RESEARCH ARTICLE OPEN ACCESS

Atm Client Authentication System Using Biometric Identifier & Otp

Jaydeep Shamdasani[*1], Prof .P.N.Matte[*2],
**1(E &TC department, GHRCEM Pune, India.)*
**2(Head of E&TC Department, GHRCEM Pune, India)*

ABSTRACT
In this paper we propose a design, to add more security to the current ATM systems by using biometric and GSM technology. In conventional method identification is done based on ID cards and static 4 digit password. Whereas in our purposed system, Bankers will collect the customer fingerprints and mobile number at the time of opening the accounts then only customer will be able to access ATM machine. The primary step of this project is to verify currently scanned fingerprint with the fingerprint which is registered in the bank during the account opening time. If the two fingerprints get matched, then a message will be delivered to the user's mobile which is the random 4 digit pin number to access the account. For every transaction new pin numbers will be send to the user's mobile thus there will not be fixed pin number for every transaction. Thus, Pin number will vary during each transaction .

Keywords ATM Terminal, Fingerprint Recognition, GSM Module, LINUX.

I. I.INTRODUCTION

The Modern banking technology has altered the way banking activities are usually done. One banking technology that has impacted to banking activities is the automated teller machine (ATM). Due to ATM technology, a customer is able to perform different banking activities such as cash withdrawal, transferring money, paying phone bills and electricity bills. In a short, ATM provides facilities to customers such as quick, easy and convenient way to access their bank accounts and to conduct financial transactions. Talking about ATM security, Personal identification number (PIN) or password is very important.PIN or password is widely used to secure financial/confidential information of customers from unauthorized access.

An ATM is a IT enabled Electro-mechanical system that has connectivity to the accounts of a banking system. It is computerized machine developed to deliver cash to bank customers without human intervention; it can be used to transfer money between different bank accounts and provide basic financial facilities such as balance enquiry, mini-statement, cash withdrawal, fast cash ,etc.

In this project the fingerprint sensor sense the thumb impression of the corresponding person and that image will be compared with registered image, if the both images are unique, then the finger print device activates particular task like access to the system, identification of the customer. The project operation contains 2 modes, the first one is

Administration mode and the second is User mode. The Administration mode is used to register the new user and gives the mode of authorization. The Administration mode has the ability to create and delete the users. The user mode is mode used for the authentication of the bank customer. In user mode of authorization, creation and deletion of a user cannot be performed.

The paper is arranged as follows. Section II deals with Research background. Section III provides the key components of Proposed ATM system. Section IV deals with Hardware Architecture. Section V described Software design. Section VI is dedicated for Fingerprint Recognition process. Section VII elaborate about GSM technology used. Section VIII presented the results and the discussions on the results and conclusion.

II. RESEARCH BACKGROUND

Crime at ATMs has become a nationwide issue that faces not only customers, but also bank operators and this financial crime case rises repeatedly in recent years. A lot of criminals tamper with the ATM terminal and steal customers' card details by illegal means. Once users' bank card is lost and the password is stolen, the users' account is vulnerable to attack. Traditional ATM systems authenticate generally by using a card (credit, debit, or smart) and a password or PIN which no doubt has some defects. The prevailing techniques of user authentication, which involves the use of either passwords and user IDs (identifiers), or identification cards and PINs (personal identification numbers), suffer from several limitations. Passwords and PINs can be illicitly acquired by direct covert observation.

When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Despite warning, many people continue to choose easily guessed PIN's and passwords - birthdays, phone numbers and social security numbers. Recent cases of identity theft have heightened the need for methods to prove that someone is truly who he/she claims to be. Biometric authentication technology may solve this problem since a person's biometric data is undeniably connected to its owner, is nontransferable and unique for every individual. The system can compare scans to records stored in a central or local database or even on a smart card. Biometrics can be defined as a 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. It is a measure of an individual's unique physical or behavioral characteristics to recognize or authenticate its identity. Common physical biometrics characteristics include fingerprint, hand or palm geometry, retina, iris and face while popular behavioral characteristics are signature and voice. Biometrics technologies are a secure means of authentication because biometrics data are unique, cannot be shared, cannot be copied and cannot be lost.

III. THE CHARACTERISTICS OF SYSTEM

The proposed ATM client authentication system depends on fingerprint recognition which is developed after analyzing existing ATM systems. The ARM 9 microcontroller (Friendly ARM) is used as the brain of these embedded systems along with fingerprint recognition module and GSM Module.
The primary components are shown as follows:

ARM 9 Microcontroller: It is the central controlling unit of the system. It controls all the peripherals.

Fingerprint recognition Module: The user's fingerprint was used as the standards of identification. It must verify the feature of the customer fingerprint before using ATM terminal.

GSM Module: It sends different 4-digit code as message to the registered mobile number of the customer for accessing the ATM.

IV. HARDWARE DESIGN

The S3C2440 chip is used as the core of entire hardware. The modules of LCD/Touch-screen, keyboard, fingerprint recognition, GSM Module are connected with the core S3C2440.The SRAM and FLASH are also embedded in this system.

The system consist of following modules :-
1.LCD module: The OMAP5910 is used as LCD module in LCD controller, it supported 1024*1024 images of 15 gray-scale or 3375 colours.
2. Keyboard/Touch-Screen module: It is used for inputting passwords.

3.Fingerprint recognition module:
FIM3030 fingerprint module is used for recognition of is used for recognition of fingerprints. This module uses optical sensor for capturing and detecting of fingerprint images.

4.GSM Modem: A GSM modem(SIM 300) provides an interface that allows sending and receiving messages over the modem interfaces.

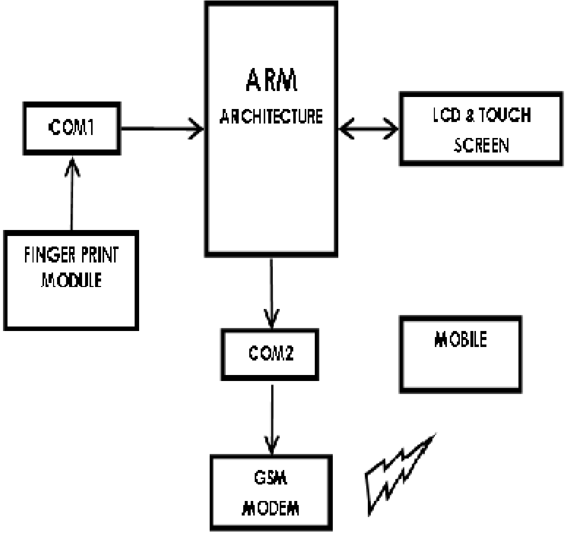

Figure1:- BLOCK DIAGRAM ATM SCURITY SYSTEM

Before providing ATM access, the fingerprint module will compare scanned fingerprint with fingerprint taken at the time of opening account, if the figure print is correct 4 digit OTP is send to registered mobile number of user. The block diagram of hardware architecture is shown in figure no 1.

V. SOFTWARE DESIGN

The system operates in below two modes.
Admin mode*:* In this mode the user finger print and mobile number are collected and saved at the time of opening the account.

User mode*:* In this mode the user finger print is validated with saved fingerprint for the identification which is required to perform transactions.

This software system is designed as follows: first of all the Linux kernel and the File systems are loaded into the ARM 9 controller.In next step, the system is initialized to check specific task, such as checking ATM terminal, GSM module and so on, and then each module is reset for ready to run commands. Before accessing ATM system, the mobile number and fingerprint of the customer are needed to be authenticated.

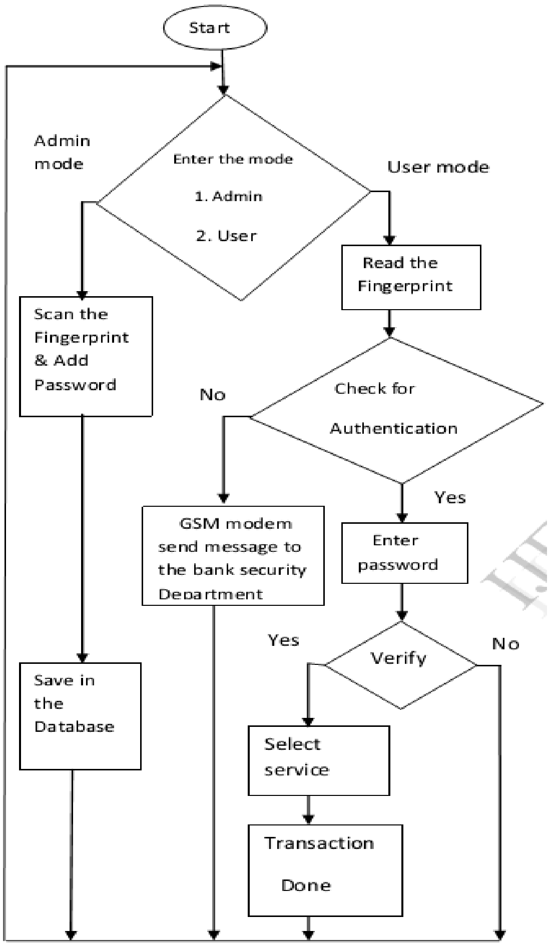

Figure 2:- The overall flow chart of Software

Step 1.The system will ask for the owner's fingerprint.

Step 2. If fingerprint is authenticated, the system would send password to the Registered mobile of Client.

Step 3. User will enter the received password in the touch-screen in order to access the ATM system.

Step 4.If authentication succeeds the access is given to user for banking transactions.

Step 5. If authentication fails then system sends the alert/warning message to the Account owner and Bank officials.

The flow chart of software design is shown in figure no 2.

In the process of capturing & validating fingerprint, the FIM3030 fingerprint module is used for recognition of fingerprints. This module uses optical sensor for capturing and detecting of fingerprint images. The captured fingerprint information will be temporarily stored in SRAM and then compared with clients fingerprint. The result of process is controlled by ARM9(S3C2440).

VI. FINGERPRINT RECOGNITION PROCESS

The analysis of fingerprint matching needs the comparison of several features of the print pattern. This consists patterns which are aggregate characteristics of ridges & minutia points. These are unique features found within the patterns. It is important to know the structure and properties of human skin to successfully recognize the scanned fingerprint.

In our proposed system the User’s currently scanned fingerprint will be validated with fingerprint of user stored at the time of opening account. If authentication succeeds further access is given to customer.

Patterns
The three patterns of fingerprint ridges are i) arch, ii) loop & iii) whorl.

***Arch*:** The ridges enter from side of the finger then rise in the center which forms an arc then exit the other side of the finger.

***Loop*:** The ridges enter from side of a finger, forming curve then exit on that same side.

***Whorl*:** Ridges form circularly around a central point on the finger.
Fingerprint processing has three primary functions i) enrol, ii) search, iii) verify.

Enrollment captures fingerprint image from the sensor. Then image is processed, enhanced, and then compressed to form fingerprint template. Various filters filter the captured image and translate it to mathematical expression, making it difficult to steal template and directly recreate fingerprint image.

Search compares scanned image to a list of enrolled fingerprint templates, through a series of screening processes. This algorithm reduces the list of templates to a manageable size. The templates that survive filtering are matched with currently scanned template and verification scores are provided. A score exceeding threshold score represents positive identification.

Verification validates a user's identity by matching candidate image to previously captured template with the use of real time & closed loop pattern matching algorithms. A score is returned after comparison representing degree of matching between candidate and template to take yes or no match decision.

Fingerprint Recognition Algorithm:

To authenticate the user by automatically extracting minutiae from user's scanned fingerprint image, fingerprint recognition algorithm is required. The fingerprint recognition algorithm involves two main steps :-

Step 1 :- Image processing step in which characteristics of scanned fingerprint are captured by having image under-going several stages,.
Step 2 :- Matching algorithm step in which user authentication is done by comparing feature data comprised of minutiae with Fingerprint Template captured at the time of opening account .

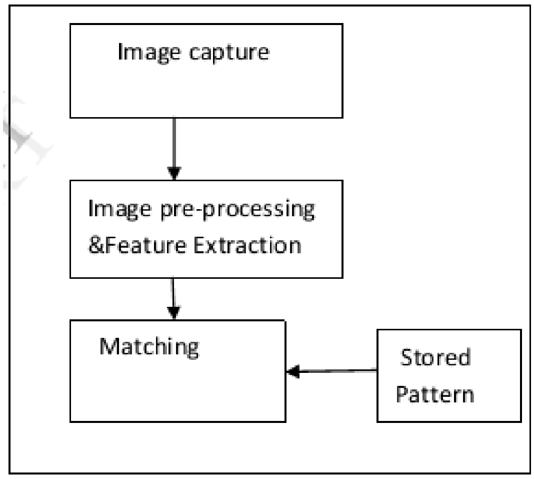

Figure 3:- Fingerprint recognition process

VII. GSM Module (SIM 300)

Global System for Mobile Communication (GSM) is a set of standards that specify the infrastructure for a digital cellular service . The standard is used in around 85 countries in the world , TC35 GSM engines operate in the GSM 900 MHz and GSM 1800 MHz frequency bands. Designed to easily provide radio connection for voice and data transmission both modules integrate seamlessly with a wide range of GSM application platforms and are ideally suited to design and set up innovative cellular solutions with minimum effort. The complete RF part is incorporated and the GSM protocol runs autonomously on a GSM baseband processor. The GSM engine uses a single 40-pin ZIF connector that connects to the cellular device application. The ZIF connector establishes the application interface for control data, audio signals and power supply lines. The cellular device application forms the Man-Machine Interface (MMI).

Access to the GSM engine is enabled by a serial interface .The mobile communication is becoming important aspect because of digital revolution. Every day millions of people make phone calls with the help of few buttons on cell phone. Very less is known about how mobile communication works.

Also less is known about security aspects and protection behind these systems. The cell phone complexity is increasing day by day as people have started sending text messages, multimedia messages and digital pictures to their friends/family. The cell phone is slowly becoming hand-held computer. All the features/advancements in cell phone technology require backbone to support it. The system has to provide better security and should be adaptive to accommodate future enhancements. General System for Mobile Communications, GSM, is one of the many solutions out there. GSM has been dubbed the "Wireless Revolution" and it doesn't take much to realize why GSM provides a secure and confidential method of communication.

In our proposed system once the fingerprint gets authenticated the User will receive 4 digit OTP on his registered mobile number. Then user enters this PIN and gets further access.

VIII. RESULTS AND CONCLUSIONS

The prototype of ATM systems authentication based on fingerprint identification will be implemented. Here we will build a system that will be stable and safe for ATM access. In the results, it will be deduced that the use of biometric security systems offers a much better authentication of ATM systems and will take advantages of the stability and reliability of fingerprint characteristics, and a new biological technology based on the image enhancement algorithm. Additionally, the system will also include the original verifying methods which are inputting owner's password. These days, still majority of ATM machine in many countries there are using magnetic card reader, so there is a need to change a method of authentication in future in order to eliminate the drawbacks identified in this project. The whole system will br built on the technology of embedded system which makes the system more safe, reliable and easy to use.

REFERENCES

[1] Pennam Krishnamurthy & 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, 2012.

[2] D. Vinod kumar, & Prof.M R K Murthy "Fingerprint Based ATM Security by using ARM7" IOSR Journal of Electronics and Communication Engineering ISSN : 2278-2834 Volume 2, Issue 5 (Sep-Oct 2012), PP 26-28.

[3] http://en.wikipedia.org/wiki/Automated_tellermachine

[4] Mr. John Mashurano & Mr. Wang liqiang "ATM Systems Authentication Based On Fingerprint Using ARM Cortex-M3"International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol.2 Issue 3, March – 2013.

[5] Moses Okechukwu Onyesolu & Ignatius Majesty Ezeani "ATM Security Using Fingerprint Biometric Identifer: An Investigative Study" International Journal of Advanced Computer Science and Applications, Vol. 3, No.4, 2012.

[6] CH S N Sirisha Devi & Maya patil "SECURITY SYSTEM FOR ATM TERMINAL BY USING BIOMETRIC TECHNOLOGY AND GSM" Global Journal of Advanced Engineering Technologies, ISSN: 2277-6370 Vol1-Issue3-2012.