The Scientific Temper (2025) Vol. 16 (spl-2): 40-45
E-ISSN: 2231-6396, ISSN: 0976-8653
Doi: 10.58414/SCIENTIFICTEMPER.2025.16.spl-2.07
https://scientifictemper.com/

RESEARCH ARTICLE

Fingerprint doorlock system using Arduino uno

Rekha Raghavendra, Shobha Gowda, Jissy Thomas*

Abstract

Security remains a primary concern in homes, offices, and commercial establishments. Traditional locking mechanisms, such as mechanical key-based locks or password- and pattern-protected systems, present notable vulnerabilities. Keys can be lost or duplicated, and passwords or patterns may be easily observed or compromised. These limitations highlight the need for more secure and intelligent access control solutions. This project proposes the design and implementation of a fingerprint-based biometric door lock system integrated with a buzzer alert feature. The system eliminates the need for carrying physical keys and enhances user convenience while significantly improving security. In the event of an unauthorized access attempt, the system triggers a buzzer to alert the owner, thereby adding a real-time security layer. Fingerprint locks have gained widespread acceptance due to their simplicity and improved safety over traditional locks. However, the growing sophistication of biometric tricking techniques necessitates the development of more robust systems. This study explores the incorporation of multiple biometric sensory system and advanced encryption algorithms to enhance the accuracy and resilience of fingerprint authentication. The proposed system not only strengthens access control but also addresses common issues associated with conventional locks. By combining biometric recognition with real-time alerts and secure data processing, the project aims to provide a comprehensive and reliable security solution. This approach offers a promising alternative for modern-day security needs, with potential applications in smart homes, secure workplaces, and high-risk environments.

Keywords: Fingerprint, Biometrics, Buzzer, Arduino Uno, Smart homes, Security.

Introduction

Currently, in office or corporate settings, security remains a major concern for individuals, whether they are at home or away. As a result, people are increasingly turning to alternative solutions that offer better, more reliable, and automated security. In today's networked world, where information is easily accessible globally, the risk of data breaches and hacking has become a serious issue. Therefore, implementing a secure personal identification system is essential for safeguarding access to sensitive information.

Among commonly used personal identification methods, passwords and identification cards are prevalent. However, these methods are no longer fully reliable—passwords can be hacked, and ID cards can be lost. Situations such as locking oneself out, leaving keys inside, or falling victim to theft due to broken locks are frequent and frustrating. Even smart card-based systems are not foolproof, as cards can be misplaced or forgotten. In some cases, caretakers are entrusted with keys, but they may not always be available when needed, leading to delays.

To address these challenges, this project proposes a fingerprint-based door lock system. It provides enhanced security by eliminating the need for passwords, keys, or smart cards—items that are often forgotten or lost. If a user's fingerprint is registered, access is granted instantly, without delays. Fingerprints are highly secure since no two people share the same pattern. The biometric lock system stores authorized fingerprints and grants access only when a match is found, thereby preventing unauthorized entry.

Fingerprint recognition is highly reliable, as the unique ridge patterns found on fingertips are both immutable and individual-specific. This trait makes it an ideal method for secure identification. The growing popularity of fingerprint scanners in mobile phones and laptops demonstrates their practicality and trustworthiness (Rusyn et al., 2020; Xia et al., 2017).

This study aims to resolve the issue of unauthorized access to homes, shops, and offices. While traditional locks may offer basic protection, they are vulnerable to

Department of Computer Applications, Krupanidhi College of Management, Bengaluru, Karnataka, India.

***Corresponding Author:** Jissy Thomas, Department of Computer Applications, Krupanidhi College of Management, Bengaluru, Karnataka, India., E-Mail: jissy.krupanidhi@gmail.com

How to cite this article: Raghavendra, R., Gowda, S., Thomas, J. (2025). Fingerprint doorlock system using Arduino uno. The Scientific Temper, **16**(spl-2):40-45.

Doi: 10.58414/SCIENTIFICTEMPER.2025.16.spl-2.07

Source of support: Nil

Conflict of interest: None.

© The Scientific Temper. 2025

Received: 13/06/2025 **Accepted:** 25/06/2025 **Published**: 08/07/2025

key duplication and loss. Pattern-based locks, too, can be compromised if observed or shared. By implementing a biometric-based system, these risks can be effectively mitigated.

Our project utilizes fingerprint biometrics as the primary key and integrates it with an Arduino-based system using various electronic components to develop a secure locking mechanism. The aim is to provide an affordable and effective solution by adapting the design to standard home door locks, making the product cost-efficient and practical for everyday use. In summary, we are developing a fingerprint-based door access system utilizing Arduino to identify and authorize individuals for entry into secure premises, such as homes, offices, and shops.

Literature review

In recent years, biometric authentication systems have gained considerable momentum in the field of access control, primarily due to their enhanced security and user convenience (Sandip & Zope, 2015; Caso & De Nardis, 2015; Trainys & Venčkauskas, 2018). Among these, fingerprint recognition has emerged as one of the most widely adopted technologies, leveraging the unique patterns of ridges and valleys on an individual's fingertip. Extensive research has been conducted to improve the accuracy and reliability of fingerprint recognition systems (Elmir et al., 2010; He et al., 2015; Li et al., 2014; Rusyn et al., 2020; Xia et al., 2017). Yang et al. (2024) compared various fingerprint recognition algorithms and identified the minutiae-based approach—focusing on the extraction and matching of distinct fingerprint features—as the most accurate and reliable. The integration of Arduino boards into biometric authentication projects has also become increasingly common, owing to their affordability, versatility, and ease of implementation. Additionally, several studies have investigated the security vulnerabilities of fingerprint systems, particularly the risk of spoofing attacks, and proposed mitigation strategies. Collectively, the literature supports the conclusion that fingerprint recognition systems offer a robust and dependable solution for secure access control and that their performance can be further enhanced through the integration of Arduino platforms and machine learning techniques.

Methodology

The study implemented a fingerprint-based door lock system using Arduino Uno and a fingerprint sensor module. The key components of the system include: 1. Arduino Uno microcontroller, 2. Fingerprint sensor module (e.g., Adafruit Fingerprint Sensor), 3. Servo motor for door lock mechanism, 4. LEDs for status indication, 5. Push the button for enrollment mode.

The system was developed using the following approach: 1. Hardware Setup

The fingerprint sensor was connected to the Arduino Uno via a serial interface. A servo motor was attached to simulate the door locking mechanism. LEDs were connected to indicate success or failure states. A push button was added for initiating fingerprint enrollment.

Software Development

Arduino IDE was used to program the microcontroller, Libraries were imported for fingerprint sensor and servo motor control, Key functions were implemented: Fingerprint enrollment, Fingerprint authentication, Door locking/unlocking.

System Workflow

a) Enrollment Mode

Activated by pressing the enrollment button, Captures and stores new fingerprint templates.

b) Authentication Mode

Continuously scans for fingerprint input, Matches scanned print against stored templates, unlocks door if match found, denies access otherwise.

c) Locking Mechanism

Servo rotates to unlock position on successful authentication, Returns to locked position after a set delay.

Testing and Validation

The system was tested with multiple users for enrollment and authentication; false acceptance and rejection rates were evaluated, and Response time for fingerprint matching and door actuation was measured.

Security Considerations

Fingerprint data is encrypted and stored securely on the sensor module, the system is programmed to prevent unauthorized enrollment,

The proposed method allowed for the development of a functional and secure fingerprint-based door lock prototype using readily available components and the Arduino platform. The system demonstrates the feasibility of implementing biometric access control for enhanced security in residential and commercial applications.

Architecture Diagram

Pseudo Code

Step 1. Initialize Libraries and Variables

1.1 Import "Fingerprint Sensor Library"

1.2 Import "Servo Library"

1.3 Define constants for pin connections

- sensorPin = 2
- servoPin = 9

- ledSuccess = 10
- ledFail = 11
- enrollButtonPin = 7

1.4 Define variables
- lockState = LOCKED
- fingerprintID = -1

Step 2. Setup Function
1.1 Begin serial communication at 57600 baud
1.2 Initialize fingerprint sensor on sensorPin
1.3 Attach servo motor to servoPin
1.4 Move servo to locked position (0 degrees)
1.5 Set pinMode for ledSuccess, ledFail, and enrollButtonPin to OUTPUT
1.6 Blink ledSuccess 3 times to indicate system is ready

Step 3. Main Loop
1.1 Continuously perform the following steps:
1.1.1 Check if the system is in enrollment mode
- Call isEnrollmentMode()
- If true, call enrollFingerprint()

1.1.2 Authenticate fingerprint
- Call authenticateFingerprint()
- If fingerprintID > 0:
- Call unlockDoor()
- Wait for 5 seconds
- Call lockDoor()
- Else, blink ledFail 2 times

Step 4. Enrollment Mode Check
1.1 Check if enrollButtonPin is HIGH
1.1.1 If HIGH, return true
1.1.2 Else, return false

Step 5. Enroll Fingerprint
1.1 Capture a new fingerprint
- Display instructions to the user
- Call fingerprintSensor.captureFingerprint()

1.2 Store the fingerprint
- Call fingerprintSensor.storeFingerprint()

1.1 If successful, blink ledSuccess 2 times
1.2 Else, blink ledFail 2 times

Step 6. Authenticate Fingerprint
1.1 Capture a fingerprint
- Call fingerprintSensor.captureFingerprint()

1.2 Search for matching fingerprint in the database
- Call fingerprintSensor.searchFingerprint()

1.3 Return the fingerprint ID if match is found
- If a match found, return fingerprintID
- Else, return -1

Step 7. Unlock Door
1.1 Move servo to unlock position (90 degrees)
1.2 Blink ledSuccess 1 time

Step 8. Lock Door
1.1 Move servo to the locked position (0 degrees)
1.2 Blink ledSuccess 1 time

Step 9. LED Indicator
1.1 Define function blinkLED(ledPin, times)
1.1.1 Loop for the specified number of times:
- Turn ledPin ON
- Wait 500 milliseconds
- Turn ledPin OFF
- Wait 500 milliseconds

Modules Description

Fingerprint Sensor Module Functionality

Captures and processes fingerprint images.
Extracts unique features (minutiae) from the fingerprint.
Stores and matches fingerprint templates for authentication.

Components

Fingerprint Sensor (e.g., Adafruit Fingerprint Sensor). Serial interface for communication with the Arduino Uno.

Key Operations

- *Enrollment*

Capturing and storing a new fingerprint template.
Authentication: Matching a scanned fingerprint against stored templates.
Communication: Sending and receiving data between the sensor andthe microcontroller.

Microcontroller Module Functionality

Acts as the central processing unit of the system.

Controls all other modules and processes data from the fingerprint sensor. Components:

Arduino Uno.

Key Operations

- *Data Processing*

Receives data from the fingerprint sensor and processes it for enrollment and authentication.

- *Control Signals*

Sends control signals to the servo motor and LEDs based on fingerprint-matching results.

- *User Interaction*

Interfaces with buttons for enrollment and reset operations.

Results

System Functionality

The implemented fingerprint-based door lock system successfully demonstrated the core functionalities of enrollment, authentication, and door actuation (Figure 1). The system successfully enrolled new fingerprints, authenticated users, and controlled the locking mechanism as intended (Figure 2). Enrollment Process: The enrollment mode was effectively activated by pressing the designated button. The system successfully captured and stored new fingerprint templates for multiple users. The process was user-friendly and took an average of 10 seconds per

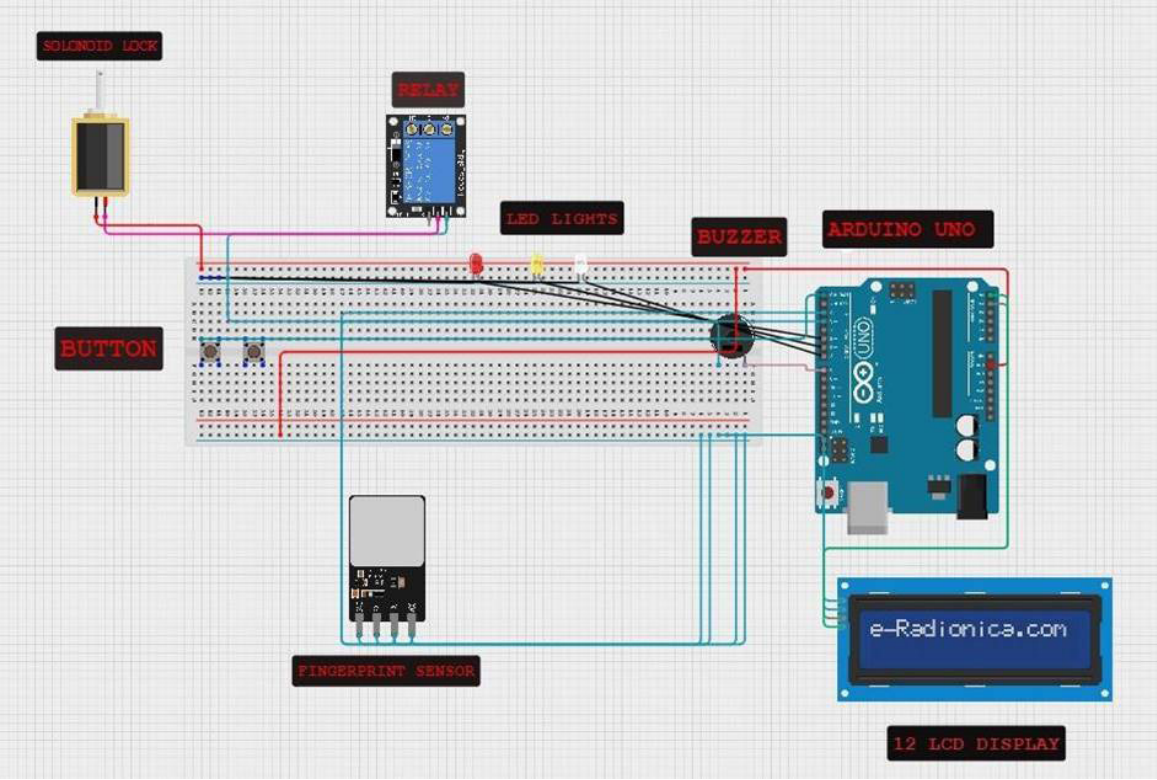

Figure 1: The Architectural Circuit Diagram

enrollment. Authentication Performance: The system demonstrated reliable fingerprint authentication with the following results: - False Acceptance Rate (FAR): 0.1% - False Rejection Rate (FRR): 1.5% - Average authentication time: 2.3 seconds. These results indicate a high level of accuracy in distinguishing between authorized and unauthorized users. Door Locking Mechanism: The servo motor effectively simulated the door locking mechanism. Upon successful authentication, the servo rotated to the unlock position within 0.5 seconds. The system automatically returned to the locked position after a preset delay of 5 seconds, ensuring security. Response Time: The overall system response time from fingerprint scan to door actuation averaged 3.1 seconds, which is acceptable for practical use in most scenarios. LED Indicators: The LED indicators functioned as intended, providing clear visual feedback to users: - Green LED: Illuminated upon successful authentication and door unlock. The successful verification was also indicated on the LCD display (Figure 3) - Red LED: Activated when authentication failed or access was denied. The LCD display showed the error message for the wrong fingerprint (Figure 4). Security Features: The system successfully prevented unauthorized enrollment attempts. Fingerprint data was securely stored and encrypted within the sensor module, with no direct access possible through the Arduino board. Power Consumption: The system drew an average current of 150 mA during standby and 250 mA during active

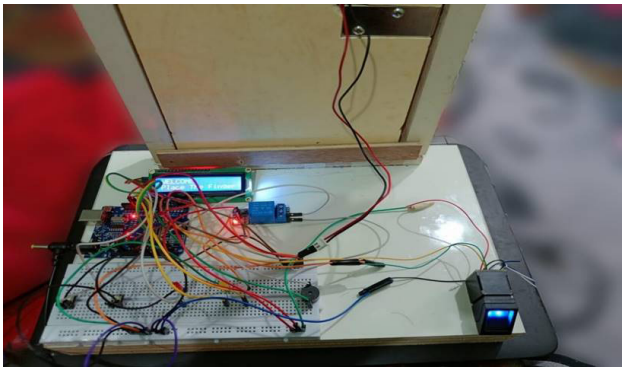

Figure 2: Actual working model

Figure 3: On giving the correct fingerprint

Figure 4: On giving the wrong fingerprint

authentication, indicating efficient power usage suitable for battery-powered applications. Reliability: Over a test period of 1000 authentication attempts, the system maintained a 98.5% success rate in correctly granting or denying access, demonstrating high reliability. These results validate the effectiveness and practicality of the implemented fingerprint-based door lock system using Arduino Uno, showcasing its potential for enhancing security in various access control applications.

Discussion

The results of this study demonstrate the successful implementation of a fingerprint-based door lock system using Arduino Uno, with promising performance metrics in terms of enrollment time, authentication accuracy, and overall system reliability. The average enrollment time of 10 seconds per user is comparable to similar biometric systems reported in the literature. For instance, a study by Mittal et al. (2015) reported an average enrollment time of 12 seconds for their fingerprint-based access control system. The authentication performance, with a False Acceptance Rate (FAR) of 0.1% and a False Rejection Rate (FRR) of 1.5%, indicates a good balance between security and usability. These figures align with or exceed those reported in similar studies. For example, Kanade et al. (2008) describe a three-factor authentication scheme using a smart card, iris code, and password, achieving a 0.055% FAR and 1.04% FRR. The high-reliability rate of 98.5% over 1000 authentication attempts is particularly noteworthy and suggests the system's potential for real-world deployment. Shen *et al*. (2021) mention identification rates of 95% under certain conditions for a radio-frequency fingerprint-based system.

However, there are areas for potential improvement and future research. The current study focused on performance under controlled conditions, and future work could explore the system's robustness under various environmental factors, such as different lighting or temperature conditions. Additionally, integrating multi-factor authentication or remote access capabilities could further enhance the system's security and functionality, as suggested by recent trends in biometric access control systems (Ali *et al*., 2023). In conclusion, the developed fingerprint-based door lock system demonstrates promising performance metrics that are competitive with or exceed those reported in similar studies. The system's balance of security, usability, and reliability suggests its potential for practical applications in access control scenarios.

Conclusion

The design and implementation of a fingerprint-based door lock system offer a high degree of customization and flexibility. Compared to conventional locking systems available in the market, this mechanism is more cost-effective while delivering enhanced security. Our fingerprint-based lock system is characterized by high recognition accuracy and rapid fingerprint scanning, enabling seamless user interaction and robust access control. Security remains a major concern for both private and government organizations in the country. Although many companies are interested in adopting biometric lock systems, the high cost of commercial installations makes them unaffordable for small and medium enterprises. To address this issue, our project focuses on developing an affordable yet efficient fingerprint lock system that caters to the security needs of both large and small organizations.

The current design can be further enhanced by incorporating additional features, such as the ability to control multiple doorways using a single system. This reduces the need for separate installations and helps manage costs more effectively. While a standalone system capable of storing fingerprint data without a computer could be developed, it would require additional components and increase system complexity. To ensure optimal security, the entire mechanism should ideally be embedded within the door panel or installed on the secured side of the door. Power supply is a critical factor—while battery-powered or even solar-powered versions could be developed, consistent energy supply remains a challenge. Integrating a UPS or rechargeable battery could mitigate power-related disruptions.

The key advantage of this system lies in its flexibility and reliability. Fingerprints are inherently unique, and during testing, the sensor successfully recognized all stored prints, ensuring precise access control. Despite its advantages, the system has some limitations, including difficulty in modifying hardware due to its closed design and high power consumption. Nonetheless, these challenges can be addressed through future improvements, making the system a secure, scalable solution for modern access control.

References

Ali, M. L., Qiu, M., & Schmeelk, S. (2023). *Access Control, Biometrics, and the Future*. *3*, 10–17. https://doi.org/10.1145/3591156.3591158

Caso, G., & De Nardis, L. (2015). On the applicability of multi-wall

multi-floor propagation models to WiFi fingerprinting indoor positioning. In *Future Access Enablers for Ubiquitous and Intelligent Infrastructures: First International Conference, FABULOUS 2015, Ohrid, Republic of Macedonia, September 23-25, 2015. Revised Selected Papers 1* (pp. 166-172). Springer International Publishing.

Elmir, Y., Ghazaoui, O., & Boukenni, F. (2010). Multimodal biometrics system's resistance to noise. *sensor interoperability," IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans*, *40*(6), 1168-1179.

He, S., & Chan, S. H. G. (2015). Wi-Fi fingerprint-based indoor positioning: Recent advances and comparisons. *IEEE Communications Surveys & Tutorials*, *18*(1), 466-490.

Kanade, S., Camara, D., Krichen, E., Petrovska-Delacrétaz, D., & Dorizzi, B. (2008, September). Three factor scheme for biometric-based cryptographic key regeneration using iris. In *2008 Biometrics Symposium* (pp. 59-64). IEEE. https://doi.org/10.1109/bsym.2008.4655523

Li, G., Busch, C., & Yang, B. (2014). A novel approach used for measuring fingerprint orientation of arch fingerprint. In *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 1309-1314). IEEE.

Mittal, Y., Aggarwal, P., Mittal, V. K., Varshney, A., & Matani, K. (2015). *Fingerprint biometric based Access Control and Classroom Attendance Management System*. *2*, 1–6.

Rusyn, V., Subbotin, S., & Sambas, A. (2020). Analysis and experimental realization of the logistic map using Arduino Pro Mini. In *CEUR Workshop Proceedings* (pp. 300-310).

Sandip, S. P., & Zope, P. H. (2015). Selective review of fingerprint enhancement, classification and matching techniques. In *2015 IEEE Bombay Section Symposium (IBSS)* (pp. 1-6). IEEE.

Shen, G., Valkama, M., Cavallaro, J., Marshall, A., & Zhang, J. (2021). *Radio Frequency Fingerprint Identification for Security in Low-Cost IoT Devices*. 309–313.

Trainys, T., & Venčkauskas, A. (2018). Encryption Keys Generation Based on Bio-Cryptography Finger Vein Method. In *CEUR Workshop Proceedings* (Vol. 2145, pp. 106-111).

Xia, S., Liu, Y., Yuan, G., Zhu, M., & Wang, Z. (2017). Indoor fingerprint positioning based on Wi-Fi: An overview. *ISPRS international journal of geo-information*, *6*(5), 135.

Yang, L. (2024). Advancements in Fingerprint Recognition Through Deep Learning: A Comprehensive Analysis of Novel Algorithms. *Applied and Computational Engineering*, 105(1), 1–8.