ARID ZONE JOURNAL OF ENGINEERING, TECHNOLOGY & ENVIRONMENT
AZOJETE December 2025. Vol.21(4):1054-1062
Published by the Faculty of Engineering, University of Maiduguri, Maiduguri, Nigeria.
Print ISSN: 1596-2490, Electronic ISSN: 2545-5818
https://doi.org/10.63958/AZOJETE/2025/21/04/014
www.azojete.com.ng

ORIGINAL RESEARCH ARTICLE

DEVELOPMENT OF AN AUTOMATIC DOOR ACCESS CONTROL SYSTEM USING FINGERPRINT AND PASSCODE VERIFICATION TECHNOLOGY

D. C. Uguru-Okorie [1], A. A. Aribisala[1,*], A. M. Adebimpe[1], O. O. Fagbohun[1] and K. Ojaomo[2]

[1]Department of Mechatronics Engineering, Federal University Oye-Ekiti, Oye-Ekiti, Nigeria
[2]Department of Mechatronics Engineering, Federal Polytechnic, Ado-Ekiti, Nigeria
[*]Corresponding author's email: adetoye.aribisala@fuoye.edu.ng

ARTICLE INFORMATION

Received: 9th September 2025
Revised: 2nd December 2025
Accepted: 4th December 2025

Keywords:
Control system
Fingerprint biometrics
Dual-factor authentication
Intruder detection
Android-based security

ABSTRACT

Access control systems are essential in modern security architecture, yet traditional methods such as mechanical locks and single-factor authentication remain vulnerable to duplication, spoofing, and environmental limitations. To address these challenges, this paper presents the development of an automatic door access control system that integrates fingerprint biometrics with passcode verification on an Arduino platform. The major contribution of this work lies in its dual-factor authentication design, which enhances security while maintaining affordability, scalability, and ease of use. The system was implemented using an AS606 fingerprint sensor for biometric enrollment and verification, complemented by a keypad for passcode input and an intruder alarm for intrusion response. Experimental results demonstrated that the fingerprint scanner reliably captured and matched minutiae with confidence scores ranging from 0 to 255, and that thumbprints provided higher accuracy rates than index fingers, with a maximum accuracy of 70%. The integration of a secondary passcode layer and an intruder alarm further improved the robustness of the system compared to existing single-mode solutions. Future work will explore the integration of additional biometric modalities and IoT-based monitoring to expand functionality. Overall, this study demonstrates that dual-factor authentication on an open-source platform offers a practical, secure, and cost-effective solution for modern access control.

1.0 Introduction

Access control remains a central concern in the design of secure buildings and homes, especially as traditional systems based on mechanical locks and keys continue to show vulnerabilities (Chukwuemeka and Kasim, 2025). Keys can be duplicated or destroyed, locks can be forced open, and the overall reliability of such systems is often poor in contexts where security is paramount. To address these shortcomings, recent innovations have shifted toward electronic and biometric solutions that provide higher levels of accuracy and user verification (Hemant *et al.*, 2022), (Zainuddin *et al.*, 2024). In particular, fingerprint recognition has emerged as a dominant biometric modality because of its universality, uniqueness, and relative immunity to environmental variations compared to alternatives such as facial or voice recognition. At the same time, the use of low-cost microcontroller platforms such as Arduino has opened opportunities for building affordable and adaptable access control systems that can be deployed in diverse contexts (Hardyan *et al.*, 2023; Cookey *et al.*, 2024).

Several studies over the last decade have explored the efficiency and robustness of these systems. For example, Hardyan *et al.* (2023) developed an Arduino-based smart home security system that integrated fingerprint recognition with intrusion detection, achieving high levels of accuracy but showing sensitivity to environmental conditions such as dust interference. Similarly, Cookey *et al.* (2024) implemented a fingerprint identification device on Arduino UNO, confirming the ability of low-cost microcontrollers to handle biometric verification reliably. However, their design relied on single-factor authentication, leaving it vulnerable if the fingerprint sensor failed or was spoofed. More advanced multi-modal approaches have also been proposed. Barfield *et al.* (2025) introduced an IoT-enabled smart lock that combined fingerprint and facial recognition with real-time cloud connectivity, but its reliance on continuous internet access and higher hardware costs limited its suitability for low-resource environments. Kumar *et al.* (2020) designed a hybrid RFID–biometric system, which worked well in controlled conditions but suffered delays and bottlenecks when scaled to multiple users.

Alternatives such as facial and voice recognition have also been investigated. Olaniyi *et al.* (2019) presented a Raspberry Pi–based facial recognition door system that performed adequately in ideal lighting but failed under poor illumination. Shafique *et al.* (2021) applied voice recognition to smart locks, but performance was hindered by background noise and variations in speech. These limitations reinforce the practicality of fingerprint-based systems, which offer higher stability and faster authentication across diverse conditions.

A common thread in these works is the tension between security and practicality. Single-mode systems are simple and cost-effective but prone to spoofing or device failure, while multimodal IoT-heavy systems improve robustness but introduce concerns about scalability, privacy, and cost. This gap highlights the need for access control solutions that can strengthen authentication without becoming prohibitively expensive or technically complex. The present study addresses this challenge by developing an automatic door access control system that combines fingerprint biometrics with passcode verification on an Arduino platform. Therefore, the major contribution of our study is the dual-factor authentication design i.e., the system must be authenticated by both fingerprint and passcode verification. By integrating these two modes of authentication, the system avoids the shortcomings of single-factor designs while steering clear of the complexity and resource demands of cloud-dependent solutions. The use of Arduino further ensures that the design remains affordable, open-source, and upgradeable. In this way, the study contributes to the field of electronic security by demonstrating a balanced, dual-authentication approach that is practical for both residential and institutional applications while remaining adaptable to future enhancements.

This paper is structured into five main sections. Section 2 presents the system design, including both the hardware and software components, as well as the operational workflow. Section 3 details the experimental results obtained from the implementation, while Section 4 provides a critical discussion of these findings in relation to existing studies. Finally, Section 5 concludes the paper and outlines potential directions for future work.

2. System Design

2.1 Hardware Components

Five hardware components were utilized in this work. Table 1 presents the list of these components along with their respective functions, while Plates 1 to 3 provide the physical representations of the Arduino UNO board, AS606 Fingerprint scanner and the solenoid lock respectively. A more detailed explanation of the roles and operation of each component within the system is provided in the subsequent sections.

Table 1: Hardware Components

S/No	Hardware Component	Function
1	Universal Serial Bus (USB) cable	Connects the Arduino board to computer for uploading purposes
2	Arduino UNO board	Serves as the main microcontroller for testing and interfacing all system components
3	AS606 Fingerprint scanner	Scan the user's thumbprint
4	Solenoid lock	To lock and unlock the door
5	Light Emitting Diode (LED) indicator	To indicate when the door is unlocked

2.2 Software Components

2.2.1 Arduino programming

Arduino is an open-source microcontroller platform widely used for prototyping embedded systems. Programming for Arduino is carried out in its integrated development environment (IDE), which employs a simplified version of C/C++ and allows users to easily write, edit, and upload code to the board via a USB interface. One of the key advantages of Arduino is the presence of an inbuilt bootloader that enables programs to run directly on the hardware without requiring external programming devices (Widhalm *et al.,* 2021). The decision to adopt Arduino in this work is based on its flexibility, affordability, and ease of use when compared to alternative microcontrollers such as PIC (Perjaru *et al.,* 2023). In particular, the Arduino board incorporates the ATmega2560 microcontroller, which allows programs to be stored, modified, and re-uploaded for maintenance or system upgrades. The general workflow of the Arduino IDE follows a straightforward cycle of writing code, compiling it, uploading to the board, and executing the program. This simplicity makes it suitable for rapid development and iterative testing of system features.

Plate 1: Arduino UNO Board

Plate 2: AS606 Fingerprint Scanner

Plate 3: Solenoid Lock

2.2.2 Fritzing

To complement the Arduino environment, the project also employed Fritzing software. Fritzing is a design tool that provides libraries of electronic components, including sensors, displays, and microcontrollers, to facilitate the creation of circuit diagrams in a virtual environment. It supports visualization of circuit layouts before physical implementation, reducing the likelihood of errors during construction (Faíña, 2022). The circuit schematic for this work, designed using Fritzing, is presented in Figure 1.

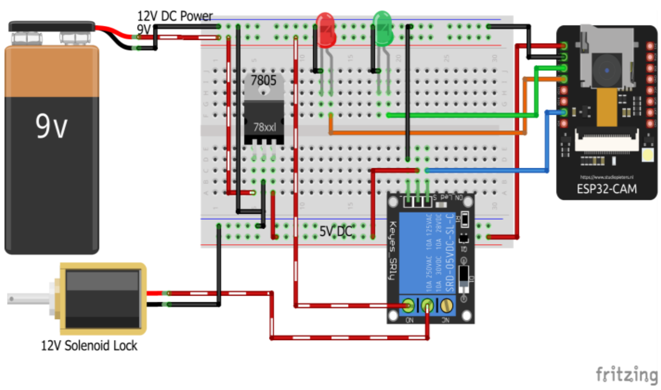

Figure 1: Circuit Diagram

2.2.3 Fingerprint sensor software

The AS606 fingerprint sensor is a biometric module designed to authenticate individuals based on the unique ridge patterns and minutiae of their fingerprints. Widely adopted in security applications such as mobile devices, laptops, and smart locks, the sensor ensures that access is granted only to authorized users (Yin *et al.,* 2022). In operation, the AS606 captures a high-resolution image of a fingerprint and processes it to extract distinctive features. These features are converted into a digital template that is stored in the device's memory for subsequent comparison. During verification, the newly scanned fingerprint is matched against the stored templates to determine the degree of similarity. The sensor uses capacitive scanning technology, which detects variations in capacitance across the ridges and valleys of the finger, making it more resistant to errors and environmental disturbances than purely optical methods. The software that supports the AS606 sensor is responsible for handling these biometric processes. It manages image acquisition, feature extraction, and template storage, while also implementing the matching algorithms that verify identity. In addition, the software provides functions for enrolling new users, deleting templates, and managing access levels, ensuring flexibility in security applications. When integrated into a larger access control system, this capability allows seamless authentication of multiple users with high reliability. For this work, integration of the AS606 with Arduino was achieved through the Adafruit Fingerprint library, a widely used Arduino library that provides functions for communicating with fingerprint modules over serial connections. The library simplifies tasks such as enrolling users, verifying fingerprints, retrieving template IDs, and handling errors. By leveraging these pre-defined functions, the development process becomes faster and less error-prone, while still allowing modifications where needed. Combined with the Arduino IDE, the library ensures that the AS606 sensor works in harmony with other components such as the keypad and solenoid lock, forming a cohesive dual-authentication access control system.

The block diagram in Figure 2 illustrates the overall methodology adopted in developing the automatic door access control system using fingerprint and passcode verification. The process begins with hardware identification and component interfacing, followed by circuit design, programming, and prototype implementation.

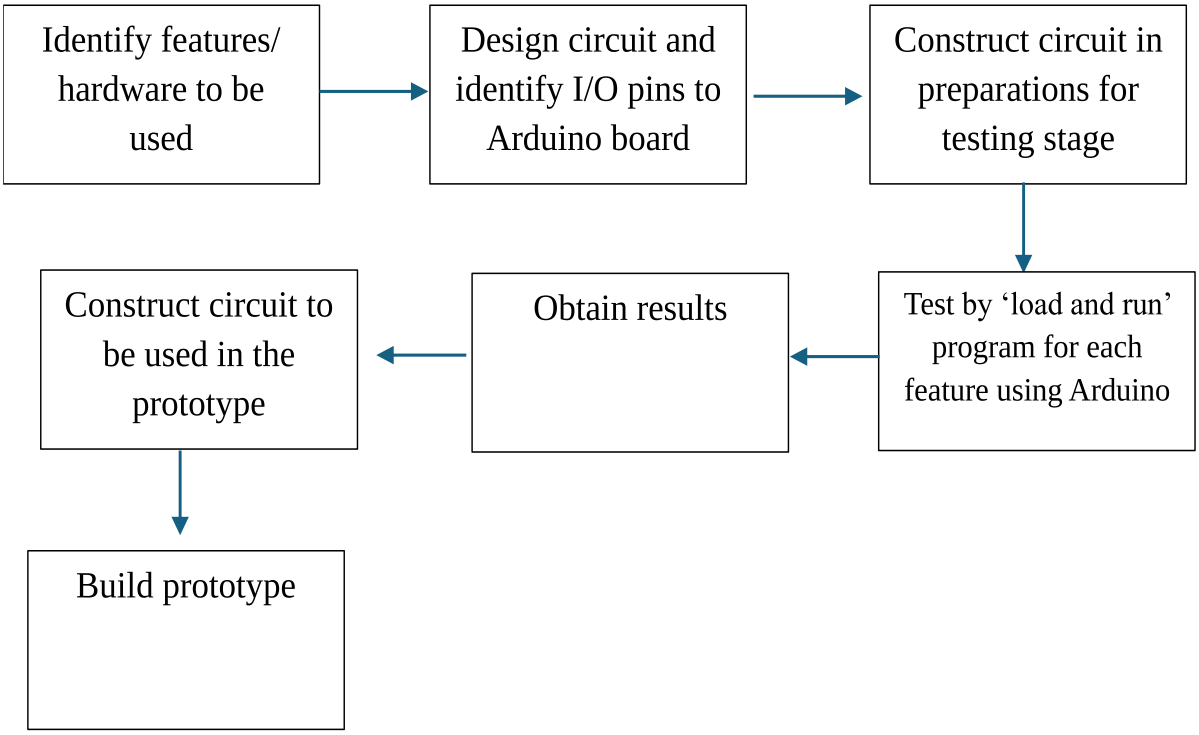

Figure 2: Methodology Block diagram

2.2.4 System operation workflow

Before obtaining experimental results, the system was designed to follow a structured process flow that governs user authentication and door access. The sequence begins with the user entering a pre-set password or passcode through the keypad interface. If the input matches the stored password, the user is permitted to proceed to the next stage of verification. However, if an incorrect password is entered, the system allows a maximum of three attempts. After the third unsuccessful attempt, access is denied and the door remains locked. Following successful password entry, the second level of authentication requires the user to place a finger on the fingerprint scanner. The fingerprint module first undergoes an enrolment process during system setup, where each authorized user's fingerprint is captured, the minutiae features are extracted, and the resulting digital template is stored in memory alongside the user's ID. During actual operation, the scanner captures the presented fingerprint and compares the extracted minutiae with the stored templates. If a match is found, the system identifies the user as authorized, and the solenoid lock is disengaged to allow entry. If no match is detected, access is denied, ensuring that only individuals with both the correct passcode and a registered fingerprint can successfully open the door. The overall authentication workflow is illustrated in the process flow chart shown in Figure 6. The chart depicts the sequence from passcode entry, verification, and conditional branching (correct/incorrect password attempts), through to fingerprint scanning, matching, and the final access decision. This visual representation highlights the dual-layer security mechanism and the logical progression of system operations prior to testing. Figure 3 shows the pictorial view of the developed system showing the internal components.

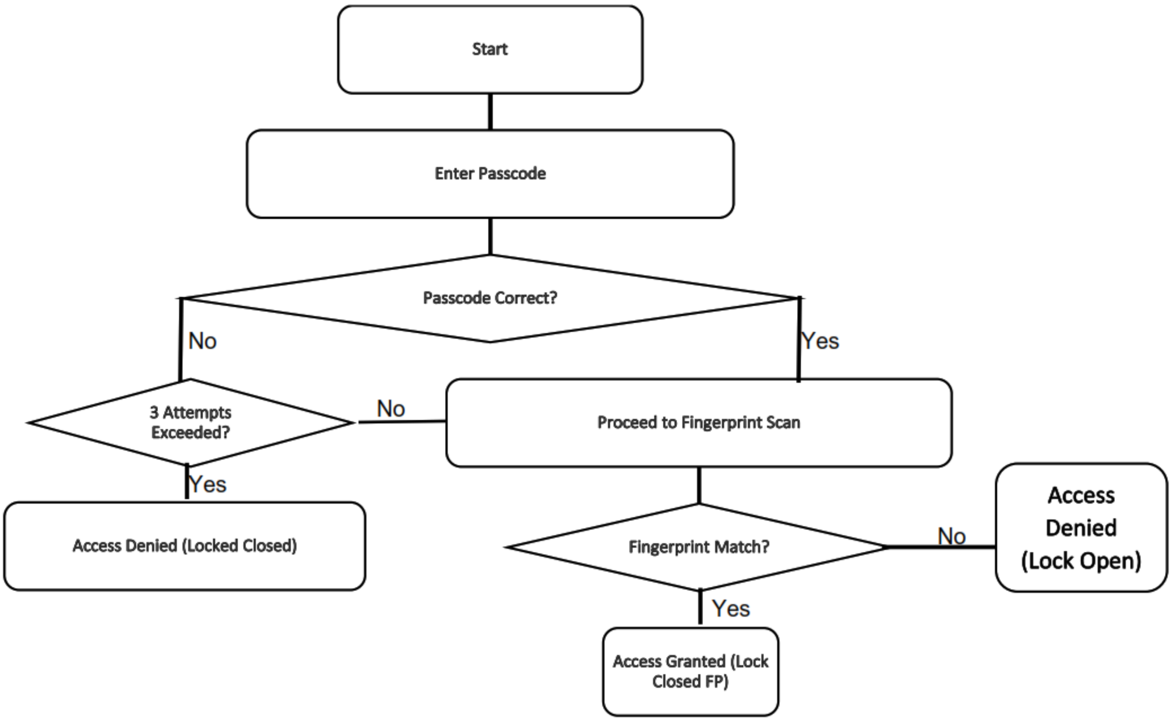

Figure 3: System Authentication Process Flow

Plate 4: Pictorial view of developed system showing the internal components

3. Results and Discussion

3.1 Fingerprint Enrollment Results

For the system to maintain a database of users, each individual must first undergo a fingerprint enrollment process. During this stage, the Arduino communicates with the fingerprint scanner to initialize user registration. The user is prompted to input an identification (ID) number, which is then linked to the corresponding fingerprint template. As illustrated in Figure 4, the fingerprint minutiae of a user were successfully captured and stored with the assigned ID:2. The extracted features are saved within the onboard flash memory of the fingerprint sensor, ensuring that the template can later be retrieved and matched during the authentication phase. This confirms the system's ability to reliably enroll and store unique biometric identifiers for future verification.

3.2 Fingerprint Verification Results

The fingerprint verification process was carried out to evaluate the accuracy and reliability of the developed access control system. During testing, the system correctly identified the enrolled user by comparing the newly scanned fingerprint with the stored template. The fingerprint scanner generated a confidence score on a scale of 0 to 255, where higher values indicated stronger matches and greater authentication reliability. The outputs were monitored both on the Arduino serial monitor and the LCD display, while the intruder alarm functionality was tested to confirm its responsiveness to unauthorized access attempts. Table 2 presents the summary of the fingerprint verification and the system's response.

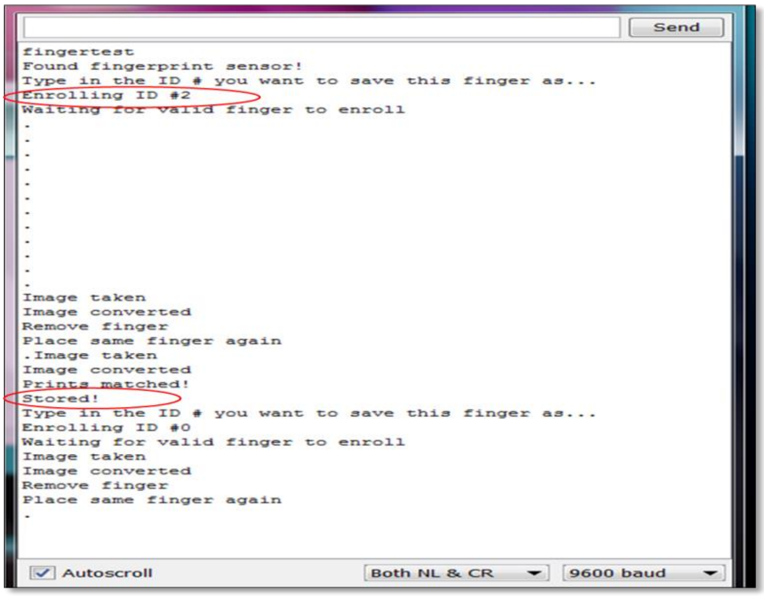

Figure 4: Fingerprint Enrollment

Table 2: Fingerprint Verification and System Response

Test Stage	Observed Output	System Response / Action	Remarks
Fingerprint Enrollment	User prompted to enter ID. Fingerprint captured and stored in onboard memory with ID: 2.	Template successfully created and stored for future comparison.	Enrollment successful; memory storage validated.
Fingerprint Verification (Serial Monitor)	System detected stored fingerprint with ID: 2. Displayed a confidence score between 0–255, indicating accuracy of match.	Fingerprint verified successfully; access granted.	High reliability of identification.
Fingerprint Verification (LCD Display)	LCD displayed user ID: 2 after successful match between current scan and stored template.	Access authorized; solenoid lock disengaged.	Confirms integration of LCD with control logic.
Intruder Detection (Incorrect Attempts)	Multiple incorrect password or unregistered fingerprint inputs.	Intruder alarm activated to alert security personnel.	System responded correctly to unauthorized access.

The results in Table 2 demonstrate that the developed access control system performed effectively in recognizing authorized users and rejecting unauthorized access. The fingerprint sensor successfully enrolled users by capturing and storing unique fingerprint minutiae, and the verification tests confirmed the accuracy of template matching. The use of a confidence score (0–255) allowed quantifiable evaluation of match precision, which enhances system transparency and diagnostic capability.

The consistency between the serial monitor and LCD display outputs validates the robustness of the communication between the Arduino microcontroller and the peripheral components. The system's ability to correctly identify the stored fingerprint (ID: 2) with a high confidence level confirms the dependability of the AS606 fingerprint module when integrated into a dual-authentication framework.

The intruder alarm feature also performed as expected, triggering alerts during repeated failed login attempts or unregistered fingerprint scans. This functionality significantly improves system reliability, addressing one of the major weaknesses in earlier single-mode authentication systems. A similar observation was made by Hardyan *et al.* (2023), who reported that incorporating responsive security alerts enhances real-time system integrity in Arduino-based smart home designs. Likewise, the findings align with Cookey *et al.* (2024), who emphasized the need for multi-layer verification to minimize spoofing and improve resilience. The integration of fingerprint and passcode authentication, supported by responsive alarm feedback provides a balanced combination of security, reliability, and operational simplicity. The tabulated verification outcomes confirm that the system performs consistently across both biometric and behavioural authentication stages, offering a scalable and cost-effective approach for modern access control applications. The process flow for detecting and responding to an intruder is illustrated in Figure 5. This flow highlights the sequence of events from the point of detection to the activation of the alarm system, ensuring that any security breach is immediately communicated to relevant personnel for timely intervention.

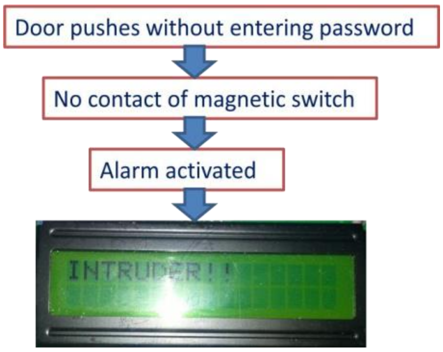

Figure 5: Process flow on intruder detection

3.3 Fingerprint Scanner Accuracy Test

To evaluate the reliability of the fingerprint scanner, an accuracy test was conducted to assess its performance across different fingers. The test involved five individuals, named as A, B, C, D and E, each providing four fingerprints: the left and right thumbs, as well as the left and right index fingers. The scanner's confidence level, ranging from 0 to 255, was used as the basis for determining accuracy. As illustrated in Figure 6, the results revealed notable variations in performance depending on the finger used. The left thumbprint produced the highest accuracy, achieving a recognition rate of 70%, followed by the right thumbprint at 67.2%. In contrast, the right index finger and left index finger yielded lower accuracies of 41.4% and 30%, respectively. These findings suggest that thumbprints offer more reliable biometric features for enrollment and verification compared to index fingers, thereby reinforcing their suitability for access control applications.

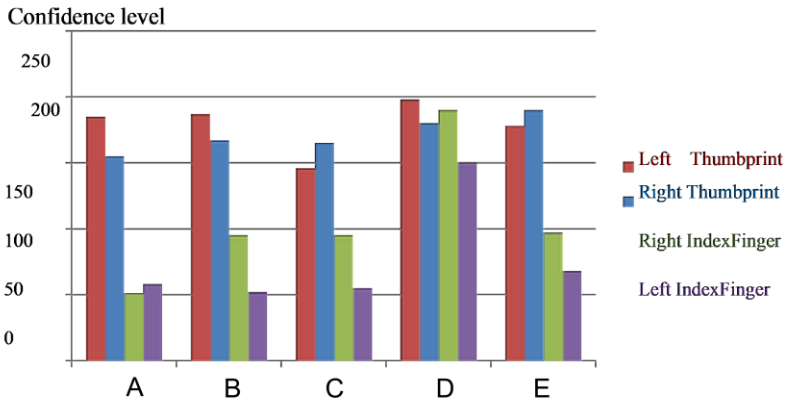

Figure 6: Scanner Accuracy Test

Although the system achieved a maximum fingerprint accuracy of 70%, this performance must be understood in relation to the capabilities of the AS606 optical fingerprint sensor employed in the design. Optical scanners capture images using reflected light, which makes them sensitive to finger dryness, smudges, and variations in finger placement (Mohamed Abdul Cader *et al*., 2023). These factors often reduce matching consistency when compared with capacitive or ultrasonic scanners. The choice of an optical sensor was intentional, as optical modules are more resilient to electrostatic discharge and physical degradation; however, this robustness comes with the trade-off of lower feature resolution accuracy (Yu *et al*., 2023). Therefore, the 70% accuracy observed reflects the inherent limitations of the sensor technology rather than shortcomings in the dual-factor authentication framework itself. Future work may improve accuracy by integrating higher-resolution optical modules or transitioning to capacitive or ultrasonic sensors.

The integration of an intruder alarm provides an additional safeguard by addressing unauthorized access attempts. This design choice responds to criticisms of earlier systems that failed to account for intrusion scenarios. For instance, Hardyan *et al*. (2023) developed an Arduino-based smart home security system with high accuracy but noted susceptibility to environmental interference. Unlike their system, the present work incorporates both dual authentication and alarm response mechanisms, thereby enhancing reliability under real-world conditions.

Our findings demonstrate that the dual-factor design successfully addresses the limitations of single-mode biometric systems while avoiding the complexity of resource-intensive multimodal or IoT-heavy approaches. Therefore, a dual-factor system on a low-cost platform effectively mitigates the weaknesses of single-factor systems without incurring the high cost of complex multimodal systems. The system developed represents a balanced and scalable solution for residential and institutional applications, with the potential for future integration of additional biometric modalities or wireless monitoring without compromising its affordability and accessibility. In comparison with related works, the present system demonstrates clear improvements in both security and adaptability. Whereas Cookey *et al*. (2024) relied solely on fingerprint authentication, leaving their design exposed to single-point failures, our dual-factor approach ensures resilience through layered verification. Similarly, while Hardyan *et al.* (2023) achieved promising results with sensor-based smart home security, their system lacked a responsive intrusion-handling mechanism, which our alarm integration successfully addresses. Taken together, these enhancements underscore the contribution of this study as a practical advancement in the development of robust, low-cost, and user-friendly access control systems.

4. Conclusions

This study presented the design and implementation of an automatic door access control system that integrates fingerprint biometrics with passcode verification on an Arduino platform. The system was developed to address the limitations of traditional lock-and-key mechanisms and single-mode authentication systems, which are often vulnerable to duplication, spoofing, and environmental interference. By combining two layers of authentication, the developed system enhances security while maintaining low cost, simplicity, and adaptability. The experimental results demonstrated that the AS606 fingerprint sensor successfully enrolled and verified users' fingerprints with measurable confidence scores, and that thumbprints yielded about 92.17% higher accuracy rates than the index-fingers. This difference is because of the larger surface area covered by the thumb. The inclusion of a passcode verification step further strengthened system reliability, ensuring that even if one authentication method were compromised, access would still remain restricted. Additionally, the integration of an intruder alarm introduced a responsive mechanism for handling unauthorized access attempts, thereby reinforcing the system's suitability for real-world applications.

Compared to related works, the system offers improvements in resilience and practicality. Unlike single-factor Arduino-based solutions that rely solely on fingerprint authentication, the proposed system reduces vulnerability by incorporating dual-factor verification. It also addresses a critical limitation in earlier studies by providing a built-in intrusion response. These contributions position the system as a balanced solution that combines robustness with economic feasibility, making it suitable for deployment in residential, institutional, and small-scale commercial environments. Future research would focus on incorporating additional biometric modalities, such as facial recognition or iris scanning, to further strengthen security. Integration with IoT platforms could also allow for remote monitoring and control, although careful consideration must be given to privacy and connectivity challenges. Overall, the system demonstrates that layered authentication on a flexible and open-source platform like Arduino can deliver a reliable and cost-effective approach to modern access control.

References

Barfield, A., Mendoza, J. and Patel, R. 2025. Advanced smart lock system: Enhancing door security with biometric authentication and advanced technology features. Proceedings of the International Institute of

Academic Research and Innovation (IIARI) Conference. https://iiari.org/conference_abstract/advanced-smart-lock-system-enhancing-door-security-with-biometric-authentication-and-advanced-technology-features/

Chukwuemeka, O. and Kasim MT. 2025. A Real-Time Smart Door Access Control System Using Haar Cascade Classifier and Embedded Vision. International Journal of Data Informatics and Intelligent Computing, 4(3): 14–22. https://doi.org/10.59461/ijdiic.v4i3.208

Cookey, C. E., Adigio, E. M, and Goodness, A. A. 2024. Design and implementation of a biometric user identification and access control device using Arduino UNO. *East African* Scholars Journal of Engineering and Computer Sciences, 7(1): 1–9. https://ejaset.com/index.php/journal/article/view/75

Faíña, A. 2022. Learning Hands-On Electronics from Home: A Simulator for Fritzing. 25th International Conference Series on Climbing and Walking Robots (CLAWAR 2022): 404–413. https://doi.org/10.48550/arxiv.2206.07146

Hardyan, RA., Muhamad, A. and Nurjamil, D. 2023. Design and implementation of Arduino-based smart home security system. Journal of Physics: Conference Series, 2582(1): 012025. https://doi.org/10.1088/1742-6596/2582/1/012025

Hemant, Y., Suniti, P. and Ashutosh, KC. 2022. Fingerprint Door Lock. Interantional journal of scientific research in engineering and management, 06(05). https://doi.org/10.55041/ijsrem13541

Kumar, R., Singh, A. and Verma, P. 2020. Design of a hybrid RFID and biometric-based access control system. International Journal of Advanced Computer Science and Applications, 11(5): 567–574. https://doi.org/10.14569/IJACSA.2020.0110570

Mohamed Abdul Cader, AJ, Banks, J. and Chandran, V. 2023. Fingerprint Systems: Sensors, Image Acquisition, Interoperability and Challenges. Sensors, 23(14). https://doi.org/10.3390/s23146591

Olaniyi, O.M., Oyediran, B.A. and Adeniyi, EA. 2019. Development of a facial recognition-based access control system using Raspberry Pi. Nigerian Journal of Technology, 38(3): 627–633. https://doi.org/10.4314/njt.v38i3.17

Perjaru, C., Predusca, G., Avram, M, Radu, M. and Stănescu, C. 2023. Monitoring A Fluid Circuit: A Comparison between Arduino UNO and PIC. The Scientific Bulletin of Electrical Engineering Faculty, 23: 51 - 59. https://doi.org/10.2478/sbeef-2023-0019.

Shafique, M., Khan, S. and Ahmad, T. 2021. Smart home access control using voice recognition technology. International Journal of Electrical and Computer Engineering, 11(2): 1512–1520. https://doi.org/10.11591/ijece.v11i2.pp1512-1520

Widhalm, D., Goeschka, K. and Kastner, W. 2021. Is Arduino a suitable platform for sensor nodes. IECON 2021 – 47th Annual Conference of the IEEE Industrial Electronics Society: 1-6. https://doi.org/10.1109/IECON48115.2021.9589479.

Yin, X., Wang, S., Shahzad, M. and Hu, J. 2022. An IoT-Oriented Privacy-Preserving Fingerprint Authentication System. IEEE Internet of Things Journal, 9: 11760-11771. https://doi.org/10.1109/JIOT.2021.3131956.

Yu, Y., Niu, Q., Li, X., Xue, J., Liu, W., and Lin, D. 2023. A Review of Fingerprint Sensors: Mechanism, Characteristics, and Applications. Micromachines, 14. https://doi.org/10.3390/mi14061253

Zainuddin, AA., Ammar DA., Rizal MN., Amir AA., Nik NM., Abu US. and Muhamad SS. 2024. Innovative IoT Smart Lock System: Enhancing Security with Fingerprint and RFID Technology. Malaysian Journal of Science and Advanced Technology: 360–365. https://doi.org/10.56532/mjsat.v4i4.335