ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 5, Issue 5, May 2018

# ATM Security using Fingerprint Authentication and OTP

[1] Aruna R, [2] Sudha V, [3] Shruthi G, [4] Usha Rani R, [5] Sushma V
[1] Assistant Professor, [2, 3, 4, 5] UG Scholars
[1][2][3][4][5] Department of Electronics and Communication Engineering, Sri Sairam College of Engineering Anekal, Bangalore.

*Abstract-* **In this paper, we propose to add more security to the current ATM Systems. By using Biometric Authentication and GSM technology, we can overcome many of the flaws introduced by our current ATM system such as shoulder surfing, use of skimming device, etc. In our proposed system, Bankers will collect the customer's as well as respective nominee's fingerprint and mobile number at the time of opening the account. The primary step is to verify currently provided fingerprint with the fingerprint which is registered in the Bank's database at the time of account opening. If the two fingerprints get matched, then a message will be delivered immediately to the user's mobile number which is the random 10 digit pin number called as One Time Password (OTP). This OTP can be used only once, thus this avoids various problems associated with the present system. For every transaction, new OTP will be sent to account holder's mobile number, thus there will not be fixed PIN number for every transaction. Thus, PIN number will vary during each transaction assuring security.**

***Keywords*- ATM; PIN; Fingerprint; security; biometric.**

## I. INTRODUCTION

Rapid development of banking technology has changed the way banking activities are dealt with. One banking technology that has impacted positively and negatively to banking activities and transactions is the advent of automated teller machine (ATM). It is a computerized machine designed to dispense cash to bank customers without need of human interaction. Today the ATM users are increasing in numbers. hey use the ATM cards for banking transactions like balance enquiry, mini statement, withdrawal, etc. The ATM machine has card Reader and keys as input devices and display screen, cash dispenser, receipt printer, speaker as output devices. ATMs are connected to a host processor, which is a common gateway through which various ATM networks become available to users. Various banks, independent service providers owned this host processor. Account information of user is stored on the magnetic strip present at the back side of the ATM card. When we enter the card in the card reader, the card reader captures the account information and the information is used for the transaction purpose. And we have to insert the pin by keys. The pin is the 4 digit number given to all ATM card holders. ATM card holder's pin is different from each other. The number is verified by the bank and allows the customers to access their account. The password is the only identity so anyone can access the account when they have the card and correct password. Once the card and is stolen by the culprit and if he/she comes to know the password by any means then the culprit can take more money from the account in the shortest period, it may bring huge financial losses to the users. In the recent days, there have been many such ATM fraud cases. Due to some of the flaws in our present ATM system such as use of static pin and ATM card, its users face many kinds of problem and there have been many issues associated with the present system. To overcome the problems associated with the present ATM System, in our project we are using biometric features. Biometrics technologies are a secure means of authentication because biometrics data are unique, cannot be shared, cannot be copied and cannot be lost. Physical characteristics include fingerprint, hand or palm geometry, retina, iris and face while popular behavioral characteristics are signature and voice.

## II. LITERATURE REVIEW

Crime at ATMs has become a nationwide issue that faces not only customers, but also bank operators and this financial crime case rises repeatedly in recent years [4]. A lot of criminals tamper with the ATM terminal and steal customers' card details by illegal means. Once users' bank card is lost and the password is stolen, the users' account is vulnerable to attack. Traditional ATM systems authenticate generally by using a card (credit, debit, or smart) and a password or PIN which no doubt has some defects [5]. The prevailing techniques of user authentication, which involves the use of either passwords and user IDs (identifiers), or identification cards and PINs (personal identification

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 5, Issue 5, May 2018

numbers), suffer from several limitations [6]. Passwords and PINs can be illicitly acquired by direct covert observation. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Despite warning, many people continue to choose easily guessed PIN's and passwords - birthdays, phone numbers and social security numbers. Recent cases of identity theft have heightened the need for methods to prove that someone is truly who he/she claims to be. Biometric authentication technology may solve this problem since a person's biometric data is undeniably connected to its owner, is nontransferable and unique for every individual. The system can compare scans to records stored in a central or local database or even on a smart card. Biometrics can be defined as a 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 [7]. It is a measure of an individual's unique physical or behavioral characteristics to recognize or authenticate its identity [8]. Common physical biometrics characteristics include fingerprint, hand or palm geometry, retina, iris and face while popular behavioral characteristics are signature and voice. Biometrics technologies are a secure means of authentication because biometrics data are unique, cannot be shared, cannot be copied and cannot be lost.

## III. PROPOSED SYSTEM

Our project proposes the idea of using fingerprint and OTP in ATMs as password instead of the traditional pin number. By using fingerprint recognition, the users will be more relieved as their accounts cannot be accessed by others and can maintain secrecy. We also have OTP feature along with the fingerprint authentication which will definitely not allow any criminal to use the password for any kind of frauds as the OTP is valid only once. Thus, it becomes useless for the next time even if any criminal gets hold of it .

The main modules of a fingerprint verification system are:

a) fingerprint sensing, in which the fingerprint of an individual is acquired by a fingerprint scanner to produce a raw digital representation

b) Preprocessing, in which the input fingerprint is enhanced and adapted to simplify the task of feature extraction

c) Feature extraction, in which the fingerprint is further processed to generate discriminative properties, also called feature vectors

d) Matching, in which the feature vector of the input fingerprint is compared against one or more existing templates.

Block diagram

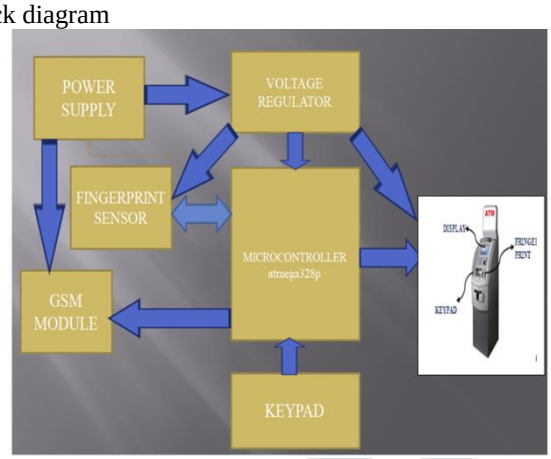



***Fig 1: Block diagram of ATM user security.***

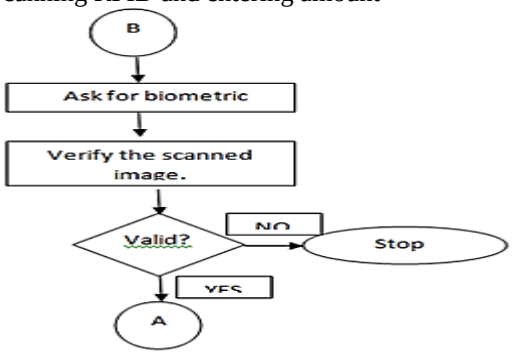
The block diagram of the proposal system and design documents of independent modules are considered. Hardware components are essential to any embedded system. Here, the below diagram shows the block diagram of biometric fingerprint based ATM authentication system. The main blocks of Fingerprint based authentication system includes power supply, micro-controller, fingerprint module, LCD,GSM module.

**Working**

The first step is to the user enters finger in fingerprint sensor and the sensor verify the currently entered finger print with registered finger print that already registered in bank database at the time of account opening. If the two fingerprint get matched , then OTP will send to respective mobile number that we have registered in the bank. After getting OTP , we have to enter in ATM and we can draw the money. And the OTP used only once at a time. From this we can give more security to the cash holder's.

**Flowchart**

Fig1. Scanning RFID and entering amount



ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 5, Issue 5, May 2018

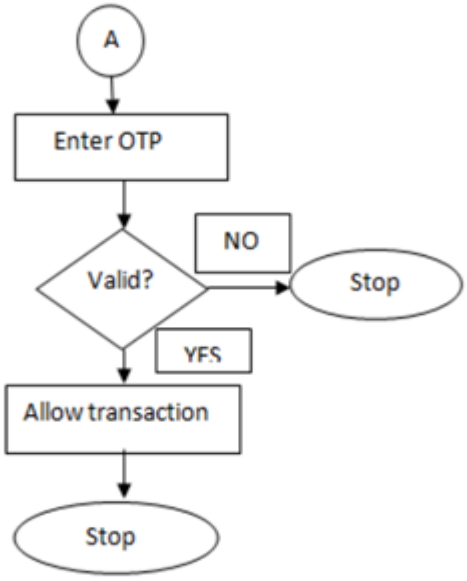



*Fig.2: Inputting OTP and scanning biometric.*

**GSM Technology**

In order to send OTP, GSM (Global System for Mobile Communication) technology is used with the help of GSM Modem. A GSM Modem is a specialized type of modem which accepts a SIM card, and operates over a subscription to a mobile operator, just like a mobile phone. From the mobile operator perspective, a GSM modem looks just like a mobile phone. When a GSM modem is connected to a computer, this allows the computer to use the GSM modem to communicate over the mobile network. While these GSM modems are most frequently used to provide mobile internet connectivity, many of them can also be used for sending and receiving SMS and MMS messages.

**Advantages**

1. It is very easy to implement and use.
2. It is very efficient as compared to other methods.
3. Moreover, it does not depend on any kind of technique that uses skin tone as one of its feature to be used for identification.
4. It provide more security.
5. No backup plan suggested to overcome the failure of finger print or OTP system.
6. Biometric tokens are the safest means of preventing ATM frauds.
7. In some application biometrics can replace or supplement the existing technology, in others, it is the only viable approach.

**Requirement Specification**

1.Atmega328p: The Atmel 8-bit AVR RISC-based microcontroller combines 32 kB ISP flash memory with read-while-write capabilities, 1 kB EEPROM, 2 kB SRAM, 23 general purpose I/O lines, 32 general purpose working registers, three flexible timer/counters with compare modes, internal and external interrupts, serial programmable USART, a byte-oriented 2-wire serial interface, SPI serial port, 6-channel 10-bit A/D converter (8-channelsin TQFP and QFN/MLF packages),programmable watchdog timer with internal oscillator, and five software selectable power saving modes. The device operates between 1.8-5.5 volts. The device achieves throughput approaching 1 MIPS per MHz.

2. Fingerprint Scanner: A fingerprint scanner is a type of technology that identifies and authenticates the fingerprints of an individual in order to grant or deny access to a computer system or a physical facility.It is a type of biometric security technology that utilizes the combination of hardware and software techniques to identify the fingerprint scans of an individual.

3. A liquid-crystal display (LCD) is a flat-panel display or other electronically modulated optical device that uses the light-modulating properties of liquid crystals. Liquid crystals do not emit light directly, instead using a backlight or reflector to produce images in color or monochrome.[1] LCDs are available to display arbitrary images (as in a general-purpose computer display) or fixed images with low information content, which can be displayed or hidden, such as preset words, digits, and seven-segment displays, as in a digital clock. They use the same basic technology, except that arbitrary images are made up of a large number of small pixels, while other displays have larger elements.

**Future scope**

In our proposed system we are dealing with fingerprint technique for draw the cash by getting OTP. Future scope is by iris and Face recognisition for draw the cash by ATM to provide more security.

## IV. CONCLUSION

Automatic Teller Machines have become a mature technology which provides financial services to an increasing segment of the population in many countries. Biometrics, and in particular fingerprint scanning, continues to gain acceptance as a reliable form of securing access through identification and verification processes. This paper identifies a high level model for the modification of existing ATM systems using both Biometric fingerprint strategy and GSM technology. We have been able to develop a

fingerprint mechanism as a biometric measure to enhance the security features of the ATM for effective banking. The developed application has been found promising on the account of its sensitivity to the recognition of the cardholder's finger print as contained in the database. This system when fully deployed will definitely reduce the rate of fraudulent activities on the ATM machines.

## REFERENCES

1.Ricardo Janes, (2010), A Study on the Available Biometric Technologies Used in Order to Control Security in Physical Access, Issue 6 Vol 5

2. Sanket Rege, Rajendra Memane, (2013), 2D Geometric shape and color recognition using Digital Image Processing, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 6

3.Maninder Singh, Shahanaz Ayub and Raghunath Verma, "Enhancing Security by averaging multiple fingerprint images," Proc. International Conference [4] S.S, Das and J. Debbarma, "Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian e-banking System", International Journal of Information and Communication Technology Research, vol.1, no. 5, pp.197-203, 2011.

[5] W.W.N. Wan, C.L. Luk, and C.W.C. Chow, "Customers Adoption of Banking Channels in Hong Kong", International Journal of Bank Marketing, vol. 23, no. 3, pp. 255-272, 2005.

[6] Wikipedia the free encyclopedia, "Biometrics", Downloaded March 20, 2012 from http://en.wikipedia.org/wiki/Biometrics.

[7] B. Richard and M. Alemayehu, "Developing E-banking Capabilities in a Ghanaian Bank: Preliminary Lessons. Journal of Internet Banking and Commerce, vol. 11, no. 2, 2006. Downloaded March 15, 2012 from http://www.arraydev.com/commerce/jibc/

[8] P.K. Amurthy and M.S. Redddy, "Implementation of ATM Security by Using Fingerprint recognition and GSM", International Journal of Electronics Communication and Computer Engineering vol.3, no. 1, pp. 83-86, 2012.

[9] N.K. Ratha, J.H. Connell, and R.M. Bolle, "Enhancing Security and Privacy in Biometrics-based Authentication Systems, IBM Systems Journal, vol. 40, no. 3, pp. 614-634, 2001.

[10] N.K. Ratha, S. Chikkerur, J.H. Connell and R.M. Bolle. "Generating Cancelable Fingerprint Templates", IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, 2007. [8] B, Schouten and B. Jacobs, "Biometrics and their use in e-passport", Image and Vision Computing vol. 27, pp. 305–312. 2009,

[11] S.A. Shaikh and J.R. Rabaiotti,. "Characteristic trade-offs in designing large-scale biometric-based identity management systems". Journal of Network and Computer Applications vol. 33, pp. 342–351, 2010.

[12] C.A. Oyeka, An Introduction to Applied Statistical methods. Enugu, Nigeria: Modern Avocation Publishing Company. Pp. 4, 36, 56. 1990.
(IJACSA) International Journal of Advanced Computer Science on Communication Systems and Network Technologies, IEEE 2013