Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Security Management Access Control System

Ajinkya M. Ghadge[#1], Taruna V. Hingorani[#2]
[#]*Computer Engineering, Watumull Institute of Electronics Engineering & Computer Technology*
[*]*Electronics and Telecommunication, Watumull Institute of Electronics Engineering & Computer Technology*

Abstract*—Authenticating a legitimate user is a trivial task, which is involved in a door lock system, safe lock and also in ATM transactions while accessing bank accounts to secure personal information. Security is a major concern due to large number of criminal and malicious activities. For better understanding let's consider the security feature of an ATM machine which uses the access card along with its PIN for verification. Now this basic level of security provided by the PIN can be enhanced along with fingerprint verification. In the proposed system we have ingrained the Global System for Mobile Communications (GSM) modem that connects to the core controller. It generates a one-time password (four digit) that is sent to the primary user's mobile number when the user (primary user or secondary user) enrolls the fingerprint. The fingerprints of the secondary user along with the cardholder (primary user) are saved inside the database. Every fingerprint entered is validated by the database. The four digit PIN should be enrolled using a keypad. Further, the transaction is completed on entering the exact information. In case the cardholder is unable to do the transaction the system also provides a facility for fingerprint identification of the nominee. Since biometric features are unique; the proposed system will solve the issue of account security. This system can be designed using ARM7 LPC2148 as a core controller. It also uses SM630 fingerprint module to capture fingerprints, which consists of an optical sensor and DSP processor. This system can be integrated with any application because of the uniqueness provided with fingerprints. Additional convenience is provided with low power requirement alongside portability.

Keywords*— fingerprint, GSM modem, one time password (OTP), personal identification number (PIN).*

I. INTRODUCTION

Expeditious development in the field of technology has modified the way we do banking activities. One such technology, which impacts banking in various ways, is the arrival of ATM without the need of human interactions. Looking at the increase in banking activities today the ATM cards are used for cash transfers, withdrawals and several such similar transactions thereby fostering the need to focus on security applications [1]. A modern day Automatic Teller Machine commonly comprises of constituents like Central Processing Unit to control the user interface and other mechanism for transactions, a Chip card reader to note the customer PIN, Pad and a protected crypto-processor generally within a secure cover a display to be used by the user for performing specific operations, key buttons, a Receipt Printer to provide the customer with a receipt of their transaction, and other elements of the machinery, which require controlled access like Vault, Housing for aesthetics, Sensors and Indicators [2].

The user's sensitive account information is stored on the backside of the ATM card. After entering the card inside the card-reader the corresponding data is captured which is utilized in the transactions. The ATM then validates and requests for the corresponding 4 digit PIN that is available to all the cardholders. The PIN is validated by the bank, which then allows the user to perform any transaction. The password being the sole security facility besides the card, once breached can allow any user to perform any sort of malicious activity.

To strengthen this security model the proposed system introduces new technology, which uses fingerprint identification system alongside the nominee of the cardholder, and also Global System for Mobile communication (GSM) technology. Biometrics being a technology that makes your data tremendously secure, distinguishing each user by their physical characteristics. Fingerprint based identification being the most mature and sophisticated technique is widely deployed and easiest way to provide higher level of security at your fingertips. It is also the least intrusive biometric available today. The fingerprint of the cardholder along side the nominee will be stored inside the banks database and will be validated during the transactions, the requesting user then has to enter the PIN to further process the transaction. The bankers validate the fingerprints; if approved with verification from the database then the 4-digit code is sent to the user using the GSM (Global system for mobile communication) technology.

GSM merely connects your device to the nearest base station in the cell to receive the OTP message. The GSM modem linked to the micro-controller delivers the 4-digit code to the mobile number of the legitimate user. The user can then access his/her account after he/she enters the one time password. Followed by which the user can perform transactions like deposits or withdrawal, etc. [1].

Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

II. FEATURES OF THE SYSTEM

The verification technique used in the proposed system is based on fingerprint recognition. Using the RFID tags and GSM modem enhances the ATM security. The core controller being LPC2148 is interfaced with the modules. The functions of each module are as follows:

A. Fingerprint Detection

The fingerprint information of the main user is used for Identification. The user is permitted access to the ATM after authorization of the fingerprint.

B. One Time Password

A unique code provided to complete the transaction i.e. OTP. This OTP is non identical for every payment.

C. Remote Authentication

The system compares the customer's fingerprint information with distant statistics stored in the server.

D. Alarming

A message containing a 4-digit code will be sent as an alarm to the main user if there is any faulty transaction-taking place. This code will help putting the alarm off.

E. Analysis Methods

Fingerprint recognition and password recognition can be used for the proposed system [4].

III.BLOCK DIAGRAM

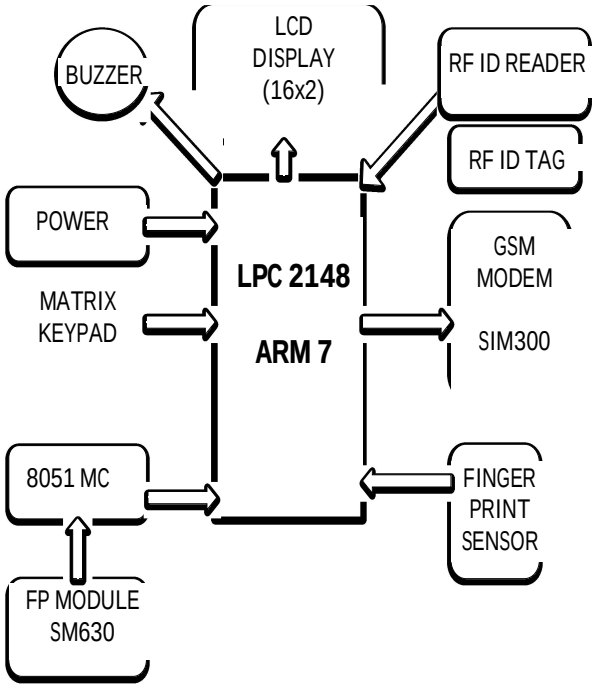

Fig. 1 Components of the system

IV.HARDWARE COMPONENTS

A. ARM7: The ARM7TDMI-S is a 32-bit microcontroller established on Reduced Instruction Set Computer (RISC) engineering. It offers low power consumption and provides high performance.

B. Fingerprint sensor: The SM 630 FPS (fingerprint scanner) consists of an optical sensor that is mounted on a small circuit board.

C. GSM modem: The modem connects with the user equipment by providing the OTP for further transaction.

D. LCD module: A display (16*2 LCD) is used at the ATM terminal.

Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

E. Keypad: A 3*4 matrix (12 keys) or 4*4 matrix (16 keys) keypad is used to provide an input for the PIN and OTP.

F. Power supply: The microcontroller and other devices get power supply from the voltage regulator (AC to DC voltage).

G. RFID reader & card: Radio-frequency identification (RFID) is a method that automatically detects information through RFID transponders that store and retrieve data.

V. SOFTWARE COMPONENTS

The arm seven LPC2148 is programmed using KeiluVision 3, which is a window based platform incorporating a robust and modern editor along with a project manager and make facility tool for development. It comprises tools to build embedded applications including HEX file generator, C/C++ compiler, linker/locator and macro assembler.

The simulator of KEIL can perform in depth simulation of a micro controller and its external signals.

Just by entering crystal frequency one can see the precise execution time of an assembly instruction or a single line of C code. Also a window can be opened for each peripheral on the device, indicating its state.

VI. WORKING STEPS

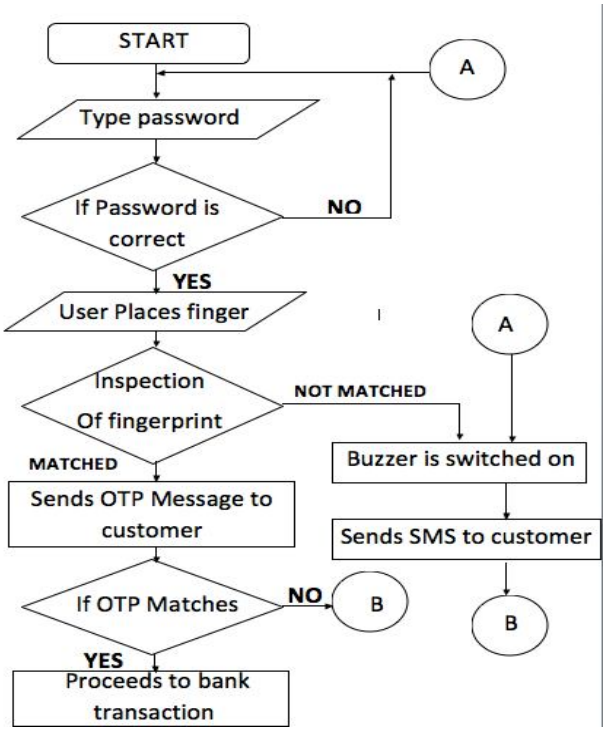

Fig. 2 Flow Chart

The steps that complete the given transaction are as follows:

Step 1: Swipe the ATM card and enter the card's password.

Step 2: The message is then sent to the customer.

Step 3: Choose the type of user, Primary User or Secondary(nominee) User.

Step 4: Access the fingerprint. The client's fingerprint, which is already saved in the database. (Step 4 follows for main user)

Step 5: The message is sent to the customer thereby triggerring the buzzer ON, if authentication fails. The card is dislodged by the machine.

Step 6: GSM sends the four digit OTP to primary user's cell phone number.(Step 6 is followed after step 4 if authentication is successful.)

Step 7: After this the customer has to enter the 4 digit OTP which is received.

Step 8: The user can complete his/her transaction. The card is retured to the user once the tranaction is complete.

Step 9: (For the secondory user) the user must enter the fingerprint then step-6, step-7, step-8 follows.

VII. ADVANTAGES

A. The GSM equipment connects the mobile devices to the nearest base station by looking for cells in the vicinity thereby making authentication faster.
B. The biometric (fingerprint) authentication will increase security.
C. If necessary the nominee user can approach the account.
D. A unique OTP is sent to the user during every transaction. This increases security for the account.

VIII. LIMITATIONS

A. Multiple authentications during the initial stages consume time. Due to this reason the system requires fast, reliable and efficient technology.
B. Speed of execution can be enhanced with the use of more sophisticated microcontroller.
C. The cost of Biometric identification devices is high. The cost can reduce in future once these devices are popular and regularly used.

IX. FUTURE SCOPE

The fingerprint authentication can be made more advanced by using the latest fingerprint sensors/scanners such as ultrasonic sensor (Qualcomm sensor id) that detects the ridges of the fingerprint, thereby reducing fraud or deceit.
Increasing the biometric authentication, eye validation/verification can be implemented to increase security. Developing an app for direct access of an ATM, locker or safe where the mobile equipment has a fingerprint detection sensor.

X. CONCLUSION

The ATM prototype can be efficiently used with fingerprint recognition. The ATM's have become widespread and mature to provide financial assistance to a large section of population in many countries. Biometrics, especially fingerprint identification has still carved an important position to provide a secure access in the authentication processes. This proposed system would definitely help us achieve a prominent model for conversion of existing ATM systems, which use security protocols as PIN & Biometric fingerprint strategy along with GSM technology.
This system when fully deployed will undeniably reduce the rate of criminal activities on the Automatic Teller Machines such that only the legitimate user and the secondary user can have access to the transactions, also allowing the secondary user to make transactions in case of emergencies. Also core controller LPC2148 and SM 630 shall provide low power consumption platform.

REFERENCES

[1] Pennam Krishnamurthy, M.Madhusudan Reddy. "Implementation of ATM security by using fingerprint."
[2] 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): 68.
[3] Deddarma, Sri Shimal Das and Smt.Jhunnu. "Designing a biometric strategy(fingerprint) measure for enhancing ATM security in Indian E-Banking system-2011." International Journal of Advance Research In Science And Engineering Vol. No.3, Issue No.9, no. ISSN-2319-8354(E) (September 2014): 122.
[4] Ravi J K.B.Raja, V. K. (n.d.). Fingerprint recognition using minutia score matching.
[5] ARM7TDMI Data Sheet. (1995 йил August). Advanced RISC Machines Ltd (ARM) .
[6] ESaatci, V. T. (2002). Fingerprint image enhancement using CNN gabor-Cpe filter[C]. Proceedings of the 7th IEEE International Workshop on Cellular Neural Networks and their Applications 377-382.
[7] G.Sekar, N.Selvaraj &. "A method to improve the security level of ATM banking systems using AES algorithm." international journal of computer applications(0975-8887) volume 3- no.6. (june 2010.).
[8] ARM7TDMI Data Sheet. (1995 йил August). Document Number: ARM DDI 0029E .