Advanced Research in Electrical and Electronic Engineering
Print ISSN: 2349-5804; Online ISSN: 2349-5812 Volume 2, Number 6 April-June (2015) pp. 39-44
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/areee.html

A Highly Secured System based on RFID, Digital Password and Biometric

Athira Nayar

Department of Electronics and Communication,Amity School of Engineering & Technology,Amity University, Noida.
E-mail: athiranayar79@gmailcom

Abstract—*This paper describes the design of RFID, Password and Biometrics based security system. The system is combination of RFID, keypad and fingerprint. The purpose of this paper is to identify the authorized person by using RFID technology, digital password system and a finger print module, by comparing the details with the data available in EEPROM memory. This system can also notify unauthorized entry to the authorized person via the GSM module. In this project we have combined three modules to make a secure & reliable security system. It is very difficult to hack this system. It can be used in banks, offices & homes.*

Keywords*: Safe, secure and reliable RFID, password and biometrics based authentication.*

1. INTRODUCTION

Security has become a major issue in today's life [1]. Many technologies were developed for security purposes[1]. Some of them were too costly or not easy to implement[1]. Some of them were not fool proof. So we need as a security system which is fool proof, economical, user friendly, environment friendly, secure and reliable. This project fulfils these attributes.

The system consist of microcontroller Atmega32, RFID module (125hz), GSM module (SIM 300), Fingerprint module(R303), reset, motor driver IC L293d, a SIM card(Idea),12v DC power supply, keypad, LCD and CD driver and 2:1 switch as shown in Fig. 3. We have used here 2:1 switch because Atmega 32 has only one UART but we require UART for RFID, keypad and Fingerprint module. For this, we have connected RFID to receiver pin of microcontroller and GSM to transmitter pin of microcontroller .But we still need one more UART for fingerprint module. Hence we have used 2:1 switch in this proposed system. The proposed security system consists of the following three stages as shown in Fig. 1 -

Stage 1: RFID module consists of RFID tag and RFID reader. When the user punches his card (containing the tag), the 12 byte serial number of the tag is read by the RFID reader and sent to the microcontroller. The microcontroller then compares the data with the existing data stored in the EEPROM memory(internal memory of the microcontroller). If the data matches with the existing data in the memory, it means the person is authorized and the user entered in the second stage of the security system.

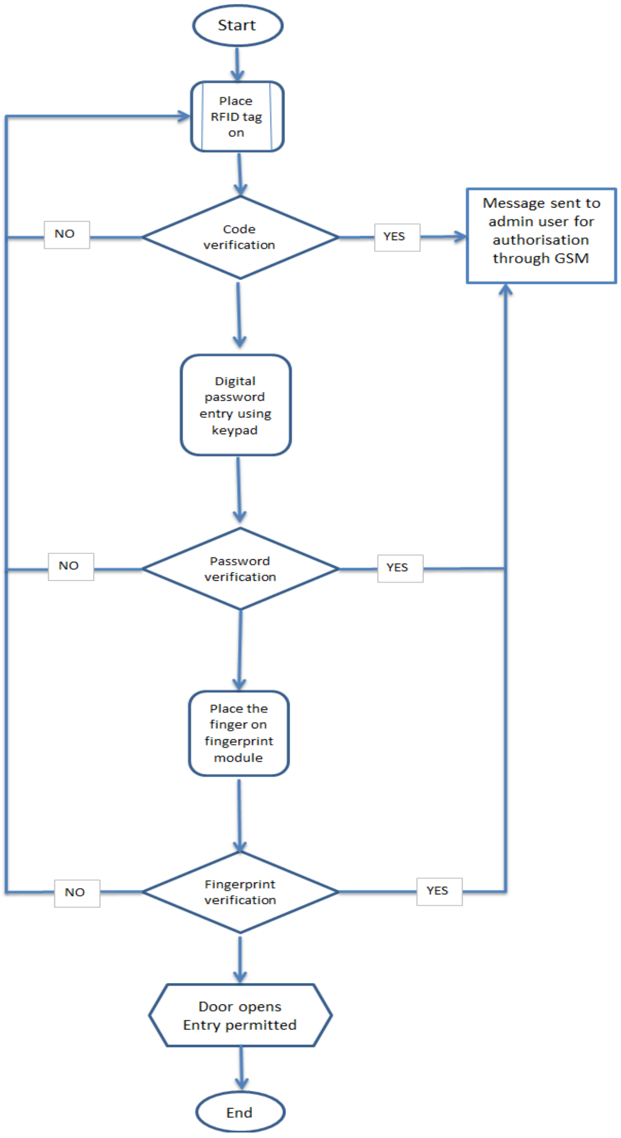

Start
Place RFID tag on
NO
Code verification
YES
Message sent to admin user for authorisation through GSM
Digital password entry using keypad
NO
Password verification
YES
Place the finger on fingerprint module
NO
Fingerprint verification
YES
Door opens Entry permitted
End

Fig. 1: Signal flow diagram

If the data is not matched then the user will not be permitted to enter the premises. The buzzer starts ringing to provide an alarm indicating the presence of an unauthorised person and a message is sent to the authorized person via GSM module.

Stage 2: The second stage includes the entering of password via the keypad by the user. But, if the password is wrong then access is denied and the authorized person is notified through the GSM module.

Stage 3: The user reaches the third stage if his RFID tag and password is correct. In the third stage he has to punch onto the fingerprint module. If the fingerprint of the person matches with the existing finger prints stored in the memory of the finger print module, then, the lock opens and the user gets access else it is denied.

The main contribution of paper is to make a highly secure and reliable security system .In this system, we have used the combination of RFID, password and fingerprint. Since RFID tag can be misplaced so RFID alone cannot secure the system. Password is hack able so digital keypad alone cannot be used in the system. By adding fingerprint verification, the system will become more secure. So by using RFID, digital keypad and fingerprint we have made better, secure and reliable security system. Unlike other security system , we can also add a new user with permission of authorised person . It is economical and user friendly.

This paper is organised as follows :-Section I describes the introduction part ,Section II describes the proposed method and methodology used with the help of flow diagram and the results are described in section III which is followed by conclusion.

2. PROPOSED METHOD

In this proposed work, RFID tag[3] is read by the RFID reader[3] and sent to the microcontroller as shown in Fig. 1. If the id is matched then it would proceed to next stage and send a message to authorized person otherwise it would stop the process and the buzzer would start ringing to provide an alarm indicating the presence of an unauthorised person and a message would be sent to the authorized person via GSM module[2]. In the next stage, the password is entered and sent to microcontroller. If the entered password is correct, it would proceed to next step and would send a message to authorized person otherwise access is denied and the authorized person is notified through the GSM module [2]. In the third stage, finger is punched into fingerprint module. If the fingerprint of the person matches with the existing finger prints stored in the memory of the finger print module [4], then, the lock opens and the user gets access else it is denied.

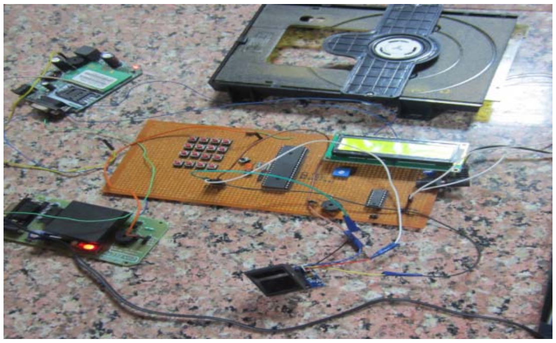


Fig. 2: Image of the proposed security system

3. WORKING

In this paper, an RFID system consists of a reader device and a transponder (tag). A transponder or tag has a unique serial number which is identified by the reader and is sent to ATmega32 for checking as shown in Fig. 3. If an unauthorized person tries to enter then a notification will be sent to the authorized person by the GSM module which is connected with the system. The user then has to enter his password via the keypad. The password is stored in EEPROM so that only registered user can reset it when desired. A keypad is used for inputting the password manually, which is a matrix of 4*4 elements. When one enters the code in the matrix keypad, microcontroller verifies the code. The code can be a combination of digits 0-9, four letters a,b,c,d and special characters * and #. If the user enters the wrong code, the buzzer connected will give an alarm and he will not be able to move on to the third stage.

The third stage is the finger print verification stage. This is done in two steps, the first step is finger print enrolment and the second is finger print matching. During enrolment, the user has to place his finger twice. The module will process the finger images and will create a template and store it in a memory slot. In the second stage of matching, 1:N matching is done in which the user enters the finger print onto the optical sensor, a template is generated and is compared with all the templates stored in the memory slots. After matching the result is displayed on the 16*2 LCD screen as success or error. If the result is success, the person gets entry.

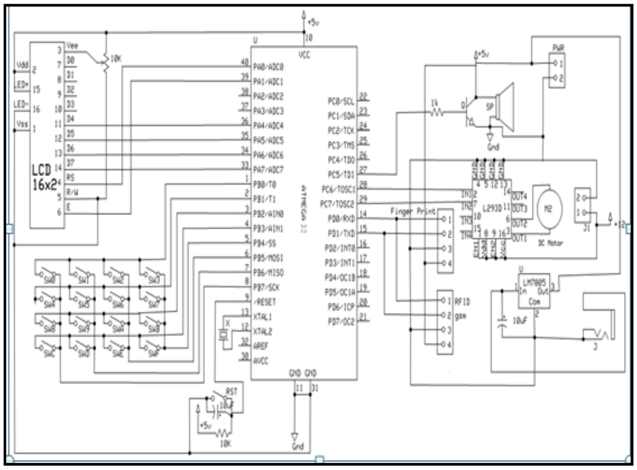


Fig. 3: Circuit diagram of security system

GSM module can be used as a receiver, which sends messages to the authorized person to notify him that an entry is being made. For this a desired mobile number is used in the system. In this, without verification it doesn't allow the door to be opened and a notification is sent to the authorized person.

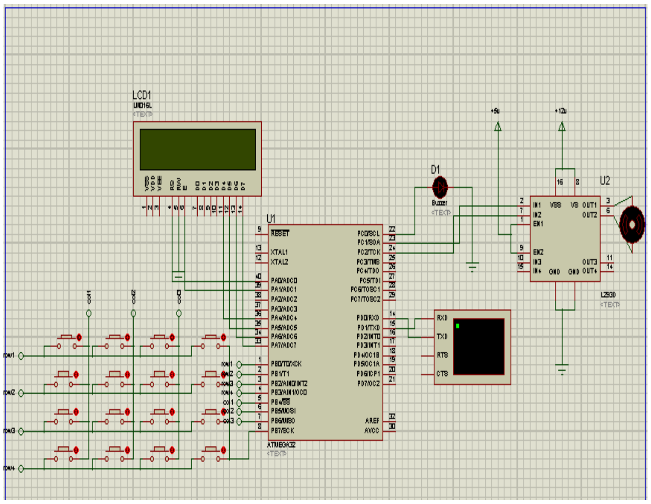


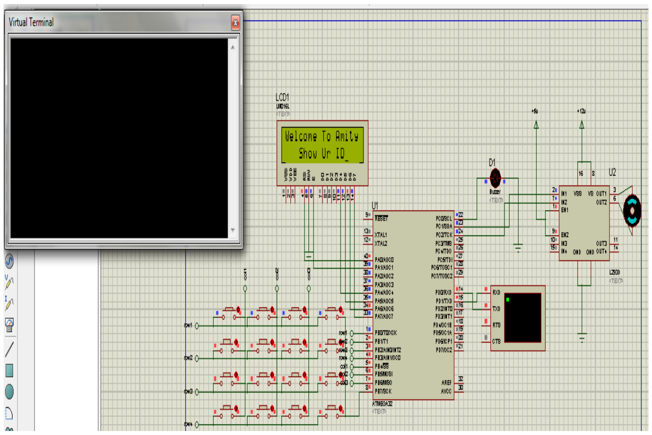
Fig. 4: Schematic diagram in Proteus.

4. RESULT

4.1 Proteus Simulation Of The Program

STEP 1:

In this step, we have loaded the hex file of the program in microcontroller ATMEGA 32 and executed the program. When we execute the program, LCD displays "Welcome To Amity. Show Ur ID" and virtual terminal appears on the screen as shown in FIG 5.

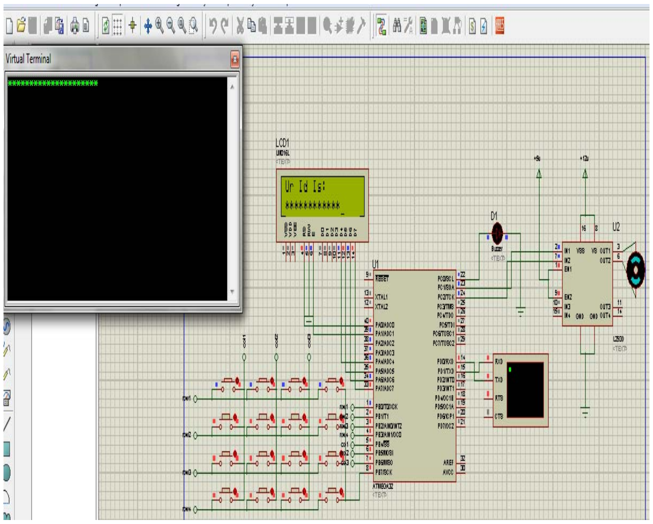


```
Welcome To Amity
Show Ur ID_
```

Fig. 5: First step of stimulation

STEP 2:

In this step, we have to type our RFID ID in virtual terminal. After typing the ID, LCD will display "Ur Id Is: ***********" as shown in FIG 6. The microcontroller verifies the ID and proceeds to the next step.



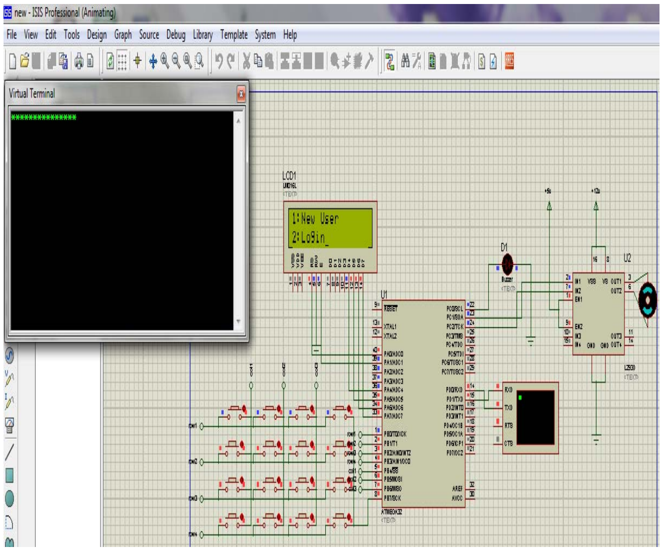
```
********************
```

```
Ur Id Is:
**********_
```

Fig. 6: LCD displays the RFID ID

STEP 3:

After verifying the ID, LCD displays " 1: New User, 2: Login". In this we will be given two choice ,one is to login as new user and other is to login as existing user as shown in FIG 7.



```
***************
```

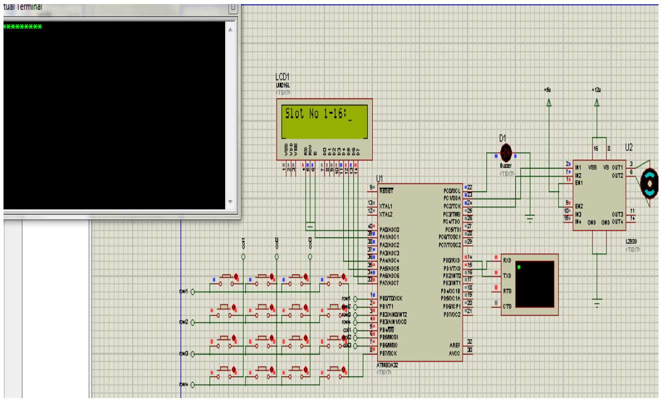
```
1:New User
2:Login_
```

Fig. 7: LCD displays the two choices either to login as new user or to login as already registered user

IF WE HAVE LOGIN AS NEW USER("1") THEN

STEP 3.1:

After selecting "1" keypad , LCD display "Slot No 1-16" as shown in FIG 8. In this we have to enter a slot number(1-16) in order to store our information in the respective slot.



```
*********
```

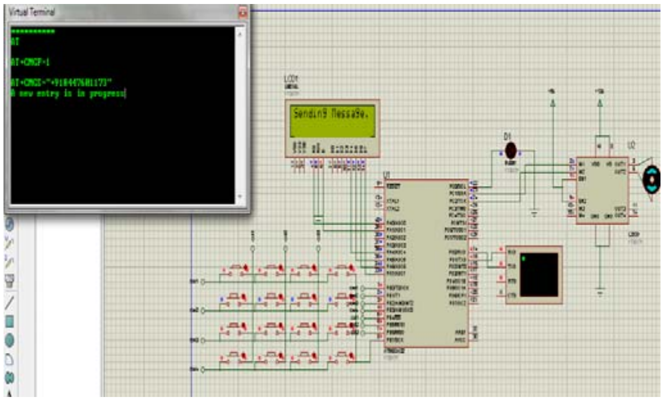
Slot No 1-16:_

Fig. 8: LCD displays slot number

STEP3.2:

After selecting the slot, LCD displays “sending message” as shown FIG 9. The virtual terminal displays AT COMANDS for sending the message “a new entry is in progress” to admin’s cell number.

After sending the message, LCD displays “ Enter Passkey” . in this one has to enter the password by using keypad . The microcontroller stores the password and proceeds to next step.

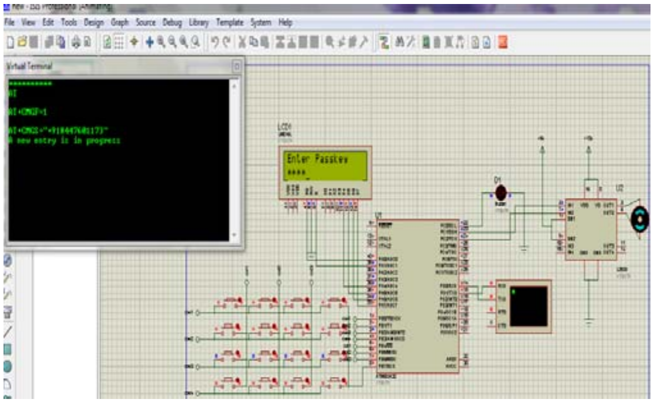


```
**********
AT
AT+CMGF=1
AT+CMGS="+918447681173"
A new entry is in progress
```

Sending Message.

Fig. 9: Message is sent via GSM Module

STEP 3.4:



```
**********
AT
AT+CMGF=1
AT+CMGS="+918447681173"
A new entry is in progress
```

Enter Passkey
****

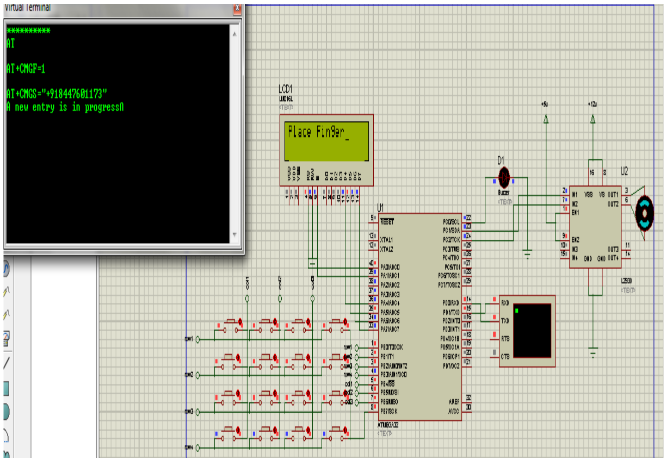
File View Edit Tools Design Graph Source Debug Library Template System Help
Virtual Terminal
LCD1
D1
U2

Fig. 10: Password is entered

After sending the message, LCD displays “ Enter Passkey” as shown in FIG 14. In this one has to enter the password by using keypad . The microcontroller verifies the password and proceeds to next step.

STEP 3.5:

After storing of password, the microcontroller proceeds to next step ie to store the fingerprint. In this step, LCD displays “Place Finger” as shown in FIG 11. We have to place finger on the finger print module so that the module can store the image of our fingerprint.



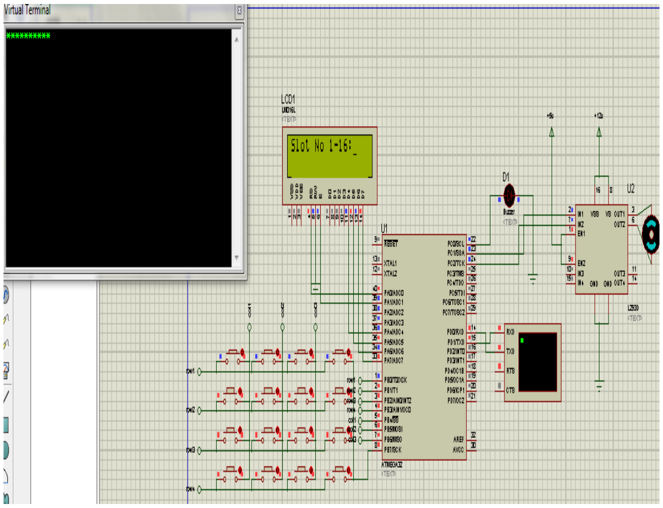
```
**********
AT

AT+CMGF=1

AT+CMGS="+918447601173"
A new entry is in progress
```

Place Finger_

Fig. 11: Finger is placed on the fingerprint module

IF WE HAVE LOGIN AS EXISTING USER THEN

STEP 3.1:



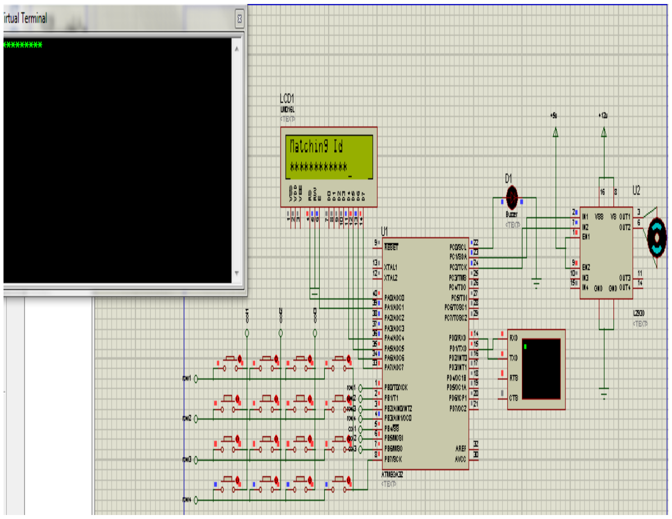
```
*********
```

Slot No 1-16:_

Fig. 12: Slot number is entered

After selecting “2” in the keypad , LCD displays “Slot No 1-16” as shown in FIG 12. In this we have to enter a slot number(1-16) from which microcontroller could verify our inputs.

STEP 3.2:

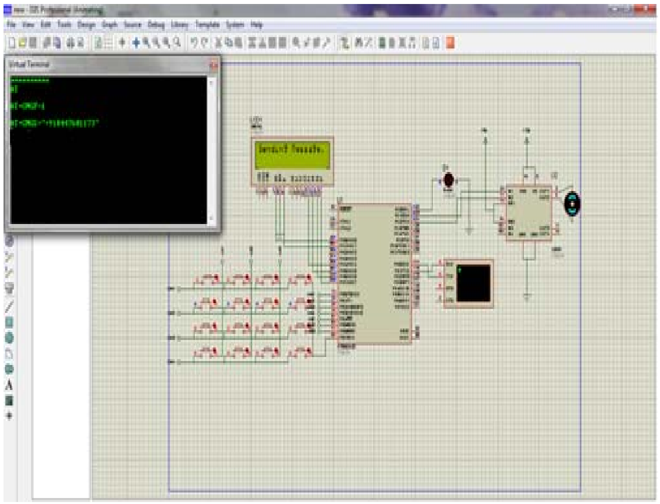


```
*********
```

Fig. 13: RFID ID is matched

In this step , the LCD displays the matching id. The microcontroller matches the input id with stored one.

STEP 3.3:


Virtual Terminal
File View Edit Tools Design Graph Source Debug Library Template System Help
LCD1

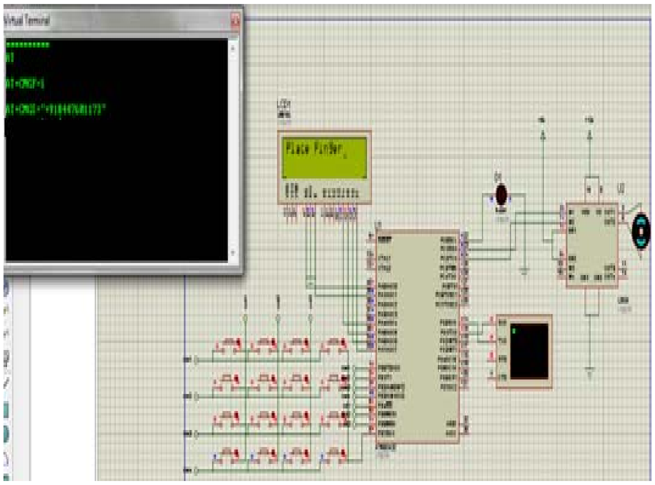
```
**********
AT
AT+CMGF=1
AT+CMGS="+918447681173"
```

Fig. 14: Password is entered

After sending the message, LCD displays “ Enter Passkey” as shown in FIG 14. In this one has to enter the password by using keypad . The microcontroller verifies the password and proceeds to next step.

STEP 3.4:

After verification of password, the microcontroller proceeds to next step i.e. to store the fingerprint. In this step, LCD displays “Place Finger” as shown in FIG 15. We have to place finger on the finger print module so that the module can verify the input fingerprint with the stored one.



```
**********
AT
AT+CMGF=1
AT+CMGS="+918447681173"
```

Fig. 15: Finger is placed on fingerprint module

5. CONCLUSION

The combination of RFID, keypad and fingerprint provides more reliable and secure security system. The advantages of this project are that it is cost effective, eco-friendly, user friendly and environment friendly. It is energy efficient and saves energy and time. We have used here 2:1 switch because Atmega 32 has only one UART but we require UART for RFID, keypad and Fingerprint module. For this, we have connected RFID to receiver pin of microcontroller and GSM to transmitter pin of microcontroller. But we still need one more UART for fingerprint module. Hence we have used 2:1 switch in this proposed system. In this system, we have used the combination of RFID, password and fingerprint. Since RFID tag can be misplaced so RFID alone cannot secure the system. Password is hack-able so digital keypad alone cannot be used in the system. By adding fingerprint verification, the system will become more secure. So by using RFID, digital keypad and fingerprint we have made better, secure and reliable security system. Unlike other security system, we can also add a new user with permission of authorised person.

6. ACKNOWLEDGEMENTS

I take this opportunity to express my sincere thanks and deep gratitude to all those people who extended their whole hearted co-operation and have helped us in completing this project successfully.

I would like to place on record our sincere thanks to our HOD Proff Dr M.K.Dutta, and faculty guide Proff Ashutosh Gupta for helping & advising me for my research paper.

REFERENCES

[1] DESIGN AND` DEVELOPMENT OF RFID BASED INTELLIGENT SECURITY SYSTEM Sukhraj Singh, Neeraj Kumar, Navjot Kaur, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)Volume 3 Issue 1, January 2014.ISSN: 2278 – 1323

[2] Ma Yuchun; Huang Yinghong; Zhang Kun; Li Zhuang, "General Application Research on GSM Module," Internet Computing & Information Services (ICICIS), 2011 International Conference on , vol., no., pp.525,528, 17-18 Sept. 2011

[3] Fazrul, F.Z.; Anuar, M.S.; Soh, P.J.; Aljunid, S.A., "125 KHz ubiquitous RFID tag signal detector system," Intelligent and Advanced Systems, 2007. ICIAS 2007. International Conference on , vol., no., pp.418,421, 25-28 Nov. 2007.

[4] Feng Lei; Zhang Xin; Liang Chunhui; Li Tianyu, "Research of fingerprint module detector system," Computer Application and System Modeling (ICCASM), 2010 International Conference on , vol.7, no., pp.V7-497,V7-500, 22-24 Oct. 2010.