IOT BASED HOME SECURITY SYSTEM USING FINGERPRINT AUTHENTICATION

[1]Balvantrao Gayatri Dhanaji, [2]Atkale Shreya Dayanand, [3]Atkale Sakshi Dayanand, [4]Sushil. S. Kulkarni

[123] B. Tech Students, [4] Head of Department
[1234] Department of Electronics and Telecommunication Engineering,
[1234]Karmayogi Institute of Technology, Shelve, Pandharpur, India.

Abstract: In recent years, home security has become a critical concern due to increasing incidents of theft and unauthorized access. Conventional locking systems based on keys and passwords suffer from several limitations such as duplication, loss, and vulnerability to guessing attacks. This paper presents an IoT-based home security system that integrates fingerprint authentication for secure access control. The system utilizes an ESP32 microcontroller, a fingerprint sensor, and an IoT platform to enable real-time monitoring and alerts. Only users are allowed entry after successful biometric verification, while unauthorized attempts trigger alerts to the homeowner. The proposed solution is cost-effective, reliable, and suitable for modern smart homes.

Index Terms **– IOT, Blynk, ESP32, Fingerprint Authentication, Home Security, Smart Lock.**

INTRODUCTION

Security is an essential requirement in modern households. Traditional locking mechanisms using keys or passwords are increasingly unreliable, as keys can be misplaced or duplicated and passwords can be guessed or shared. Therefore, there is a need for a more secure and intelligent system.

This work proposes a smart home security system that combines biometric authentication with Internet of Things (IoT) technology. Fingerprint recognition ensures that only authorized individuals can access the premises, while IoT connectivity allows remote monitoring and control.

NEED OF THE STUDY.

Security is a major concern in modern life. Traditional locks using keys or passwords can be easily broken or forgotten. To solve this, a smart and secure system using biometric technology and the Internet of Things (IoT) is introduced. The proposed system uses a fingerprint sensor to identify authorized persons and an IoT platform to monitor and control the door lock remotely. If the fingerprint matches the stored data, the system allows entry; otherwise, access is denied, and an alert is sent to the owner through the internet. This project provides a simple, low-cost, and reliable solution to modern home security problems.

In today's world, security has become a major concern for every household and workplace. Traditional locking systems that use keys or passwords are not completely safe keys can be lost or duplicated, and passwords can be guessed or forgotten. Hence, there is a strong need for a system that provides high security, reliability, and convenience. The IoT-based home security system using fingerprint fulfils this need by combining biometric technology (which ensures that only authorized persons can access) with IoT connectivity (which allows remote monitoring and control).

THEORETICAL FRAMEWORK.

Recent advancements in the Internet of Things (IoT) and biometric authentication technologies have significantly improved modern home security systems. Traditional security methods such as keys and passwords are vulnerable to theft, duplication, and unauthorized access. To overcome these limitations, researchers have focused on integrating biometric systems with IoT for enhanced security and remote monitoring.
Biometric authentication, according to Jain et al. (2016), fingerprint-based systems provide high accuracy due to the uniqueness and permanence of fingerprint patterns.

In the field of IoT, Gubbi et al. (2013) described IoT as a network of interconnected devices capable of collecting and exchanging data in real-time. This project implements a similar setup by using Biometric Authentication for fingerprint recognition and IoT dashboards for personal identification.

SYSTEM DESIGN.

This system is acts as a smart solution. This system is comprised of this two main functional blocks Home Security Unit and Fingerprint Authentication.

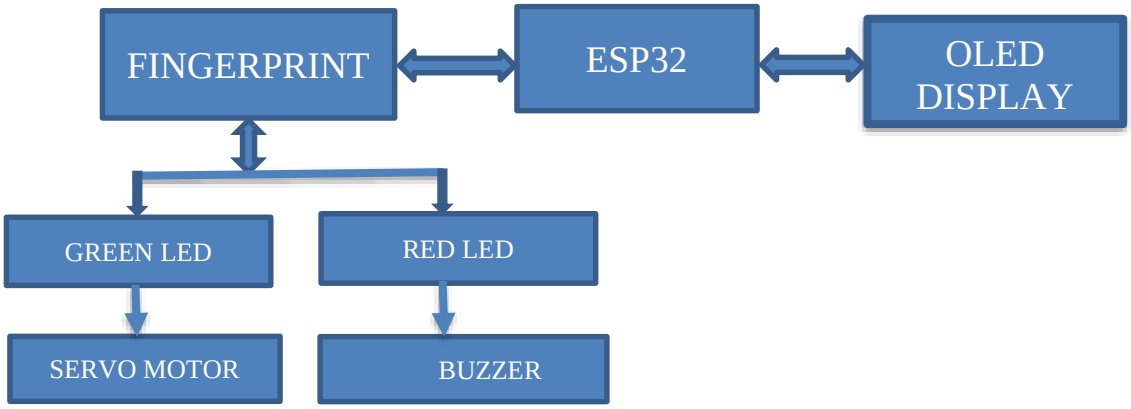


Fig 1: Block Diagram of IOT based Home Security System using fingerprint Authentication

4.1 Hardware Design.

- The ESP32 is the main processing unit of the system. It handles fingerprint recognition, controls the lock mechanism, and connects to the internet using Wi-Fi. It also sends notifications through the IoT platform when any event occurs.
- The fingerprint sensor is used to scan and verify the fingerprints of authorized users. It stores enrolled fingerprints in its internal memory and compares them during authentication. The servo motor or relay mechanism is connected to the door lock. When an authorized fingerprint is detected, the ESP32 activates the servo motor to unlock the door. After a few seconds, it automatically locks again.
- The Blynk IoT platform allows real-time monitoring and control of the home security system. The user can receive notifications, check access logs, or manually control the lock through the mobile application. Provides the required voltage (usually 5V and 3.3V) to all components. It includes a voltage regulator for stable operation. Provides alert indications.
- The buzzer or LED glows or beeps during access attempts—green for authorized entry, red for denied access.

4.2 Circuit Diagram and Working.

The circuit involves interfacing the fingerprint sensor, servo motor, LEDs, and buzzer with the ESP32 microcontroller. The fingerprint sensor sends digital data to the controller for authentication, and based on the result, the controller activates output devices such as the servo motor for door locking/unlocking and LEDs/buzzer for indication.

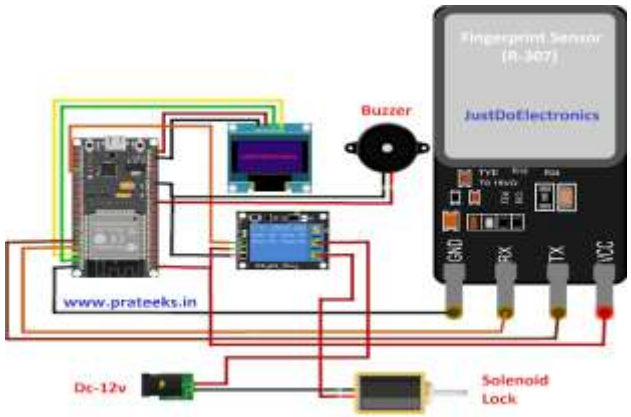


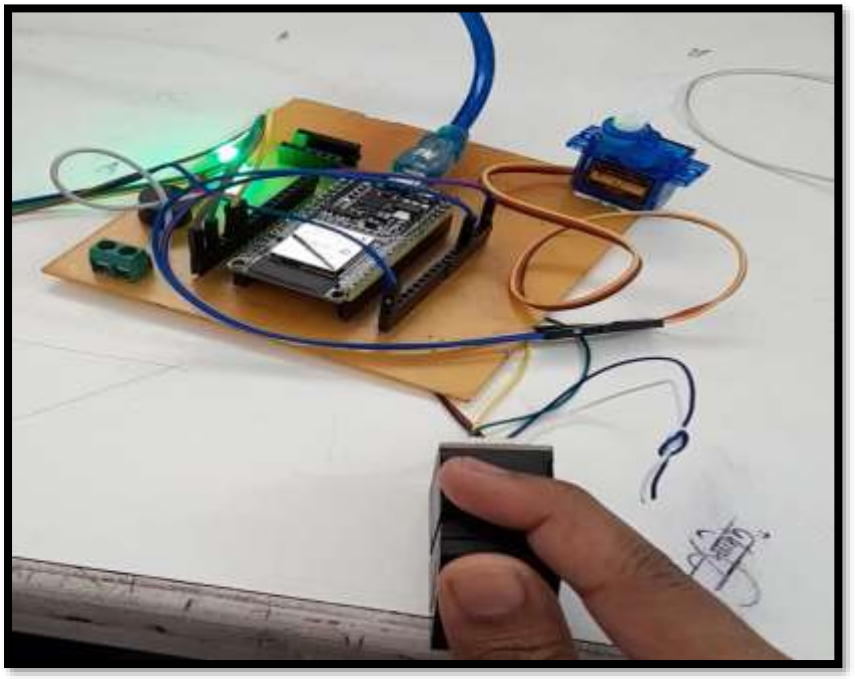
Fig 2: Circuit Diagram of the System

RESULTS AND DISCUSSION.

This system was tested under real-word condition**,** yielding results in both Fingerprint Authentication and IOT Dashboard (real-time monitoring).

5.1 Hardware Implementation.

The complete hardware setup, including the sensor interface and power supply, all hardware was assembled and tested successfully.



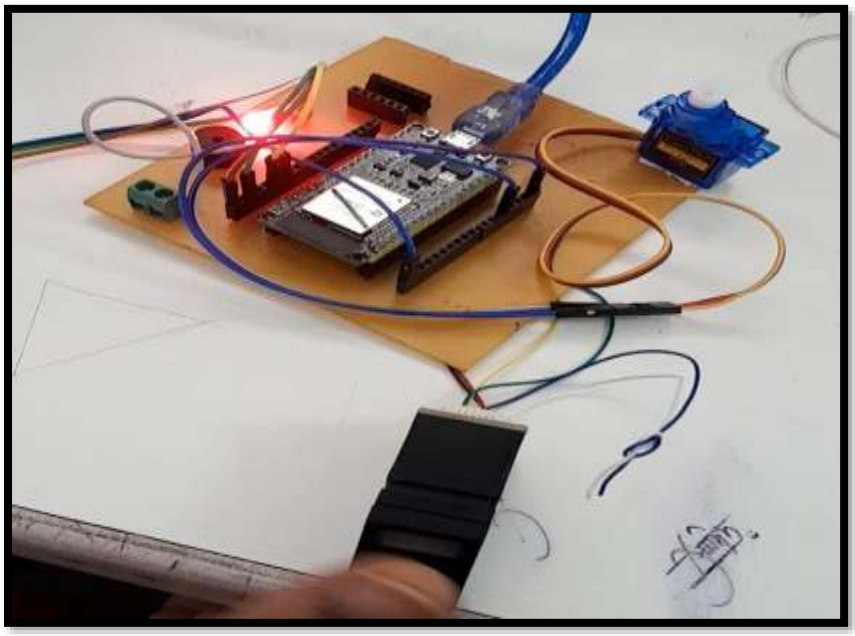


Fig 3: Hardware Project Phototype

5.2 Image Capturing and Analysis.

To Increase home security using fingerprint authentication, to Eliminate the need for traditional keys or passwords, to Provide real-time monitoring and control via IoT, to Send notifications or alerts when unauthorized access is attempted.

Fig 4: Web Interface showing Fingerprint based Home Security Authentication Results

5.3 IoT Sensor Monitoring.

The Blynk IOT dashboard are display the real-time access status of the home security system using fingerprint authentication

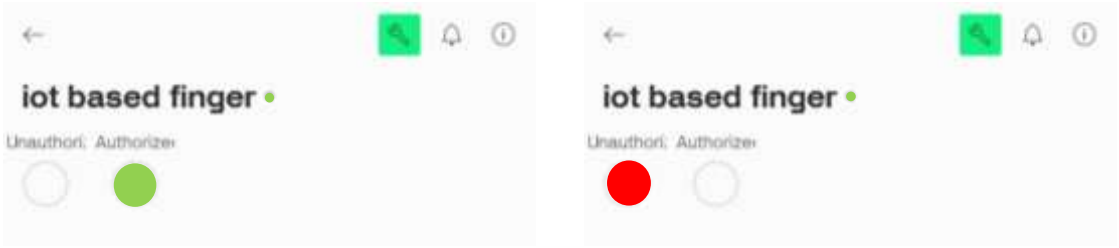


Fig 5: Blynk IOT Dashboard Display Real-Time Data

CONCLUSION.

The IoT-Based Home Security System using Fingerprint Authentication successfully demonstrates a modern, reliable, and secure method of controlling home access. By replacing traditional keys and passwords with biometric authentication, the system ensures that only authorized individuals can enter the premises. The integration of IoT technology further enhances the system by enabling real-time monitoring, instant notifications, and remote supervision through a mobile application. The results show that the fingerprint sensor provides accurate identification, while components like LEDs, buzzer, and door lock mechanism work smoothly to indicate system status. The system is cost-effective, user-friendly, and offers a higher level of security compared to conventional methods. Over all, this project proves that combining biometric identification with IoT can create a smart, automated, and highly secure home security solution suitable for modern households.

FUTURE SCOPE.

Future improvements include enabling fully automated cloud integration for real-time storage of access logs and alerts without manual intervention. Additionally, integrating advanced security features such as multi-factor authentication (fingerprint combined with face recognition or OTP) would further enhance system reliability. The system could also be expanded to include smart home automation features such as remote door control, CCTV integration, and voice assistant support for improved convenience and security.

ACKNOWLEDGEMENT

We would sincerely like to thank our HOD and Guide Sushil. S. Kulkarni for his constant encouragement and support in this project. We also thank our project coordinator prof. P. R. Kulkarni and Dr. S. P. Patil for providing the necessary facilities

REFERENCES

S. M. A. Zaidi, M. J. Khan, and A. Sadiq, "IoT Based Smart Home Security System Using Biometric Authentication," International Journal of Advanced Research in Computer Science, vol. 10, no. 5, pp. 45–50, 2020.

P. Verma and A. Tripathi, "Fingerprint Based Door Locking System," International Journal of Engineering Research & Technology (IJERT), vol. 8, no. 6, pp. 112–116, 2019.

T. Alma, "A Reliable Communication Framework and Its Use in Internet of Things (IoT)," International Journal of Scientific Research in Computer Science, vol. 3, no. 5, pp. 1–9, 2018.

A. K. Das and R. K. Mohapatra, "Biometric Security System using Microcontroller," International Journal of Computer Applications, vol. 180, no. 47, pp. 12–16, 2018.

M. A. Rahman et al., "Secure Smart Home Using IoT and Fingerprint Recognition," IEEE International Conference on Computing, Power and Communication Technologies, pp. 540–545, 2021.

M. A. Rahman et al., "Secure Smart Home Using IoT and Fingerprint Recognition," IEEE International Conference on Computing, Power and Communication Technologies, pp. 540–545, 2021.