



---

## Development of a Solar-Powered Autonomous Door Lock System

\*Nwaokocha, C., Layeni, A., Omale, E., Ajani, E., Nasamu, E., Poheto, D., & Agboola, T.

Clean Energy Research Group, Department of Mechanical Engineering, Olabisi Onabanjo University, Ago-Iwoye, Nigeria

\*Corresponding author email: [collinsnwaokocha@oouagoiwoye.edu.ng](mailto:collinsnwaokocha@oouagoiwoye.edu.ng)

---

### Abstract

This paper describes the design, development, and installation of a smart door lock for an administrative office. There were some persistent issues with traditional door lock systems in institutional settings. It includes the inability to access audit history, the susceptibility to duplication, and the absence of flexible and continuous authentication choices. The system combines biometric identity, intelligent automation, and sustainable energy to provide a single access control solution. Using an R307 optical fingerprint sensor with a facial recognition module powered by a Deepface library and a 4x4 matrix keypad for PIN-based security entry with flexible multimodal access, the system was built around a Raspberry Zero Was the core controller. There is a provision of physical actuation by a 12V solenoid lock, and the autonomous and sustainable off-grid energy source is powered by a solar energy system. The system performance was evaluated in a real-world environment with different lighting and weather conditions taking into consideration. With 94% accuracy for fingerprint recognition, 85% reliability for facial recognition in typical illumination, and 100% accuracy for keypad entry, all authentication choices answered in less than three seconds. In line with Sustainable Development Goals 9 and 11 as well as one of the ideas of the Fourth Industrial Revolution, the work offers an adaptable, multimodal, and energy efficient access control system.

---

**Keywords:** Access control, Solar power, Biometrics, Internet of Things, Energy, Environment

---

### Introduction

Security of official spaces in an institutional or academic environment remains a critical concern, as it serves as a safeguard for institutional resources, intellectual property, and personal safety. Any breach of such spaces can lead to reputational damage, significant operational disruption, and financial loss. Hence, the need to reduce or eliminate the risks of unauthorized access, compromise of confidential information and outright theft, and unauthorized duplication, which provided no means for real time monitoring and remote control. Through cost effective and popular, serious limitations exists like keys has been lost, stolen, or duplicated without detection, and compromised which may go unnoticed after a breach that has happened (Gupta & Johari, 2019; Mahajan et al., 2019; Lin et al., 2021). Lock systems with passwords offer some improvement, except that password can be guessed, observed, should surfed, or shared inappropriately resulting in limited security for sensitive administrative offices (Lakshmi, et al., 2017; Patil et al., 2026). Recent progress of Internet of Things (IoT), biometric authentication, and renewable energy have provided a new generation of smart door lock systems that combine security, user convenience, and operational sustainability, allowing for multi-factor authentication with remote monitoring and data driven decision making, thus addressing the vulnerabilities of traditional locks (Dharme et al., 2022; Nassirudin et al., 2018). The lock systems that are enabled with Internet of Things communicate with mobile or cloud platforms for control and notifications while integrating RFID, facial recognition, fingerprint sensors, and entry (Nayak et al., 2026). Nevertheless, a number of existing solutions have specific shortcomings which includes the following; dependance on grid power, vulnerability to

communication issues, environmental sensitivity of biometric sensors, and limited compatibility with existing door hardware.

In short, this work details the design, development, and practical implementation of a solar powered door lock system produced for the Head of Mechanical Engineering Department office at Olabisi Onabanjo University, Ibojun Campus, Nigeria. The system was installed on an existing office door and it is based on a Raspberry Pi Zero platform. It offers various authentication options which are; fingerprint, facial recognition, and keypad PIN. In addition to these features, it uses a Telegram based contributions of this work are as follows:

1. Design and implementation of a multi modal authentication architecture integrating facial recognition, keypad entry, fingerprint scanning, and Telegram alerts on a low embedded platform.
2. Real world deployment on an existing office door, including mechanical integration, sensor placement, and power management using a dedicated solar energy system.
3. Experimental evaluation of authentication accuracy, environmental robustness, response time, and user experience, compared against performance reported in related smart lock literature.
4. Discussion of how the system supports Sustainable Development Goals and Fourth Industrial Revolution in an Institutional contexts.

## Literature Review

Recent door lock systems have evolved from simple mechanical mechanisms to integrate cyber physical systems leveraging IoT, biometrics, and machine learning to improve usability and security.

Modern access control systems have been facilitated by Internet of Things (IoT) technology. This is achieved by activating remote monitoring, real time alerts, and automatic authentication mechanisms. Smart locks that are IoT based integrate wireless communication with hardware and cloud connectivity. This allows users to gain access and control doors remotely. With the adoption of Raspberry Pi, real time surveillance and remote monitoring are provided by smart surveillance security systems that integrate Webcam and network connectivity to capture images of visitors and transmit alerts to authorized users. Such systems validate how low-cost technologies can improve security in homes and administrative facilities (Mahesh et al., 2019). Similarly, IoT enabled access system can incorporate communication modules such as the GSM to notify users of door activity and wireless messaging technologies can send lock status updates and intrusion alerts to authorized users (Hussein & Al Mansoori, 2017; Nayak et al., 2026; Nwankwo et al., 2013).

Biometric authentication has become a key component of modern access control systems due to its ability to uniquely identify individuals based on psychological characteristics, in particular fingerprint and facial recognition. It also has higher resistance to credential theft as compared to physical keys or static passwords. Due to its high accuracy, dependability, and simplicity of use, fingerprint identification continues to be one of the most used methods (Zainuddin et al., 2024). For example, Nasirrudin et al. (2018) showed how fingerprint sensors can be integrated with IoT based systems to allow for centralized access management. This technique increases system flexibility, particularly in environments where access privileges are always shifting. Conversely, facial recognition technology is used to enable contactless user authentication. Kumar and Kumari (2020) implemented a face recognition-based access system, they highlight its usefulness and flexibility for hands free operation. However, facial recognition systems are vulnerable to environmental factors like lighting conditions and changes in user locations or angles. Which in turn affect detection accuracy unlike fingerprint-based methods. Overall, even while fingerprint and facial recognition technologies have many advantages for smart security systems. Their individual disadvantages highlight the need for multimodal biometric systems that combine several authentication methods to boost reliability and resilience.

In smart security, systems that uses several layers of authentication are becoming more popular because they overcome the weaknesses of just relying on just one method. These systems combine different ways to verify identity such as biometrics, passwords or Radio Frequency Identification (RFID) with the aim of minimizing the effects of single point method failures and prevention of unauthorized access. Dharme et al., (2022) in their study, developed an access

control for facilities such as libraries and tolerates using multifactor authentication framework. The developed system included a biometric verification from mobile application, demonstrated an improved system security and flexibility in user authentication. For a more security efficiency, Hamas et al., (2021) adopted the use of a SMS security pass code to be sent to the authorized user. The system is designed to flag a several wrong code attempts and suspicious human activities around the door. With this type of hybrid method, failures that comes from a single authentication method can be minimized in order to ensure a more efficient security system. These systems also feature alternative access options for users, where users can choose which option is most preferable, this making the technology more versatile. However, integrating multiple authentication techniques into the system may be responsible for problems such as increased system complexity, higher computational requirements, and potential latency in real time operation. Therefore, for a more efficient multimodal authentication system, recent research has focused balancing security, computational cost, and user convenience, especially for embedded platforms such as Raspberry Pi based smart security systems.

Integrating renewable energy sources into smart security systems is becoming more and more popular as the world economy continues the search for more sustainable and efficient way to control access. This can be accomplished using a method of energy harvesting from sliding doors in which the system harvest energy from the door's rotational motion. Hamas et al., (2021) created a system that used rechargeable batteries to store the energy produced by micro DC generators that were connected to a sliding door via a roller and gear mechanism. However, there are still challenges in developing security systems that can run solely on renewable energy, making further study a necessity. Multi user access control, real time monitoring, backup systems, modular scalability, and energy efficient operation are just a few of the characteristics found in contemporary smart lock solutions. While access records facilitate auditing and forensics, real time alerts via GSM or internet based messaging offer prompt feedback on lock state and access attempts. Even so, there are still issues with the state of the art systems, such as the need for reliable network access, the vulnerability of biometric modules to environmental factors, the expense of hardware and installation, and usability issues for users with little technical expertise.

Targeting a particular institutional use case in an academic office, the system created in this work expands on these trends by combining multi-modal authentication, local edge processing of biometric data on a Raspberry Pi, and a solar-based power supply to lessen reliance on grid electricity.

## Materials and Method

### System Overview

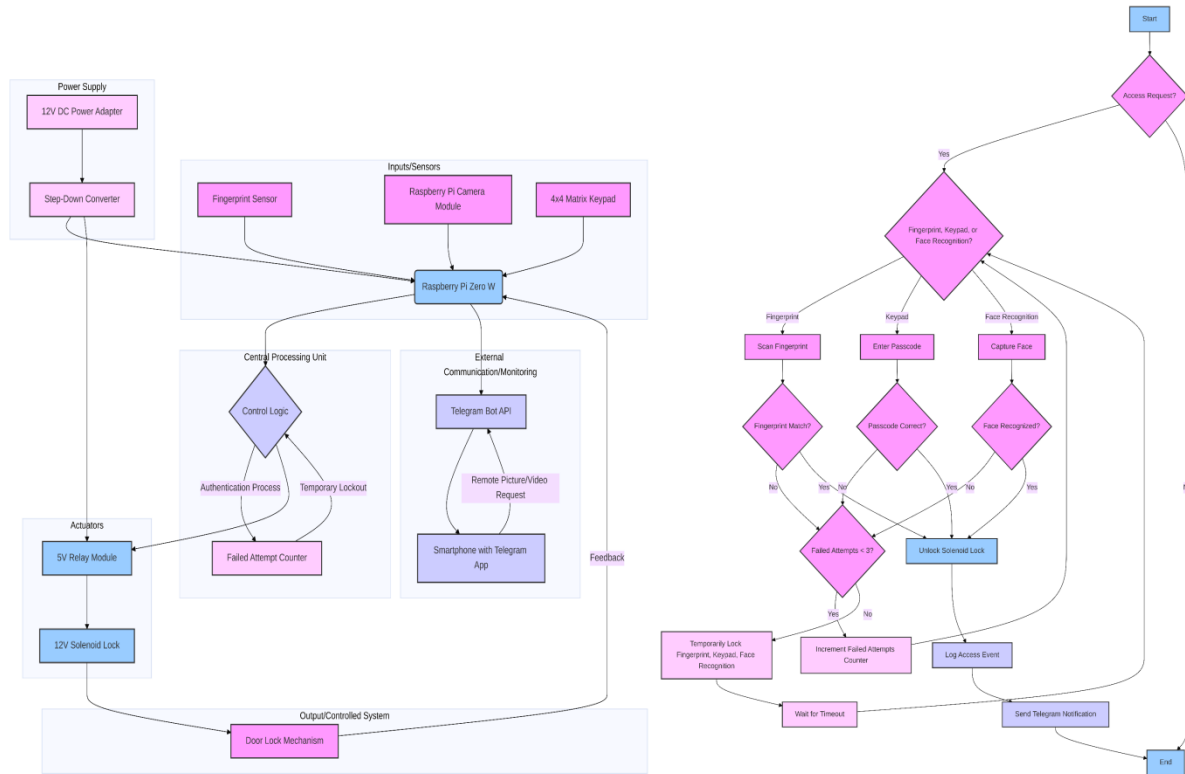
Installed on the current HoD office door, the smart door was designed as a modular IoT based access control platform based on a Raspberry Pi Zero W. Fingerprint scanning, facial recognition, keypad PIN entry can all be used for authentication. Upon successful verification, 12V solenoid lock is activated, and a Telegram bot logs and notifies the user at the same time. The lock and electronics are powered by a specialized solar power system, allowing for independent functioning. The autonomous door lock system's control and flow diagram is displayed in Figure 1.

### Hardware Components

The following are the major hardware components included:

- Raspberry Pi Zero W: Sensor interface, picture processing, decision logic, and network connection are all handled by a single-board computer with integrated Wi-Fi and General-Purpose for Mobile Communications (GPIO) pins acting as the central controller.
- 12 V solenoid lock: Electromechanical lock that retracts when energized to unlock the door, providing rapid actuation and low maintenance for repeated operations.
- Fingerprint sensor (R307): Biometric module supporting enrollment and matching of fingerprint templates, interfaced via UART with the Raspberry Pi for one to one authentication.
- Raspberry Camera module: The camera is positioned and tilted to provide enough coverage in normal daylight circumstances, and it is installed close to the entrance to record facial images for facial recognition.
- 4x4 matrix keypad: Numeric keypad enabling PIN based access as a fallback or alternative to biometric methods.

- Buzzer: An audio feedback device that indicates lockout occurrences, errors, and successful access.
- Power electronics: The Raspberry Pi and its accessories receive a regulated 5 V supply from a 12 V DC adapter and step-down converters, which are connected with a solar power system to enable autonomous operation.
- Mechanical fixtures: Wooding mounting frame, brackets, and hardware for securing components to the door and frame while protecting wiring and electronics.

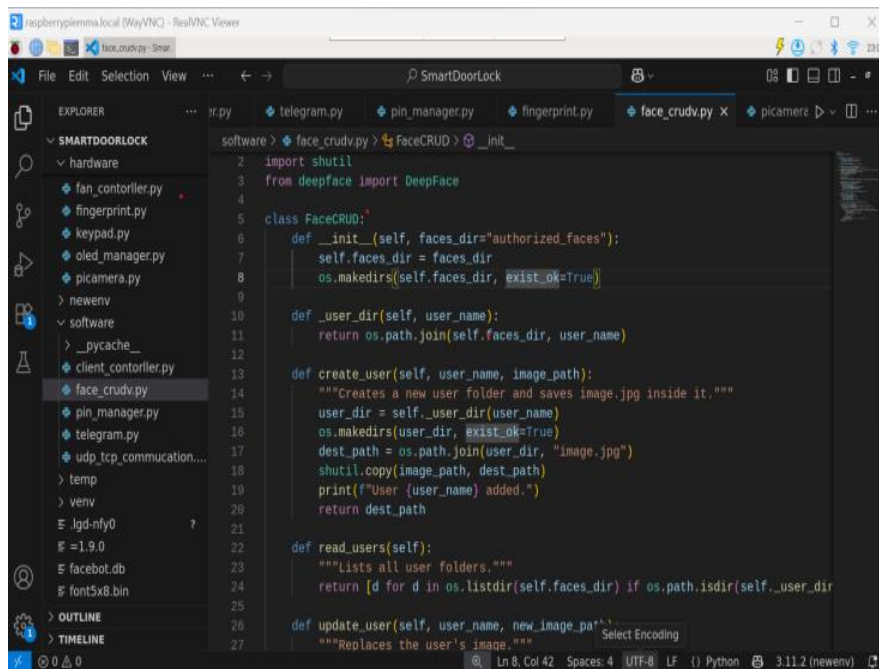


**Figure 1. Control and Flow Diagram of the Autonomous Door Lock System**

**Software architecture**

Using a number of libraries and Application Programmes Interfaces (API), Python was used to implement the system software on the Raspberry Pi. While the deepface library carried out facial detection and recognition against pre-controlled facial templates, the Open Computer Vision (OpenCV) library managed video capture and pre-processing. The openCV facial recognition implementation is depicted in Figure 2. In order to handle enrolment and verification, a serial communication module interfaced with the fingerprint sensor and returned success or failure flags to the main application.

A message interface was implemented using the Telegram Bot API, which allowed the system to instantly send notifications to the HoD's smartphone that contained text, pictures, or brief videos when access attempts happened or when the user specifically requested it. To preserve responsiveness and avoid blocking multithreaded execution was used to manage keypad monitoring, solenoid control, facial recognition, fingerprint scanning, and message sending. There is continuous monitoring of authentication inputs and enforcement of security policies, such as a temporary lockout following three unsuccessful tries using any combination of methods, during which additional authentication requests were disregarded for a predetermined period of time, were conducted by a primary control loop.



```

1  import shutil
2  from deepface import DeepFace
3
4
5  class FaceCRUD:
6
7      def __init__(self, faces_dir="authorized_faces"):
8          self.faces_dir = faces_dir
9          os.makedirs(self.faces_dir, exist_ok=True)
10
11      def _user_dir(self, user_name):
12          return os.path.join(self.faces_dir, user_name)
13
14      def create_user(self, user_name, image_path):
15          """Creates a new user folder and saves image.jpg inside it."""
16          user_dir = self._user_dir(user_name)
17          os.makedirs(user_dir, exist_ok=True)
18          dest_path = os.path.join(user_dir, "image.jpg")
19          shutil.copy(image_path, dest_path)
20          print(f"User {user_name} added.")
21          return dest_path
22
23      def read_users(self):
24          """Lists all user folders."""
25          return [d for d in os.listdir(self.faces_dir) if os.path.isdir(self._user_dir(d))]
26
27      def update_user(self, user_name, new_image_path):
28          """Replaces the user's image."""

```

**Figure 2. Implementation of OpenCV for Facial Recognition**

### System Design Installation

In order to reduce the latency and improve privacy, the system uses an edge-computing architecture in which all biometric processing and decision-making tools place locally on the Raspberry Pi without the need for external cloud servers. The Raspberry Pi controller inputs the modules (cameras, fingerprint, sensors, keypad), actuation (solenoid lock, buzzer), and communication (Telegram Interface) all make up the architecture's block diagram (Figure 1).

These particular aspects Ergonomics and mechanics had to be carefully considered during installation on the HoD's current office door. L-brackets were used to place solenoid locks inside door frames and protected passages were used to move hidden cabling. The camera was set up to record users frontal facial views, and the fingerprint sensor and keyboard were placed at the proper hand height. The Raspberry Pi and power electronics were stored in a hidden housing with careful attention to ventilation and avoid damage.

### Evaluation methodology

After installation, Experimental evaluation of the system followed under realistic operating conditions.

The test procedures are:

- Functional verification of each authentication modality
- Measurement of authentication success, false rejection rate (FRR), and false acceptance (FAR) for fingerprint and facial recognition.
- Measurement of response time from successful authentication to lock actuation for each method
- Performance assessment under varying environmental conditions, including normal lighting, low light, bright sunlight, and high humidity.
- Security testing with spoofing attempts and brute-force PIN trials, observing the behavior of the lockout mechanism and notification system.
- Collection of user feedback from the HoD and authorized staff regarding ease of use, perceived security, and overall satisfaction.

Result were compared qualitative with performance benchmarks reported in related smart door lock studies.

## Results

### Authentication performance

This work recorded and assessed authorised users with thirty attempts at fingerprint recognition using R307 sensor. With an average authentication time of 2.5 - 3.0 seconds, the system reported successful recognition, 3 false rejections, and 0 incorrect acceptances. The reasons for the recorded false rejections was due to moisture on the sensor surface and incomplete finger placement. The facial recognition software Deepface and OpenCV were assessed in various lighting scenarios. The successful recognition rate decreased to around 50% in low light, but it increased to about 90% in normal lighting, with typical recognition periods of 2.5 - 3.0 seconds. For codes that were entered correctly, Keypad-based 4-digit PIN entry recorded 100% success. There is no record of interpretation mistakes.

### Response time

The measured reaction time from successful authentication to door unlocking was within the 3- second threshold for each technique. Fingerprint access took about 2 seconds on average, facial recognition took about three seconds, and keypad entry was about 1.5 seconds since PIN verification has a lower computational cost.

### Environmental robustness

The system's performance under various environmental conditions is summarized in Table 1.

**Table 1. Environmental impact on authentication performance**

Condition	Fingerprint performance	Facial recognition performance	Keypad performance
Normal lighting	Excellent	Excellent	Excellent
Low light	Good	Fair	Excellent
Bright sunlight	Good	Good	Excellent
High humidity	Fair	Good	Excellent

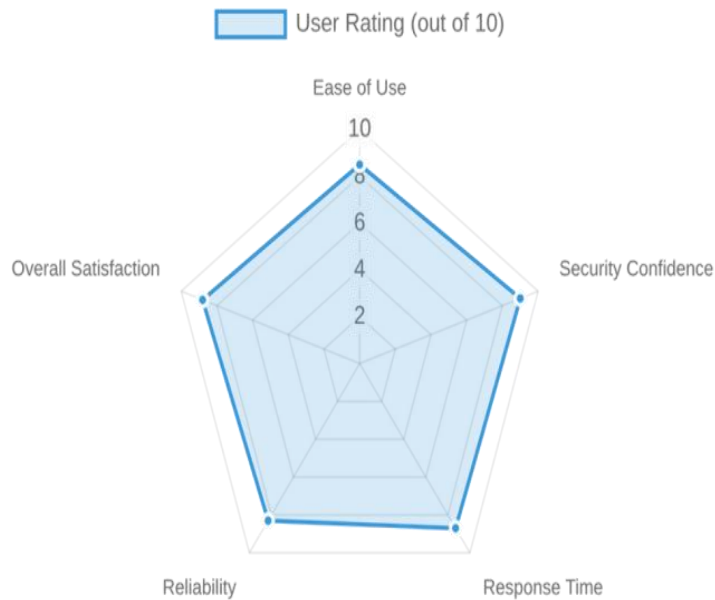
### Security and notifications

Security testing revealed that the three-failed-attempt lockout method, which momentarily stopped all authentication inputs, efficiently mitigated spoofing attempts and brute-force PIN trials. Near real time remoting was made possible via a Telegram based notifications that sent access alerts and related photos or brief videos to the HoD with usual delays of 1-2 seconds.

The implemented system falls within or above typical ranges for fingerprint accuracy (94% vs 90-95%), facial recognition rate (about 85% vs 80-90%), response time (less than 3s vs. 2-5s), and notification delay ("1-2s vs. "2s), according to a comparison with data from related IoT smart lock studies.

### User feedback

Authorized users' comments revealed favorable opinions of the system's security and usability. Users expressed particular gratitude for biometric access and real-time smartphone warnings, rating convenience of use at about 8.5/10 and confidence in a security at about 9/10. The radar map for evaluating user experience is shown in Figure 3.



**Figure 3. Radar Chart showing User Experience Evaluation**

### Discussion

The autonomous smart door lock system that was put into place effectively shows that a multimodal Internet of Things based control solution can be established and run dependably in an actual academic and administrative office setting. The combinations of these three methods provides flexibility and redundancy when a single modality is compromised by environmental or user-related variables, allowing users to select the most practical solution while maintaining security. While the edge processing of biometric data on the raspberry Pi improved privacy and reduced reliance on cloud connectivity. The solar power system allows continuous operation even in the absence of grid power, which is particularly crucial during power outages and in off-grid locations. Performance metrics shows that the system meets reasonable usability requirements, with typical authentication times of less than three seconds and accuracy that is comparable to or higher than values reported in related literature.

Nevertheless, certain drawbacks were noted, including reduced facial recognition precision in low light and occasional false fingerprint rejections due to moisture or improper contact. These disadvantages emphasize the need for improved lighting, such as LED or infrared lighting, as well as possibly more advanced sensors or flexible algorithms. Due to the requirement for steady internet connection for Telegram notifications there is a need for developing a dependable offline logging and local alert systems. Looking at the aspect beyond its technical capabilities, this system shows the support smart access management offers to a number of institutional goals by enhancing security. It also enables remote oversight, and demonstrates the practical use of biometric and IoT technologies in a university setting.

### Conclusion

This work presents the design, development, and deployment of an autonomous smart door lock system for an administrative and academic office. It blends keypad entry, facial recognition, fingerprint recognition, and Telegram based notifications with the help of a Raspberry Pi Zero W that is powered by a solar system. It offers various features, according to experimental evaluation, high authentication accuracy, quick response times, robust performance in various environmental conditions, multimodal authentication that compensates for the shortcomings of individual methods. By offering real-time monitoring and remote access awareness, the solution addressed the main drawbacks of conventional key based locks. Additionally, it strengthens the system resistance to the loss and duplication of key. Future research should focus more on developing a customer mobile application with improved control and logging features, as well as delving into encrypted cloud storage for biometric and access log data.

The research should boost lowlight facial recognition by increased lighting and adding power backup devices e.g batteries or UPS, for increased resilience. The system usefulness and scalability would be further improved by integrating it with Campus wide access control systems and adding further modalities like RFID or speech recognition.

### Acknowledgement

The authors acknowledge the support of the Department of Mechanical Engineering, Olabisi Onabanjo University, and thank the students, academic staffs, and administrative personnels for their support feedback during installation and testing.

### Nomenclature

V	Voltage	UPS	Uninterrupted Power Supply
≤	Less than or equal to	SDGs	Sustainable Development Goals
%	Percentage	LED	Solar collector Efficiency
s	Seconds	HoD	Head of Department
vs	Versus	IOT	Internet of Things
DC	Direct Current	PIN	Personal Identification Number
GSM	Global System for Mobile Communication	GPIO	General-Purpose for Mobile Communications
APIs	Application Programme Interfaces	RFID	Radio Frequency Identification
FRR	False Rejection Rate	OpenCV	Open Computer Vision Library
FAR	False Acceptance Rate	LED	Light-Emitting Diode

### References

- Dharme, S., Diksha, D., Kadwe, S., Bilwane, R., & Khule, R. B. (2022). Door lock security system using recent technology. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, 10(1), 684-686.
- Djupsjö, K., & Almosawi, M. (2018). IoT security applied on a smart door lock application. *International Conference on Security of Smart Cities, Industrial Control System and Communications*.
- Gupta P. & Johari, R. (2019). IoT Based Smart Energy Monitoring System. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol. 8(3): 1045–1052.
- Hamas, A., Muneer, A., & Fati, S. M. (2021). Smart security door system using SMS based energy harvest. *International Journal of Electrical and Computer Engineering (IJECE)*, 11(4), 3410–3423. <https://doi.org/10.11591/ijece.v11i4.pp3410-3423>
- Hussein, N. A., & Al Mansoori, I. (2017, September). Smart door system for home security using raspberry pi3. In *2017 International Conference on Computer and Applications (ICCA)* (pp. 395-399). IEEE.
- Kumar, A. & Kumari, M. (2020). Design and analysis of IoT-based real-time system for door locking/unlocking using face detection. *International Journal of Recent Technology and Engineering*, 8(5), 2093–2095. DOI:10.35940/ijrte.E5794.018520
- Lakshmi, R. D., Priya, P. L., Lokanyaa, G., & Sharmila, J. (2017). Security system using Raspberry Pi with door lock controller. *International Journal of Engineering Science*, 7(4), 10090-10094.
- Lin Y, Jiang X., Rong L., Shiman X., Huasheng W., & Qi, P. (2021). Failure Analysis of Intelligent Door Lock Master Control Chip. *IOP Conf. Series: Materials Science and Engineering*, 1043:032035. doi:10.1088/1757-899X/1043/3/032035
- Mahajan, S., Patil, P., & Chavan, M. (2019). Automatic door opening system. *International Journal of Research in Engineering, Science and Management*, 2(3), 268–271.
- Mahesh, K., Ashok Kumar, P. S., Naveen Raj, H. N., Naik, P. P., & Apoorv, M. N. (2019). IoT based smart surveillance security system using Raspberry Pi. *International Journal of Advance Research, Ideas and Innovations in Technology*, 5(3): 1356-1358.
- Motwani Y., Seth S., Dixit D., Bagubali A. & Rajesh R (2021). Multifactor door locking systems: A review. *Materials Today: Proceedings*, 46: 7973-7979. <https://doi.org/10.1016/j.matpr.2021.02.708>

- Nasirruddin, M., Balpande, A., Kachhwaha, P., Bondre, P., & Gawande, M. (2018). IoT and Fingerprint Based Door Looking System. *International Journal on Recent and Innovation Trends in Computing and Communication*, 6(6), 233-235.
- Nayak, P., Gupta, G. P., Raj, V., Nayaka, M., & HS, S. S. (2026, February). LockEase-Smart Door Security System. In *2026 International Conference on Visual Analytics and Data Visualization (ICVADV)* (pp. 1640-1646). IEEE.
- Nwankwo, P. N., Nsionu, I. I., & Joseph, E. C. (2013). Design and Implementation of Microcontroller Based Security Door System (Using Mobile Phone & Computer Set). *Journal of Automation and Control Engineering*, 1(1): 65–69. doi:10.12720/joace.1.1.65-69
- Patil, P., Gawande P. G., Kulkarni S. V., Patil R., Wale A. & Zod, S. (2026). An Intelligent Multi-Module Workstation for Enhancing Safety and Productivity in EMS Environments. *2026 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 2026*, pp. 1-6, doi: 10.1109/ESCI68015.2026.11493215.
- Zainuddin, A.A., Abd Rahman, A.D., Nor, R.M., Hussin, A.A A., Mohd, N.N.M.S.N., Shamsudin, A.U., & Sapuan, M.S. (2024). Innovative IoT smart lock system: Enhancing security with fingerprint and RFID technology. *Malaysian Journal of Science and Advanced Technology*, 4(4):360-365. <https://doi.org/10.56532/mjsat.v4i4.335>