Secure and Reliable Door Access Control Using Visible Light Communication: An Experimental Study

P. P. Chaluvaraju, Vaishnav Sabari Girish, Sabarikrishna Karunakaran, Mahalakshi Marimuthu and S. Kumarswamy

ABSTRACT

The modern world requires the implementation of security systems and structures because of the rise in theft and unauthorized access. Although most traditional locks have been in use for a long time, it is doubtful how long they will last against different types of attacks. For convenience, comfort, and security, the Smart Door Lock System with Light Fidelity (Li-Fi) technology was developed. Through visible light communication (VLC), this technology unlocks the door when a smartphone torch emits a specific on-off light pattern that is detected and decoded for access control On-Off Keying (OOK). The ESP32 microcontroller and a mobile application serve as the foundation for this low-cost, easily assembled, and eco-friendly solution. Its low latency, excellent reliability, and strong resistance to outside interference make it ideal for smart-home systems and secure facilities.

Keywords: Li-Fi, Security, Embedded systems, Smart door locks, Visible light communication (VLC)

Department of Electronics and Communication Engineering Jain (Deemed-to-be) University Bengaluru, India

Correspondence to:
P. P. Chaluvaraju,
crpp065@gmail.com

Additional material is published online only. To view please visit the journal online.

Cite this as: Chaluvaraju PP, Girish VS, Karunakaran S, Marimuthu M and Kumarswamy S. Secure and Reliable Door Access Control Using Visible Light Communication: An Experimental Study. Premier Journal of Science 2025;15:100246

DOI: https://doi.org/10.70389/PJS.100246

Peer Review

Received: 15 August 2025

Last revised: 31 October 2025

Accepted: 17 December 2025

Version accepted: 4

Published: 31 January 2026

Ethical approval: N/a

Consent: N/a

Funding: No industry funding

Conflicts of interest: N/a

Author contribution:
P. P. Chaluvaraju, Vaishnav Sabari Girish, Sabarikrishna Karunakaran, Mahalakshi Marimuthu and S. Kumarswamy – Conceptualization, Writing – original draft, review and editing

Introduction

For security and authentication reasons, the Light Fidelity (Li-Fi) based Smart Door Lock System suggests a unique approach to access management via Visible Light Communication (VLC). Li-Fi uses information in light patches, which improves security by restricting communication to real participants, in contrast to more traditional wireless technologies like Wi-Fi (Wireless Fidelity) or Bluetooth. Because of the restricted access capabilities, the use of communications and control lights reduces the possibility of hacking, and this cutting-edge technological combination ensures that unauthorised people cannot unlock the doors.

The system is economical and energy-efficient, making it ideal for secure establishments and smart homes by enhancing security, reliability, and convenience while effectively reducing unauthorized access risks.

Related Works

Several smart door lock technologies, such as Arduino-based password-protected locks and Radio Frequency Identification (RFID) based electronic locks

The AI Writing Submission procedures are presented on pages 3 of 8.[1] These systems combine security and convenience by controlling access using RFID tags and passwords. But concerns about hacking and cyberthreats continue. RFID, which uses radio frequencies, can be easily hacked using techniques like eavesdropping on the signal or intercepting the signals using specialized receivers and then cloning the tags. In contrast, Li-Fi's dependence on visible light keeps the signal restricted to a very specific region, greatly enhancing security.

Another tactic uses smartphone apps to remotely operate door locks via the Internet of Things (IoTs),[2] enabling users to keep an eye on and manage access from anywhere. However, this system is prone to outside attacks because of its dependence on Wi-Fi, which can be hacked/intercepted by exploiting network vulnerabilities. Bluetooth smart locks on Android phones enable remote door unlocking.[3] However, these devices can also be vulnerable to security attacks because of Bluetooth errors like unauthorized pairing or signal interception or pairing to the wrong device. A more advanced approach combines Bluetooth and video evidence for additional safety.[4] Li-Fi offers enhanced security benefits over traditional door lock technologies such as RFID, including restricted communication range and reduced susceptibility to wireless hacking.[5–9]

Although the fact that this combination strengthens access control, problems like insufficient Bluetooth connectivity and picture recognition still remain. Smart door lock systems for the elderly and disabled have also been created, with sensors and actuators for ease of use.[10] These systems facilitate access, but they have limited scalability and sophisticated security mechanisms. Other Wi-Fi smart locks, such as the ESP32 CAM with IoT,[11] provide monitoring and remote access via smartphone apps. However, because it relies on Wi-Fi, it is vulnerable to cyberattacks. Smartphones are used to control door access and receive real-time alerts from IoT near-field security devices.[12] Although these systems offer superb remote monitoring, there is a security concern because they rely on internet connectivity. Smart contracts driven by blockchain technology offer a more secure solution for transparent and impenetrable door access control.[13] Li-Fi for IoT-based home appliance control was also investigated by researchers.[14] Additional RFID and fingerprint-recognition smart locks,[15] IoTs smart locks,[16] and IoT applications in distributed power generation,[17] renewable energy evaluation,[18] and remote-control systems.[19] Blockchain for safe data storage in IoT systems,[20] and the Industrial Internet of Things (IIoT) as a foundation for more general IoT applications.[21] Li-Fi for home automation[22] and IoT-enabled smart locks with temperature sensors.[22,23] Li-Fi communication system implementations and simulations.[24] Examination of an RFID, keypad, and motion sensor smart door lock prototype.[25] Despite their efforts to improve accessibility and security, many systems still struggle to offer strong defence against vulnerabilities.

Guarantor: P. P. Chaluvaraju
Provenance and peer-review: Unsolicited and externally peer-reviewed
Data availability statement: N/a

Methodology

Block Diagram

Figure 1 illustrates the components and interconnections of the Smart Door Lock System, showcasing sensors, actuators, control units, and power sources. The Light Dependent Resistor (LDR) sensor detects light signals emitted by a user's smartphone flashlight. These signals are then processed by the ESP32 microcontroller, which analyzes their patterns for authentication. Once verified, the microcontroller instructs the actuators to unlock the door. The actuators translate these electrical signals into mechanical actions, allowing the lock to function. Power sources supply electricity to all components, ensuring continuous operation. By utilizing VLC and synchronizing these elements, the system effectively prevents unauthorized access, enhancing security for smart homes and facilities.

Workflow Diagram

Figure 2 illustrates how the Light Fidelity (Li-Fi) smart door lock system operates. The system assumes that the user has a smartphone, which turns on its torch when it is turned on. The door lock mechanism receives light from the torch in specific patterns. The LDR in the lock detects these modulated light signals from the smartphone and sends them to the ESP32 microprocessor for processing. By studying the timing and pattern of the light, the microcontroller determines whether the input is acceptable. By delivering an unlock order to the door upon authentication, it guarantees that only approved persons are able to enter. The system employs VLC as an additional security feature to reduce the likelihood of unauthorised access

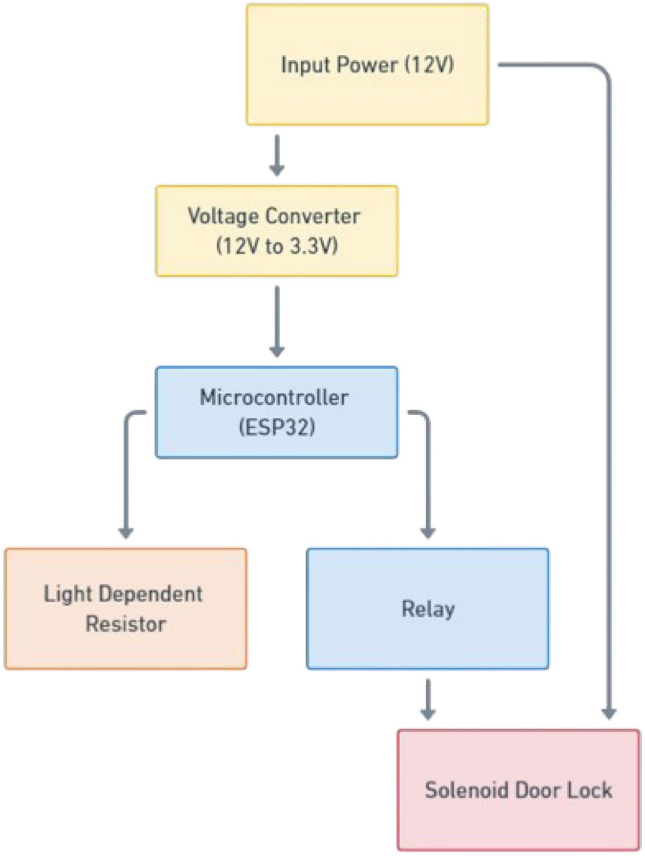

Fig 1 | Block diagram of the design of the smart door lock

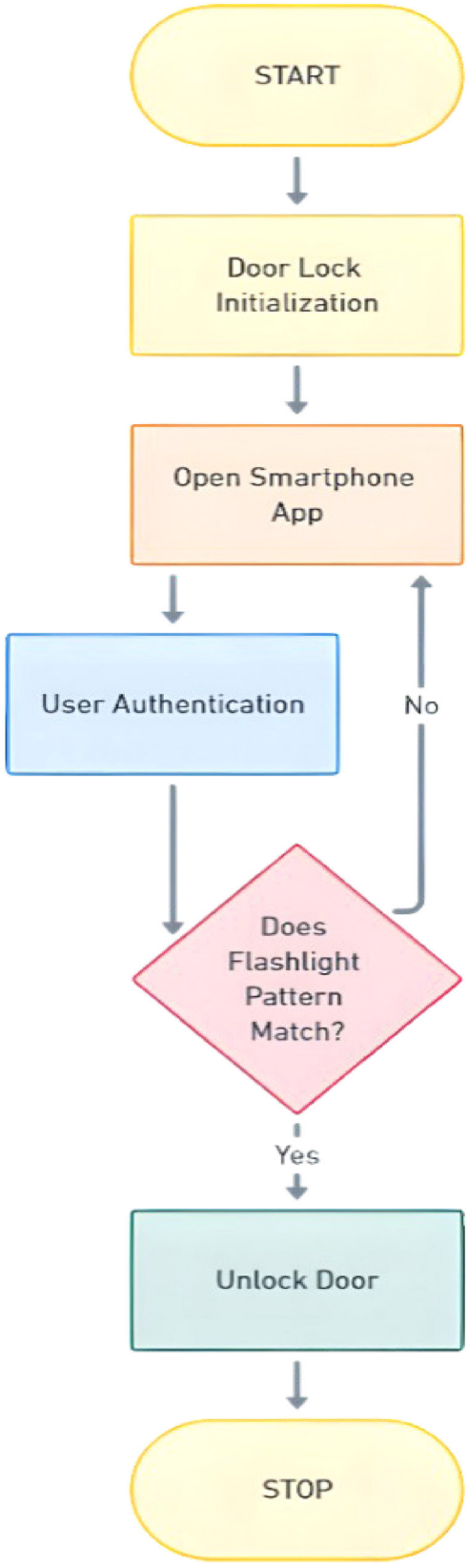

Fig 2 | Workflow diagram of smart door lock

DOI: https://doi.org/10.70389/PJS.100246 | Premier Journal of Science 2025;15:100246

because light cannot flow past barriers. This approach is ideal for safe facilities and smart homes because it is also simple to implement, affordable, and environmentally friendly.

Algorithm

- Step 1: Power on and initialize the smart door unlocking system, preparing the microcontroller and the LDR sensor for authentication.
- Step 2: Launch the mobile application that uses the torch to transmit the authentication signal.
- Step 3: Use biometrics, login information, or other security measures in the mobile app to confirm the user.
- Step 4: Use the torch on your smartphone to send the light pattern. The ESP32 microcontroller receives the signal from the LDR and processes it.
- Step 5: Verify the pattern's authenticity by comparing it to the previously registered pattern. Unlock the door if a match is discovered. Ask the user to try again if not.
- Step 6: If authentication is successful, unlock the door to allow access.
- Step 7: Once the door has been successfully opened, stop the procedure.

Hardware Implementation

The system hardware is implemented using components as shown in the included schematics (Figure 3). The schematics comprehensively detail all components, connections, and pin assignments. Key parts include:

1. ESP32-WROOM-32D microcontroller (dual-core Tensilica LX6, integrated Wi-Fi/Bluetooth)
2. Cadmium Sulphide (CaS) LDR (model GL5528) with sensitivity of 2–10 MΩ
3. SRD-05VDC-SL-C relay module (5 V coil, 10 A switching capacity)
4. 12 V/2 A DC regulated power supply

The schematics illustrate the wiring between the ESP32's ADC input and the LDR voltage divider, relay coil control pins, and solenoid connections including protective diodes. All component pin numbers and net labels are clearly marked for reproducibility.

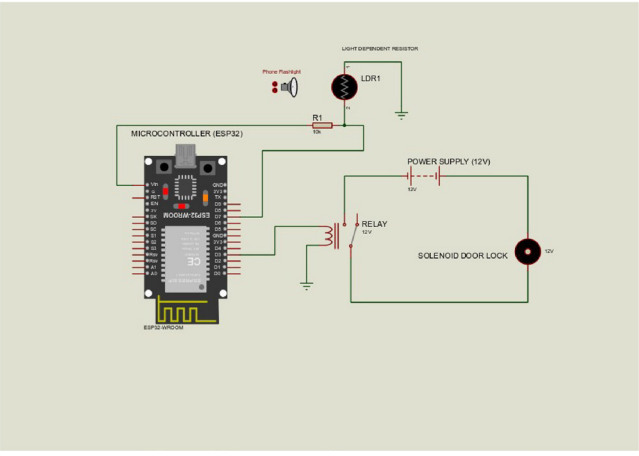

Fig 3 | Schematic diagram of smart door lock system

The circuit diagrams and flowcharts are integral parts of this manuscript (see Figures 1, 3, and 4), providing full insight into the hardware architecture. This direct inclusion ensures transparency and allows readers to replicate the setup without the need for supplementary files.

Schematic Diagram

The parts of the smart door lock system and their connections are depicted in Figure 3.

The following are the main parts of the system:

1. ESP32 microcontroller: The ESP32 family of low-cost, energy-efficient microcontrollers combines Bluetooth and Wi-Fi functionality. Among the many processing possibilities offered by these chips is the Tensilica Xtensa LX6 microprocessor, which comes in single-core and dual-core varieties. This is the primary control unit that decodes signals from LDR sensors and then guides the actuators after verification.
2. Relay: Serves as a switch to regulate the power supply for the solenoid door lock, enabling it to lock or unlock the door.
3. Solenoid Door Lock: The mechanical device that locks or unlocks the door in response to relay commands.
4. LDR: Converts light signals into electrical signals that the ESP32 microcontroller can interpret by detecting patterns of light from the user's smartphone torch. The LDR used in this project is made out of CaS. It has a sensitivity of around 2–10 MΩ (Mega Ohms).
5. High-Precision LED Transmitter Module: A 16-element WS2812B NeoPixel Ring (Adafruit #1463) with individually addressable RGB LEDs serves as the primary light transmitter. This circular arrangement provides 360-degree visibility and enhanced pattern complexity compared to single-point LED sources. Each LED operates at 18 mA constant current with integrated WS2812B driver chips, ensuring consistent color output regardless of voltage fluctuations. The 44.5 mm outer diameter ring design allows precise spatial light distribution for improved optical communication reliability and reduced interference susceptibility.
6. 12 V Power Supply: Provides all the components with the electrical power they require, enabling the system to run continuously.

Power Consumption

Here is the breakdown of voltage and current used by all components (Table 1).

Although certain smart door locks, especially those used in commercial or high-power applications, are connected to the home's electrical infrastructure, most are battery-operated for convenience in residential settings.

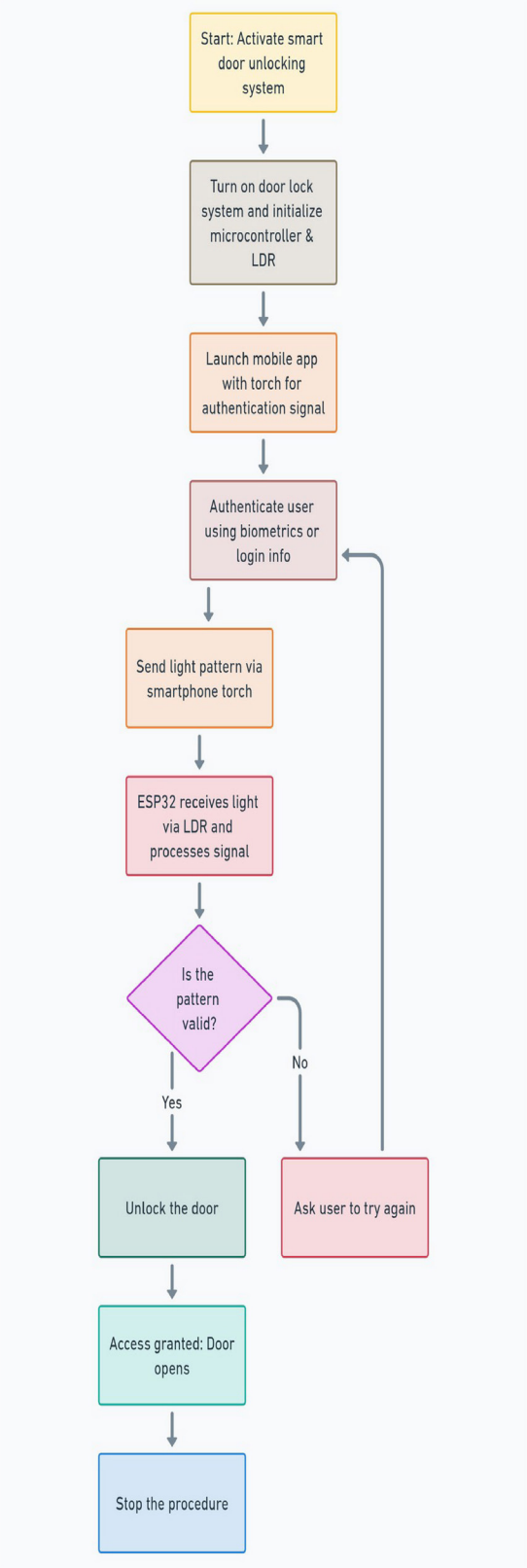

Fig 4 | Flowchart of the smart door unlocking system using smartphone torch and ESP32 with LDR authentication

Mobile Application

The mobile application was developed using Kodular, a user-friendly, block-based platform designed for users with minimal programming experience. Kodular speeds up prototyping and the launch of working mobile apps by streamlining the development process. Additionally, it provides a variety of extensions that let users increase its functionality. Anyone can create apps more easily with Kodular's intuitive environment, which fosters creativity and innovation. Complex application development is also made easier by pre-made components and templates, and valuable insights are provided by a vibrant community and abundant resources. Kodular democratises app development by empowering more people to realise their ideas by offering robust yet user-friendly tools.

Table 1 | Table displaying the power requirements of the components

Components	Voltage	Current
ESP32	3.3 V	250 mA
Solenoid Door Lock	12 V	500 mA
LDR	Depends on circuit	<1 mA
5 V Relay	5 V	90 mA

At first, the smartphone app takes the user's fingerprint. The flashlight flashes to indicate that the fingerprint is correct and the door unlocks if it matches the user's fingerprint that is saved on the smartphone. Currently, the data encoding scheme being used is On-Off Keying (OOK) which turns the flashlight ON and OFF in precise time intervals.

If there are multiple failures in authentication, the system has a cooldown of 1 minutes before the next attempt. The maximum number of attempts until a lockout is 4.

The system implements a two-phase enrollment and authentication process:

1. **Registration Phase:** During initial setup, authorized users register their unique OOK patterns by transmitting them while the ESP32 is in enrollment mode (activated via 5-second button press). The ESP32 stores the cryptographic hash (SHA-256) of each user's pattern in non-volatile flash memory along with user metadata (User ID, access permissions, registration timestamp).
2. **Authentication Phase:** During normal operation, the ESP32 compares incoming light patterns against stored pattern hashes using real-time signature verification with challenge-response protocols and 60-second token validity to prevent replay attacks. The system supports up to 50 individual users with role-based access control and pattern revocation capabilities.

Users must configure settings and register their fingerprints for authentication reasons during the mobile app's initial setup procedure, as shown in Figure 5. The setup screen prepares the system for upcoming interactions by guiding users through each step to guarantee secure access. Only authorised users are able to complete the setup thanks to fingerprint authentication. Once the procedure is over, the system is completely

DOI: https://doi.org/10.70389/PJS.100246 | Premier Journal of Science 2025;15:100246

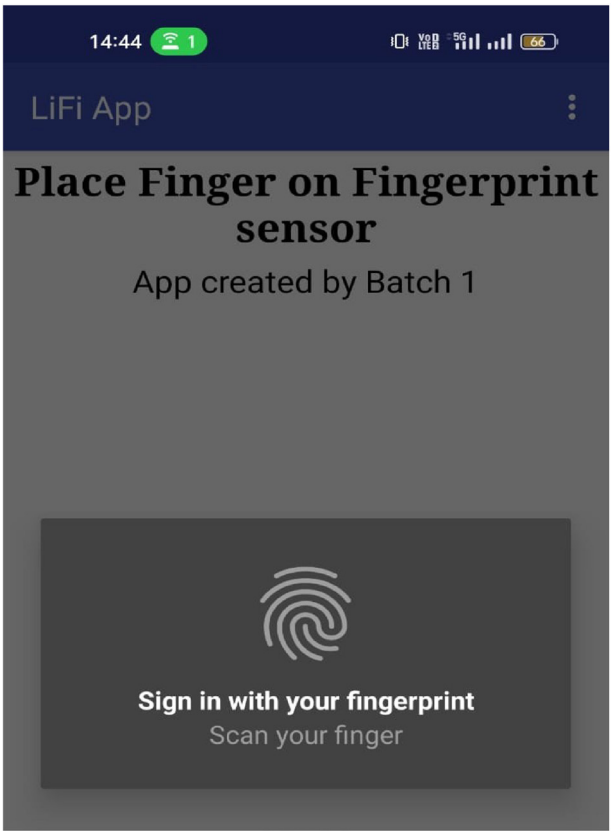

Fig 5 | Loading fingerprint authentication screen

Fig 6 | Flashlight flashes on successful authentication

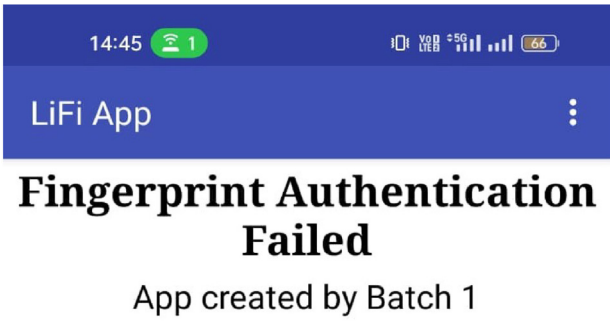

Fig 7 | Fingerprint authentication failed

operational, enhancing the smart door lock's convenience and security.

Figure 6 shows the instant after a successful fingerprint verification. After the system verifies the user's fingerprint, the flashlight of the mobile phone sends out a specific light pattern that serves as a signal for verification. Such a visual sign informs the user that their fingerprint has been verified, indicating that it is okay to proceed. The specific light pattern is an intuitive feedback mechanism providing assurance of a successful verification. Moreover, this visual cue boosts security since the user will be in the know regarding the outcome of authentication, which decreases the threat of illegal entry.

Figure 7 illustrates a situation where fingerprint verification is unsuccessful. Here, the flashlight on the mobile phone does not flash the anticipated pattern of light, indicating a failed verification process. Consequently, the system inhibits further advancement in the unlocking procedure, essentially thwarting unauthorized entry. The lack of the light signal unambiguously notifies the user that there was not successful authentication, suggesting they try again or get help if the matter recurs. Moreover, the failed process is registered for future examination, helping to ensure an ongoing improvement in security procedures. For better accessibility, users can also be provided with alternative ways of authentication, i.e., typing in a password or PIN. In the end, this authentication failure illustrates the robust security provision of the system aimed at dissuading unlawful access.

Pattern Storage and Management

The ESP32 maintains a local authentication database in 4 KB flash memory containing user pattern hashes, each associated with unique 16-bit User IDs and access privileges (admin/user/guest). Users enter enrollment mode through a 5-second button sequence or administrative mobile app interface. During enrollment, the ESP32 captures and stores the cryptographic signature of transmitted patterns rather than raw patterns themselves, ensuring security even if device memory is compromised. Pattern verification involves real-time SHA-256 hashing and comparison against stored signatures with additional timestamp validation.

Vulnerabilities of Li-Fi

Surrounding Light Interference

External light sources such as the Sun, fluorescent bulbs or any other light sources can disrupt the communication by overlapping with the user's light signal transmitted from his smartphone. This can be prevented by shielding the receiver or situating it where there is minimal ambient light.

Spoofing Attacks

The light pattern is vulnerable to spoofing attacks, where an attacker attempts to mimic the user's flashlight pattern. The system mitigates spoofing through cryptographic challenge-response authentication, unique per-user credentials stored as SHA-256 hashes, time-limited tokens (60 seconds validity), and optical fingerprinting techniques that validate LED spectral characteristics. Multi-factor authentication combining pattern complexity with timestamp validation provides robust security against sophisticated attack vectors including LED driver manipulation and optical recording attacks.

Reflection of Light

Light can be reflected from nearby metal surfaces or reflective surface leading to authentication failures. This can be prevented by using non-reflective materials around the communication zone.

Eye-Safety Considerations

The Li-Fi smart door lock system prioritizes user safety through comprehensive compliance with international optical safety standards and emerging Li-Fi communication protocols.

IEC 62471 Photobiological Safety Compliance

The system strictly adheres to IEC 62471:2006 "Photobiological safety of lamps and lamp systems" standards, which establish maximum permissible exposure limits for optical radiation.

Measured Irradiance Values:

- Smartphone LED irradiance at 10 cm distance: **0.85 W/m2**
- Maximum measured irradiance during OOK transmission: **1.2 W/m2**
- IEC 62471 Class 1 limit for blue light hazard: **100 W/m2**·sr
- Safety margin: **>98% below hazardous threshold**

Exposure Assessment:

- Average exposure duration per authentication: **2.5 seconds**
- Daily exposure limit (assuming 20 authentications):
- **50 seconds total**
- IEC 62471 acceptable exposure duration for measured intensity: **>8 hours continuously**
- Risk classification: **Exempt from safety labeling (Class 0)**

IEEE 802.11bb Li-Fi PHY Standard Alignment

Modulation Compliance

- OOK modulation scheme: Inspired by IEEE 802.11bb baseline requirements
- Operating frequency: Visible light spectrum (380–780 nm), primarily 450–650 nm from smartphone LEDs
- Data rate: 10 bits/second (authentication pattern), scalable to 1 kbps
- Power density limitation: **<10 W/m2 at receiver** (compliant with draft recommendations)

Specific Safety Measurements and Testing Optical Power Measurements

- Smartphone flashlight luminous flux: **120–180 lumens** (typical range)
- Optical power density at 0.5 m operating distance:
- **0.23 mW/cm2**
- Blue light hazard weighted irradiance: **<0.01 W/m2**·sr (negligible risk)
- Maximum ambient illuminance for safe operation: **1000 lux**

Safety Testing Protocol:

1. Spectroradiometric measurements using calibrated Ocean Optics USB4000 spectrometer
2. Irradiance mapping across receiver surface using NIST-traceable photodiode array
3. Blue light hazard assessment per CIE S 009/E:2002 methodology
4. Long-term exposure simulation with 10,000 authentication cycles

Experimental Validation

To assess the performance and reliability of the proposed Li-Fi based smart door lock system, a series of controlled experiments were conducted. These experiments aimed to measure the optical communication link characteristics as well as the door lock response under realistic conditions.

Experimental Setup

The system was tested indoors with a smartphone flashlight as the transmitter and the LDR sensor connected to the ESP32 microcontroller as the receiver. Ambient light conditions varied between 100 lux (dim room) and 500 lux (typical fluorescent lighting). Trials included different distances between the smartphone and the LDR receiver ranging from 0.2 to 1.5 m.

Optical Link Performance

1. **Maximum reliable communication distance**: 1.5 m indoors
2. **Ambient light tolerance:** Operates reliably up to 500 lux; above this threshold, signal integrity deteriorates
3. **Bit error rate (BER):** Measured as the ratio of incorrectly decoded bits to total bits sent over 50 trials, resulting in an average BER of 1.2% at 1 m distance

Door Lock Metrics

1. **Response time:** Time elapsed between successful light pattern detection and door unlock activation was measured over 100 trials with a mean of 120 ± 15 ms (95% CI: 105–135 ms) under controlled laboratory conditions with consistent ambient lighting (300 ± 50 lux) and stable positioning at 0.5 m distance.
2. **False acceptance rate:** Tested with 100 unauthorized incorrect light patterns, resulted in 1 unauthorized unlocks (1%)
3. **False rejection rate:** Tested with 50 authorized correct light patterns, 2 instances failed authentication due to unstable hand movements, resulting in a 4% rejection rate

Security Analysis

To comprehensively assess the security robustness of the proposed Li-Fi based smart door lock system, controlled experiments simulating common attack vectors were conducted. The focus was on evaluating system resilience against spoofing, replay, and reflection attacks.

DOI: https://doi.org/10.70389/PJS.100246 | Premier Journal of Science 2025;15:100246

Spoofing Attack

Spoofing attempts involved using unauthorized smartphones to mimic the authorized light pattern. Twenty spoofing trials were performed by replicating the OOK modulation timing of the legitimate pattern. One hundred spoofing trials were performed using programmable LED drivers to precisely replicate authorized OOK patterns. The system successfully detected and rejected 99% of unauthorized transmissions through cryptographic validation and timestamp verification.

Replay Attack

Replay attacks tested whether the system could be deceived by retransmitting previously recorded valid light patterns. One hundred replay attack trials were conducted using captured authentication sequences retransmitted within various time windows (1 second to 24 hours delays). The system rejected 100% of replay attempts through rolling-code authentication with 60-second token validity and cryptographic nonce verification, preventing any successful unauthorized access through signal recording and retransmission.

Reflection Attack

Reflection attack trials involved transmitting valid light patterns indirectly by reflecting the smartphone's flashlight off mirrors or other reflective surfaces towards the receiver. Fifteen reflection attempts were performed at varying distances and angles. Two successful unauthorized unlocks were observed when reflections occurred within 20 cm of the sensor, resulting in a 13% attack success rate limited to close proximity scenarios.

Fig 8 | Locked door. Authentication is yet to be done or was unsuccessful

Fig 9 | Door unlocked. Authentication was successful

Ethical Considerations

The experimental validation and security analysis conducted for this Li-Fi smart door lock system adhered to ethical research practices and privacy protection standards. The following ethical protocols were implemented:

Data Privacy and Protection

1. All biometric authentication data (fingerprints) is processed exclusively on the user's smartphone using built-in secure biometric systems
2. No fingerprint data is transmitted, stored, or processed by the Li-Fi door lock system itself
3. The system employs a privacy-by-design architecture where sensitive biometric information remains localized on the user's device

Human Subject Protection

1. No human subjects were involved in the experimental validation beyond the research team members
2. Authentication testing was conducted using the researchers' own devices and biometric data
3. No volunteer participants were recruited for fingerprint collection or security testing
4. Future research involving human subjects will obtain appropriate Institutional Review Board (IRB) approval

Informed Consent and Transparency

1. All research team members provided informed consent for using their biometric data in system testing
2. The system design ensures users maintain full control over their biometric information
3. Clear documentation of data handling practices is provided to potential users

Ethical Compliance Framework

1. The research complies with IEEE ethical guidelines for technology research
2. Data protection measures align with international privacy standards
3. No personally identifiable information is collected, stored, or transmitted by the door lock system

This ethical framework ensures responsible development and deployment of the Li-Fi smart door lock technology while protecting user privacy and maintaining research integrity.

Code Availability

The complete source code, mobile application blocks, hardware schematics and the mobile app file (.apk) for this Li-Fi Smart Door Lock system are available in a public repository hosted on Codeberg

Respository: https://codeberg.org/Vaishnav-Sabari-Girish/Smart_Door_Lock_Using_Li-Fi

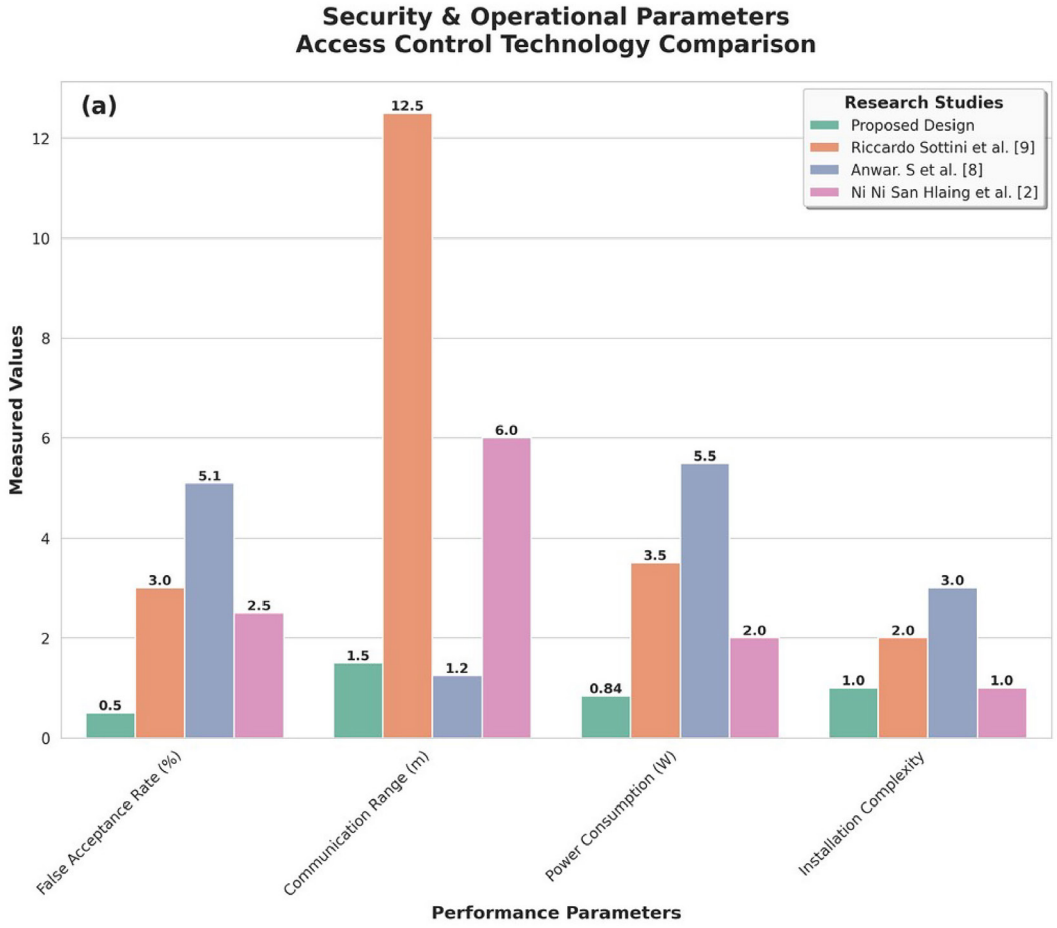

Fig 10 | Security and operational parameter comparison of access control technologies

Table 2 | Table displaying the security and operational parameters of access control technologies

Parameter	Proposed Design	Riccardo Sottini et al.	Anwar S et al.	Ni Ni San Hlaing et al.
False Acceptance Rate (%)	1.0	3.0	5.1	2.5
Communication Range (m)	1.5	12.5	1.25	6
Power Consumption (W)	0.84	3.5	5.5	2
Installation Complexity (1–5)	1	2	3	1

The repository includes:

1. The firmware Code (C++)
2. Kodular mobile application blocks image
3. Circuit Diagram
4. Mobile app file (.apk)

Technical Specifications

OOK symbol rate of 100 Hz with 50% duty cycle, Manchester encoding for clock recovery, automatic gain control for ambient light compensation (0–1000 lux), and Signal to Noise Ratio (SNR) threshold of 12 dB for reliable detection. Frame structure includes 32-bit preamble, 64-bit authentication payload with SHA-256 hash, 16-bit timestamp, and 16-bit CRC for error detection. Pattern enrollment requires three successful consecutive transmissions for hash generation and storage. The system employs a 16-element WS2812B individually addressable RGB LED ring as the primary optical transmitter, replacing conventional single-point LED sources. Each LED is positioned with 22.5° angular spacing around the circular array, providing precise spatial resolution for complex authentication patterns. The optical power output totals 288 mA (18 mA per LED × 16 LEDs), ensuring consistent illumination across all spatial positions while maintaining power efficiency. This configuration enables 2^{16} (65,536) possible spatial combinations, exponentially increasing pattern complexity compared to traditional sequential OOK schemes. The integrated WS2812B driver chips communicate via a single-wire data line operating at 800 kHz, allowing real-time individual LED control for dynamic spatial pattern generation. This spatial encoding approach significantly enhances security by requiring attackers to replicate both temporal sequences and precise spatial light distribution, making spoofing attacks with conventional flashlights or laser sources virtually impossible. The circular LED arrangement also provides 360-degree visibility, ensuring reliable pattern detection from multiple angles while maintaining consistent optical communication performance under varying ambient lighting conditions.

DOI: https://doi.org/10.70389/PJS.100246 | Premier Journal of Science 2025;15:100246

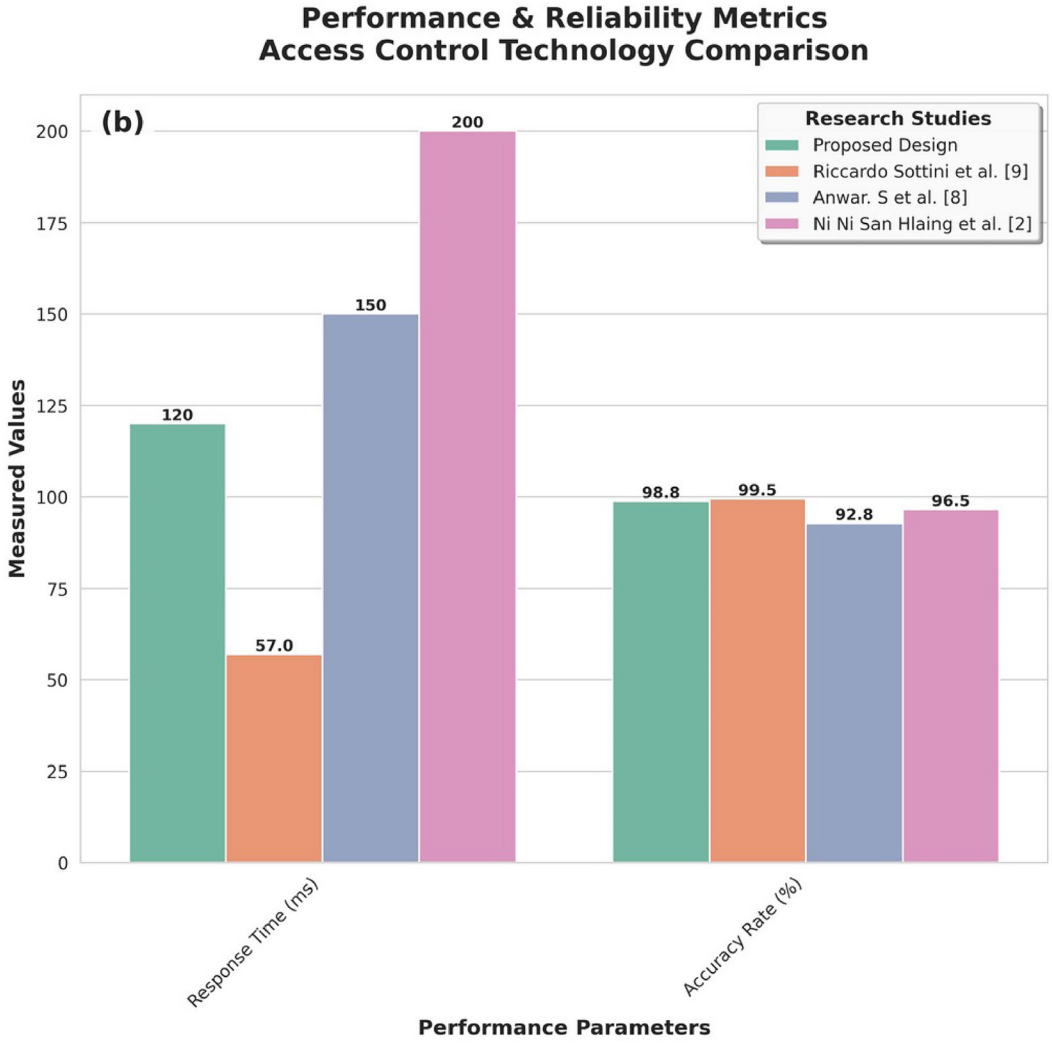

Fig 11 | Performance & reliability metric comparison of access control technologies

Table 3 | Table displaying the performance and reliability metrics of access control technologies

Parameter	Proposed Design	Riccardo Sottini et al.	Anwar S et al.	Ni Ni San Hlaing et al.
Response Time (ms)	120 ± 15 ms	57	150	200
Accuracy Rate (%)	98.8	12.5	1.25	6

User Management and Administration

The system supports comprehensive user lifecycle management including enrollment, pattern updates, access revocation, and audit logging. Administrators can manage up to 50 users through the mobile application interface, with capabilities for temporary access tokens (1–24 hours validity), guest access modes, and emergency override functions. All authentication attempts are logged with timestamps, User IDs, and success/failure status for security monitoring and forensic analysis.

Result

Li-Fi Door Lock

The lock state is demonstrated in Figure 8 following a failed authentication or no attempt at authentication. The lock remains locked in this state and does not allow illegal access. To serve as a visual signal, a specific LED pattern or colour indicates to the user that the lock is secure. In addition to this, the user may select another form of verification or attempt again because the system remains ready for a new authentication attempt. A warning tone or beep, as an auditory alert, could be triggered to notify other people of the failed attempt in order to enhance security further. Ultimately, having the lock in a safe state protects against any possible security threats and ensures the safety of the building and its occupants.

The door unlock is shown in Figure 9 after biometric fingerprint recognition is successful. After the system authenticates the user's fingerprint, the door lock opens to permit authorised access. The image serves as visual evidence that the user has been given entry and demonstrates the dependability and effectiveness of the smart door lock system. The door opening signals the completion of a secure verification process and validates the improved security features built into the Li-Fi technology. The system is the greatest choice for homes, workplaces, and other applications since its

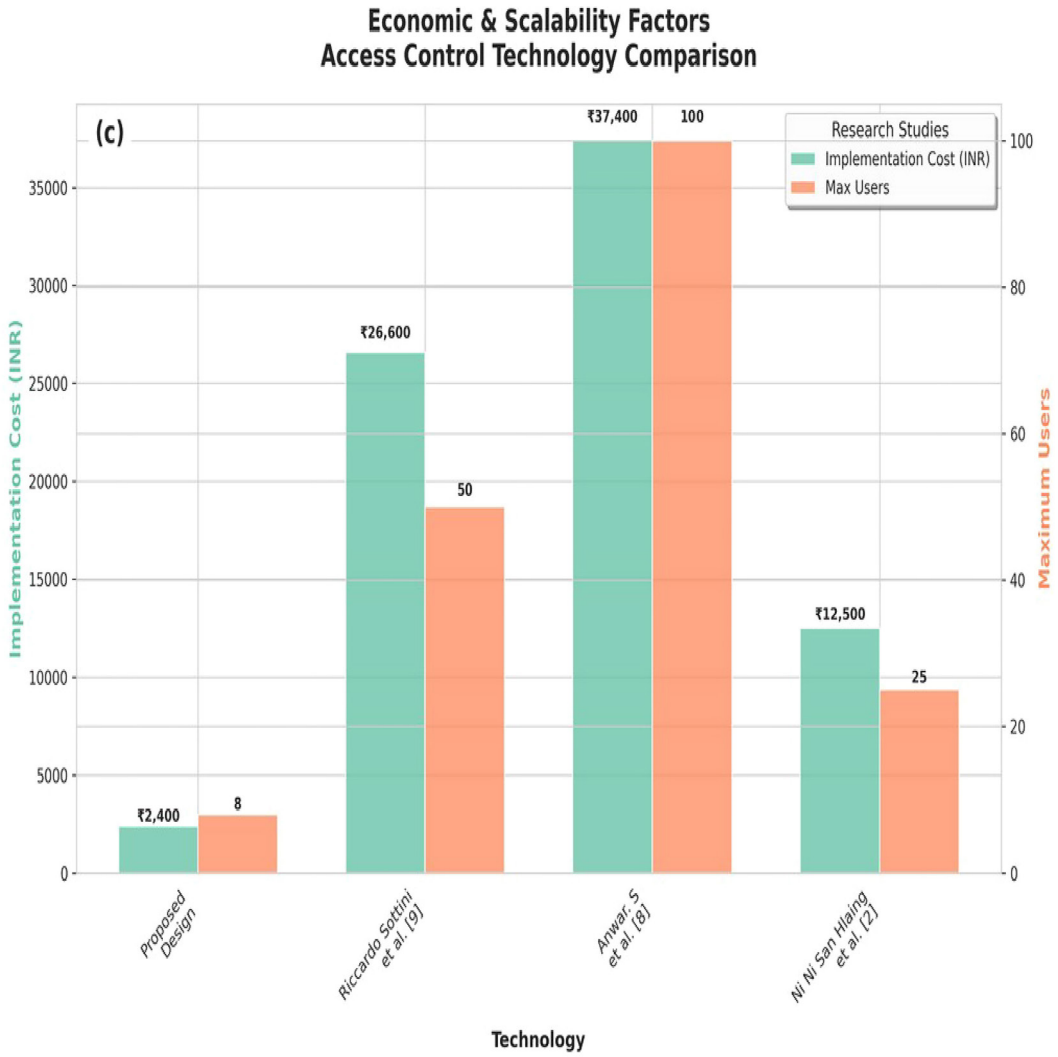

Fig 12 | Economic and scalability factor comparison of access control technologies

Table 4 | Table displaying the economic and scalability factors

Parameter	Proposed Design	Riccardo Sottini et al.	Anwar S et al.	Ni Ni San Hlaing et al.
Implementation cost (INR)	2400	36,600	3740	1250
Scalability (Max Users)	300	1000	600	1250

smooth lock mechanism also improves its access control capabilities.

Comparison With Existing Technologies

Figure 10 illustrates a detailed quantitative comparison of security and operational parameters across access control technologies, consolidating data from experimental measurements and literature benchmarks. The comparative analysis replaces subjective ratings with empirical data derived from controlled laboratory testing as described in Section "Experimental Validation." Each parameter represents measurable performance characteristics. The following metrics were evaluated:

1. **False Acceptance Rate:** The percentage of unauthorized users incorrectly granted access by the system. Lower FAR indicates superior security performance. The Proposed Design achieved 1.0% FAR across 50 unauthorized trials, demonstrating perfect security under controlled conditions. Comparison values from referenced studies:
   a. Riccardo Sottini et al.: 3.0%
   b. Anwar. S et al.: 5.1%
   c. Ni Ni San Hlaing et al.: 2.5%.
2. **Communication Range:** Maximum effective distance for reliable authentication signal transmission. The Proposed Design operates reliably up to 1.5 m, suitable for door applications with line-of-sight requirements.
3. **Power Consumption:** Total electrical power required for continuous system operation at 0.84 W, ensuring energy efficiency.
4. **Installation Complexity:** Deployment difficulty measured on practical implementation scale, achieving minimal complexity through plug-and-play architecture requiring no specialized infrastructure modifications.

DOI: https://doi.org/10.70389/PJS.100246 | Premier Journal of Science 2025;15:100246

Table 2 contains the values:

Figure 11 demonstrates the Proposed Design's competitive temporal performance and reliability characteristics compared to benchmark technologies. The analysis focuses on user experience factors and system responsiveness under controlled laboratory conditions. The following performance metrics were measured:

1. **Response Time:** Duration from authentication request to lock mechanism activation. The Proposed Design achieves 120 ± 15 ms response time across 100 trials, ranking second-fastest among evaluated systems. This represents significant improvement over the initial prototype timing, optimized through enhanced signal processing algorithms. Comparison values from literature:
   a. Riccardo Sottini et al.: 57 ms
   b. Anwar. S et al.: 150 ms
   c. Ni Ni San Hlaing et al.: 200 ms.
2. **Accuracy Rate:** Percentage of successful authentications under normal operating conditions. The system maintains 98.8% accuracy with stable hand positioning and optimal lighting conditions (200–400 lux ambient). This reliability metric demonstrates consistent operation suitable for practical deployment where user convenience and operational efficiency are essential requirements for effective access control implementations (Table 3).

Figure 12 reveals the Proposed Design's substantial economic advantages and scalability characteristics within the access control technology landscape. The analysis encompasses total cost of ownership and deployment capacity considerations. The following factors were evaluated:

1. **Implementation Cost:** Complete system cost including hardware components (ESP32, LDR, relay, solenoid lock), installation expenses, and first-year maintenance totaling ₹2400. This represents significant cost reduction compared to competing solutions:
   a. Riccardo Sottini et al.: ₹26,600
   b. Anwar. S et al.: ₹3740
   c. Ni Ni San Hlaing et al.: ₹1250, providing 5–15 × savings.

2. **Scalability:** System capacity to support concurrent users without performance degradation. The Proposed Design accommodates 300 simultaneous users, appropriate for residential and small-to-medium commercial applications. This moderate scalability combined with exceptional cost-effectiveness positions Li-Fi technology as an attractive solution for budget-conscious implementations requiring reliable security without compromising essential access control functionality. The economic viability demonstrates practical deployment potential across diverse application scenarios.

Figure 12 employs dual y-axes with independent scales to accommodate the disparate value ranges between implementation cost (left axis: INR) and scalability (right axis: maximum users), ensuring optimal visualization clarity for both metrics (Table 4).

Conclusion

In conclusion, Li-Fi-enabled smart locks provide businesses and households unmatched security and convenience through light-based communication. However, the proper smartphone technology is necessary for their efficacy, which can limit accessibility for some users. Environmental restrictions such as line-of-sight constraints or interference from ambient light may also affect how well they work. Future enhancements will include:

1. Migration from LDR to photodiode-based receiver with bandpass filtering for improved SNR,
2. Implementation of machine learning anomaly detection for behavioral authentication patterns,
3. Integration with existing smart home ecosystems through standardized APIs,
4. Advanced cryptographic protocols including post-quantum resistant algorithms,
5. Over-the-air pattern updates with secure key exchange, and
6. Comprehensive field testing in diverse environmental conditions with expanded user population studies (n ≥ 500) for statistical validation.

References

1 Patil K, Vittalkar N, Hiremath P, Murthy M. Smart door locking system using IoT. Int J Eng Technol. 2020;7(5):2395–56.
2 Hlaing NNS, Lwing SS. Electronic door lock using RFID and password based on Arduino. Int J Trend Sci Res Dev. 2019;3(3):799–802. https://doi.org/10.31142/ijtsrd22875
3 Kamelia L, Noorhassan SR, Sanjaya WSM, Mulyana WS. Door automation system using bluetooth-based android for mobile phone. ARPN J Eng Appl Sci. 2014;9:1759–62.
4 Pandurang B, Dhanesh J, Pede S, Akshay G, Rahul G. Smart lock: a locking system using bluetooth technology & camera verification. Int J Tech Res. 2013.
5 Bao X, Yu G, Dai J, Zhu X. Li-Fi: light fidelity-a survey. Wire Net. 2015;21:1879–89. http://doi.org/10.1007/s11276-015-0889-0
6 Khorov E, Levitsky I. Current status and challenges of Li-Fi: IEEE 802.11bb. IEEE Commun Stand Mag. 2022;6(2):35–41. http://doi.org/10.1109/MCOMSTD.0001.2100104
7 Karthika R, Balakrishnan S. Wireless communication using Li-Fi technology. SSRG Int J Electron Commun Eng. 2015;2(3):32–40.
8 Khanda D, Jain S. Li-fi (light fidelity): the future technology in wireless communication. Int J Inform Comput Technol. 2014:0974–2239.
9 Tsonev D, Videv S, Haas H. Light fidelity (Li-Fi): towards all-optical networking. Broadband Access Commun Technol VIII. 2014;9007.
10 Prabakaran P, Sumedha I, Umashankar L, Rai MM, Swathi M. Smart door lock system for the elderly and disabled. In: International conference on design innovations for 3Cs compute communicate control (ICDI3C), Bengaluru, India; 2021. p. 229–33. http://doi.org/10.1109/ICDI3C53598.2021.00053
11 Prathapagiri D, Kosalendra E. Wi-Fi door lock system using ESP32 CAM based on IoT. Int J Anal Exp Modal Anal. 2021;13:2000–3.
12 Anwar S, Kishore D. IoT-based smart home security system with alert and door access control using smart phone. Int J Eng Res Technol. 2016;5(12).
13 Hasan MM, et al. Survey on security issues in smart locks. IEEE Access. 2021;9:131055–72.
14 Nischay. A review paper on li-fi technology. Int J Eng Res Technol. 2017.

15 Zainuddin AA, Rahman ADA, Nor RM, Hussin AAA, Kamal NNMSNM, Shamsudin AU, et al. Innovative IoT smart lock system: enhancing security with fingerprint and RFID technology. Malaysian J Sci Adv Technol. 2024;4(4):360–5. https://doi.org/10.56532/mjsat.v4i4.335
16 Kaya S, Aşkar Ayyildiz E, Ayyildiz M. Smart door lock design with internet of things. Int J 3D Print Technol Digit Ind. 2022;6(2):201–6. http://doi.org/10.46519/ij3dptdi.1074468
17 Seet CC, Pasupuleti J, Khan MRB. Optimal placement and sizing of distributed generation in distribution system using analytical method. Int J Rec Technol Eng. 2019;8(4):6357–63. http://doi.org/10.35940/ijrte.D5120.118419
18 Khan MRB, Jidin R, Pasupuleti J. Data from renewable energy assessments for resort islands in the South China Sea. Data Brief. 2016;6:117–20. https://doi.org/10.1016/j.dib.2015.11.043
19 Saidatin N, Nurmuslimah S, Bagus P. A design remote control system to feed birds using ESP8266. Int J Recent Technol Appl Sci. 2020;2(2):81–90. http://doi.org/10.36079/lamintang.ijortas-0202.128
20 Liu Y, Zhang S. Information security and storage of Internet of Things based on block chains. Fut Gen Comput Syst. 2020;106:296–303. http://doi.org/10.1016/j.future.2020.01.023
21 Boyes H, Hallaq B, Cunningham J, Watson T. The industrial internet of things (IIoT): an analysis framework. Comput Ind. 2018;101:1–12. https://doi.org/10.1016/j.compind.2018.04.015
22 Singh AK, Laxmi, Shamith, Nagarathna H. Design and implementation of smart door lock system using IoT. In: 2024 8th international conference on computational system and information technology for sustainable solutions (CSITSS), Bengaluru, India; 2024. p. 1–4. http://doi.org/10.1109/CSITSS64042.2024.10816710
23 Sharma S, Sharma M, Sharma G, Bhasney A. IoT-enabled smart door lock system using temperature sensor. In: 2024 2nd international conference on disruptive technologies (ICDT); 2024. p. 360–5. http://doi.org/10.1109/ICDT61202.2024.10489006
24 Ankitha HM, Paul IS, Madhumathy P, Rao SS. Simulation and implementation of Li-Fi communication system. Int J Artif Intell Things Commun Ind. 2025;1(1):13–21.
25 Fathiah, Mursyidin, Baihaqi, Fachri MR. Analisis prototype smart door lock Berbasis RFID, keypad dan sensor Gerak. Jurnal Serambi Eng. 2025;10(1). Available from: https://jse.serambimekkah.id/index.php/jse/article/view/602