International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

General Article

ATM Security using Fingerprint Authentication and OTP

Rathishala Rajendran†*, Kavita Anandraj†, Edwina Jacob† and Chhaya Narvekar†

†Information Technology Department, Xavier Institute of Engineering, Mahim (W), Mumbai, India

Accepted 12 April 2015, Available online 20 April 2015, **Vol.5, No.2 (April 2015)**

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.

Keyword: *ATM, Fingerprint Recognition, GSM, OTP, AT Commands.*

1. 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. They 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.

The table 1 shows a comparison of existing biometric systems in terms of the parameters that it characterizes as biometry, the parameters are:

i.Universality - each person around the world obligatorily must have the physiological or behavioral characteristic;

ii.Uniqueness - this characteristic must be enough different between people;

iii.Permanence - the characteristic must be enough invariant during a certain period of time;

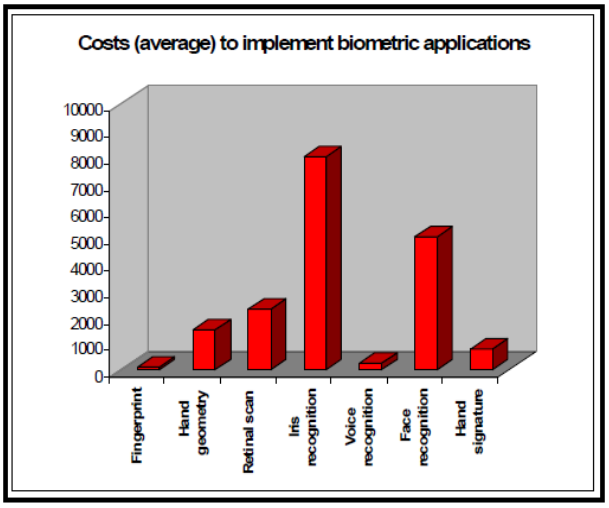
*Corresponding author: **Rathishala Rajendran**

iv. Collectability - the characteristic can be measured quantitatively, and the measurement can be stored (Ricardo Janes, 2010).

Table 1 Parameters of a biometry technology

BIOMETRICS	Universality	Uniqueness	Permanence	Collectability
Fingerprint	MEDIUM	HIGH	HIGH	MEDIUM
Hand geometry	MEDIUM	MEDIUM	MEDIUM	HIGH
Retinal scan	HIGH	HIGH	MEDIUM	LOW
Iris recognition	HIGH	HIGH	HIGH	MEDIUM
Voice recognition	MEDIUM	LOW	LOW	MEDIUM
Face recognition	HIGH	LOW	MEDIUM	HIGH
Hand signature	LOW	LOW	LOW	HIGH

The following graph depicts the cost of implementation of various biometric applications.



Graph 1 – Costs of implementation of biometric Applications

Thus by considering the factors such as ease of use, high efficiency, less cost of implementation, high security we use the fingerprint for the identification purpose.

2. 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 (Sanket Rege *et al,* 2013).

2.1 Fingerprint Authentication System

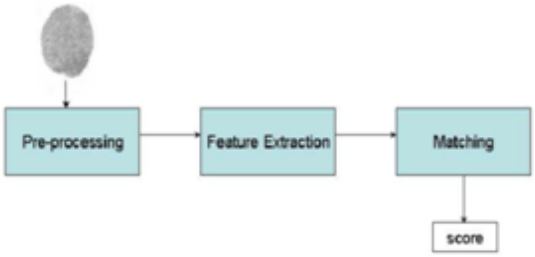


Fig.1 Fingerprint verification processes

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.

We in our project are using the Geometric Algorithm as it has various advantages as follows:

- It is very easy to implement and use.
- It is very efficient as compared to other methods.
- Moreover, it does not depend on any kind of technique that uses skin tone as one of its feature to be used for identification.

It basically, takes the fingerprint as the input from the user and calculates the R,G,B values of each pixel of the provided fingerprint as well as of the one stored in the database, then the squares of the difference of the R,G,B values of both the fingerprints is computed. If this value is greater than the threshold value then the pixel is different else it is the same. The number of same and different pixels is calculated, then with this value the difference percentage is computed. If the difference percentage is less than the predetermined threshold value then the fingerprint is matched and the user logs in to the system else the fingerprint is different and the access is denied.

2.2 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. To perform these tasks, a GSM modem must support an "extended AT command set".

2.2.1 AT Commands

AT commands are instructions used to control a modem. AT is the abbreviation of ATtention. Every command line starts with "AT" or "at". That's why modem commands are called AT commands. There are two types of AT commands:

- Basic commands are AT commands that do not start with a "+". For example, D (Dial), A (Answer), H (Hook control), and O (Return to online data state) are the basic commands.
- Extended commands are AT commands that start with a "+". All GSM AT commands are extended commands. For example, +CMGS (Send SMS message), +CMGL (List SMS messages), and +CMGR (Read SMS messages) are extended commands.

Thus, using the extended AT Commands OTP can be sent to any mobile number using the GSM Modem.

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

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

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