International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-3 Issue-4, April 2014

Fingerprints in Automated Teller Machine-A Survey

Gazal Betab, Ranjeet Kaur Sandhu

Abstract— The main objective of this system is to develop a system that will increase the ATM security. However, despite the numerous advantages of ATM system, ATM fraud has recently become more widespread. In this paper, we provide an overview of the possible fraudulent activities that may be perpetrated against ATMs and investigates recommended approaches to prevent these types of frauds.. The ATM will service one customer at a time. A customer will be required to enter a login id and validate his finger print and both will be sent to the bank for validation as part of each transaction. This makes the developed ATM software more secure as compared to the software that authenticates the user merely by using a PIN or password.

Index terms— ATM Fraud, ATM Fraud Countermeasures Biometrics, Fingerprint Verification.

I. INTRODUCTION

An automated teller machine was first introduced in 1960 by City Bank of New York on a trial basis, the concept of this machine was for customers to pay utility bills and get a receipt without a teller. As we know that over the past three decades, consumers have been largely depending on and trust Automatic Teller Machine, known as ATM machine to conveniently meet there banking needs. Using an ATM, customers can access their bank accounts in order to make cash withdrawals, debit card cash advances, and check their account balances as well as purchase prepaid cell phone credit. with the convenient banknote trading is very common. However, the financial crime case rises repeatedly in recent years, a lot of criminals tamper with the ATM terminal and steal user's credit card and password by illegal means. Once user's bank card is lost and the password is stolen, the criminal will draw all cash in the shortest time, which will bring enormous financial losses to customer. Authentication methods for ATM cards have little changed since their introduction in the 1960's. Typically, the authentication design involves a trusted hardware device (ATM card or token). The card holder's Personal Identification Number (PIN) is usually the only means to verify the identity of the user. The security limitations of ATM are mostly derived from
the security pitfalls of the magnetic media. The security limitations of ATM are mostly derived from the security pitfalls of the magnetic media.

Manuscript published on 30 April 2014.
***** Correspondence Author (s)
Er. Gazal Betab persuing M.Tech in computer science and technology from D.A.V University Jalandhar 2013-2015 and have completed B.Tech in Information Technology 2009-2013 from DAVIET Jalandhar under Punjab, India.
Ranjeet Kaur Sandhu received her bachelorDegree with Honours in Computer science & Engineering from Punjab technical university, Jalandhar in 2008 and M.Tech in computer science & engineering from Punjab Technical University Jalandhar, India.

We tried to purpose a prototype model for the same, which uses PIN number along with the fingerprint verification scheme to verify the user before he can access his/her account and make the transactions. However ATMs using single layer of verification i.e. biometric verification can also be developed using our prototype model.

II. AUTOMATED TELLING MACHINE

"ATM" stands for Automated Teller Machine. This machine allows the account holder to have transactions with their own accounts without allowing them to access the entire bank's database. ATM machine was 1invented by John shepphardbaren on June 1967 at Barclays bank in Enfield, United Kingdom . In India, Hong Kong and Shanghai banking corporation (HSBC) installed first ATM in 1987. Indian bank 2and Citi bank introduced ATMs at various stages [1]**.**
For **A**synchronous **T**ransfer **M**ode,network technology based on transferring data in cells or packets of a fixed size. The cell used with ATM is relatively small compared to units used with older technologies. The small, constant cell size allows ATM equipment to transmit video, audio, and computer data over the same network, and assure that no single type of data hogs the line.Some people think that ATM holds the answer to the Internet bandwidth problem, but others are skeptical. ATM creates a fixed channel, or route, between two points whenever data transfer begins. This differs from TCP/IP, in which messages are divided into packets and each packet can take a different route from source to destination. This difference makes it easier to track and bill data usage across an ATM network, but it makes it less adaptable to sudden surges in network traffic.

Figure 1. ATM transaction

III. ATM ATTACKS

There are a variety of ATM attacks because it is such an attractive target. There are three basic types of ATM attacks [1]

A. Physical attack: Brute force attack to ATM machines with the intention of gaining access to cash within the safe.

B. ATM Fraud: Theft of bank card information.

C. Software and network attack: Theft of sensitive information or controlling ATM spew out bills automatically

V. ATM AUTHENTICATION

To continue the ATM operation we authenticate the valid identity of a customer using three different parameters: a. What we have i.e. an ATM card b. What we know i.e. a PIN code or a Password c. What we are i.e. Biometrics it may be Fingerprint, Face, Iris etc. We usually authenticate the user with combination of what we have and what we know but a password can be easily guess or can be trapped and an atm card can be lost or borrowed. But with a dual combination of three way authentication which is a card, a password and with the addition of biometric technique we can protect our ATM transaction more safely.

IV. BIOMETRICS

Biometrics refers to the quantifiable data (or metrics) related to human characteristics or traits. Biometrics identification (or biometric authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information.

VI. BIOMETRIC TECHNOLOGY

Biometric refers to any and all of variety of [8] identification technique which are based on some physical behavioural characteristics. Biometric ATM support only at ATM machine which is facilitates these types of services. The ATMs are network connected centralised computer system with controls ATMs. The biometric identification is possible at an ATM and identification data stored in main bank branch. Generally an ATM machine operates in two stages, first card slot and second key guard. Most of the ATMs use magnetic strip card and personal identification number to identified account holders. The Biometric ATM [7] solution consists of central server which holds a repository of customer finger prints and verification of accounts. The central server provides platforms of independent; it uses java run time on 3UNIX and oracle/ McIntosh SQL server customisation to bas 24 switches .

Biometric ATM technique divides into various parts namely:

A. *Physiological technique* Included finger, hand and fingerprint
B. *Geometry technique* Included eye, retinas, iris, face, and wrist (vein)
C. *Behavioral technique* Included Voice, signature, typing and pointing.

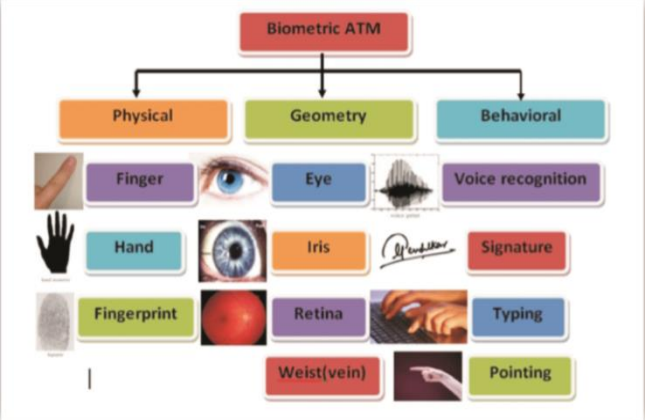

Figure 2. various biometric techniques

VII. VARIOUS BIOMETRIC TECHNOLOGIES

A. Fingerprint verification:-

In this technique [2], 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'shand 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 soughted 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 pattrns of the ratina of the customers.Retinal [6] scanning devices are the most accurate physical biometric available today since there is no known way to replicate a retina

E. Iris scanning:-

Irisscanning 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.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

H. Vascular patterns:-

Vascular patterns described a full picture of the veins in a person's handor face. The thickness and location of these veins are believed to be uniqueenough to an individual to be used to verify a person's identity.

I. Keystroke recognition:-

This keystroke recognition technology has recently gained in the music industry; this information would be used to protect songs pirates against unauthorized distribution and illegal use.There are various banking products of biometric but the most commonly used biometrics are fingerprint scanning, voice recognition, retina scan and face recognition.

Biometric characteristic	sality	ss					
Facial thermo gram	H	H	L	H	M	H	L
Hand vein	M	M	M	M	M	M	L
Gait	M	L	L	H	L	H	M
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Ear	M	M	H	M	M	H	M
Hand geometry	M	M	M	H	M	M	M
Fingerprint	M	H	H	M	H	M	M
Face	H	L	M	H	L	H	H
Retina	H	H	M	L	H	L	L
Iris	H	H	H	M	H	L	L
Palm print	M	H	H	M	H	M	M
Voice	M	L	L	M	L	H	H
Signature	L	L	L	H	L	H	H
DNA	H	H	H	L	H	L	L

Table 1. comparison between various biometrics

J. Palm print:-

Palm print biometrics is a system that measures the physical characteristics of an individual's palm. The 4specified palm is placed on a reader where the measurements are taken.

K. Vein pattern:-

Vein pattern matching involves scanning the vein patterns on the back of a customer's hand. The customer's 5place their hand into a reader . Inside a small black and white camera and LED array are used to capture the 6digital image. There is difficulty of identify vein pattern changing over a time.

VIII. 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 in Figure. 2. 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 .

IX. WHY BIOMETRIC FINGERPRINT?

- Uniqueness
- Surety over the Cards and Keypads
- Against to Cards Duplication, misplacement and improper disclosure of password
- No excuses for RF/Magnetic Cards forget ness
- No need to further invest on the Cards Cost

X. CONCLUSION

This paper identifies a model for the modification of existing ATM systems to economically incorporate fingerprint scanning; and, outlines the advantages of using such system. It should be noted that the customers' perception cannot be generalized as it was highly affected by the tradition/culture of the users involves. As we know that fingerprints are the most acceptable biometrics all over the world in identifying a person. In this paper fingerprint are chosen for its uniqueness, ease of use and also convenience to user; as fingerprints can't be stolen, it is not transferable and the use don't need to remember. The security features were enhanced largely for the stability and reliability of owner recognition. The whole system was build on the technology of embedded system which makes the system more safe, reliable and easy to use.

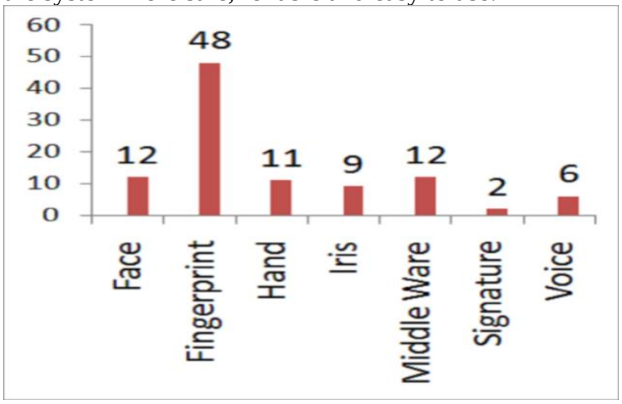

Figure 3. survey on fingerprints

ACKNOWLEDGMENT

I would like to thank all those who co-operated with the conduct this survey and for allowing themselves to be co-operated with the conduct this survey and for allowing themselves to be co-operated with the conducted interviewed. In order to preserve anonymity they cannot be named. Without their help this survey could not have been carried out.

I am equally grateful to my teacher Er. Ranjeet Kaur Sandhu , she gave me moral support and guided me in different matters regarding the topic. she had been very kind and patient while suggesting me the outlines of this project and correcting my doubts.I thank her for her overall supports. Last but not the least, I would like to thank my parents who helped me a lot in gathering different information.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

REFERENCES

[1] ”Automatic Teller Machine”. The history of computing project. Thocp.net. 17 April 2006
[2] Bhawna Negi 1 , Varun Sharma”Fingerprint Recognition System”, International Journal of Electronics and Computer Science Engineering 872 , www.ijecse.org ISSN- 2277-2011.
[3] Bhupesh Gour, T. K. Bandopadhyaya and Sudhir Sharma, “Fingerprint Feature Extraction using Midpoint Ridge Contour Method and Neural Network”, International Journal of Computer Science and Network Security, vol. 8, no, 7, pp. 99-109, (2008).
[4] 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).
[5] Pennnam Krishnamurthy and Mr. M. Maddhusudhan Redddy. “Implementation of ATM Security by Using Fingerprint recognition and GSM”, International Journal of Electronics Communication and Computer Engineering.Volume 3, Issue (1) NCRTCST, ISSN 2249 – 071X
[6] Pennam Krishnamurthy, Mr. M. Maddhusudhan Redddy,” Implementation of ATM Security by Using Fingerprint recognition and GSM”, International Journal of Electronics Communication and Computer Engineering Volume 3, Issue (1) NCRTCST, ISSN 2249 – 071X,(2012)
[7] Robert Hastings, “Ridge Enhancement in Fingerprint Images Using Oriented Diffusion”, IEEE Computer Society on Digital Image Computing Techniques and Applications, pp. 245-252, (2007).
[8] S.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.

Er. Gazal Betab persuing M.Tech in computer science and technology from D.A.V University Jalandhar 2013-2015 and have completed B.Tech in Information Technology 2009-2013 from DAVIET Jalandhar under Punjab technical university with aggregate 73%.

Ranjeet Kaur Sandhu received her bachelorDegree with Honours in Computer science & Engineering from Punjab technical university, Jalandhar in 2008 and M.Tech in computer science & engineering from Punjab Technical University Jalandhar in 2011. She is having five year teaching experience as a Assistant professor. Her interest research includes Cloud computing, Programming languages, Digital image processing especially in Image de-noising and MANET. At present she is working as assistant professor in department of Computer Science & Engineering at DAV University, Jalandhar-Punjab.
Email id : er.ranjeetsandhu@gmail.com