ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

New Secured Architecture for Authentication in Banking Application

K.Senthil Kumar[1], Dr.S.Vijayaragavan[2]

P.G. Student, Department of Computer Science &Engineering,Paavai Engineering College,Nammakal, India[1]

Professor, Department of Computer Science &Engineering,Paavai Engineering College,Nammakal, India[2]

Abstract:ATM Machines uses ATM Card and user password as a access control mechanism. Today due to intruder's advancements & technology improvement it is possible to fix ATM Card scanners in ATM Machine to obtain encrypted data from ATM Card, which is again used to produce the duplicate ATM card and to make fraudulent transactions. Our proposed system going to use a Combination of Bio Metrics , Face Recognition & retina to authenticate the user in ATM Machine. This help to protect the users from fraudulent transaction. Our System reduces the usage of plastic which helps environment to avoid plastic wastes. Our proposed system will improve the security of ATM machine over existing systems.

Keywords:Bio metric based authentication system for banking application.

I. INTRODUCTION

Banking Sector started using Finger Print Based Authentication system to protect the user against ATM Card frauds, also it help users to access the accounts without remembering pins and no need to carry plastic ATM Cards. This technique will act a new path to introduce ATM Services to Rural & illiterate masses. Many Indian Banks already installed such ATMs as pilot projects to name a few Union bank of India launched this service in sivagangai district of Tamil Nadu under the name of Kisan ATM to provide ATM Services to Farmers. Dena Bank, Andra Bank, Corporation Bank and Indian Bank also introduced as a pilot project.

According to the study conducted by these banks they faced some problems in scanning finger prints accurately due to dirt, cuts and other physical changes in the pattern of the finger print recorded during the account creation process. The Finger Print is scanned at the time of creating account in bank and it is stored in bank database. The next time when user gives his impression in finger print scanner located in ATM, it will capture the finger image and compares with the stored finger print image of the user in database and if its matches then it will allow the user to access the account if it's not matches then it will issue a warning message to reenter the user name. The real problem comes here because we can't say every time the finger print is same to farmers due to cuts and dirt's. In our system, The combination of finger print along with retina scanning will solve the issues, The authentication process is three steps, Initially it will authenticate using finger print and if finger prints failed then it will ask for retina scan and finally it will perform face recognition using inbuilt camera located in ATM. Then based on the combination of matches in Finger print, retina and face recognition the system will authenticate the user. Our proposed system will use these three combinations to solve the problem of existing Finger Print Based ATMs.

II. OBJECTIVES

1. To study issues in Finger Print Based Authentication Technique in ATM
2. To propose a Module which help for simple operation of ATM with Secure Authentication using combination of Bio Metric Technologies?
3. Providing Suggestion with advantages and limitation of proposed model.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

III. LITERATURE REVIEW

A. International Reference

John Hall, Spokes Man, American Banker Association said customer should understand technologies provides greater benefit than using ATM Card and PIN System. Bill Spence, A Bio Metric Expert working with Campbell, California based Recognition System Inc said ATM Cards also act as debit cards and getting that wallet space is very important. However South American Companies where already started producing finger print based ATM and American banks started implementing this as a pilot project. Diebold Inc of North Conton, Ohio supplier these kind of finger print based ATM to banks in Chile. NCR Corp installed 400 finger based machines in Colombia Ban Care, for the use of coffee growers and to get them open accounts. The growers can use finger prints instead of cards for authentication.

B. What is identification?

Identification refers validating a particular user using a authentication system. The authentication system can be as simple as single password or higher end retina based authentication system to identify a particular user. Authentication is a program or process that confirms the service used by particular user belongs to them. Authentication using password is simple method and it's like saying computer "This is Example User and authenticate me using my credentials" and authentication using password is like computer looks at hand geometry and says "You are Example User and you are authenticated to access the service which is subscribed by you". The safer and secured method is finger based authentication because here authentication credentials is checked each time by computer using pre stored templates of user.

C. What is biometric Authentication?

Biometric is a Greek Words, Bio refers life and metric refers measuring some objects that have life. Biometric measures the characteristics of both physiological and behavioral. These characteristics are finger prints, Voice patterns, hand measurements, irises and others. These characteristics used to identify humans. These characteristics are connected to an individual user and cannot be forgotten stolen or shared or easily hacked like passwords. These characteristics can easily and uniquely identify a person by using personal biometrics and user no need to memorize the passwords or codes.

The two categories of biometric identifiers are physiological and behavioral characteristics. Physiological refers to the shaper of the body and include but at the same time not limited to finger prints, face recognition, DNA, Palm Print , hand geometry, iris recognition and odor/scent. Behavioral Characteristics are related to personal behavior of the person includes typing speed, gait, digital signature and voice. The traditional access control is based on tokens such as passport and knowledge based identification system such as password or PIN.

Today, The device will recognize the following biometric finger prints, hand geometry, retina and iris, voice, handwriting, blood vessels in the fingers and face authentication. If we combine multiple characteristics then we can design full and secured authentication system without need of plastic ATM Cards.

D. Finger Scan Technology

Finger Print technology is the initial bio metric sciences and uses unique features of the fingerprint to identify or verify the identity of individuals. Finger scan technology is most deployed technology among other bio metric characteristics, used in application ranging from physical access and logical access. Each and every human have unique characteristics and patterns. A Finger Print pattern or sample consists of lines and spaces. These lines are referred as ridges while the spaces between these ridges are called valleys. These ridges and valleys are matched for verification and authorization. These unique finger print traits are referred as "minutiae" and comparisons are made on these traits. The typical live scan produces 40 "minutiae". The federal Bureau of investigation has reported that no more than 8 common minutiae can be shared by two individuals [11].

There are five stages in finger scan verification and identification they are finger print image acquisition, image processing, and location of distinctive characteristics, template creation and template matching.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

A Scanning device takes a mathematical snapshot of user unique biological traits. This snap shot is saved in a finger print database as a minutia file. The major challenge with finger scanning system is image quality of a finger print. Image quality is measured in dots per inch (DPI) – More dots per inch means a higher resolution image. Lower DPI refers the finger print with as low as 350 DPI but the standard for forensic quality fingerprinting is images of 500 DPI [12]. Image scanning is biggest task finger scan developers since the quality of print differ from person to person and from finger to finger. In some cases it's not practically possible to have faints or difficult to acquire finger prints, due to wear or tear or physiological traits [11]. Using oils in the finger help to capture a better finger print. In cold weather, these oils naturally dry up. Pressing the scanning platen harder will also give better finger print quality.

Image processing is the process of converting the finger image into a usable format. These results in a series of thick black ridges contrasted to white valleys [13]. In this process image features are detected and enhanced for verification against the stored minutia file. Image enhancement is used to reduce the distortion of fingerprint caused by dirt, cuts, scars, sweat and dry skin [14]. The next stage in the finger process is to locate particular distinctive characteristics. The average finger print have good amount of information. This information stays for user life time. Finger print ridges and valleys form particular patterns such as swirl, loops and arches. Finger print have a core, a central point around which swirls, loops or arches are curved. These ridges and valleys are characterized by irregularities known as minutiae. The common types of minutiae are ridge endings and bifurcation. This is the point at which one ridges divides into two. A typical finger scan creates between 15 and 20 minutiae. Then template is created using that.

E. **Facial-Scan Technology**

A facial recognition will scan the human face and authenticate the user using pre stored images of the user. The facial scan technology comes in various forms such as software only solution that process images processed through existing camera to full-fledged acquisition and processing systems including camera , workstation and back end processor[15]. Facial Recognition Technology uses a digital camera to take image of the user and analyses the facial characteristics such as the distance between eyes, mouth or nose. These data's are stored in data base and used to compare with a subject standing before the camera. The facial recognition system is divided into two types. The first type is Controlled Scene where by the subject being tested is located in a known environment with a minimal amount of scene variation. In this method, the user will stand in front of the camera two feet from it. The system locates the user face and perform matches against the claimed identify or facial database. Sometimes the user need to verify more than once if user changes his position from the image stored on the facial database. The second type is Random Scene here the subject to be tested might appear anywhere within the camera scene.

Facial scan technology is based on the standard biometric sequence of image acquisition, image processing, distinctive characteristic location, template creation and matching [16].An Optimal image is captured using high resolution camera with moderate lighting and user directly facing a camera. The enrollment images define the facial characteristics to be used in all future verification. The issues in the image acquisition process include distance from user, angled acquisition and lighting. The distance from camera reduces facial size and this image resolution. Additionally user with darker skin tone is difficult to acquire. After image acquisition are worked out. The process of image processing takes place. Color images are normally reduced to a black and white and images cropped to emphasize facial characteristics. Images are normalized to account for orientation and distance. The main image can be enlarged or re oriented as long as a point between the eyes servers as a point of reference.

F. **Retinal Scan Technology.**

The Retina scan technology makes use of the user retina, which is nothing but surface on the back of the eye that processes light entering though subject. The blood vessel pattern is used in retina scan technology as authentication characteristics. The blood vessel at the retina provide unique pattern which is used to identify the user. Infra-Red Energy is absorbed faster by blood vessel in retina than by surrounding tissue, It used to illuminate the eye retina. Analysis of the enhanced retina blood vessel image then takes place to find the characteristic patterns. Retina scan devices are used mainly for physical access application and are usually used in environment which requires high degree of security authentication.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

Acquiring images using retina technology is difficult because retina is small and embedded, which require special hardware and software to scan and acquire images. The user position his eyes close to the unit embedded lens with the eye socket resting on the sight. To capture retinal image, the user must gaze directly into the lens and remain still, movement defeat the capturing process requires another attempt. Vascular pattern of retina is scanned using low intensity light source. The 360 degree circular scan of the area taking over 400 Readings in order to establish the blood vessel pattern. Then this is reduced to 192 reference points before being distilled into a digitized 96 byte template and stored in memory for subsequent verification process. The enrollment process is lengthy. The enrollment can take over 1 minute with some user not being able to be enrolled at all. After the image is captured then the software is used to compile unique features of the retinal blood vessel into a template.

IV. WORKING OF BIOMETRIC AUTHENTICATION

The bio metric devices works based on some human characteristics, such as finger prints or voice patterns. Authentication will provide unforgivable physical characteristics to authenticate users. The database of user contains a sample of user bio metric characteristics. During authentication the user is required to provide another sample of the users biometric characteristics. This is again matched with the one in database, and if two samples are same then user is allowed to access the service. Following Fig 1.shows the working of biometric authentication process[17].

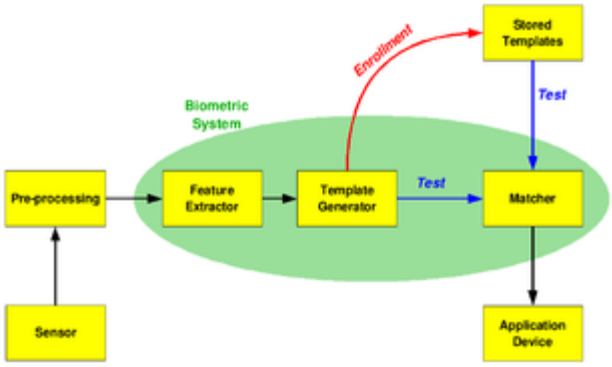

Fig 1.Working of Biometric Authentication.
Source: http://en.wikipedia.org/wiki/File:Biometric_system_diagram.png

V. DRAWBACKS OF EXISTING SYSTEMS

1. The card holder with PIN no becomes owner of the card without any additional verification which creates huge security issues.
2. The processing time of damaged card or older card is too high and sometimes it's not possible to access the account.
3. If card is missed then there is high possibility of misuse of card.
4. If card is stolen then it requires huge process to generate a new card for that particular user.
5. After 3 wrong password attempt the card will be blocked inside the ATM machine and bank should provide new Card to the ATM user which incurs additional charges to the bank.
6. The use of plastic cards is harmful to our environment.
7. If user have more than one account then user have to maintain multiple cards it's become trouble to remember all passwords.

VI. REQUIREMENT FOR PROPOSED SYSTEM

1. ATM Center Should have biometric device includes finger print scanner, retina scanner and camera to face recognition technology and optionally a numeric keypad.
2. Authentication is based on per transaction.
3. If User fail to authenticate more than 4 times then the system should block the account for that day for security purpose

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

4. If such blocks happens more than 5 times then the user account should blocked permanently and ask the user to regenerate the new authentication in home bank.

VII. PROPOSED SYSTEM

Our proposed System makes use of the Finger Print Scanning Technology, Retina Scanning Technology and Face Recognition Technology to authenticate the user. Our proposed System require user to generate the finger print sample, retina sample and face images at the time of creating account in bank. Then these data's are stored in authentication database. The user now uses the ATM machines without any cards.

The User can now enter the ATM Room and have to place his fingers in the finger print scanning device. Then the system will authenticate with samples stored in authentication database. If the accuracy is 98% with the sample stored in database then it will check for the facial recognition as additional measure and if its matches the finger print present in the authentication database now the user is authenticated inside the ATM and he can perform the single transaction using the authentication.

If the user finger print accuracy comes below 98% then additionally the user is requested to authenticate additionally in retina based scanner for security purpose. If its matches with pre stored sample then after completing the facial recognition the user are allowed to access the account for single transaction.

If both authentications fall below 90%, then authentication is failed and if the 3 consecutive authentications are failed then the system will block the user account and request the user to re generate all the details at the home bank.

VIII. ADVANTAGES OF PROPOSED SYSTEM

1. Provide 3 Step Strong Authentication
2. Our System replaces card system with physiological characteristics.
3. Hidden cost of ATM Card Management can be avoided.
4. It's ideal for rural masses
5. Account Holder may use another person which will have identification of same account
6. Useful for senior system because no need to carry cards and memorize passwords
7. Card Stolen problems and related call centers are not required which will reduce the cost of operation of bank.
8. Due to bio metric system no one is able to access the other systems.
9. User can change the authentication any time in home branch with few simple procedures.

IX. LIMITATION

1. The requirement of bio metric devices in ATM Machines will improve the cost of ATM Machine but it will balance in operation cost of the ATM Machine.
2. Every time, account holders should come to ATM to collect money
3. Due to three step authentication process timing is very high but it ensures absolute security to users.

X. FUTURE WORK

1. The special combination based algorithm can be designed so that, if accuracy of one authentication goes below acceptable percentage, based on algorithm, the ATM can calculate the average authentication values based on other two authentication acceptable values.
2. The Scanner Device can be made accurate by improving the DPI of scanned images using software instead of using higher end scanner which will reduce the cost of bio metric devices used in ATM.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

XI. CONCLUSION

Proposed model is designed for ATM users to perform various banking operation without the need to carry plastic ATM Cards and the same time , the security problems related to old card based ATM are solved using these techniques. These Techniques can be costlier while implementing because of higher production cost but in long run and when production increases automatically cost will come down and the operation cost of ATM will be reduced which is compensate the initial total cost of ownership. This card less ATM machines is useful for rural masses because it never ask for passwords or any other kind of numbers. Due to our unique method of authentication, the entire operational cost, time, efforts of both banks as well as service user will be reduced.

REFERENCES

1. KahateAtul, "User Authentication Mechanism", Cryptography and Network Security, pp.303-304, IIIrd Edition, McGraw - Hill Publications.
2. Biometric ATMs for rural India, "Weekly Insight for Technology Professionals", www. expresscomputeronline.com, Accessdate 16-Dec – 2011
3. Handbook of Biometrics. Springer. pp.1–22.ISBN 978-0-387-71040-2. http://www.springer.com/computer/image+processing/ book/978-1-4419-4375-0, access on 10-Dec-2011, 5.00pm
4. International References: http://www.rediff.com/money/2005/oct/11atm.htm, Access on 16- Dec- 2011, 11.00 am
5. Jain, A., Hong, L., &Pankanti, S. "Biometric Identification", Communications of the ACM, Vol no 43, pp. 91-98, 2000.
6. Jain, Anil K.; Ross, Arun. "Introduction to Biometrics", pp. 45-60, 2011
7. Krause Micki, Tipton Harold F., Handbook of Information Security Management (Imprint: Auerbach Publications) (Publisher: CRC Press LLC), ISBN: 0849399475, http://www.ccert.edu.cn/education/cissp/hism/ewtoc.html, data access on 13-Dec-2011, 3.50 pm
8. Laudon Kenneth, TraverCarol Guercio," E-Commerce Second Edition" , pp. 237-239, Pearson Education (Singapore), Pvt. Ltd.
9. ONeil Erin, Back to the future at your local ATM, http://banking.about.com/od/securityandsafety/a/biometricatms.htm, access on 16-Dec-2011 at 11.45 am
10. Pfleeger Charles P., Pfleeger ShariLacorence, Shah Deven N, Security in Computing, "User Authentication", pp. 257-258, IVth Edition, Pearson Publication, 2011.
11. Ibid.p. 50
12. Samir Nanvati,,Biometrics:Identity Verification in a Networked World, New York: Wiley and Sons, Inc, page 48, 2002
13. Ibid.p. 51
14. ZeenaMarchant, Biometrics: Fingerprint Authentication, SANS Reading Room,http://rr.sans.org/authentic/fingerprint.php
15. ManojGupta,Biometric Technologies Overview , SANS Reading Room, http://rr.sans.org/authentic/biometric2.php.
16. Samir Nanvati. (2002), Biometrics: Identity Verification in a Networked World , New York: Wiley and Sons, Inc, page 65
17. Pfleeger Charles P., Pfleeger ShariLacorence, Shah Deven N, "User Authentication",Securityin Computing, pp. 257-258, 2009