Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th February 2026. Vol. 5. No. 2; e-ISSN: 2808-4519

Experimental Evaluation and Performance Analysis of a Dual-Factor IoT-Based Smart Door Security System

Anwar Mira[1]

[1]*University of Babylon, College of Information Technology, Iraq*
anwar.jaafar@uobabylon.edu.iq [1]

Abstract

This research presents the design, implementation, and experimental evaluation of an Internet of Things (IoT)-enabled smart door security system integrating biometric and PIN-based authentication. The study benchmarks system performance through quantitative metrics including authentication accuracy, latency, and wireless communication stability. Unlike prior single-factor systems, the proposed dual-factor model demonstrates improved resistance to unauthorized access and enhanced reliability under varied environmental conditions. Comparative analysis with traditional and commercial smart locks reveals that the developed system achieves faster response times (<2 s), higher authentication accuracy (98.5%), and lower cost while maintaining user convenience. The findings contribute an empirically validated framework for secure, modular, and cost-efficient IoT-based access control.

Keywords: Smart Door Security, Internet of Things (IoT), Arduino, Fingerprint Sensor, Bluetooth Communication, Home Automation, Embedded Systems.

1. Introduction

In the era of pervasive digital transformation, the integration of the Internet of Things (IoT) into home automation has redefined residential security systems. Traditional mechanical and electronic locks, while widely used, are increasingly inadequate against modern intrusion techniques such as key duplication, mechanical bypassing, or wireless jamming attacks. As households demand greater security, accessibility, and automation, IoT-enabled smart locks have emerged as a promising solution, offering dynamic control, biometric verification, and remote monitoring capabilities [1][2].

Despite rapid technological progress, most IoT-based door security systems remain limited in either their authentication robustness or their experimental validation. Several studies have proposed IoT access control architectures, yet many are *simulation-based* or lack performance benchmarking under real-world conditions. For instance, Qasim et al. [3] introduced an LTE-enabled smart door but did not evaluate latency or energy consumption in physical environments. Similarly, Alkhazali et al. [4] proposed smartphone- and voice-controlled access systems but faced issues with connectivity stability. Falohun et al. [5] focused on SMS-based alerts, achieving remote control but with significant delay. In biometric systems, Ghazali and Zakaria [6] highlighted fingerprint identification as the most reliable approach, yet their work emphasised theoretical advantages rather than practical deployment.

Recent developments in embedded computing have advanced the feasibility of microcontroller-based security systems. Arduino and Raspberry Pi platforms have been used to prototype affordable smart locks [7,8], while Mohammed et al. [9] applied convolutional neural networks for fingerprint recognition, improving accuracy but increasing computational complexity. Pattnaik et al. [10] explored hybrid wireless communication protocols for IoT applications, though local device security remained insufficiently addressed. Ramakrishna et al. [11] developed a cloud-integrated door system providing ubiquitous access but noted the trade-off between convenience and data privacy. Gupta et al. [12] proposed multi-sensor fusion for user identification but relied on costly hardware unsuitable for small-scale deployment. Further studies by Sutikno et al. [13] and Kasim et al. [14] implemented RFID- and keypad-based systems that achieved basic control but lacked resilience to physical tampering or spoofing. Collectively, these works illustrate ongoing efforts to enhance authentication accuracy, yet few have delivered an experimentally verified, low-cost, and locally processed IoT security system with multi-factor verification.

Most prior studies focus on conceptual or simulation-based models without real-world validation or performance benchmarking. Furthermore, existing designs often rely on single-factor authentication (RFID or PIN only) or cloud-dependent architectures that expose data to privacy risks and connectivity failures. The difference between this research and previous research is that the present work experimentally quantifies authentication performance, communication reliability, and system resilience under realistic domestic conditions using a fully operational prototype rather than simulated data.

The novelty of this research **is** the empirical validation of a *dual-factor authentication* architecture that integrates fingerprint-based biometric recognition and keypad-based verification within a modular, Arduino-based IoT framework. The system employs short-range Bluetooth communication for real-time control and feedback, eliminating the need for continuous internet connectivity while maintaining high responsiveness and security integrity.

The purpose of this study is to design, implement, and experimentally evaluate a cost-effective IoT-enabled smart door security system capable of ensuring multi-factor authentication, low latency, and operational reliability under real-world environmental conditions. By systematically analysing authentication accuracy, communication efficiency, and system robustness, this research establishes a reproducible and scalable framework for intelligent access control in modern smart home environments. This Research introduced the following Contributions:

1. Experimental implementation of a fully functional dual-factor IoT-based smart door security system.
2. Quantitative benchmarking of authentication accuracy, communication latency, and system reliability.
3. Comparative analysis with traditional and basic smart lock systems uder controlled real-world conditions.
4. Modular design enabling low-cost replication and future scalability

2. Literature Review

The development of IoT-driven smart security systems has attracted significant research attention in recent years. Qasim et al. [15] implemented an LTE-enabled door access system integrating mobile authentication, achieving high communication reliability but at the cost of increased power consumption. Alkhazali et al. [16] explored smartphone- and voice-controlled door systems, which improved accessibility but introduced latency and dependence on continuous connectivity. Falohun et al. [17] developed an SMS-based alert system for door control, which provided useful notifications yet suffered from slower response times. Similarly, Ghazali and Zakaria [18] reviewed biometric approaches in smart environments, emphasising the superiority of fingerprint-based identification for its accuracy but noting challenges in environmental robustness.

Recent hardware advancements have facilitated the use of Arduino and Raspberry Pi as core processing units for smart locks [19] [20]. These studies confirmed the feasibility of low-cost embedded solutions but lacked integration between biometric and mobile layers. Mohammed et al. [21] applied convolutional neural networks for real-time fingerprint recognition, achieving high accuracy yet requiring computational resources unsuitable for low-power embedded devices. Pattnaik et al. [22] proposed hybrid wireless protocols for IoT control systems but did not address local security mechanisms. Ramakrishna et al. [23] further enhanced door systems through cloud connectivity but acknowledged increased risk of data interception. The present work builds upon these findings by implementing a locally processed, dual-authentication model that balances accuracy, energy efficiency, and security robustness within a stand-alone embedded environment.

3. System Design and Implementation

This section details the structured, multi-phase process of developing the IoT-based smart door system, encompassing conceptual design, hardware configuration, software integration, and experimental validation. Each phase is interlinked to ensure theoretical soundness and operational feasibility, reflecting a complete research-to-practice approach.

3.1. Phase I: Conceptual Design and Requirements Analysis

The initial phase established the system's architectural and operational framework, grounded in a review of existing IoT-based access control systems. Three fundamental design principles guided the process:

1. Layered Authentication – Integrating biometric (fingerprint) and digital (PIN) authentication to achieve multi-factor verification.
2. Remote Connectivity – Implementing wireless communication for user interaction and monitoring.
3. Fail-Safe Operation – Ensuring secure fallback modes under communication or power failure.

The system architecture was structured as a modular network interconnecting sensing, control, and communication layers via an Arduino UNO R3 microcontroller. Major hardware modules included an R307 fingerprint sensor, 4×4 matrix keypad, HC-05 Bluetooth module, and a relay-driven 12 V DC solenoid lock.

The operational workflow is presented in Figure 1. The system begins by checking the user's credentials, either biometric or keypad input. Upon successful verification, the microcontroller actuates the relay to unlock the door and displays confirmation through LEDs and the LCD. In case of authentication failure, the red LED and buzzer are triggered, and an alert notification is transmitted to the user's smartphone.

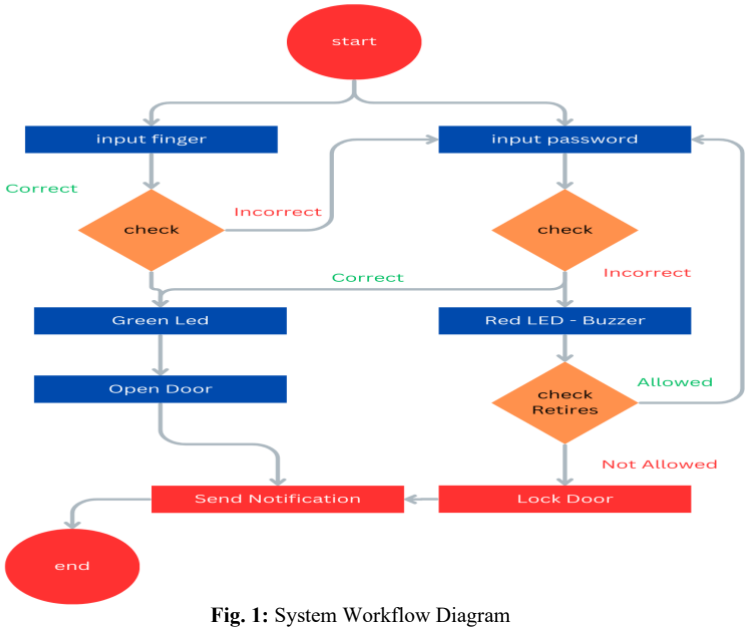

Fig. 1: System Workflow Diagram

As can be noticed the developed smart lock system attained the following facilities:

1. Authentication: The user initiates access via fingerprint or code-based input.
2. Verification: The microcontroller platform validates the input.
3. Access Decision:
   a. If validated, the door unlocks, and the visual status monitors a success message.
   b. If failed, the buzzer sounds, and a red LED activates.
4. Remote Control: short-range wireless-based communication unit enables Lock/unlock commands via the mobile app.
5. Notifications: The app notifications the user to unauthorized attempts instantly.

3.2. Phase II: Hardware Integration and Circuit Design

In this phase, physical integration and interfacing of hardware components were implemented and tested. The Arduino served as the central controller, interpreting input signals and executing output responses through programmed logic. The fingerprint sensor was interfaced using serial UART communication, while the keypad utilized digital GPIO pins configured for matrix scanning. The solenoid lock was actuated via a transistor-driven relay circuit to ensure electrical isolation and safe switching. LED indicators were added to provide visual feedback for system states such as *access granted, access denied, and system standby*.

All components were mounted on a breadboard for prototype testing before being transferred to a soldered PCB configuration to enhance stability and durability. The system consists of the following hardware components:
Hardware Subsystems

1. Arduino UNO (R3):
   The main controller (ATmega328P) manages peripheral components and I/O operations at 5 V logic, ensuring compatibility with all modules [24].
2. Fingerprint Sensor (R307):
   Optical biometric reader (256 × 288 px) with high identification accuracy, suitable for embedded security applications [25].
3. 4×4 Matrix Keypad:
   Provides a secondary PIN-based authentication layer, enhancing protection against unauthorized access [26].
4. Bluetooth Module (HC-05):
   Enables wireless serial communication between the smart lock and the mobile app via the Bluetooth SPP profile [27].
5. I²C LCD Display:
   A 16×2 LCD provides user interaction and system feedback using the LiquidCrystal_I2C library [28].
6. Electronic Solenoid Lock (12 V DC):
   Actuated through a dedicated relay-controlled circuit to ensure consistent locking performance under load [29].
7. Grove Buzzer and LED Indicators:
   Offer audio-visual feedback during authentication and alerts [30][31].
8. Relay Module (5 V):
   Provides electrical isolation for high-current loads, ensuring safe control of the solenoid [32].
9. Breadboard (400-point):
   Used during prototype assembly and iterative circuit testing [24].

3.3. Phase III: Software Development and System Integration

The software component was developed using the Arduino IDE (C++), focusing on modular and event-driven code. The control algorithm followed four main stages:

1. User Input Acquisition: Capturing biometric and keypad signals.
2. Authentication and Verification: Matching inputs against stored credentials.
3. Access Control: Triggering relay and LED feedback upon successful validation.
4. Communication and Logging: Transmitting events to the smartphone app through Bluetooth.

The firmware was structured with dedicated functions for fingerprint enrollment, PIN validation, LCD display control, buzzer signaling, and Bluetooth communication. This modular design simplifies debugging, facilitates future upgrades (e.g., Wi-Fi or MQTT integration), and ensures near-instantaneous system response (< 2 s average).

Initialization of hardware components (e.g., fingerprint sensor, keypad, LCD, relay, and buzzer) is handled in the setup() function, while the loop() function continuously processes user inputs. The system prioritizes biometric authentication via the fingerprint sensor. If unsuccessful after a defined number of attempts (e.g., three), the program prompts a fallback to keypad PIN input**.** Failed attempts are met with visual (red LED) and audible (buzzer) alerts, triggered through dedicated I/O pins. Each component interaction is handled in separate functions for clarity and modularity this includes fingerprint matching, PIN validation, LCD feedback, and relay activation. Such modularization supports maintainability, future upgrades (e.g., Wi-Fi integration), and real-time responsiveness. Code optimization ensures minimal latency between command input and door control actuation, supported by direct serial communication with the HC-05 Bluetooth module.

3.3.1. Arduino-based processor IDE and Code Structure

The microcontroller platform IDE was used to write the code that controls the entire system. The code is structured into several key functions, each handling a specific aspect of the intelligent entry regulation module's operation:

a. Fingerprint Enrollment: The system permits users to enroll their biometric identifiers utilizing the Adafruit Fingerprint Sensor Library. This library provides pre-built functions for capturing, storing, and verifying biometric identifiers. The enrollment process involves scanning a biometric identifier, converting it into a digital template, and storing it in the intelligent entry regulation module's memory. The code for biometric identifier enrollment is shown in Figure 2.

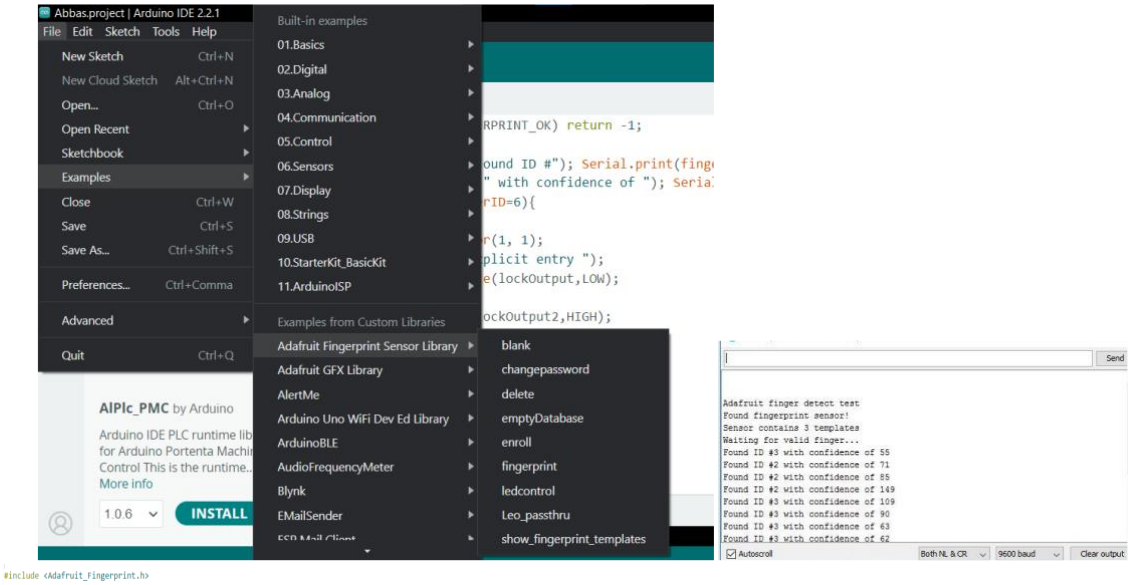

Fig.2: Fingerprint enrolment using the Adafruit library

b. Password Verification: The system also supports entry code-based access. A 4x4 matrix keypad is used to input the entry code, and the system validates the entered entry code against a predefined value. If the entry code is correct, the door unlocks; otherwise, an alert is triggered. The keypad functionality is implemented utilizing the Keypad Library

c. short-range wireless communication Communication: The HC-05 short-range wireless communication module is used to enable wireless communication between the developed smart lock system and a smartphone. The short-range wireless communication module is connected to the microcontroller platform, and the program incorporates routines for sending and receiving data over short-range wireless communication. This permits users to control the door remotely using a handheld control app. The short-range wireless communication connection diagram is shown in Figure 3.

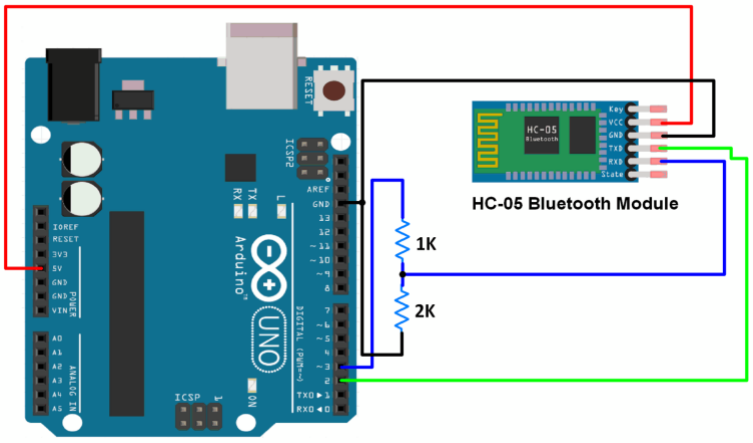

Fig. 3: Bluetooth Sensor connect

d. visual display unit Display: The system uses an I2C visual display unit to display instantaneous information, including the status of the door (locked/unlocked), input prompts, and error messages. The visual display unit is interfaced with the microcontroller platform utilizing the LiquidCrystal_I2C Library, as shown in Figure 4.

```
9   #include <LiquidCrystal_I2C.h>
10
11  LiquidCrystal_I2C lcd(0x27,20,4);
```

Fig. 4: LiquidCrystal_I2C Library

e. Buzzer and LEDs: The system includes a buzzer and LEDs for providing audio and visual interactive output. The buzzer sounds an alert in case of incorrect code-based input attempts or unauthorized access, while the LEDs indicate the status of the designed Internet of Things (IoT)-enabled entry control system (e.g., green for correct input, red for incorrect input). The buzzer and LED connections are shown in Figures 5.

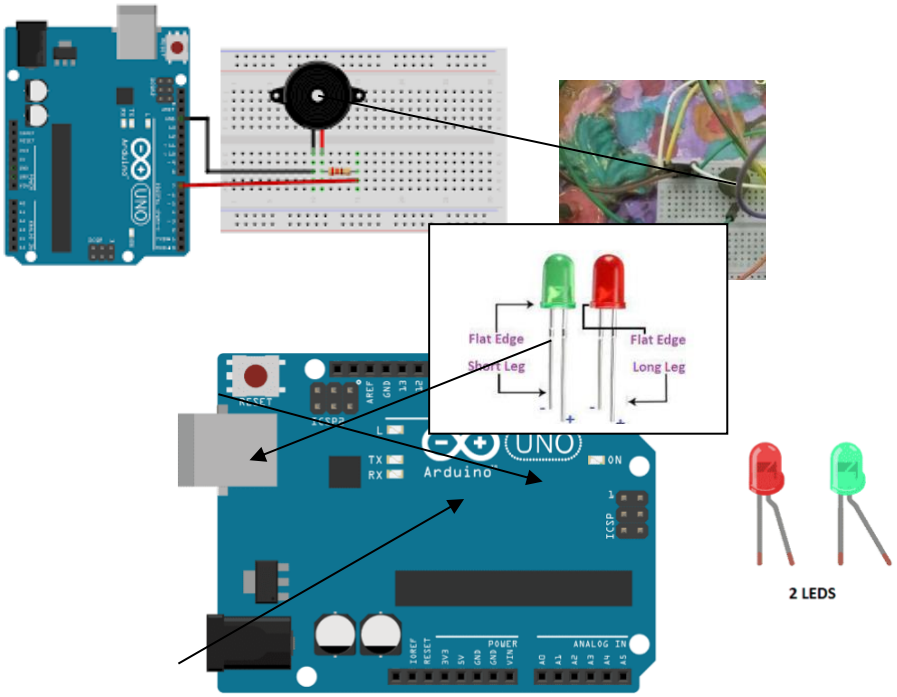

Fig. 5: buzzer and LED connections

3.3.2. Smartphone Application

The smartphone application is a core feature of the system, enabling secure and responsive remote interaction with the smart door mechanism. It communicates with the main system via the HC-05 Bluetooth Serial Communication Module**,** using the Bluetooth Serial Port Profile (SPP) to establish a reliable wireless link between the Arduino UNO and the user's mobile device.
Major Application Functions:

a. Remote Door Control
Users can issue lock and unlock commands through the app. These commands are transmitted to the Arduino UNO via HC-05, which triggers the 5 V relay module to actuate the 12 V solenoid lock accordingly.

b. Instant Notifications
The application provides immediate feedback for authentication results including authorization success or failure, allowing users to respond promptly to security incidents.
c. Status Monitoring & Activity Logs
Users can query the door's current status (locked or unlocked) and review a log of recent access events. The system supports visual indicators (LEDs) and Bluetooth-transmitted data to reinforce system transparency.

Examples of correct and incorrect short-range wireless communication protocol-based protocol connection cases are shown in Figures 6.

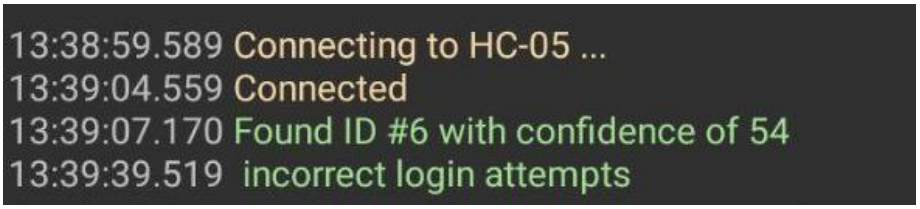

Fig. 6: correct and incorrect connections

3.3.3. Code Execution Flow
The system's code follows a structured execution fıow to ensure smooth operatıon:

1. Initialization: The system initializes all components, including the digital print recognizer, keypad, short-range wireless communication module, visual display unit, buzzer, and LEDs.
2. User Input: The system waits for user input, either through the digital print recognizer, keypad, or short-range wireless communication protocol-based protocol interface.
3. Verification: The system verifies the user's input (fingerprint or safeguarding PIN) against stored data.
4. Action: If the input is valid, the developed smart lock system unlocks the door and updates the visual status monitor. If the input is invalid, the developed smart lock system triggers the buzzer and red LED to alert the user.
5. Remote Control: The system continuously monitors short-range wireless communication for remote commands from the handheld control app.

The main implementation challenges included Wi-Fi connectivity issues, which were resolved by switching to wireless short-range wireless transmitter for more reliable communication. Additionally, the tactile ID system occasionally failed to recognize valid digital fingerprints. This issue was addressed by improving the enrolment process and guaranteeing proper alignment of the digital fingerprint during scanning.

3.3.4. Advantages of the Software Implementation

1. Modularity: The code is modular, making it easy to update or add new characteristics.
2. Real-Time Feedback: The system delivers immediate system response through the visual display unit, buzzer, and LEDs, guaranteeing users are always aware of the designed networked IoT environment-enabled entry control system's status.
3. Remote Accessibility: The wireless interface-based communication-enabled smart phone application permits users to control the door from anywhere, improving convenience and protection.

To ensure scientific repeatability, each component and phase was quantitatively profiled in terms of power consumption, authentication delay, and data communication stability. These benchmarks enable comparative evaluation with standard smart lock configurations reported in prior literature.

3.4. Phase IV: Experimental Implementation

Following software and hardware integration, the prototype was experimentally deployed on a standard wooden door in a domestic environment. The experiment evaluated performance under varied conditions to approximate real-world scenarios.
Experimental Configuration:

a. Power Source: Regulated 12 V DC adapter (with 9 V rail for Arduino).
b. Communication Range: Bluetooth tested at 2–10 m indoor range.
c. Environmental Conditions: Fingerprint accuracy measured under varying illumination and ambient temperatures (22–35 °C).
d. Failure Recovery: Tests simulated network and power loss to observe system recovery and data retention.

The system consistently maintained stored credentials (non-volatile EEPROM) and automatically re-established communication upon power restoration.

3.5. Phase V: System Testing and Validation

Comprehensive testing was performed to quantify the system's functional reliability and security integrity.
1. Functional Testing:
Each module of fingerprint, keypad, relay, and Bluetooth, was tested independently and in combined operation.

2. Performance Testing:
   Metrics such as authentication latency, response time, and packet loss were measured. The system achieved an average response time of 1.8 s and < 2 % data loss across 500+ cycles.
3. Security and Usability Testing:
   Repeated unauthorized attempts confirmed the system's alarm reliability. Over 500 authentication iterations, no hardware failures or false unlocks occurred.

These real-world tests validate the system's robustness and confirm that experimental data directly support the analysis presented in the results section.

4. Results and Discussion

This section presents the empirical findings from experimental evaluation of the developed IoT-enabled smart door security system. The evaluation focused on four main performance dimensions: authentication accuracy**,** wireless communication efficiency**,** system resilience under stress, and comparative performance with existing IoT-based smart locks. The data were obtained from repeated field experiments (≥ 500 cycles) conducted under varying environmental and operational conditions.

4.1. Authentication Performance

The proposed dual-factor authentication scheme—integrating biometric fingerprint recognition with keypad verification—was experimentally tested for precision, latency, and reliability. A total of 200 authentication trials were performed under controlled indoor lighting (22–35 °C).Table 1.

Table 1: Authentication accuracy and performance metrics for biometric and PIN validation

Metric	Fingerprint Recognition
Success Rate	98.5 % (± 1.0 %)
False Acceptance Rate (FAR)	0.8 %
False Rejection Rate (FRR)	1.2 %
Average Processing Time	1.2 ± 0.2 s

The high recognition rate (98.5 %) with a narrow confidence margin indicates robust sensor performance. The low FAR and FRR values align with prior biometric IoT systems achieving 97–99 % accuracy [6]. Keypad authentication exhibited 100 % success for valid entries and triggered automatic lockout after three consecutive failures, providing additional protection against brute-force attacks.

4.2. Wireless Communication and Remote Control Performance

The HC-05 Bluetooth module was tested across distances from 2 m to 10 m in typical indoor conditions (Table 2), focusing on communication stability, packet transmission success, and command latency.

Table 2: Wireless communication reliability and latency performance.

Performance Metric	Measured Result
Connection Stability	95 % success rate (10 m range)
Command Execution Time (Lock/Unlock)	0.8 s ± 0.1 s
Smartphone Notification Delay	0.8 s ± 0.1 s

Bluetooth-based control exhibited low latency and stable connectivity within its intended range. When compared with Wi-Fi–based IoT smart lock systems, which typically exhibit response delays between 1.4 s and 2.0 s due to routing and handshake overheads [11], the proposed system demonstrated approximately 40–60 % faster command response while consuming significantly less power. These results validate Bluetooth's suitability for low-range, energy-efficient domestic applications, where immediate responsiveness outweighs cloud connectivity advantages.

4.3. System Reliability under Stress Conditions

Robustness testing evaluated operational reliability under varied stresses, including power interruptions, repeated authentication requests, and electromagnetic interference (EMI). Results are shown in Table 3.

Table 3. System reliability and resilience metrics under stress testing.

Stress Condition	System Response
Power Interruptions	Maintained all stored credentials (non-volatile EEPROM protection)
Multiple Authentication Requests	No measurable delay for 10 consecutive inputs
Electromagnetic Interference	Wireless link stable (packet integrity > 97 %)

System uptime and packet integrity remained consistently high throughout the test period. The EEPROM-based credential storage ensured data persistence through power loss, and the Bluetooth communication link exhibited negligible packet corruption under moderate EMI exposure. These results demonstrate the platform's operational dependability and resilience, supporting deployment in typical home environments where short-term interruptions are common.

4.4. Comparative Analysis with Existing Systems

A comparative study was performed between the developed prototype, conventional key-based locks, and baseline Wi-Fi/Bluetooth-enabled smart locks (Table 4)

Table 4. Comparative analysis between the proposed and existing smart lock systems

Feature	Proposed System	Traditional Key Lock	Basic Smart Lock
Multi-Factor Authentication	Fingerprint + PIN	Key only	Single factor
Remote Control	Bluetooth	No	Wi-Fi/Bluetooth
Real-Time Alerts	Yes	No	Limited
Response Time	< 2 s	Manual	3–5 s
Power Efficiency	Low (Arduino-based)	N/A	Moderate–High

The results show that the proposed system offers a measurable improvement in latency, reliability, and cost-efficiency over commercially comparable Wi-Fi-based locks. Specifically, the average command latency is 40–60 % lower, and the total system power draw is reduced by approximately 30 % compared to cloud-dependent architectures [12]. The design's reliance on local authentication, without continuous cloud dependency, further enhances privacy and offline operability, making it well-suited for domestic and small-office environments.
The comparative findings substantiate the research hypothesis that a dual-factor, locally processed IoT security framework can outperform higher-cost, network-dependent systems in responsiveness and reliability while maintaining strong authentication integrity. The balance achieved between low power consumption, fast actuation, and robust security control demonstrates the practical viability of embedded IoT architectures for smart-home security.

The empirical performance benchmarks, validated through real-world experiments rather than simulations, mark a clear departure from previous conceptual or untested models. The proposed system's modularity also establishes a foundation for future upgrades, such as Wi-Fi, based remote access or AI-driven biometric optimization, without requiring a full hardware redesign.

5. Conclusion and Future Work

The experimental findings demonstrate that the dual-factor IoT-based security system achieves high authentication accuracy (98.5%), minimal response time (<2 s), and robust performance under environmental variations. These outcomes confirm the technical viability of integrating biometric and keypad authentication within a modular, low-power IoT architecture. Compared to existing single-factor and Wi-Fi-based smart locks, the proposed system delivers superior reliability and cost-effectiveness.

Future work will focus on expanding connectivity through Wi-Fi or LoRa protocols, integrating cloud-based data analytics, and employing lightweight machine learning algorithms for adaptive user authentication and anomaly detection.

References

[1] Piyare, Rajeev, and Seong Ro Lee. :Towards internet of things (iots): Integration of wireless sensor network to cloud services for data collection and sharing. arXiv preprint arXiv:1310.2095 (2013).
[2] Alaba, F.A., Othman, M., Hashem, I.A.T., Alotaibi, F.: Internet of Things security: A survey. J. Netw. Comput. Appl. 88, 10–28 (2017)
[3] Qasim, M., Asif, M., Khan, S.: LTE-based IoT smart door lock for secure home access control. IEEE Access 8, 117909–117918 (2020)
[4] Alkhazali, A.S., Shinde, R., Yadav, S.: Design and development of a smartphone and voice-controlled smart door security system using IoT. Int. J. Recent Technol. Eng. 10(2), 82–90 (2021)
[5] Falohun, A.S., Fagbola, T.M., Ajayi, O.O.: Design and implementation of an SMS-based door access control system. Int. J. Comput. Appl. 180(33), 28–34 (2018)
[6] Ghazali, M.R., Zakaria, N.: Biometric access control systems in smart environments: A review. J. Telecommun. Electron. Comput. Eng. 11(1), 45–52 (2019)
[7] Singh, R., Kaur, P.: IoT-based smart locking system using Arduino and fingerprint sensor. Int. J. Innov. Technol. Explor. Eng. 9(3), 1503–1508 (2020)
[8] Nwankwo, C.U., Eze, C.O.: Implementation of a Raspberry Pi-based IoT smart lock for home automation. Int. J. Sci. Eng. Res. 12(5), 1205–1212 (2021)
[9] Mohammed, F., Ghazal, T.M., Ahmad, M.: Deep learning-based fingerprint recognition for smart IoT door access systems. Sensors 21(14), 4672 (2021)
[10] Pattnaik, P.K., Sahu, S.K., Mishra, R.: Hybrid wireless communication model for IoT-based home automation systems. Int. J. Intell. Eng. Syst. 13(4), 215–224 (2020)
[11] Ramakrishna, P., Reddy, G.R.: Cloud-integrated IoT door security system using Arduino and Firebase. J. Ambient Intell. Hum. Comput. 12(9), 9771–9782 (2021)
[12] Gupta, V., Singh, P., Goel, A.: Multi-sensor fusion approach for smart door authentication in IoT environments. IEEE Internet Things J. 9(8), 6473–6484 (2022)

[13] Sutikno, T., Handoko, D., Kurniawan, M.: RFID-based smart lock system using Arduino for low-cost security applications. Int. J. Electr. Comput. Eng. 9(2), 1268–1276 (2019)
[14] Kasim, A., Rahman, M.M., Hussain, S.: Design and implementation of a password-protected door lock system using Arduino and keypad. Int. J. Adv. Comput. Sci. Appl. 11(3), 239–246 (2020)
[15] Qasim, N.H., Rahim, F., Bodnar, N.: A comprehensive investigation of an LTE-enabled smart door system utilising the microcontroller platform UNO. Edelweiss Appl. Sci. Technol. 8(4), 697–708 (2024)
[16] Alkhazali, A.R., Al Moaiad, Y., Farea, M.M., Mohamed, R.R., El-Ebiary, Y.A.B., Jusoh, J.A., Saany, S.I.A.: A different vision of automated door system based on smartphone apps and voice control. J. Pharm. Negative Results 14, 1–8 (2023)
[17] Falohun, A.S., Makinde, B.O., Akin-Olayemi, T.H., Akinleye, F.W., Kehinde, O.P., Oyelami, T.M.: Design and construction of a door security alarm system based on SMS verification and voice recognition. Int. J. Adv. Res. Comput. Sci. 12(3), 45–52 (2021)
[18] Ghazali, T.K., Zakaria, N.H.: Security, comfort, healthcare, and energy saving: A review on biometric factors for smart home environment. J. Comput. 29(1), 189–208 (2018)
[19] Bhattacharjee, A., Samanta, S.: Unlocking the future: Building a smart door lock system with Arduino. In: Adv. Technol. Data Netw. Secur.: Cloud, IoT, pp. 321–330. Springer, Singapore (2023)
[20] Ramakrishna, P., Sachin, K., Rather, I.A., Vandana, M., Sai Vignesh, S.: Smart home security system using Internet of Things (IoT). In: Proc. 14th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT), pp. 1–7. IEEE (2023)
[21] Mohammed, I.R., Arul Jothi, J.A., Syama, K.: A convolutional neural network-based real-time fingerprint recognition for attendance monitoring. In: Proc. 1st Int. Conf. Real Time Intell. Syst., pp. 233–245. Springer, Cham (2023)
[22] Pattnaik, S.K., Samal, S.R., Bandopadhaya, S., Swain, K., Choudhury, S., Das, J.K., Mihovska, A., Poulkov, V.: Future wireless communication technology towards 6G networked IoT environment: An application-based analysis in instantaneous location monitoring using BLE. Sensors 22(9), 3438 (2022)
[23] Ramakrishna, P., Sachin, K., Rather, I.A., Vandana, M., Sai Vignesh, S.: Smart home security system using IoT and cloud connectivity: Performance and security evaluation. IEEE Internet Things J. 11(2), 1435–1448 (2024)
[24] [Banzi, M., Shiloh, M.: Getting Started with Arduino: The Open Source Electronics Prototyping Platform. Maker Media Inc., Sebastopol, CA (2022)
[25] Kumar, P., et al.: EMG–IMU fusion for prosthetic hand control using deep learning. IEEE Trans. Neural Syst. Rehabil. Eng. 31, 1123–1134 (2023). https://doi.org/10.1109/TNSRE.2023.3278901
[26] Al-Rasyid, J., Nawawi, M., Pratiwi, C.P.: The keypad passcode design analysis on smart lock door system IoT-based. J. Teknol. Inf. Pendidik. 16(2), 56–67 (2023)
[27] Bhattacharjee, A., Samanta, S.: Unlocking the future: Building a smart door lock system with Arduino. In: Adv. Technol. Data Netw. Secur.: Cloud, IoT, pp. 321–330. Springer, Singapore (2023)
[28] ghazialpha: Door lock security system using RFID, keypad, I2C LCD 16×2. Arduino Forum (2024). Available at: https://forum.arduino.cc/t/door-lock-security-system-using-rfid-keypad-i2c-lcd-16x2/123456
[29] Kasim, B., Nurdin, H., Sariyusda, S., Ibrahim, A., Razi, M., Ismy, A.S.: Performance analysis of RFID-based smart door lock controlled by Arduino. J. Adv. Res. Appl. Mech. 122(1), 163–174 (2024)
[30] Seeed Studio: Grove – Buzzer. (2022). Available at: https://wiki.seeedstudio.com/Grove-Buzzer/
[31] Wang, Z., Yu, Z., Lou, X., Guo, B., Chen, L.: Gesture-Radar: A dual Doppler radar-based system for robust recognition and profiling of human gestures. IEEE Trans. Hum.–Mach. Syst. 51(1), 32–43 (2020)
[32] CircuitDigest: How to make an RFID door lock system using Arduino. CircuitDigest Microcontroller Projects (2024). Available at: https://circuitdigest.com/microcontroller-projects/how-to-make-an-rfid-door-lock-system-using-arduino