International Journal of Research in Engineering, Science and Management
Volume-2, Issue-5, May-2019
www.ijresm.com | ISSN (Online): 2581-5792

Controlling ATM Scams using Biometrics System

Shruthi J. Shetty[1], Pavan Kamath[2], Rakshith Rai[3], Prasanna[4], Rakesh Kotian[5]
[1]*Assistant Professor, Dept. of Computer Science and Engg., Alva's Inst. of Engg. & Tech., Moodbidri, India*
[2,3,4,5]*Student, Dept. of Computer Science and Engg., Alva's Inst. of Engg. & Tech., Moodbidri, India*

***Abstract*: Atm are electronic machines used in different places and the customer can carry transactions without the help of bank staffs. With the help of this atm an user can do various banking activities like cash withdrawal, paying of electricity and phone bills. Authentication and verification is major concern nowadays. If an atm pin is hacked by someone there is risk of losing moneys. To overcome this problem we needed to add more security to a current automated teller machine. Biometrics is one of the systems that are being integrated with the current atm technology to provide high security. By this security frauds in atm can be controlled easily by the methods like face recognition, fingerprint, and iris scanning. This paper consists of multimodal biometrics which tells us about integrating different biometrics system in an atm, different methodologies adopted and the working of the system. Biometrics provides us high security in authentication thereby preventing from unauthorized access.**

***Keywords*: Biometric, Fraudulent, Multimodal, Hurdle.**

1. Introduction

Atm provides us with easy and convenient way to carry out all our banking tasks. Atm provides us with non-stop cash solutions and is almost popular in all over the country. ATM card or debit card authenticates a person after his/her verification. ATMs uses pin based security to carry out transactions. This is pin as fed as input which is encrypted at the client side and decrypted at the server side. After the match transaction is carried out. inspite of this advantage fraudsters have led a lot of attack on this machine. day by day the technology is getting improved making this pin data to be retrieved and frauds on going on increasing. Passwords and PIN numbers are the key targets to be stolen or discovered by any means and retrieving, it can be exploited by people with criminal mindset over the internet and also at other business places. Since the data are available on cloud, data is retrieved and this is major drawback. Hence this made a call for the biometrics systems to be integrated in the atms. A biometric system is essentially a pattern recognition system that recognizes a person based on feature vector derives from physiological or behavioral characteristics that the person possess. Hence the reason of adding a higher security that is biometrics to the current technology to reduce the fraudulent attack. Biometric security eliminates the need of multi password authenticating system, thereby getting the entire access control by finger touch, face recognition or iris scanning. Biometric security can be easily adopted with the traditionally used techniques in financial organizations banks. Smart cards, ATMs, credit and debit cards, it may work as standalone or in combination with pin to security identify user as a genuine owner of the card and the person who has permission to exchange money. Biometric has emerged as a measure for highly secure identification and personal verification. To conduct the verification biometric system requires a sensor every time to collect the biometric sample. This sensor is exposed to dusty, sweaty and oily hands depending on person to person thus effects the sensitivity of sensor to gather the accurate sample for verification, even it implements multiple algorithms for matching purpose.

2. Multimodal biometric in atm system

Multi biometrics is the combination of one or more biometrics. It overcomes the problems of unimodal biometrics. This system is more reliable due many pieces of evidences. Based on multiple sources multi biometrics are classified as Multi sensor systems, multi algorithm system, multi sample system. The finger print, iris, face is used to provide security. In multimodal biometrics the advantage is if one system fails we can use another system. The system flows like the person needs to insert atm card and enter the pin number, if it is valid then it undergoes for face scan, and other biometrics is are verified. Templates are created which are being matched with the template stored in database in the enrollment phase and the user will be able to access the account.

3. Methodologies

There are many ways for biometrics scanning below are four commonly used biometrics methods in ATMs.

A. Iris recognition

Iris recognition technology captures the intricate iris patterns with a help of an iris scanning devices. This data is then digitalized and stored in a database for future reference along with some other patterns like name and address. Iris data is more reliable and database because this iris is covered by a protective sheath which protects it from damage. Due to this durability iris recognition system requires only a single enrollment. Other technologies are subjected to wear and tear

due to nature of the work environment which requires repeated enrollment.

The iris is a muscle within the eye that regulates the amount of light entering the eye by controlling the size of pupil. The system is to be composed of a number of sub-systems, which corresponds to every stage of iris recognition technique. Iris based biometric ATM's are more secure than conventional pin based ATM's because it requires biometric verification which cannot be stolen, copied or faked.

B. Signature recognition

Handwritten signature authentication is based on systems for signature verification and signature identification. Whether the given signature belongs to a particular person or not is decided through a signature identification system. Whereas the signature verification system decides if a given signature belongs to a claimed person or not. Signature-based authentication can be either static or dynamic.

In the static mode (referred to as off-line), only the digital image of the signature is available. In the dynamic mode, also called "on-line", signatures are acquired by means of a graphic tablet or a pen-sensitive computer display. A signature is a biometric attribute created by a complex process originating in the signer's brain as a motor control "program", implemented through the neuromuscular system and left on the writing surface by a handwriting device. Consequently, signature-based identification and verification is also considered as an important authentication technique among all of the most popular biometric-based authentication methods in the area of personal identification.

C. Face recognition:

Face recognition system is a one type of biometric computer application which can identify or verify a person from a digital image by comparing and analysing patterns. These biometric Systems are used in ATMs. Present facial recognition systems work with face prints and these systems can recognize 80 nodal points on a human face. Nodal points are nothing but end points used to measure variables on a person's face, which includes the length and width of the nose, cheekbone shape and the eye socket depth. Face recognition systems work by capturing data for the nodal points on a digital image of a person's face and resulting data can be stored as a face print and the person is not aware of being scanned. When the conditions are favorable, these systems use a face prints to identify accurately.

D. Fingerprint recognition

Fingerprint Recognition includes taking a fingerprint image of a person and records its features like arches, whorls, and loops along with the outlines of edges, minutiae and furrows.it is one of the oldest personal identification and extensively used today. Matching of the Fingerprint can be attained in three ways, such as minutiae, correlation and ridge. To capture the fingerprints, present methods employ optical sensors that use a CMOS image sensor or CCD; solid state sensors work on the principle of transducer technology using thermal, capacitive, piezoelectric sensors or electric field or ultrasounds sensors work on echography in which the sensor sends acoustic signals through the transmitter near the finger and captures the signals in the receiver. Scanning of the fingerprint is very stable and also reliable. It safeguards entry devices for building door locks and access of computer network is becoming more mutual. At present, a small number of banks have initiated using fingerprint readers for approval at ATMs.

4. Working of biometric system

Biometrics systems work by recording and comparing characteristics as shown in Fig (1). There are two phases. First is the enrollment phase second is the verification phase. In enrollment phase, that is when an individual uses biometric system initially the individual identifying features are enrolled as a reference for future comparison and this reference is stored in a database. The verification phase involves these steps:

- *Collection of data:* This is the first step where a user encounters a physical contact with sensing device data is presented to the captured device.
- *Pre-processing:* In this step there is Enhancing of the quality of the captured biometric data. The removal of noise and distortion takes place.
- *Feature extraction:* In this stage the biometric data is recorded, the preprocessed data is reprocessed and with limited size.
- *Creation of Template:* Template is a model that is created for comparison. This template is relayed for matching algorithm.
- *Matching:* This is the final stage which involves the implementation of comparison algorithms. Template stored is matched with the collected sample that is in the database to grant or deny access.

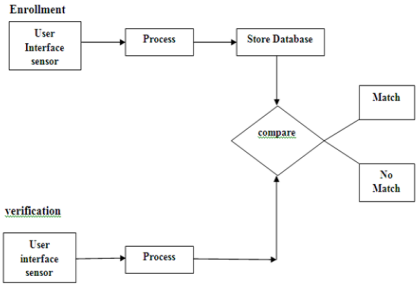

Fig. 1. Block diagram of working of biometrics system

5. Conclusion

The use of biometrics as password has made atm transaction system more reliable and secured. Moreover, the system is built on embedded technology which makes it user friendly and secure. Biometrics security system has revolutionized the people general perceive security. The only hurdle is that the people must accept theses biometric system. Biometric system

with the existing system and technology can produce a very well protected system.

References

[1] Namit Gupta & Anu Sharma, “Review of biometric technologies used for atm security,” in International Journal of Engineering and Innovative Technology, vol. 3, no. 2, pp. 460-465, August 2013.

[2] S. Singh, A. Singh and R. Kumar, "A constraint-based biometric scheme on ATM and swiping machine," *2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT)*, New Delhi, 2016, pp. 74-79.

[3] P. C. Mondal, R. Deb and M. N. Adnan, "On reinforcing automatic teller machine (ATM) transaction authentication security process by imposing behavioral biometrics," *2017 4th International Conference on Advances in Electrical Engineering (ICAEE)*, Dhaka, 2017, pp. 369-372.

[4] A. T. Siddiqui, "Biometrics to Control ATM scams: A study," *2014 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2014]*, Nagercoil, 2014, pp. 1598-1602.

[5] V. Rajesh and S. Vishnupriya, "IBIO-A new approach for ATM banking system," *2014 International Conference on Electronics and Communication Systems (ICECS)*, Coimbatore, 2014, pp. 1-5.

[6] A. Taralekar, G. Chouhan, R. Tangade and N. Shardoor, "One touch multi-banking transaction ATM system using biometric and GSM authentication," *2017 International Conference on Big Data, IoT and Data Science (BID)*, Pune, 2017, pp. 60-64.

[7] Okechukwu Onyesolu, “ATM Security Using Fingerprint Biometric Identifer: An Investigative Study,” 2012.

[8] G. R. Jebaline and S. Gomathi, "A novel method to enhance the security of ATM using biometrics," *2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015]*, Nagercoil, 2015, pp. 1-4.