WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

IoT based anti-theft security system using biometric and mail notification

Arvind R Ghosh[1], *Meghna R Raheja*[2], *Rahul S Kannoujiya*[3]

[1] Department of Electronics and telecommunication Engineering college Dumberwadi, Junnar. Arvindrg143@gmail.com
[2] Department of Electronics and telecommunication Engineering college Dumberwadi, Junnar. meghnaraheja143@gmail.com
[3] Department of Electronics and telecommunication Engineering college Dumberwadi, Junnar. rahulkannoujiya@gmail.com

ABSTRACT

In this paper a new system is proposed for the security and home automation this in this paper we will explores about the integration of IoT biometrics and smart alert in the development of anti-theft security systems. The integration of IoT technology can bring a new era in security systems. This solution establishes unmatched access control by utilizing biometric authentication, which makes use of fingerprints. The system improves user experience and guarantees an effective security measure against unauthorized access and potential theft by identifying the individuals and sending pictures on mail. The core of this security system is IoT, which allows exchange of information and real time to enhance user awareness and responsiveness. This system incorporates a mail notification feature which ensures that the users receive real time alerts and updates via email, enabling them to stay informed and take necessary actions to response to the threat. The integration of IoT biometric and mail notification not only increases the security measures but also improves the standard for comfortable living and taking security measures to the threats on our own.

Keywords: IoT, Biometric, Security system, Home automation

INTRODUCTION

The integration of IoT capabilities amplifies the system's effectiveness. Real-time data exchange and connectivity empower the security system to communicate seamlessly with other devices and platforms, creating a dynamic and responsive network. In the event of a security breach or suspicious activity, the system can trigger immediate alerts and take predefined actions to mitigate the threat.

The integration of IoT enhances the efficiency of traditional biometric systems. Real time data exchanging using mail notification empowers security in case of suspicious activity. We can even connect alarm in case of 2 to 3 failed attempts to increase the security.

This system aims to raise awareness about security concerns. This project will get the users to receive email-based alert and updated about security events in real time, giving them instant information to act quickly and proactively to the theft. Regardless of the nature of activity whether it is an attempted breach, unidentified entry attempt or anything else, the user can stay informed and take necessary action and take security measures.

RELATED WORKS

The security system has evolved over significantly over the few years, from lock key-based system CCTV surveillance to using biometrics to unlock the doors, then we moved toward electronics security using key cards and PIN codes, Driven by constant need to improve and protect our valuable assets we are constantly improving this technology.

In the start of 20th century when the biometric authentication was introduced used the fingerprint and face recognition technology has gained a popularity which provides convenient and secure means of access control, but when it used standalone it lacks the connectivity and intelligence which can be seen in modern IoT based solution.

The future of this security system can be achieved by integrating IoT biometrics and intelligent notification systems. Below are some key aspects which can help understand the future of this solution.

Integration with IoT for interconnected security: IoT based systems will continue to grow by connecting devices and by creating a new security ecosystem. This connectivity will enable real time communication between humans and machines allowing quick response at the time of security incidents.

Biometric technology can also advance further, like using iris scan instead of fingerprint or facial scan or introducing 2 step verification using face and iris scan.

To do all this AI will play a crucial role in anti-theft security systems. Machine learning algorithms can continuously analyze the pattern and adapt to the evolving threats. The intelligent notification systems such as email with remain. However, new communication methods such as SMS alert app notification or some action using smart home device can be incorporated.

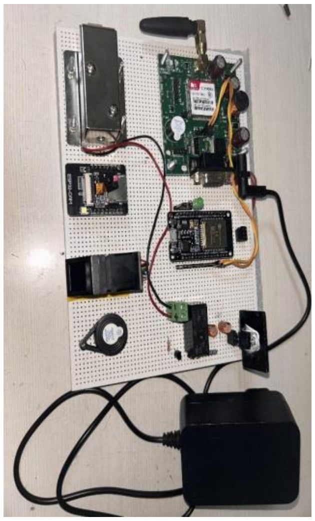
IoT based security system is designed to keep scalability and adaptability in mind. These systems can grow the number of connected devices and make an ecosystem which will then adapt to the emerging technologies ensuring rapid evolving technological advancement. The future of anti-theft security systems will be defined by integrating IoT, advanced biometric artificial intelligence user friendly design. These systems will not only provide increased security but also offer more seamless experience for users to make a shift from conventional security approach to IoT based advanced security approach.

PROPOSED SYSTEM

The main objective of this paper is to implement an Anti-theft system for home and office premises which can be easily installed and handled by the owners, and which can protect the assets of the owner in case of any security threat. It is very essential that this system must be compact easy and easily maintained. Therefore, we are proposing the system which consists of biometrics-based fingerprint identification and mail notification. The system goes live when fingerprint matches the set fingerprint, this will unlock and relay which is in this case can be viewed as the door lock. In case of failed attempt the camera module will capture the image of intruder and send a mail notification to user that there is a security breach, We are also introducing an Alarm in case of 2 or 3 failed fingerprint attempts so that even if the user is not available at the intrusion site the alarm sound scares the intruder and if someone hears the alarm they can inform the security about the potential threat.

HARDWARE MODULES

The hardware system is built using components like ESP32 Board PCB, Power supply, Wi-Fi Module, Fingerprint Sensors, CAM32 and Relay Driver. They are programmed using Arduino IDE with embedded C to perform the tasks assigned to them. It is connected to the IoT to transfer the data and send mail to the user.



Power Supply - A step-down transformer is a type of transformer that is designed to reduce the voltage of an alternating current (AC) power supply. To step down 230VAC to 5V, a transformer with a voltage reduction ratio of 46:1 is required. This means that the secondary voltage of the transformer will be 5V when the primary voltage is 230V.

The step-down transformer is typically followed by a rectifier and a filter circuit to convert the AC voltage to DC voltage and remove any ripple from the output. The rectifier circuit is responsible for converting the AC voltage to DC voltage by using diodes. A full-wave rectifier circuit is commonly used, which consists of four diodes arranged in a bridge configuration. After the rectifier circuit, a filter circuit is used to remove any residual AC voltage or ripple from the DC voltage. The filter circuit typically consists of a capacitor that is connected in parallel to the output of the rectifier circuit. The capacitor charges up during the positive half-cycle of the AC voltage and discharges during the negative half-cycle, resulting in a smooth DC voltage at the output.

ESP32 - The ESP32 is a powerful microcontroller board that is designed for a wide range of applications, including the Internet of Things (IoT), robotics, and automation. Here is a brief overview of how the ESP32 board works.

Microcontroller - The ESP32 board features a powerful microcontroller that is based on the Xtensa LX6 processor. It has two cores that can run up to 240 MHz, and it has 520KB of SRAM and 4MB of flash memory.

Wireless Connectivity - The ESP32 board has built-in Wi-Fi and Bluetooth capabilities, which allows it to connect to a wide range of wireless devices and networks. It supports various Wi-Fi protocols, such as 802.11b/g/n and 802.11ac, as well as Bluetooth 4.2 and Bluetooth Low Energy (BLE). GPIO Pins: The ESP32 board has a large number of GPIO (General Purpose Input/Output) pins, which can be used to connect various sensors, actuators, and other devices. The board has a total of 34 GPIO pins, including 14 analog inputs and 24 digital inputs/outputs.

Development Environment - The ESP32 board can be programmed using various development environments, such as the Arduino IDE, the ESP- IDF (Espressif IoT Development Framework), and Micro Python. The development environment allows developers to write code, compile it, and upload it to the board for execution.

CAM32 Module - The ESP32-CAM module features a camera sensor that can capture images and videos in various resolutions, including 2 megapixels (1600 x 1200 pixels), 1 megapixel (1280
x 720 pixels), and VGA (640 x 480 pixels).

Fingerprint Sensors - Secure your project with biometrics - this all-in-one optical fingerprint sensor will make adding fingerprint detection and verification super simple. These modules are typically used in safes there's a high-powered DSP chip that does the image rendering, calculation, feature-finding and searching.
Connect to any microcontroller or system with TTL serial, and send packets of data to take photos, detect prints, hash, and search. You can also enrol new fingers directly - up to 162 fingerprints can be stored in the onboard FLASH memory. There's a red LED in the lens that lights up during a photo so you know it's working.

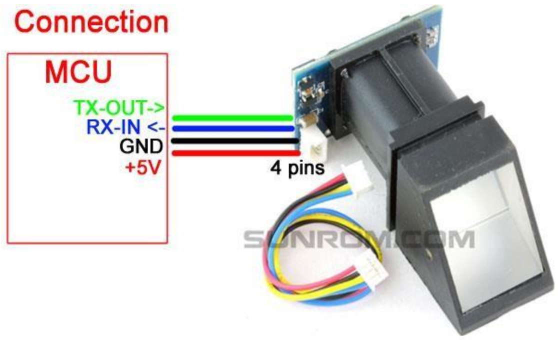


Figure 1: Fingerprint Sensor

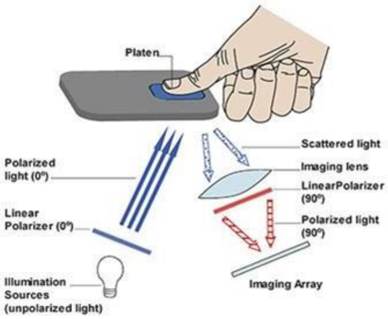


Figure 2: Sensor Concept

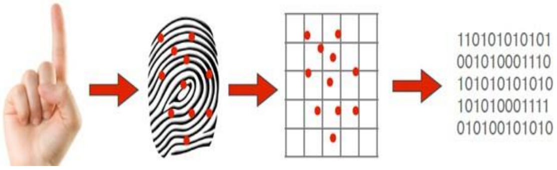


Figure 3: Sensor Scan Method

Relay Driver - This is a device consisting of a coil of wire wrapped around an iron core. When electricity is applied to the coil of wire it becomes magnetic, hence the term electromagnet. The A B and C terminals are an SPDT switch controlled by the electromagnet. When electricity is applied to V1 and V2, the electromagnet acts upon the SPDT switch so that the B and C terminals are connected. When the electricity is disconnected, then the A and C terminals are connected. It is important to note that the electromagnet is magnetically linked to the switch but the two are NOT linked electrically.

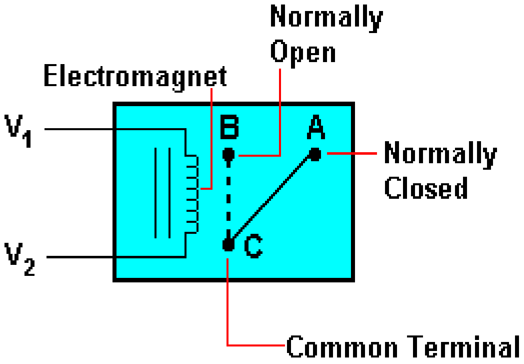


Figure 4: Internal schematic of Relay Driver

ESP32 is used as a main controller in this system. Internal peripherals of the ESP32 are configured. for the system to work. Wi-Fi module is connected to the ESP32 via serial port 1 and the Fingerprint sensor is connected to the serial port 2. Buzzer is connected to ESP32 via a GPOI and LED indication is connected parallel to the buzzer. Hence whenever buzzer will blow LED will also indicate the same. Relay module is connected to ESP32 via a GPIO. Whenever relay will switch then automatically lock will open and close with respect to the state of the relay. CAM32 module is also connected to the ESP32 via a GPIO in accordance with the controlling pin. Power supply gives the power to the ESP32 for functioning. Power supply is having step down transformer and 7805 regulators to convert the 12V output of the transformer to the regulated 5V.

WORKING

The system is totally built up on the ESP32 module. General purpose Input and Output port of the ESP32 is used to handle Relay, Buzzer, Camera module. Wi-Fi Module and the Fingerprint sensor is access using serial ports. Below figure shows the pin configuration of the ESP32.

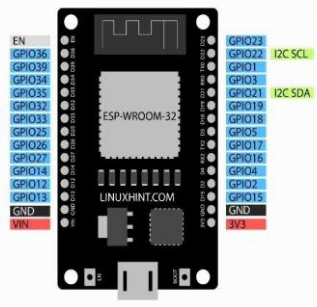


Figure 5: Pin Diagram of ESP32

A fingerprint security system is a biometric authentication method that uses a person's unique fingerprint to grant access to a secured location or device. The system works by capturing an image of the person's fingerprint and analysing it to determine if it matches the stored template of an authorized user. Here's how a fingerprint security system typically works:

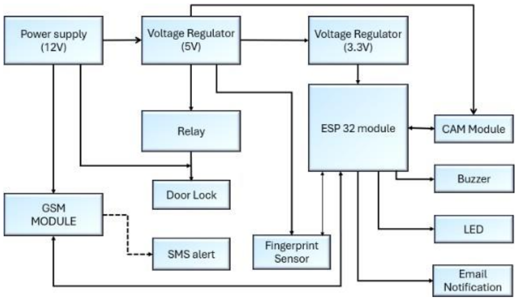


Figure 6: Block Diagram

Initialisation - At Power ON, power supply turns on the system and initialised all the peripherals. Wi-Fi module, CAM32 and ESP32.

Enrolment - The user's fingerprint is captured
and stored in the system's database. The fingerprint is usually scanned several times from different angles to create a complete and accurate image.

Authentication - When the user wants to gain access to a secured location or device, they place their finger on a fingerprint scanner. The scanner captures an image of their fingerprint and compares it to the stored template in the database.

Verification - If the captured fingerprint matches the stored template, the system grants access to the user and Wi-Fi module also send a message to the registered mobile number that that "Access given to unlock the door". If captured fingerprint does not match, then access is denied. Buzzer blows and LED indication turn ON to indicate that un- authorised person tried to access the door. Also, when buzzer turned ON, camera module turns ON and image of the person get captured. As soon as image is captured GPRS module is enabled, and image is sent to the registered Emil ID also Wi-Fi module send message to the registered mobile number that "Un-authorised person tried to access the door".
The fingerprint security system works by using advanced algorithms to analyse the unique features of a person's fingerprint, such as the ridges, valleys, and minutiae points. These features are used to create a mathematical representation of the fingerprint, which is then compared to the stored template for authentication.

FLOWCHART

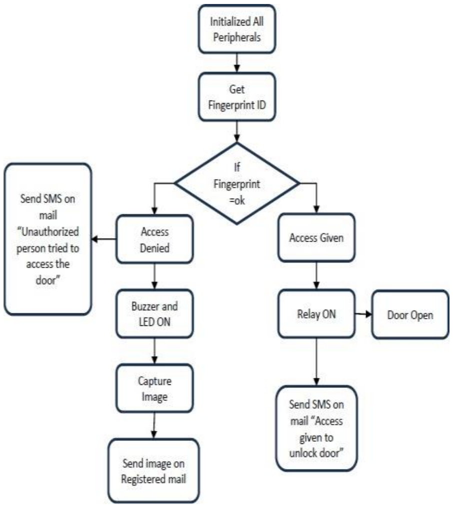
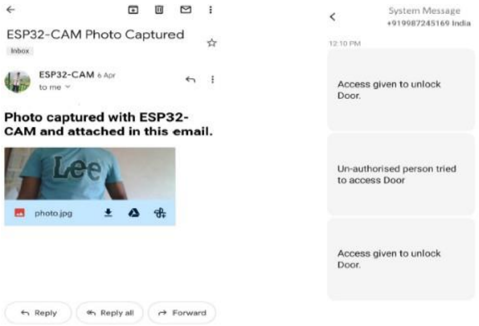

Initialized All Peripherals
Get Fingerprint ID
If Fingerprint =ok
Send SMS on mail "Unauthorized person tried to access the door"
Access Denied
Access Given
Buzzer and LED ON
Relay ON
Door Open
Capture Image
Send SMS on mail "Access given to unlock door"
Send image on Registered mail

Figure 7: Flowchart

RESULT

Fingerprint security systems are highly secure and accurate, as each person’s fingerprint is unique
and cannot be replicated. Additionally, they are easy to use and convenient, as users do not need to remember passwords or carry access cards. The system is developed successfully with the help of ESP32 microcontroller. Once the fingerprint set up is done, the user will have an account of their own unique access and can generate notification on the set email address. The system features providing access generating alarm & sending notification. The intermediate results of the interaction can be shown below through
Figure. 9



ESP32-CAM Photo Captured

ESP32-CAM 6 Apr
to me

Photo captured with ESP32-CAM and attached in this email.

System Message
+919987245169 India

12:10 PM

Access given to unlock Door.

Un-authorised person tried to access Door

Access given to unlock Door.

Figure 8: Actual mail notification

Below is the result,
When unauthorised person tries to access the system then camera captures the image and sends to the registered email ID.
When authorised or unauthorised person tries access the system then system sends the alarm message to registered mobile number.

Future Work

Improving fingerprint recognition algorithms: The accuracy and reliability of fingerprint recognition algorithms are essential for any fingerprint security system. Researchers can work on improving the accuracy and reliability of these algorithms to make them more robust and effective.
Enhancing communication channel security: Wi- Fi networks is susceptible to different types of attacks such as interception and eavesdropping. Future research can focus on developing methods to enhance the security of communication channels between the fingerprint scanner and the central server, including using encryption or other secure communication protocols.
Integrating other biometric modalities: Fingerprint recognition is just one of many biometric modalities that can be used for security purposes. Future research can explore the feasibility of integrating other biometric modalities such as facial recognition, iris recognition, or voice recognition to enhance the security of the system.
Investigating the potential use of blockchain technology: Blockchain technology has gained popularity recently because of its security and decentralization features. Future work can investigate the feasibility of using blockchain technology to enhance the security and privacy of fingerprint security systems.
Evaluating the system’s performance in real- world scenarios: While fingerprint security systems using Wi-Fi show promise in laboratory environments, it is essential to evaluate their performance in real-world scenarios. Future work can focus on conducting
large-scale field trials to assess the system’s effectiveness and identify potential limitations or challenges.

Conclusion

In summary, a fingerprint security system that employs Wi-Fi can serve as a secure and efficient method for authentication and access control. The system’s ability to validate a person’s identity based on their unique fingerprints makes it difficult for unauthorized individuals to access sensitive information or restricted areas. Additionally, the real-time communication between the fingerprint scanner and the central server facilitated by Wi-Fi technology enables quick response times and remote monitoring.
Nevertheless, to guarantee the system’s effectiveness and security, further research is necessary to improve the accuracy and reliability of fingerprint recognition algorithms, enhance the security of communication channels, explore the integration of other biometric modalities, investigate the potential for using blockchain technology, and evaluate the system’s performance in real-world scenarios.

BIBLIOGRAPHY

1. Jain, A. K., Ross, A. (2012) *Handbook of biometrics Springer US*
2. Gaur, M. S., Dhaka, V. (2015). *Fingerprint recognition based on minutiae extraction and matching*
3. *using GPRS International Journal of Computer Science and Mobile Computing*
4. Kumar, A., Singh, D. (2017) *A low-cost fingerprint recognition system using GSM module International*
5. *Journal of Applied Engineering Research*
6. Nagar, N., Suresh, S. (2018). *Fingerprint authentication system using GPRS and Arduino International*
7. *Journal of Computer Sciences and Engineering*
8. Suthar, M., Patel, S. (2020). *A novel approach for fingerprint recognition technology International Journal of Scientific and Technology Research*
9. Chaturvedi, S., Kesharwani, S. (2018). *A review of biometric authentication technology.*
10. *International Journal of Computer Applications*
11. Youtube
12. Wikipedia