MICROCONTROLLER & INTERFACING PROJECT REPORT

RFID BASED SECURITY SYSTEM

Nehanshu Prajapati (22BEC077)

Karan Patel (22BEC085)

Panthil Patel (22BEC089)

1. Introduction:

- RFID technology operates by utilizing electromagnetic fields to wirelessly communicate between a reader and passive or active tags. These tags, embedded with unique identifiers, can be attached to objects, vehicles, or individuals, enabling swift and accurate identification without the need for physical contact. This inherent advantage makes RFID systems particularly suitable for access control applications, where speed, accuracy, and reliability are essential.
- The integration of RFID technology with microcontrollers, such as the widely-used 8051 series, facilitates the development of sophisticated access control systems with enhanced functionalities. By leveraging the processing power and versatile input/output capabilities of microcontrollers, RFID-based security systems can effectively manage access permissions, authenticate users, and log access events in real-time.

2. Components Used:

- 8051 Microcontroller: Acts as the main control unit, interfacing with RFID reader, keypad, LCD display, and other peripherals.
- RFID Reader: Reads RFID tags placed within its range and communicates the tag information to the microcontroller.
- Keypad: Allows users to input a passkey for additional security verification.
- LCD Display: Provides visual feedback to the user, displaying messages, prompts, and access status.
- Buzzer: Generates audio signals for indicating access status, such as granted or denied.
- Motor Drivers: Control the locking mechanisms or gates to grant physical access upon successful verification.

3. System Operation:

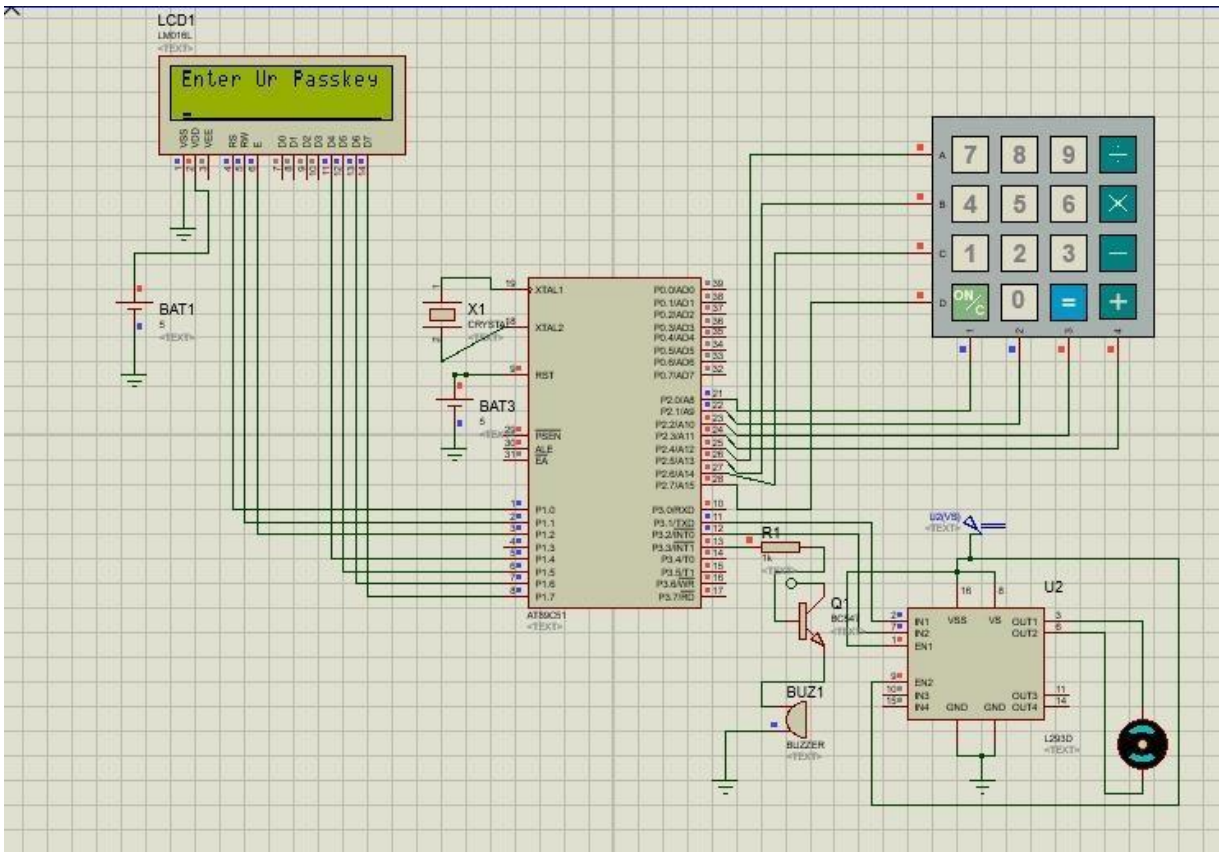
- Upon system startup, the LCD displays a welcome message indicating the initiation of the security system.
- The RFID reader continuously scans for RFID tags within its range.
- When a tag is detected, its unique identifier is transmitted to the microcontroller.
- The microcontroller compares the received RFID tag ID with pre-defined IDs stored in its memory to determine the identity of the person.
- If the RFID tag matches any stored IDs, the system prompts the user to enter a passkey using the keypad.

- The entered passkey is compared with the stored passkey associated with the detected RFID tag.
- If the passkey matches, access is granted, and the LCD displays a success message along with the person's identity.
- Additionally, the motor drivers are activated to unlock the door or gate, allowing physical access.
- If either the RFID tag or passkey doesn't match, access is denied, and the system alerts the user with a corresponding message on the LCD and activates the buzzer.
- The system then resets and waits for the next RFID tag detection.

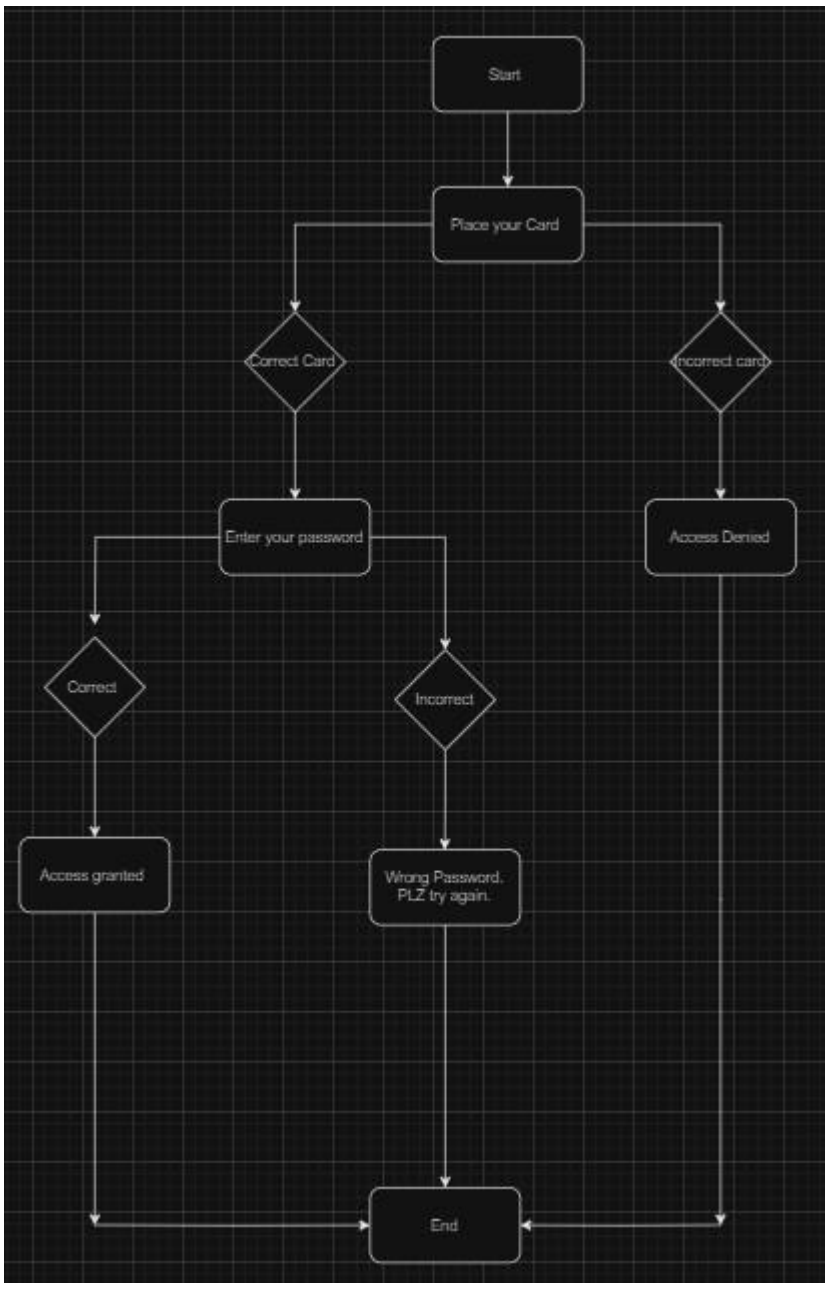
4. Security Considerations:

- The system uses both RFID tags and passkeys for dual-factor authentication, enhancing security.
- Passkeys add an extra layer of protection, ensuring that only authorized individuals with the correct passkey can gain access.
- Continuous scanning of RFID tags ensures real-time detection and response to access attempts.
- Access denied alerts, such as the buzzer sound, serve as deterrents and notify security personnel of potential unauthorized access attempts.

Circuit diagram:


LCD1
LM016L
Enter Ur Passkey
BAT1
X1
CRYSTAL
BAT3
AT89C51
R1
Q1
BC547
BUZ1
BUZZER
U2
L293D

Flow chart:



Algorithm: RFID-Based Security System using 8051 Microcontroller

1. Initialize System:

- Initialize the 8051 microcontroller and all connected peripherals (RFID reader, keypad, LCD display, buzzer, motor drivers).
- Display a welcome message on the LCD to indicate system initiation.

2. Main Loop:

- Enter an infinite loop to continuously monitor for RFID tag detections and handle access control operations.

3. RFID Detection:

- Continuously scan for RFID tags using the RFID reader.
- If an RFID tag is detected:

a. Read the unique identifier (RFID ID) from the tag.
b. Display a message on the LCD prompting the user to place their card.

4. Authentication:

- Compare the received RFID ID with pre-defined IDs stored in the microcontroller's memory.
- If a matching ID is found:

a. Prompt the user to input a passkey using the keypad.
b. Read and store the entered passkey.
c. Compare the entered passkey with the stored passkey associated with the detected RFID ID.

d. If the passkey matches:

- Display an "Access Granted" message on the LCD.
- Activate the motor drivers to unlock the door/gate.
- Optionally, display the name or identity of the authorized person.

e. If the passkey doesn't match:

- Display a "Wrong Passkey" message on the LCD.
- Activate the buzzer to indicate access denial.

f. If no matching RFID ID is found:

- Display an "Access Denied" message on the LCD.
- Activate the buzzer to indicate access denial.

5. Handle Access:

- Depending on the access status (granted/denied), activate corresponding actions:

• Access Granted:
- Unlock the door/gate using motor drivers.
- Display access status and authorized person's identity on the LCD.

• Access Denied:
- Activate the buzzer to indicate denial of access.
- Display access status on the LCD.

6. Loop Continuation:

   - Continue looping to monitor for new RFID tag detections and handle access control operations indefinitely.

7. End of Algorithm.

Code :-

```
#include<reg51.h>

#include<string.h>

#include<stdio.h>

#define lcdport P1

sbit col1=P2^0;

sbit col2=P2^1;

sbit col3=P2^2;

sbit col4=P2^3;

sbit row1=P2^4;

sbit row2=P2^5;

sbit row3=P2^6;

sbit row4=P2^7;

sbit rs=P1^0; sbit

rw=P1^1; sbit

en=P1^2;
```

```
sbit m1=P3^1; sbit
m2=P3^2; sbit
buzzer=P3^3; char
i,rx_data[50]; char
rfid[12],ch=0; char
pass[4]; void
delay(int m){
        int i,j;   for( i=0;i<m;i++){
        for( j=0;j<1275;j++){
                }
        }
} void
dataen(){
        rs=1;
rw=0;  en=1;
        delay(10);
  en=0; } void lcddata(unsigned
char ch){
lcdport=ch&0xf0;
   dataen();
        lcdport=(ch<<4)&0xf0;
dataen();
} void
command()
{
```

```
        rs=0;
rw=0;  en=1;
        delay(10);
en=0;
} void lcdcmd(unsigned char ch
){
        lcdport=ch&0xf0;
command();
        lcdport=(ch<<4)&0xf0;
command();
} void lcdstring(char
*str)
{
        while(*str){
lcddata(*str);
                str++;
        }
} void
lcd_init(void) {
delay(10);
lcdcmd(0x02);
delay(10);
   lcdcmd(0x28);
delay(10);
   lcdcmd(0x0e);
delay(10);
```

```
   lcdcmd(0x01);
        delay(10);
} void
uart(){
        TMOD=0x20;
        SCON=0x50;
 TH1=0xfd;
 TR1=1;
} char
rxdata()
{
        while(!RI);
ch=SBUF;      RI=0;
        return ch;
} void keypad() {     lcdcmd(1);
lcdstring("Enter Ur Passkey");
lcdcmd(0xc0);
   i=0;
while(i<4)
   {     col1=0;
col2=col3=col4=1;
if(!row1)
    {
lcddata('1');
pass[i++]='1';
while(!row1);
```

```
}       else
if(!row2)
    {
lcddata('4');
pass[i++]='4';
while(!row2);    }
else if(!row3)
    {  lcddata('7');
pass[i++]='7';
while(!row3);    }
else if(!row4)
    {        lcddata('*');
pass[i++]='*';
while(!row4);    }
col2=0;
col1=col3=col4=1;
if(!row1)
    {
lcddata('2');
pass[i++]='2';
while(!row1);    }
else if(!row2)
    {
lcddata('5');
pass[i++]='5';
```

```
while(!row2);    }
else if(!row3)
    {
lcddata('8');
pass[i++]='8';
while(!row3);    }
else if(!row4)
    {
lcddata('0');
pass[i++]='0';
while(!row4);
  }
 col3=0;
col1=col2=col4=1;
if(!row1)
    {
lcddata('3');
pass[i++]='3';
while(!row1);    }
else if(!row2)
    {
lcddata('6');
pass[i++]='6';
while(!row2);    }
else if(!row3)
```

```
    {
lcddata('9');
pass[i++]='9';
while(!row3);
  }       else
if(!row4)
    {         lcddata('#');
pass[i++]='#';
while(!row4);    }
col4=0;
col1=col3=col2=1;
if(!row1)
    {
lcddata('A');
pass[i++]='A';
while(!row1);
  }   else
if(!row2)
    {
lcddata('B');
pass[i++]='B';
while(!row2);
}       else
if(!row3)
    {
lcddata('C');
```

```
pass[i++]='C';
while(!row3);    }
else if(!row4)
    {
lcddata('D');
pass[i++]='D';
while(!row4);
  }
 } } void
accept()
{
        lcdcmd(1);
lcdstring("Welcome");
lcdcmd(192);
        lcdstring("Password accept");
delay(200);
} void
wrong(){
        buzzer=0;
lcdcmd(1);
lcdstring("Wrong Passkey");
lcdcmd(192);
        lcdstring("PLZ Try
Again");         delay(1000);
buzzer=1;
}
```

```
void main() {          buzzer=1;
uart();   lcd_init();   lcdstring("
RFID     Based                  ");
lcdcmd(0xc0);
lcdstring("Security  system  ");
delay(400);    while(1)
   {       lcdcmd(1);
lcdstring("Place Your Card:");
lcdcmd(0xc0);      i=0;
          for(i=0;i<12;i++){
rfid[i]=rxdata();
          }
          rfid[i]='\0';
lcdcmd(1);
          lcdstring("Your ID No. is:");
lcdcmd(0xc0);   for(i=0;i<12;i++){
                    lcddata(rfid[i]);
          }
                              delay(100);
       if(strncmp(rfid,"3E00EA7CAE06",12)==0)
       {           keypad();
if(strncmp(pass,"1473",4)==0)
          {           accept();
lcdcmd(1);           lcdstring("Access
Granted ");           lcdcmd(0xc0);
```

```
lcdstring("Person1");           m1=1;
m2=0;           delay(300);
m1=0;           m2=0;
delay(200);           m1=0;
m2=1;           delay(300);
m1=0;           m2=0;
        }
else
wrong();        }

            else if(strncmp(rfid,"3E00EA7CC961",12)==0)
          {           keypad();
if(strncmp(pass,"1369",4)==0)
          {           accept();
lcdcmd(1);           lcdstring("Access
Granted ");           lcdcmd(0xc0);
lcdstring("Person2");           m1=1;
m2=0;           delay(300);
m1=0;           m2=0;
delay(200);           m1=0;
m2=1;           delay(300);
m1=0;           m2=0;
        }
else
wrong();
    }
```

```
            else if(strncmp(rfid,"3E00EA7CAD05",12)==0)
          {
   keypad();
if(strncmp(pass,"7413",4)==0)
          {           accept();
lcdcmd(1);            lcdstring("Access
Granted ");           lcdcmd(0xc0);
lcdstring("Person3");           m1=1;
m2=0;           delay(300);
m1=0;           m2=0;
delay(200);           m1=0;
m2=1;           delay(300);
m1=0;           m2=0;
         }
else
wrong();       }
else
       {          lcdcmd(1);
lcdstring("Access Denied");
buzzer=0;
          delay(100);
buzzer=1;
       }
}
}
```

Conclusion :-

In conclusion, the RFID-based security system, powered by the 8051 microcontroller, presents a sophisticated and efficient solution for access control across various environments. By seamlessly integrating RFID technology with auxiliary components such as keypads and LCD displays, the system enables swift identification and authentication of individuals while ensuring user-friendly operation. Leveraging the processing capabilities of the 8051 microcontroller, the system orchestrates real-time validation of RFID tags and passkey authentication, bolstering security measures with a multi-layered approach. As technology continues to evolve, the system holds potential for further enhancements, including the integration of advanced authentication methods and scalability improvements, ensuring its continued relevance and effectiveness in addressing the dynamic security challenges of the future