Password-Based Authentication and Automatic Entry Monitoring System with Security Alert and Thief Detector

Digital Logic Design sessional Project

Submitted by

Mohammed Mahbub Alam

2108017

Level 2 Term 2

Department of Electronics and Telecommunication Engineering

Submitted to

Dr. Nurshedul Mamun,

Assistant Professor,

Department of Electronics and Telecommunication Engineering

1. Abstract

This project presents a password-based authentication and automatic entry monitoring system designed using digital logic components. The system restricts unauthorized access by verifying a predefined password stored using a CD4043 SR latch. Incorrect password attempts activate visual and audio alerts, while a laser and LDR-based sensing mechanism detects and counts authorized entries. The entry count is displayed in real time using a seven-segment display. The system provides an efficient, low-cost security solution suitable for restricted environments such as laboratories and offices.

2. Introduction

Security systems play a crucial role in protecting restricted areas from unauthorized access. Conventional locking systems lack real-time monitoring and alert mechanisms. This project addresses these limitations by implementing a digital logic-based authentication system that not only validates users through a password but also monitors and records authorized entries. The design integrates logic gates, latches, sensors, counters, and indicators to achieve reliable security and monitoring.

3. Objectives

The main objectives of this project are:

- To design a password-based authentication system using digital logic.
- To store the password securely using a CD4043 SR latch.
- To generate alerts for incorrect password attempts.
- To monitor and count authorized entries automatically.
- To display the entry count in real time using a seven-segment display.

4. Working Principle

The system consists of three major sections: password storage and verification, security alert generation, and entry monitoring with counting.

The password is initially entered using DIP switches and stored in a CD4043 SR latch. The latch holds the password as long as power is supplied, ensuring stable storage. A

setting switch controls when the password can be stored, and when the supply voltage is low, the setting mechanism is disabled to prevent accidental or unauthorized modification.

When the main switch is turned ON, the system becomes active and the user re-enters the password. The entered password bits are compared with the stored bits using XOR gates. If the bits match, the XOR output remains LOW; if there is any mismatch, the output becomes HIGH. The outputs of all XOR gates are combined using NOR gates to determine whether the password is correct.

If the password is incorrect, a red LED and buzzer are activated, providing visual and audio alerts indicating an unauthorized access attempt. If an intruder attempts to bypass the system physically, a laser and LDR arrangement detects the interruption.

When the password is correct, a green LED turns ON, enabling the entry monitoring system. A laser beam continuously falls on an LDR sensor, and when a person crosses the entry point, the beam interruption generates a logic pulse. This pulse is fed to a counter circuit, which increments by one for each valid entry. The total number of entries is displayed on a seven-segment cathode display.

5. Components Used

5.1. Integrated Circuits

- CD4043 SR Latch
- XOR Gate IC 7486
- NOR Gate IC 7402

5.2. Input and Output Devices

- DIP switches
- Push buttons and tactile switches
- Green and red LEDs
- Buzzer
- Seven-segment cathode display

5.3. Sensors and Power Supply

- Laser light

- Light Dependent Resistor (LDR)
- 5V to 12V DC power supply

6. Simulation

The proposed password-based authentication and automatic entry monitoring system was simulated using digital logic simulation software to verify its correct operation. The simulation includes the password storage using the CD4043 SR latch, password comparison using XOR and NOR gates, alert generation for incorrect passwords, and entry counting using laser interruption logic.

During simulation, the stored password and the entered password were compared successfully. For incorrect password inputs, the red LED and buzzer were activated, indicating unauthorized access. For correct password inputs, the green LED was activated and the counter circuit was enabled. The laser and LDR mechanism was simulated by generating logic pulses, which incremented the counter. The total number of entries was displayed correctly on the seven-segment cathode display.

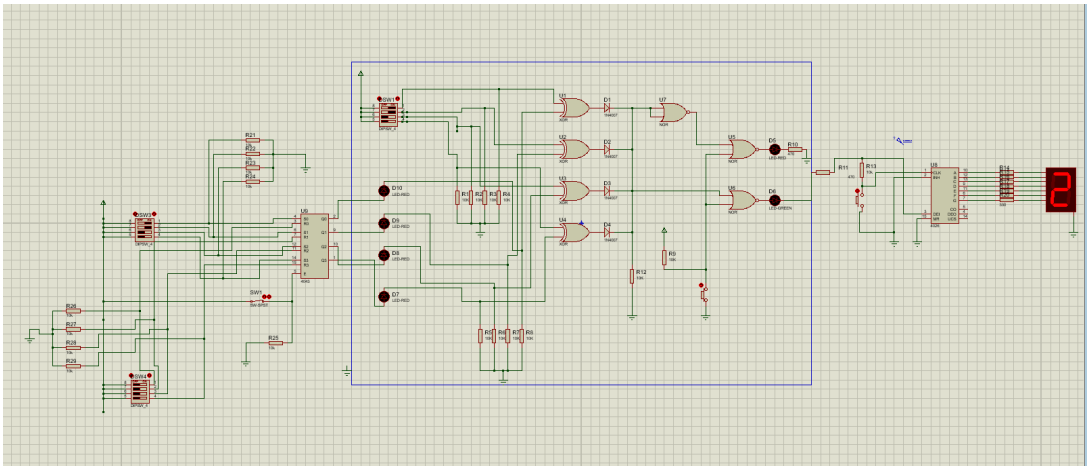

Figure 1: Simulation of Password-Based Authentication and Entry Monitoring System

7. Advantages

- Enhanced security using password authentication.
- Stable password storage using SR latch.
- Immediate alert for unauthorized access.
- Real-time monitoring and entry counting.

- Cost-effective and easy to implement.

8. Limitations

- Limited scalability for multiple entry points.
- Requires continuous power supply.
- Laser and LDR performance may be affected by environmental conditions.

9. Conclusion

The password-based authentication and automatic entry monitoring system successfully demonstrates the application of digital logic concepts for security purposes. The use of a CD4043 SR latch ensures reliable password storage, while XOR and NOR gates provide accurate password verification. The integration of alert mechanisms and laser-based entry counting enhances system reliability. This project offers an effective and economical solution for restricted access environments.