International Journal of Engineering Research and Advanced Technology (IJERAT)

DOI: 10.31695/IJERAT.2024.3.2

E-ISSN : 2454-6135

Volume. 10, No.3
May - 2024

Design and Development of Biometric and Keypad Based Smart Door Security System for Residential Building

Y. Lavanya[1], M. Rajitha Lakshmi[2], Vasamsetti Tarun[3], Putta Suma[4], Pandi Rakesh[5]

Associate Professor[1] , Assistant Professors[2], & Students[3,4,5]

Department of Electronics and Communciation Engineering

Ramachandra College of Engineering

Eluru, A.P, India

ABSTRACT

A door access system's development involves a wide range of characteristics, from the most basic a keypad to the most sophisticated using smart cards and biometrics. The Arduino-Based Door Access System was created to address the problems associated with maintaining and upgrading the current system. This study covers the use of an Arduino microcontroller in a door entry system. One kind of microcontroller that has its own programming language is the Arduino. It may be used for experiments because it contains an electrical prototyping platform of its own. The keypad and fingerprint scanner are the two inputs for this project. The outputs consist of an LCD display, a siren, an indicator, and a magnetic switch. Based on the accuracy results of testing five people, each with four distinct fingerprints, connecting all inputs and outputs with Arduino led to accurate results in opening the door. The result that appears on the LCD display is the output, and the inputs are the password that is entered via the keypad and the details that are retrieved by scanning a fingerprint. This project is trustworthy because it uses an Arduino Microcontroller and a straightforward technique to raise the security level of the door access mechanism.

Keywords: Access Control System, Fingerprint Scanner, Arduino-based Security, Dual-factor Authentication.

1. INTRODUCTION

A door access system is crucial for maintaining security in buildings, ensuring that only authorized individuals can enter. This project aims to develop a fully automated security access system, integrating fingerprint technology for user-friendly access control. By employing a solid-state fingerprint sensor, this system offers reliable and secure authentication, surpassing traditional methods like passwords or keycards. Let's explore the features, hardware components, and advantages of this innovative door access system.

1.1 Key Features and Components

The heart of this system is a fingerprint module interfaced with an onboard microcontroller. This microcontroller processes the fingerprint data and controls the door's locking mechanism. The project's hardware includes:

- Fingerprint module
- LCD Display for door status information
- Doors (as the output module)
- Power Supply components (Rectifier and Regulator)
- Microcontroller (e.g., PIC Microcontroller)
- Push Buttons for manual overrides
- Project Usage

The fingerprint-based security system offers unparalleled security benefits:

Highest Security: Unlike keys or passwords that can be stolen or leaked, fingerprints are unique to each individual, ensuring only authorized access.

Convenience: Users need not carry keys or remember passwords, enhancing convenience and reducing the risk of unauthorized access due to lost or forgotten credentials.

Persistent Memory: The system retains stored fingerprints even during power outages, maintaining security and convenience.

Efficiency: Fingerprint scanning provides rapid access compared to RFID cards, passwords, or keys.

1.2 Biometric Technology Advantages

Biometrics, such as fingerprint recognition, offer superior security over traditional methods. It requires the physical presence of the authorized person for authentication, preventing unauthorized access more effectively than passwords or smartcards. This technology finds application in various security systems like ATMs, time attendance, and vehicle access control.

1.3 Fingerprint Recognition

Fingerprint recognition, one of the oldest biometric methods, dates back to 2200 BC. This system utilizes fingerprint data to control door access, allowing only enrolled users' fingerprints to open doors. Here's how it works:

- Valid users' fingerprints are stored in a database within the microcontroller.
- When a person attempts access, their fingerprint is compared against those in the database.
- If a match is found, the door is unlocked; otherwise, an alarm warns of unauthorized attempts.

2. LITERATURE SURVEY

The door access system is a crucial security feature used worldwide to protect people and assets from unauthorized access and potential threats such as burglaries or kidnappings. To develop an effective door access system, various hardware components like keypads, smart cards, RFID cards, and biometric sensors are integrated with software programming. In particular, the implementation of a keypad and fingerprint scanner in this Arduino-based Door Access System was chosen for its user-friendliness, intelligence, and heightened security compared to alternatives like face verification or smart cards. Research by Hassaballah et al. (2015) and Jain et al. (2011) demonstrates the challenges and inefficiencies of face recognition systems, which are time-consuming due to the need for multiple images and sensitivity to factors like illumination and aging. Voice recognition systems, as studied by Picone et al. (1993) and Hanifa et al. (2021), face similar difficulties with background noise and speech modeling. In contrast, fingerprint scanners offer advantages in accuracy and speed, with Oluwatoyin et al. (2016) highlighting their superiority in preventing issues like lost ID cards and ensuring ownership integrity.

This paper’s reliance on an optical fingerprint scanner underscores the efficiency and reliability of biometric technology in security applications, applicable across industries, offices, and homes. The fingerprint sensor, a key component, utilizes various techniques such as optical methods to detect unique human fingerprints swiftly and accurately. The system operates in two modes: Settings/Admin mode, where user data is entered into the fingerprint sensor's database, and Normal/Search mode, where fingerprints are compared for access control. When a match is found, the system activates the appropriate devices using a microcontroller, enhancing security and access control efficiency. This project exemplifies the intersection of biometrics and embedded system technology, leveraging the unique characteristics of fingerprint identification for robust security solutions (Oluwatoyin et al., 2016).

3. EXISTING SYSTEM

A lock and a physical key is the most widely used locking and unlocking mechanism for doors. Everything about the process is mechanical. The complete locking mechanism needs to be replaced if the key is forgotten, lost, or stolen. The issue of physical keys becomes more problematic in large organizations because staff members are required to carry many keys for various entrances. The issue of physical keys becomes more problematic in large organizations because staff members are required to carry many keys for various entrances. There is very little security in the current system. A new fingerprint-based high security door access system is suggested as a preventative measure.

4. PROPOSED SYSTEM

The flow of the project process is shown as the user will first enter the password that the system has previously generated. The user can proceed by inputting their ID if the password they submitted is correct. In the event that not, the user will get three chances to input their password. If the incorrect password is entered on the third try, an alert will sound. Next, a template of each authorized user's fingerprint is stored in memory. Users must place their finger on the fingerprint scanner in order to have their fingertips scanned in order to enter the building. Enrolling the user ID is the first step in the fingerprint scanner storage process. The fingerprint is captured by the fingerprint scanner as soon as the user places their finger. After that, it will extract the specifics and store the result in memory. Finding

DOI : 10.31695/IJERAT.2024.3.2

the match is the next step in the process. It uses the stored fingerprint details along with the most current ones that were captured. The magnetic door lock will be disabled if the user's minutia matches their own minutiae that has already been saved. This will allow the user to access the door. In the event that not, users will need to reenter their ID number.

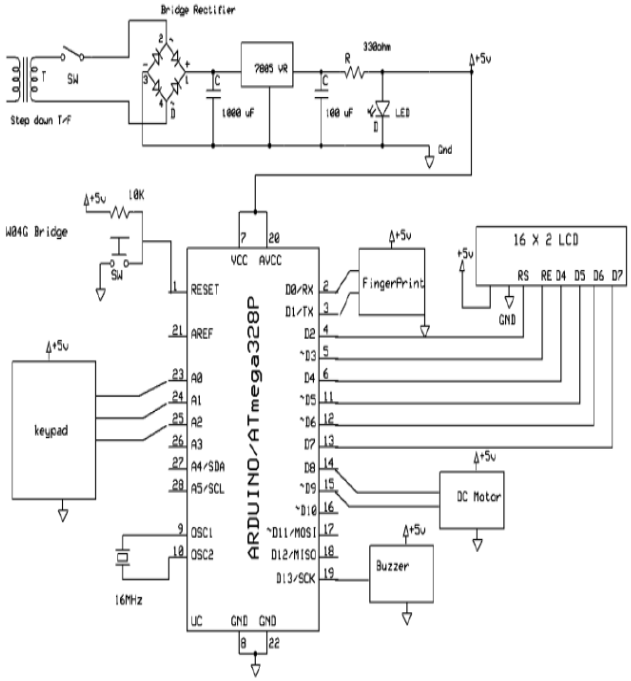

Figure 1.1 : The Proposed System

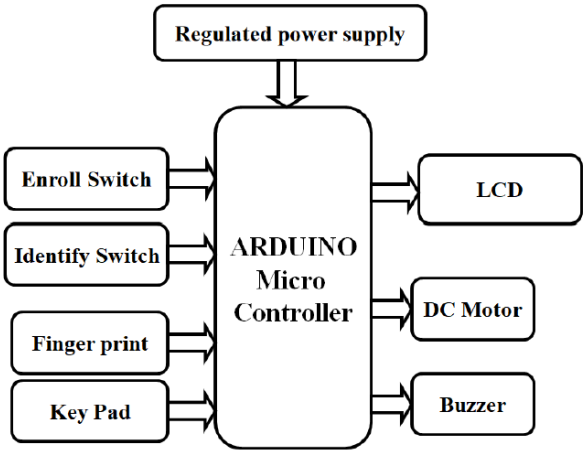

Figure 1.2: Circuit Diagram of the Proposed System

Three attempts will be granted to the users. An alert signaling the presence of intruders will sound if the users are unsuccessful on their third try.

The hardware employed for this undertaking. The Arduino Mega board, fingerprint scanner, 4x4 keypad, and 16x2 LCD display are the five primary pieces of hardware. The features that are used to open the door are the fingerprint scanner and keypad. On the other hand, the Arduino platform is intended for use in testing, where features are connected to its I/O ports and programs are uploaded to the Atmel Arduino microcontroller. The LCD display's job is to show the output, and the Atmel Arduino microcontroller and the embedded C programming language are communicated with each other via the USB cable.

DOI : 10.31695/IJERAT.2024.3.2

4.1 FLOW CHART

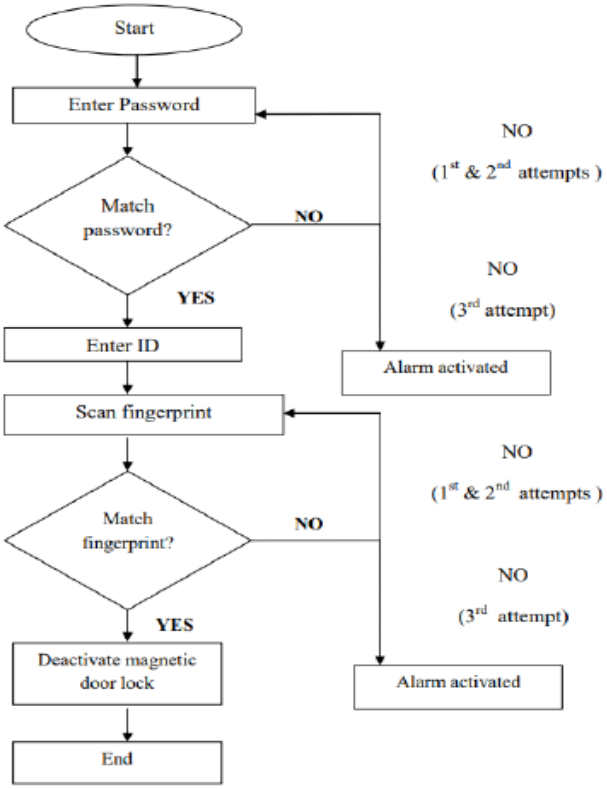

Figure 1.3: Flow Chart of the Proposed System

5. METHODOLOGY

The methodology for developing the Arduino-based Door Access System with keypad and fingerprint scanner involves several key steps, encompassing hardware setup, software development, and system integration. The following methodology outlines a systematic approach to implement this security system effectively:

5.1 Hardware Setup

- Gather Components: Collect necessary hardware components including Arduino board, fingerprint sensor module, keypad, LCD display, relay, buzzer, motor, and necessary connecting wires.
- Connect Hardware: Establish connections between components based on circuit diagrams and datasheets. Connect the fingerprint sensor, keypad, LCD display, relay, buzzer, and motor to the Arduino board as per the system design.
- Test Hardware: Ensure each component is functioning correctly by running basic tests and diagnostics to confirm proper connections and functionality.

5.2 Software Development

- Arduino IDE Setup: Install and set up Arduino Integrated Development Environment (IDE) on a computer.
- Write Arduino Sketch: Develop the software (sketch) for the Arduino board. Write code to initialize and communicate with the keypad, fingerprint sensor, LCD display, relay, buzzer, and motor.
- Implement Control Logic: Program the Arduino to read inputs from the keypad and fingerprint sensor, display information on the LCD, and control the relay and motor based on access authorization.
- Error Handling: Include error handling routines to manage cases such as incorrect keypad entries or failed fingerprint scans.

DOI : 10.31695/IJERAT.2024.3.2

5.3 System Integration

- Integrate Components: Combine the hardware setup with the developed software. Upload the Arduino sketch to the Arduino board.
- Calibration and Testing: Calibrate the fingerprint sensor by enrolling authorized fingerprints and testing the entire system under various scenarios (e.g., valid access attempts, invalid attempts).
- Fine-Tuning: Refine the system behavior based on testing results. Adjust parameters, thresholds, or control logic to optimize performance and reliability.
- User Documentation: Prepare user manuals or instructions detailing how to operate and maintain the door access system.
- Deployment and Evaluation:
- Install System: Deploy the Arduino-based Door Access System at the desired location (e.g., building entrance).
- User Training: Provide training to end-users on operating the system, including enrollment of new fingerprints and troubleshooting common issues.
- Continuous Monitoring: Regularly monitor the system performance post-deployment. Address any issues or feedback from users to ensure continuous functionality and security.

  By following this methodology, the development and implementation of the Arduino-based Door Access System can be executed efficiently, ensuring a reliable and user-friendly security solution for controlling access to buildings or secured areas.

6. MERITS

The Arduino-based Door Access System integrating a keypad and fingerprint scanner delivers a high level of security with dual-factor authentication, utilizing unique fingerprint patterns for robust access control. This system offers a user-friendly interface through the keypad and LCD display, ensuring straightforward interaction for users during enrollment and access management. With rapid and accurate fingerprint recognition provided by the optical sensor, the system operates efficiently, facilitating real-time authentication and response. Built on the reliable Arduino platform, the system ensures durability and consistent performance over time. It also supports scalability and customization, allowing for easy integration with existing infrastructure and the addition of new features as needed. Cost-effectiveness is another key benefit, leveraging open-source hardware and software components to minimize initial setup costs while providing a versatile and adaptable security solution for various environments.

7. CONCLUSION

A residential security is increased via fingerprint and keypad identification, which limits who is allowed to operate the vehicle. Therefore, compared to a traditional lock and key, one can ensure far higher security and exclusivity by installing this rather inexpensive and readily available technology on a car. Therefore, it can be concluded that biometric security systems provide a far more effective and reliable way to prevent unauthorized individuals from using automobiles. The created prototype acts as a catalyst for further research aimed at creating more reliable and integrated real-time fingerprint-based automated door lock systems.

8. FUTURE SCOPE

The primary goal of our project, "Fingerprint based Bank Locker Accessing System," is to use a Bluetooth module to operate devices via a PC. A microcontroller is the system's main controlling component. The microcontroller is interfaced with a Bluetooth module and relays. Relays are supplied to the microcontroller as input. This data is processed by the microcontroller and sent via Bluetooth to be received by the PC. The controller loads a program written in the Embedded "C" language to accomplish the operation. Instead of sending people there and having issues on the ground, we may obtain the temperature of dangerous zones directly from our personal computers by linking temperature, gas, and sensor systems to the system. The idea can be expanded by deploying a robot there, where a sensor will measure the temperature and provide information to a microcontroller, which will then communicate that information to a transceiver, which will allow us to obtain data on the computer side. We can obtain

DOI : 10.31695/IJERAT.2024.3.2

information about smoke concentration by attaching a smoke sensor to the robot. Information is sensed by the sensor, sent to the microcontroller and transceiver, and then processed by the computer to provide the desired information.

REFERENCES

[1] Advantages of Arduino, Arduino Guide, Retrieved on 5 Nov 2012 at 0810, from http://arduino.cc/en/Guide/Introduction (2012)

[2] Arduino Mega2560 Microcontroller Board, Retrieved on 17 Nov 2012 at 2230,from http://members.home.nl/bzijlstra/software/examples/wiz83wiz830mj.htm (2012)

[3] Parallax 4x4 Matrix Keypad, Retrieved on 17 Nov 2012 at 2240, from http://www.zekotec.ch/parallax/zubehoer/bs-peripherie/4x4-matrix-membranekeypad.php (2012)

[4] Matrix Keypad Interfacing with Microcontrollers: Introduction, Retrieved on 17 Nov 2012 at 2243, from https://encryptedtbn2.gstatic.com/images?q=tbn:ANd9GcRVF_VUL6PITMFaV96eyL5iuG1xMIYu MnBZF5n0O9PMIcBsfFmx (2012)

[5] B. Andrew, Comparing fingerprint, Retrieved on 18 Nov 2012 at 0712, from http://www.uh.edu/engines/epi2529.htm (2012)

[6] Adafruit products, Retrieved on 18 Nov 2012 at 0800, from http://www.adafruit.com/products/751 (2012)

[7] LCD 16x2 interface, Retrieved on 19 Nov 2012 at 0700, from http://ramoliyabiren.blogspot.com/2011/12/lcd-16x2-interface-with-Arduino.html (2012)

[8] Magnetic contact switch, Retrieved on 19 Nov 2012 at 081, from http://www.supplierlist.com/product_view/bestkey/3783/100521/magnetic_contact_s witch.htm (2012)

[9] Understanding relays, Retrieved on 19 Nov 2012 at 1030, from http://www.autoshop101.com/trainmodules/relays/107.html (2012)

[10] Red and green LED, Retrieved on 19 Nov 2012 at 1040, from http://www.123rf.com/photo_593493_red-and-green- light-emitting-diodes-whiteled.html(2012)

[11] Azzad Firdaus, Z., Electronic Combination Lock Using PIC , Final Year Project Report, Universiti Teknikal Melaka (2008)

[12] Khan, S. R., Development of Low Cost Private Office Access Control System (OACS), International Journal of Embedded System and Application (IJESA), Vol.2, No.2, (2012

[13] Hassaballah, Mahmoud, and Saleh Aly. "Face recognition: challenges, achievements and future directions." IET Computer Vision 9.4 (2015): 614-626.

[14] Jain, Anil K., Brendan Klare, and Unsang Park. "Face recognition: Some challenges in forensics." 2011 IEEE International Conference on Automatic Face & Gesture Recognition (FG). IEEE, 2011.

[15] Picone, Joseph W. "Signal modeling techniques in speech recognition." Proceedings of the IEEE 81.9 (1993): 1215-1247.

[16] Hanifa, Rafizah Mohd, Khalid Isa, and Shamsul Mohamad. "A review on speaker recognition: Technology and challenges." Computers & Electrical Engineering 90 (2021): 107005.

[17] Oluwatoyin, Kadiri Kamoru, Alimi Maryam Odunola, and A. O. Alabi. "Effective and Efficient Means to Prevent and Minimize Identity and Identity Cards Theft, Criminal Vices and Unauthorized Access to Places in Nigeria." Journal of Scientifics Research and Reports 9.4 (2016): 1-17

DOI : 10.31695/IJERAT.2024.3.2

International Journal of Engineering Research and Advanced Technology (IJERAT)

DOI: 10.31695/IJERAT.2024.3.2

E-ISSN : 2454-6135

Volume. 10, No.3
May - 2024