Improving Security in Automatic Teller Machines (ATM) using Biometrics & OTP or IRIS Recognition

1st Mr. Shubham Modi
School of Computer Science
MIT- World Peace University
Pune, India

2nd Mr. Pushkar Parmar
School of Computer Science
MIT- World Peace University
Pune, India

3rd Mr. Shohrat Ali
School of Computer Science
MIT- World Peace University
Pune, India

5th Ms. Pratiksha Vidhale
Vidhale *School of Computer Science* MIT- World Peace University Pune, India

6th Dr. C.H. Patil
School of Computer Science
MIT- World Peace University
Pune, India

***Abstract*--The loot of ATM cards has been increasing over the past few years, in the current system PASSCODE are used for ATM transactions. Which can easily be stolen, speculated or misused in many ways with it. It inspired to increase user security by adding biometric and OTP to the existing system. It also brought up some issues including sensor durability and time consumption. As a solution We introduce a constraint on transactions by ATMs involving biometric (finger print) to improve the system to resolve performance and issues. If we exceed the amount entered, we are adding a limit on the cash amount It is necessary to present the limit, biometric. There is no biometric scanning if one is required to withdraw the minimum cash. Mandatory will only enter OTP for user authentication. It helps users to save time and maintain sensor performance Their biometric not presented for a few hundred except to maintain security.**

I. INTRODUCTION

Quick advancement of banking innovation has changed the manner in which banking exercises are managed. One financial innovation that has affected emphatically and adversely to banking exercises and exchanges is the approach of robotized teller machine (ATM). It is an automated machine intended to administer money to account holder without the need of human connection. Today the number of ATM clients are expanding in huge numbers. hello utilize the ATM cards for banking exchanges like parity enquiry, small scale proclamation, withdrawal, and so on. The ATM machine has card Reader and keys as info gadgets and show screen, money distributor, receipt printer, speaker as yield gadgets. ATMs are associated with a host processor, which is a typical portal through which different ATM systems become accessible to clients. Different banks, free specialist co-ops claimed this host processor. Record data of client is put away on the attractive strip present at the posterior of the ATM card. When we enter the card, the machine catches the data and the data is utilized for the exchange reason. Also, we need to embed the passcode or ATM pin by keys. The passcode number is given to all ATM card holder. ATM card holder's ATM pin or passcode is not the same as one another because the passcode was randomly generated for every user. The number is checked by the bank and permits the clients to get to their record. The secret pin is the main character so anybody can get to the record when they have the card and address secret phrase. When the card and is taken by the offender and in the event that he/she comes to know the secret word using any and all means then the guilty party can take more cash from the record in the most limited time frame, it might carry gigantic money related misfortunes to the clients. In the ongoing days, there have been numerous such ATM extortion cases and ATM phishing cases happened in India or in the world. Due to a portion of the defects in our present ATM framework, for example, utilization of static pin and ATM card, its clients face numerous sorts of issue and there have been numerous issues related with the present framework, Many Times ATM Machines were not capable to read the card because of old framework which were present in it. To defeat the issues related with the present ATM System, in our venture we are utilizing biometric highlights. Biometrics advances are a safe method for verification since biometrics information are remarkable, can't be shared, can't be duplicated and can't be lost and the chance of fraud happen with biometrics is very less. Physical attributes unique mark, retina, iris, hand or palm and face while well-known social qualities are mark and voice.

II. EXISTING SYSTEM

In old days no security layer is applicable in ATM card except PIN number, now a day there will be a microchip present in the ATM card but this chip is not fully secured, it might be hacked. It will be very expensive for the bank to include fingerprint and iris scanners in normal transactions. ATM card falling into wrong hands, stolen and PIN number being cracked by a stranger. Then strangers can easily use the ATM card to withdraw the whole amount from the account.

A. Functions involved in fingerprint reorganization:

- Fingerprint Identification: Standards of identification we will use client's fingerprint information. It should authenticate the facility of human fingerprint before using the ATM system.

- Remote Authentication: To the remote fingerprint data server the system can compare the fingerprint information of the current client.

III. PROPOSED SYSTEM

A. Biometrics & OTP

In this proposed system we are securing the ATM user transactions using OTP and biometrics. Here we are using RFID card as ATM card and using finger print OTP number sent to the registered GSM mobile number which will be entered by keys. In addition, a tilt sensor is used for protection in the ATM machine, if anyone tries to steal or harm the machine which is sensed by the tilt sensor the interface for the ATM machine will indicated by and Buzzer alert and sends the alert message to bank as-well-as police also. They are all connected to the sensor **ARM7 LPC2148** Microcontroller shown in block diagram below.

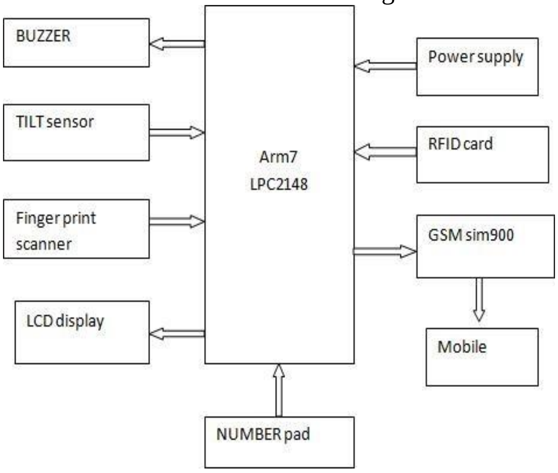


Fig.*1*

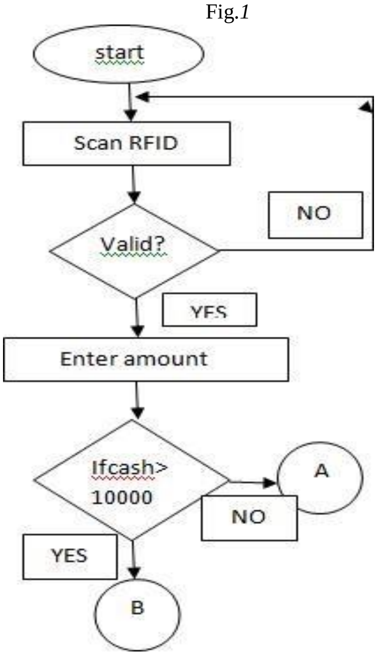


Fig. 2 The flow of this block diagram is seen below.

First of all, we will start the components and start the process by scanning the RFID, we will ask to enter the amount if it is below the limit then move to point A and then we only need to enter the OTP and the diagram below.

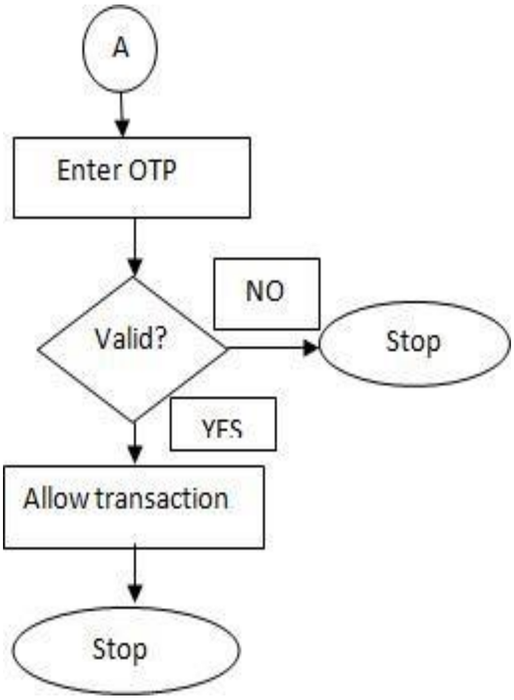
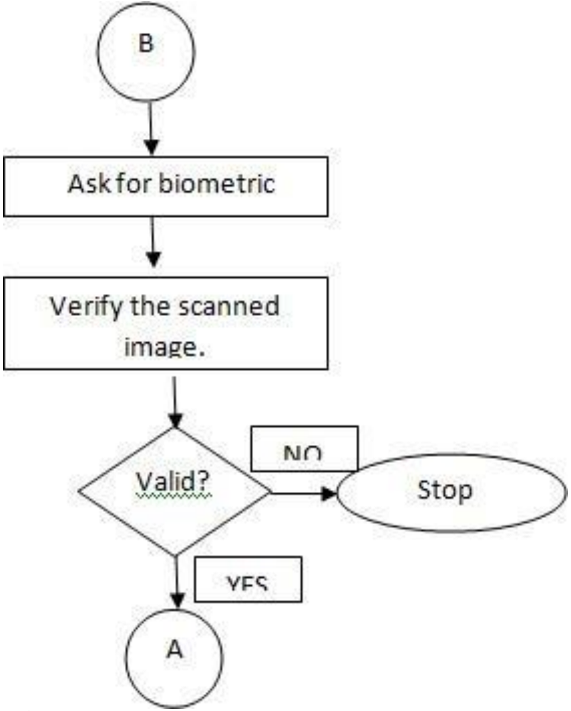


Fig. 3 Input OTP & Scanning biometric.



If the entered amount is more than limit decided by the bank, Then the ATM machine need to scan the fingerprint, then we need to enter the OTP, if the OTP matches transaction will be allowed. Otherwise it stops we have to do the transaction again.

B. Iris Recognition Technology

When the account holder shows his RFID card then the ATM transaction process starts, then the RFID reader scan the RFID card. Account connect with unique RFID number will be accessed. After scanning RFID card, the next step will be iris scanning, for capturing the image of the iris pattern, we will use CMOS camera, it will generate a code for the iris. If the code matches with the iris pattern stored in the database of the account, then the account being accessed, the client will be allowed to do the transaction. Otherwise, the ATM did not display the account information and further activity will be disabled for the client.

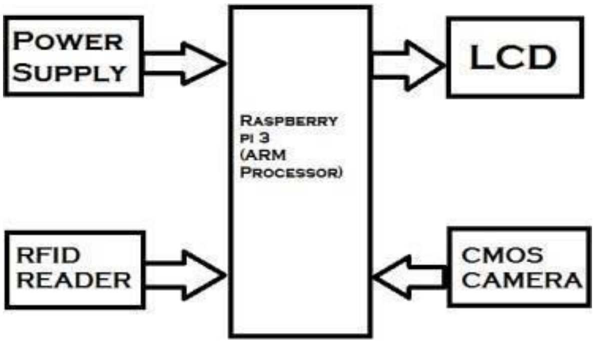


Fig. 4 Block Diagram.

Analyzing the random pattern of iris for recognizing a person is the only process for iris recognition. Number of sub-systems which is to be composed by a system, which is used at every stage of iris recognition technique. The stages that are involved in iris recognition are as follows: Image Acquisition –using Cmos camera it will capture the eye image, Segmentation –The iris region in an eye image that is located by segmentation, Normalization - Consistent representation of the iris region which is dimensionally created, Encoding – creating a template containing only the most discriminating features of the iris, Recognition – proper matching and recognition is done.

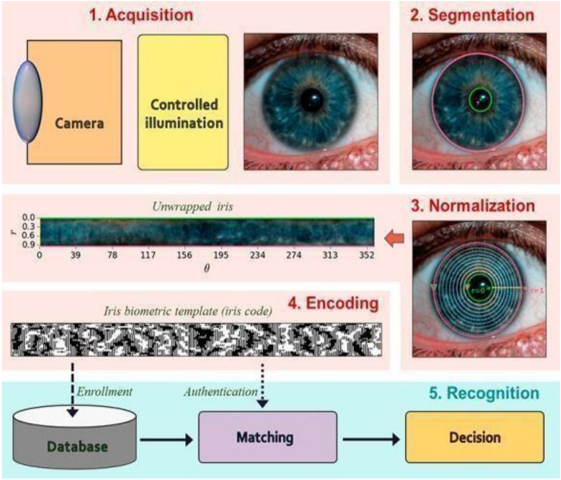


Fig. 5 Iris Recognition Procedure.

Image Acquisition- Acquiring or capturing the image of an eye the process of Image Acquisition starts. The image of the iris should be rich in iris texture as the acquisition method is depends on the image quality. Therefore, to get a high-quality image of the iris, we are using a cameo camera. CMOS camera requires less power and provides a higher quality of image. The main motive of CMOS camera is to converts light energy into electrons. To get the image, a distance between the user and the camera must be 9 cm and 12 cm from the source of light. To locate the outer radius of the iris, pattern the center of the pupil will be used. By searching the edge image, we can locate the iris inner and outer borders. Normalization- Un-wrapping the iris and converting it to its polar counterpart is the process for normalization. Daugman's rubber sheet model is used for this process. For the reference point we considered center of the pupil and to convert the points on the Cartesian to the polar scale remapping formula is used.

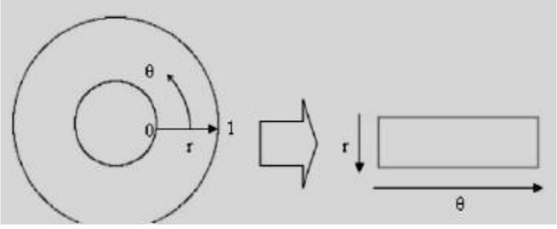


Fig. 6 Normalization Process.

Iris Recognition - Iris biometric technology is the final process for iris recognition. When the iris stored in the database is matched with the user's iris, then the system gives a message in form of text, that the iris has been recognized and the further steps can access by the user and eventually perform the transaction is.

FUTURE SCOPE

In our proposed system we are dealing with fingerprint technique, OTP and IRIS to draw the cash by getting. Future scope is by QR code and Face recognition to draw the cash by ATM to provide more security.

CONCLUSION

ATM's have become a full-grown innovation which offers money related types of assistance to an expanding portion in numerous nations. Specifically, unique finger impression filtering and biometrics, keeps on picking up acknowledgment as a dependable type of verifying access through distinguishing proof and confirmation forms. Iris acknowledgment is a helpful and flexible strategy. Iris acknowledgment is profoundly exact strategy. This method has fruitful applications. This strategy increments both protection and character. Exceptionally secure biometric technique. Iris acknowledgment is an exceptionally simple procedure including less advances. Iris acknowledgment expends less time in contrast with other biometric acknowledgment strategies. This research paper recognizes a significant level model for the changing of existing ATM frameworks with both Biometric unique mark technique and GSM innovation and utilizing the IRIS acknowledgment innovation which makes the exchange progressively verify and less tedious.

REFRENCES

[1] ATM Security using Iris Recognition Technology and RFID (2017).

[2] https://www.computerweekly.com/tip/ATM-security-The-dos-and-donts

[3] https://en.wikipedia.org/wiki/Security_of_automated_teller_machines