



International Journal of Research Publication and Reviews

Journal Homepage: www.ijrpr.com ISSN 2582-7421

Digital Security System with Password & RFID

Pranav Balasaheb Borade¹, Sanket Sunil Batwak², Raj Subhash Shinde³, Prof. Satpute A. S⁴

¹⁻³ Student, ⁴Guide

Department of Electronics And Telecommunication Engineering, Samarth Rural Educational Institute's Department of Electronics And Telecommunication Engineering, Samarth Rural Educational Institute's

ABSTRACT

The **Digital Security System with Password and RFID** is an electronic security system designed to provide secure and reliable access control. The system uses two authentication methods: a password and a Radio Frequency Identification (RFID) card. It helps prevent unauthorized access to restricted areas, lockers, rooms, and other secured locations.

The system consists of a microcontroller, an RFID reader, RFID cards, a keypad, and an electronic locking mechanism. When a user scans an RFID card, the system verifies whether the card is authorized. If the card is valid, the user is prompted to enter a password. The system checks the entered password against the stored password. If both authentication methods are successful, the electronic lock is activated, allowing access. If an invalid RFID card or incorrect password is detected, access is denied, and the system may display an error message.

The main objective of this project is to improve security by combining RFID technology with password-based authentication. Unlike traditional lock-and-key systems, this approach provides better access control and reduces the risk of unauthorized entry. The system is cost-effective, easy to implement, and suitable for applications such as offices, laboratories, homes, lockers, and restricted areas.

In conclusion, the Digital Security System with Password and RFID offers an effective solution for modern access control. By combining two authentication methods, it enhances security, improves reliability, and provides a convenient way to protect valuable resources and restricted spaces.

Keywords: Digital Security, RFID, Password Authentication, Microcontroller, Access Control, Electronic Lock, Security System.

1. INTRODUCTION

In today's modern world, security has become an important concern in homes, offices, educational institutions, banks, laboratories, and other restricted areas. Traditional security systems, such as mechanical locks and keys, are widely used but have several limitations. Keys can be lost, stolen, or duplicated, which may lead to unauthorized access. Therefore, there is a need for a more secure, reliable, and convenient digital security system.

The **Digital Security System with Password and RFID** is designed to improve access control by combining two authentication methods: password verification and Radio Frequency Identification (RFID) technology. This system ensures that only authorized users can access a secured area. It uses electronic components such as a microcontroller, an RFID reader, RFID cards, a keypad, and an electronic locking mechanism to provide secure access.

RFID technology uses radio waves to identify and authenticate RFID cards or tags. When a user scans an RFID card near the reader, the system reads the card's identification number and checks whether it is registered. If the card is valid, the user can proceed to enter a password using the keypad. The microcontroller verifies the entered password against the stored password. When both the RFID card and password are correct, the system activates the electronic lock and grants access. If either authentication step fails, access is denied.

2. LITERATURE SURVEY

Overview

The proposed **Digital Security System with Password and RFID** can be implemented using an Arduino Uno or another suitable microcontroller. An RFID reader is used to identify authorized RFID cards, while a keypad allows users to enter a password for authentication. An LCD display provides instructions and authentication messages, while a buzzer alerts users when an invalid card or incorrect password is detected. An electronic lock or relay is used to control access to the protected area.

The main objective of this project is to develop a cost-effective, reliable, and easy-to-use security solution. It can be used in homes, offices, educational institutions, laboratories, libraries, and personal lockers. The system can also be extended with additional features, such as automatic relocking, limited password attempts, alarm notifications, and access-record management.

Overall, the Digital Security System with Password and RFID demonstrates how RFID technology and password-based authentication can be integrated to improve electronic access control and help protect valuable resources from unauthorized access.

RFID Module-Based Authentication

RFID (Radio Frequency Identification) technology is widely used in electronic identification and access-control systems. Common RFID modules include the MFRC522 (RC522) and PN532. These modules communicate with RFID cards or tags to obtain identification information and transfer it to a microcontroller for verification.

When a user presents an RFID card near the reader, the module reads the card's identification number. The microcontroller compares this information with the registered card details stored in the system. If the card is authorized, the user can proceed to the next authentication step. Otherwise, access is denied.

RFID technology is commonly used in door access control, attendance management, inventory tracking, transportation systems, and electronic security applications. Its contactless operation provides convenience and reduces the time required to identify authorized users.

Microcontroller-Based Security System

Microcontrollers such as **Arduino Uno, ESP32, and other embedded controllers** are commonly used in electronic security systems. The microcontroller acts as the main control unit and manages communication between the RFID reader, keypad, LCD display, buzzer, and electronic locking mechanism.

The controller receives identification data from the RFID reader and password input from the keypad. It processes the information according to predefined instructions and determines whether access should be granted or denied.

The microcontroller can also control output devices such as **LCD displays, LEDs, buzzers, relays, and electronic locks**. This allows the security system to operate automatically without requiring continuous human supervision.

The **ESP32** is particularly useful for smart security applications because it provides processing capabilities along with built-in **Wi-Fi and Bluetooth connectivity**. These features allow the system to be extended with IoT-based monitoring, remote notifications, and access-record management.

3. PROBLEM STATEMENT

Traditional security systems that use mechanical locks and keys have several limitations, including the risk of lost keys, unauthorized key duplication, and difficulty in managing access to restricted areas. Similarly, security systems that rely only on passwords or RFID cards may be vulnerable if passwords are shared or cards are lost or stolen. These limitations create a need for a more reliable, convenient, and secure access-control system.

The **Digital Security System with Password and RFID** aims to develop an electronic security solution that combines RFID card identification with password authentication to prevent unauthorized access. The system uses a microcontroller to process the information received from the RFID reader and keypad. Access is granted only when the RFID card is authorized and the entered password is correct. If either authentication method fails, the system denies access and can generate an alert.

The main problem addressed by this project is the lack of an effective, affordable, and easy-to-use security mechanism that provides multiple levels of authentication. The proposed system is designed to improve access control, reduce the risk of unauthorized entry, and provide a convenient method for protecting restricted areas.

The system can be implemented in homes, offices, educational institutions, laboratories, libraries, and personal lockers. Additional features, such as automatic relocking, incorrect-password attempt limits, and alarm notifications, can further enhance its security and reliability.

4. METHODOLOGY

The methodology of the **Digital Security System with Password and RFID** involves designing and implementing an electronic access-control system that combines RFID card identification and password authentication to improve security. The system consists of a microcontroller such as Arduino Uno, an RFID reader, RFID cards, a keypad, an LCD display, a buzzer, and an electronic locking mechanism. These components work together to identify authorized users and prevent unauthorized access to the protected area.

Initially, the system is powered on, and the microcontroller initializes all connected components. The LCD displays a message asking the user to scan an RFID card. When the user brings the card near the RFID reader, the reader captures the card's identification number and sends it to the microcontroller for verification. The controller compares the received identification number with the registered card information stored in the system. If the card is invalid, access is denied, and the buzzer may generate an alert. If the card is authorized, the system prompts the user to enter a password using the keypad.

After receiving the password, the microcontroller compares it with the stored password. If the entered password is correct, the system activates the electronic locking mechanism through a suitable relay or driver circuit, allowing the authorized user to access the secured area. If the password is incorrect, access is denied, and an error message is displayed on the LCD. The system can also be programmed to limit the number of incorrect password attempts to reduce the risk of unauthorized access.

The LCD display provides information and instructions throughout the authentication process, including messages such as *Scan RFID Card*, *Enter Password*, *Access Granted*, and *Access Denied*. The buzzer provides audible alerts when an invalid card or incorrect password is detected. After granting access for a predefined period, the system can automatically return to the locked state to maintain security. These features make the system convenient to operate and improve the monitoring of access attempts.

Finally, the complete system is tested under different conditions to evaluate its functionality and reliability. Testing includes scanning valid and invalid RFID cards, entering correct and incorrect passwords, checking the operation of the electronic lock, and verifying the responses of the LCD display and buzzer.

5. Conclusion

The **Digital Security System with Password and RFID** provides an effective and reliable solution for improving security and controlling access to restricted areas. The system combines RFID card identification with password authentication to provide an additional layer of protection against unauthorized entry. By using a microcontroller, RFID reader, keypad, LCD display, buzzer, and electronic locking mechanism, the system verifies user credentials and grants access only when both the RFID card and password are valid.

The proposed system overcomes several limitations of traditional security methods, such as the loss or duplication of physical keys and the risks associated with using only one authentication method. It is cost-effective, easy to operate, and suitable for applications in homes, offices, educational institutions, laboratories, libraries, and personal lockers. The LCD display provides clear instructions, while the buzzer can alert users to invalid cards or incorrect passwords. Additional features, such as automatic locking, limited password attempts, and access-record management, can further enhance the system's functionality and security.

6. Reference

1. Arduino, *Arduino Uno Rev3 Documentation*. Available: <https://docs.arduino.cc/hardware/uno-rev3/>
2. Arduino, *Arduino Programming and Software Documentation*. Available: <https://docs.arduino.cc/>
3. NXP Semiconductors, *MFRC522 Standard Performance MIFARE and NTAG Frontend Datasheet*. Available: <https://www.nxp.com/docs/en/data-sheet/MFRC522.pdf>
4. NXP Semiconductors, *PN532 Near Field Communication (NFC) Controller Documentation*. Available: <https://www.nxp.com/>
5. Microchip Technology, *Microcontrollers and Embedded Systems Documentation*. Available: <https://www.microchip.com/>
6. Espressif Systems, *ESP32 Series Datasheets and Technical Documentation*. Available: <https://docs.espressif.com/projects/esp-idf/en/stable/esp32/>
7. GeeksforGeeks, *Radio Frequency Identification (RFID) Technology*. Available: <https://www.geeksforgeeks.org/>
8. Electronics Tutorials, *Electronic Security Systems and Digital Electronics*. Available: <https://www.electronics-tutorials.ws/>
9. TutorialsPoint, *Embedded Systems and Microcontroller Fundamentals*. Available: https://www.tutorialspoint.com/embedded_systems/
10. International Organization for Standardization (ISO), *ISO/IEC 14443: Identification Cards—Contactless Integrated Circuit Cards*. Available: <https://www.iso.org/>