ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 2, August 2013

REVIEW OF BIOMETRIC TECHNOLOGIES USED FOR ATM SECURITY

Namit Gupta[1], Anu Sharma[2]
Department of Computer Science & Engineering, Teerthanker Mahaveer University, Moradabad, UP, INDIA

Abstract- ***Biometric recognition refers to an automatic recognition of individuals based on a feature vector(s) derived from their physiological and/or behavioral characteristic. In order to deal with security, Authentication plays an important role. Biometric recognition systems should provide a reliable personal recognition schemes to either confirm or determine the identity of an individual. Applications of such a system include computer systems security, secure electronic banking, mobile phones, credit cards, secure access to buildings, health and social services. By using biometrics a person could be identified based on "who she/he is" rather than "what she/he has" (card, token, key) or "what she/he knows" (password, PIN). We have also outlined opinions about the usability of biometric authentication systems, limitation, comparison between different techniques and their advantages and disadvantages in this paper. Present study deals with new innovative model for biometric ATMs which replace card system by biometric technology for operating ATMs. Proposed model provides high security in authentication which also protects service user from unauthorized access. In this proposed model user required to authenticate himself with biometric identification (Thumb/ Fingerprint/Iris etc.), Personal Identity Number (PIN) and selection of bank branch from displayed list if necessary. These ATMs talk's to the Farmer in their local languages. This proposed model is designed for the rural farmers, semi-literate peoples. This model reduces complexity with authentication as "authentication is always with you" with high security. It also saves time, cost, and efforts compared with card based ATMs and also saves environmental pollution problem of excess number of plastic cards.***

Keywords**-Biometrics, Multimodal Biometrics, Recognition, Verification, Identification, Security, pattern, authentication.**

I. INTRODUCTION

The word "biometrics" is derived from the Greek words 'bios' and 'metric'; which means life and measurement respectively [5]. "Biometrics" means "life measurement" but the term is usually associated with the use of unique physiological characteristics to identify an individual. A biometric system is essentially a pattern-recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioral characteristic that the person possesses [1]. The physiological characteristics are generally more reliable than one which adopts behavioral characteristics, even if the latter may be easier to integrate within certain specific applications.

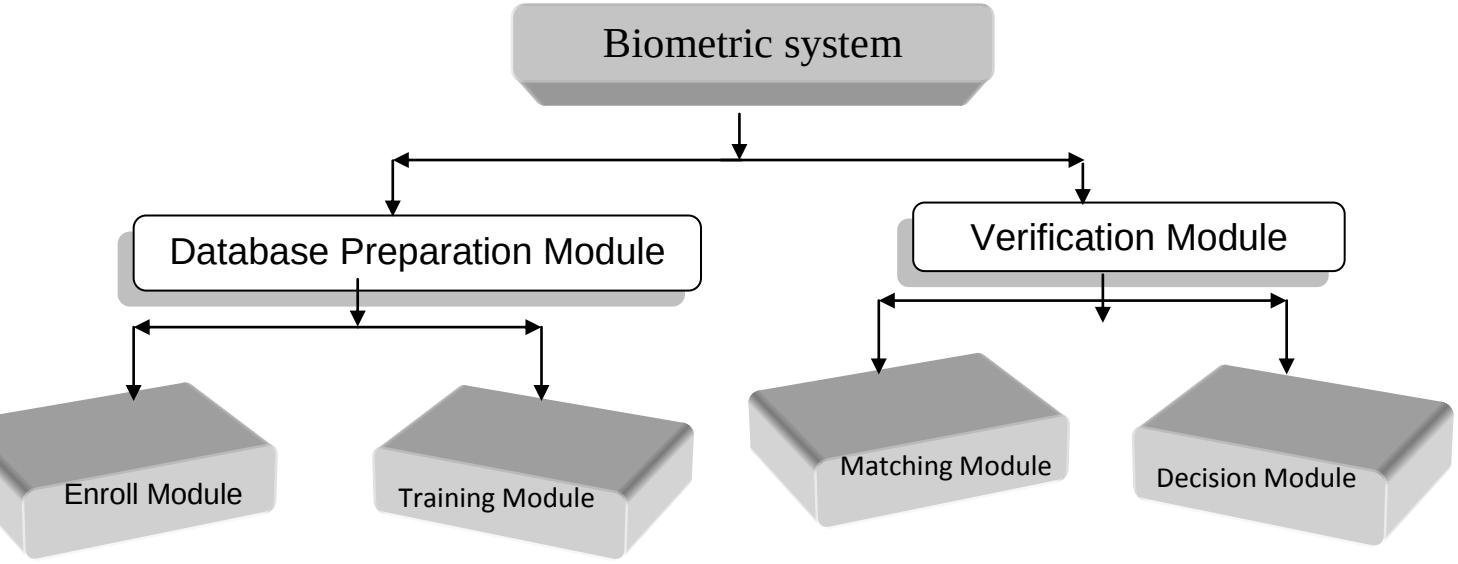

Fig 1: Biometric System

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 2, August 2013

Biometric characteristic	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Facial thermogram	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 I Comparison of various biometric technologies [7]

A. Multimodal Biometric Systems

A multimodal biometric verification system can be considered as a classical information fusion. We can be combine evidence provided by different biometrics system so that we can improve the overall decision accuracy for the system. Those that are utilize more than one physiological or behavioral characteristic for enrollment, verification, or identification. In applications such as border entry/exit, access control, civil identification, and network security, multi-modal biometric systems are looked [2]:

1. Reducing false non-match and false match rates.
2. Providing a secondary means of enrollment, verification, and identification if sufficient data cannot be acquired from a given biometric sample.
3. Combating attempts to fool biometric systems through fraudulent data sources such as fake fingers.

B. Automatic Teller Machine

ATM (Automatic Teller Machine) which is provides customers with the convenient banknote trading are 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. How to carry on the valid identity to the customer becomes the focus in current financial circle. Traditional ATM systems authenticate generally by using the credit card and the password, the method has some defects. Using credit card and password cannot verify the client's identity exactly. In recent years, the algorithm that the fingerprint recognition continuously updated and sending the four digit code by the controller which has offered new verification means for us, the original password authentication method combined with the biometric identification technology verify the clients' identity better and achieve the purpose that use of ATM machines improve the safety effectively [3].

II. TYPES OF ATM ATTACK

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

- Physical attack: Brute force attack to ATM machines with the intention of gaining access to cash within the safe [4].

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 2, August 2013

- ATM Fraud: Theft of bank card information.
- Software and network attack: Theft of sensitive information or controlling ATM spew out bills automatically.

III. BIOMETRIC TECHNOLOGY USED FOR ATM

After feeding your card into the ATM, you place your hand or finger over a scanner which recognizes your unique data to authorize the transaction. From a security point of view I can see that if you do not need to enter a PIN when making an ATM transaction, then your card is less vulnerable to compromise - the magistrate data can still be skimmed, but trapping your card for fraudulent subsequent cash withdrawal would no longer be viable (unless the fraudsters keep you with it, in which case it becomes a duress attack). It would be really interesting to know what the fraud stats show for ATM skimming, when comparing ATMs before and after the introduction of such technology.

An enthusiastic supporter of EMV or Chip and PIN technology, for which the holy grail would be the introduction one day of chip-only cards. Do we really need biometrics for ATM transactions? Something in me is uncomfortable with the thought of entrusting any form of my biometric data to organizations that may lose, misuse, or otherwise fail to properly secure and control it. I am being paranoid, or is keeping such biometric data private one of the last frontiers of individual personal privacy in a world where it is becoming increasingly impossible to remain invisible, and where virtually every phone call, email, website visited, electronic payment transaction and journey made is monitored, recorded, processed and stored by others.

Fig 2: Biometric Technology Used For ATM [6]

A. Limitations Of Biometric Systems Using Any Single Biometric Characteristic [7]

1) ***Noise in Sensed Data*:** Example is a fingerprint with a scare. Noisy data can also result from accumulation of dirt on a sensor or from ambient conditions.
2) ***Intra-Class Variations*:** Biometric data acquired from an individual during authentication may be very different from the data that was used to generate the template during enrollment. This variation is typically caused by a user who is incorrectly interacting with the sensor.
3) ***Distinctiveness*:** While a biometric trait is expected to vary significantly across individuals, there may be large inter-class similarities in the feature sets used to represent these traits. This limitation restricts the discriminability provided by the biometric trait.
4) ***Non-Universality*:** While every user is expected to possess the biometric trait being acquired, in reality it is possible that a group of users do not posses that particular biometric characteristic.
5) ***Spoof Attacks*:** An individual may attempt to forge the biometric trait. This is particularly easy when signature and voice are used as an identifier.

IV. APPLICATION AREAS

While there are many potential applications for biometrics, the primary ones can be divided into the following three categories [8]:

PHYSICAL ACCESS SYSTEMS: These systems "monitor, restrict, or grant movement of a person or object into or out of a specific area" [9]. In these systems, biometrics replace or complement keys, access cards, or security cards, allowing authorized users access to rooms, vaults, and other secure areas. Physical access systems are often deployed in major public infrastructure settings, such as airports, in order to monitor and restrict movements of unauthorized or suspicious persons. In addition to entry to secure rooms, physical access systems, when applied in business settings, include time-and-attendance systems by combining access to a location with an audit of when the authentication occurred.

LOGICAL ACCESS SYSTEMS: These systems "monitor, restrict, or grant access to data or information" [9]. Examples include accessing a computer or network or accessing an account. In logical access systems, biometrics replaces or complements PINs, passwords, and tokens [9].

Because of the tremendous value of information stored on corporate networks and the transaction value of business-to-business (B2B) and business to consumer (B2C) e-commerce, the biometric industry views logical access as a much more lucrative industry segment in the long run than physical access.

ENSURING UNIQUENESS OF INDIVIDUAL: These biometric identification systems typically focus on preventing double enrollment in some programs or applications, such as a social benefits program [8]. The

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 2, August 2013

main use of this application occurs in the public sector although similar systems could be implemented to prevent double enrollment in employee benefits programs.

V. Advantages and Disadvantages of the Various Biometric Technologies

There is no universal "best" biometric authentication system. Each of the five leading biometric technologies carries specific advantages and disadvantages. Some biometric technologies are more appropriate for certain applications and environments than their counterparts. An organization in the midst of evaluating potential biometrics authentication implementation must recognize that there will be trade-offs in any selection, such as cost for accuracy, privacy versus user acceptance, etc., and there are not yet any universal decision factors for selecting a particular biometric technology for a specific application. There is, however, substantial research into many of the advantages and disadvantages of biometrics. Table 3 provides a summarized comparison of the features of the five leading biometric technologies analyzed in this dissertation. The features, shown in the extreme left column, were excerpted from various researcher efforts and the rankings represent an amalgam of the rankings found in the literature [8, 10].

VI. Summary, Conclusion and Recommendation

A. Summary

From the test carried out we have been able to prove that the biometric ATM is practicable and could be implemented in a real production environment. Biometric tokens are the safest means of preventing ATM frauds. The most widely used biometric tokens are finger prints, irises, faces and palms. The fraudster may match everything but they can never match the biometric peculiarities.

B. Conclusion

Biometrics refers to an automatic recognition of a person based on her behavioral and/or physiological characteristics. The main reason for introducing biometric systems is to increase overall security. Biometrics offers greater security and convenience than traditional methods of personal recognition. In some applications, biometrics can replace or supplement the existing technology. In others, it is the only viable approach. Decision-makers need to understand the level of security guaranteed through the use of biometric systems and the difference that can exist between the perception and the reality of the sense of security provided. The biometric system is only one part of an overall identification or authentication process, and the other parts of that process will play an equal role in determining its effectiveness. Supposing biometrics does bring an increase in security. Fingerprint-based systems have been proven to be very effective in protecting information and resources in a large area of applications. . Multimodal biometric systems can integrate information at various levels, the most popular one being fusion at the matching score level. Biometrics the technology developments have been in advance of ethical or legal ones.ATM users for various transactions like withdrawing cash, balance enquiry etc. Point of Sales (POS) machines will also use biometric authentication. This system requires biometric authentication (finger print, iris recognition) which is always with user, PIN code and selection of bank branch, which then creates virtual account (V-ID) it helps for identification and authentication of service user. This is card less e-banking technique for ATMs, which reduces efforts of handling, operating and various risks associated with cards. The same and simplified procedure will be helpful for Internet, Mobile and POS transactions. Due to unique method of authentication it reduces cost, time, and efforts of both banks as well as service users.

C. Recommendation

We recommend the following for future research:

- Using a 3-D API for a Graphical User Interface (GUI). Example is openGL in place of Java Swing API.
- The JDBC architecture can be extended to three-tier using application server like APPLET server, JSPservlet on APACHE thumb card versus database.
- There is need to Develop a fingerprint matching algorithm.

REFERENCES

[1] http://www.nfstc.org/forensic-technology/technology-evaluations/

[2] Smt Pranali Ravikant Hatwar, Ravikant B Hatwar, Bio-signal based Biometrics Practices: International Journal of Creative Research Thoughts, Volume 1, Issue.4, April 2013, pp-1-9.

[3] 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 pp-83-86.

[4] http://www.grgbanking.com/en/exh/images/Best%20Practice%20for%20ATM%20Security %20- GRGBanking. Pdf.

[5] http://thesingularityeffect.wordpress.com/biometrics/biometrics-defined/.

[6] http://www.finextra.com/community/fullblog.aspx?blogid=4419.

[7] A. K. Jain, A. Ross, S. Prabhakar, "An Introduction to Biometric Recognition", IEEE Trans. on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp 4-19, January 2004.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 2, August 2013

[8] Bolle, Connell, Pankanti, Ratha, & Senior, 2004; Nanavati, Thieme, & Nanavati, 2002 (Nanavati, Thieme, & Nanavati, 2002, p. 14.

[9] Harris & Yen, 2002; Kleist, Riley & Pearson, 2005; Woodward, Orlans, & Higgins, 2003).

AUTHOR BIOGRAPHY

Namit Gupta is born in India. He completed his B.Tech from MIT, Moradabad in 2002. He completed M.Tech (CSE) from Teerthanker Mahaveer University in 2012. He is having experience of more than 10 years. Presently working as an Assistant Professor in Teerthanker Mahaveer University, Moradabad (U.P).

Anu Sharma is born in India on November 18, 1984. She completed her B.Tech from N.C College, Israna, Panipat (haryana) in 2006. She completed M.Tech (CSE) from MMEC, Mullana, Ambala (haryana) in 2011.She is having experience of more than 6.5 years. Presently working as an Assistant Professor in Teerthanker Mahaveer University, Moradabad (U.P).

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 2, August 2013

APPENDIX

Finger Scan	Facial Scan	Hand Scan	Iris Scan	Voice Recognition
Accuracy	High	Low	Medium	Very High	Low to Medium
Ease of Use	High	Medium	High	Low to Medium	High
User Acceptance	Medium	High (overt) Low (covert)	High	Low to Medium	High
Privacy Concerns	High	Very High (overt)	Medium	High	Very Low
Cost	Low to Medium	Low to Medium	Medium	High	Low
Performance	High	Low	Medium	High	Low
Potential for Circumvention	Medium	High	Low to Medium	Very Low	High
Distinctiveness	High	Low	Medium	Very High	Low
Barriers to Universality	Worn ridges; hand or finer impairment	None	Hand impairment	Visual impairment	Speech impairment
Susceptibility to Changes in Biometric	Low to Medium	Medium to High	Medium	Low	Low to Medium
Susceptibility to Changes in the Environment	Low	High	Very Low	Low	Medium to High

Table 2 (a) Comparison of Leading Biometric Technologies

Finger Scan	Facial Scan	Hand Scan	Iris Scan	Voice Recognition
Error-causing Factors	Age, trauma, degradation of prints	Lighting, contrast, pose, movement, expression	Hand injury or trauma, inability to place correctly	Positioning, eye angle, glasses, disease	Illness, age, quality of communication system, ambient noise
Mitigations for Potential Errors	Periodic reenrollment, enrollment of multiple fingers	Frequent reenrollment, multiple scans, controlled environment	Periodic reenrollment, enrollment of both hands	Periodic reenrollment, user training, enroll both irises	Periodic reenrollment, control ambient noise

Table 2 (b) Comparison of Leading Biometric Technologies