Asian Journal of Convergence in Technology Volume IV, Issue I
Issn No.:2350-1146, I.F-5.11

Fingerprint based biometric authentication for ATM system

V. P. Baraskar[1], R. R. Gawande[2], P. R. Jibhakate[3], U. D. Dattasamje[4], A. S. Chandak [5]
(E&Tc, Modern Education Society's College of Engineering, Pune, Savitribai Phule Pune University, India)
vaibhavbaraskar51@gmail.com [1], jpranjali1309@gmail.com [2], grashmee511@gmail.com[3], ulbiradar@mescoeune.org [4], aschandak@gmail.com [5].

***Abstract*—In this modern world, technologies are rapidly transforming. The technology provides simplicity and comfort yet in addition brings a major worry for security. So to increase the security to the present ATM framework, biometric and GSM technology can be used. In this paper, we proposed a system in which banker will collect customer's fingerprint and mobile number while opening accounts and at that point just client will have the capacity to get to ATM machine. The essential advance of this framework is to check as of now filtered unique mark with enrolled fingerprints. If these fingerprints are matched, then an OTP will send to the customer's mobile using GSM technology. This system needs fingerprint scanner, card reader and raspberry pi is used to interface all components.**

Keywords— *Biometric, fingerprint, authentication, raspberry pi, card reader,OTP.*

I. INTRODUCTION

Now-a-days many people use ATM technology. The use of ATM allows customers to pay house bill, phone bill, electricity bill [1]. ATM provides facilities to fast and easy access to back account and thus allows financial transaction conveniently. PIN or password is used to secure unauthorized access to the account. However financial crimes are increasing day by day. Criminals steals user's credit card and password is stolen, the criminal will take all the cash and will lead to financial losses to customer [2].

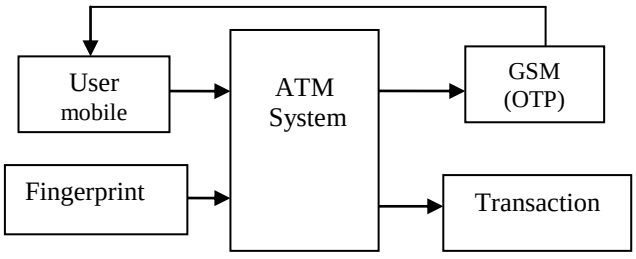

Fig1. General system diagram

The main objective of this system is to research the scope of biometric techniques for authentication in ATMs. In this system, the standard of identification is the fingerprint information of customer. This system has two modes: 1) Fingerprint recognition 2) password recognition.

Finger scan verification and identification involves five stages: fingerprint image acquisition, image processing, and location of distinctive characteristics, creation of template and matching of templates. Some people have faint or hard to obtain finger impression whether because of wear and tear of biological traits [3].

The rest parts of paper consist of: Section II having papers studied before to define problem and solution approach. Section III highlights the working of the system. Section IV concludes the paper and focuses on future scope of the system.

II. LITERATURE SURVEY

Fingerprint technology is proved to be unique mark innovation and gives high level of exactness. There are various biological attributes such as iris and retina which are more accurate than finger impression, yet mechanized ID innovation fit for using these qualities have been created in past couple of years. The innovation has become smaller, more competent and with numerous arrangement accessible. Gadgets somewhat thicker than a coin and in square in size can catch and process picture. Biometric template cannot be figured out to reproduce individual personal data and they can't be stolen and used to get individual data [3]. Some papers [4-6] have been proposed the way to deal with bring down the time and space complexity of unique finger impression coordinating. By including their idea to our framework, can enhanced general performance of the system. U.Jayaram [5] has characterized how unique mark confirmation plan could be enhanced to diminish time of check. Authors of [7, 8] analyzed the performance of system by comparing with other schemes. R.S.Germain [9] has defined clustering component to accelerate matching to biometric process. Namrata [1] has explained the various biometric technologies and compared those technologies to decide which one is suitable for various applications. The idea of cryptography and steganography are known to us. In unique finger impression based ATM framework, they mean to utilize the unique mark based picture caught by finger impression scanner [10]. Ahmad Tasnim Siddiqui has summarized various ways of biometric scanning such as fingerprint

verification, face recognition, scanning of retina, scanning of hand geometry, vein geometry recognition, iris scanning, Signature biometrics, voice analyzing [11].

III. METHODOLOGY

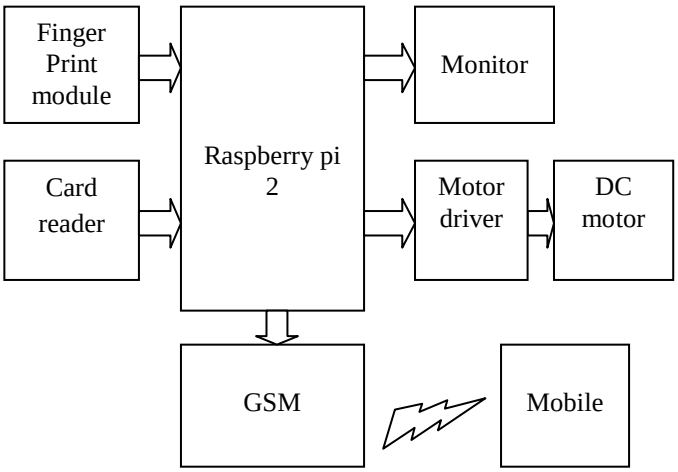

Fig2. Block diagram

The block diagram consists of various blocks such as fingerprint module,GSM module, monitor screen keyboard DC motor, card reader. All these module are connected to each other via raspberry pi 2. There are some module consisted as follows:

Raspberry pi is a series of small single board computer. It is based on linux operating system. Python is used for programming the raspberry pi.

Fingerprint recognition module R305 is optical fingerprint sensor. It has life of 100 millions time.It can be interface via USB1.1 or UART. Verifiaction speed is 0.3 sec and scanning speed is 0.5 sec.

Monitor of laptop is used for display purpose and **keyboard** is used for entering OTP and choosing options.

GSM module is used to send the OTP generated to user's mobile phone. GSM Sim900 provides features to send or receive the message . It is compatible with AT cellular commands. IT has built in simcard holder.

Smart card reader is designed for sle 4442 type of smart cards, bit wise addressable(256), 8 bit EEPROM.It uses half- duplex transmission protocol. It is easy to install, use and integratein a computer based system.

Software design

This system follows the step given below:Initially for implementing the systemcontact number and finger impression of account holder is necessary. This information is stored in data base while opening account in bank. Firstly, customer swipes the credit card.Then he asked to scan finger.when finger imression scanned matches with the stored one, then OTP is generated and sent to the user. Otherwise the process will be interupted and need to start from first step. When user receives the OTP, he has to enter that. Again OTP will be verified and then will continue with the transaction.

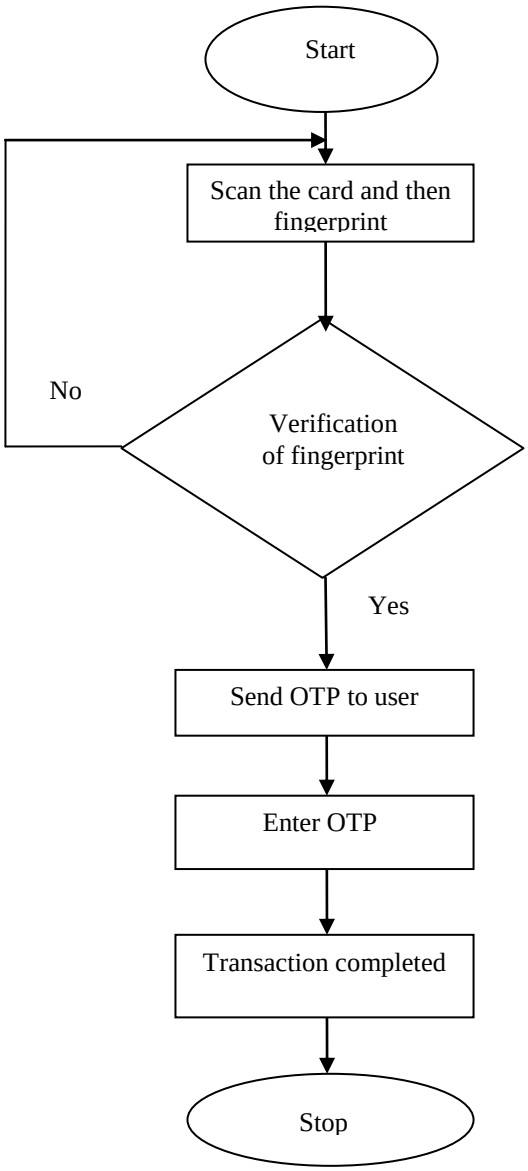

Fig3. Software Design Flow

IV. RESULT

The model for ATM system authentication based on fingerprint identification is executed. In fig.4 we interface the fingerprint module with raspberry pi. We implemented the

enrollment and verification of the fingerprints as shown in fig5-6.If the fingerprint matches then OTP will be generated. Then user has to enter the OTP in the window as shown in fig 7.

Fig4. Interfacing Fingerprint module

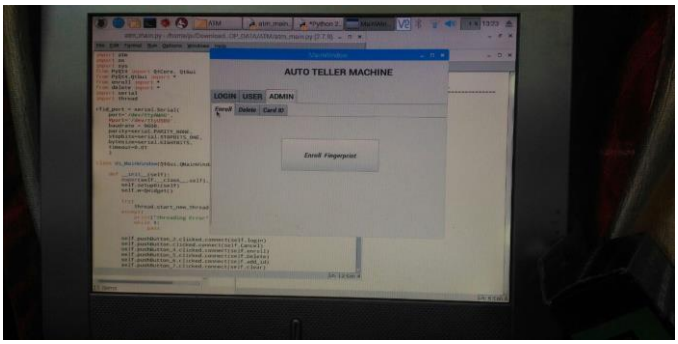

Fig5.Fingerprint enrollment

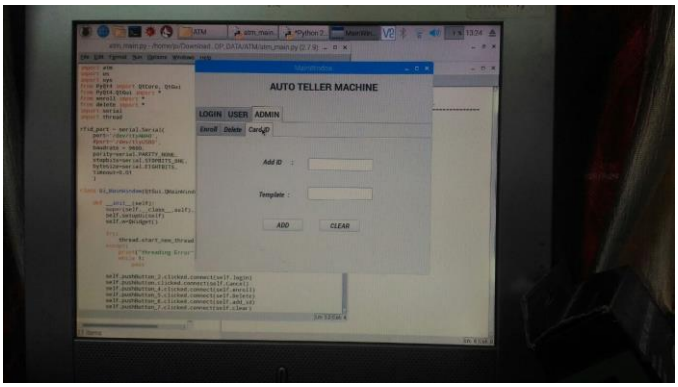

Fig6.Template creation

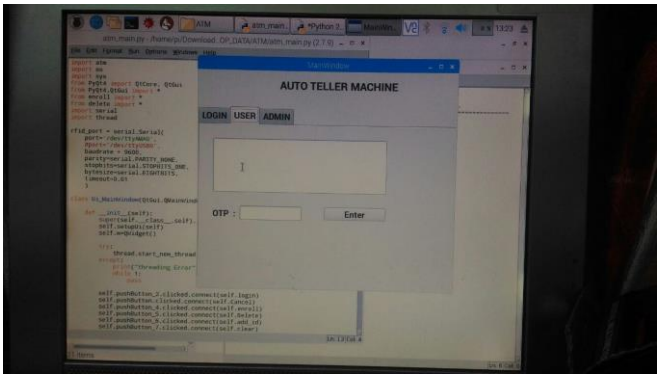

Fig7.Entering OTP

V. CONCLUSION

This paper is all about the secured authentication to the ATM system. This system consists of Monitor & Keyboard of laptop fingerprint module, GSM module, card reader and Raspberry pi 2. Here we are using DC motor to see output i.e. when the finger prints will be verified, the dc motor will indicate the transaction done. This system is suitable for illiterate people also. This system gives advantages as the biological traits can't be lost or forgotten or copied. In case of emergency, if the user is unable to come to ATM machine. This is the limitation to the proposed system. So we can improve the system for two or three nominees. Also security level can be increased.

REFERENCES

[1] Namrata & Dr. Sukhvir Singh, "Review paper on enhanced the ATM security using fingerprint recognition", International Journal of Computer Science and Mobile Applications, Vol.3 Issue. 10, 2015, pp. 38-47 ISSN: 2321-8363.

[2] Jaydeep Shamdasani & Prof. Pravin Matte, "ATM client authentication system using biometric identifier & OTP", International Journal of Engineering Trends and Technology (IJETT) – Vol. 11 Issue 5, 2014, pp. 255-258. ISSN: 2231-5381.

[3] Dhiraj Sunehra, "Fingerprint based biometric ATM authentication system", International Journal of Engineering Inventions, Vol. 3, Issue 11, 2014 pp: 22-28, e-ISSN: 2278-7461, p-ISSN: 2319-6491.

[4] S. Barman, S. Chattopadhyay, D. Samanta, S. Bag& G. Show, "An efficient fingerprint matching approach based on minutiae to minutiae distance using indexing with efficiently lower time complexity" International Conference of Information Technology,2014, pp: 179-183.

[5] U. Jayaram, J. Viswanthan, A.K. Gupta, P. Gupta, "Minutiae based geometric hashing for fingerprint database" International Conference on Intelligent Computing, 2012.

[6] R.Boro, S.D. Roy, "Fast and robust projective matching for fingerprint using geometric hashing" In proceeding on Computer Vision, Graphics and Image Processing, 2004, pp: 681-686.

[7] P. Grother and E. Tabassi, "Performance of biometric quality measures" IEEE Transaction on Pattern Analysis and Machine Intelligence, Vol. 29 Issue 4, 2007, pp: 531-543.

[8] D. A. Kumar and T.U.S.Begam, "The comparative study of fingerprint matching algorithms for EVM", Journal of Computer Sciences and Applications, Vol. 1, Issue 4, 2013, pp: 55-60.

[9] R.S. Germain, A. Califano and S. colville, "Fingerprint matching using transformation parameter clustering", IEEE Computing in Science and Engineering, Vol. 4, Issue 4, 1997, pp: 42-49.

[10] Nisha Bhanushali, Meghna Chapaneria, Krishani Mehta, Mansing Rathod, "Fingerprint based ATM system", Journal for Research, Vol. 2, Issue 12, 2017, pp: 31-34, ISSN: 2395-7549.

[11] Ahmad Tasnim Siddiqui, "Biometrics to control ATM scams: A study", International Conference on Circuit, Power and Computing Technologies, 2014, pp: 1598-1602.