Smart Security System Using Fingerprint Authentication

Mr. Ritesh D. Falfale, Mr. Shubham R. Gaikwad, Mr. Ankur S. Gatpalli, Mrs. Aparna B. Dalvi

Professor, Professor, Professor, Professor
Department of Electronics & Telecommunication Engineering,
MGM's College of Engineering, Nanded
s23_falfale_ritesh@mgmcen.ac.in, s23_gaikwad_shubhamramdas@mgmcen.ac.in,
s23_gatpalli_ankur@mgmcen.ac.in, dalvi_ab@mgmcen.ac.in

***Abstract*—Growing security challenges in residential and industrial spaces demand access control systems that are both reliable and user friendly. Conventional methods such as keys, cards, and passwords are vulnerable to loss, duplication, and misuse. To address these limitations, this paper proposes a smart security system that combines smartphone-based fingerprint authentication with IoT technology. User verification is carried out on the mobile device, and a secure wireless command is transmitted to an ESP8266 microcontroller to operate a relay-controlled solenoid lock. Since biometric data is processed locally on the smartphone, the system enhances privacy while eliminating the need for physical keys or external fingerprint modules. The proposed approach offers a secure, economical, and scalable solution suitable for smart homes, offices, and restricted access areas.**

***Index Terms*—Fingerprint Authentication, Smart Security System, ESP8266, IoT, Solenoid Lock, Biometric Access Control**

I. Introduction

Rapid urbanization has increased the demand for secure access control, while traditional methods such as keys and passwords remain vulnerable to loss, duplication, and misuse. Biometric authentication offers a more reliable alternative, with fingerprint recognition being widely adopted due to its accuracy, uniqueness, and ease of use. The widespread availability of fingerprint sensors in smartphones has further improved accessibility.[1] This paper introduces an IoT-based security system that uses smartphone fingerprint authentication, where verification occurs locally on the device and only an encrypted command is sent to an ESP8266 controller to operate an electromechanical lock. By eliminating external biometric hardware, the system reduces cost, simplifies design, enhances privacy, and is suitable for smart homes, offices, and restricted environments.[9]

II. Literature Review

Access control systems include mechanical locks, electronic locks, biometric systems, and IoT-based solutions. Mechanical locks are cheap but vulnerable to picking and duplication, while electronic locks face issues like password leaks and card cloning. Fingerprint-based biometric systems improve security but often require costly hardware and local storage of biometric data, raising privacy concerns.[6]

IoT smart locks with controllers like ESP8266 offer remote access but usually rely on less secure methods or built-in fingerprint sensors. Smartphone-based fingerprint authentication provides better security through built-in secure environments. This study addresses the gap by combining smartphone fingerprint verification with a low-cost IoT controller for secure, private, and scalable access control.[2][7]

III. System Architecture

The system architecture of the proposed smart security system integrates biometric authentication, wireless communication, and electromechanical locking into a cohesive framework. The architecture consists of four main components:

A. Smartphone with Fingerprint Authentication:

The user's smartphone serves as the primary biometric authentication device. It utilizes the built-in fingerprint sensor to verify the identity locally within a secure environment, ensuring biometric data privacy.[6]

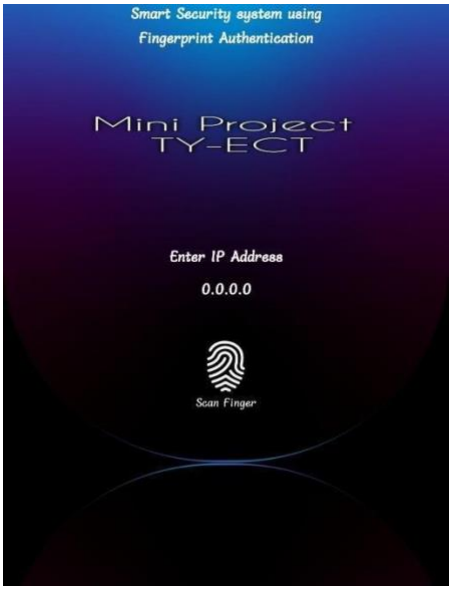

Fig 1. Smartphone Interface

B. Wireless Communication Layer:

After successful authentication, the smartphone transmits an encrypted command over a Wi-Fi network to the smart controller. This wireless transmission allows remote and contactless access control.[8]

C. ESP8266 Microcontroller:

The ESP8266 NodeMCU module acts as the central control unit. It receives the encrypted unlock command, decrypts and verifies its validity, and controls the relay module based on the received instructions.[3]

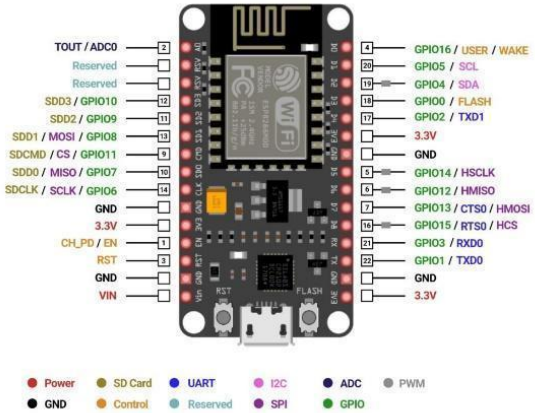

Fig 2. ESP8266 Module

D. Relay and Solenoid Lock:

The relay acts as an electrical isolator and switch, allowing the microcontroller to safely operate the solenoid lock. The solenoid lock mechanically secures the door and unlocks only when energized by the relay.[2]

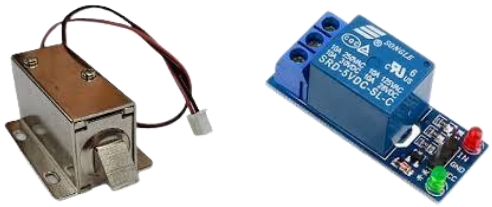

Fig 3. Solenoid Lock & Relay

The overall architecture supports secure, remote, and user-friendly access control by combining biometric verification with IoT-enabled actuation. The separation of biometric processing (on the smartphone) and lock control (on the microcontroller) reduces hardware costs and enhances security.[9]

IV. Methodology

The methodology outlines the systematic process and design approach used to develop the smart security system:

A. Hardware Design

The ESP8266 microcontroller acts as the central controller due to its built-in Wi-Fi capability, low power consumption, and compatibility with IoT applications. A relay module is used to electrically isolate the low-voltage microcontroller from the high-current solenoid lock. The solenoid lock provides secure physical locking and operates only when energized by the relay. A regulated power supply ensures stable operation of all components.[7][2]

B. Software Design

The ESP8266 firmware is developed using the Arduino IDE and connects to Wi-Fi, acting as a web server that listens for encrypted HTTP requests from the mobile app. The smartphone app handles fingerprint authentication using the device's built-in biometric system, ensuring all biometric data is processed locally. No fingerprint information is transmitted or stored outside the phone, maintaining strong privacy and security for the user. This setup enables secure and seamless communication between the app and the ESP8266 without compromising sensitive biometric details.[4]

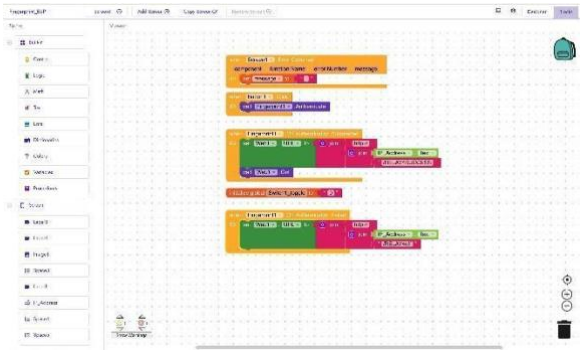

Fig 4. Mobile Application Backend Design.

V. Implementation

The system uses smartphone-based fingerprint authentication to control an IoT-enabled electromechanical lock. An Android application verifies the user locally using the phone's built-in fingerprint sensor, ensuring biometric data remains on the device. Upon successful authentication, an encrypted Wi-Fi command is sent to an ESP8266 NodeMCU. Acting as a web server, the ESP8266 validates the request and triggers a relay via a GPIO pin to operate a solenoid lock for a fixed duration, followed by automatic relocking. Invalid or unauthorized commands are rejected to prevent accidental access. Real-time testing over a local Wi-Fi network confirmed stable, secure, and reliable operation.[5][3]

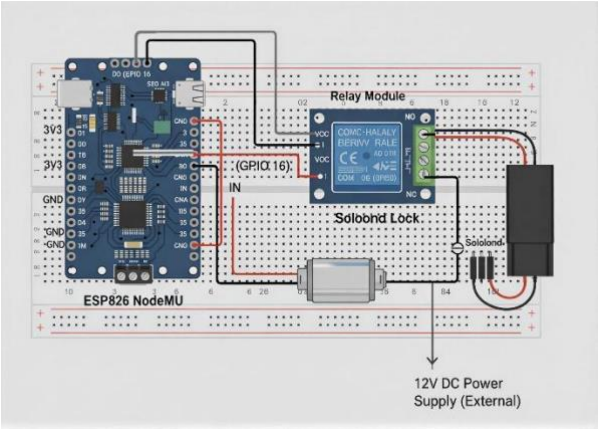

Fig 5. Circuit Diagram of Smart Security System

VI. Results & Discussion

The system was tested under normal operating conditions to evaluate its effectiveness, efficiency, and security. The key outcomes are outlined below:

A. Reliable Fingerprint Authentication

The biometric module accurately captured and matched fingerprint data using a built-in sensor. Authentication success depended on comparing the scanned fingerprint template with stored authorized templates, minimizing false acceptances or rejections.[4]

B. Secure Wireless Communication

Encrypted HTTP requests transmitted between the smartphone application and the ESP8266 microcontroller protected sensitive data during communication. This encryption prevented interception and unauthorized command execution.[1]

C. Consistent Solenoid Lock Operation

The solenoid actuator responded reliably to control signals, physically locking and unlocking the door with precision. Mechanical wear was minimal during repeated testing cycles, indicating durability, and the actuator operated quietly, ensuring minimal noise disruption.[6]

D. Enhanced Security without Physical Keys

By removing conventional keys, risks related to lost or duplicated keys were eliminated, reducing potential security breaches common in traditional locking systems.

Overall, the system's combination of fast, secure, and reliable components makes it ideal for residential and small office environments, balancing convenience with enhanced protection.[6]

VII. Future Scope

The system supports future expansion through cloud-based access logging, multi-user and role-based permissions, and alternative authentication methods such as OTP or Bluetooth access. Reliability can be improved with backup power options, while support for protocols like MQTT and smart home integration enhances compatibility. Adding extra sensors and multi-factor authentication can further increase security and intrusion detection capabilities.

VIII. Conclusion

This work proposes an IoT-based access control system that uses smartphone fingerprint authentication to replace keys, passwords, and external biometric hardware. Built-in mobile biometrics enhance security and privacy, while an ESP8266 wirelessly controls an electromechanical lock via a relay. Testing shows quick response, automatic relocking, and strong protection against unauthorized access. The solution is affordable, scalable, and suitable for smart and secure environments.

References

[1] Jain, A. K., Ross, A., & Prabhakar, S., "An Introduction to Biometric Recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, 2004.

[2] Ratha, N. K., Bolle, R. M., & Pankanti, S., "Biometric Authentication: Security, Privacy, and User Acceptance," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948–960, 2004.

[3] Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S., *Handbook of Fingerprint Recognition*, 2nd ed., Springer, New York, 2009.

[4] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M., "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[5] ESP8266 Technical Reference Manual, Espressif Systems, 2020. Available: https://www.espressif.com

[6] Al-Qutayri, M. A., & Jeedella, J., "Smart Door Lock System Using IoT and Biometric Authentication," *International Journal of Engineering Research and Technology*, vol. 9, no. 4, pp. 512–517, 2020.

[7] Conti, M., Das, S. K., Bisdikian, C., Kumar, M., Ni, L. M., Passarella, A., & Zambonelli, F., "Looking Ahead in Pervasive Computing: Challenges and Opportunities in the Internet of Things," *IEEE Pervasive Computing*, vol. 11, no. 1, pp. 84–93, 2012.

[8] Arduino Documentation, "Arduino IDE and ESP8266 Programming," Available: https://www.arduino.cc

[9] Zhang, Y., Chen, X., & Li, J., "Secure and Privacy-Preserving Biometric-Based Authentication Scheme for Smart Environments," *Security and Communication Networks*, vol. 2019, pp. 1–10.