Biometric Automated Teller Machine with GSM Technology for OTP

[1]MOHAMMED MATEEN AHMED, [2]SHANILA MAHREEN
[1]PG Scholar, Dept of ES, Nawab Shah Alam Khan College of Engineering and Technology, Hyderabad, TS, India.
[2]Associate Professor, Dept of ES, Nawab Shah Alam Khan College of Engineering and Technology, Hyderabad, TS, India.

Abstract: Frauds attacking the automated teller machine has increased over the decade which has motivated us to use the biometrics for personal identification to procure high level of security and accuracy this paper describes a system that replaces the ATM cards and PINs by the physiological biometric fingerprint authentication. Moreover, the feature of one time password (OTP) imparts privacy to the users and emancipates him/her from recalling PINs. In this system during enrollment the genuine user's fingerprint samples of are retained in the database. The process of transaction begins by capturing and matching fingerprints patterns. The system will automatically distinguish between real legitimate trait and fake samples. A GSM module connected to the ARM7 LPC2148 will message a 3-digit code generated by the system to the registered mobile number. After the valid OTP is entered the user can either withdraw or deposit cash or check his/her balance. In any kind of fake access attempts the account is blocked.

Keywords: Authentication, Biometrics, Global System for Mobile Communication (GSM), Minutiae Based Algorithm, One Time Password (OTP).

I. INTRODUCTION

A 24 x7 self-banking service has made the ATM the heart of banking. The surplus use of ATMs, has not only lead to an increase in their number but has also increased fraudulent attacks on the ATMs. This calls for the biometric systems to be integrated in the traditional ATM. The author in Built an ATM based on fingerprint verification and incorporated the fingerprints of the users into the database of the respective banks to simulate it for ATM operations. Due to the lack of the fingerprint matching algorithm it proved to be inefficient. Proposed a system which performed authentication by including both the fingerprint and GSM technology into the traditional PIN based ATM system. In an algorithm was constructed based on Short Message Service (SMS) verification to enhance the ATM authentication system. Authors in secured the system using fingerprint, along with this the system used RFID reader module. Developed a RFID card as input to the microcontroller for identification and a GSM module to send messages. Authors in proposed a system which incorporated facial recognition in the traditional ATM for authentication of users. The later part of this paper is designed as follows: The system development is furnished in Section II .Proposed Biometric identification techniques are described in Section III. GSM technology for OTP generation is explained in Section IV. Experimental results are focused upon in Section V. In Section VI finally conclusion are drawn with the help output screen shots.

II. SYSTEM DEVELOPMENT

A. An Overview of the Proposed System

In the proposed system we present a fraud detection method using biometrics to detect various types of illegal access attempts during the ATM transaction. The objective of the proposed system is to enhance the security of the ATM transaction using biometric recognition frameworks. In this system ARM7 based LPC2148 controlling is used for smart ATM access. The fingerprint module utilizes the minutiae based algorithm for fingerprint recognition it captures the fingerprint of the person and compares it with the fingerprint of the genuine person stored during enrollment. If the person is a valid user the controller will display a message "VALID PERSON" on the LCD. This process is done through the GSM module which is interfaced to the ARM board. Depending on whether the OTP entered is correct or wrong messages like" CORRECT CODE "or "REENTER CODE" is displayed on the LCD. After the entered code is found valid the banking process begins and a message "BAL, DEP, WTD" for entering the option for the task to be performed is displayed on the LCD. After the task is performed finally a message "TRANSACTION COMPLETED" is displayed on the LCD.

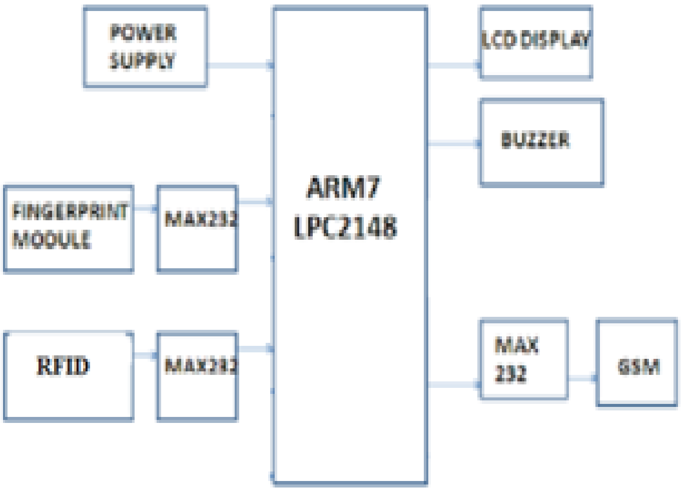


Fig 1: Block Diagram

1. ARM

A mind boggling guidance set PC, ordinarily known as CISC, is in finished complexity to the diminished guidance set PC, generally known as RISC. Both represent two totally unique methods of insight in present day PC design. Some microcontrollers underpins the RISC engineering some microcontrollers bolsters the CISC design. The case of the RISC design is 8085 microcontroller and ARM microcontrollers underpins the RISC engineering.

Features of ARM7TDMI-S

- 32/16-bit RISC engineering (ARM v4T)
- 32-bit ARM guidance set for most extreme execution and adaptability
- 16-bit Thumb guidance set for expanded code thickness
- Unified transport interface, 32-bit information transport conveys the two guidelines and information
- Three-organize pipeline
- 32-bit ALU
- Very little kick the bucket size and low power utilization
- Fully static task
- Coprocessor interface
- Extensive investigate offices:
  – Embedded ICE-RT constant investigate unit
  – JTAG interface unit

The ARM7TDMI Core

The ARM7TDMI center is the business' most generally utilized 32-bit installed RISC microchip. Streamlined for expense and power-delicate applications, theARM7TDMI arrangement gives the low power utilization, little size and superior required in versatile, implanted applications. Key highlights are:

- Hard large scale cell
- Portable down to 65nm
- Performance up to 133 MHz
- Thumb and ARM guidance sets
- Three-arrange pipeline
- Unified transport design
- Low power, completely static plan
- Small kick the bucket estimate
- Coprocessor interface
- Embedded ICE-RT investigate rationale
- Embedded Trace Microcell™ (ET) interface

2. Global System for Mobile communication

GSM (GLOPAL SYSTEM FOR MOBILE COMMUNICATION) is the most prominent standard for versatile communication frameworks on the planet. The GSM Association, its advancing industry exchange association of cell phone transporters and producers, gauges that 80% of the worldwide portable market utilizes the standard. GSM is utilized by over 1.5billion individuals, crosswise over in excess of 212 nations and regions. This pervasiveness implies that supporters can utilize their telephones all through the world, empowered by worldwide meandering game plans between versatile system administrators. GSM contrasts from its antecedent advancements in that both flagging and discourse channels are computerized, and in this way GSM is viewed as a second era (2G) cell phone framework. This likewise encourages the wide-spread usage of information correspondence applications into the framework. The GSM standard has been preference to the two buyers, who may profit by the capacity to meander and switch transporters without supplanting telephones, and furthermore to arrange administrators, who can pick gear from numerous GSM hardware sellers.

3. RFID

RFID (Radio Frequency Identification) innovation has been around for a long time. Before the year 2000, basic uses for RF-ID in the USA included toll way passes, get to ID cards and the little ID chips that are embedded in creatures for ID. The ongoing presentation of RFID in the store network just as a few commands has added to the mindfulness and estimation of this innovation. RFID labels work at a few unique frequencies. Most of RFID labels work at either 13 MHZ or 900 MHZ. Think about these two frequencies as the AM and FM groups on your radio. Everyone has its favorable circumstances. For instance, one works better when encompassed by metal while the other will work better over long separations.13 MHZ (HF) labels are commonly better at entering fluids and are normally utilized for access control, for example, in security cards and wristbands. The read range at this recurrence is around 3 feet or 1 meter. 900 MHZ (UHF) labels work better when perusing numerous labels at the same time, and in this manner is commonly the label sort of decision for stock purposes. To put data in the tag, an encoder must be utilized. A standout amongst the most well-known strategies for encoding is with a RFID Capable Label Printer that has a worked in encoder and RFID Capable Barcode Label Software.

4. Voltage Level Convetor

The MAX232 is a double driver/beneficiary that incorporates a capacitive voltage generator to supply EIA-232 voltage levels from a solitary 5-V supply. Every collector changes over EIA-232 contributions to 5-V TTL/CMOS levels. These recipients have a common limit of 1.3 V and a run of the mill hysteresis of 0.5 V, and can acknowledge ±30-V inputs. Every driver changes over TTL/CMOS input dimensions into EIA-232 dimensions. The driver, recipient, and voltage-generator capacities are accessible as cells in the Texas Instruments Lin ASIC library.

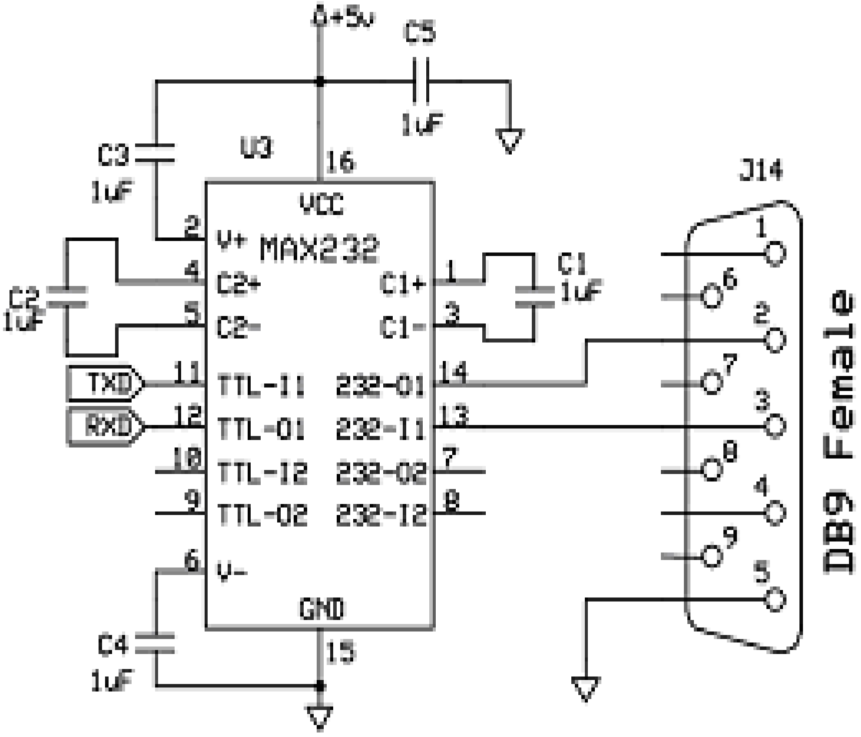


Fig 2: Schematic diagram of MAX-232.

5. Liquid Crystal Display (LCD)

LCD (Liquid Crystal Display) screen is an electronic display module and find a wide range of applications. A 16x2 LCD display is very basic module and is very commonly used in various devices and circuits. These modules are preferred over seven segments and other multi segment LEDs. The reasons being: LCDs are economical; easily programmable; have no limitation of displaying special & even custom characters (unlike in seven segments), animations and so on. A 16x2 LCD means it can display 16 characters per line and there are 2 such lines. In this LCD each character is displayed in 5x7 pixel matrix. This LCD has two registers, namely, Command and Data. The command register stores the command instructions given to the LCD. A command is an instruction given to LCD to do a predefined task like initializing it, clearing its screen, setting the cursor position, controlling display etc. The data register stores the data to be displayed on the LCD. The data is the ASCII value of the character to be displayed on the LCD.

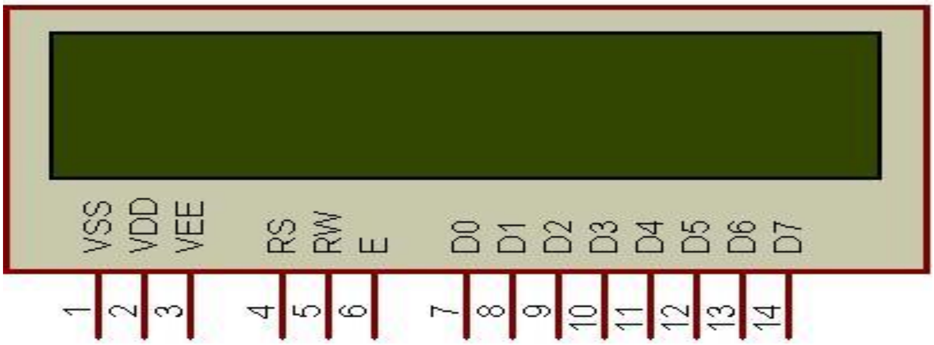


Fig 3: 16x2 LCD.

6. Finger Print Scanner

This is a finger print sensor module with TTL UART interface for direct connections to microcontroller UART or to PC through MAX232 / USB-Serial adapter. The user can store the finger print data in the module and can configure it in 1:1 or 1: N mode for identifying the person. The FP module can directly interface with 3v3 or 5v Microcontroller. A level converter (like MAX232) is required for interfacing with PC serial port. Optical biometric fingerprint reader with great features and can be embedded into a variety of end products, such as: access control, attendance, safety deposit box, car door locks

Features

- Integrated image collecting and algorithm chip together, All-in-one
- Fingerprint reader can conduct secondary development, can be embedded into a variety of end products
- Low power consumption, low cost, small size, excellent performance
- Professional optical technology, precise module manufacturing techniques
- Good image processing capabilities, can successfully capture image up to resolution 500 dpi

Specifications

- Fingerprint sensor type: Optical
- Sensor Life: 100 million times
- Static indicators: 15KVBacklight: bright green
- Interface: USB1.1/UART(TTL logical level)
- RS232 communication baud rate: 4800BPS~115200BPS changeable
- Dimension: 55*32*21.5mm
- Image Capture Surface 15—18(mm)
- Verification Speed: 0.3 sec
- Scanning Speed: 0.5 sec
- Character file size: 256 bytes
- Template size: 512 bytes
- Storage capacity: 250
- Security level: 5 (1,2,3,4,5(highest))
- False Acceptance Rate (FAR) :0.0001%
- False Rejection Rate (FRR): 0.1%
- Resolution 500 DPI
- Voltage :3.6-6.0 VDC
- Working current: Typical 90 mA, Peak 150mA
- Matching Method: 1: N
- Operating Environment Temperature: -20 to 45° centigrade

7. Buzzer

A buzzer or beeper is a signaling device, usually electronic, typically used in automobiles, house hold appliances such as a microwave oven, or game shows. It most commonly consists of a number of switches or sensors connected to a control unit that determines if and which button was pushed or a preset time has lapsed, and usually illuminates a light on the appropriate button or control panel, and sounds a warning in the form of a continuous or intermittent buzzing or beeping sound. Initially this device was based on an electromechanical system which was identical to an electric bell without the metal gong (which makes the ringing noise).

Often these units were anchored to a wall or ceiling and used the ceiling or wall as a sounding board. Another implementation with some AC-connected devices was to implement a circuit to make the AC current into a noise loud enough to drive a loudspeaker and hook this circuit up to a cheap 8-ohm speaker. Nowadays, it is more popular to use a ceramic-based piezoelectric sounder like a Sound alert which makes a high-pitched tone. Usually these were hooked up to "driver" circuits which varied the pitch of the sound or pulsed the sound on and off. In game shows it is also known as a "lockout system," because when one person signals (“buzzes in”), all others are locked out from signaling. Several game shows have large buzzer buttons which are identified as “plungers”.

Fig 4: Buzzer

III. OUTPUT SCREEN SHOTS

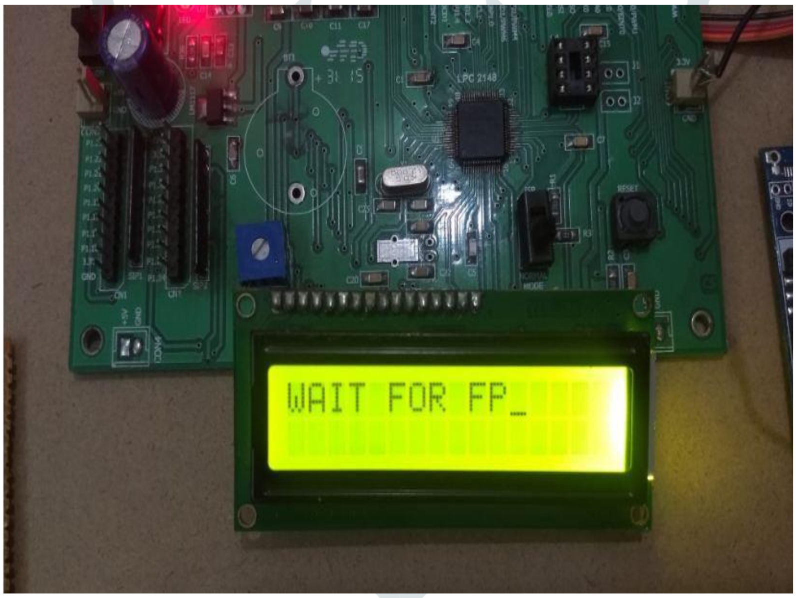
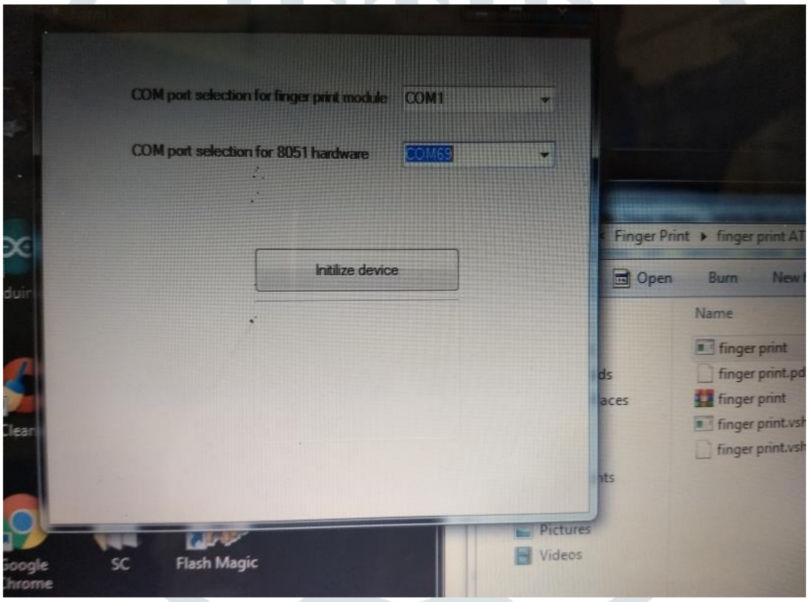


Fig 5: Finger Print Module

Fig 6: Output screen shot for Fingerprint Module



COM port selection for finger print module COM1

COM port selection for 8051 hardware COM69

Fig 7: Application Screen for Fingerprint in PC

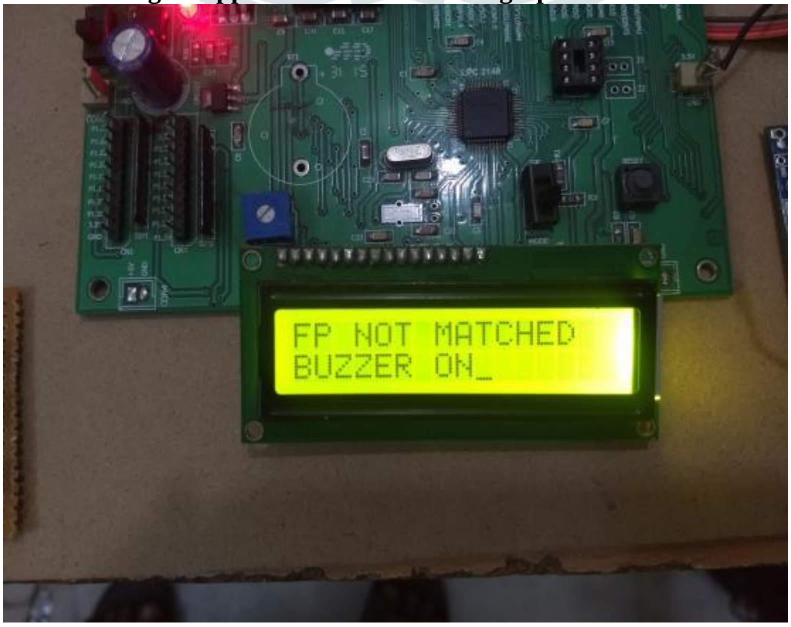


Fig 8: Output Screen shots of Not Matched Fingerprint.

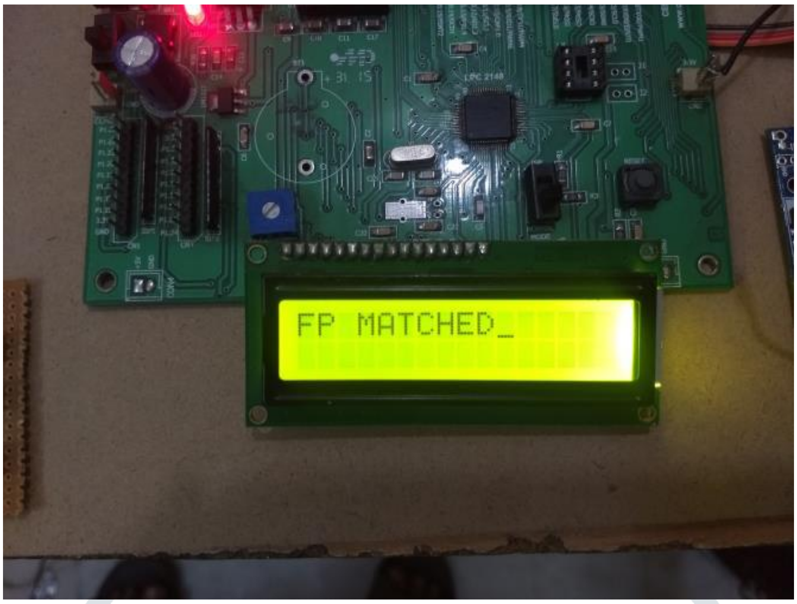


Fig 9: Output Screen shots of Match Fingerprint.

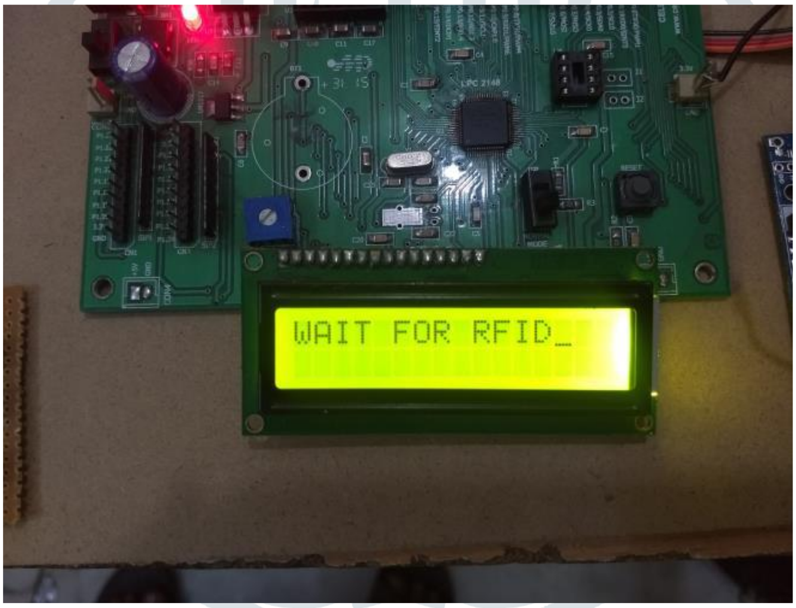


Fig 10: Output Screen shots for waiting for RFID.

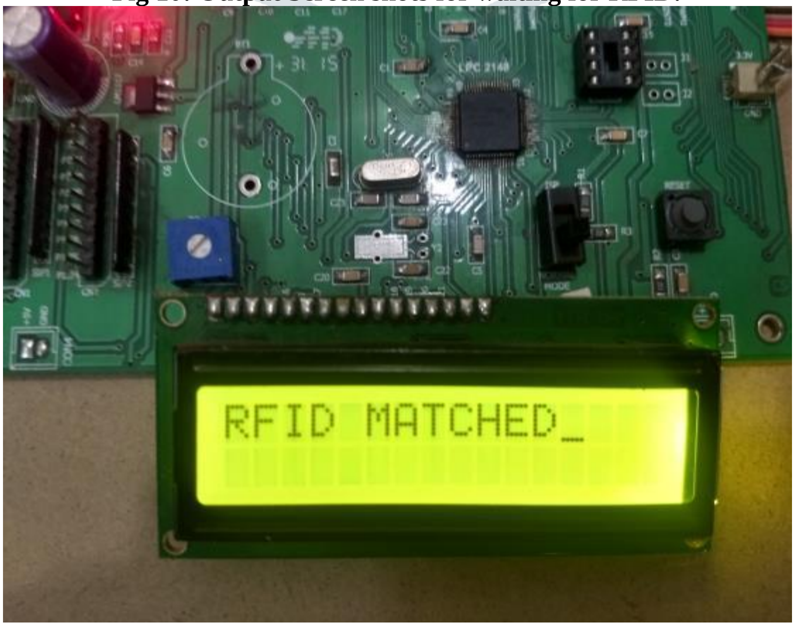
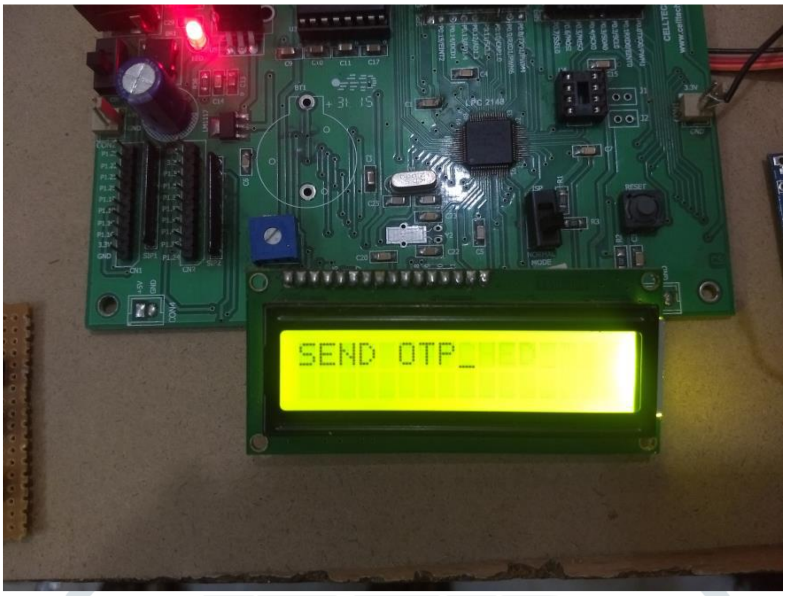
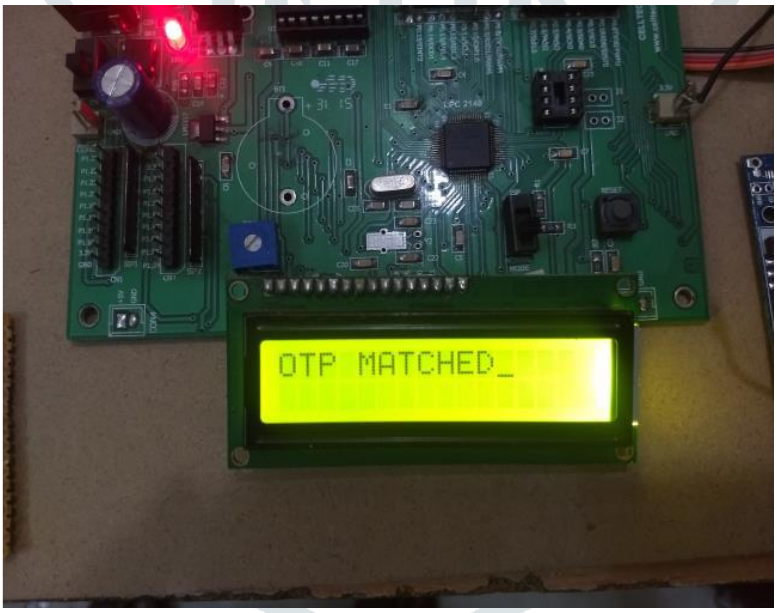


Fig 11: Output Screen shots for waiting for RFID card to swipe and checking the RFID Card.



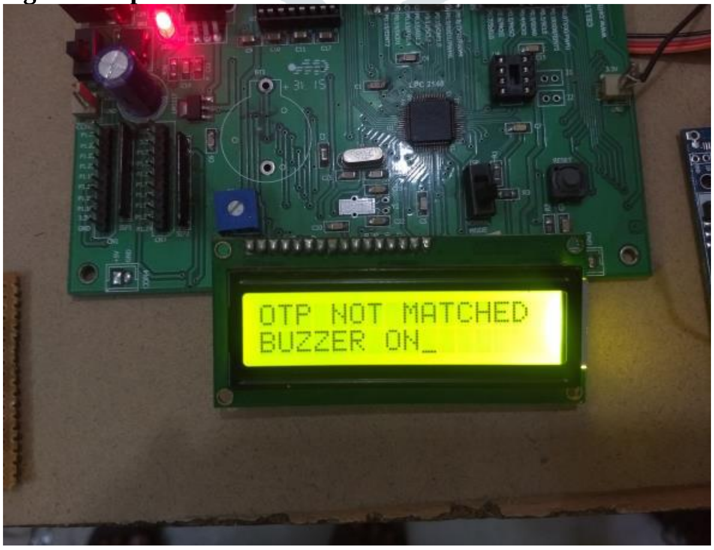
```
SEND OTP_
```

Fig12: Output screen for OTP authentication.



```
OTP MATCHED_
```

Fig 13: Output screen shots for Matched and Unmatched OTP.



```
OTP NOT MATCHED
BUZZER ON_
```

Fig 14: Output screen shots for Matched and Unmatched OTP.

IV. CONCLUSION

Here conclusion in this project we centers around how the transaction exchange in an ATM machine will be anchored by giving separate distinguishing proof by examining biometrics like finger prints designs which are known for their dauntlessness and assorted variety. Hence biometric are fixed to our system which will give authentication via RFID card and OTP will be generator and sent to GSM mobile to authentication the One time Password and it allows the access to person for process.

V. REFERENCES

[1] Anil K. Jain, Jianjiang Feng, Karthik Nandakuma, “Fingerprint Matching”, *IEEE* Computer Society2010, pp. 36-44,0018-9162/10.

[2] Khatmode Ranjit P, Kulkarni Ramchandra V,”ARM7 Based Smart ATM Acess and Security System Using Fingerprint Recognition and GSM Technology”, International Journal of Emerging Technology and Advanced Engineering ,Vol.4,Issue 2,Feb. 2014.

[3] G.Udaya Shree,M. Vinusha”Real Time SMS-Based Hashing Scheme for Securing Financial Transactions on ATM terminals”, International Journal of Scientific Engineering and Technology Research,Vol.2 Issue 12. Sep.2013.

[4] D.Shelkar Goud,Ishaq Md,P.J.Saritha,”A Secured Approach for Authentication system using fingerprint and iris”,Global journal of Advanced Engineering Technology,Vol,Issue3-2012.

[5]Mrs.S.P.Balwir, Ms.K.Katole, Mr.R.D.Thakare, Mr.N.S.Panchbudhe, Mr.P.K.Balwir,"Secured ATM transaction system using microcontroller”, International Journal of Advanced Research in computer science and software engineering “,Vol.4,Issue4,April2014.

[6] Kriti Sharma, Hinanshu Monga, “Efficient Biometric Iris Recognition Using Hough Transform with Secret Key”, International Journal of Advanced Research in Computer Science and Software Engineering. Vol.4,Issue 7, July 2014.

[7] Ritu Jindal, Gagandeep Kaur, “Biometric Identification System Based on Iris, palm and Fingerprint for Security Enhancements”, International Journal of Engineering Research and Technology,Vol.1, Issue 4, June 2012.

[8] Deepa Malviya, “Face Recognition Technique : Enhanced Safety Approach for ATM”, International Journal of Scientific and Research Publications, Volume 4, Issue 12, December 2014.

Author’s Profile:

Mr. Mohammed Mateen Ahmed has completed his B.Tech(ECE) from Shadan College of Engineering and Technology, Moinabad, RR District. JNTU Hyderabad. Presently, He is pursuing his Masters in Embedded System from Nawab Shah Alam Khan College Of Engineering and Technology, Hyderabad, JNTU Hyderabad, TS. India.

Ms. Shanila Mahreen has completed B.Tech (ECE) from Shadan Women College of Engineering and Technology, JNTUH University, Hyderabad and M.Tech (Embedded Systems) from Royal Institute Of Technology and Science JNTU University, Hyderabad. Currently she is working as an Associate Professor of ECE Department in Nawab Shah Alam Khan College Of Engineering and Technology, Hyderabad, TS. India.