ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

VF-ATM Machine: Accepts Finger Prints, Voice Pin and OTP Code

Harshal Deshpande, Bhagyoday Toke, Rajesh Dangat, Aditya Dabhade, Prof.P.P.Waghralkar

Department of Computer, PVPIT College of Enginerring, Savitribai Pule Pune University, India

ABSTRACT: A VF-ATM machine is an electronic device which facilitates banking transaction via an electronic device. This machine accepts biometric input credentials such as finger prints and Voice Pin for preceding the transaction. The VF-ATM machine also allows a particular person to open an account without going bank. The user of the machine can see list of all accounts which he/she holds in corresponding bank. The traditional ATM(s) requires user to carry card and pin number for preceding the transaction. If the user of the machine lost his card or forgets his pin he needs to follow hectic process of the bank to reissue the card and pin number. The VF-ATM solves this issue by providing biometric access for financial transaction. The VF-ATMs do not allow a user to open multiple accounts with different names whereas currently used ATMs do not put any audit of this kind. The VF-ATM is extremely secure and easy way for handling your financial transaction. Its features like biometric access, showing list of accounts and provision of opening account in an automated way makes it different.

KEYWORDS: ATM machine security, VF-ATM.

I. INTRODUCTION

This machine is particularly used to perform financial transactions without the need of human cashier or clerk or teller. This machine is available in two type the first type of machine helps the user to withdraw cash, check balances , create accounts whereas the other type of ATM helps for depositing cash , Paying utility bills. Currently installed ATM(s) make use of two things to authorize a particular user one is a Card and other is a PIN number associated with that card. User of the machine first inserts the card and then enters the Pin for any kind of transactions, providing single layer of security. This kind of authentication mechanism is not so reliable, prone to fraud and provides lower level of security. Hence the current developments of VF-ATMs make use of physical/ behavioral characteristics such as finger prints and voice of the user for authentication purpose. These kinds of VF-ATMs are getting popularity particularly in the field of forensic work, biometric locker and law enforcement. However, currently known VF- ATMs are not without limitations. Safety of bank customer fund in banking has always been a concern in currently known VF-ATMs. Moreover, it is very difficult to prevent another person from attaining and using a legitimate person's card in currently known ATMs.

The field of invention is related to Automatic Teller Machine. This electronic banking outlet helps the user to make the banking transaction process easy and automated. Since this machine does the entire task related to banking therefore the user of this machine must be an authorized user. The focus of the invention is related to this authentication process of ATM machine. The invention involves capturing the behavioral characteristics of the user such as finger prints and Voice for accessing the ATM machine. The finger print scanning creates a unique identification of the user by finding finger ridges and minutia points for a specific pattern. The voice pin recognition provides extra layer of security by capturing acoustic characteristics of the user. This pattern matching and pattern recognition system makes the process more secure.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

II. RELATED WORKS

In ordinary technique recognizable proof is done in light of ID cards and static 4 digit watchword. Though in our purposed framework, Bankers will gather the client fingerprints and portable number at the season of opening the records then just client will have the capacity to get to ATM machine. The essential advance of this venture is to confirm at present filtered unique mark with the finger impression which is enrolled in the bank amid the record opening time. In the event that the two fingerprints get coordinated, at that point a message will be conveyed to the client's portable which is the irregular 4 digit stick number to get to the record. For each exchange new stick numbers will be send to the client's portable along these lines there won't be settled stick number for each exchange. Subsequently, Pin number will differ amid every exchange [1].

We have built up the login security framework utilizing OTP that is scrambled with MD5 Hash, and the OTP is sent naturally to the enrolled client telephone cell number. The upside of this framework is the utilization of MD5 Hash to scramble an arrangement of Student ID, Phone Number, and Time stamp (date and hour of access). MD5 Hash makes comes about that never been the same with the beforehand created OTP. Contrasted with the OTP produced with Pseudo Random Number Generator (PNRG) may make similar codes. This setup time is sufficiently short contrasted with different applications, i.e. Facebook and Google that utilization 20 minutes to hold up the client enter in the OTP [2].

These days we perform the greater part of our bank exchanges and m-business utilizing advanced mobile phones and PDAs which comes convenient. It spares parcel of cash and time and managing an account made part simpler. In this exploration paper we have proposed a novel technique for consolidating mystery 4-digit individual file number and feistal strategy for encryption for improving the security to the following level. This is a basic yet a compelling measure to battle the diverse online record robberies and cheats to secure our m-trade exchanges [3].

Our work demonstrates that Commercial Off-the-Shelf (COTS) based multimodal unique mark and face biometric frameworks can accomplish preferable execution over unimodal COTS frameworks. Further, in the event that we consider relative execution picks up, an EER change of 1 percent will mean splitting of false acknowledge and false reject numbers when we have an exceptionally precise framework (e.g., initially having 2 percent EER). However, this 1 percent EER reduction may not mean a substantial change if the fundamental framework was less exact (e.g., initially having 5 percent EER), as it will prompt only 20 percent diminish in false acknowledge and false reject numbers [4].

Multimodal biometric frameworks combine the proof introduced by different biometric sources and ordinarily give better acknowledgment execution contrasted with frameworks in view of a solitary biometric methodology. Despite the fact that data combination in a multimodal framework can be performed at different levels, joining at the coordinating score level is the most widely recognized approach because of the straightforwardness in getting to and consolidating the scores produced by various matchers. In any case, explores likewise uncover that the min– max and z-score standardization methods are delicate to exceptions in the information, featuring the requirement for a hearty and effective standardization technique like the tanh standardization. It was likewise watched that multimodal frameworks using client particular weights perform better contrasted with frameworks that dole out a similar arrangement of weights to the different biometric qualities of all clients [5].

III. PROPOSED ARCHITECTURE

The foregoing objects of the present invention are accomplished and the problems and shortcomings associated with the prior art, techniques and approaches are overcome by the present invention as described below in the preferred embodiments.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

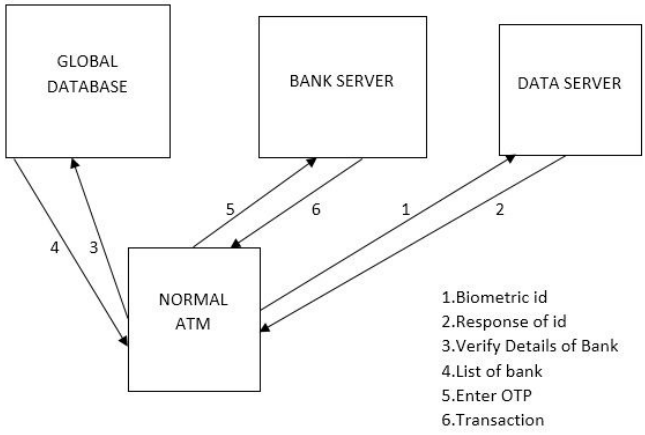

Fig.1. Block Diagram of proposed system

FIG. 1 shows overall flow of the VF-ATM system. The VF-ATM machine comprises of three servers: Global Banks Data Server 120, Bank Servers130 and Government Data Centers or Servers 140.In current context of the invention, The Bank's Global Data Center/Server 120 stores all the information required to open an account in the bank, information such as name, signature, father's name, mobile number, date of birth, e- mail address, postal address, alternative address, nominee name, date of birth, and the like. The VF-ATM machines110 accepts the input credentials from the user. For the purpose of opening an account the VF-ATM machine takes ID for the first time and then with the help of this ID all information of the user is fetched from the Government Data Centers/Servers. When the information gets fetched the VF-ATM machine asks the user to give finger prints and Voice. These finger prints and voice input credentials are associated with the ID and then stored into Global Data Center or Server for verification at the time of further transaction. After this an account number is auto generated and displayed over the screen of VF-ATM machine. Once the account has been opened the account holder can make use of Voice Pin and finger prints for any kind of financial transactions.

Fingerprint: As uniqueness and permanence of fingerprint recognition is higher than other biometric recognitions, so we mostly use fingerprint authentication system as a means of identification of a person. There are two critical points in a fingerprint i.e. core and delta. Fingerprint is recognized by an automatic pattern recognition system. For Fingerprint recognition, there are three types of fundamental stages.

Data Acquisition: In this stage, through user interface the fingerprint data is acquired. The image obtained is stored in database.

1) Feature extraction: In this stage, fingerprint features are extracted and then stored in database along with the details.

2) Matching: In this stage, the decision is made for a person to authenticate identity who intends to access the system Fingerprint images are acquired by pressing finger on flat surface of an electronic fingerprint sensor.

One Time Password (OTP): One Time Password (OTP) is utilized as an additional factor in multifactor authorization/authentication applications. There are two main approaches to OTP. In the first approach, called time-based OTP, the one-time password changes at frequent intervals (say, every two minutes).In the second approach, called event-based OTP, the one-time password is generated for every transaction or login from a different IP address.

Voice Recognition: The Fourier Transform is a tool that breaks a waveform (a function or signal) into an alternate representation, characterized by sine and cosines. The Fourier Transform shows that any waveform can be re-written as the sum of sinusoidal functions.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

IV. SYSTEM ALGORITHM

We propose an algorithm to describe the operation of the system.

a. Algorithm

- Algorithm for fingerprint authentication

Algorithm

```
def fingerPrintAuthentication(fingerprint):
    1.image preprocessing and feature extraction
    2.userRegistered=matched fingerprint with stored pattern
    3.If
      (userRegistered.userId)
        a.send OTP(userRegistered.userId)
    4.else:
        a.return "No such user"
```

- Algorithm for user login

```
def allowUserToLogin();
1. UserRegistered= fingerPrintAuthentication(fingerprint);
2. If (userregistered) then
    a. userAuthenticated:= voiceAuthentication(userRegistered.userId,otp)
    b. if(userAuthenticated) then
        i. do transactions
        ii. return
    c. Else
        iii. Show message "OTP does not match"
3. Else
    a. Show message "user not registered"
```

```
Algorithm voiceAuthentication(userId, otp)
        def voiceAuthentication(userId, otp):
```

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

b. Flow Chart

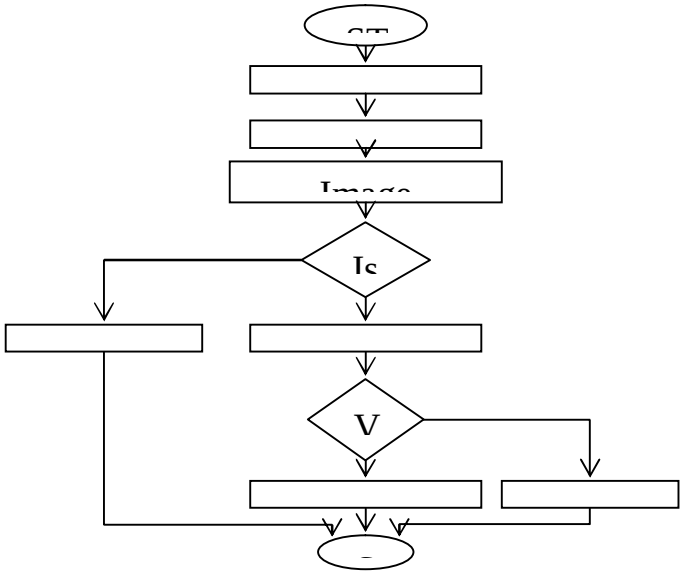

Fig 2 Flow of system operation

V. RESULT

The VF-ATM is extremely secure and easy way for handling your financial transaction. So it is very to hacker to access. This Machine helps to provide more security to ATM machine. This machine provides user's biometrics, OTP, Voice Reorganization security.

c. Hardware Model

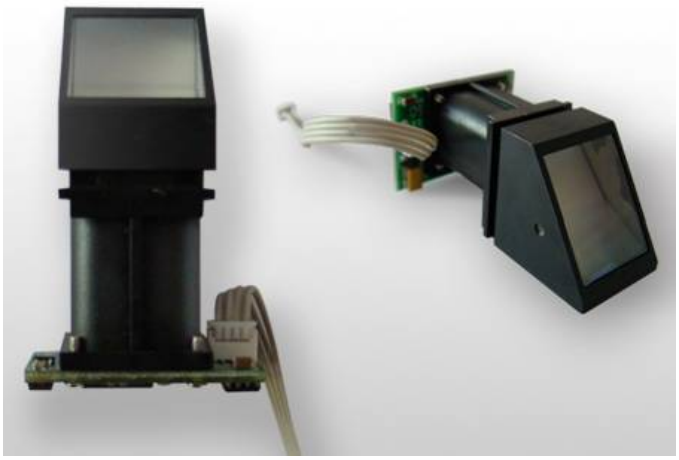

Fig.3. Authentication using Fingerprint

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

d. Web Page/Mobile App

Fig 4shows the login page of theVF-ATM Machine: Accepts Finger Prints, Voice Pin and OTP Code

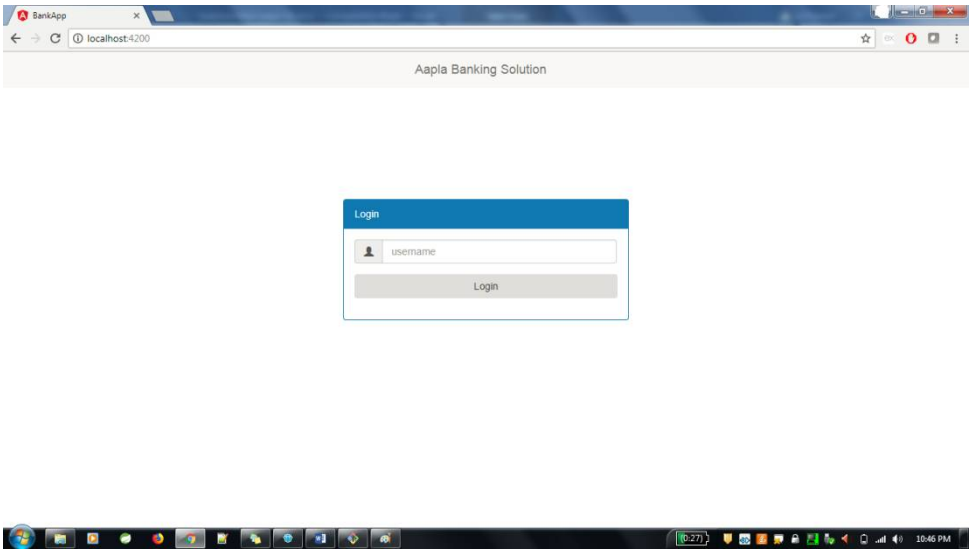

Fig 4: login page

VI. ANALYSIS

Parameters	Existing system	Proposed system
Speed (MHZ)		
RAM (MB)		
Architecture (bit)		
Operating voltage (volt)		
No. of GPIO		

VII. CONCLUSION

The machine capturing the behavioral characteristics of the user such as finger prints and Voice for accessing the ATM machine. The finger print scanning creates a unique identification of the user by finding finger ridges and minutia points for a specific pattern. The voice pin recognition provides extra layer of security by capturing acoustic characteristics of the user. This pattern matching and pattern recognition system makes the process more secure.

REFERENCES

[1] Jaydeep Shamdasani, Prof .P.N.Matte "ATM Client Authentication System Using Biometric Identifier & OTP" Int. Journal of Engineering Research and Applications www.ijera.com ISSN: 2248-9622, Vol. 4, Issue 4(Version 5), April 2014, pp.74-78
[2] Ki-Young Kim, "The Study on the authentication system based onOne-time password," Journal of the Information Security, vol. 17 no. 3,Jun. 2017.
[3] OTP Encryption Techniques in Mobiles for Authentication and Transaction Security International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 10, October 2016
[4] Snelick, R., Uludag, U., Mink, A., Indovina, M., Jain, A.: Large-scale evaluation of multi-modal biometric authentication using state-of-the-art systems. IEEE Trans. on Pattern Analysis and Machine Intelligence 27(3), 450–455 (2015).
[5] Jain, A., Nandakumar, K., Ross, A.: Score normalization in multimodal biometric systems.Pattern Recognition 38(12), 2270–2285 (2005)