ARM 7 BASED MULTI LEVEL SECURITY FOR ATM ACCESS USING FINGER PRINT AND GSM TECHNOLOGY

M.S.Umamaheswari[1], Mr.G.Rama krishan [2]

[1]M.Tech II Yr (Embedded systems), [2]Professor, Dept of ECE,
SVCET, Chittoor, AP (India)

ABSTRACT

Identification and verification of a person today is a common thing; which may include door-lock system, safe box and vehicle control or even at accessing bank accounts via ATM, etc which is necessary for securing personal information. There is need for improve security in ATM transactions. Due to tremendous increase in the number of criminals and their activities, the ATM has become insecure. ATM systems today use an access card and PIN for identity verification. The Personal Verification Number (PIN) only not gives good security. The fingerprint is unique and cannot duplicate by others. This system combines the pin verification and fingerprint recognition technology for identification. With fingerprint recognition technology and pin verification we embedded the GSM modem connected to the microcontroller generates the 4 digit one time password and it send to the main user mobile number when the user (main user or nominee user) enrol the fingerprint. The fingerprint of the nominee and the card holder are collected and stored in the database. Every fingerprint which enrols is check by the db. The 4digit one time password should be entered by pressing the keys on the touch screen. After enter all the correct information customer can begin the further transaction. We also proposed nominees fingerprint identification process while actual card holder unable to do the transactions. The biometric features cannot be replicated; this proposal will go a long way to solve the problem of account safety. Authors design a simple fingerprint recognition system using LPC2148 as a core controller. The system uses SM630 fingerprint scanner to capture fingerprints with its DSP processor and optical sensor. This system can be employed at any application with enhanced security because of the uniqueness of fingerprints. It is convenient due to its low power requirement and portability.

Keywords: ARM 7 Processor, Finger Print Recognition Module, GSM Module,OTP .

I 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 increase in numbers. They use the ATM cards for banking transactions like deposits, transfers, balance enquiry, mini statement, withdrawal, fast cash, etc [1].

A modern ATM is typically made up of the devices like CPU to control the user interface and devices related to transaction, Magnetic or Chip card reader to identify the customer, PIN Pad, Secure crypto-processor generally within a secure cover, Display to be used by the customer for performing the transaction, Function key buttons, Record Printer to provide the customer with a record of their transaction, to store the parts of the machinery requiring restricted access -Vault , Housing for aesthetics, Sensors and Indicators [2]. 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 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 [3].

To increase security level we are introducing new technology which works the technology fingerprint recognition system and nominee for the main user and GSM technology. Biometrics is a technology that helps to make your data tremendously secure, distinguishing all the users by way of their personal physical characteristics. The fingerprint based identification is one of the most mature and proven technique [4]. Fingerprint technology is the most widely accepted and mature biometric method and is the easiest to deploy and for a higher level of security at your fingertips.Thus, fingerprint recognition is considered among the least intrusive of all biometric verification techniques.

The fingerprint of the card and nominee will be stored in the db of the bank when the cardholder or the nominee tries to access the account; they will have to enter the pin and need to enroll the fingerprint. The finger print is check by the bankers, if it is in the data base the 4 digit code is send to the user by the GSM technology (Global system for mobile communication).

The GSM technology is cellular network which means that mobile phone connect to it by searching for cells in the immediate vicinity [3]. The GSM modem connected to the microcontroller generates the 4 digit code to the main user mobile number [1]. The user can access the account after he/she enter one time password. After they can begin the transactions. We made the transactions what we want like deposits or withdrawal, etc. After complete our transaction we can get the card.

1.1 The characteristics of system design

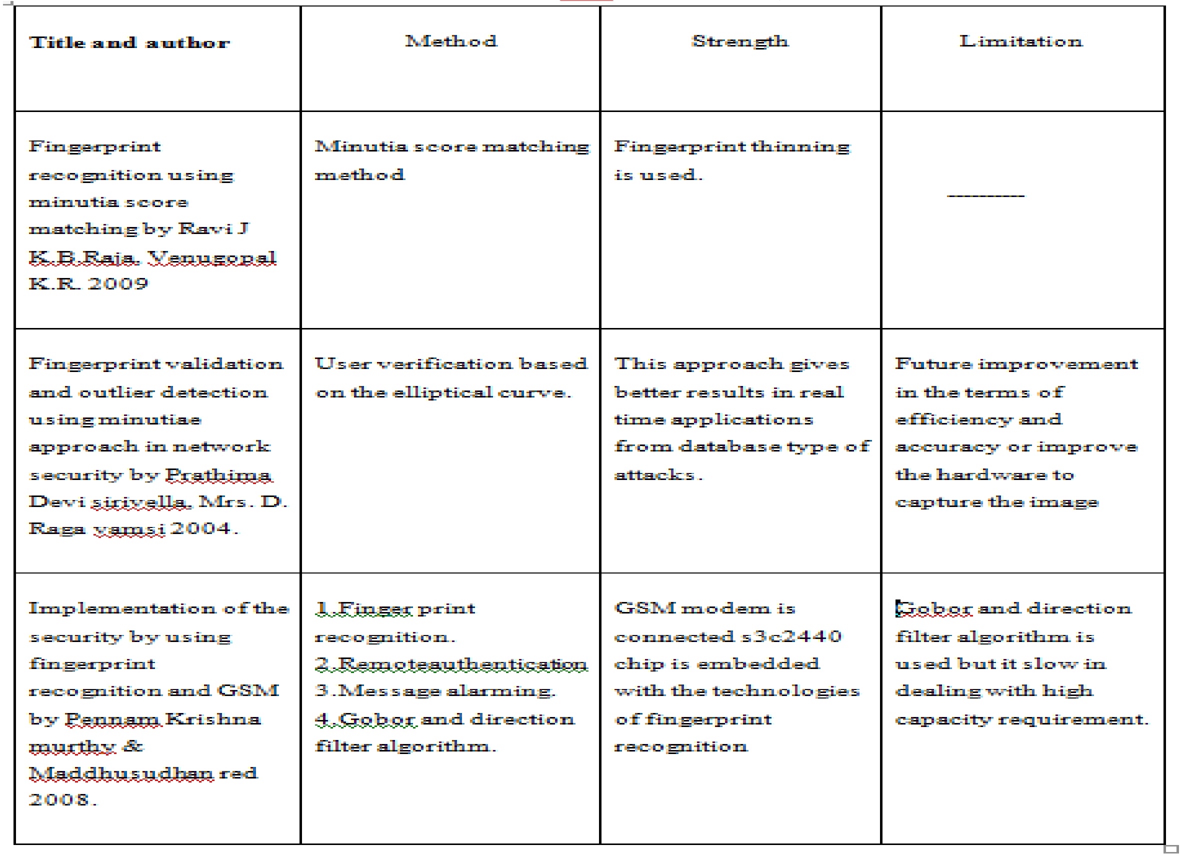
The embedded ATM client authentication system is based on fingerprint recognition which is designed after analyzed existed ATM system. The LPC2148 chip is used as the core of these embedded system which is associated with the technologies of fingerprint recognition and current high speed network communication. The primary functions are shown as follows:

1. **Fingerprint recognition:** The masters' fingerprint information was used as the standards of Identification. It must certify the feature of the human fingerprint before using ATM system. Which was stored in data base.
2. **Remote authentication:** System can compare current client's fingerprint information with remote fingerprint data server.
3. **OTP:** This is One Time Password which is used for increasing security of money transaction. This code will be different for each payment..
4. **Message alarming:** different 4 digit code as a message to the mobile of the authorized customer without any noise, in order to acess the Terminal.
5. **Two discriminate analysis methods:** Besides the fingerprint recognition, the mode of password recognition can be also used for the system.

II LITERATURE REVIEW

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.

TABLE 1 COMPARATIVE TABLE



Title and author	Method	Strength	Limitation
Fingerprint recognition using minutia score matching by Ravi J K.B.Raja. Venugopal K.R. 2009	Minutia score matching method	Fingerprint thinning is used.	----------
Fingerprint validation and outlier detection using minutiae approach in network security by Prathima Devi sirivella. Mrs. D. Raga vamsi 2004.	User verification based on the elliptical curve.	This approach gives better results in real time applications from database type of attacks.	Future improvement in the terms of efficiency and accuracy or improve the hardware to capture the image
Implementation of the security by using fingerprint recognition and GSM by Pennam Krishna murthy & Maddhusudhan red 2008.	1.Finger print recognition. 2.Remoteauthentication 3.Message alarming. 4.Gobor and direction filter algorithm.	GSM modem is connected s3c2440 chip is embedded with the technologies of fingerprint recognition	Gobor and direction filter algorithm is used but it slow in dealing with high capacity requirement.

III HARDWARE SYSTEM DESIGN

The ATMs are networked and connected to a centralized computer (Switch), which controls the ATMs. The use of biometric identification is possible at an ATM. The information can be stored at a bank branch or Network Provider. The typical ATM has two input devices (a card reader and keypad) and four output devices (display screen, cash dispenser, receipt printer, and speaker). Invisible to the client is a communications mechanism that links the ATM directly to an ATM host network. The ATM functions much like a PC, it comes with an operating system (usually OS/2) and application software for the user interface and communications. While most ATMs use magnetic strip cards and personal identification numbers (PINs) to identify account holders, other systems may use smart cards with fingerprint validation. The ATM forward information read from the client's card and the client's request to a host processor, which routes the request to the concerned financial institution. If the cardholder is requesting cash, the host processor signals from the customer's bank account to the host processor's account. Once the funds have been transferred, the ATM receives an approval code authorizing it to dispense cash. This communication, verification, and authorization can be delivered in several ways. Leased line, dial-up or wireless data links may be used to connect to a host system, depending on the cost and reliability of the infrastructure. The host systems can reside at a client's institution or be part of infrastructure. The host systems can reside at a client's institution or be part of an EFT network. The EFT network supports the fingerprint authentication..With the fingerprint reorganization method we also embedded the GSM technique. That the GSM modem connects to microcontroller. That will send the 4 digit code to the user(when the card insert by the main user or nominee the 4digit number only send to the main user only for the knowledge of the main user). After enter the 4digir number the transaction will begin. The user may do the transactions like fund transfer, cash withdrawal, mini statement, bill payment, balance enquiry. After all the transactions done the card will comes out from the machine. So the system is so safe and secure, and it avoid the security problems what we face in the previous works.

3.1 Block Diagram

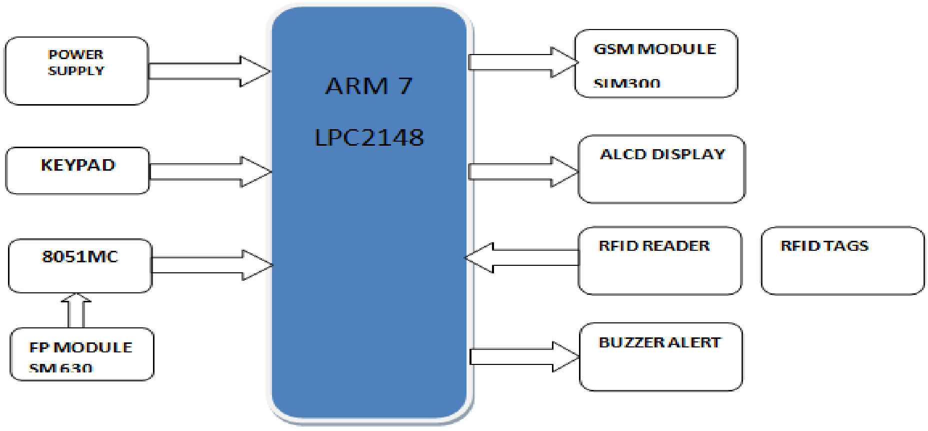


Fig 1: Overview of the System

To implement the proposed security for ATM terminals with the use of fingerprint recognition, we use the different hardware and software platforms. Fig .1 shows the major system modules and their interconnections. it consist of ARM7(LPC2148),finger frint module GSM module,RFID reader and tags ALCD display.

3.2. Functionality of the system

This system consists of 3 validation functions. First it validates the pin number second fingerprint. At last it validates the one time password which is send by GSM modem to the main user mobile number. The functionality of the system will explain by the below steps.

Step 1: swipe the card

Step 2: Enter card's password. Correct password means step-4 follows false means step-3 follows

Step 3: The card comes out from the machine and the message send to customer and makes buzzer ON.

Step 4: choose user type. Main user means step-5 follows. Nominee means Step-10 follows.

Step 5: Enroll the finger print. The user finger print already saved in the database. If authentication failure means next step follows. If success means step-7 follows.

Step 6: The card comes out from the machine and the message send to customer and makes buzzer ON.

Step 7: With the help of GSM four digit one time pass word is send to main user mobile number.

Step 8: We need to type the 4 digit one time password on ATM machine

Step 9: Then the transaction begins after completion of transaction the card will come out.

Step 10: If second type user means the nominee must enroll the finger print then step-7, step-8, step-9 follows.

3.3 Microcontroller (LPC2148)

The ARM7TDMI-S is a 32-bit microcontroller based on RISC architecture. It offers high performance for low power consumption. It uses 3 stage pipeline to increase the speed of the flow of instruction. The 3 stages are fetch, decode and execute. During normal operation, while one instruction is being executed, its successor is being decoded, and a third instruction is being fetched from memory. Program Counter (PC) points to the instruction being fetched rather than to the instruction being executed.The ARM7TDMI-S has Von-Neumann architecture, with a single 32-bit data bus carrying both instructions and data. Data can be 8, 16 and 32 bits length. It also supports for 16-bit THUMB architecture.

The system uses LPC2148 from ARM7 family. It is the core controller in the system. It has ARM7TDMI core which is a member of the Advanced RISC Machines (ARM) a family of general purpose 32-bit microprocessors. It offers high performance for very low power consumption and price. The ARM architecture is based on RISC (Reduced Instruction Set Computer) principles, and the instruction set and related decode mechanism are much simpler than those of micro-programmed Complex Instruction Set Computers (CISC) [5]. This simplicity results in a high instruction throughput and impressive real-time interrupt response from a small and cost-effective chip. All parts of the processing and memory systems can operate continuously since, pipelining is employed. Typically, while one instruction is being executed, its successor is being decoded, and a third instruction is being fetched from memory [6]. The ARM memory interface has been designed to allow the performance potential to be realized without incurring high costs in the memory system. Speed-critical control signals are pipelined to allow system control functions to be implemented in standard low-power logic, and these control signals facilitate the exploitation of the fast local access modes offered by industry standard dynamic RAMs [7].

The LPC2148 is interfaced to different modules via GPIO (General Purpose I/O) pins. It receives the fingerprint template produced by the fingerprint module. It will match the same with the reference template stored at installation of the system. If the received template gets matched with the reference one, the person is allowed to access the further system. In case of successive mismatch of templates, the system will initialize the GSM module to send message to the enrolled user and simultaneously will raise the alarm through buzzer.

We have used LPC2148 from NXP semiconductors (founded by Philips). It shows features as follows-

a) 16/32-bit ARM7TDMI-S microcontroller in a tiny LQFP64 package.

b) 240 kB of on-chip static RAM and 512 kB of on-chip flash program memory.

c) In-System/In-Application Programming (ISP/IAP) via on-chip boot-loader software.

d) Two 10-bit A/D converters provide a total of 14 analog inputs, with conversion times as low as 2.44 μs per channel.

e) Single 10-bit D/A converter provide variable analog output.

f) Multiple serial interfaces including two UARTs (16C550), two Fast I2C-bus (400 kbit/s), SPI and SSP with buffering and variable data length capabilities.

g) Vectored interrupt controller with configurable priorities and vector addresses.

h) Up to 45 of 5 V tolerant fast general purpose I/O pins in a tiny LQFP64 package .

3.4 Finger Print Module (SM630)

Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity.Fingerprint processing includes two parts: fingerprint enrollment and fingerprint matching (the matching can be 1:1 or 1:N). When enrolling, user needs to enter the finger two times. The system will process the two time finger images, generate a template of the finger based on processing results and store the template.The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns It is also necessary to know the structure and properties of human skin in order to successfully employ some of the imaging technologies[9].

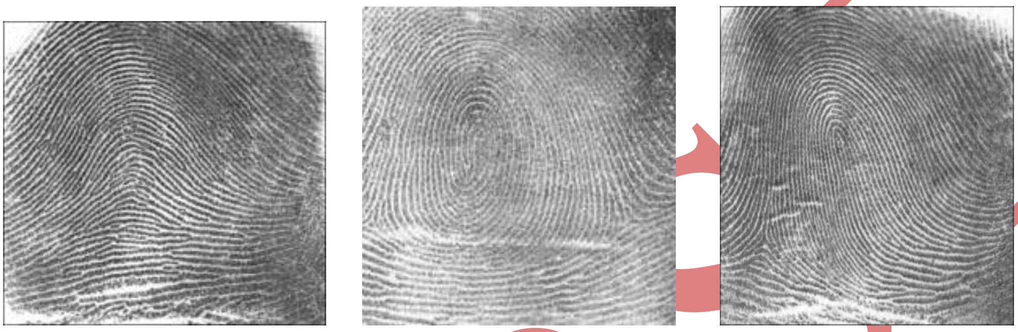
a) why fingerprint

1. There is very less chances of two people having same fingerprint.

2. Human fingerprint may change in scale but cannot change in appearance compared to other biometrics
3. It is easy to take fingerprint.

The three basic patterns of fingerprint ridges are the arch, loop, and whorl as shown in Fig:

- **arch:** The ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger.
- **loop:** The ridges enter from one side of a finger, form a curve, and then exit on that same side
- **whorl:** Ridges form circularly around a central point on the finger.



a) Arch pattern **b) whorl pattern** **c) Loop pattern**

Fig 2: shows the different pattern

SM630 has functions of fingerprint enrollment, identification, partial and entire deletion and reset in a single board, thereby offering convenient development environment. Here this SM630 supports the serial communication protocol which is RS-232 while LPC2148 works on TTL logic. Interfacing of SM630 to LPC2148 for bidirectional communication is made possible through IC called MAX-232 used as a level converter for reading and writing data. It uses overall supply voltage of 3.3 V.

3.5 GSM Modem (SIM 300)

A GSM modem is a wireless modem that works with a GSM wireless network. Global system for mobile communication (GSM) is a globally accepted standard for digital cellular communication.While accessing the system, we don’t replace the password verification. If password is correct, the system will capture and match fingerprint of the customer. As shown in Fig 4, if fingerprint does not match with the account registry , buzzer will be made ON and a message will be delivered to customer’s cellphone and bank authority . Thus, GSM MODEM to communicate with the mobile phone to which we are going to send the message is also interfaced with LPC2148.

The system uses SIM300 is a Tri-band GSM/GPRS engine that works on frequencies EGSM 900 MHz, DCS 1800 MHz and PCS 1900 MHz. SIM300 features GPRS multi-slot class 10/ class 8 (optional) and supports the GPRS coding schemes CS-1, CS-2, CS-3 and CS-4.

Semen’s GSM/GPRS Smart Modem is a multi-functional, ready to use, rugged unit that can be embedded or plugged into any application. The Smart Modem can be controlled and customized to various levels by using the standard AT commands.

3.6 One time password

A One Time password (OTP) is a password that is valid for only one login session or transaction. OTPs provides strong authentication for remote access such as high level IT resources, web service, mail server, online transaction.

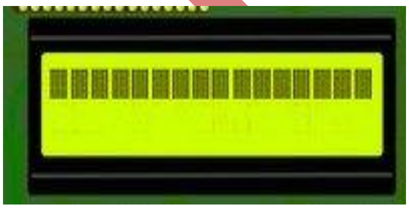
3.7 RFID reader & card

Radio-frequency identification (RFID) is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders. The technology requires some extent of cooperation of an RFID reader and an RFID tag.

An RFID tag is an object that can be applied to or incorporated into a product, animal, or person for the purpose of identification and tracking using radio waves. Some tags can be read from several meters away and beyond the line of sight of the reader The RFID reader and where this is used to receive the information from the RFID card and sends those information to processor unit.

3.8 User Interface

The user interface makes the communication between user and the system model easier. It includes a display unit and a function keyboard. For displaying the status of the process running in system and instructional steps for the user, we interfaced 16 x 2 LCD matrix with LPC2148 through GPIO pins of port 1. And also keypad is used to provide user's pin and OTP.



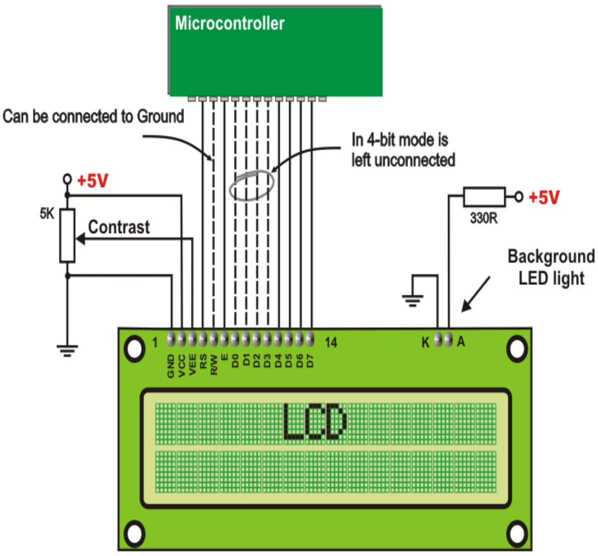


Fig 3:16x2 alpha numeric LCD

Fig 4: Interfacing of 16 x 2 LCD with microcontroller LPC2148.

3.9 Power supply

The microcontroller and other devices get power supply from AC to Dc adapter through voltage regulator. The adapter output voltage will be 12V DC non regulated. The 7805 voltage regulators are used to convert 12 V to 5VDC.

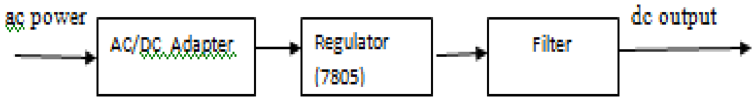


Fig 5 Block diagram of Power supply unit

Figure 5 shows how the input AC power is converted into output DC power. The adapter output voltage will be 12V DC non regulated. The 7805/7812 voltage regulators are used to convert 12 V to 5V/12V DC. . Further, LM317 is used to provide variable power e.g. 3.3V to LPC2148.

IV SOFTWARE DESIGN

The embedded platform discussed above is programmed in C language with KeilµVision3 to follow the program logic shown in Fig 6 as follows

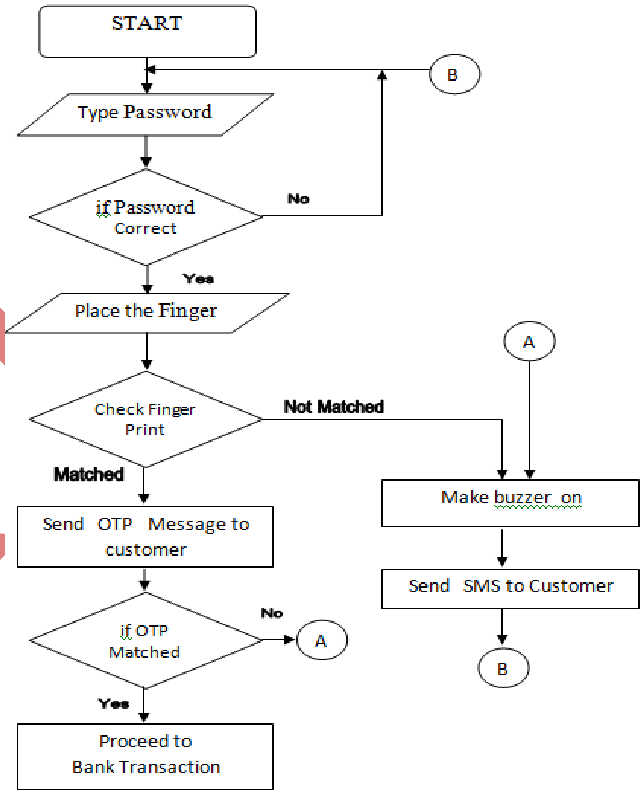


Fig 6: Realization of flow of tasks for the proposed system

4.1 Keil µVision 3

The LPC2148 is programmed with KeilµVision3. It is a window-based software platform that combines a robust and modern editor with a project manager and make facility tool for development. It integrates all the tools to develop embedded applications including a C/C++ compiler, macro assembler, linker/locator, and a HEX file generator. µVision helps expedite the development process of embedded applications by providing the IDE (Integrated Development Environment). KEIL is used to create source files; automatically compile, link and covert using options set with an easy to use user interface and finally simulate or perform debugging on the hardware with access to C variables and memory. Unless we have to use the tolls on the command line, the choice is clear. This IDE i.e. KEIL Greatly simplifies the process of creating and testing an embedded application. The user of KEIL centers on projects. A project is a list of all the source files required to build a single application, all the tool options which specify exactly how to build the application, and if required how the application should be simulated. A project is exactly the binary code required for the application. Because of the high degree of flexibility required from the tools, there are many options that can be set to configure the tools to operate in a specific and desired manner. It would be very tedious to have to set these options up every time the application is being built; therefore they are stored in a project file. Loading the project file into KEIL informs KEIL which source files are required, where they are, and how to configure the tools in the correct way. KEIL can then execute each tool with the correct options. Source files are added to the project and the tool options are set as required. The project can then be saved to preserve the settings. The project is reloaded and the simulator or debugger started, all the desired windows are opened. [8].

4.2 Simulator & Debugger

The simulator/ debugger in KEIL can perform a very detailed simulation of a micro controller along with external signals. It is possible to view the precise execution time of a single assembly instruction, or a single line of C code, all the way up to the entire application, simply by entering the crystal frequency. A window can be opened for each peripheral on the device, showing the state of the peripheral. This enables quick trouble shooting of mis-configured peripherals. Breakpoints may be set on either assembly instructions or lines of C code, and execution may be stepped through one instruction or C line at a time. The contents of all the memory areas may be viewed along with ability to find specific variables. In addition the registers may be viewed allowing a detailed view of what the microcontroller is doing at any point in time [8].

4.3 Embedded C Language

The KeilµVision4 platform put forward the options for assembly language and high level language programming. C language being the most convenient language to access different port pins of LPC2148, we programmed the algorithm to control the sm630 fingerprint module through host controller LPC2148 in C language. The program follows the control actions as shown in the flowchart.

4.4 Flash Programming Utility

For downloading the application program into Flash ROM, this utility tool is necessary. The program code generated in C language after processing produces object code in hex form. It is referred as .hex file. To dump this hex code in the flash ROM of the controller the facility is provided with Keil version 3.

V ADVANTAGES OF PROPOSED SYSTEM

[1]. The GSM technology is cellular network, which means that mobile phones connect to it by searching for cells in the in the immediate vicinity it will make the authentication fast.

[2]. The fingerprint recognition will make the system so secure.

[3]. The nominee user also used so instead of the main user the nominee will access the account in case of emergency.

[4]. The one time password send by GSM modem to the main user changes every time so it provide good security

VI RESULT

Fig 7shows the hardware setup for proposed system. It has been demonstrated successfully using SM630 (Fingerprint scanner) and LPC2148 (ARM7 -Microcontroller).

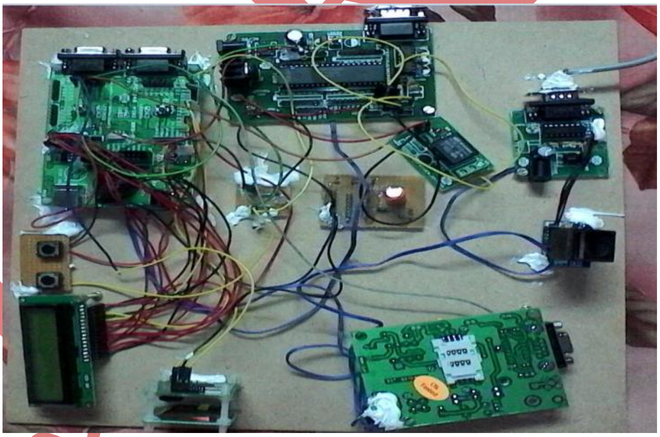
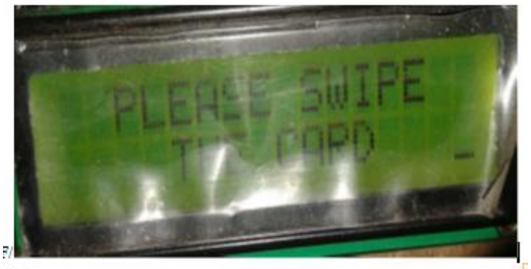


Fig 7: Hardware setup developed for the proposed System



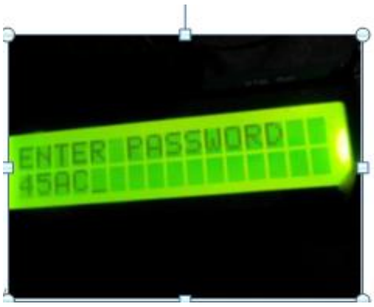
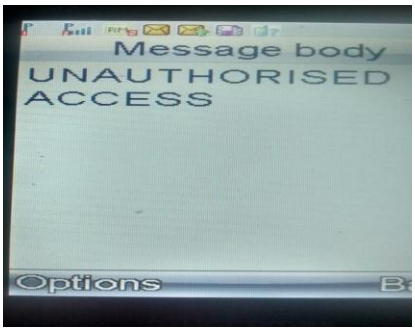


Fig 8 : Initial Step in Universal card **Fig 9: Entering password**

when the system is initialized, first step is to swipe a card shown in fig 8. This message is displayed in the LCD. After swiping Universal Card, next step is to enter the password to carry out the transaction as shown in fig 9 In proposed system, after swiping card the next step is to enter the password. Hear the first step of verification done whether the user is authorized user or non unauthorized user.

After typing the password the next step is place the finger as shown in fig 11 here the second verification process is done.if the finger print is valid it will send 4 digit OTP to the customer s mobile shown in fig 10.other wise it unauthorized access to the customer and also makes buzzer ON.


Message body
UNAUTHORISED
ACCESS

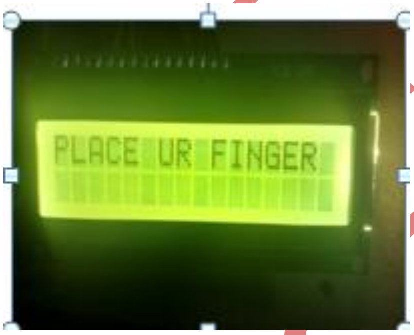

PLACE UR FINGER

Fig 10: Unauthorized access message **Fig 11: Place The Finger**

The next step enter the OTP received by the customer if the OTP is matched then transaction starts. Here the third verification is done shown in fig 12 & 13.

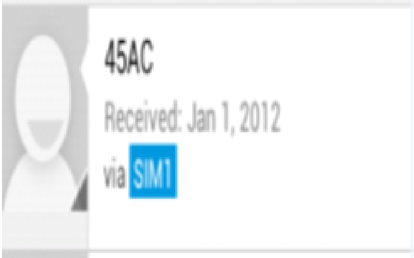
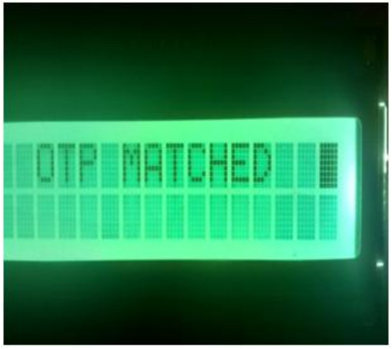

45AC
Received: Jan 1, 2012
via SIM1

Fig 12: A 4 digit password to customer mobile number


OTP MATCHED

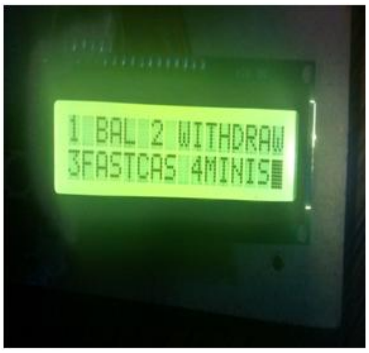

1 BAL 2 WITHDRAW
3FASTCAS 4MINIS

Fig 13 : OTP Message display **Fig 14 :Transaction Starts Display**

VII CONCLUSION

After testing the system developed, we came to know that ATM prototype can be efficiently used with fingerprint recognition. 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 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. The prototype of the developed application has been found promising on the account of its sensitivity to the recognition of the cardholders and nominees‟ finger print as contained in the database. This system when fully deployed will definitely reduce the rate of fraudulent activities on the ATM machines such that only the registered owner of a card and nominee, access to the bank account, and the nominee user also will do the transaction so it is more comfortable in case of emergency. LPC2148 and SM 630 provide low power consumption platform. Speed of execution can be enhanced with the use of more sophisticated microcontroller

VIII FUTURE DIRECTIONS

In this project we are using finger print module as mode of authentication.this has many advantages such as protects privacy from fraudsters and finger print do not change over time so we can stop un authorized access.In future biometrics will be preferred for security purpose against forgery. And also there are so many fingerprint recognition models are available practice with new fingerprint recognition method. And also Try this with two or more nominees. We can also Use the minutia approach for avoiding the database type attacks.

IX ACKNOWLEDGMENT

It gives me great pleasure to express my deep gratitude to my project guide Mr.G Ramakrishan Professor for his support and help me from time to time during this work.It is my pleasure to acknowledge deep sense of gratitude to my Friends and family.

REFERENCES

[1] Implementation ATM security by using fingerprint recognition and GSM by Pennam Krishna murthy & Maddhusudhan reddy

[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, pp.

[3] Designing a biometric strategy(fingerprint) measure for enhancing ATM security in Indian E-Banking system-2011 by Sri Shimal Das smt.Jhunnu Deddarma

[4] A method to improve the security level of ATM banking systems using AES algorit:hm, N.Selvaraj & G.Sekar, international journal of computer applications(0975-8887)volume 3- no.6.,june 2010.

[5] Steve Furber, ARM System-on-Chip Architecture, Second Edition, 2000, Addison Wesley, ISBN 0-201-67519-6

[6] Andrew Sloss, Dominic Symes, Chris Wright, ARM System Developer's Guide, 2004, Morgan Kaufmann, ISBN: 1-55860-874-5

[7] ARM7TDMI Data Sheet, Document Number: ARM DDI 0029E, Issued: August 1995, Advanced RISC Machines Ltd (ARM)

[8] MDK-ARM, KeilTM Tools By ARM, Keil0223-3 \ 01.11J.S.

[9] Fingerprint recognition using minutia score matching by Ravi J K.B.Raja, Venugopal K.R

[10] ARM7TDMI Data Sheet, Document Number: ARM DDI 0029E, Issued: August 1995, Advanced RISC Machines Ltd (ARM)