Smart Door Lock using Fingerprint Sensor and RFID

Ganesh B S[1], Pratham D T[2], Amey C K[3], Yash S C[4]
[1,2,3,4] *Students of B.Tech, Computer Science, Rajiv Gandhi College of Engineering Research and Technology, Chandrapur, India*

As the demand for enhanced security and convenience in residential and commercial environments increases, smart door locks have become a focal point in the evolution of access control systems. Among the various technologies employed in these locks, fingerprint sensors and Radio Frequency Identification (RFID) stand out for their effectiveness and user-friendliness. These advanced locking mechanisms not only improve security but also streamline user interactions, making them an integral part of modern security solutions.

Fingerprint sensors offer a high level of security by utilizing unique biometric data for authentication. This technology ensures that only authorized individuals can gain access, effectively reducing the risks associated with lost keys or forgotten passcodes. On the other hand, RFID technology enables quick and seamless entry, allowing users to unlock doors with the tap of a card or fob, thereby enhancing the convenience factor.

Combining these two technologies, smart door locks equipped with fingerprint sensors and RFID provide a dual-layered approach to security. This paper investigates the functionalities, advantages, and potential vulnerabilities of such systems. It explores user acceptance, technical challenges, and the broader implications of integrating biometric and RFID technologies into smart home ecosystems. By examining these innovative solutions, this study aims to highlight their significance in the ongoing quest for safer and more accessible living and working environments.

Smart door locks represent a significant advancement in home security technology. Combining traditional locking mechanisms with modern biometric and RFID (Radio Frequency Identification) technologies, these devices enhance security while providing convenience and accessibility. Among the various types of smart locks, those equipped with fingerprint sensors and RFID capabilities are particularly noteworthy for their effectiveness and ease of use.

Functionality

1. Fingerprint Sensors:

- Biometric Authentication: Smart locks with fingerprint sensors use biometric data to verify the identity of users. This method is highly secure, as fingerprints are unique to each individual.
- User Management: Many models allow multiple fingerprints to be stored, enabling access for family members or trusted individuals while maintaining control over who can enter the property.
- Quick Access: Users can unlock the door in seconds, eliminating the need for keys or codes.

RFID Technology:

- Contactless Access: RFID-enabled smart locks typically come with key fobs or cards that can be scanned to unlock the door. This provides a fast and convenience
- Versatility: RFID tags can be issued to guests, service personnel, or family members, allowing temporary access without the need to share keys.
- Security Features: RFID systems often include encryption to protect against unauthorized access, making them a secure option for modern homes.

Benefits

- Enhanced Security: The integration of fingerprint scanning and RFID technology significantly reduces the risk of unauthorized entry. Unlike traditional keys, which can be lost or copied, biometric data and RFID tags offer a higher level of security.
- Convenience: Smart locks simplify entry and exit for users. With features such as remote access via smartphones, users can monitor and control their doors from anywhere, adding an extra layer of convenience.

- Data Logging: Many smart locks provide logs of entry and exit, allowing homeowners to track who accessed their home and when. This feature is valuable for monitoring activity, especially when multiple users have access.
- Integration with Smart Home Systems: These locks can be integrated into broader smart home ecosystems, enabling users to manage multiple devices from a single platform, enhancing overall home automation.

Challenges

Despite their advantages, smart locks also face challenges:

- Power Dependency: Most smart locks require a power source, whether batteries or wired connections. Users must ensure that their locks remain powered to maintain functionality.
- Vulnerability to Hacking: Like all connected devices, smart locks can be susceptible to cyber threats. Manufacturers must prioritize security measures to protect user data and access.
- Cost Considerations: The initial investment for smart locks can be higher than traditional locks, which may deter some users.

I. SYSTEM DESCRIPTION AND BLOCK DIAGRAM

A Smart Door Lock System with fingerprint and RFID authentication is an electronic locking solution designed to enhance security and convenience. This system integrates biometric (fingerprint) and RFID (Radio Frequency Identification) technologies, providing a multi-modal authentication mechanism for unlocking doors. Here's an overview of its main functionalities:

1. Fingerprint Authentication: A biometric fingerprint sensor is used to identify authorized individuals based on their unique fingerprint patterns. When an individual places their finger on the sensor, the system compares the input fingerprint to a database of stored templates. If a match is found, the lock is disengaged, allowing access.

2. RFID Authentication: RFID technology provides an alternative or supplementary authentication method. Authorized users possess RFID tags/cards which, when scanned by the system's RFID reader, are cross-verified against a database of registered tags. If the RFID tag is authenticated, the lock opens.

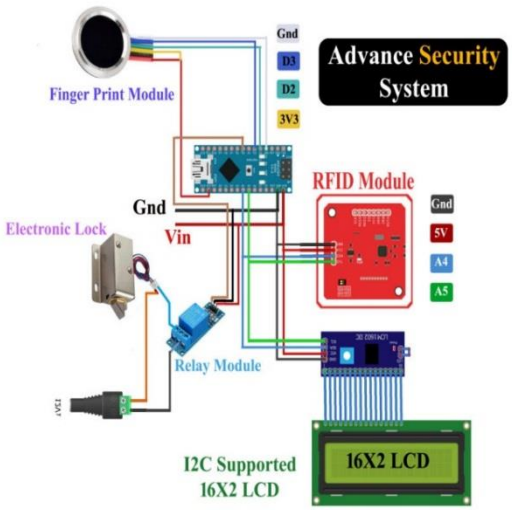
3. Microcontroller: The microcontroller serves as the system's main control unit, processing inputs from both the fingerprint and RFID modules. It handles decision-making by verifying user credentials, managing system states, and activating the locking mechanism based on the authentication outcome.

4. Locking Mechanism: This is typically an electronic or solenoid-based lock that engages or disengages in response to signals from the microcontroller. When access is granted, the lock is released, allowing the door to open; otherwise, it remains securely locked.

5. Power Supply: A stable power source, often DC-based, is required to power the microcontroller, fingerprint sensor, RFID reader, and locking mechanism. Some systems may include a battery backup to maintain functionality during power outages.

6. Additional Features: Advanced systems may integrate with mobile apps, offering users remote access and monitoring capabilities. Security alerts, logging, and time-based access control are also possible features.

Block Diagram



Here's a typical block diagram layout for a Smart Door Lock System with Fingerprint and RFID Authentication

II. SYSTEM IMPLEMENTATION

The **Smart Door Lock System** with fingerprint and RFID authentication combines hardware and software elements for robust access control. Implementing such a system requires careful integration of components, microcontroller programming, and user data management. The implementation process is outlined in stages, highlighting the design, hardware assembly, software programming, and testing.

1. **Hardware Components and Setup**

- **Microcontroller (e.g., Arduino, ESP32)**: The microcontroller acts as the central control unit. For this project, a microcontroller with sufficient I/O pins and memory to handle data from the fingerprint sensor and RFID module is selected.

- **Fingerprint Sensor Module**: Modules such as the R307 or FPM10A are commonly used for fingerprint recognition. They include an onboard processor to capture and match fingerprints, which can be integrated with a microcontroller via UART or SPI interface.

- **RFID Reader Module**: Typically, the RC522 RFID module is used. It operates on a 13.56 MHz frequency, communicating with RFID tags within a 2-5 cm range. It connects to the microcontroller using an SPI interface.

- **Locking Mechanism**: An electromagnetic lock, solenoid lock, or motorized latch is driven by the microcontroller based on successful authentication. This mechanism is powered by a DC power source, and a relay may be used to control the high-power locking device.

- **Power Supply**: A stable power source (e.g., a 5V or 12V DC adapter) is essential. A battery backup can also be added to maintain functionality during power outages.

2. **System Wiring and Assembly**

- **Connections to Microcontroller**: - The fingerprint sensor is connected to the microcontroller through serial UART pins. - The RFID module is connected using SPI pins for data transfer.The locking mechanism is connected through a relay circuit, which the microcontroller controls based on the authentication outcome.

- **Power Routing**:

- Ensure separate power for high-power components like the lock. The microcontroller should handle logic-level signals while the relay activates the lock mechanm.

3. **Software Development**

The software is developed in stages: data capture, processing, decision-making, and control output.

Programming Environment: An IDE such as Arduino IDE, MicroPython, or PlatformIO is used for writing, compiling, and uploading code to the microcontroller.

- **Fingerprint Enrollment**: - A fingerprint enrollment function is implemented to add new users. This function captures and stores fingerprints in a database or the sensor's internal memory. Upon enrollment, each fingerprint is assigned an ID, enabling the microcontroller to verify future matches against this ID.

- **RFID Tag Registration**:RFID tags/cards are registered by capturing the unique ID of each tag and storing it in the microcontroller’s memory or an external EEPROM.

- **Authentication Process**:**Fingerprint Matching**: When a fingerprint is placed on the sensor, it is compared to stored templates. If a match is found, the system flags it as an authenticated fingerprint.

- **RFID Tag Matching**: When an RFID tag is scanned, its ID is checked against the stored list. If it is recognized, authentication is successful.

- **Decision-Making Logic**: If either the fingerprint or RFID match is authenticated, the microcontroller sends a signal to the relay circuit to release the lock.

- **Fail-Safe and Security Mechanisms**: The software includes features to handle invalid attempts, such as a delay after a certain number of failed attempts and logging unauthorized access trials if connected to a monitoring system.

4. **Testing and Calibration** **Functional Testing**: Each component (fingerprint sensor, RFID module, and locking mechanism) is tested independently, followed by integration testing to ensure seamless operation.

- **Calibration**: The fingerprint sensor is calibrated for accuracy by testing with multiple users.

- RFID tag range and reliability are adjusted by testing tag readability at various distances.

- **Failure Mode Testing**: Scenarios such as power outages, sensor failures, or multiple failed login attempts are tested. Additionally, battery backup functionality is verified if implemented.

5.**System Integration and Deployment****System Assembly in Housing**: The system is enclosed in a protective housing near the door. The fingerprint sensor and RFID reader are positioned for easy user access.

- **User Interface**: Some systems may include an LCD display or LEDs to indicate successful authentication or errors, providing feedback to the user.

- **Deployment and Maintenance**: The system is installed on the door, and periodic maintenance checks are scheduled for like the fingerprint sensor, which may require occasional cleaning, and the RFID reader.

6. **Additional Features (Optional)**

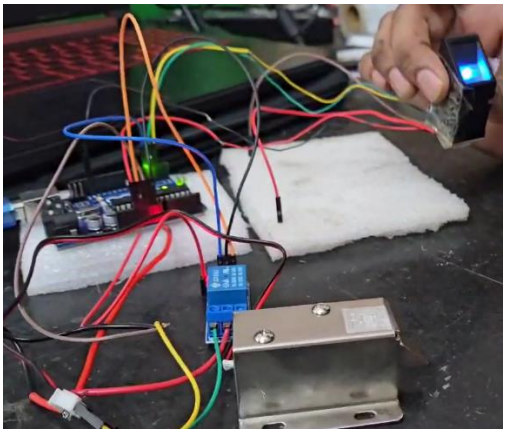
- **Remote Access**: The system can be connected to a network module (e.g., Wi-Fi or Bluetooth) to enable mobile app control or monitoring.

- **Logging and Analytics**: User access logs can be stored locally or sent to a cloud service for monitoring and review.

- **Alarm System Integration**: An alarm can be triggered in case of multiple failed attempts, alerting users to potential unauthorized access.

This implementation provides a secure, reliable, and user-friendly access control system combining biometric and RFID technologies. It is flexible for further expansion, like integration with mobile applications and remote monitoring.

III. OUTPUT



IV. CONCLUSION

Thus, the principal objective of this framework is executed and verified. In this framework, we have just validated individual can open the entryway through RFID and Fingerprint impression. The finger impression sensor will check approaching picture with selected information and it will convey affirming message. Similarly, the same is done with RFID. If both RFID check and finger impression picture affirmation are coordinated, the microcontroller will drive entryway valve as indicated by sensors at entryway edges. This framework is safer than different frameworks since two codes assurance techniques are utilized.

- Summarize the key findings and insights derived from the results and discussion.
- Emphasize the significance of the proposed door locking system in addressing security challenges and providing user-friendly access control solutions.
- Reinforce the importance of continued research and innovation in biometric authentication technologies for enhancing security in various environments.

By presenting and discussing the results of your experiments and evaluations in a structured manner, you can provide a comprehensive understanding of the performance and implications of the proposed door locking system using RFID and fingerprint sensor with Arduino.

V. REFERENCES

[1] Bhatt, H.S., Bharadwaj, S., Vatsa, M., Singh, R., Ross, A. and Noore, A. (2011) ‘A framework for quality-based biometric classifier selection’, Proc. of International Joint Conference on Biometrics, pp.1–7.

[2] Dieckmann, U., Plankensteiner, P. and Wagner, T. (1997) 'SESAM: a biometric person identification system using sensor fusion', Vol. 18, No. 9, pp.827–833.
[3] Hsu, S-P., Evans, W.B., Messenger, F.A. and Zsolnay, L.D. (2007) Controlled Access to Doors and Machines Using Fingerprint Matching, European Patent 0924655A2.
[4] Jain, A.K., Ross, A. and Prabhakar, S. (2004) 'An introduction to biometric recognition', IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image and Video-Based Biometrics, Vol. 14, No. 1, pp.160–170.
[5] Kumar, D. and Ryu, Y. (2009) 'A brief introduction of biometrics and fingerprint payment technology', International Journal of Advanced Science and Technology, Vol. 4, No. 1, pp.185–192.
[6] Kumar, D., Ryu, Y. and Kwon, D. (2008) 'A survey on biometric fingerprints: the cardless payment system', IEEE ISBAST, pp.1–6.
[7] Maes, S.H. and Beigi, H.S.M. (1998) 'Open sesame! Speech, password or key to secure your door?', Asian Conference on Computer Vision, Hong Kong, China, pp.531–541.
[8] Meenakshi N, Monish M, Dikshit KJ, Bharath S. Arduino Based Smart Fingerprint Authentication System (2019) 1st International Conference on Innovations in Information and Communication Technology (ICIICT) (pp. 1-7). IEEE.
[9] Baidya J, Saha T, Moyashir R, Palit R. (2017) Design and implementation of a fingerprint-based lock system for shared access. IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 1-6). IEEE.
[10] Anu, Bhatia D. (2014) A smart door access system using finger print biometric system. International Journal of Medical Engineering and Informatics; 6(3):274-80.