TEAM – 10

Configurable Password Security System Using 8051

components:

8051 microcontroller (e.g., AT89S52)

Keypad

LCD display

Buzzer

LEDs

Resistors

Capacitors

Crystal oscillator

Push buttons for configuration

Power supply

SAFE LINK :
https://www.youtube.com/watch?v=CA3hx6A1WZo&list=PLAY30bf7ZN4zelHC3EpcWVhfWYIVPaMH4

Hardware Setup:

Connect the keypad to the microcontroller's input ports.

Connect the LCD display to the microcontroller.

Connect the buzzer and LEDs for indicating access status.

Connect push buttons for configuration.

Initialize Peripherals:

Initialize the keypad, LCD display, buzzer, and LEDs in your code.

Password Storage:

Define a default password and a configurable password in the program memory of the microcontroller.

Provide options to the user to change the password using push buttons.

User Interface:

Display a prompt on the LCD asking for the password.

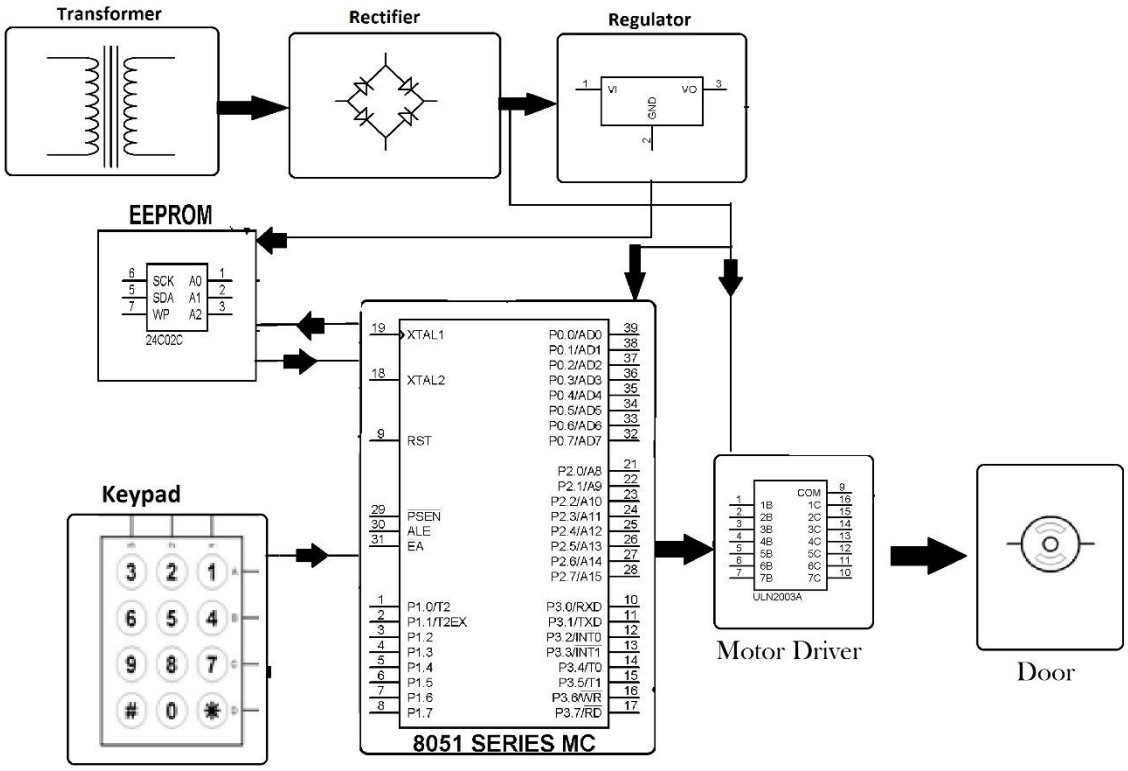
Read the entered password from the keypad.

Compare the entered password with the stored password.

Access Control:

If the entered password matches the stored password, grant access by activating LEDs and providing a message on the LCD.

If the entered password is incorrect, deny access by activating the buzzer and displaying an error message on the LCD.



Configuration Mode:

Provide a configuration mode accessed by a specific combination of push buttons.

In this mode, allow the user to change the password.

Save the new password to the memory.

Security Features:

Implement timeout mechanisms to prevent brute force attacks.

Encrypt the stored password to enhance security.

Testing and Debugging:

Test the system thoroughly under various scenarios to ensure reliability and security.

Debug any issues encountered during testing.

Deployment:

Once the system is fully functional and tested, deploy it in the desired environment.

Documentation:

Document the system design, hardware connections, software algorithms, and any special considerations for maintenance and troubleshooting.

User Instructions:

Provide clear instructions to users on how to operate the system, change passwords, and troubleshoot common issues.

Future Enhancements:

Consider adding features such as multiple user support, logging access attempts, or integrating with external systems for more comprehensive security solutions.