WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal Homepage: www.ijrpr.com ISSN 2582-7421

Low Power IoT Security System

Amruta Patil[1], Amulya Chougale[2], Amulya Pawar[3], Prerana Gobbani[4], Dr. Manjula Emmi[5]

[1-4] Final Year Student, Electronics and Communication Engineering, S G Balekundri Institute of Technology, Belagavi, India

[5] Senior Project Mentor, Electronics and Communication Engineering, S G Balekundri Institute of Technology, Belagavi, India

ABSTRACT—

This work presents a smart door security system that combines fingerprint-based identity verification with internet-connected monitoring. Entry is granted only to enrolled users, while a camera snapshot of every unrecognised visitor is emailed to the owner, and the owner can follow entry activity through a mobile application.

Keywords—IoT, Fingerprint Sensor, ESP32-CAM, Smart Door Lock

Introduction

Protecting homes, offices and other restricted spaces from unwanted entry remains a pressing concern. A mechanical lock depends entirely on a physical key, and such a key may be misplaced, stolen or duplicated without the owner knowing. A conventional lock also gives no indication of who approached the door while the owner was away.

As connected devices have become common, security solutions have grown smarter and easier to use. A fingerprint reader verifies who the person is, and a network link lets the owner receive door information from a distance. Joining the two ideas gives a more dependable way to control entry and to keep an eye on visitors. The proposed Smart Door Access Control and Visitor Photo Notification System is centred on an ATmega controller that coordinates all other modules. A fingerprint sensor and a keypad handle user verification, whereas an ESP32-CAM takes a picture of the person at the door and emails it to a registered Gmail address over the internet. A mobile application built with MIT App Inventor lets users sign up and look through the log of entries. Smoke and vibration sensors are added to flag abnormal conditions, an LCD shows the current system status, and a servo motor operates the lock. In this way, secure entry, photo alerts and continuous monitoring are delivered by one compact unit.

Literature Survey

1. Earlier studies on fingerprint-operated door locks confirm that biometric verification is a reliable way of restricting entry. A sensor reads the finger placed on it and compares the result with templates saved earlier; the door opens on a match and stays shut otherwise. Because a fingerprint cannot be forgotten, easily lent out or lost like a key or a password, this approach is considerably safer, and it ensures that only registered people can open the door.
2. Work on IoT-enabled security shows how wireless links make remote supervision and control possible. A connected door unit can report its state to the owner through a smartphone application or by email. With a camera module attached, the unit can photograph whoever is at the entrance and forward the image to the owner, who can then recognise the visitor without being on site. The owner thus stays informed about what is happening at the entrance in real time.
3. More recent smart-lock designs focus on merging microcontrollers, biometric readers, cameras and wireless modules into one package that offers several protective functions. Extra sensors, for instance smoke or vibration detectors, can recognise unusual events and raise an alarm for the owner, while a mobile app simplifies enrolling users and reviewing entry history. The common goal of these efforts is to unite user verification, visitor image alerts and sensor-based supervision in a single solution. Making every one of these functions cooperate reliably, with dependable communication between modules, is still the main difficulty.

Modeling and Analysis

This section explains how the proposed smart door security system, built on IoT and fingerprint-based verification, is designed and how it functions. It brings together fingerprint recognition, automated door actuation, wireless communication and sensor-driven supervision. The order of operations, from power-up through credential checking to the raising of a security alert, is shown with the help of a flow chart and an algorithm. The ATmega32 acts as the main controller and coordinates every hardware module in the design.

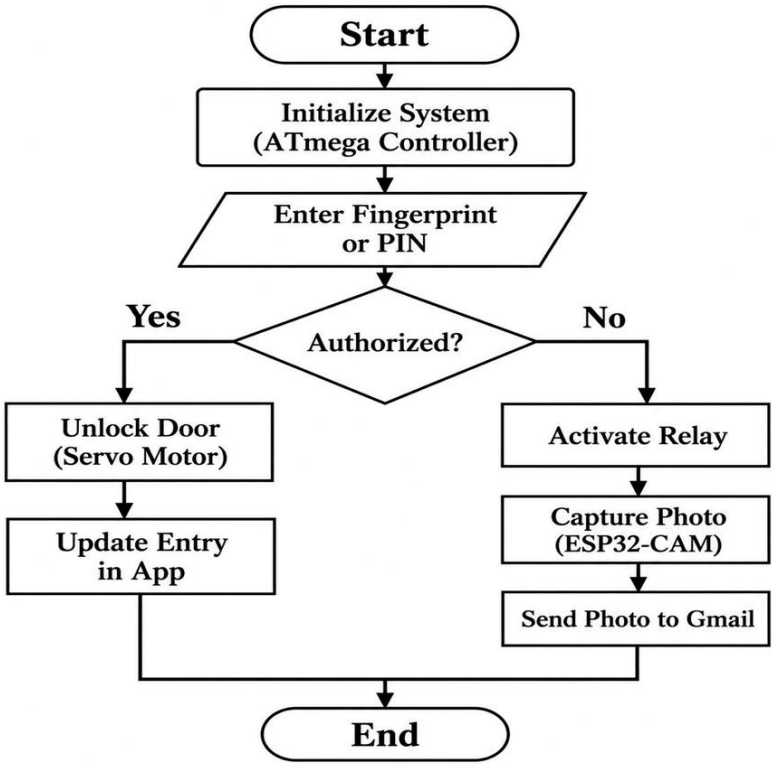
Firmware for the ATmega32 is written in embedded C using a suitable development environment and loaded onto the chip with a programmer. It takes care of fingerprint verification, reading the sensors, driving the servo and showing messages on the LCD. While running, the controller collects readings from the fingerprint module and the security sensors, evaluates them and responds according to the programmed logic. The ESP8266 Wi-Fi module gives the system a wireless path for passing security events on to the chosen notification service.

The ATmega32 drives a servo motor that moves the lock. Once the fingerprint sensor confirms a valid user, the controller commands the servo to shift the latch to its open position, and after a preset delay the servo brings the latch back to the closed state. When the fingerprint is not recognised, the door stays locked. The LCD reports the verification outcome and the present state of the system, so the user always receives clear feedback and the whole entry process runs without manual effort.

The fingerprint sensor is central to the design because it establishes the identity of the person seeking entry. In the enrolment stage, the fingerprints of permitted users are saved in the memory of the sensor, provided the module supports template storage. During normal use, the sensor scans the finger placed on it and checks it against the saved templates. The controller allows entry when a match is found and rejects the attempt when none is found. This lessens dependence on physical keys and keeps entry limited to registered individuals.

For additional supervision, the system includes a vibration or tilt sensor along with an MQ-2 smoke sensor. The vibration sensor responds to any knock, shake or tampering at the door, whereas the MQ-2 reacts to smoke and several flammable gases. Whenever a reading crosses its configured threshold, the controller can show a warning on the display and ask the ESP8266 module to send out a notification. As a result, the system covers not only door access but also protection against physical tampering and hazardous surroundings.

Flow chart:



Algorithm:

Step 1: Start.

Step 2: Initialise all modules of the system through the ATmega controller.

Step 3: Accept the user's fingerprint on the scanner or a PIN on the keypad.

Step 4: Compare the entered fingerprint or PIN with the records of authorised users.

4.1: When the credentials are correct, the servo motor opens the lock and the entry is logged in the Android app.

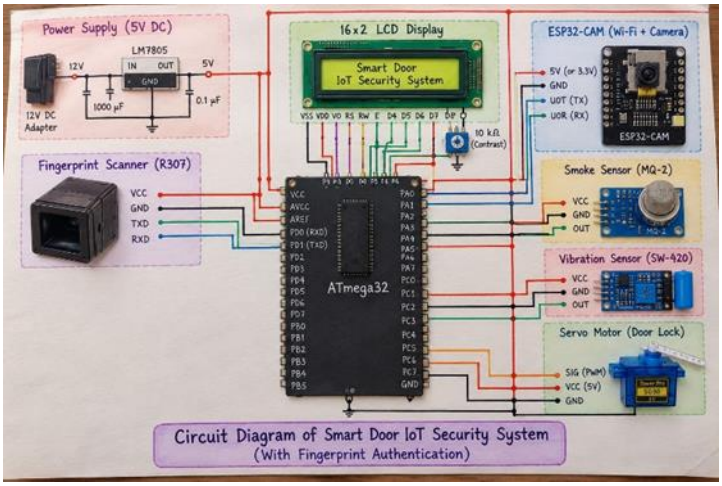
4.2: When the credentials are wrong, the relay module is switched on.

4.3: The ESP32-CAM is triggered to capture a picture of the visitor.

4.4: The captured picture is emailed to the configured Gmail account.

Step 5: Stop.

Circuit Diagram:



Conclusion

A door security system that pairs fingerprint verification with IoT connectivity is an effective means of protecting homes and offices. Traditional lock-and-key arrangements have weaknesses, since keys get lost and unauthorised people can gain entry. A fingerprint-operated lock is more convenient and modern, because it admits only the person whose fingerprint has been verified.

A major strength of the design is that entry is governed by biometric checking. The sensor confirms whether the presented fingerprint belongs to a registered user, and the ATmega32 microcontroller then uses that result to decide whether the servo motor should open or keep closed the lock. A clear message on the LCD tells the user what the outcome was.

A second important feature is the set of extra sensors used for monitoring. A vibration or tilt sensor notices disturbance around the door, and the MQ-2 sensor responds to smoke and certain flammable gases. The ESP8266 Wi-Fi module allows security alerts to be sent wirelessly, which takes the design well beyond simple fingerprint-based entry control.

The project also demonstrates that biometrics and IoT can work together as a genuine smart security solution. Since the design is modular, new capabilities such as better remote monitoring or more advanced alerting can be introduced later, which makes it adaptable to different security requirements.

To conclude, the IoT and biometric Smart Door Security System offers convenient access control through fingerprint verification, automatic door operation and sensor-based supervision. It eliminates the need to carry physical keys and can issue security alerts when required. Suitable places for its use include homes, offices and other premises where entry must be restricted.

Reference

1. K. A. K. Permana, I. Piarsa and A. A. K. A. Wiranatha, "IoT-Based Smart Door Lock System with Fingerprint and Keypad Access", Journal of Information Systems and Informatics, vol. 6, no. 3, pp. 2086-2098, 2024. doi: 10.51519/journalisi.v6i3.844
2. J. A. J. Alsayaydeh, M. F. Yusof, S. Mamchenko, R. A. Hamzah and S. G. Herawan, 'Design and Evaluation of a Biometric IoT-Based Smart Lock System with Real-Time Monitoring and Alert Mechanisms', Int. J. Adv. Comput. Sci. Appl., vol. 16, no. 7, 2025. doi: 10.14569/IJACSA.2025.0160737.
3. X. W. Pua and K. N. Ramli, "Development of a Fingerprint-Based Door Lock with Database System", Evolution in Electrical and Electronic Engineering, vol. 5, no. 1, pp. 252–258, 2024.
4. P. Shirisha, G. Satish Kumarr, K. Shivanjan, K. Shiva Rama Krishna and K. Vineela, 'An IoT-Based WiFi Fingerprint Door Lock System with Raspberry Pi & Webcam', MATEC Web of Conferences, issue 392, article 01066, 2024. doi: 10.1051/matecconf/202439201066.
5. H. Fauziman and R. Mukhaiyar, "Rancang Bangun Sistem Keamanan Pintu Menggunakan Fingerprint Berbasis Internet of Things (IoT)," JTEIN: Jurnal Teknik Elektro Indonesia, vol. 4, no. 2, pp. 529, 537, 2023. doi: 10.24036/jtein.v4i2.438.
6. S. Bhowmick, A. Kumar, and S. Manas, "Fingerprint Door Lock Using Arduino UNO R3", International Journal for Multidisciplinary Research, volume 5, number 3, 2023. DOI: 10.36948/ijfmr.2023.v05i03.3819.

7. P. Nguyen Huu, D. Nguyen Quang, H. Nguyen Trong, P. Pham Ngoc, and Q. Tran Minh, 'Design of a Smart Lock System Using Fingerprint and Password for Enhancing Security', in Future Data and Security Engineering, Communications in Computer and Information Science, vol. 1688, pp. 285–298, Springer, 2022. doi: 10.1007/978-981-19-8069-5_19.

8. A. Saroha, A. Gupta, A. Bhargava, A. K. Mandpura, and H. Singh, "Biometric Authentication Based Automated, Secure, and Smart IoT Door Lock System", in Proceedings of the 2022 IEEE India Council International Subsections Conference (INDISCON), 2022. doi: 10.1109/INDISCON54605.2022.9862840.

9. M. S. Mohd, M. H. Ahmat Kamil, M. K. N. Mohamad, and M. A. Razali, "A Door Lock System Using Fingerprint", Multidisciplinary Applied Research and Innovation, volume 3, number 1, pages 364 to 372, 2022.

10. W. Yang, S. Wang, N. M. Sahri, N. M. Karie, M. Ahmed, and C. Valli, "Biometrics for Internet-of-Things Security: A Review", Sensors, volume 21, number 18, article 6163, 2021. DOI: 10.3390/s21186163.