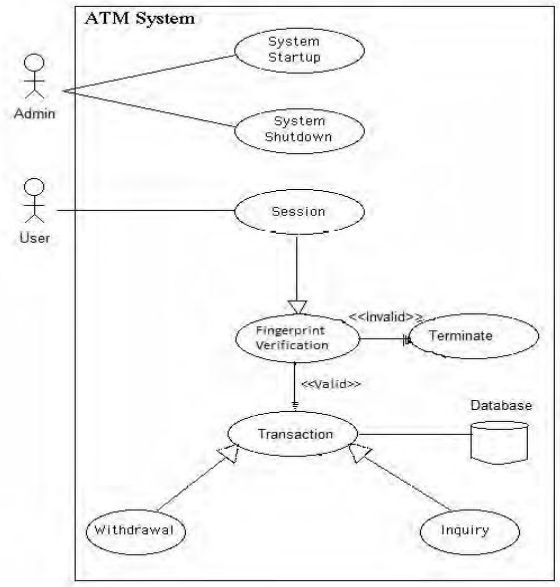

Figure 2- Use Case Diagram

Use case diagram represents the interaction between the customer and the system. Admin controls the proper functioning of ATM machine; User performs the transaction process such as withdrawal, inquiry etc and the Database requests and permits valid transactions.

E. System Design

A generic biometric system is shown in the below figure. It consists of five sub systems. They are data collection, transmission, signal processing, decision and data storage. Each of them is explained below.

Data Collection:- Data collection is the beginning of the biometric authentication system. The behavioral or physiological characteristic of the individuals is gathered. The presenting character of the individual is to be measured to a sensor.

Transmission:- The data gathered during data collection is then transmitted for further processing. To conserve bandwidth and storage space the gathered data is compressed before transmission.

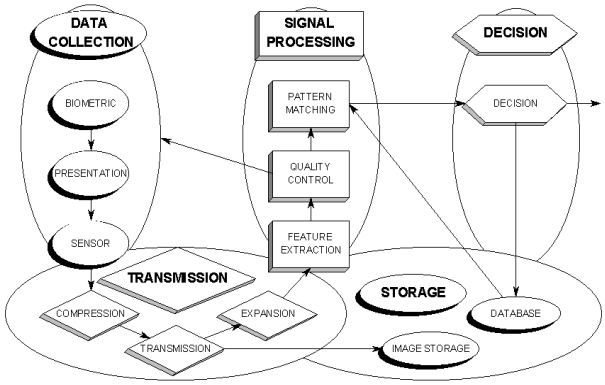

Figure 3- A Generic Biometric System

Signal Processing:- This subsystem consists of two phases. The first phase is the feature extraction and the second one is quality control. Feature extraction is a non-reversible compression. It ensures that the biometric image can't be reconstructed from the extracted features. Quality control verifies whether the signal received from data collection is of high quality or not.

Decision:- This is the actual part of the system. It determines whether a match has been made or not. It compares the sample traits received against a database of templates. An accept/reject decision is made based on the comparison results. This system policy determines how closely the data collected must match the data in the database before it is either accepted or rejected.

Storage:- The last sub system is the actual storage of the data collected in a database. This is done automatically at the time of registration.

V. CONCLUSION

ATMs have become more important to the society. There are millions of money transactions that happen in a single day through ATM. There are many frauds that occur in ATM, mainly due to PIN. Biometrics offers greater security and convenience than traditional methods of personal recognition. So, the proposed system of biometric fingerprint ATM enhances security on money transactions and has also made ATMs an easier access for the less educated. This method when fully deployed will not only increase the authentication, but will also help in the implementation of complex ATMs (performs deposits and money transfer), as this system provides increased security. This card less ATM machines is useful for rural masses because it never ask for passwords or any other kind of numbers. Due to the unique method of authentication, the entire operational cost, time, efforts of both banks as well as service user will be reduced. Biometric tokens are the safest means of preventing ATM frauds.

ACKNOWLEDGEMENT

I would like to extend my gratitude to the reference authors, review committee and my guide Ms. Veena Ramachandran L

REFERENCES

[1] S. Ramakrishnan, Sowmya Rravikumar, Sandhya Vaidyanathan, B. Thamotharan, (2013), A New Business Model For ATM Transaction Security Using Fingerprint Recognition, ISSN : 0975-4024, Vol. 5 No 3, Jun-Jul 2013

[2] Misra, D. K., Dr. Tripathi, S. P., Singh, A., (2012), Fingerprint Image Enhancement, Thinning and Matching, International Journal of Emerging Trends & Technology in Computer Science (ISSN 2278-6856), Volume 1, Issue 2.

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

[4] Feng, J.,(2008),Combining minutiae descriptors for fingerprint matching, Pattern Recognition 41, 342 – 352.

[5] Jain, A.K., Prabhakar, S., Hong, L., (1999), A multichannel approach to fingerprint classification, IEEE Trans. Pattern Anal. Mach. Intell. 21 (4),348–359.

[6] FVC2002, Second international fingerprint verification competition, _http://bias.csr.unibo.it/fvc2002/_. IJETR/03/1306