Password Operated Device Control

EMBEDDED C PROGRAMMING PROJECT REPORT

Team number – 05

Afreen S (21BEC1017)

Aniket Chattopadhyay (21BEC1564)

Madirakshini Ramani (21BEC1627)

Sadhana (21BLC1422)

Submitted to Prof. Gowri Prasood U

WINTER SEMESTER 2023 – 2024 | VELLORE INSTITUTE OF TECHNOLOGY, CHENNAI

ABSTRACT

This report examines the functions and features of electronic locks, also known as digital locks, which integrate advanced electronic entry controls Users use a keypad and the device connects, and access is gained using password input. Successful input triggers a mechanism represented here as the electric bulb's operation or operation, depending on its current state. Conversely, an incorrect password triggers an exciting red alert with an audible buzzer confirmation.

The main components of this system are a keypad, LCD display for feedback, and a controller, specifically the AT89C51, part of the iconic 8051 microcontroller series other components include a relay driver, buzzer, red LED and electric bulb, all enclosed necessary for the functioning of the rhythm. Using a 4x3 matrix keypad and a 16x2 LCD, the system uses widely accepted input and output devices, respectively, to ensure a smooth user interface will remain secure by the need for a four-square password securely stored in system memory.

Through this comprehensive analysis, the report sheds light on the complexity and functionality of electronic launchers, and highlights the importance of modern access control systems plant. This report examines the functions and features of electronic locks, also known as digital locks, which integrate advanced electronic entry controls Users use a keypad and the device connects, and access is gained using a password entry system. Successful input triggers a mechanism represented here as the electric bulb's operation or operation, depending on its current state. Conversely, an incorrect password triggers an exciting red alert with an audible buzzer confirmation.

The main components of this system are a keypad, LCD display for feedback, and a controller, specifically the AT89C51, part of the iconic 8051 microcontroller series other components include a relay driver, buzzer, red LED and electric bulb, all enclosed necessary for the functioning of the rhythm.

Using a 4x3 matrix keypad and a 16x2 LCD, the system uses widely accepted input and output devices, respectively, to ensure a smooth user interface will remain secure by the need for a four-square password securely stored in system memory. Through this comprehensive analysis, the report sheds light on the complexity and functionality of electronic launchers, and highlights the importance of modern access control systems plant.

INDEX

Introduction:

At a time when security is paramount and technological advances continue to shape our daily lives, access control systems are at the forefront of innovation. Among these systems, electronic doors, also known as digital doors, have emerged as key solutions to enhance safety and security in various situations by combining electrical components with sophisticated mechanical devices, electronic gates give users superior control over access to secure areas.

This report takes a deeper look at the complexity of electronic locks, examining how they work, features and relevance in today's society. From basic operating principles to applications in various industries, this review aims to provide a comprehensive understanding of electronic launch and its importance in modern anticipatory systems in access to it.

By analyzing key components such as keypad, LCD display, microcontroller, various input/output devices, this report sheds light on the electronic gate industry and also, highlights the important role of electronic devices in safety systems promoting, improving accessibility and facilitating innovation in the field related to accessibility monitoring technologies.

Furthermore, the report analyzes the motivation behind the development of electronic locks which stems from the urgent need for robust security solutions in today's dynamic and interconnected world Also highlights the importance of electronic locks meet today's security challenges and emphasize changing the evolving technological landscape. By shedding light on the capabilities, advancements and potential applications of electronic locksmiths, this report aims to provide valuable insights to researchers and manufacturers.

Platform/Technology:

Keil µvision5 and Proteus 8 Professional

Literature Survey/ Background:

In today's digital age, safety and security have become a major concern among businesses, leading to the growing adoption of electronic locksmiths. These sophisticated locking mechanisms offer advanced features such as password protection, IoT ecosystem integration, and easy accessibility, making them indispensable assets in the protection of valuable assets and the maintenance of access roads to secure areas This literature review examines the multi-dimensional use of electronic locks Focused There is The objective of this review is to provide detailed insights into the development, integration and updating of electronic locks in the context of password-based access control by examining the following key elements

1. Enhanced Security: Compared to traditional mechanical locks, electronic locks offer a higher level of security. With features such as password protection and alarm systems, they offer advanced security systems to protect homes, offices and other valuable assets. In an age where safety is a major concern, it is important to develop and understand electronic locks.

2. Convenience and accessibility: Electronic gateways provide user convenience and accessibility. With the ability to type passwords instead of carrying keys, users can enjoy logging in and out of secure environments hassle-free. This convenience feature is especially important in environments that require high volumes of people, such as offices, hotels, and common areas.

3. Integration of IoT and smart home technologies: Electronic gateways can be installed in smart homes or larger Internet of Things (IoT) ecosystems. This integration allows users to remotely monitor and manage access to their property.

4. Innovation and Advancements: With advancements in technology, electronic locks continue to evolve. From biometric authentication to voice recognition, there is a steady stream of innovation aimed

at improving security and user experience. Analyzing electronic portals allows us to analyze these developments and encourage innovation in the industry.

5. Application in various industries: Electronic banqueting systems are used in a wider range of industries than traditional residential and commercial settings. Emphasizing versatility and high relevance, it is used in healthcare facilities, educational institutions, government buildings and more. Electronic live gateways open up opportunities for versatility.

Problem Definition:

The available work revolves around the creation, implementation and testing of electronic locking systems with the goal of providing improved access in systems, also known as digital gate Goals in particular is the safety and ease of use for controlling access to specific areas or assets and should so design the equipment.

Important aspects of the problem include:

1. Access Control Mechanism: The system should provide a secure access control mechanism, which allows access to authorized persons when unauthorized access is blocked approach.

2. User Interaction: An electronic lock is operated via a keypad, which requires a specified password to be entered to gain access. The system should facilitate seamless and intuitive interactions for users.

3. Response Mechanism: The system should respond appropriately after entering a password. Correct inputs should activate or disable embedded devices (such as electric bulbs), while incorrect inputs should trigger visual and audible warnings to sound the user report a failed attempt.

4. Component Integration: The system includes many components, including keypad, LCD display, microcontroller (AT89C51), relay driver, buzzer, red LED, electric bulb Smooth integration of these components is essential for efficient operation of electronic lock system.

5. Input and output devices: The system uses a 4x3 matrix keypad for user input and a 16x2 LCD display to provide feedback. The use of communication is essential to ensure that these input and output devices are compatible and function properly.

6. Password Security: Users must enter a four-digit password to login. It is also important to implement strong security measures to properly store and validate the password.

Flowchart/Architecture:

1. Interface LCD and keypad with AT89C51 in Proteus and Keil (C):

- In Proteus, the connection between the AT89C51 microcontroller, the LCD display, and the keypad is simulated. This involves establishing the necessary connections between the microcontroller pins and the input/output pins of the LCD and keypad.
- In Keil, C code is written to initialize and interact with the LCD and keypad. This includes configuring the microcontroller's ports and pins to send and receive data from the LCD and keypad.

2. Enter the password and check whether it's correct or wrong:

- In the first attempt the user enters a password.

- Since the password entered earlier was wrong, the LCD displays that it was the wrong password and the user has two more attempts out of three remaining.
- Since the user entered the correct password in the second attempt the lcd displays "Correct Password " and the electric bulb will glow.
- When all the three attempts are over, the LCD just displays "Wrong Password " with no more attempts remaining for the user to enter the password, and the buzzer also turns on along with the LED.

3. Create a .hex File for the Built Corresponding Embedded C Code in Keil:

In Keil, once the C code is compiled, a .hex file is generated. This file contains the machine code that will be flashed onto the microcontroller to execute the desired functionality.

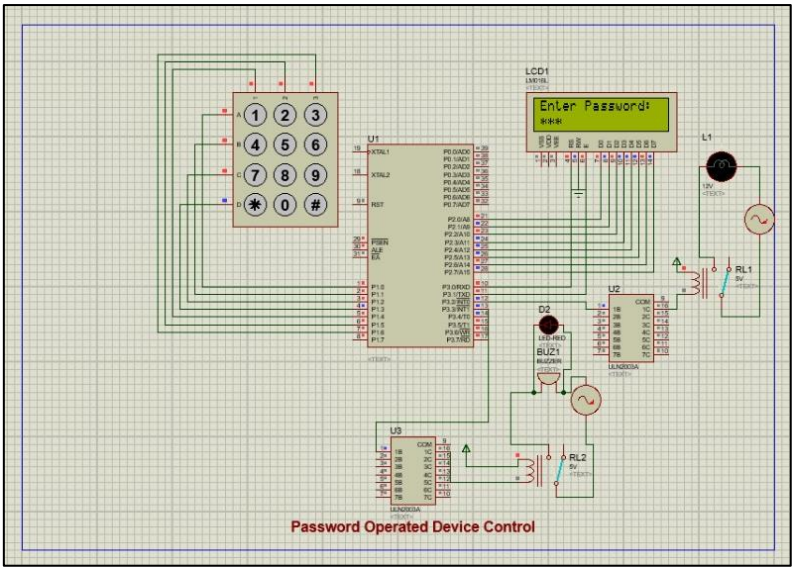
4. Add the .hex File in the AT89C51 of the Proteus Connection:

In Proteus, load the .hex file onto the AT89C51 microcontroller. This simulates programming the microcontroller with the compiled code.

5. Run the Simulation by Entering the Password:

With all connections established and the .hex file loaded onto the microcontroller; run the simulation in Proteus. Enter the password through the keypad to observe the system's response, including activating the device for correct passwords and triggering the LED and buzzer for incorrect passwords.

Schematic Diagram:



Module-wise explanation:

- In the above Proteus schematic diagram, the keypad is connected to the AT89C51 microcontroller via its port 1. The keypad interface is actually used to give the password as the input to the system.
- The LCD display is connected to port 2 of the AT89C51 microcontroller via its D0 to D7 pins (datapins) and the read-write enable pins are connected to the port 3's respective pins. This LCD display will display the status of entered password whether it's correct or wrong.
- The interrupt 0 and 1 is given via high voltage, high current Darlington transistor arrays to execute the LEDs and buzzer operation which are connected to it via 5-volt relays and functions accordingly.

Code:

The following code is implemented in Keil µvision5 platform and its .hex file is connected to the proteus schematic design as shown and discussed in the previous module wise explanation.

```
#include <REGX51.H>
#include "string.H"  //for strcmp: to check whether entered pwd matches the stored pwd

#define keypad  P1
#define LCD_dat P2

sbit rs =P3^0; //control pins
sbit en =P3^1;
sbit device = P3^2; //green LED for correct password
sbit red_led = P3^3; //red LED for wrong password
sbit buzzer = P3^3; //buzzer for wrong password

void dely(unsigned int dly);
void lcd_cmd(unsigned char ch);
void lcd_data(unsigned char ch);
void lcd_str(unsigned char *str);
char get_keypad_key(void);

void main(void)
{
   char KeyVal =0; //value entered by the user is updated here
   unsigned int KeyCnt =0; //user entered pwd must be counted
   unsigned int CmpPassword =0; //the string comparison value is copied, if both pwd are same, value
is 0
   char DefaultPassword[5]="6666"; //when correct pwd is set, the bulb glows, on second entry the bulb
goes off
   char EnteredPassword[5];
   device = 0; //device initial status
   red_led = 0; //red LED initial status
   buzzer = 0; //buzzer initial status
   lcd_cmd(0x38);
   lcd_cmd(0x0C);//lcd interfacing
   lcd_cmd(0x06);
   lcd_cmd(0x01);

   unsigned int attempts = 3; // Number of attempts allowed

   while(1)
   {    //main logic
      lcd_cmd(0x80); //lcd command for distance upto first row
      lcd_str("Enter Password: ");

      KeyVal = get_keypad_key(); //reading the input keypad value

      if(KeyVal != 0) //checks each value of entered pwd and stores in it and checks the condn
      {
         EnteredPassword[KeyCnt] = KeyVal;    //first entered pwd value to the array is updated
         lcd_cmd(0xc0+KeyCnt); //when user enters first key
         lcd_data('*');    //second row should display star - to hide pwd
         KeyCnt =  KeyCnt + 1; //to get next value
      }
```

```
        if(KeyCnt == 4) //condn to check if the keyval reached the max keycnt
        {
           lcd_cmd(0x01);
           KeyCnt =0;            //6666 - clearing for next time operation
           CmpPassword = strcmp(DefaultPassword,EnteredPassword);

           if(CmpPassword == 0)
           {
              device = ~device; // Device control for correct password
              lcd_cmd(0x80); //to display in first row
              lcd_str("Correct Password"); //display string
              dely(500);
           }
           else
           {
              attempts--; // Reduce attempts on wrong password entry

              if (attempts == 0) {
                 red_led = 1; // Turn on red LED for wrong password
                 buzzer = 1; // Turn on buzzer for wrong password
                 lcd_cmd(0x80);
                 lcd_str("Wrong Password");
                 dely(500);
                 red_led = 0; // Turn off red LED after a delay
                 buzzer = 0; // Turn off buzzer after a delay
              } else {
                 lcd_cmd(0x80);
                 lcd_str("Wrong Password. ");
                 lcd_cmd(0xC0);
                 lcd_data('0' + attempts); // Display remaining attempts
                 lcd_str(" more attempts left.");
                 dely(1000); // Wait for a moment before clearing the display
              }
           }
        }
     }
}

char get_keypad_key(void)
{
    char key_val =0;
          keypad = 0xFE; //ROW1 =0
         if(keypad == 0xee) // button 1
                 {
          key_val = '1';
                 }
         if(keypad == 0xde) // button 2
                 {
          key_val = '2';
                 }
                  if(keypad == 0xbe) // button 3
                 {
          key_val = '3';
                 }

                 keypad = 0xFD; //ROW2 =0
```

```
                if(keypad == 0xED) // button 4
                {
                key_val = '4';
                }
                if(keypad == 0xDD) // button 5
                {
                key_val = '5';
                }
                 if(keypad == 0xBD) // button 6
                {
                key_val = '6';
                }

                keypad = 0xFB; //ROW3 =0
                if(keypad == 0xEB) // button 7
                {
                key_val = '7';
                }
                if(keypad == 0xDB) // button 8
                {
                key_val = '8';
                }
                 if(keypad == 0xBB) // button 9
                {
                key_val = '9';
                }

                    keypad = 0xF7; //ROW3 =0
                if(keypad == 0xE7) // button *
                {
                key_val = '*';
                }
                if(keypad == 0xD7) // button 0
                {
                key_val = '0';
                }
                 if(keypad == 0xB7) // button #
                {
                key_val = '#';
                }
   return key_val;
}


void lcd_str(unsigned char *str)
{
   unsigned int loop =0;
   for(loop =0; str[loop]!= '\0'; loop++)
   {
      lcd_data(str[loop]);
   }
}
void lcd_data(unsigned char ch)
{
   LCD_dat = ch;
   rs = 1;  // data
```

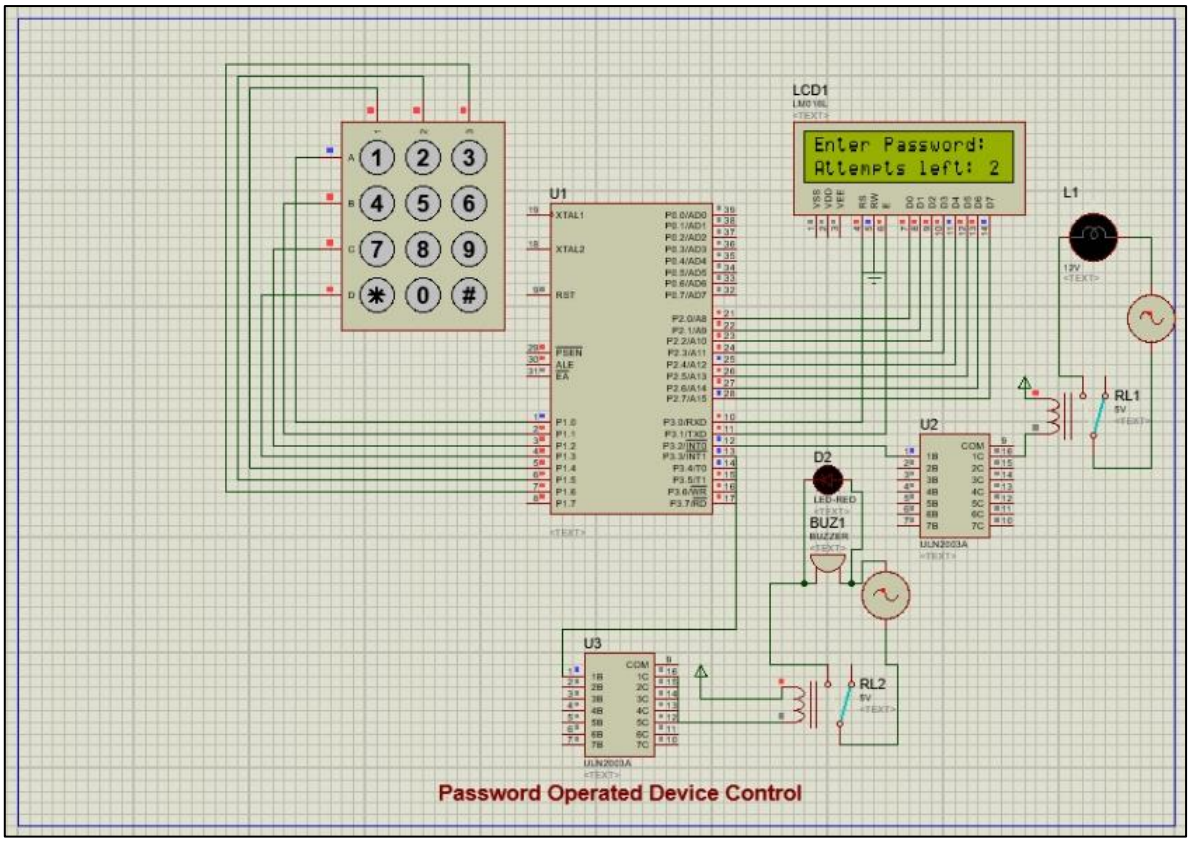
```
    en = 1;
    dely(10);
    en = 0;
}

void lcd_cmd(unsigned char ch)
{
    LCD_dat = ch;
    rs = 0;  // cmd
    en = 1;
    dely(10);
    en = 0;
}
void dely(unsigned int dly)
{
    unsigned int loop =0;
    unsigned int delay_gen =0;
    for(loop =0; loop < dly; loop++)
    for(delay_gen =0; delay_gen < 1000; delay_gen++); /* delay */
}
```

Output:

Here the user will get three attempts to give the password to check.

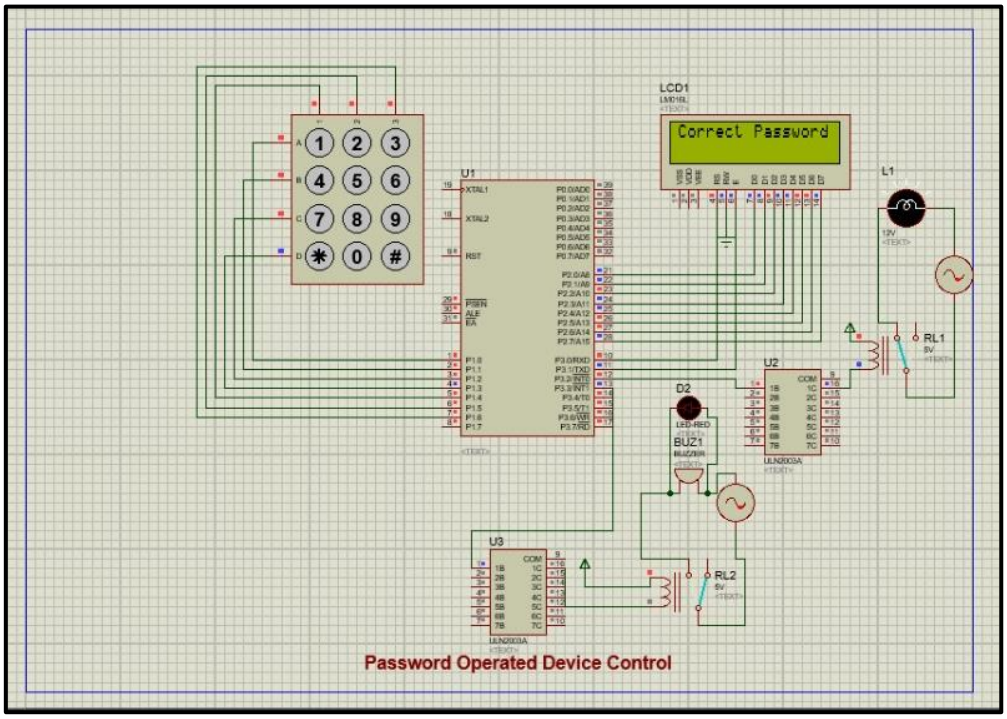
First attempt:

In the first attempt the user enters a password. Since the password entered earlier was wrong, the LCD displays that it was the wrong password and the user has 2 more attempts out of 3 remaining.



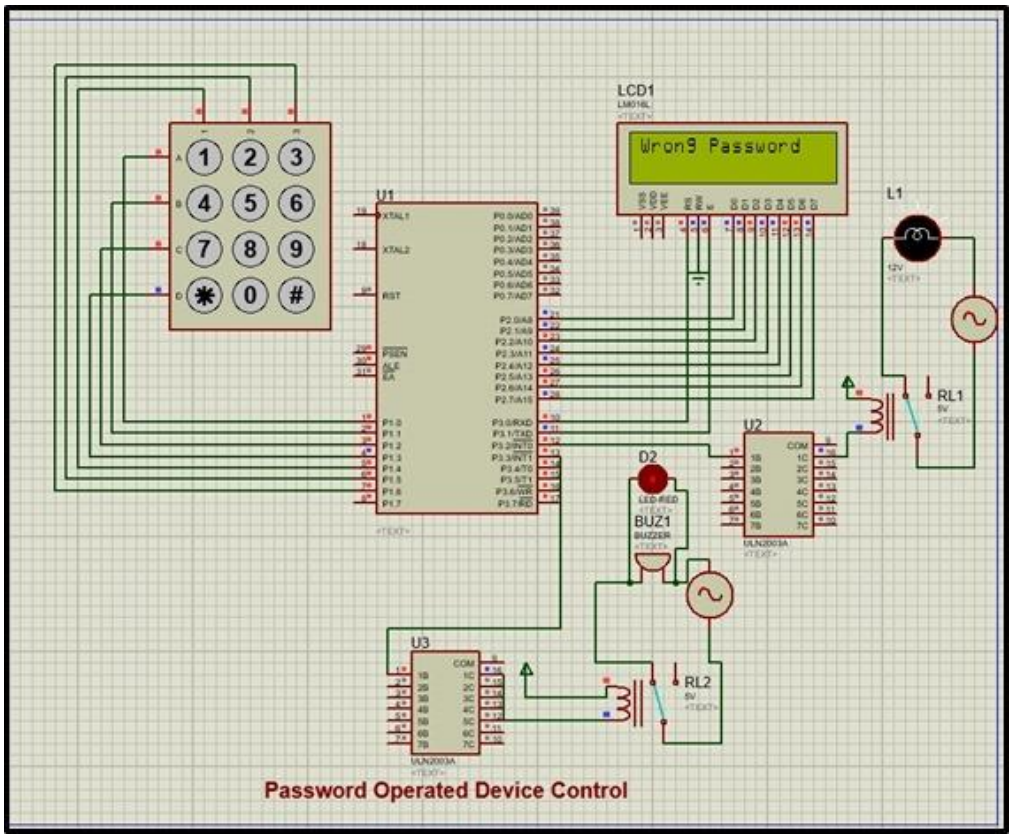
Second attempt:

Since the user entered the correct password in the 2nd attempt the LCD displays "Correct Password" and the Electric bulb will glow (remains in ‘ON’ state until it is entered with correct password).



Third attempt:

When all the 3 attempts are over, the LCD just displays "Wrong Password" with no more attempts remaining for the user to enter the password (LED glows red and the Buzzer turns ‘ON’).



References:

[1] Amos S.W. & James M., Principles of transistor circuit: Introduction to the Design of Amplifiers, Receivers and Digital Circuits, 6th Ed., Hartnolls Ltd.

[2] Datasheet Search System, http://www.alldatasheet.com.

[3] Forrest M., Engineer's Mini Notebook, Volume I. Timer, Op Amp & Optoelectronic Circuits & Projects, 1st Ed.

[4] Horowitz P. & Hill W., The art of Electronics, 2nd Ed., Cambridge University Press, U.S.A.,

[5] How stuff works, http://www.howstuffworks.com/.

[6] Theraja B.L. & Theraja A.K., A text book of electrical technology, Ed. 21st, Publisher; publication of division of Nirja construction and Development co., Ltd. Ram Nagar.

[7] Aneke, C., Ezenkwu, C. P., & Ozuomba, S. Design and implementation of a Microcontroller -Based keycard. ResearchGate. https://www.researchgate.net/publication/366205375_Design_And_Implementation_Of_A_Microcontroller-Based_Keycard?enrichId=rgreq-28a4356a3a721506bd5d0714e6c7660c-XXX&enrichSource=Y292ZXJQYWdlOzM2NjIwNTM3NTtBUzoxMTQzMTI4MTExMTE2NzA3MUAxNjcyOTE4OTQ2NzE5&el=1_x_3&_esc=publicationCoverPdf

[8] Douglas Hall "Microprocessor and Interfacing". (pg 20-24, 32).

[9] ELECTRONIC CIRCUITS (Fundamentals of Transistor Applications in Digital Circuit designing By Prof. G. N. Onoh.

[10] Practical Approach to Corporate Data Processing by Prof H.C Inyiama.

[11] Oke, A.O., O.M. Olaniyi, O.T. Arulogun, and O.M. Olaniyan. "Development of a Microcontroller-Controlled Security Door System". Pacific Journal of Science and Technology. 10(2):398-403.

[12] Inderpreet Kaur."Microcontroller Based Home Automation System with Security".International Journal of Advanced Computer Science and Applications,Vol. 1.