American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-6, Issue-8, pp-41-45
www.ajer.org
Research Paper Open Access

ATM Transaction Security Using Fingerprint Recognition

Mithun Dutta[1], Kangkhita Keam Psyche[2] and Shamima Yasmin[3]
Student, Department of CSE, Jahangirnagar University, Savar, Dhaka.
Corresponding Author: Mithun Dutta

ABSTRACT: *This paper deals with the solutions related to the ATM (Automated Teller Machine) security. Today, ATMs and Credit cards are used for the purpose of money transactions which play a vital role in the nature of trade. The weaknesses of existing authentication scheme such as password and PIN number caused the leakage of information stored in ATM smartcard which lead to the lost of money in bank account and private information misuses. To overcome this shortcoming of piracy in money transactions, we propose the idea of using fingerprints of customers as password included with traditional PIN number. After authorized 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. Fingerprint biometric of every person is unique and unchangeable as well as one of the famous techniques for smart card security.*

Keywords: *ATM, Fingerprint, PIN, Biometric.*

Date of Submission: 05-04-2017 Date of acceptance: 14-08-2017

I. INTRODUCTION

Today the ATM users are increase in numbers. An Automated Teller Machine (ATM) is a computerized telecommunications device that enables the clients of any financial institution to perform financial transactions like deposits, transfers, balance enquiries, mini statement, withdrawal and fast cash. The ATM machine has card Reader and keys as input devices and display screen, cash dispenser, receipt printer, speaker as output devices. ATMs are connecting 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. ATM card holders pin are different from each others. The number is verifying by the bank and allows the customers to access their account. The password is only identity so anyone can access the account when they have the card and correct password. Once the card and the password is stolen by the culprit they can take more money from the account in shortest period, it may bring huge financial losses to the users [2].

Biometric technology is the most widely accepted and mature biometric method and is the easiest to deploy and for a higher level of security. Using biometric identifiers offers several advantages over traditional and current methods. It is simple to install and also it takes little time and effort to acquire one's fingerprint with a fingerprint identification device. Thus, fingerprint recognition is considered among the least intrusive of all biometric verification techniques. Though fingerprint images are initially captured, the images are not stored anywhere in the system. Instead, the fingerprints are converted to templates from which the original fingerprints cannot be recreated; hence no misuse of system is possible.

II. RELATED WORK

ATM can be described as Any Time Money. We can get money at anytime anywhere only through ATM machines. To do the secure transactions we need biometric authentication. Biometric authentication is a growing and controversial field. Today biometric laws and regulations are in process and biometric industry standards are being tested. According to [11], there are three popular attacks against ATM: Skimming, PIN logging and Integrity violation. There are also attacks against mobile phone: Fake mobile apps installation, key logging software and grab PIN number during transmission. Besides that, an attack may also be a combination of both types of said attacks. Information also can be exploited by a side channel attack [4]. It is found that attackers try to get the user's account information that stored on the magnetic strip present at the back side of ATM card. Password is the only identity that can use to authenticate the owner of ATM card. It means anyone can access the account bank through ATM machine as the password entered is correct. So, once the ATM card

and password is lost or stolen by anyone, they can withdraw the money from that account easily without the problem of user authentication [4]. Thus, it can see that the most serious issue raised in ATM card security is about user authentication. User authentication is important because it lead to the integrity violation of bank account information. It seems that this issue is worse as anyone can access all information stored when they entered the correct password towards accessing ATM card at ATM machine. Other than that, it is strongly emphasized that the security issues need technology improvements and better security policy as a countermeasure.

Amurthy and Redddy [5] developed an embedded fingerprint system, which is used for ATM security applications. In their system, bankers collect customers' finger prints and mobile numbers while opening accounts, then customer only access ATM machine. The working of the ATM machine is such that when a customer place a finger on the finger print module it automatically generates every time different 4-digit code as a message to the mobile of the authorized customer through GSM modem connected to the microcontroller. The code received by the customer is entered into the ATM machine by pressing the keys on the touch screen. After entering it checks whether it is a valid one or not and allows the customer further access. Biometrics can be defined as 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.

III. PRESENT ATM SYSTEM

ATMs extend traditional banking hours by dispensing cash and making other transactions available 24 hours a day. At the beginning of 1974, there were only 1,656 operating ATMs. Today, online debit cardholders initiate approximately 12 billion ATM transactions per year at thousands of ATMs. In modern cash machines, the customer is identified by inserting a plastic ATM card with a magnetic stripe or a plastic smart card with a chip that contains a unique card number and some security information such as an expiration date. Authentication is provided by the customer entering a personal identification number (PIN) [8-wiki]. PIN is a four digit number which is generated by the respective financial institution. PIN is very easily remembered and is also changeable according to the user and PINs are 4-digit numbers in the range 0000-9999 resulting in 10,000 possible numbers, so that an attacker would need to guess an average of 5000 times to get the correct PIN [1][12]. The PIN supplied by the customer is always compared with the recorded reference PIN in the financial institutions. In the present system, the user has to insert the card and the PIN number. If PIN is correct, the system allows for transaction. Otherwise, the system asks for PIN again and it allows maximum of three times to enter it.

IV. PROPOSED ATM SYSTEM

The proposal is to use fingerprints in ATMs as passwords involved with the PIN number. Fingerprint recognition will make users relax by preventing unauthorized account access and assuring security. Here, a fingerprint module generates 4-digit code as a message to the customer's assigned mobile number by placing finger on it and on the basis of validation of this code, customers are allowed for further access.

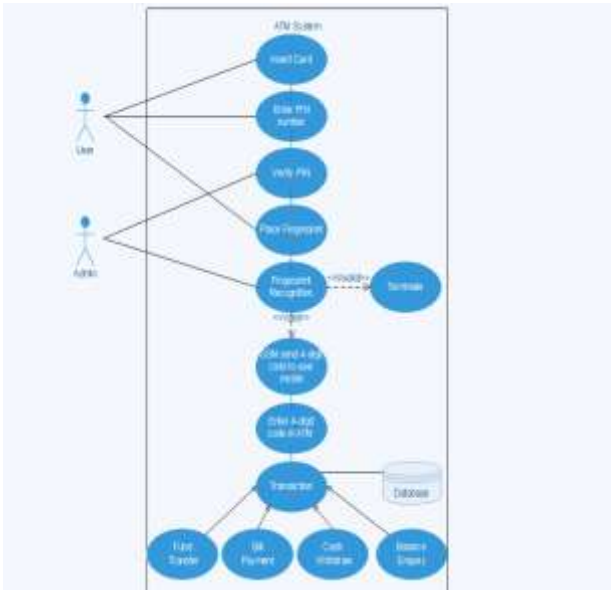
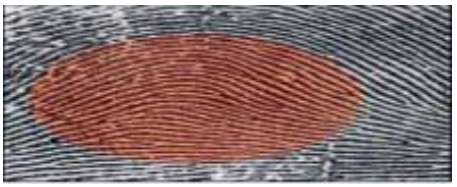


Fig: 4.1 Use case diagram

V. FINGERPRINT RECOGNITION AND VERIFICATION

Fingerprint image (over view): A fingerprint in its narrow sense is an impression left by the friction ridges of a human finger. In a wider use of the term, fingerprints are the traces of an impression from the friction ridges of any part of a human hand. A friction ridge is a raised portion of the epidermis on the fingers and toes (digits), the palm of the hand, consisting of one or more connected ridge units of friction ridge skin. [9]

Loop: In a loop pattern, theridges enter from from either side, re-curve and pass out or tend to pass out the same side they entered



Arch: In a arch pattern, theridges enter one side, make a rise in the center and exit generally on the opposite side

Whorl:In a whorl pattern,theridges are UsuallyCircular

Block Diagram of fingerprint recognition:

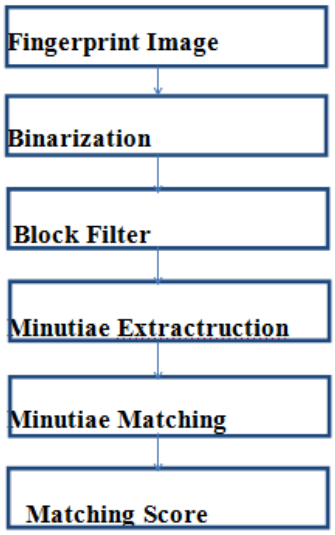


Fig 5.1: Block diagram of fingerprint recognition

Fingerprint: A fingerprint is the feature pattern of a finger
Binarization: A Process to convert gray scale image into binary image by fixing the threshold value.
Block Filter: A process to to reduce the thickness of all ridge lines to a single pixel width to extract minutiae points effectively.
Minutiae Extractruction: The minutiae location derived after minutiae extraction.
Minutiae Matching: To compare the input fingerprint data with the template data Minutiae matching is used.
Matching Score: it is used to calculate the matching score between the input and template data

Software Design: This software is implemented by the steps as follows: first of all. The system is initialized to implement specific task, such as checking ATM system, GSM communication and so on, and then each module reset for ready to run commands. Before using ATM terminal, the mobile number and fingerprint of the customer is required.

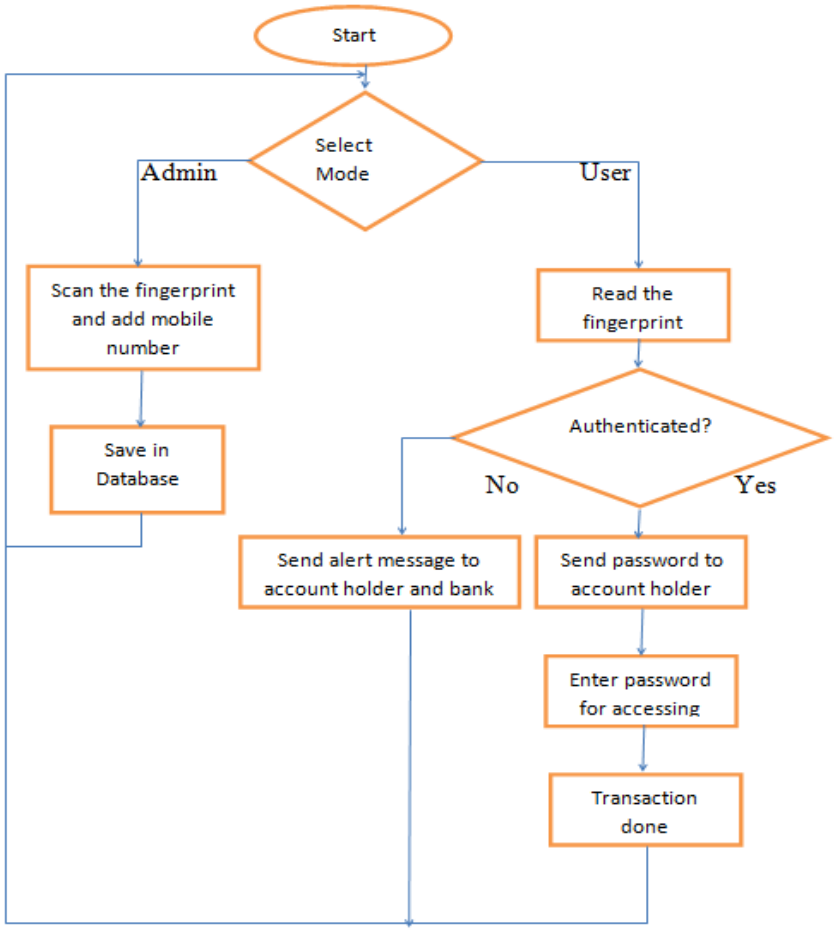


Fig 5.2: Workflow of the software

Algorithm for fingerprint recognition:
Input: Grey-scale Fingerprint image.
Output: Verified fingerprint image with matching score.
1. Fingerprint is binarized
2. Thinning on binarized image
3. Minutiae points are extracted. Data matrix is generated to get the position, orientation and type of minutiae.
4. Matching of test fingerprint with template
5. Matching score of two images is computed, if matching score is 1 images are matched and if it is 0 then they are mismatched.

Implementation:
The following hardware components are needed to implement the system. They have to be integrated together just like the figure 5.2
1. Microcontroller (LPC2148)
2. Fingerprint Module (FIM3030)
3. GSM Modem
4. User Interface
5. Power Supply

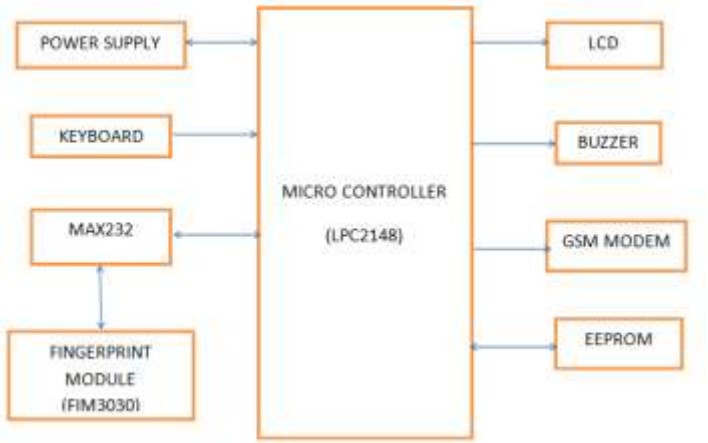


Fig 5.3: System Overview

VI. ADVANTAGES OF THE NEW PROPOSED SYSTEM

1. The proposed system will improve the level of security of ATM transaction system.
2. Initially captured fingerprint images are converted to templates instead of storing anywhere which makes misuse of the system totally impossible.
3. Customers need not to be anxious about secure transaction.
4. This system is easy to install, less time consuming and mostly approved biometric method.

VII. CONCLUSION

Automatic Teller Machines is the most used technology in the increasing financial transaction of the current world. There are many possible way to misuse ATM card using PIN. Fingerprint recognition helps to achieve an authentic state of security access through verification and validation. This paper identifies a high level model for the modification of existing ATM systems using both security protocols as PIN & 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 [2].

REFERENCES

[1]. Sowmya Ravikumar, Sandhya Vaidyanathan, B. Thamotharan, S. Ramakrishnan, A new business model for ATM transaction security using fingerprint recognition, International Journal of Engineering and Technology (ISSN : 0975-4024), Vol 5 No 3 Jun-Jul 2013.
[2]. V. Padmapriya, S. Prakasam, Enhancing ATM Security using Fingerprint and GSM Technology, International Journal of Computer Applications (0975 – 8887), Volume 80 – No 16, October 2013.
[3]. Lynne Coventry, Antonella De Angeli and Graham Johnson, Usability and Biometric Verification at the ATM Interface, Springer Verlag, London, 2000.
[4]. Nor Fazlina Mohd Amin, Shorayha A/P Eh Chong, Nur Zafirah Abd Hashim, Hassan Chizari, Security Issues in ATM Smart Card Technology, International Journal of Mathematics and Computational Science, Vol. 1, No. 4, 2015, pp. 199-205, http://www.aiscience.org/journal/ijmcs
[5]. Moses Okechukwu Onyesolu, Ignatius Majesty Ezeani, ATM Security Using Fingerprint Biometric Identifer: An Investigative Study, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No.4, 2012.
[6]. Ayesha Khatoon R. Syed, Vijay R. Wadhankar, Theft Identification and Remote Information of ATM Card by a Unique System, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064, Volume 4 Issue 7, July 2015.
[7]. https://leesys.wordpress.com/2011/02/12/atm-project-report/
[8]. Arun Ross, A Prototype Hand Geometry-based Veri_cation System.
[9]. Omari, Richard Kwaku Bamfo (PG4134210), An assessment of the use of Automated Teller Machine (A.T.M) of Barclays Bank Ghana Limited Akim Oda Branch, Kwame Nkrumah University of Science and Technology, SEPTEMBER 2012.
[10]. Mr. Mahesh A. Patil Mr.Sachin P.Wanere Mr.Rupesh P.Maighane Mr.Aashay R.Tiwari, ATM Transaction Using Biometric Fingerprint Technology, International Journal of Electronics, Communication & Soft Computing Science and Engineering ISSN: 2277-9477, Volume 2, Issue 6.
[11]. Pennan 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.
[12]. Petrlic, Ronald, and Christoph Sorge. Establishing user trust in automated teller machine integrity. IET Information Security, 2013. 8(2) p: 132-139.
[13]. Namrata, Dr. Sukhvir Singh, Review paper on enhance the ATM security using fingerprint recognition, International Journal of Computer Science and Mobile Applications, ISSN: 2321-8363, Vol.3 Issue. 10, October- 2015, pg. 38-47.

Mithun Dutta " ATM Transaction Security Using Fingerprint Recognition." American Journal of Engineering Research (AJER) 6.8 (2017): 41-45.