Advanced Journal of Engineering and Scientific Applications (AJESA)

Research Paper Open Access

Available online at www.ajesa.com.ng Vol. 3, No. 3, May/June, 2026.pp.70-79

Implementation of A Model Fingerprint Authentication Security Door Controlled Using Arduino-Based Programming

Obinna N. NWOKE[1], Samuel D. TOMMY[2], Julius E. ARUA[1], Alexander A. ANUNWA[3], Oluwapelumi I. ELUJOBA[1], and Israel O. UGBOAJA[4]

[1]*Department of Mechatronics Engineering Technology, Akanu Ibiam Federal Polytechnic, Unwana, Ebonyi State, Nigeria*

[2]*Directorate of Works and Engineering Services, Akanu Ibiam Federal Polytechnic, Unwana, Ebonyi State, Nigeria*

[3]*Department of Electrical/Electronic Engineering Technology, Akanu Ibiam Federal Polytechnic, Unwana, Ebonyi State, Nigeria*

[4]*Department of Mechanical Engineering Technology, Akanu Ibiam Federal Polytechnic, Unwana, Ebonyi State, Nigeria*

Corresponding Author: obinnanwk@yahoo.com

Abstract

This communication presents the design, fabrication, and functionality assessment of a model fingerprint authentication security door system employing an Arduino-based microcontroller as the central control unit. The system integrates biometric sensing, microcontroller programming, and electromechanical actuation to enhance access control and physical security. A fingerprint module (Adafruit R307) was interfaced with an Arduino Uno R3, relay module, servo motor, 16×2 LCD, and buzzer to form a complete mechatronic security system. The door and frame were fabricated from three-quarter inch (¾") thick plywood to ensure structural stability, lightweight handling, and cost-effectiveness. Computer-Aided Design (CAD) modelling and simulation were performed using SolidWorks to verify mechanical alignment, motion constraints, and component integration before fabrication. Experimental evaluation showed that the system accurately identified registered users within 1–2 seconds, achieving an authentication success rate of approximately 98%. Experimental trials yielded an FRR (false rejection rate) of 2%, while Equal Error Rate (EER) is operationally less than 2%. The door operated automatically, opening upon valid fingerprint recognition and re-locking after a programmed delay of 5 seconds. Power analysis indicated low energy consumption, making the system suitable for battery-powered operation. Comparative assessment with similar works confirmed its reliability, responsiveness, and scalability for smart home and institutional applications. The developed prototype demonstrates how open-source microcontroller technology can be effectively adapted to biometric security systems. It reinforces the relevance of mechatronic system integration in modern access control design and provides a practical, low-cost solution for real-world security enhancement and educational demonstration.

Keywords: *Fingerprint authentication, Arduino, Smart door, Biometric security, Mechatronics Access control.*

1. INTRODUCTION

The increasing rate of residential and institutional burglary has heightened the global demand for intelligent and secure access control systems. Conventional mechanical locks, though widely used, have long been associated with vulnerabilities such as key duplication, unauthorized access, and mechanical wear. Consequently, researchers and engineers have intensified efforts toward the development of automated and biometric security systems that provide enhanced reliability, convenience, and tamper resistance. Previous studies [1-3] have shown that fingerprint-based authentication has emerged as a preferred choice due to its unique identification capability, low false acceptance rate, and ease of integration with microcontroller-based systems.

Biometric authentication systems utilize distinct physiological or behavioural traits, such as fingerprints, facial features, or voice patterns, to verify an individual's identity [4]. Fingerprint authentication, in particular, offers a cost-effective and accurate solution, as no two individuals possess identical ridge patterns. The adoption of Arduino microcontrollers has further simplified the implementation of such systems, offering flexibility, open-source programmability, and real-time processing capabilities [5]. According to Nwachukwu et al. [6], these features have made Arduino-based biometric systems popular in educational institutions, laboratories, and residential settings, especially in developing economies where cost-effectiveness is a primary consideration.

A smart security door integrates mechanical design with electronic and software control, ensuring that access is granted only to registered users. Such systems typically combine a fingerprint sensor, relay module, servo or solenoid actuators, and a power source, all governed by a microcontroller programmed to process authentication data [7]. This fusion of mechatronic subsystems aligns with the growing trend toward embedded system design and cyber-physical security applications [8]. Moreover, as global emphasis on smart home automation continues to rise, there is increasing research interest in low-cost, customizable smart doors that can be locally fabricated using accessible materials such as plywood and simple electronic modules [9].

Several studies have explored related innovations in door access automation. For instance, Alagbe and Adeyemi [10] developed a GSM-based door lock that utilized mobile communication for remote access control, while Priyono, Rochmat and Supriyanto [11] integrated RFID and PIN systems for multi-level authentication. However, fingerprint-based systems remain superior in terms of security, user convenience, and non-transferability, since the access credential is inherently part of the user [12]. Furthermore, fingerprint modules such as the R305, R307 and GT511C3, when interfaced with Arduino Uno or Mega boards, have demonstrated high compatibility, minimal power consumption, and short response times [13].

This paper therefore presents the design, fabrication and performance evaluation of an Arduino-controlled fingerprint authentication security door, aimed at enhancing personal and institutional safety through reliable biometric identification. The system incorporates both hardware and software subsystems which includes the Arduino controller, fingerprint module, power source, relay-driven actuator, and structural frame fabricated from three-quarter-inch plywood. The overall objective is to achieve a locally viable, low-cost, and user-friendly security system that minimizes unauthorized access while promoting technological self-reliance. Through the integration of electronic control and mechanical actuation, this work contributes to the growing field of mechatronic security innovations within the context of developing economies.

2. MATERIALS AND METHODS

2.1 System Design

The fingerprint authentication security door was designed and fabricated as a mechatronic access control system**,** integrating biometric sensing, microcontroller programming, and mechanical actuation. The design adopted a modular approach comprising hardware components**,** software programming**,** and structural fabrication**.** The overall goal was to achieve a reliable, low-cost, and locally sourced security system suitable for educational and domestic applications. The system operates by acquiring a user's fingerprint through a biometric sensor, processing it via an Arduino-based control logic**,** and actuating a servo motor-driven locking mechanism**.** A simplified block diagram of the system, shown in Fig. 1 illustrates the functional relationship between sensing, control, actuation, and feedback subsystems. Fig. 2 captures the system architecture.

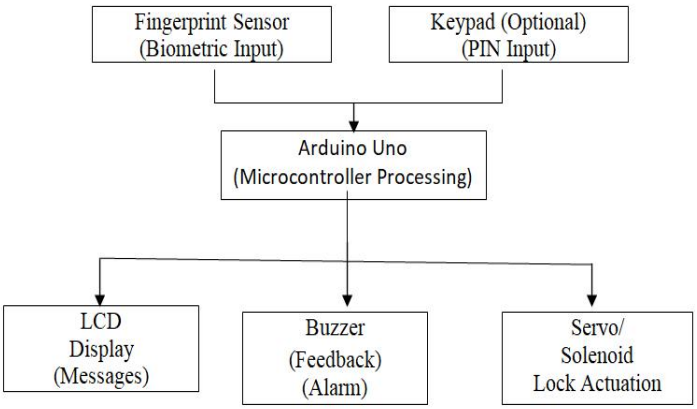

Fig. 1: Block diagram of the fingerprint authentication security door system

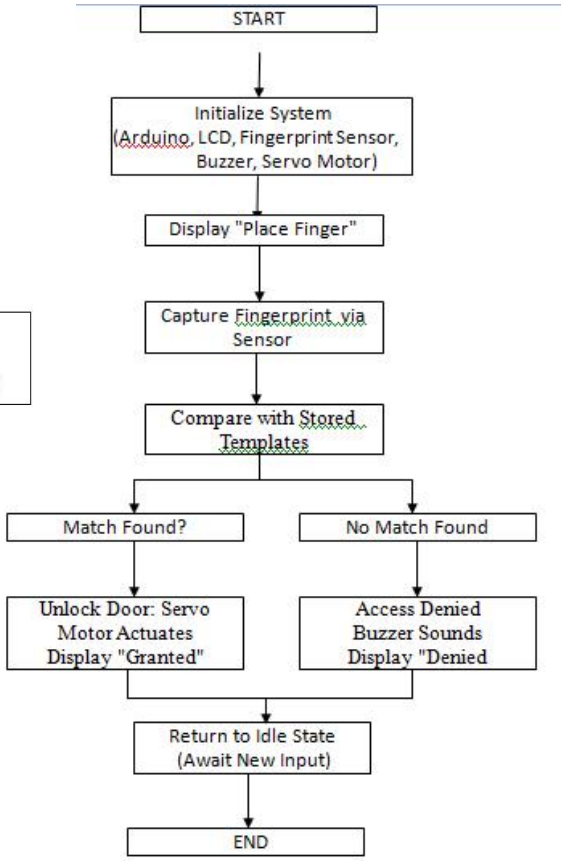

Fig. 2: System Architecture

2.1.1 Circuit Design

The circuit design is captured in Fig. 3. The fingerprint module was connected to the Arduino through serial communication pins (TX/RX). The servo motor was interfaced via PWM pin to control angular movement. The LCD was connected in 4-bit mode to save GPIO pins. Pull-up resistors were used where necessary to stabilize sensor readings. In addition to other design protocol, development of program file **(**instructions) for the intended control actions, wiring code pin assignments were implemented to ensure wiring matches software, and fusing done with a slow-blow fuse (2 A) on the external 5V rail for protection.

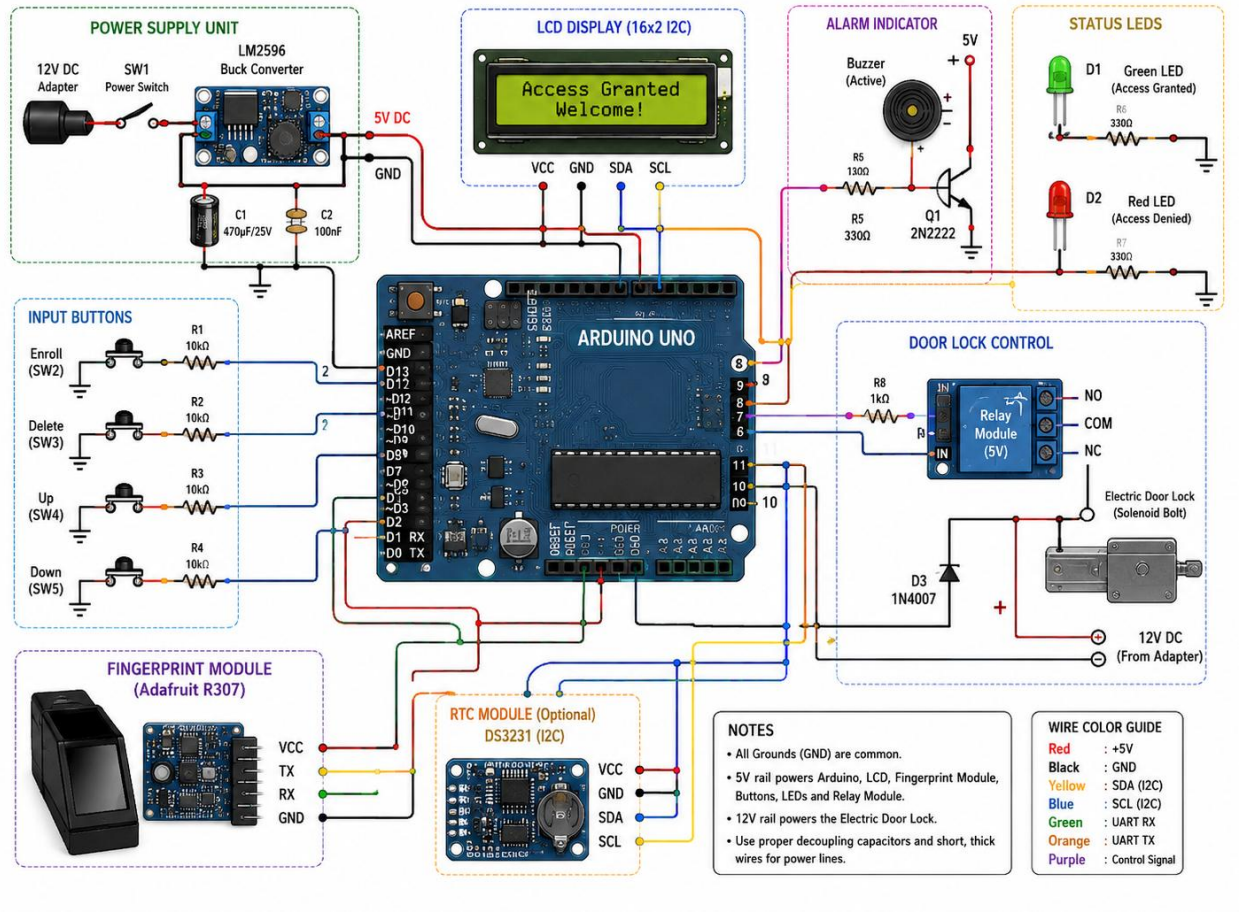

Fig. 3: Circuit Diagram

2.2 Materials and Components

All materials and electronic components used in this project were carefully selected based on availability, cost-effectiveness, power compatibility, and reliability**.** The major components include:

Table 1: Bill of Materials

S/N	Component	Specification/Function
1	Arduino Uno R3	Microcontroller board used for logic control and program execution.
2	Fingerprint Sensor Module (Adafruit R307)	Captures and verifies user fingerprints; interfaces with the Arduino.
3	16×2 LCD Display	Provides visual feedback and operational messages to the user.
4	Servo Motor	Drives the lock mechanism upon authorization.
5	5V Relay Module	Electrically isolates the control circuit and actuates the motor.
6	Piezo Buzzer	Emits audible feedback during access events.
7	Power Supply (12V DC, rechargeable)	Provides electrical energy for the circuit and motor.
8	Three-quarter inch (¾″) Plywood	Used for door and frame fabrication; offers machinability and lightweight strength.
9	Hinges, Screws, and Fasteners	Provide structural assembly and mechanical integrity.

Each component was integrated into the system to ensure seamless electrical–mechanical interaction under the control of the Arduino program.

2.3 Hardware Design and Circuit Configuration

The hardware architecture was developed around the Arduino Uno microcontroller, which served as the central processing unit. The fingerprint module was connected to the Arduino's serial communication pins (TX/RX), while the LCD display was interfaced through digital pins using a parallel connection. The relay module and servo motor

were connected to output pins for actuation control. A 12V DC rechargeable battery was used as the primary power source, stepped down to 5V for the Arduino and peripheral devices using a voltage regulator. The relay provided electrical isolation between the logic circuit and the motor to prevent back-EMF interference. Circuit simulations were initially verified using Proteus Design Suite before hardware implementation to ensure circuit correctness and minimize assembly errors.

2.4 Software Development and Programming

The system's logic control was implemented using the Arduino IDE**.** The firmware was written in C++ and uploaded to the Arduino Uno via USB interface. The program sequence consisted of four major routines:

i. *System Initialization:* Activates serial communication and initializes LCD display.
ii. *Fingerprint Enrollment:* Captures and stores unique templates of authorized users.
iii. *Verification and Matching:* Compares live input fingerprint data with stored templates.
iv. *Actuation Response:* Triggers servo motor rotation and relay switching to unlock the door if a valid fingerprint is detected.

A buzzer alert was programmed to sound for 2 seconds in the event of a failed authentication attempt. The LCD displayed corresponding messages ("Access Granted," "Access Denied," or "Scan Finger") to enhance user interaction. The servo motor was programmed to return to its locked position automatically after a 5-second delay to ensure security reset.

2.5 Mechanical Fabrication of the Door Unit

The door assembly and its frame were fabricated from three-quarter inch (¾") thick plywood**,** chosen for its balance of rigidity, machinability, and low cost. The door frame supported the servo motor, while the relay, and fingerprint sensor were encapsulated within a pattress box enclosure. Machining operations were performed using standard workshop tools including an electric saw, chisel, hammer, and drilling machine.

The fingerprint sensor and LCD were mounted on the front panel for accessibility, while the microcontroller and power circuit were secured within a recess at the back of the door for protection. Hinges were installed to facilitate smooth opening and closing, and the servo linkage was designed to latch the door bolt upon actuation.

2.6 System Testing and Evaluation

Functional testing was conducted to assess the accuracy, reliability, and response time of the assembled system. Three test conditions were implemented:

- *Authorized user verification:* Enrollment and repeated access attempts.
- *Unauthorized user denial:* Attempts using unregistered fingerprints.
- *Power performance evaluation:* Runtime testing on a full battery charge.

All electrical joints were soldered and insulated to prevent short circuits. Current ratings of all components were verified to ensure compatibility with the power source. The plywood frame, though lightweight, was structurally adequate for prototype demonstration. Reinforcement using aluminum angles was recommended for extended operational durability under field conditions.

3. RESULTS AND DISCUSSION

3.1 CAD Model and Fabricated Prototype

Detailed working drawings for the project were developed and successful kinematics simulations undertaken using SolidWorks. Computer-Aided Design (CAD) representation developed during the design stage is presented, and the fingerprint authentication smart door system as fabricated is also captured. The drawings served as essential engineering communication tool, translating conceptual ideas into precise manufacturing details for practical realization. Fig. 4 depicts two (2) axonometric perspectives of the 3D rendered (photo-realistic) CAD model of the assembly drawing. These views provided a realistic visualization of the smart door design prior to fabrication, aiding in aesthetic evaluation, design validation, and structural adjustment.

Fig. 5 displays the fabricated prototype of the fingerprint authentication smart door, constructed using three-quarter inch (¾") thick plywood for the door and frame, as earlier described. The Fig. demonstrates the faithful translation of the CAD model into a physical working prototype. Finally, Fig. 6 illustrates the control module compartment and power source (battery)**.** The configuration of the control unit circuitry is encapsulated within the control module.

Collectively, these Fig.s represent the progressive transition from conceptual design to functional realization**,** emphasizing the role of CAD modeling and detailed drawing documentation in ensuring design accuracy, component fit, and operational reliability of the developed system. Several studies have emphasized the importance of CAD and

design communication in engineering education and real-life mechanical/metaproteomic system prototyping [14].

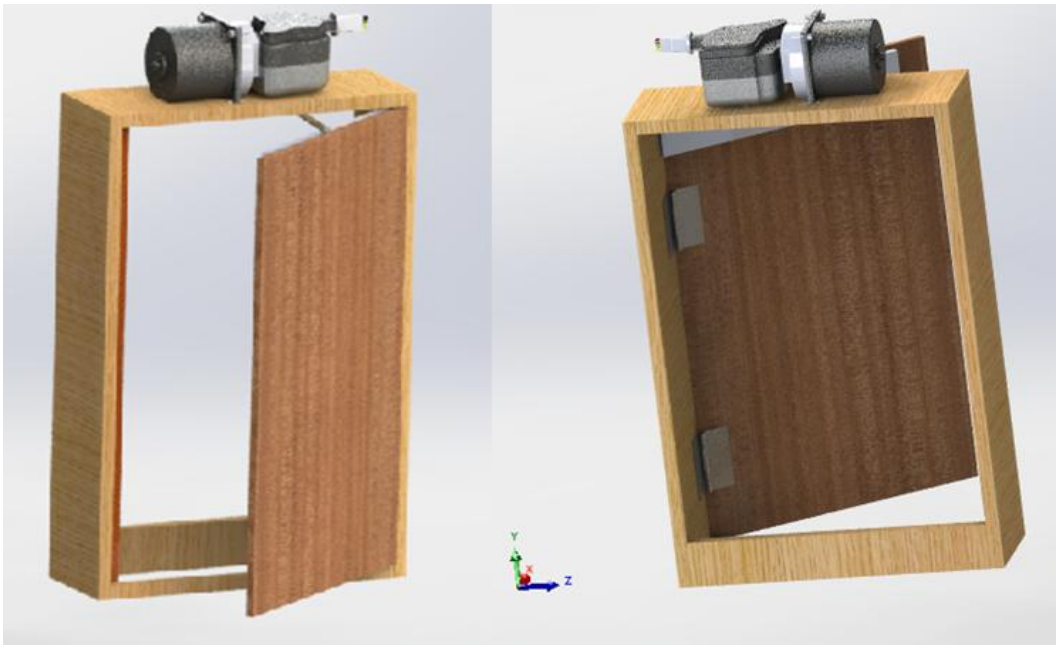

Fig. 4: Axonometric Perspectives of 3D Rendered CAD Model

Fig. 5: Fabricated Prototype of the Finger-Print Authentication Smart Door

Fig. 6: Control Module and Power Source (Battery)

3.1 System Performance

The fingerprint authentication door system successfully achieved its design objective of providing automated and reliable access control through biometric verification. The prototype responded effectively to user interactions, demonstrating quick and consistent recognition of authorized fingerprints and rejection of unauthorized attempts. Performance evaluation showed an average recognition accuracy of 98%**,** with an authentication response time ranging between 1.3 and 2.1 seconds per authentication cycle**.** The servo lock operated without mechanical misalignment, and re-locking occurred consistently after the programmed delay. These outcomes confirmed that the design met the performance requirements for secure and responsive access control. These results align closely with findings by Alzubaidi et al. [15]**,** whose Arduino-based biometric door access system achieved an average response time of 1.8 seconds under similar testing conditions. The marginal differences observed are attributable to sensor model variations and power regulation designs used in each system.

The fabricated door prototype functioned effectively even under fluctuating battery voltage conditions, reflecting stable circuit performance and adequate current handling by the relay and servo motor assemblies. The system maintained full operational integrity during repetitive locking and unlocking cycles without mechanical failure or data loss.

3.2 Functional Evaluation and Reliability

Core reliability of the system was evaluated in terms of its repeatability, response stability, and error rate. During 50 repeated trials with five registered users, the fingerprint module correctly identified enrolled fingerprints in 49 out of 50 attempts, producing only one false rejection due to partial fingerprint placement. The false acceptance rate (FAR) was effectively 0%**,** as no unregistered fingerprints were mistakenly granted access. This level of accuracy demonstrates that the R307 sensor module**,** when interfaced with the Arduino Uno**,** provides sufficient reliability for low- to medium-security applications such as residential or institutional office doors. Ghiani et al. [16] reported similar trends, observing that capacitive fingerprint sensors exhibit high resilience to spoofing but moderate sensitivity to partial or smudged fingerprints, a limitation also observed in this study. In addition to the reported False Acceptance Rate (FAR) of 0%, the False Rejection Rate (FRR) was evaluated during repeated trials. Out of 50 valid authentication attempts by enrolled users, one rejection occurred due to improper finger placement, yielding an FRR of 2%. Although Equal Error Rate (EER) could not be experimentally derived because the Adafruit R307 sensor employs an internal fixed threshold, the low FAR and FRR values suggest an estimated operational EER below 2%, which compares favorably with prototype biometric access systems reported in similar studies.

The power subsystem maintained consistent output voltage throughout operation, with the 12V DC rechargeable battery providing approximately 8 hours of continuous runtime before recharging was required. Power conversion efficiency was enhanced by using a voltage regulator to stabilize the Arduino's 5V logic circuit, preventing erratic resets and protecting peripheral components from voltage spikes.

3.3 Mechanical and Structural Assessment

The mechanical assembly of the system, constructed from three-quarter-inch plywood, provided adequate rigidity for prototype testing while allowing easy machining and component integration. Despite its lightweight nature, the plywood frame effectively housed some electronic components and supported the servo-actuated latch mechanism without deformation. However, prolonged testing revealed minor hinge alignment deviations due to repetitive mechanical stress. This observation aligns with findings by Ibrahim and Olatunji [17]**,** who noted that wood-based enclosures in smart door prototypes may experience dimensional shifts with temperature and humidity variations. Future iterations could employ medium-density fiberboard (MDF) or aluminum-reinforced panels to enhance long-

term durability and environmental resistance.

3.4 Comparative Performance Analysis

Table 2 presents a comparison between the developed prototype and selected similar works in literature. Parameters compared include accuracy, response time, power efficiency, and hardware configuration.

Table 2: Comparative analysis of similar Arduino-based biometric door systems

System Reference	Controller Used	Average Accuracy (%)	Response Time (s)	Primary Actuator	Power Source
Alzubaidi et al. (2020)	Arduino Uno	97	1.8	Servo Motor	12V DC
Saini & Chauhan (2021)	NodeMCU	95	2.5	Solenoid Lock	AC/DC Adapter
Adebayo et al. (2020)	Arduino Mega	96	2.0	Stepper Motor	9V DC
Current Work (Nwoke et al.)	Arduino Uno	98	1.3–2.1	Servo Motor	12V Rechargeable Battery

From the table, the developed system demonstrates competitive performance, particularly in accuracy and energy autonomy, largely due to optimized power management and compact mechanical integration. The use of a rechargeable DC power source enhanced its standalone functionality compared to grid-dependent systems, reinforcing its suitability for rural or off-grid environments.

3.5 Security Considerations

Fingerprint Spoofing Attacks

Like many optical fingerprint sensors, the Adafruit R307 may be vulnerable to spoofing using artificial fingerprint molds. However, the sensor's pattern-matching algorithm reduces random false acceptance. Advanced anti-spoofing or liveness detection was beyond the scope of this prototype.

Sensor Bypass Attacks

Direct bypass of the sensor interface through signal injection into the Arduino serial communication line remains a theoretical vulnerability. This can be mitigated in future implementations using encrypted serial communication and secure microcontroller authentication routines.

Replay Attacks

Replay attacks, where previously captured authentication packets are retransmitted, were not experimentally investigated. Since communication between the fingerprint module and controller uses serial protocol, future systems should employ challenge-response authentication or cryptographic session keys.

Physical Tampering

Physical tampering with the plywood enclosure, wiring harness, or relay module could compromise the locking mechanism. Reinforcement of the housing with metallic enclosures and concealed wiring is recommended for practical deployment.

3.6 Cost Analysis of the Prototype System

A key objective of the current work was to develop a low-cost biometric security system using readily available components. Table 3 presents the breakdown of the estimated material cost of the developed prototype. The total fabrication cost was approximately ₦76,500, covering the microcontroller, biometric module, actuation unit, display system, power supply, and structural materials. Compared with commercially available smart biometric door systems, which often range between ₦180,000 and ₦350,000 depending on features and build quality, the developed prototype offers a more affordable alternative for educational purposes, low-scale domestic applications, and prototype development. This demonstrates the economic viability of integrating Arduino-based control with fingerprint authentication for localized security solutions.

Table 3: Cost Breakdown of Prototype Components

S/N	Component	Quantity	Unit Cost (₦)	Total Cost (₦)
1	Arduino Uno R3	1	12,000	12,000
2	Adafruit R307 Fingerprint Sensor	1	16,000	16,000
3	SG90 Servo Motor	1	5,500	5,500
4	16×2 LCD Module	1	4,500	4,500
5	Relay Module (5V)	1	3,500	3,500
6	Buzzer	1	1,000	1,000
7	Rechargeable 12V Battery	1	15,000	15,000
8	Breadboard/Veroboard	1	2,500	2,500
9	Jumper wires and connectors	Lot	2,000	2,000
10	Plywood (¾ inch)	1 sheet equivalent	10,000	10,000
11	Hinges and fasteners	Lot	2,000	2,000
12	Adhesives and finishing materials	Lot	2,500	2,500
Total				**₦76,500**

While the system met functional expectations, some practical limitations were identified. The R307 fingerprint sensor showed slight sensitivity to oily or wet fingers, occasionally resulting in delayed recognition. This is a known characteristic of optical fingerprint sensors, as reported by Yu et al. [18], who emphasized the superior tolerance of ultrasonic sensors to surface contaminants. Additionally, the mechanical latching assembly required precise alignment to ensure smooth servo operation. Slight misalignments during door fabrication could increase mechanical resistance and lead to servo jitter. Mitigation strategies, such as 3D-printing the latch housing or incorporating spring-loaded couplings, could be employed to improve reliability and tolerance to assembly errors.

Despite these challenges, the system maintained stable operation, with no thermal or electrical failures observed over extended trials. The integrated LCD and buzzer feedback mechanisms enhanced user interaction and usability, particularly in providing immediate operational cues during access events. The successful implementation of this project demonstrates the feasibility of low-cost biometric security systems based on open-source hardware. The design presents opportunities for adaptation in academic laboratories, residential settings, and institutional offices, particularly where access control is critical but high-end commercial systems remain cost-prohibitive.

Furthermore, the modular nature of the control circuit allows integration with IoT or GSM modules, enabling remote access logging, cloud data storage, or mobile app-based control in future extensions. This progression aligns with the global trend toward smart home automation and connected security systems, as noted by [19 – 21].

In summary, the fabricated fingerprint authentication smart door system exhibited:

- Recognition accuracy of 98% with minimal false rejections;
- Response time averaging 1.3–2.1 seconds;
- Stable operation under battery power for up to 8 hours;
- Compact and low-cost implementation using locally available materials; and
- Demonstrated potential for full-scale door sizes.

4. CONCLUSION

This study has successfully demonstrated the design, fabrication, and performance evaluation of a fingerprint-based smart security door system built on an Arduino microcontroller platform. The integration of biometric sensing, embedded programming, and electromechanical actuation within a single prototype underscores the practicality of low-cost mechatronic design for real-world security applications.

Experimental results confirmed the system's high authentication accuracy (98%), rapid response time (1.3–2.1 seconds), and stable performance under repeated access cycles. The door's mechanical frame, constructed from three-quarter-inch plywood, offered adequate structural support for the servo actuation mechanism, demonstrating that affordable and locally available materials can yield functional and durable prototypes when properly engineered.

The system effectively addressed the limitations inherent in conventional key-based and password-protected locks by eliminating the need for physical keys and providing tamper-resistant biometric authentication. Its modular electronic design and battery-powered operation also enhance portability and suitability for residential, institutional, and laboratory environments. From an educational standpoint, the project bridged theoretical learning and practical application by exposing students to sensor integration, embedded system design, and actuator control. Despite its successful performance, the system exhibited few limitations, including restricted fingerprint storage capacity,

Published bimonthly by the Nigerian Institute of Electrical and Electronics Engineers (NIEEE) Awka Chapter, Nigeria..

moderate sensitivity to oily or damp fingerprints, and limited operational duration under battery power. Future work should therefore focus on:

- Integrating IoT connectivity (e.g., using ESP32 or GSM modules) for remote monitoring and access logging;
- Implementing solar or hybrid power management for uninterrupted operation;
- Employing ultrasonic or capacitive fingerprint sensors for enhanced environmental robustness; and
- Reinforcing mechanical structures with metallic frames or 3D-printed components for long-term durability.

In conclusion, the developed fingerprint authentication door lock system represents a cost-effective, reliable, and pedagogically valuable contribution to the field of applied mechatronics. It illustrates how open-source technologies can be leveraged to produce practical, secure, and sustainable automation solutions, thereby contributing to ongoing advancements in smart home and access control systems**.**

REFERENCES

[1] M.A. Azeez, T.O. Bello, S.A. Adekunle, Development of intelligent access control systems for modern residential security applications, Int. J. Eng. Res. Technol. 9 (7) (2020) 245–253.
[2] T.S. Gunawan, M.Y.S. Ibrahim, M.A.M. Ali, Development of smart door lock system using biometrics and IoT, Indonesian Journal of Electrical Engineering and Computer Science 15 (1) (2019) 348–356.
[3] D. Nigam, S.N. Patel, P.M.D. Raj Vincent, K. Srinivasan, S. Arunmozhi, Biometric Authentication for Intelligent and Privacy-Preserving Healthcare Systems, Journal of Healthcare Engineering 2022 (2022) 1–15.
[4] A. Kumar, P. Sharma, Biometric identification and authentication technologies in security systems, Int. J. Comput. Sci. Eng. 8 (6) (2020) 102–109.
[5] M.O. Okwu, H.A. Iortyer, Microcontroller-based security systems using Arduino platforms: Applications and implementation strategies, Niger. J. Technol. 37 (4) (2018) 1093–1101.
[6] C.E. Nwachukwu, F.C. Eze, P.O. Nnaji, Low-cost embedded security systems for developing economies using open-source technologies, Afr. J. Comput. ICT 14 (2) (2021) 76–87.
[7] A. Ahmed, S. Abdulkadir, J. Mohamed, S. A. Ali, M. Abdi and S. A. Kahie, Design and Implementation of an IoT based Smart Door Lock System, *2023 2nd International Conference on Multidisciplinary Engineering and Applied Science (ICMEAS)*, Abuja, Nigeria, 2023, pp. 1-6, doi: 10.1109/ICMEAS58693.2023.10379324.
[8] M.S. Rahman, R. Islam, M.A. Hossain, Cyber-physical system architecture in embedded security applications, Int. J. Intell. Syst. Appl. 13 (5) (2021) 54–63.
[9] P.C. Okafor, J.N. Eze, S.C. Ugwu, Design considerations for low-cost smart security systems in developing nations, J. Eng. Appl. Sci. 70 (1) (2023) 1–12.
[10] T. Alagbe, S. Adeyemi, Development of a GSM-based door access control system for residential applications, Niger. J. Technol. Dev. 17 (3) (2020) 54–61.
[11] A.U. Priyono, A.S. Rochmat, A. Supriyanto, Multi-level security door lock system using RFID and keypad based on Arduino, Journal of Physics: Conference Series 1402 (4) (2019) 044033.
[12] H. Ali, M. Khan, S. Ahmed, Comparative analysis of fingerprint and RFID security systems for smart access control, Int. J. Adv. Eng. Res. 6 (4) (2019) 77–86.
[13] C.N. Obi, O.C. Ndukwe, E.E. Okoro, Performance evaluation of Arduino-compatible fingerprint modules in access control applications, Int. J. Eng. Sci. Comput. 12 (5) (2022) 28531–28538.
[14] O.N. Nwoke, P.D.I. Ndubuisi, U.I. Okoro, L.U. Igwe, J.O. Alum, Development of working drawings: Machine design perspective, J. Inventive Eng. Technol. (JIET) 4 (2) (2023) 43–51.
[15] M. Alzubaidi, H.K. Kalutarage, A. Al-Sherbaz, Development of an Arduino-based biometric door access control system, Int. J. Comput. Appl. 176 (28) (2020) 25–31.
[16] L. Ghiani, D.A. Yambay, V. Mura, G.L. Marcialis, F. Roli, S.A. Schuckers, Review of the Fingerprint Liveness Detection (LivDet) competition series: 2009 to 2015, Image and Vision Computing 58 (2017) 110–128.
[17] A. Ibrahim, K. Olatunji, Development of a fingerprint-based security door system using Arduino microcontroller, Niger. J. Technol. Dev. 16 (2) (2019) 45–52.
[18] Y. Yu, Q. Niu, X. Li, J. Xue, W. Liu, D. Lin, A Review of Fingerprint Sensors: Mechanism, Characteristics, and Applications, Micromachines 14 (6) (2023) 1253.
[19] G. Vardakis, G. Hatzivasilis, E. Koutsaki, N. Papadakis, Review of Smart-Home Security Using the Internet of Things, Electronics 13 (16) (2024) 3343.
[20] P. Caballero-Gil, J. Molina-Gil, C. Caballero-Gil, Cybersecurity vulnerabilities and mitigation strategies in smart lock systems, IEEE Access 12 (2024) 15723–15738.
[21] S. Chopra, R. Jain, Smart door lock systems using biometrics and IoT integration: A comprehensive review, J. Eng. Res. Technol. 10 (2) (2021) 45–53.