ATM Transaction Security Using Fingerprint/OTP

[1]Krishna Nand Pandey, [2]Md. Masoom, [3]Supriya Kumari, [4]Preeti Dhiman
[1,2,3,4]Electronics & Instrumentation Engineering, Galgotias College of Engineering & Technology
Greater Noida, Uttar Pradesh- 201308, India

***Abstract-* This paper deals with the solutions related to the ATM security. We are going to make use of fingerprint or One Time Password (OTP) verification along with the use of ATM pin. In this system, the user can have third party authentication either temporary or permanent. In the whole process, the first party i.e. the banker will maintain a database of the customer including fingerprint and mobile number. The banker will provide the ATM card along with its PIN. For the transaction after entering the ATM pin, the customer will be asked to choose an option either fingerprint or OTP verification. The OTP will be sent to the registered mobile number of the customer through GSM module connected to the system. After authorised verification, the customer will be able to proceed for transaction else after three successive wrong attempts, the ATM card will be blocked for 24 hours and a message will be sent to the registered mobile number.**

***Keywords*- ATM, OTP, fingerprint, ATM pin, mobile number, microcontroller.**

I. INTRODUCTION

With the advent of modern technology, there is a drastic increase in fraud. One easy way is ATM fraud which includes fraudulent cash transactions so there is a need to regularly develop consumer favourable systems to deal with these frauds related to ATM transactions may be of several ways viz. Eavesdropping, Spoofing, Skimming Attack, Card Trapping, PIN Cracking, Phishing Attack, ATM Malware, ATM hacking [5],[6].

Several biometric authentication methods can be used to minimise such cases which includes fingerprints, face, iris before any transaction through ATM.

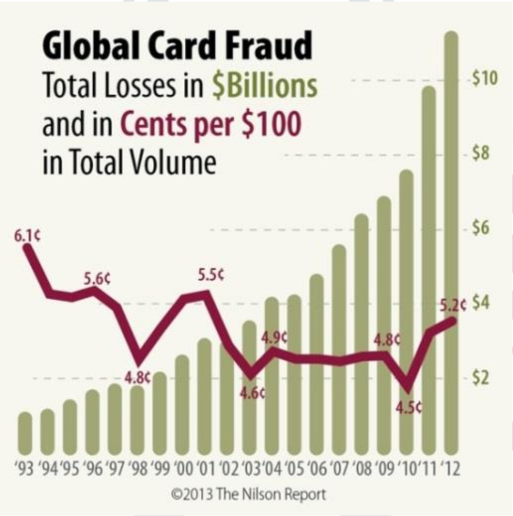

Fig.1 Chart Representing Global Card Fraud

One approach to deal with ATM frauds is face detection technology [1]. Here the transaction is allowed if and only if the face of the user is detectable. But it has a drawback that it does not authenticate the legal user of the ATM and instead it just asks for detectable face of suspects who tend to hide their face.

Another approach is the iris recognition system. It has very high accuracy in verifying an individual's identity [2]. It works on four steps- image acquisition, segmentation, encoding and matching but work is still going on to make this technology feasible and cost effective.

The third approach is Palm Vein Technology to run financial transactions. In this system, the user is required to provide his/her palm vein since these veins are unique for each individual. It is being practised in Japan. But it requires an overall update of database which is a tedious and costly process [3].

A better approach is a combination of fingerprint and One Time Password (OTP) authentication along with ATM pin. It is cost effective and user friendly method since all the required data is already available in the database of the banker [5],[7][8],[10].

In this system, the user is required to enter the ATM pin, after inserting the ATM card. Immediately after that the user will be asked to choose between two methods, either fingerprint or OTP. By selecting the fingerprint option the user will get two options- Admin mode and Transaction mode. The user may proceed with transaction mode to carry out financial transactions. In admin mode, user can add another authorised person by adding his/her fingerprint (only for transaction purpose). Also user can add/change the customer's registered mobile number [4],[5].

If the user selects the OTP option, he/she will be authorised for financial transaction purpose only after OTP verification. The OTP will be received at the customer's registered mobile number. This OTP will be valid for only one transaction. In this mode the user does not have the admin control. After three successive wrong attempts in either fingerprint or OTP method the account will get automatically blocked for next 24 hours and an SMS will be sent to the registered mobile number.

II. FINGERPRINT- AN OVERVIEW

A fingerprint is a print made by an impression of the ridges in the skin of a finger; often used for biometric identification. A ridge is a raised portion of the epidermis on the fingers, toes and the palm of the hand. These epidermal ridges serve to amplify the vibrations, for example, when fingertips sweep across a rough surface, the signals are transmitted to sensory nerves involved in fine texture perception. Impressions of fingerprints may be left behind on a surface by the natural secretions of sweat from the eccrine glands that are present in friction ridge skin [3],[6].

Some of the fingerprint patterns is shown in fig.2&3.

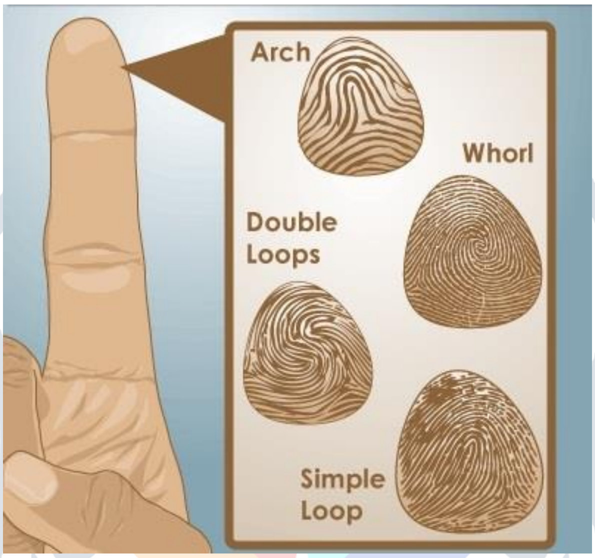

Fig.2 Different shapes of fingerprint impression

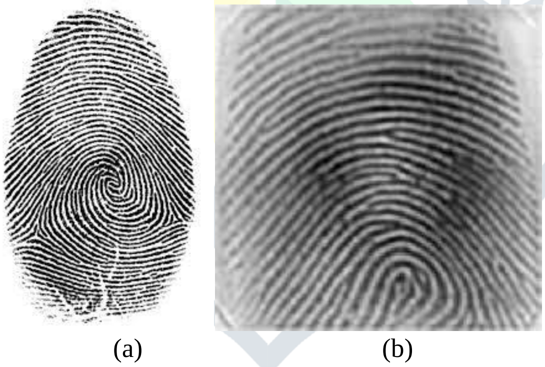

Fig.3 (a) Greyscale fingerprint (b) Binarized fingerprint

A. Advantages of Fingerprint over other Biometric Methods

- It is unique for every individual.
- Easy to install compared with other biometrics.
- Robust and easy to use.
- Low maintenance cost.
- Since is already available in the banker's database, so no extra cost for database management.

A comparative survey of biometric methods as shown in fig.3, shows that the use of fingerprint dominates over other kinds of biometrics such as iris, face, palm vein, etc. for identification.

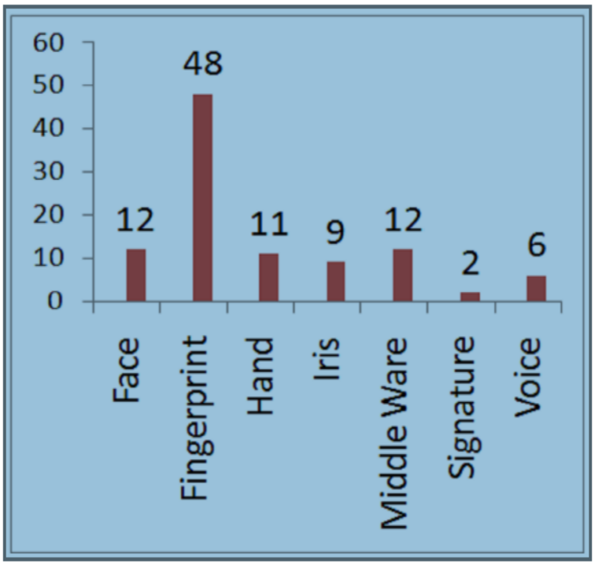

Fig.4 A comparative study of different types of biometrics used

III. PROPOSED METHOD

After complete analysis of the advantages of the fingerprint biometrics system, we propose an advanced ATM security system by making combined use of fingerprint with One Time Password (OTP) authentication. Here we are going to explain our hardware and software model.

A. Hardware Description

We are going to design this model after analysing all the existing embedded ATM client authentication system. We have studied all previously used components of existing designs and we are proposing the best hardware description.

We make use of S3C2440 chip and the LCD, keyboard, alarm, fingerprint scanner are connected to this chip along with SRAM and FLASH.

1) LCD Module: OMAP5910 is used in this module as a LCD controller; it supported 1024*1024 image of 15 Grey-scale or 3375 colours.

2) Keyboard Module: It is of numeric type to input numeric values.

3) SRAM and FLASH: A 16-bit FLASH chip and a 32-bit SRAM chip are used to store the running code, the information of fingerprint and the algorithm.

4) Fingerprint Scanner Module: A 500dpi resolution, anti-press, anti-static fingerprint scanner is used.

5) Ethernet Switch Controller: A 10/100 Mbps RMII Ethernet port is used to connect with the remote data server.

6) GSM module: A GSM modem is used to send the OTP to the registered mobile number.

The proposed hardware model of this system is shown in fig.5.

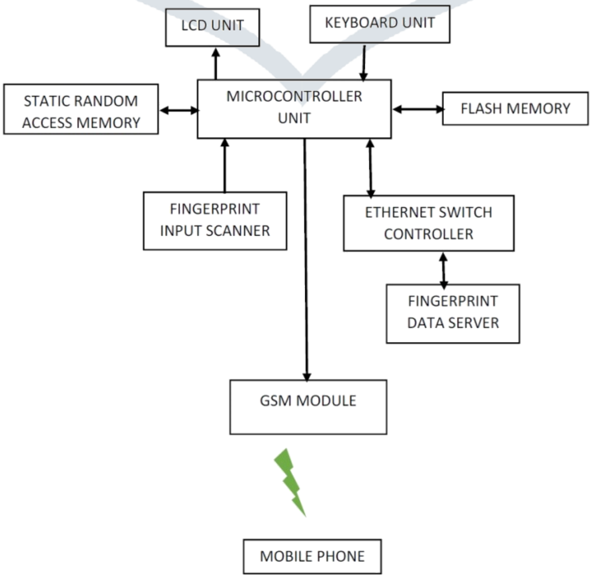

Fig.5 Hardware model of the system

B. Software Model

The software design includes two stages. First of all the first module of code will be designed for user interface with ATM machine and other module of code will be for scanning and matching of fingerprint. The overall flow diagram of software design is given in fig.6.

C. Process Of Scanning And Matching Of Fingerprint

When the finger is pressed over the fingerprint scanner, this linear sensor captures the fingerprint image. This captured image is matched with the database on the remote server. This whole process is controlled by the central microcontroller chip. During the matching process the information is stored in SRAM. The flow diagram of the fingerprint recognition process is shown in fig.7.

IV. CONCLUSION AND COMPARISON

The method used in this paper is of significant use. As a result of the work proposed there will be benefit to human beings for the purpose of ATM security. The review paper submitted here is plan of our project which is still to be completed. As a result of this project, there will be tremendous change in ATM security system. As the research work in this area is still going on, we can expect a better outcome through our project than previous existing ones.

Several works have been done in the field of ATM transaction security. A 3D password based system was proposed in 2008 but it was still traceable. In 2010, a face recognition based system was proposed which was only helpful for tracking suspects and it did not authorise the legal card holder. Again in 2012, a system was proposed using fingerprint and OTP together to authorise the user but there was no backup plan to overcome the failure of fingerprint or OTP system. Another method was proposed in 2012 using iris recognition technology, though it is highly accurate and secure but it has a high installation and maintenance cost. A system using only OTP as authentication purpose was also proposed in 2013, as mobile connectivity was necessary for such type of system therefore it was not reliable for every region.

The detailed comparison of previous works along with their limitations is discussed briefly in table 1 [9],[1],[6],[2],[10].

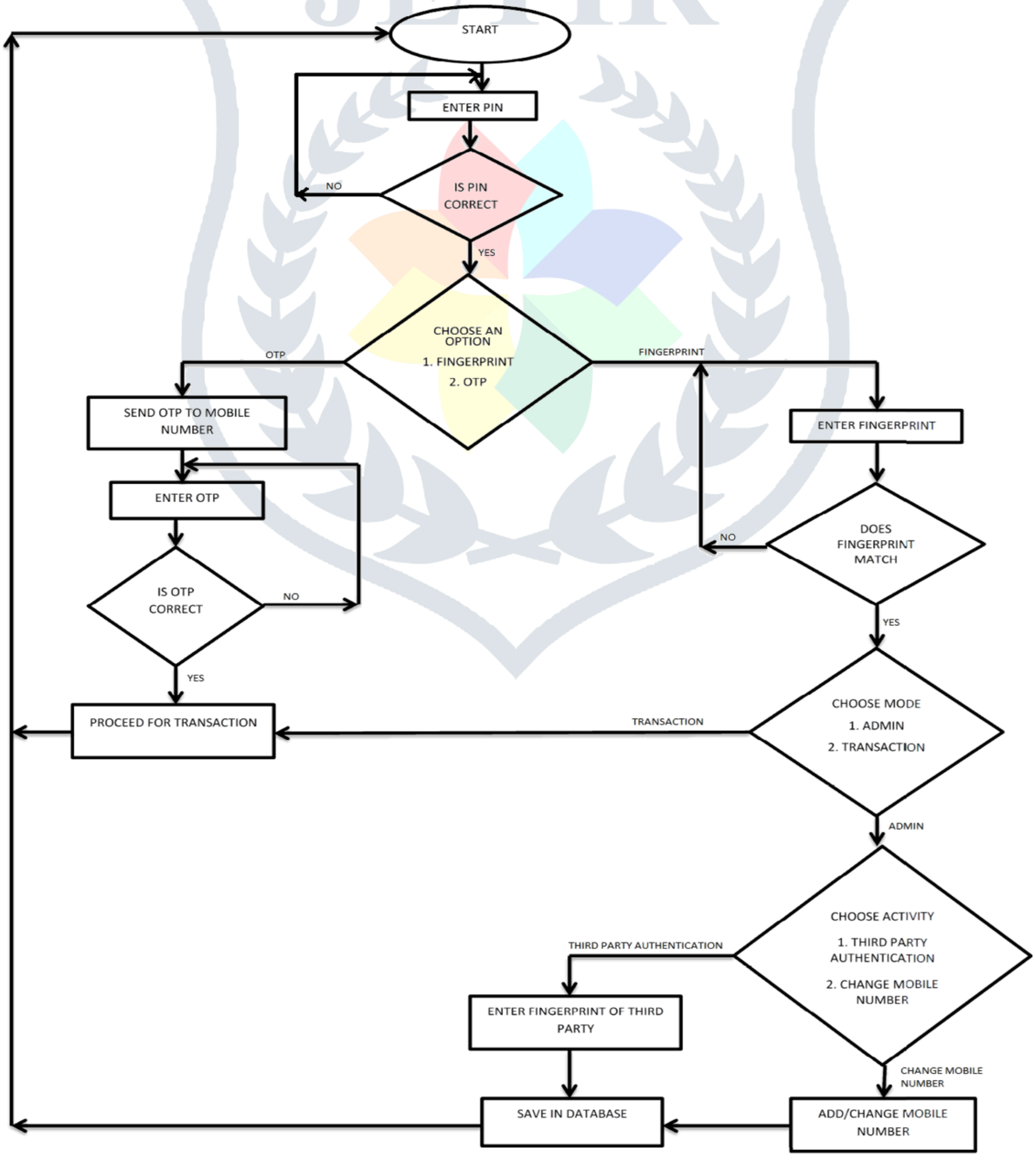

Fig.6 Flowchart of overall software model

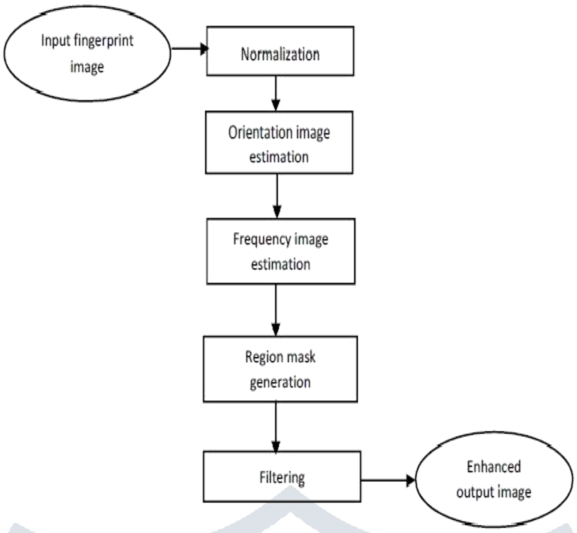

Fig.7 Flow diagram for fingerprint scanning

V. FUTURE SCOPE

According to latest scenario ATM fraud is a very grave problem for banks. This project leads to establish authentication results which can be used by banks as well as various organisations. Now a days security system used in ATMs is completely based on PIN security system which is vulnerable. Banks provide four digit PIN to the user which can be changed later by the user. After first use, user usually changes the password and keeps password quite guessable. This is the main drawback of this PIN type ATM system. When ATM card is lost or stolen it is required to close the ATM card by contacting the bank immediately.

To avoid the above stated problem a security model is being proposed. This system includes application of either fingerprint or OTP authentication. The user can choose between either of the methods according to his/her convenience. The main advantage of this method over the existing and other proposed methods is that it has low installation and maintenance cost and user friendly with a backup plan in case of a failure of one of the methods. In future this technology can be beneficial for each type of user and can be used for authentication in both banks as well industries wherever individual's identification is required.

TABLE I. COMPARATIVE STUDY OF PREVIOUS WORKS

Title	Author (Year of Publication)	Method	Significance	Strength	Limitations
Three Dimensional password for more secure information	Fawaz A. Alsulaiman (08)	3-D password	Generation of graphical password using combination of alpha-numeric-Special characters	Strong password	Possibility of password being traced.
Face Recognizability Evaluation for ATM applications with exceptional occlusion handling	Sungmin Eum (10)	Face Recognition	Transaction proceeds only after recognizing the face of the user	Helpful in tracking of suspects	Does not authenticate the legal card holder.
ATM security using fingerprint recognition and GSM	Pennam Krishnamurthy (12)	Fingerprint and OTP	Both fingerprint and OTP are required at the time of transaction	Secure	No backup plan suggested to overcome the failure of fingerprint or OTP system.
Recognition technique for ATM based on IRIS technology	K. Laxmi Narshima Rao (12)	Iris recognition	Iris of the user is verified	High accuracy and secure	High installation and maintenance cost
Protected cash withdrawal in ATM using Mobile phone	M. R. Dinesh Kumar (13)	One Time Password (OTP)	Sends an OTP to the registered mobile phone	Secure	Not feasible for everyone.

REFERENCES

[1] Sungmin Eum, Jae Kyu Suhr, and Jaihie Kim *"Face Recognizability Evaluation for ATM Applications With Exceptional Occlusion Handling*" School of Electrical and Electronic Engineering, Yonsei University,Republic of Korea

[2] K. Laxmi Narshima Rao "*Recognition Technique for ATM Based on Iris Technology"* International Journal of Engineering Research and Development **e**-ISSN: 2278-067X, **p**-ISSN: 2278-800X, www.ijerd.com Volume 3, Issue 11 (September 2012), PP. 39-45.

[3] K. Lavanya "*A Comparative Study on ATM Security with Multimodal Biometric System*" International Journal of Computer Science & Engineering Technology (IJCSET) ISSN : 2229-3345 Vol. 4 No.06 Jun 2013

[4] Lin Hong, Wan Yifei, Anil Jain. "*Fingerprint image enhancement: algorithm and performance evaluation".* IEEE Transactions on Pattern Analysis and Machine intelligence. 1998, 20(8): 777-789.

[5] Mahesh A. Patil "*ATM Transaction Using Biometric Fingerprint Technology*" International Journal of Electronics, Communication & Soft Computing Science and Engineering ISSN: 2277-9477, Volume 2, Issue 6.

[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] 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).

[8] Jinwei Gu, Jie Zhou, and Chunyu Yang, *"Fingerprint Recognition by Combining Global Structure and Local Cues*", IEEE Transactions on Image Processing, vol. 15, no. 7, pp. 1952 – 1964, (2006).

[9] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik "*Three-Dimensional Password for More Secure Authentication*" IEEE Transactions On Instrumentation And Measurement, Vol. 57, No. 9, September 2008.

[10] M.R.Dineshkumar "*Protected Cash Withdrawal in Atm Using Mobile Phone*" International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 4 April, 2013 Page No. 1346-1350.