

A Review Approach on Cardless ATM Access with Biometric Security Using IOT

^[1]Mr.J.A Patel Ms. ^[2] Darade Bhavna ^[3] Ms.Baglane Ruchita ^[4] Ms.Bodke Punam
^[5]Ms.BodkeArchana

Sandip Foundation,Nashik.

Abstract: This paper describes a method of implementing two way authentications. The first one is biometric thumb verification is done and in second is 4 digit pin verification. If it's wrong then we find that the user is fake and LCD displays the THEFT message and also the buzzer is ON. If it is right then we find that the user is not fake and the LCD displays ENTER THE KEY message, in this case buzzer is OFF.

Keywords: PIC18F458, thumb scanner, power supply, Wi-Fi, crystal oscillator, LCD, Keypad.

I. INTRODUCTION

Biometric ATM are used in many applications like a Banking Security, to reduced ATM fraud and criminal activities. Biometric ATM is a combination of Multifactor Authentication = Card + PIN + Biometrics. By using biometric technology, It is more helpful to senior citizens because it is difficult to carry card with him. Biometrics ATM's will eliminate financial burden place on customers for insurance and maintenance of ATM card. To implement the proposed security for ATM terminals with the use of fingerprint recognition, we use the different hardware and software platform. These ATM's will also reduce complaints related to ATM cards at the customer cares of bank on bank staff. And customer that uses ATM.

II. BACKGROUND: DIFFERENT BIOMETRICS TECHNIQUES.

1. Facial Recognition:

Face Recognition is considered a biometric identification. It has an ability to distinguish among individuals appearance. With face recognition technology, a digital high definition (HD) camera is used to analyze the characteristics such width of nose, etc. This has found limited success because it includes acquisition environment and facial characteristics changes that result in error in matching.

2. Fingerprint Scan:

The fingerprint scan technology is used to produce the best identification of users. Fingerprint follow methods from matching. Fingerprint characteristics such as whorls, cups and ridge. These characteristics are very useful to

Identify unauthorized access. There are some weakness in fingerprint scanning as lower quality fingerprints.

3. Hand Geometry:

Every person has an unique hand geometry and the shape and size of the hand does not change till the person dies. Biometrics of hand technology produce the results of measurement of the hand such as size of hand, length of finger, thickness shape, size, etc. It is generally used where fingerprint is considered as intrusive

4. Voice recognition:

In Voice Recognition, voice of the user is analyzed with the stored voice prints. Voice identification is not reliable as it contains the noise disturbances within it.

5. Retinal Scan:

This technology is based on the blood vessels located on the eye. Blood vessels can absorb infrared energy easily than the surrounding tissues. It is very expensive. Retina scan consists of both iris-scan and fingerprinting.

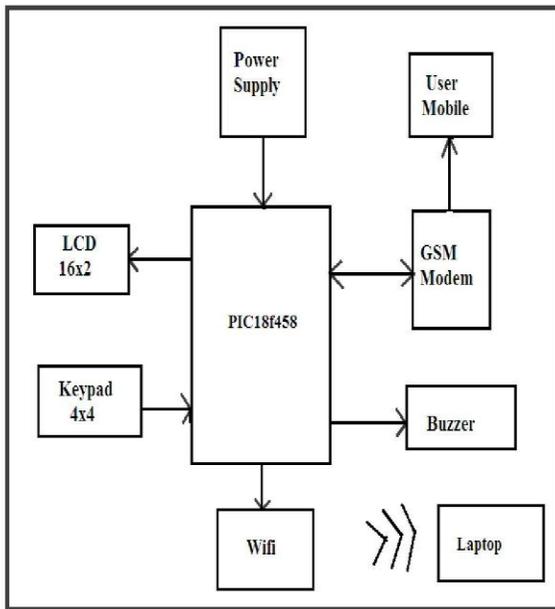
6. Iris Scan:

Every Iris is a unique structure of a complex pattern. Once the eye is stable and the image is captured when the camera is focused. The iris scanning technology is acceptable by many users as it is not intrusive. First, depending upon the blackness existing in the image and second is the size of iris changes.

**International Journal of Engineering Research in Electronics and Communication
Engineering (IJERECE)
Vol 4, Issue 2, February 2017**

III. SYSTEM DEVELOPMENT

An ATM with Fingerprint scanner and GSM enable device. Stores the data account information, personal information,etc.



Firstly the user input is taken with the help of the thumb scanner. Then if the thumb is matched the user receives a 4 digit pin through GSM. In the next stage, if both are matched then the user information is displayed on the LCD that the user is valid and hence the further transactions can be made successfully.

If the fingerprint and the 4 digit pin do not match then the user is given 3 more chances to match the pin and the thumbprint. At the end if the thumb and the pin do not match the buzzer will turn On and the authorized user will get a message through GSM that a fake login to his/her account was made. In this way we find the fake users by using Biometric Thumb Scanner. It is very helpful to avoid ATM hacking.

IV. ADVANTAGES OF THUMB TECHNIQUE

1. It Provides a very strong authentication.
2. Biometric system replaces card system with physiological characteristics.
3. It is more helpful to senior citizens because it is difficult to carry and maintain card with him.
4. Due to biometric authentication no individual is able to access others accounts and hence hacking can be reduced.
5. Users never forget their YOB (Birth year) hence it can be used as 4 digit Pin.

VI. APPLICATIONS

1. It can be used for security.
2. Used in banking.
3. ATM fraud and criminal activities can be reduced or eliminate completely.
4. Enhance the use of ATM by banking customers.
5. It will eliminate financial burden place on customers for insurance and maintenance of ATM card.
6. It will also reduce complaints related to ATM cards in the bank will reduce.

VII. CONCLUSION

This cardless ATM if implemented will help to eliminate completely the problems associated with use of ATM card, then enhances efficiency in ATM usage, also reduces congestion in banking hall especially at the customer care section where complaints relating to ATM card and issuance and collection is always tendered. The system will use both PIN and biometric technology as access control. Hence guarantee maximum security of customer account access and transaction from such account.

VIII. FUTURE SCOPE

By Improving of DIP of scanned image using software the scanner device can be made accurate, instead of using higher in scanner so cost can be reduced. Transaction can be done at a very high level of security. Can be used where security is a major issue e.g. military.

**International Journal of Engineering Research in Electronics and Communication
Engineering (IJERECE)
Vol 4, Issue 2, February 2017**

IX.ACKNOWLEDGMENT

The Authors would like to Thank Asst.Prof.Jagdish Patel his help.This work was supported in part by Sandip Foundation(SITRC),Nashik(MS).

REFERENCES

- [1]Prof. Chandrakant.D.Patel, Prof. Sanket trivedi, Prof.Sanjay patel , "Biometric in IRIS Technology- A survey", International journal of scientific research publication, Vol-2,issue 1, jan-2012.
- [2]Z.Riha, V.Matyas, "Biometric Technology based authentication system ", Series- 2000-08. [3].M.gupta, "Biometric technology Research", /aunthetic/biometric.php.
- [4].J. Dhole., " persons by a diagnosis by statistics", November.2015.
- [5]Pennam Krishnamurthy and Madhusudhan Reddy,"ATM security by using Fringerprint Biometrics", Electronics Engg Volume 3.
- [6]Dileep Kamat and Yeoneung , "Introduction of Biometrics and Fingerprint tranctions technology",International Journal of ,March 2009.
- [7].S.Sivasubramaniam,"Online Transaction using Finger print scanner", International Journal.
- [8]H.Mahmoud and Shaikh,"techique for steganography in fingerprint images: Implementations.
- [9]G.S,"financial transaction without card "Mar.21 2015,US Patent.
- [10]S.N.S.W., "Financial transaction GSM based",Feb.2012.