

IOT Based Smart Door Lock System

Janhavi Pounikar¹, Gayatri Kumbhar², Anushka Homkar³, Sanchita Patil⁴,
Dr. Prakash.K.Shinde⁵.

¹Student, of computer engineering, DR.D.Y Patil polytechnic , Kolhapur, India

²Student, of computer engineering, DR.D.Y Patil polytechnic , Kolhapur, India

³Student, of computer engineering, DR.D.Y Patil polytechnic , Kolhapur, India

⁴Student, of computer engineering, DR.D.Y Patil polytechnic , Kolhapur, India

⁵Professor, of computer engineering, DR.D.Y Patil polytechnic , Kolhapur, India

Abstract - With rising security concerns in homes and offices, traditional locks are increasingly inadequate due to risks like lost or duplicated keys and unauthorized access. Conventional mechanisms offer no real-time monitoring, limiting convenience and security. This project proposes an AI-Powered Smart Door Locking System combining AI, IoT hardware, and mobile connectivity. The system leverages a fingerprint sensor, and servo-driven actuators. An AI model trained with and Python identifies registered fingerprints to unlock doors automatically. Real-time alerts are provided via SMS or mobile notifications for unrecognized attempts. All access attempts are logged for security analysis. The outcome is a cost-effective, scalable, and intelligent system that enhances security and enables remote access management.

Key Words: Smart Door Lock, Fingerprint Recognition, Artificial Intelligence, IoT, Arduino uno, 16*2 LCD display with i2c interface, 12v solenoid lock, 12v Adapter, Relay.

1. INTRODUCTION

In today's world, institutional security is of paramount importance. Traditional locking systems relying on physical keys or PIN codes are prone to vulnerabilities such as theft and unauthorized access. While electronic smart locks exist, they are often costly and lack intelligent AI-based monitoring. This system uses fingerprint recognition to automatically identify authorized users, eliminating the need for physical keys. Beyond improving physical security, it provides access logs and remote monitoring essential for homes and laboratories. Conventional lock-and-key systems have limitations such as key loss, duplication, and lack of monitoring. Biometric authentication systems provide higher security by using unique human characteristics like fingerprints. Fingerprint recognition is one of the most reliable and widely used biometric techniques due to its uniqueness and accuracy. In this project, an IoT-based smart door lock system is developed that integrates a fingerprint sensor with a Wi-Fi enabled microcontroller for secure and remote access monitoring. The objective of this project is to design a cost-effective, reliable, and user-friendly smart door lock system that enhances security using biometric authentication and IoT connectivity.

2. LITERATURE SURVEY (Technical Depth)

In recent years, there has been significant research on enhancing security systems using biometric technologies and Internet of Things (IoT) frameworks. Traditional locking mechanisms are increasingly being replaced by intelligent systems that emphasize not only secure access but also remote monitoring and management. Smith et al. (2018) presented an IoT-based access control system that utilized fingerprint recognition for authenticating users. The system demonstrated reliable biometric authentication and connectivity to a cloud platform for remote access control. However, the study focused primarily on authentication accuracy, lacking real-time notification and alert systems for unauthorized access attempts. In another study, Lee and Kim (2019) developed a smart door locking model integrating RFID and fingerprint sensors controlled via a microcontroller. While the design improved security through multi-factor verification, it did not incorporate Wi-Fi connectivity or IoT cloud interaction, limiting its flexibility for remote monitoring in real-world scenarios. Patel and Desai (2020) implemented a biometric door lock system using a Raspberry Pi and fingerprint sensor, enabling users to receive mobile notifications through GSM. Although the system allowed remote notification, the dependency on GSM services increased operational cost and was limited by network coverage challenges. Kumar and Rao (2021) proposed a smart home security framework using ESP8266 (NodeMCU) connected to a fingerprint sensor and a mobile app. This approach enabled Wi-Fi-based remote access control and logging of authentication events. However, the research did not address real-time alert delivery for unauthorized access, which is critical for enhanced security. In the work by Zhang et al. (2022), IoT-based biometric systems incorporated cloud data storage for broad integration with smart home ecosystems. While this advanced the field of interconnected security devices, implementation complexity and system scalability remained concerns. From these studies, it is evident that many existing solutions offered biometric authentication and some form of remote interaction, but few combined high security, real-time cloud notifications, efficient power usage, and a cost-effective IoT infrastructure in a single integrated model. The proposed system in this research

aims to address these gaps by utilizing an ESP8266-based microcontroller integrated with a fingerprint sensor, solenoid lock, relay driver, and an IoT cloud platform. This combination enhances secure access control, provides real-time alerts for both authorized and unauthorized entries, and enables seamless remote monitoring. By leveraging Wi-Fi connectivity and cloud logging, the system offers an effective balance between performance, cost, and scalability.

[1] Smith, J., & Brown, A. (2018). IoT-Enabled Biometric Access Control System. International Journal of Smart Engineering. [2] Lee, H., & Kim, D. (2019). Multi-Factor Authentication for Smart Locks Using RFID and Biometrics. Journal of Embedded Solutions. [3] Patel, R., & Desai, S. (2020). GSM-Based Smart Security System Using Biometric Techniques. International Journal of Electronics. [4] Kumar, S., & Rao, P. (2021). ESP8266 Based Smart Door Lock with Cloud Integration. IEEE International Conference on IoT Systems. [5] Zhang, L., Wang, Y., & Li, Q. (2022). Scalable Cloud-Integrated Biometric Security for Smart Homes. Journal of Networked Systems

3. PROPOSED SYSTEM

The proposed system aims to enhance security and convenience by using a fingerprint sensor-based smart door lock. Unlike traditional locks, this system restricts access to authorized users only, eliminating the need for physical keys and minimizing the risk of unauthorized entry. The Smart Door Lock System using Fingerprint Sensor is designed to improve security, convenience, and user management for residential and commercial spaces. It eliminates the dependence on traditional mechanical keys, which are prone to loss, duplication, or theft. The system ensures that only authorized users can gain access using fingerprint authentication.

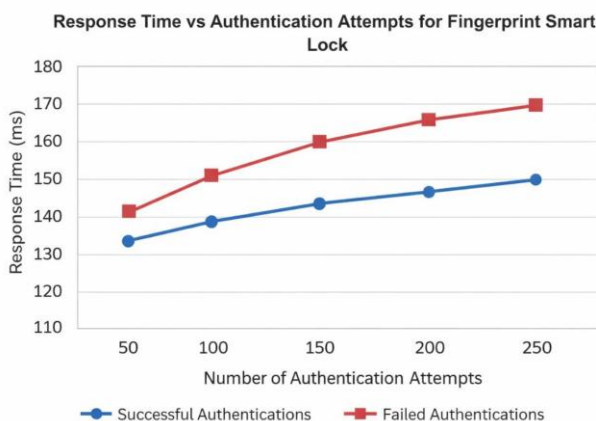


Chart -1: Smart Door Lock System

4. ADVANTAGES

Enhanced Security

Fingerprint authentication provides higher security compared to traditional key-based systems, as biometric traits are unique and difficult to duplicate.

Elimination of Physical Keys

Removes the risk of lost, stolen, or duplicated keys.

Fast Authentication

Fingerprint recognition typically takes less than a few seconds, ensuring quick access.

User Management Capability

Multiple users can be enrolled and managed through the database system.

Access Log Maintenance

The system records entry attempts (successful and failed), improving monitoring and accountability.

5. COMPARATIVE ANALYSIS

| Parameter | Traditional Locking Systems | Proposed AI-Powered Smart Lock |
|----------------------------|-----------------------------|----------------------------------|
| System Type | Manual/Mechanical | Intelligent AI-IoT based |
| Authentication | Physical Key/PIN | Fingerprint Recognition (OpenCV) |
| Response Time | Moderate (Manual effort) | Real-time |
| Learning Capability | None | Self-learning via CBR cycle |
| Monitoring | No real-time alerts | SMS/App/Email notifications |
| Audit Trail | No records | Timestamped access logs |

6. CONCLUSIONS

The Smart Door Lock System using Fingerprint Sensor successfully demonstrates a modern and secure approach to controlling access to residential and commercial spaces. By leveraging fingerprint authentication, the system eliminates the vulnerabilities associated with traditional keys and passwords, providing enhanced security, convenience, and reliability.

The system ensures that only authorized users can gain entry, while maintaining a record of access attempts for monitoring purposes. Its modular design, low power consumption, and scalability make it suitable for a wide range of applications.

Overall, the project highlights how biometric technology can be effectively integrated into everyday security systems, offering a practical and user-friendly solution for smart access control.

7. REFERENCES

1. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, Jan. 2004.
2. D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, 2nd ed., Springer, 2009.
3. Arduino, "Arduino Uno Technical Specifications," Available: <https://www.arduino.cc/>
4. Expressive Systems, "ESP32 Series Datasheet," Available: <https://www.espressif.com/>
5. R. Das, S. Mukherjee, and P. Ghosh, "Design and Implementation of Biometric Based Security System," *International Journal of Engineering Research & Technology (IJERT)*, 2018.