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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Biometrics: Cardless Secured Architecture for Authentication in ATM using IRIS Technology

Nachiket Sainis[1], Reena Saini[2]

Assistant Professor, Dept. of CSE, B.K.Birla Institute of Engineering &Technology, Pilani, Rajasthan, India[1]

Assistant Professor, Dept. of IT, B.K.Birla Institute of Engineering & Technology, Pilani, Rajasthan, India[2]

ABSTRACT: This paper discusses several Biometric scan technologies: finger-scan, facial-scan and retinal-scan and others. Retinal-scan& IRIStechnology is a relatively new entrant to thebiometricfield and offers significant promise. One of the continuing challengesforthe banking industry is to reduce the fraud and security issues. Here we are proposing cardless security architecture for ATM using IRIS. Our proposed system provide unique authentication technique to improve security of ATM machine over present system.

KEYWORDS: Biometrics, authentication, IRIS scan, ATM, Cardless secured architecture.

I. INTRODUCTION

In modern era people are very much sensible about security issues in banking applications, like we go to the ATM to withdraw money, so every time we need to carry ATM card for that purpose and need to remember password i.e. 4 digit ATM pin to authenticate successfully. But, now the technology has been changed and people don't want to carry ATM card and keep remembering password given by bankevery timeto withdraw money from ATM (Automated Teller Machine).

The word “biometrics” comes from the Greek language and is derived from the words bio (life) and metric (to measure). The biometrics technologies used to measure and analyze personal characteristics. These characteristics include fingerprints, voice patterns, hand measurements, irises and others, all used to identify human characteristics and to verify identity. These biometrics or characteristics are tightly connected to an individual and cannot be forgotten,shared, stolen or easily hacked. These characteristics can uniquely identify a person, replacing or supplementing traditional security.Personal biometrics cannot be easily stolen and an individual does not need to memorize passwords or codes. Since biometrics can better solve the problems of access control, fraud and theft. This paper will discuss the recent history of biometrics, benefits of biometrics over traditional authentication methods and how IRIS scan is so effective compare to other technology in banking industry for ATM purpose.

II. BACKGROUND: DIFFERENT BIOMETRIC TECHNIQUES

Various biometric techniques are [1, 2, 3]-

1. Facial Recognition

Facial recognition technology is considered a natural means of biometric identification since the ability to distinguish among individuals appearance is proposed by humans. With facial recognition technology a digital video camera image is used to analyze facial characteristics such as distance between eyes, width of nose, cheekbones, jaw line and chin characteristics.These measurements are stored in a database and used to compare with a subject standing before a camera. This has found limited success because it include acquisition environment and facial characteristics changes that effect matching accuracy and the potential for privacy abuse.

DOI: 10.15680/ijircce.2015.0306040

2. Fingerprint Scan

The fingerprint scan technology had the greatest potential to produce the best identification accuracy. Scanning is done by fingerprint scanning devices, most commonly based on optical, thermal, silicon or ultrasonic principles. Fingerprint device follow various methods from matching. Print patterns such as whorls, cups and ridge the matching of at least 15 different characteristics. There are five stages involved in fingerprint scan verification and identification: 1) Fingerprint image acquisition 2) Image processing 3) Location of distinctive characteristics 4) Template creation and 5) Template matching. There are some weakness in fingerprint scanning as lower quality fingerprints, the fingerprints characteristics of an individual can change, making identification and verification difficult.

3. Hand geometry

Hand geometry is based on the fact that every person's hand is shaped differently and that the shape of a person's hand does not change after certain age. Hand geometry systems produce estimates of certain measurement of the hand such as shape, size, finger length, thickness etc. It is generally used where fingerprint is considered intrusive.

4. Voice Recognition

Voice recognition is to analyze the voice of the user in order to store a voiceprint that is later used for identification/verification. Voice verification is not effective because acoustics and other external disturbances interfere with the process.

5. Retinal Scan

Retina scan is based on the blood vessel pattern in the retina of eye. Infrared light source is necessary to illuminate the retina. The infrared energy is absorbed faster by blood vessels in the retina than by surrounding tissue. The image of the retina blood vessel pattern is then analyzed for characteristics points within the pattern. The main drawback of the retina scan is its intrusiveness. Retinal scanning is used only rarely today because it is not user friendly and still remains very expensive. Retina scan enrolments take longer than both iris-scan and fingerprinting. Users claim discomfort with the fact that they must position their eye very close to the device that can harm their eyes in some way.

6. Iris Scan

The iris is the colored ring of textured tissue that surrounds the pupil of the eye. Each iris is a unique structure featuring a complex pattern. This can be a combination of specific characteristics known as corona, crypts, filaments, freckles, pits, furrows, striations and rings. The iris pattern is taken by a special gray-scale camera in the distance of 10-40 cm from the camera. Once the eye is stable and the camera has focused properly the image of the eye is captured. The iris scanning technology is not intrusive and thus acceptable by most users.

Once the gray-scale image of the eye is obtained then the software tries to locate the iris within the image. If an iris is found then the software creates a net of curves covering the iris. Based on the darkness of the points along the lines the software creates the iris code, which characterizes the iris. When computing the iris code two influences have to be taken into account. First, the overall iris code darkness of the image is influenced by the lighting conditions so the darkness threshold used to decide whether a given point is dark or bright cannot be static, it must be dynamically computed according to the overall picture darkness. And second, the size of the iris dynamically changes as the size of the pupil changes. Beforecomputing the iris code, a proper transformation must be done. In the decision process the matching software given 2 iris codes computes the Hamming distance based on the number of different bits. The Hamming distance is a score (within the range 0 – 1, where 0 means the same iris codes), which is then compared with the security threshold to make the final decision. Computing the Hamming distance of two iris codes is very speed fast (it is in fact only counting the number of bits in the exclusive OR of the two iris codes).

The iris recognition was the fastest identification out of all the biometric systems we could work with. Discrimination rate we have never encountered a false acceptance (the database was not very large, however) and the false rejection rate was reasonably low.

The manufacturer quotes the equal error rate of 0.00008%, but so low false rejection rate is not achievable with normal (nonprofessional) users. The iris is also unique and offers high confidence in identification. There isonly a

DOI: 10.15680/ijircce.2015.0306040

chance ofone in 1078 that two iriseswill be identical. The main advantage of the iris scans is the ability to perform them from a distance of up to three feet and short time of scan of only 20 seconds initially, with subsequent identification requiring only two seconds. Glasses and cont- act lenses do not interfere with the scanning process and identification [1, 2, 3].

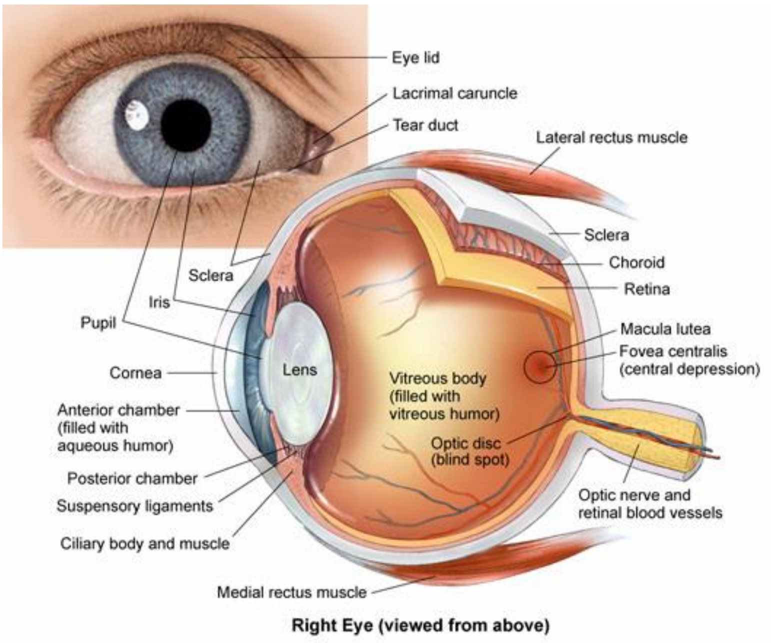

Fig.1 Eye Anatomy [9]

The iris, due to its situation and anatomy, provides several important characteristicswhich make it suitable for biometric purposes[4].

1. Its structure is unique, even the two irises from the same person are different.This is due to the iris development during the pre-natal morphogenesis (7thmonth of gestation), which leads to a random structure which is not geneticallydependant.
2. Iris patterns possess a high degree of randomness, which make them suitable forlarge scale identification applications [5]:

-variability: 244 degrees-of-freedom
-entropy: 3.2 bits per square-millimeter
-uniqueness: set by combinatorial complexity

3. Due to the location of the iris between the lens and the cornea and aqueoushumour, it is protected naturally from possible modifications or accidents. Thisprotection makes it even more difficult to change the iris structure without riskingvision damage, and therefore, reducing the possibility of changing it [6],this avoids potential intruders from modifying iris characteristics to defraud therecognition system.
4. Although the iris is an internal organ, it is visible thanks to the transparent lenswhich covers it. Iris patterns can be observed in images which are taken fordistances of up to 1 meter between the user and sensor. Therefore, this modalitydoes not need to be intrusive, as no direct contact is required between the user andsensor. Nowadays, sensors exist which can acquire iris images at larger distances[7].
5. The iris is present in almost all users; just a small portion of the population donot possess an iris, this is mainly because of aphakia illness [8] or iris removalduring cataract surgery.
6. The iris structure does not change during the user's lifespan, although its colourdoes change [5], so lifetime recognition is possible for each user.

DOI: 10.15680/ijircce.2015.0306040

7. The main function of the iris is to control the light which enters the eye throughthe pupil. The natural dilations and contractions it makes can be used to provethe natural physiology of it, and thus, liveness detection of the sample examined.
8. The computational time required to perform the identification is relatively low,this makes real-time iris detection applications possible.
9. Due to cultural issues, iris detection is suitable for use in places where other partsof the body, such as fingerprint or faces are not shown.
10. The eye tissue, especially the iris, degrades rapidly after death. This characteristicprovides an extra countermeasure against the use of eyes from a corpse toaccess systems.

III.PROPOSED METHDOLOGY

This proposed system makes use of IRIS scanning Technology, the biometric device IRIS scanner which scan IRIS (Physical part of human eye) to identify the user. Our proposed system require user to generate the IRIS sample at the time of creating account in bank. This users sample is stored in bank authentication database. Then for Authentication pin is required that 4 digit pin is nothing but the user YOB (Year of Birth). User now uses the ATM machines without any cards. Following figure 2 shows the cardless biometric authentication.

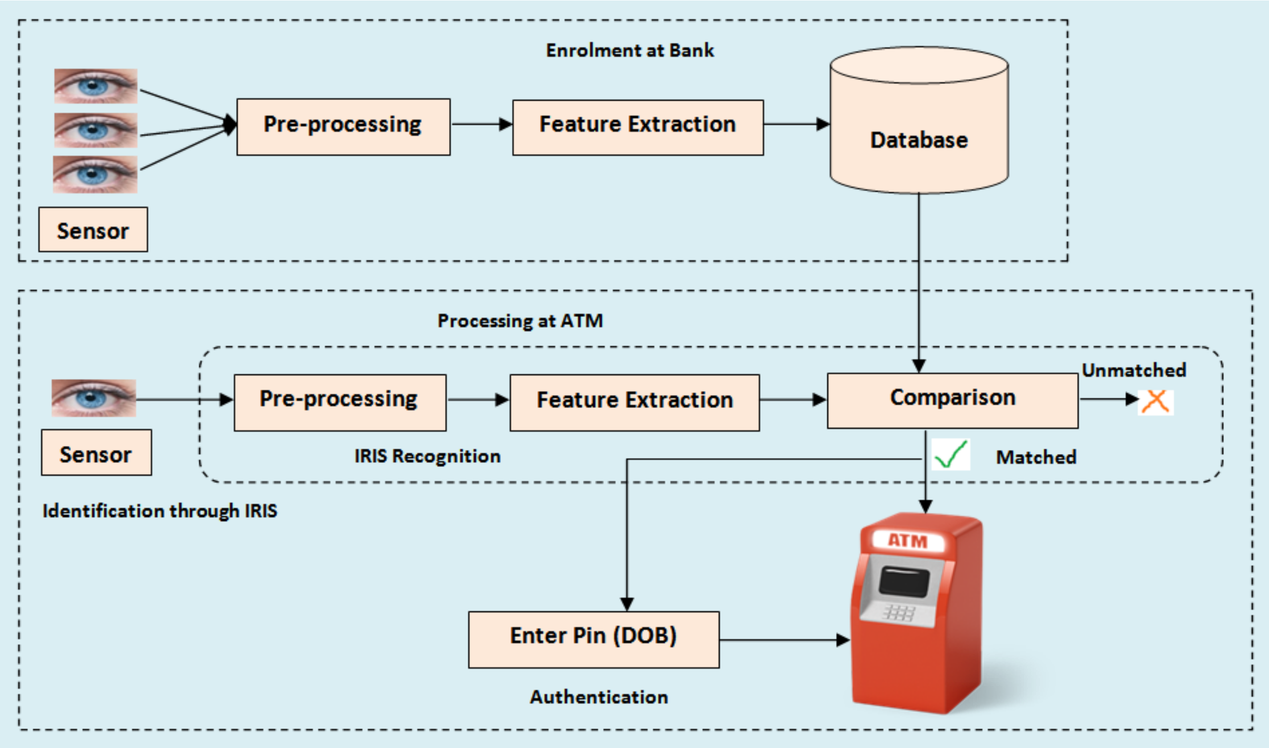

Fig.2 IRIS Process for ATM

The user can now enter the ATM Room and have to scan his eyes in IRIS scanning device. Then the System will identify the user with samples stored in authentication database. If identification has been done successfully then machine will prompt the voice “enter the pin” and after entering correct pin, ATM machine will be available to the user to perform the single transaction. For every transaction user have to perform the same process every time.If 3 consecutive authentications are failed then the system will block the user account for 24 hours.

III. REQUIREMENT FOR PROPOSED SYSTEM

1. ATM Centre should have biometric device (IRIS Scanner) and numeric keypad.
2. If 24 hours account blockage occurs more than five times then the user account should block permanently and ask the user to regenerate the new authentication at home bank.

IV. DRAWBACKS OF EXISTING CARD BASED ATM SYSTEM

1. Existing system is on card basis so it requires more time to process cards.
2. If card is lost /stolen there is high possibility of misuse of card.
3. If card is stolen /lost then bank requires more time to regenerate new card also it is costly.
4. After 3-4 years or after repeated transactions card will unable to operate, hence bank should have to provide new card to account holder then it is expensive costly and time consuming.
5. Excess use of plastic cards is harmful for environment.
6. If an account holder has multiple cards then it is difficult to remember password for all the cards [10].

V. ADVANTAGES OF IRIS TECHNIQUE

1. Provides strong authentication.
2. Biometric system replaces card system with physiological characteristics.
3. Hidden costs of ATM card management like- card personalization, delivery, management, re-issuance, helpdesk, and re-issuance can be avoided.
4. Ideal for Indian rural masses.
5. Account holder may nominate for another person which will have valid identification for same account.
6. It is more helpful to senior citizens because it is difficult to carry and maintain card with him.
7. Complaints regarding card such as - stolen cards regenerating new cards, maintaining and recording of cards etc. will be eliminated. Thus it is helpful to bank to reduce cost, time and efforts for card process.
8. Flexible account access allows service users to access their accounts as per their convenience.
9. Due to biometric authentication no one is able to access others account.
10. Users never forget their YOB (Birth year) i.e. used as 4 digit Pin [10].

VI. LIMITATIONS OF IRIS TECHNIQUE

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. Due to biometric only account holder (except nominee) can access account.
3. Every time, account holders should come to ATM to collect money

VII. FUTURE WORK

1. By improving DPI of scanned image using software, the scanner device can be made accurate, instead of using higher end scanner. So that cost can be reduced.
2. Biometrics do not eliminate the possibility of robbers dragging victims at gunpoint to withdraw money from ATMs, but there will have the option of using sensors and cameras with biometric devices to detect stress and various unwanted movements. If such movements occur then it will message or alarm to the nearby Police station.

VIII. CONCLUSION

Biometrics allow for increased security, convenience and accountability while detecting and deterring fraud. Proposed approach is suitable for the ATM users without the need to carry ATM card. In this system biometric device i.e. IRIS scanner to get identified and no need to remember password anymore, just used YOB (Year of Birth) as your 4 digit pin to get authentication. It helps for identification and authentication of service user. This approach reduce effort of handling, operating and various risk associated with cards. This method reduce time, effort of both bank as well as service users but the implementation of this technique can be costlier.

REFERENCES

1. prof. Chandrakant.D.Patel, Prof. Sanket trivedi, Prof. Sanjay patel , "Biometric in IRIS Technology- A survey", International journal of scintific research publication, Vol-2, issue 1, jan-2012.
2. Zdenek Riha, Vaclav Matyas, "Biometric authentication system ", FIMU- Report Series- 2000-08.
3. Manoj gupta, "Biometric technology overview", SANS reading room. http://rr.sans.org/aunthetic/biometric2.php.
4. John G. Daugman. High con¯dence visual recognition of persons by a testof statistical independece. IEEE TRansaction on Pattern Analysis and MachineIntelligence, November 1993.
5. John Daugman. http://www.cl.cam.ac.uk/ jgd1000, 2003.
6. Michael E. Snyder, Christopher Khang, Scott E. Burk, and = Robert H. Osher. http://www.osnsupersite.com/view.aspx?rid=23421, 2007.
7. J. R. Matey, O. Naroditsky, K. Hanna, R. Kolczynski, D.J. LoIacono, S. Mangru, M. Tinker, T. M. Zappia, and W.Y.Zhao. Iris on the move: Acquision on images for iris recognation in less contrained enviroments. Proceedings of IEEE, 94[11]:1936{1947, November 2006.
8. Aphakia. http://en.wikipedia.org/wiki/aphakia, 2009.
9. http://www.onlyeyesknew.com/wp-content/uploads/2013/05/iris.jpg
10. S.T. Bhosale, Dr. B.S. Sawant, Security in e- banking via card less biometric ATMs, International journal of Advance Technology & Engineering Research, Volume 2, issue 4, July-2012

BIOGRAPHY

Nachiket Sainis is a Assistant Professor in the Computer Science Department, B.K. Birla Institute of Engineering & Technology, Pilani. He received Master of Computer Application (MCA) degree in 2014 from IGNOU, New Delhi, India

Reena Saini is a Assistant Professor in the Information Technology Department, B.K. Birla Institute of Engineering & Technology, Pilani. She received M.Tech in Software Engineering from Bansthali Vidyapeeth, Jaipur, Rajasthan, India in 2006-2008. Ms.Reena Saini is the member of The Institution of Engineers (India).

DOI: 10.15680/ijircce.2015.0306040