Card-less ATM Transaction Using Biometric And Face Recognition– A Survey

Manish C M [1], N Chirag [1], Praveen H R [1], Darshan M J [1], D Khasim Vali [2]

[1, 2] Department of Computer Science and Engineering
Vidyavardhaka College of Engineering, Mysuru, Karnataka India

[2]dkv@vvce.ac.in

Abstract

A fraud attacking the Automated Teller Machine (ATM) has increased over the decade which has motivated the use of biometrics with image for personal identification to procure high level of security and accuracy. The project describes a system that replaces the ATM cards and PINs by the physiological biometric fingerprint authentication and face recognition. Moreover, the feature of one-time password (OTP) imparts privacy to the users and emancipates him/her from recalling PINs. In this system during enrollment the genuine user's fingerprint and face is retained in the database. The process of transaction begins by capturing and matching fingerprints and face patterns. The system will automatically distinguish between real legitimate trait and fake samples. A GSM module connected to the Microcontroller will send a 4-digit code (OTP) generated by the system to the registered mobile number. After the valid OTP is entered the user can perform banking transaction. In any kind of fake access attempts the account is blocked and the image of the person will be captured and transmitted via email.

Keywords: ATM, Biometric, Fingerprint authentication, Face recognition, Face patterns, PINs, GSM, OTP.

1 Introduction

ATM can be described as Any Time Money. We can get money at anytime anywhere only through ATM machines. To do the secure transactions we need biometric authentication. Biometric authentication is a growing and controversial field. Today biometric laws and regulations are in process and biometric industry standards are being tested. According to, there are three popular attacks against ATM: Skimming, PIN logging and Integrity violation. There are also attacks against mobile phone: Fake mobile apps installation, key logging software and grab PIN number during transmission. Besides that, an attack may also be a combination of both types of said attacks.

Information also can be exploited by a side channel attack. It is found that attackers try to get the user's account information that stored on the magnetic strip present at the back side of ATM card. Password is the only identity that can use to authenticate the owner of ATM card. It means anyone can access the account bank through ATM machine as the password entered is correct. So, once the ATM card and password is lost or stolen by anyone, they can withdraw the money from that account easily without the problem of user authentication. Thus, it can see that the most serious issue raised in ATM card security is about user authentication. User authentication is important because it lead to the integrity violation of bank account information. It seems that this issue is worse as anyone can access all information stored when they entered the correct password towards accessing ATM card at ATM machine. Other than that, it is strongly emphasized that the security issues need technology improvements and better security policy as a countermeasure.

First, the bankers collect customers' finger prints, facial ID and mobile numbers while opening accounts, then customer only access ATM machine. The working of the ATM machine is such that when a customer place a finger on the finger print module it automatically checks to give authorization for the transaction and its followed by a face recognition. And when both are checked out, it then 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. Biometrics can be defined as 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.

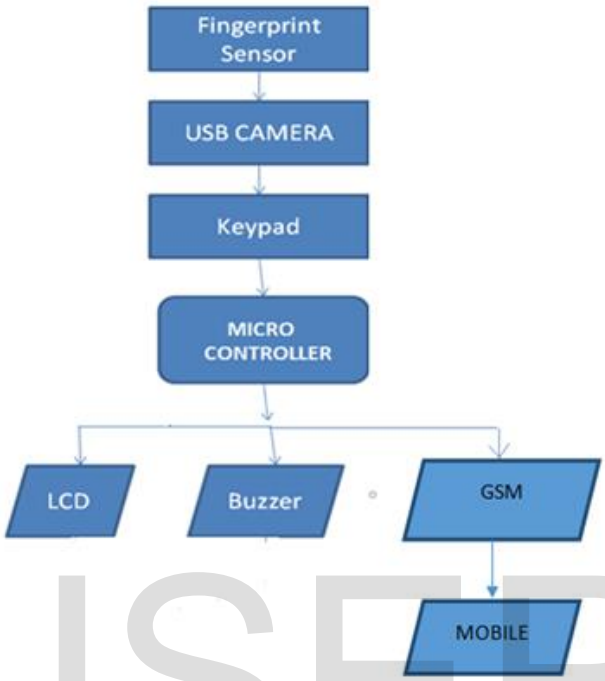

Figure 1.1 Flowchart of the working model

2. Literature Survey

A survey, as a comparative case study is given in the Table I. It deliberates the biometric and facial recognition techniques in enhancing the security for Card-less ATM transaction.

TABLE I : Literature review table

Title of the paper	Technology / Methods	Advantages	Disadvantages
Enhanced ATM security system using biometrics (2012) [1]	Finger print biometric token.	• Developed an ATM based fingerprint verification and simulated it for ATM operations by incorporating the fingerprints of users into the bank's database.	1. As there was no algorithm for finger print matching, the system became inefficient. 2. The system build does not enhance the existing system.
A new business model for ATM (2013) [2]	Finger print recognition in digital image processing using both primary and reference fingerprint to authenticate users instead of the traditional pin number	• A new business model which would enhance ATM security was proposed.	1. The method used here could be a way for security breech which is accepting a reference fingerprint which may belong to a family member of the nominee. 2. The existing system was not considered while preparing the proposed system.
Enhancing Security by averaging multiple fingerprint images (2013) [3]	A combination of fingerprint biometric token and GSM technology	• Proposed a system architecture that incorporates both the finger print and GSM technology into the existing PIN-based authentication process.	1. Another reference method used here could be a way for security breech which is accepting a reference fingerprint which may belong to a family member of the nominee.
Enhanced Automated Teller Machine using Short Message Service authentication	Short Message Service (SMS) verification.	• Developed an algorithm for enhancing ATM authentication	1. The system proposed here only accepts a minimum withdrawal amount, which when

verification (2014) [4]		system using Short Message Service (SMS) verification. • Conducted a usability testing of the proposed system	exceeds the system will not proceed.
A Self Banking Biomtric M/C with Fake Detection Applied to Fingerprint and Iris along with GSM Tech. for OTP (2016) [5]	RFID, Biometric and GSM	• Trusted Authentication • Increases the security • High accuracy	1. Maybe GSM module or network failure occurs
A Constraint- based Biometric Scheme on ATM and Swiping Machine (2016) [6]	Electronic data capture (EDC)	• Durability of sensor • Security and reliability	1. Time consumption, noise and sensor issue
Biometrics in Human-Machine Interaction (2015) [7]	Human-Machine interaction technologies, decision making techniques.	• Provide decision making support to system	1. System needs to be sensitive to cultural differences, facial expressions.
A Novel Method to Enhance the Security of ATM using Biometrics (2015) [8]	Encryption and decryption, blowfish algorithm , binaized fingerprint images and Gray scale fingerprint image.	• Reduces the time and the bandwidth required for the transmition. • Provide the security.	1. Identify the core points image fed may vary in angle.
Biometric quality: a review of fingerprint, iris and face (2014) [9]	QA algorithm	• Strong performance	1. More noise created
SHORT TERM FACE RECOGNITION FOR AUTOMATIC TELLER MACHINE (ATM) USERS (2013) [10]	Magnetic stripe for data storage	• Data can be altered if necessary. • Inexpensive.	1. Breakable data can be destroyed.
ATM terminal design is based on fingerprint recognition (2010)	ARM 9, GSM, Gabor filter algorithm and direction filter.	• Stability and reliability of finger print characteristics. • Security.	1. Fingerprint image contains a lot of noise, thus, it is time consuming.

[11]			

Conclusion

The use of the biometrics has made the ATM transaction system more reliable and secured. The OTP and face recognition concept added to the system further enhances the security and avoids the need to remember passwords. Moreover, the system is built on embedded technology which makes it user friendly and non-invasive. The time taken for the overall ATM transaction is reduced for each user in comparison to the traditional ATM transaction systems. Comparing the proposed system with the previous ATM transaction systems, it shows that the accuracy and security of the proposed system is maximum and more efficient. The proposed system provides greater degree of security and convenience to the users for easy, fast and Card-less ATM transactions.

Acknowledgment

The authors express gratitude towards the assistance provided by our mentors and faculty members who monitored us throughout the research and helped us in achieving desired results in given time.

References

[1] Oko, S. and Oruh, J. (2012): Enhanced ATM security system using biometrics. IJCSI International Journal of Computer Science Issues, September 2012. Vol. 9, Issue 5, No 3, pp. 352-357.

[2] Ravikumar, S., Vaidyanathan, S., Thamotharan, S. & Ramakrishan, S. (2013), A new business model for ATM

[3] Maninder Singh, Shahanaz Ayub and Raghunath Verma, "Enhancing Security by averaging multiplefingerprint images," Proc. International Conference on Communication Systems and Network Technologies, IEEE 2013.

[4] Jimoh, R.G. and Babatunde, A. N. (2014). Enhanced Automated Teller Machine using Short Message Service authentication verification. World Academy of Science, Engineering and Technology. International Journal of Computer, Information Science and Engineering 2014. Vol:8 No:1 pp.14-17

[5] Joyce Soares, A. N.Gaikwad "A Self Banking Biomtric M/C with Fake Detection Applied to Fingerprint and Iris along with GSM Tech. for OTP," International Conference on Communication and Signal Processing, April 6-8, 2016,India.

[6] Shweta Singh , Akhilesh Singh, Rakesh Kumar, "A Constraint- based Biometric Scheme on ATM and Swiping Machine," 2016 International Conference on Computational Techniques in Information and Communication Technologies(ICCTICT).

[7] W. A. Shier, S. N. Yanushkevich "Biometrics in Human-Machine Interaction," The International Conference On Information and Digital Technologies2015.

[8] G. R. Jebline, S. Gomathi," A Novel Method to Enhance the Security of ATM using Biometrics", 2015 International Confernce on Circuit, Power and Computing Technologies [ICCPCT].

[9] Samarth Bharadwaj, Mayank Vatsa* and Richa Singh, "Biometric quality: a review of fingerprint, iris,and face,"Bharadwaj et al. EURASIP Journal on Image and Video Processing2014,2014:34http://jivp.eurasipjournals.com/content/ 2014/1/34

[10] Ekberjan Derman#1, Y. Koray Gecici#2, Albert Ali Salah*, "SHORT TERM FACE RECOGNITION FOR AUTOMATIC TELLER MACHINE (ATM) USERS," 978-1-4799-3343- 3/13/$31.00 ©2013IEEE.

[11] Yun Yang , JiaMi, "ATM terminal design is based on fingerprint recognition,"

978-1-4244-6349-7/10/$26.00 ©201 0 IEEE.