International Journal of Research in Engineering, Science and Management
Volume-1, Issue-11, November-2018
www.ijresm.com | ISSN (Online): 2581-5792

Cardless ATM System Using Fingerprint and IVRS

Arjun Nambiar[1], Akshay More[2], Rohit Sharma[3], Prajakta Patil[4], Manisha Bharati[5]
[1,2,3,4]*UG Student, Dept. of Computer Engineering, Indira College of Engineering and Management, Pune, India*
[5]*Professor, Dept. of Computer Engineering, Indira College of Engineering and Management, Pune, India*

***Abstract*: Hackers can steal PINs, but they cannot do the same with biometrics such as Fingerprint. Real finger has many properties that cannot be presented by a fake replica. In a fingerprint secured ATM, customers only need to rest their finger on scanner surface and identity gets verified instantly. Basically user has to enroll fingerprint in ATM system and enter the usual PIN, and select from which bank they want to transact. So it means that the user can access multiple banks on a single system without using multiple cards.**

An IVR System is provided for the visually challenged people for enabling better guidance to them. The Braille Keyboard will guide the visually challenged people to access the ATM with the guidance of the IVR System. This will help increase the accessibility and usability of the ATM system.

***Keywords*: ATM, Biometrics-Fingerprint Authentication, IVR System, PIN, Braille Keyboard**

1. Introduction

ATM is a system which enables humans to have banking transactions without any other human interference. But with traditional methods of Card and PINs it is easier for hackers to get a hold of genuine user's identity as they can use card skimming to get the data on the magnetic strip of the card and with the help of cameras PINs can be stolen. Also the data on magnetic strip of card can be easily destroyed by either magnetic fields or if the card gets damaged. Also if a user has multiple bank accounts, he/she will have multiple ATM cards in addition to their credit cards. This leads to having different PINs for each card which makes it difficult for the user to remember. Moreover it takes time to replace lost or stolen cards. Hence it can be concluded that cards are a weak entity for authentication in ATMs.

Another idea was to use mobile as means of authorization by sending OTP to the mobile and using that OTP as a PIN for your transactions. But it is not possible to get reception to every network provider in every area i.e. the mobile won't be able to receive text messages for the OTP. Also it's mandatory for the user to always carry a mobile phone with them. In case of emergencies or if the mobile gets stolen it's not possible to carry out transactions in ATM. Hence we use biometric authentication in our system.

As we know biometrics means your physical features of your body which can act as ID for data. This includes fingerprint, iris, voice, facial features, etc. Table I shows the comparative study of biometric platform for authorization. It shows that the best device is to use a fingerprint sensor because it is low cost device, gives high accuracy and acceptability is fairly high. Hence we use fingerprint as an authentication medium in ATM.

Table 1
Device comparison

Biometric technology	Cost	Acceptability	Accuracy
Fingerprint	Low	High	High
Facial Recognition	Medium	High	Medium
Voice	Medium	High	Medium
Iris	High	Low	High

Hence in our ATM system the user only has to place finger on the sensor, enter the PIN and carry out the further transactions. Once authorized the user has to select bank from which the transaction should take place. This provides the multiple banks in single touch feature for the system. Also our system will provide a way for the visually challenged people to access the ATM with ease. This works using an IVR (Interactive Voice Response) System for which the challenged people can give inputs using Braille keyboard. For every input given to the system, a new set of voice instructions are given to the user. The Braille keyboard works as a way for selection of different options and also a way to enter the PIN.

2. Problem statement

In current scenario, ATM system has Card and Pin code as security, enabling the other person other than owner to access account very easily i.e. using card skimming and other techniques the data on the card and PIN can be easily hacked which concludes that the traditional ATM system is not fully secured. Also having multiple cards means to remember PIN codes for each card and if a card is stolen then it takes time to fetch a new card. Also the limitation for visually challenged people to access the ATM facility is not fulfilled. So to avoid this and to access multiple bank accounts in a single touch we propose "Cardless ATM System using Fingerprint and IVRS".

3. Literature review

The Table 2, shows a survey of different proposed ATM systems.

Table 2
Literature review

S. No.	Title	Advantages	Limitations
1	One Touch Multi-banking Transaction ATM System using Biometric and GSM Authentication	Card less Transactions	If ATM card is lost or stolen, wait till a new ATM card is handed out to you. Mobile is always required.
2	MFCC and VQ Voice Recognition Based ATM Security.	All the bank accounts are managed in a single finger touch thus no need to carry multiple cards and remember their passwords.	Cough, colds or overall health condition of the speaker may provide variations in speaker's voice quality
3	A Self Banking Biometric Machine with Fake Detection Applied to Fingerprint and Iris along with GSM Technology for OTP	Using the two most stable physiological biometrics as ameans of identification of an individual has made the system more reliable.	Mobile is always required.
4	Introduction of capacitive fingerprint sensor packaging technology	The capacitive sensor is integrated on a single chip by more than more than 100 thousand capacitors, epoxy resin package, coating on the surface, or mount ceramic or glass cover in surface.	The accuracy ofvisual inspection is low, and the speed of performance testing is slow. How to improve the speed and accuracy of detection is not known.
5	Comparative Analysis and Review of Interactive Voice Response Systems	Interactive Voice Response (IVR) systems can be considered as one of the most recent fruitful outcome of mobile technology. This system can be used to get a wide range of information in different fields.	A comprehensive work could be done on security and privacy to make IVR systems more reliable and dependable.
6	Prospective solution to bank card system Using fingerprint	The system deals with only one account of the customer but a customer may have more than one account in various banks	The same fingerprint should detect all the associated accounts of the customer in different banks and he/she must be able to transact in every account one at a time
7	Face Detection based ATM Security System using Embedded Linux Platform	The smart ATM security system based on embedded Linux platform is suggested here. Security is provided by detecting the face of the person in a systematic way.	If the face is not detected properly, it warns the user to adjust him/her properly to detect the face. Still the face is not detected properly the system will lock the door of the ATM cabin for security purpose
8	A Novel Approach to Fingerprint Identification Using Method of Sectorization.	The usage of Artificial Intelligence will also enhance our method and increase the solution accuracy.	The analysis of minutiae number in different sectors would enable us to dynamically divide the image into areas.

If from this we identified the Cardless ATM System using Fingerprint. In this system we are going to improve the performance of the system, like the One Time Password system used has a drawback like if there is no range to the mobile the OTP is not received which is not feasible. In this project we are going to use a Minutiae Algorithm to match the fingerprint 3 received during the operation with the database, it leads to quick performance compared to direct matching algorithm, also the IVR System and Braille Keyboard for better guidance for the visually challenged people.

4. Proposed system

The proposed system will replace the traditional system of only magnetic strip based card and PIN. For this the user has to enroll his/her fingerprint with their respective banks first. Only once for each user fingerprints are saved in a secured database connected to bank server and also the consortium. Once the fingerprints are stored, then the user will be allocated a single unique PIN for all accounts. He/she can then access the ATM using fingerprint and PIN. This will work as the user is able to select from which bank they should complete the transaction. The default IVRS is enabled for the visually challenged people, but others can disable it with a single touch. This will make the ATM system easily accessible to the challenged people. Hence it will remove the drawbacks of existing system i.e. Card skimming, stolen cards, PIN stealing, lost cards, etc.

A. Objectives of proposed system

- To provide card less transactions in ATM system.
- To provide biometric security through fingerprint authentication in ATM system.
- To provide access to multiple account in a single touch.
- To provide high security based transactions.
- To provide a Braille keyboard for the visually challenged people.
- IVR system for better guidance to user.

B. Key Features/Algorithms

C. Minutiae based extraction in fingerprint recognition

It is the most widely use technique of fingerprint representation and its configuration is highly distinctive. It is better compared to other correlation based systems and the template size is smaller in minutiae based fingerprint representation. Here two fingerprints match if their minutiae points match. The minutiae technique is classified into two categories:

- Binarised Fingerprint Images
- Gray Scale Fingerprint Images

D. Interactive Voice Response System

IVRS is an application which stores pre-recorded messages that supplies information as required or desired by the organization. It can also take inputs from the user. The IVR system is responsible for the audio alerts. When the customer presses any key, this speaker confirms the pressing of key by a reply. It also assures that the keypad is working.

E. Braille Keyboard

It is a system of writing and printing for blind or visually impaired people, in which varied arrangements of raised dots representing letters and numerals are identified by touch. A single character is made up of six dot positions. Dots are arranged in rectangle with two columns of three dots each.

5. Architecture

This section will give us an idea about the system architecture and the flow of the system.

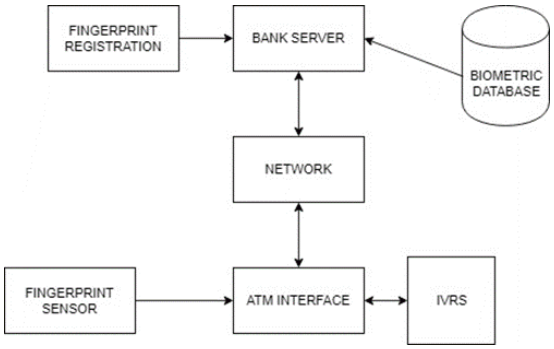

Fig. 1. System architecture

Here in Fig 1. We can clearly see that the ATM is connected to the bank server where the biometrics is stored from the registration workstation. An IVRS is available in each and every ATM system. The IVRS will give voice instructions to the user via speakers and the user can give input using the Braille keyboard. The database is on web based service hence it will available to all bank accounts and ATMs.

Here the fingerprint sensor is the main part of the whole system hence it should provide accurate results in less time, security and compatibility to different features of a fingerprint. Also the algorithm used for matching the fingerprints should be optimized and accurate. There are mainly two types of algorithms used:

- Direct Matching
- Minutiae based Matching

Here we use Minutiae based matching because it is faster and more accurate than Direct matching technique-- where the images are directly overlaid and matched which takes a lot of time.

In Minutiae based algorithm each location of minutiae is calculated and stored as a function of F(x, y, Θ) where (x,y) is the location on template and Θ is the angle it makes with baseline.

Table 3
Fingerprint sensors

S. No.	Device	Cost	Security
1	Optical	Low	Low
2	Ultrasonic	High	High
3	Capacitive	Low-Medium	High

In Table 3, we can see that capacitive sensors provide high security and will detect fake fingerprints. The cost is also less compared to Ultrasonic sensors hence we use it.

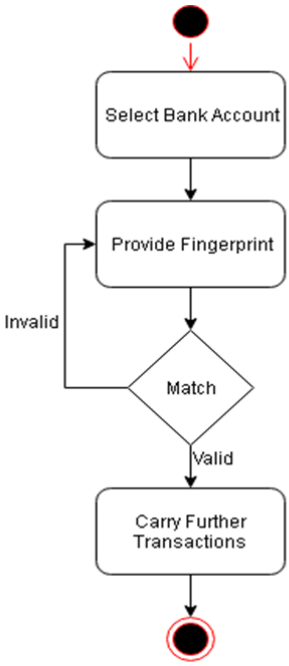

Fig. 2. Activity diagram for bank selection

In Fig 2. We can clearly see that the bank selection process will come before the fingerprint enrolment in ATM as it makes it faster to fetch the fingerprint.

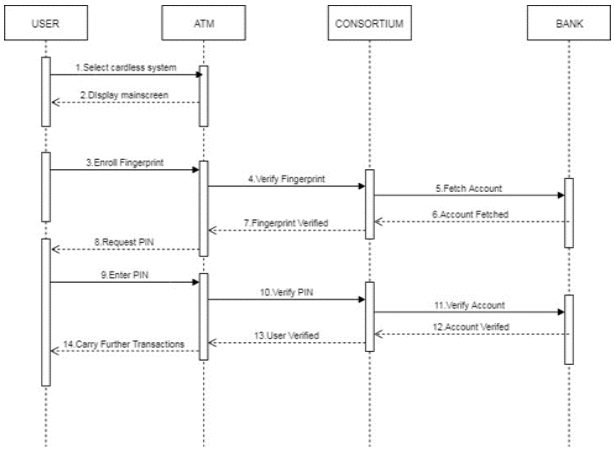

Fig. 3. Sequence diagram for authorization

Then the fingerprint is provided to the sensor and if it matches the user can carry out further transactions. If it doesn't

match it will give three chances to enroll fingerprint and verify it. The following figure will show the sequence of how the flow of the system goes from enrolling fingerprint to carrying out transactions.

As we have an option to either select card or fingerprint, here the first option for the user is to select the cardless system, then the authorization happens with the consortium and the bank.

6. Functional requirements

A. Authorization

1) Functional requirement 1

- Description: The ATM has to check if the entered card is a valid fingerprint
- Input: Customer enrolls his/her fingerprint
- Processing: Check if it is a valid fingerprint. It will be valid if the fingerprint can be read properly and is linked to a bank account.
- Output: Display message.

2) Functional requirement 2

- Description: If the fingerprint is valid, the ATM should ask for PIN.
- Input: Customer enters 4-digit PIN.
- Processing: Check if it is a valid PIN linked to a bank account.
- Output: Accept or reject authorization from bank.

3) Functional requirement 3

- Description: Log the details.
- Input: Details from fingerprint.
- Processing: Log the number.
- Output: Update to log file

4) Functional requirement 4

- Description: If the fingerprint and PIN are verified, the authorization process is finished.
- Input: The ATM gets authorization.
- Processing: Finishing authorization
- Output: Start transaction dialog.

5) Functional requirement 5

- Description: If a fingerprint was entered more than three times and the PIN was wrong each time for 3 times, a message will be displayed that the customer should call the Bank.
- Input: Entering a wrong PIN for the fourth time in succession.
- Processing: Initiate authorization process.
- Output: Display the message that the customer should call the bank.

B. IVRS

1) Functional requirement 1

- Description: The ATM will announce voice based commands to user.
- Input: Customer selects the desired input from Braille keyboard
- Processing: Select the function linked to the keyboard.
- Output: Next command starts or banking transaction initiates.

2) Functional requirement 2

- Description: The IVRS shuts down if customer chooses it.
- Input: Customer selects to shut IVR down for that transaction.
- Processing: Shut down the IVRS.
- Output: No voice from speakers.

7. Advantages and applications

1. Card less Transactions.
2. More Security.
3. Access to multiple accounts in a single touch.
4. No need to carry multiple cards and works even if there is no mobile phone in ATM.
5. The problems like fraud, unlawful entry, cards getting stolen or duplicated are prevented.
6. All other ATM functionalities such as
   - PIN change
   - Transfer Money
   - Enquiry Balance
   - Mini Statement

8. Conclusion and future scope

The proposed card less ATM system has advantages such as saves manufacturing cost of cards and overcomes drawbacks of the traditional system like carrying multiple cards, losing of card, fraud calls related to ATM card, etc. and provides high security by using authentication like fingerprint therefore making it easy to use multiple bank account transaction in a single touch. Also it enables visually challenged people to use ATM properly by usage of Braille keyboard and IVR system.

Performance of system can be increased by increasing efficiency of fingerprint algorithm. Biometric authentication can be used for payments in merchant shops instead of traditional card swiping for payments.

References

[1] A. K Jain, K Nanda Kumar, and A Nagar, “Biometric Template Security,” 2008, ACM.

[2] E. D. Dimaunahan, "Raspberry Pi Based Automated Teller Machine Security for the DSWD Biometric System Using Fingerprint Recognition with Fast- Fourier Transform Image Enhancement and Multi-Stage Minutia Extraction," ACM, p. 6, 2017.

[3] Zhao Yingding. Research on fingerprint identification technology based on embedded application Beijing: Institute of computing technology, Chinese Academy of Sciences, 2005.
[4] A. A. Azeta, C. K. Ayo, A. A. Atayero and N. A. Ikhu-Omoregbe. "A Framework For Intelligent Voice-Enabled E-Education Systems", Turkish Online Journal of Distance Education-TOJDE July 2009 vol: 10 No 3, Article 10. pp. 155- 168.
[5] The Biometric Consortium, "Introduction to Biometrics", (http://www.biometrics.org), 2006.
[6] K. Kadir, M. Kamaruddin, H. Nasir& S. Safie, "4th International Conference on Engineering Technology and Technopreneuship (ICE2T)", 2014, p. 335
[7] Lee. R., Comber. B., Abraham. J., Wagner. M., Lennard. C., Spindler. X., Roux. C., „Supporting fingerprint identification assessments using a skin stretch model – A preliminary study", Forensic Science International, Volume 272, March 2017, pp. 41 – 49.
[8] S. P. Balwir, K. Katole, R. D. Thakare, N. S. Panchbudhe, P. K. Balwir, "Secured ATM transaction system using micro-controller", International Journal of Advanced Research in computer science and software engineering,Vol.4, Issue 4, April 2014.
[9] M. Raj and Anitha Julian, "Design and Implementation of Antitheft ATM Machine using Embedded Systems," International Conference on Circuit, Power and Computing Technologies [ICCPCT], pp. 1-5, 2015.