Smart ATM Pin Recovery and Secured ATM Transactions based on Fingerprint Identification

Aditya M Ramesh[1], Sindhuja H[1], C K Vanamala[2]

[1]*Dept. of ISE, The National Institute of Engineering, Mysuru*
[2]*Associate Professor, Dept. of ISE, The National Institute of Engineering, Mysuru*

Abstract - *Cryptography and Biometrics are two efficient and powerful technologies to appreciate high proven information security. Biometric authentication verifies a user's identity using biometric traits. However, a biometric authentication fails to shield the user's biometric template stored during a database, because it is at risk of various attacks. This system is sort of a bio-cryptosystem that mixes cryptography and biometrics together to beat the difficulties of those technologies. This project work aims at exploring the system to secure ATM pins and passwords with the fingerprint data specified only the legitimate user can access the pins and passwords by providing the valid fingerprint.*

In ATM machines the user is identified by inserting an ATM card and authentication is provided by the customer entering a PIN. The PIN provided by the customer is compared with the recorded reference PIN within the bank Server .If the customer forgets the PIN after 3 trials ATM cards are blocked, to reactivate he needs to attend the bank and do the formalities which could be a time consuming job. So fingerprint biometric is introduced to cut back this sort of error.

Key Words: **Fingerprint, ATM, PIN, Biometrics.**

1. INTRODUCTION

Reliable information protection and identity management mechanisms are required within today's era of cyber-crime. Cryptography is the technique of securing information and communications through use of codes. PIN based verification generally done in machine transactions. Enhancing this security, user authentication process is a vital activity. The foremost important problems include shoulder-surfing attacks, replay attacks, card cloning, and PIN sharing.

In today's digital era, a personal has multiple ATM pins and passwords for his or her multiple accounts. A common person tends to write down or store it in his phone's notepad or in a smartcard because it is difficult to memorize multiple pins and passwords. This could be easily compromised. With the recent advances in technology there is a requirement to create a system that Securely stores multiple pins and passwords and also the user could easily retrieve it whenever needed, within seconds. This research work aims to change the system to secure ATM pins and passwords with user's fingerprint data such that only the real user can access the pins and passwords by providing the valid fingerprint which is stored within the database. Experiments were conducted on fingerprint databases to check the performance of the proposed system.

2. OVERVIEW

Cryptography is a technique to exchange messages between one user with another user or to secure communication between them, by encrypting the message to be safe from a third party because issued with a key that is not owned by the third party. Encryption is a process of converting plain text into cipher text. Decryption is a process of converting the encrypted data into its original form. It is generally a reverse process of encryption.

A cryptographic attack is a method for overcoming the protection of a cryptographic system by finding a weakness in a code, cipher, cryptographic protocol or key management scheme. This process is additionally called "Cryptanalysis". The attacks like if another person takes cash from the cardholder's account, then it violates the authentication that the protection must run to the customer's account. Here in this system authentication is completed by fingerprint identification.

ADO.NET is used to speak between software applications and databases. It is a platform which is employed for developing software applications like browser based, desktop applications, mobile applications.
.NET framework consists of various APIs, languages and libraries which helps to form various software applications.

Visual Studio is an Integrated Development Environment(IDE) developed by Microsoft to develop GUI(Graphical User Interface), Web applications, web apps, mobile apps, cloud, and web services, etc. It provides support for 36 different programming languages. It is available for Windows in addition to macOS.

MySqlServer is an open source database. It comprises many classes. MySQL is written in C and C++. Its SQL parser is written in yacc, but it uses a home-brewed lexical analyzer. MySQL works on many system platforms. The MySQL server software itself and also the client libraries use dual licensing distribution. They are offered under GPL version 2, or a proprietary license.

3. PROPOSED SYSTEM

The objective of proposing this technique is to avoid time consumption. Usually the user inserts an ATM card and enters the identification number for transactions. If a user enters the inaccurate PIN then the user will be given two more attempts to enter the correct one. If the user fails to enter a legitimate PIN after three attempts, the card will block and thus the user must visit the bank to reactivate the ATM card which is time consuming. So the subsequent are the objectives of this proposed system,

- To avoid the user to go to the bank and do the formalities to reactivate his/her ATM card.
- To activate the ATM card of the user at the ATM centre itself with the help of finger print of the user.

3.1 Activity Diagram

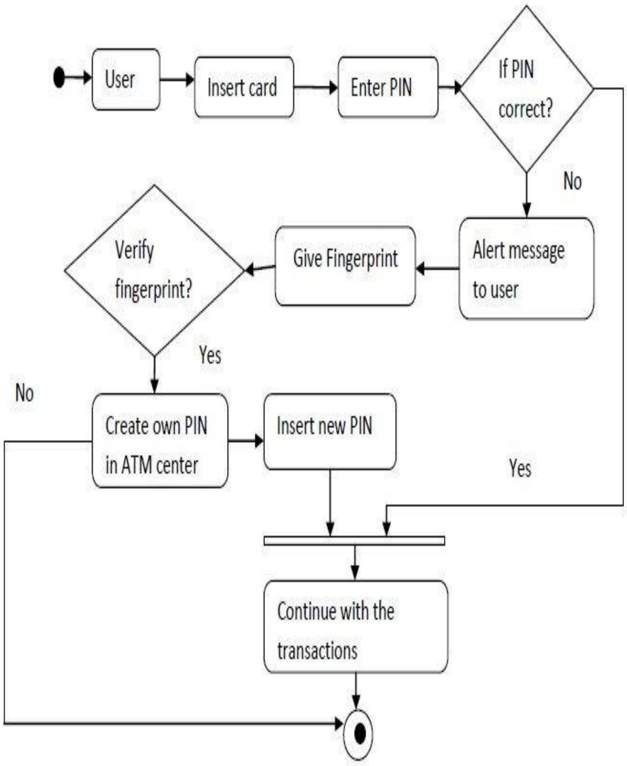

Fig -1: Activity Diagram of the Proposed System

The overall flowchart of the proposed system,

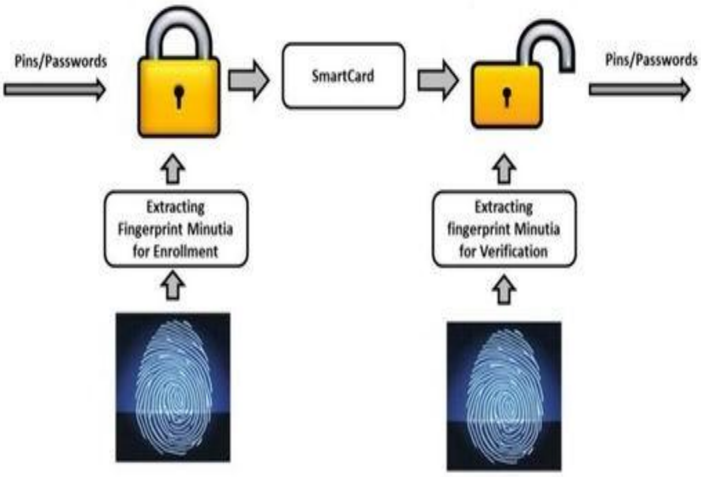
Pins/Passwords
SmartCard
Pins/Passwords
Extracting Fingerprint Minutia for Enrollment
Extracting fingerprint Minutia for Verification

Fig - 2: Flowchart of the Proposed System

When the user swipes the smart card , in case invalid attempts, then by verifying fingerprints the PIN is shared. The fingerprint reference given during transactions is verified with fingerprint reference given during enrollment.

4. IMPLEMENTATION

This proposed system is used to make easier bank transactions. Here the ATM machine is installed and can perform all bank related transactions so that no need to visit the bank.

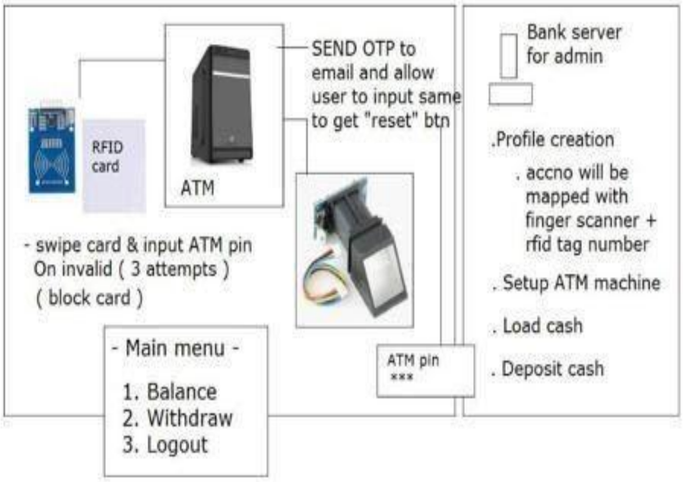
RFID card
ATM
SEND OTP to email and allow user to input same to get "reset" btn
Bank server for admin
.Profile creation
. accno will be mapped with finger scanner + rfid tag number
. Setup ATM machine
. Load cash
. Deposit cash
- swipe card & input ATM pin On invalid (3 attempts) (block card)
- Main menu -
1. Balance
2. Withdraw
3. Logout
ATM pin ***

Fig -3: Description of the System

The following are the actors considered in this implementation:

1. Admin
2. ATM Registration Staff
3. Account Holder/User

1. Admin

In this module, the works done are initially login through ID/password. Then banks are added and can view those. Adding customer details to bank accounts and if there are multiple accounts it maps customer's details. Admin can deposit an amount to a particular customer account. Admin sends identification number to the customer through Email ID using SMTP concept. Also Admin approves to ATM Machine Registration. Then loads cash to the ATM machine, views the service request from the customer.

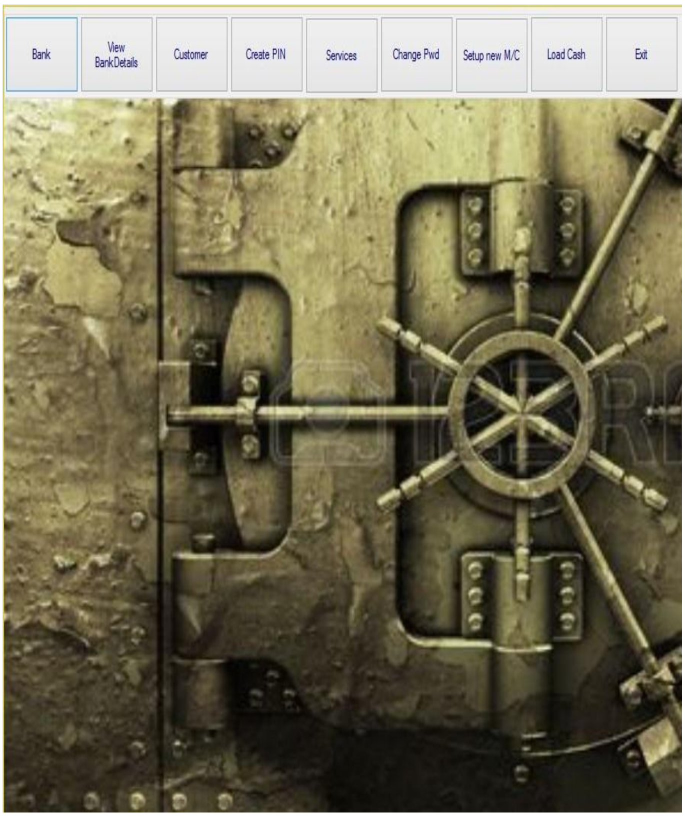

Fig - 4: Admin Panel

2. ATM Registration Staff

The security of ATM transactions relies mostly on the integrity of the secure cryptoprocessor: the ATM often uses general commodity components that sometimes are not considered to be "trusted systems". So sensitive data must be prevented from fraud. To prevent encryption is done which is a cryptographic method.

To install an ATM machine, firstly the bank basic details should be given with ID. Then the registration process is sent to the admin. Once the admin approves ATM setup/Machine registration then the customer can use the ATM machine.

3. Account Holder/User

When the customer swipe card and enters the PIN number, the system verifies PIN with card number registered, if valid then the customer home navigates to a different page where it displays multiple accounts bank names, there customer should choose required bank. There the user can check balance, withdraw, view withdraw amount, view deposit, transfer amount, view amount transfer details.

If the registered number and entered PIN are invalid, the machine gives three attempts to enter valid PIN. After three invalid attempts the card will be blocked. Then the user is asked to swipe through the fingerprint scanner, if it is the correct one then the PIN number is shared through registered Email where he can login and enter the right PIN. Also he can change PIN number in the ATM machine.

5. CONCLUSION

ATM authentication using PIN entry during transactions results in cryptographic attacks. In this system we proposed the Secured PIN based authentication using fingerprint and OTP based authentication service to beat the attacks. From the experiments carried out in this system can be used in a real time environment and also it provides the power to vary the PIN in the ATM machine itself. This technique will be future enhanced to multiple bank accounts by mapping to their accounts.

REFERENCES

[1] Fingershield ATM – ATM Security System using Fingerprint Authentication, Christiawan; Bayu Aji Sahar; Azel Fayyad Rahardian; Elvayandri Muchtar 2018 International Symposium on Electronics and Smart Devices (ISESD)

[2] Securing ATM pins and passwords using Fingerprint based Fuzzy Vault System, Sweedle Machado; Prajyoti D'silva; Snehal D'mello; Supriya Solaskar; Priya Chaudhari 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)

[3] www.seminarsonly.com

[4] www.geeksforgeeks.org

[5] wikipedia.org

[6] itstillworks.com