IJFEAT

INTERNATIONAL JOURNAL FOR ENGINEERING APPLICATIONS AND TECHNOLOGY

# A Survey on Smart ATM PIN Recovery Using Fingerprint Authentication

**Samiksha Tote[1], Sumit Khunkar[2], Sagar Gajbhiye[3] , Asst. Prof. Sachin Inzalkar[4]**

*IV[th] Year BE (CSE Department), JDIET, Yavatmal- stote1998@gmail.com*
*IV[th] Year BE (CSE Department), JDIET, Yavatmal- sumitkhunkar11@gmail.com*
*IV[th]Year BE (CSE Department), JDIET, Yavatmal- sgrgjbh123@gmail.com*
*Assistant Professor, JDIET, (CSE Department), Yavatmal –sachininzalkar@gmail.com*

**Abstract**

**ATM (Automated Teller Machine) is an electronic telecommunication device which is used to perform financial transaction without any need for human clerk or bank teller. ATMs extend traditional banking hours by cash dispenser and makes all other transaction should be available 24 hours a day. In ATM machines, the user is analyzed by including an ATM card and authentication is implemented by the customer entering a PIN. The PIN provided to the customer is correlated with recorded reference PIN number in the bank server. In the actual system, the user has to insert the card and the PIN number. If the PIN is perfect, the system is granted for the transaction. Otherwise, the system demand for the PIN again and it is granted for maximum of three times to enter it. After processing of 3 trials the ATM card will be blocked. To reactivate the card, user must visit the bank and do the bank formalities, which is annoying and moderate job. Biometrics is the science of chartering the status of an individual based on physical, chemical or behavioural attributes of a person. Fingerprint is a arrangement of ridges and valleys on the surface of a fingertip. It is generally used for biometric identification. Fingerprints are complicated, nearly exclusive, tough to alter and dependable over the life of an individual. To reactivate ATM card in the ATM centre, we are applying fingerprint biometric.**

***Index Terms:*** **Fingerprint, Automated teller machine, PIN, Harris corner detection algorithm, SURF algorithm.**

---------- *** ----------

## 1. INTRODUCTION

PIN based authentication is usually worn out the automated teller machine transactions. Appreciating this security, user authentication process is a necessary activity. Foremost problems encompass shoulder-surfing attacks, replay attacks, card cloning, and PIN sharing. Multiple researches have also been managed to create systems supporting card-less transactions. These are earning popular, where customers can use additional personal devices, like mobiles, to control atm transactions. Shoulder-surfing attacks also are called observation attacks. Shoulder-surfing attacks are common threat for ATM authentication.

In this case, the attacker simply views the entry procedure of the PIN by the authorized user to induce hold of the key information. Master card and positive identification frauds because of identity thefts are increasing per annum. Additionally, there are scamming techniques using fake terminals, master card cloning, and remote relay which make the method of user protection harder. The attacker is standing in queue behind the authenticating person and looking out at the PIN entry and executes a shoulder-surfing or observation attack. The attacker may install a little camera on the highest surface of the ATM terminal to record PIN entries of users at the point-of-service.

The attacker can install a card skimming device on the ATM machine to induce hold of the user's card information. Such devices fit at the cardboard slot on ATM machines and record the cardboard information because the user slides in their card. the protection level is thus improved by providing a PIN authentication protocol for ATM using mobile

applications in smart phones. Image processing technique is further used for user identity checking process when a maximum of three PIN attempts is formed by the user.

## 1.1 OBJECTIVES

Usually the user inserts the ATM card within the ATM machine and enters Personal Identification Number (PIN) for the transactions. If the user forgets the PIN and enters the incorrect PIN then the ATM machine will allow two more attempts to enter the valid PIN. If the user fails to produce the right PIN after three attempts, the bank server will block the ATM card of the user. Now user needs to visit the bank to reactivate his/her ATM card, which is time consuming.
1) To avoid the user to go to the bank and do the formalities to reactivate his/her ATM card.
2) To activate the ATM card of the user at the ATM centre itself with the assistance of finger print of the user.
3) To alert owner of the ATM card just in case of misuse

## 2. LITERATURE REVIEW

Crime at ATMs has become a nationwide circulate that faces not entirely customers, but jointly bank operators and this financial crime case rises typically in new years. A lot of criminals change with the ATM terminal and steal customers' card details by prohibited implies that.Once users' bank card is lost and thus the watchword is purloined, the users' account is vulnerable to attack. ancient ATM systems manifest generally by employing a card (credit, debit, or smart) and a password or PIN that very little question has some defects. The prevailing techniques of user authentication, that involves the use of either passwords and user IDs or identification cards and PINs (personal identification numbers), suffer from many limitations . Passwords and PINs area unit typically illicitly nonheritable by direct covert observation.

When credit and ATM cards area unit lost or purloined, an unauthorized user will typically come back up with the right personal codes. Despite warning, many of us still choose simply guessed PIN's and passwords - birthdays, phone numbers and Social Security numbers. Recent cases of identity theft have heightened the need for strategies to prove that someone is actually World Health Organization he/she claims to be. Biometric authentication technology might solve this drawback since a person's biometric information is undeniably connected to its owner, is untransferable and distinctive for every individual.

The system will compare scans to records hold on throughout a central or native info or maybe on a wise card. biometry area unit typically defined as a measurable physiological and activity characteristic which is able to be captured and later correlated with another instance at the time of verification. It is machine-controlled strategies of recognizing somebody supported a physiological or activity characteristic . it is a live of somebody's distinctive physical or activity characteristics to acknowledge or manifest its identity .

Common physical biometry characteristics embody fingerprint, hand or palm pure mathematics, retina, iris and face while standard activity characteristics area unit signature and voice. biometry technologies area unit a secure means that of authentication as a result of biometry information area unit distinctive, cannot be shared, cannot be traced and cannot be lost.

## 3. PROPOSED SYSTEM

This paper determines the thought of observe fingerprint and OTP in ATMs as identification rather than the normal PIN. By observe fingerprint recognition, the users unit of measurement progressing to be various relieved as their accounts can't be accessed by others and can maintain secrecy. we have a tendency to tend to tend to even have OTP feature at the aspect of the fingerprint authentication which could beyond any doubt not permit any corrupt to use the identification for any fairly fakes as the OTP is valid one time. Thus, it becomes useless for the next time admitting any criminal gets hold of it.

The main elements of a fingerprint verification system are:

a) fingerprint sensing, throughout that the fingerprint of academic degree individual is learned by a fingerprint scanner to provide a raw digital illustration.

b) Preprocessing, throughout that the input fingerprint is increased and tailored to vary the task of feature extraction.

c) Feature eradication, throughout that the fingerprint is any processed to urge discriminative properties, additionally declared as feature vectors.

d) Matching, throughout that the feature vector of the input fingerprint is compared against one or various existing templates.

Block diagram :

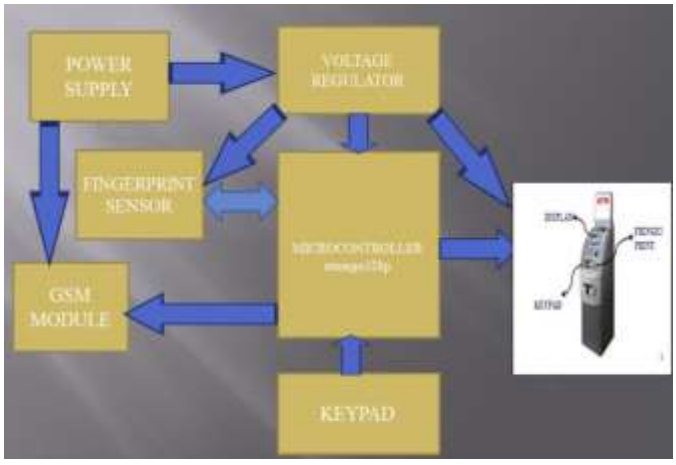


Fig 1: Block diagram of ATM user security.

The diagram of the proposal system and style documents of independent modules are considered. Hardware components are essential to any embedded system. Here, the below

diagram shows the 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.

### 3.1 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.

### 3.2 FLOWCHART

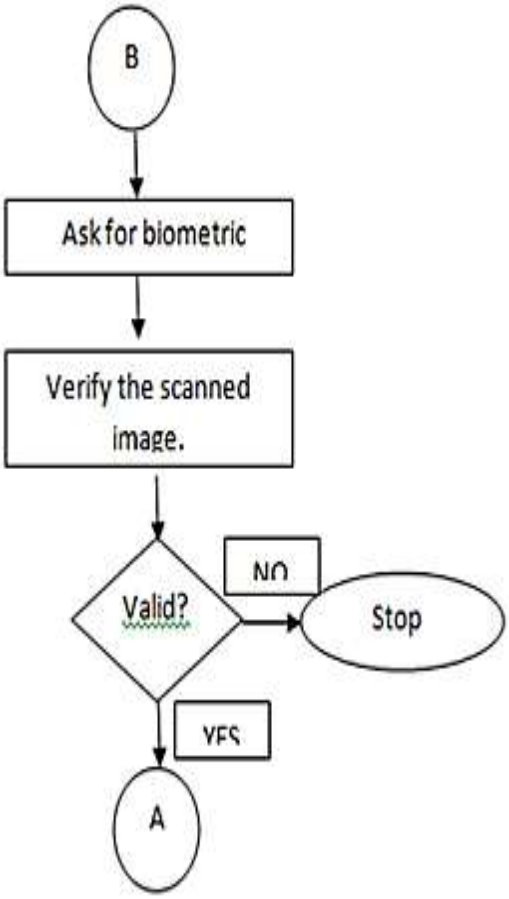


Fig 2: Scanning RFID and entering amount.

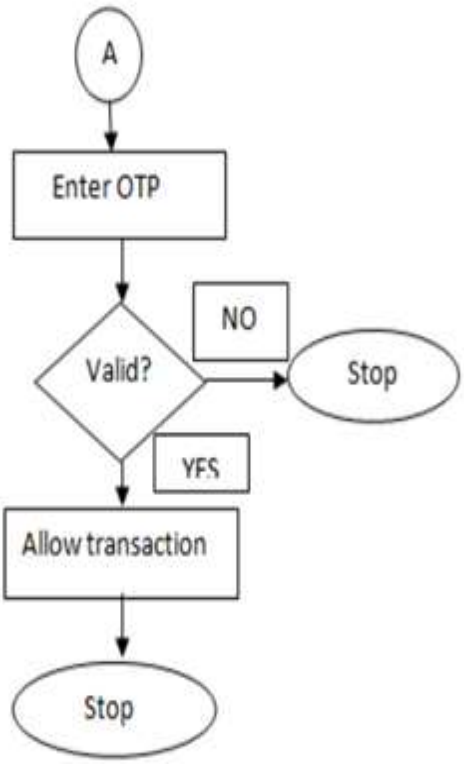


Fig 3: Inputting OTP and scanning biometric.

### 4. ADVANTAGES

1. It is easy to implement and use.
2. It is efficient as compared to other methods.
3. Moreover, it does not depend on any kind of technique which uses skin tone as one of its feature to be used for Identification.
4. It produces more security.
5. No backup plan suggested to overcome the failure of fingerprint 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.

### 5. REQUIREMENT SPECIFICATION

**1.Atmega328p:** The Atmel 8-bit AVR RISC-based microcontroller combines 32 kB ISP flash reminiscence with read-while-write capabilities, 1 kB EEPROM, 2 kB SRAM, 23 general cause I/O lines, 32 general motive working registers, 3 bendy timer/counters with compare modes, internal and external interrupts, serial programmable USART, a byte-orientated 2-cord serial interface, SPI serial port, 6-channel 10-bit A/D converter (8-channelsin TQFP and QFN/MLF packages),programmable watchdog timer with inner oscillator, and five software program selectable power saving modes. The tool operates between 1.8-5.five volts. The tool achieves throughput drawing close 1 MIPS/MHz.

**2. Fingerprint Scanner:** A fingerprint scanner is a kind of

technology that identifies and authenticates the fingerprints of an man or woman with the intention to furnish or deny get admission to computer gadget or a bodily facility.It is a type of biometric security era that makes use of the combination of hardware and software techniques to identify the fingerprint scans man or woman.

**3. Liquid-Crystal Show:** A liquid-crystal show (LCD) is a flat-panel display or other electronically modulated optical tool that makes use of light-modulating homes of liquid crystals. Liquid crystals do now not emit mild directly, instead the use of a backlight or reflector to produce pictures in color or monochrome. LCDs are available to display arbitrary pix (as in general-purpose computer show) or fixed pix with low records content, which can be displayed or hidden, such as preset words, digits, and seven-segment presentations, as in a virtual clock. They use the identical basic technology, except that arbitrary pictures are made of a huge variety of small pixels, even as other displays have larger elements.

## 6. CONCLUSION

Automatic Teller Machines became a mature technology which provides financial services to an increasing segment of the population in many countries. Biometrics, and particularly fingerprint scanning, continues to gain acceptance as a reliable variety of securing access through identification and verification processes. This paper analyzes a high level model for the adjustment of existing ATM systems using Biometric fingerprint strategy . we've got been able to develop a fingerprint mechanism as a biometric measure to boost the security factores of the ATM for effective banking. The developed application has been found promising on the account of its sensitivity to the popularity of the cardholder's finger print as contained within the database. This system when fully deployed will certainly reduce the speed of fraudulent activities on the ATM machines.

## REFERENCES


1. Aruna R, Sudha V and Usha Rani R."ATM Security using Fingerprint Authentication". "International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)" Vol 5, Issue 5, May 2018

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

3. 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

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