Namrata *et al*, International Journal of Computer Science and Mobile Applications,
Vol.3 Issue. 10, October- 2015, pg. 38-47 **ISSN: 2321-8363**

REVIEW PAPER ON ENHANCE THE ATM SECURITY USING FINGERPRINT RECOGNITION

Namrata[1], Dr. Sukhvir Singh[2]

[1]M.Tech C.S.E Department N.C College Of Engineering, Israna Panipat, vij.namrata276@gmail.com
[2]Associate Professor in C.S.E Department N.C College Of Engineering, Israna Panipat, boora_s@yahoo.com

ABSTRACT

Identification and verification of a person today is a common thing; which may include door-lock system, saf box and vehicle control or even at accessing bank accounts via ATM, etc which is necessary for securin personal information. The conventional methods like ID card verification or signature does not provid perfection and reliability. The systems employed at these places must be fast enough and robust too. Use of th ATM (Automatic Teller Machine) which provides customers with the convenient banknote trading is facing new challenge to carry on the valid identity to the customer. Since, in conventional identification methods wit ATM, criminal cases are increasing making financial losses to customers. This system can be employed at an application with enhanced security because of the uniqueness of fingerprints. It is convenient due to its lov power requirement and portability

***Keywords**:* Fingerprint Recognition, ATM security, Identification, Verification, Pin

1. INTRODUCTION

Biometrics is the art of science and technology of measuring and analyzing biological data. If biometrics refers to technologies that measure and analysis human body characteristics, such as DNA, fingerprinting, eye retina and irises, voice pattern, facial pattern and measurement for authentication purposes.

Biometrics identifier method provides several advantages over the traditional method and current method used in our daily life. Basically concentrate on two function one is for identification and other verification. A modern ATM is typically made up of the devices like CPU to control the user interface and devices related to transaction, magnetic or chip card reader to identify the customer, Pin pad, secure crypto-processor generally within a secure cover. Display to be used by the customer for performing the transaction, function key button, record printer to provide the customer with a record of their transaction, to store the parts of the machinery requiring restricted access- vault, housing for aesthetics, sensors and indicators.

In this modern era there are many people using ATM. Fast development of banking has various advantages and disadvantages. It is situated at different places and easily access by the customer like to withdrawal cash payment money transfer facility. It is the commercial need of the today era customer easily pay house bill

phone bill without banking staff member and easily update all the transaction of the account to the staff. The account holder will hold the ATM card and PIN (personal identification number) and password.

There is a need for improve security in ATM transaction:-

1. Low educated people can access easily.
2. When our ATM card misplaces then no one use or access.
3. It automatically blocks.
4. No one can hake the pin code.
5. The hackers can easily guess the 4 digit pin code.
6. Stop crime which is happening in ATM become a serious issue that affects not only customers but also bank operators. A large number of population in our country only 85 percent of the population use the ATM while 15 percent of the population is yet to use the machine. This 15 percent of the population is still skeptical about using ATM because of the issues associated with it. Such issues as inability of the machine to service" usually displayed by the machine which most of the time is disappointing and frustrating among others. 100 percent of the population is aware of one form of ATM fraud or another. 89 percent of the population thinks that ATM transactions are becoming too risky this necessitated 93 percent of the population affirming that they will continue the use of ATM because of security issues associated with the machine. Hence, 100 percent of the population preferred a third authentication aside the use of ATM card and PIN and this population believed that with the infusion of biometrics characteristics to the existing ATM card and PIN, ATM security will be improved drastically.

Figure 1: ATM Transaction

Fingerprint technology is the most widely accepted and mature biometric method and is the easiest to deploy and for a higher level of security at your fingertips. It is simple to install and also it takes little time and effort to acquire one's fingerprint with a fingerprint identification device. Thus, fingerprint recognition is considered

among the least intrusive of all biometric verification techniques. Ancient times officials used thumbprints to seal documents thousands of years ago, and law agencies have been using fingerprint identification since the late 1800s [1]. We here carry the same technology on digital platform. Although fingerprint images are initially captured, the images are not stored anywhere in the system. Instead, the fingerprints are converted to templates from which the original fingerprints cannot be recreated; hence no misuse of system is possible.

Fingerprint is one of the essential variables used for enforcing security and maintaining a reliable identification of any individual. Fingerprints are used as variables of security during voting, examination, operation of bank accounts among others.

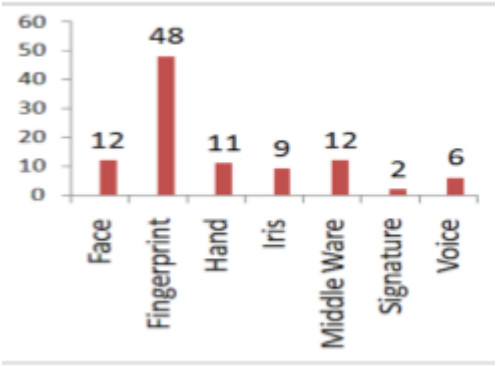


Figure 2: Survey of fingerprint with other Biometrics

1.1 VARIOUS BIOMETRIC TECHNOLOGIES

A. Fingerprint verification:- In this technique , Bank customer's finger matching a minutiae and straight pattern and unique marks in fingerprint.

B. Hand geometry:- Hand geometry is a biometric solution that reads a person's hand and/or fingers for access. This technique concerned with measuring the physical characteristics of the customer hand and fingers.

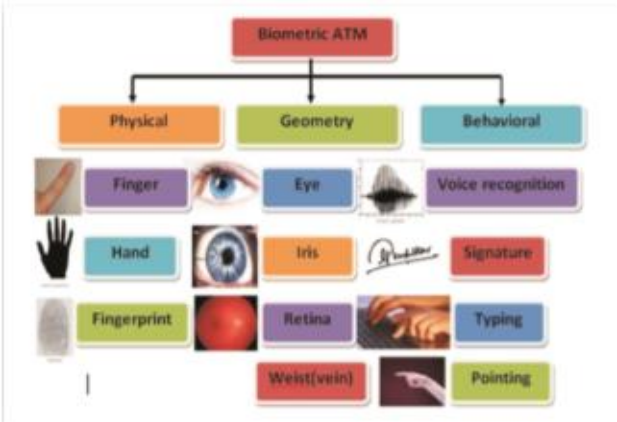
C. Voice verification:- This techniques followed some types of word, key, number sought by the customers at the front of ATM machines and Biometric ATM machines recognition voice and identify the customers voice next process has been done.

D. Retinal scanning:- This technique used to identify the unique patterns of the retina of the customers. Retinal scanning devices are the most accurate physical biometric available today since there is no known way to replicate a retina

E. Iris scanning:- Iris scanning is eye related biometric systems, Iris scans analyze the features that exist in the colored tissue surrounding the pupil of an eye, it is utilized a conventional camera element and requires no intimate contract between user and reader.

F. Facial recognition:- Facial recognition analyzes the characteristics of a person's face. Access is permitted only if a match is found. The process works when a user faces a digital video camera, usually standing about

two feet from it, where the overall facial structure, including distances between eyes, nose, mouth, and jaw edges are measured.



G. Signature verification:- The technology examines such dynamics writing speed of the persons, directions of writing, and pressure of ball point writing.

H. Vascular patterns:- Vascular patterns described a full picture of the veins in a person's hand or face. The thickness and location of these veins are believed to be unique enough to an individual to be used to verify a person's identity.

1.2 COMPARISON BETWEEN BIOMETRICS

The use of fingerprints as a biometric is both the oldest mode of computer-aided, personal identification and the most prevalent in use today. In the world today, fingerprint is one of the essential variables used for enforcing security and maintaining a reliable identification of any individual. Fingerprints are used as variables of security during voting, examination, operation of bank accounts among others. They are also used for controlling access to highly secured places like offices, equipment rooms, control centers and so on . The result of the survey conducted by the International Biometric Group (IBG) in 2012 on comparative analysis of fingerprint with other biometrics is presented . The result shows that a substantial margin exists between the uses of fingerprint for identification over other biometrics such as face, hand, iris, voice, signature and middleware .

1.3 WHY BIOMETRIC FINGERPRINT?

1. Uniqueness.

2. Surety over the Cards and Keypads.

3. Against to Cards Duplication, misplacement and improper disclosure of password.

4. No excuses for RF/Magnetic Cards forget ness.

5. No need to further invest on the Cards Cost.

1.4 ADVANTAGES

1. Biometric traits cannot be lost or forgotten (while passwords can).

2. Biometric traits are difficult to copy, share and distribute (passwords can be announced in crackers‟ websites).

3. They require the person being authenticated to be present at the time and point of authentication.

1.5 DISADVANTAGES

A biometric authentication system seems to be an excellent solution to authentication problems; however biometric authentication has some weaknesses:

1. Education required: While an increasing number of available technologies are "plug and play", they still require some user education. Users need to know how to position their finger, face, and eye. Additionally, implementers will need training on proper installation and maintenance of biometric systems.

2. Expensive: While there are several models of fingerprint, voice, and signature verification available in the $100 range, a majority of technologies are still closer to the $500 mark. Unless biometrics can get below the cost of password administration costs, business will get below the cost of password administration costs, business will not chose to implement.

3. Affected by environment and disease: It is not the case that your fingerprints, face, or voice remain constant from day to day, small fluctuations (cold or moist hands for fingerprint scanners, different ambient lighting for face recognition, and background noise for voice authentication) can block the devices. Setting the sensitivity lower makes the product more forgiving but increases the odds of a false positive a faker logging on as someone else. Higher sensitivity means greater security, but it also means that an authorized user may be erroneously rejected.

4. Harmful: The method of obtaining a retinal scan is personally invasive - a laser light (or other coherent light source) must be directed through the cornea of the eye and uses an infrared light source to highlight the biometric pattern. This can harm an individual's eye.

1.6 BIOMETRIC APPLICATIONS

Biometrics is a rapidly evolving technology that is being widely used in forensics, such as criminal identification and prison security, and that has the potential to be used in a large range of civilian application areas. Biometrics can be used to prevent unauthorized access to ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. In automobiles, biometrics can replace keys with keyless entry devices.

1. Government - Passports, national identification (ID) cards, voter cards, driver's licenses, social services, and so on.

2. Transportation - Airport security, boarding passes, and commercial driver's licenses.

3. Healthcare - Medical insurance cards, patient/employee identity cards.

4. Financial - Bankcards, ATM cards, credit cards, and debit cards.

5. Security - Access control and identity verifications, including time and attendance.

6. Public justice and safety - Prison IDs, county probation offices‟ use for identification of parolees, county courthouses‟ use for ID systems.

7. Education - Student/teacher identity verification and access control. Biometrics is now being implemented in large-scale ID systems around the globe. Many new passport and national ID card systems use some type of biometric encoded in a bar code or smart chip.

8. Driver's licenses - Technologies being recommended by American Association of Motor Vehicle Administrators (AAMVA), the organization that oversees DMV standards, include biometrics and two-dimensional bar codes. Georgia, North Carolina, Kentucky, and others already utilize biometrics on their respective state driver's licenses.

9. Access control - one of the most traditional of applications for biometrics, accessing buildings, offices, cars, and even homes are applications for biometric implementations.

10. Time and attendance - a growing number of work places are implementing biometric technologies to allow employees to "punch the clock". This prevents employees from "buddy punching" and ensures that employee productivity actually matches up with recorded times.

11. Law enforcement - while this is a substantial section of the market for fingerprint scanners, the hardware is often different than commercially targeted hardware, geared for collection of a large number of one individual.

2. OBJECTIVE

There are two main objective of this paper, as follows:-

1. To integrate the fingerprinting in access control for ATM system.
2. To purpose a framework for the ATM system using fingerprint verification.

The working of the ATM machine is such that when a customer place a finger on the finger print module it automatically generates every time different 4-digit code as a message to the mobile of the authorized customer through GSM modem connected to the microcontroller. The code received by the customer is entered into the ATM machine by pressing the keys on the touch screen. After entering it checks whether it is a valid one or not and allows the customer further access.

2.1 HOW DOES BIOMETRICS WORK?

Most biometric technology systems use the same basic principles of operation. First, a person must be registered, or enrolled, on the biometric system.

1. Enrollment: The process by which a user's biometric data is initially acquired, accessed, processed, and stored in the form of a template for ongoing use in a biometric system is called enrollment. Subsequent verification and identification attempts are conducted against the template(s) generated during enrollment.

2. Presentation: Presentation is a process by which user provides biometric data to an acquisition device-the hardware used to collect biometric data. Depending on the biometric system, presentation may require looking in the direction of a camera, placing a finger on a platen, or reciting pass phrase.

3. Biometric data: The biometric data users provide in an unprocessed image or recording of a characteristic. The unprocessed data is also referred to as raw biometric data or as a biometric sample. Raw biometric data cannot be used to perform biometric matches. Instead, biometric data provided by the user during enrollment and verification is used to generate biometric templates, and in almost every system is discarded thereafter. Thus Biometric systems do not store biometric data-systems use data for template creation. Enrollment requires the creation of an identifier such as a username or ID. This identifier is normally generated by the user or administrator during entry of personal data. When the user returns to verify, he or she enters the identifier, and then provides biometric data. Once biometric data has been acquired, biometric templates can be created by a process of feature extraction.

4. Feature extraction: The automated process of locating and encoding distinctive characteristics from biometric data in order to generate a template as called feature extraction. Feature extraction takes place during enrollment and verification-any time a template

is created. The feature extraction process includes filtering and optimization of images and data in order to accurately locate features. For example, voice-scan technologies generally filter certain frequencies and patterns, and finger-scan technologies often thin ridges present in a fingerprint image to the width of a single pixel. Since quality of feature extraction directly affects a system's ability to generate templates, it is extremely important to the performance of a biometric system.

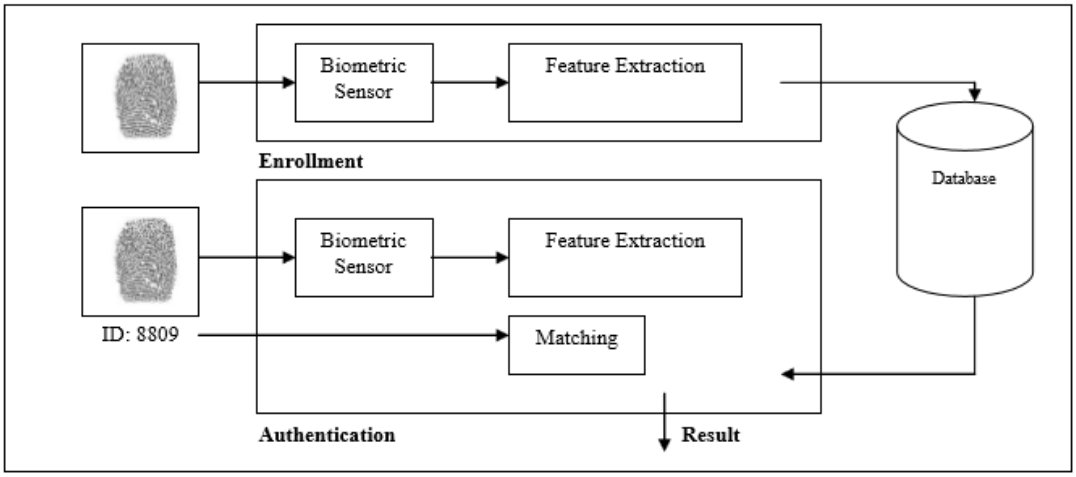


Figure 3: General Biometrics System

2.2 RELATED WORK

Jain et al. Suggest that earlier security for ATM is not very much efficient. In an earlier ATM machine only password provided by bank to user, but it is not safety for customers. Because of some limitation, therefore they research a biometric method for more verification.

Mr. Wang et al. Expresses his view like that now a day ATM with magnetic strip authenticated only by inserting password on the ATM machine. But according to today's scenario, cases of fraud are another problem. So they provided fingerprint for more security. Now a days we are directing towards the pile of new powerful,

intelligent, auto rated system, which will give us easy to do the work smoothly, Thus systems are not dependant on human support, one of these 'ATM SECURITY SYSTEM' which we have evolved.

M. Subha and S. Vanithaasri's they proposes ATM access with biometric security system which is highly authenticated to the client. For authentication fingerprint static points are applied in the related works by conventional way. The minutiae points of fingerprint, ridge features, and iris are considered in the proposed system for increasing the matching scores against the occurrence of distortions and non-linear deformations. Consecutive steps are processed in the proposed system. Hence, the authentication is high in the proposed application of ATM access.

RESEARCH BACKGROUND Crime at ATMs has become a nationwide issue that faces not only customers, but also bank operators and this financial crime case rises repeatedly in recent years . A lot of criminals tamper with the ATM terminal and steal customers' card details by illegal means. Once users' bank card is lost and the password is stolen, the users' account is vulnerable to attack. Traditional ATM systems authenticate generally by using a card (credit, debit, or smart) and a password or PIN which no doubt has some defects . The prevailing techniques of user authentication, which involves the use of either passwords and user IDs (identifiers), or identification cards and PINs (personal identification numbers), suffer from several limitations . Passwords and PINs can be illicitly acquired by direct covert observation. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Despite warning, many people continue to choose easily guessed PIN's and passwords - birthdays, phone numbers and social security numbers. Recent cases of identity theft have heightened the need for methods to prove that someone is truly who he/she claims to be. Biometric authentication technology may solve this problem since a person's biometric data is undeniably connected to its owner, is nontransferable and unique for every individual. The system can compare scans to records stored in a central or local database or even on a smart card. Biometrics can be defined as a measurable physiological and behavioral characteristic that can be captured and subsequently compared with another instance at the time of verification. It is automated methods of recognizing a person based on a physiological or behavioral characteristic. It is a measure of an individual's unique physical or behavioral characteristics to recognize or authenticate its identity . Common physical biometrics characteristics include fingerprint, hand or palm geometry, retina, iris and face while popular behavioral characteristics are signature and voice. Biometrics technologies are a secure means of authentication because biometrics data are unique, cannot be shared, cannot be copied and cannot be lost.

3. CONCLUSION

The system also contains the original verifying methods which was inputting owner's password which is send by the controller. The security features were enhanced largely for the stability and reliability of owner recognition. The whole system was build on the fingerprint technology which makes the system more safe, reliable and easy to use.
As we know that fingerprint are the most acceptable biometrics all over the world in identifying a person. Some government in the world are still implementing fingerprints technique to identify their citizens and the criminal from the scene of crimes in forensic work.

FUTURE SCOPE

A lot of criminals tamper with the ATM terminal and steal customers' card details by illegal means. Once users' bank card is lost and the password is stolen, the users' account is vulnerable to attack. Traditional ATM systems authenticate generally by using a card (credit, debit, or smart) and a password or PIN which no doubt has some defects . The prevailing techniques of user authentication, which involves the use of either passwords and user

IDs (identifiers), or identification cards and PINs (personal identification numbers), suffer from several limitations . Passwords and PINs can be illicitly acquired by direct covert observation. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Despite warning, many people continue to choose easily guessed PIN's and passwords - birthdays, phone numbers and social security numbers. Recent cases of identity theft have heightened the need for methods to prove that someone is truly who he and she claims to be. Biometric authentication technology may solve this problem since a person's biometric data is undeniably connected to its owner, is nontransferable and unique for every individual. The system can compare scans to records stored in a central or local database or even on a smart card. This technique is very useful in future for avoiding the fraud in ATM system.

References:-

1. G.Sambasiva Rao, C. NagaRaju, L. S. S. Reddy and E. V. Prasad, "A Novel Fingerprints Identification System Based on the Edge Detection", International Journal of Computer Science and Network Security, vol. 8, pp. 394-397, (2008).

2. S, Das and J. Debbarma, "Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian e-banking System", International Journal of Information and Communication Technology Research, vol.1, no. 5, pp.197-203, 2011.

3.Anil K. Jain, Jianjiang Feng, Karthik Nandakumar, "Fingerprinting Matching", IEEE Computer Society 2010, pp.36-44,0018-9162/10.

4.Wan W.W.N;Luk,C.L;and Chow, C.W.C.(2005),Customers Adoption of banking channels in Hong K34rong, International Journal of Bank Marketing, Vol. 23, no.3,pp. 255-272.

5. Jain, A.K.; Ross, A.; Prabhakar, S., "An introduction to biometric recognition," Circuits and Systems for Video Technology, IEEE Transactions on, Vol. 14, no. 1, pp. 4,20, Jan. 2004 doi: 10.1109/TCSVT.2003.818349 2.

6. Mr. John Mashurano1, Mr. Wang liqiang2, "ATM Systems Authentication Based On Fingerprint Using ARM Cortex-M3" International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 3, March - 2013 ISSN: 2278-0181 1 www.ijert.org IJERTIJERT

7. M. Subha and S. Vanithaasri "A study on authenticated admittance of ATM clients using biometrics based cryptosystem" International Journal of Advances in Engineering & Technology, Sept 2012. ©IJAET ISSN: 2231-1963 Vol. 4, Issue 2, pp. 456-463.

8. "Automatic Teller Machine". The history of computing project. Thocp.net. 17 April 2006

9. Bhawna Negi 1 , Varun Sharma"Fingerprint Recognition System", International Journal of Electronics and Computer Science Engineering 872, , www.ijecse.org ISSN- 2277-2011.

10. Arpita Gopal, Chandrani Singh, e-World : Emerging Trends in Information Technology, Excel Publication, New Delhi (2009).

11. James L. Wayman, Anil K. Jain, Davide Maltoni, and Dario Maio, Biometric Systems: Technology, Design and Performance Evaluation, Springer.

12. Moses Okechukwu Onyesolu, Ignatius Majesty Ezeani, "ATM Security Using Fingerprint Biometric Identifer: An Investigative Study", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No.4, 2012, pp. 68-72.

BIOGRAPHY

Namrata

I completed my bachelor's in Computer Science And Engineering from N.C.I.T to Kurukshetra University in 2014. Presently pursuing the M.Tech from N.C College of Engineering, Israna Panipat and working as a Teaching Assistant. My research interest include Image Processing and Networking.

Dr. Sukhvir Singh

I completed my PHD in Computer Science And Engineering from M.D University, Rohtak and studied in National Polytechnic University of Armenia in (1996). I have 18 Yrs, experience in teaching. Presently am working in N.C. College of Engineering, Israna Panipat as a Associate Professor in Department Of Computer Science And Engineering.

