Bulletin of the *Transilvania* University of Braşov • Vol. 18(67) No. 1 – 2025
Series I: Engineering Sciences
https://doi.org/10.31926/but.ens.2025.18.67.1.3

INTELLIGENT ACCESS SYSTEM BASED ON DIGITAL FINGERPRINT RECOGNITION

F. T. TELEKI[1] M. C. CARP[2]

Abstract: *This paper presents the design and implementation of an IoT-based biometric access control system that integrates ESP32, fingerprint recognition, and a web-based remote management platform. The system leverages FreeRTOS for efficient task scheduling and real-time processing, ensuring stable operation even during network disruptions. Experimental tests demonstrate a 98% fingerprint recognition accuracy, stable Wi-Fi connectivity, and low power consumption, confirming the system's feasibility and scalability. This work contributes to biometric authentication research by integrating modern security techniques with embedded IoT systems, making it a viable solution for smart buildings and secure access environments.*

Key words: *biometric authentication, internet of things (IoT), ESP32, FreeRTOS, fingerprint recognition, remote management.*

1. Introduction

The rapid development of Internet of Things (IoT) technologies has made secure and scalable authentication systems a priority for modern digital infrastructure. Traditional authentication mechanisms—such as passwords, access cards, or PINs—are frequently compromised due to loss, theft, or unauthorized duplication [1], [7]. Biometric authentication has emerged as a more secure alternative, leveraging unique biological characteristics to verify identity.

Among the most researched biometric modalities are fingerprint recognition, facial recognition, iris scanning, and hand geometry [2], [11]. While iris and facial recognition offer non-contact interaction and high accuracy, they also present higher implementation costs or susceptibility to spoofing. Fingerprint recognition remains the most balanced option, offering high security, low cost, rapid processing, and seamless integration in embedded platforms [5], [9]. Its practicality makes it ideal for IoT applications where local decision-making, real-time processing, and energy efficiency are essential.

This paper introduces an intelligent access control system based on fingerprint

[1] *Transilvania* University of Braşov, telekitibi21@gmail.com
[2] *Dept. of Electronics & Computers, Transilvania* University of Braşov

recognition, designed using the ESP32 microcontroller and integrated with a web-based management platform. By leveraging FreeRTOS, the system supports concurrent task execution and real-time responsiveness. Experi testing validates the system's performance in terms of fingerprint accuracy, Wi-Fi stability, and environmental resilience, suggesting its feasibility for use in real-world secure access scenarios.

2. System Architecture and Hardware Components

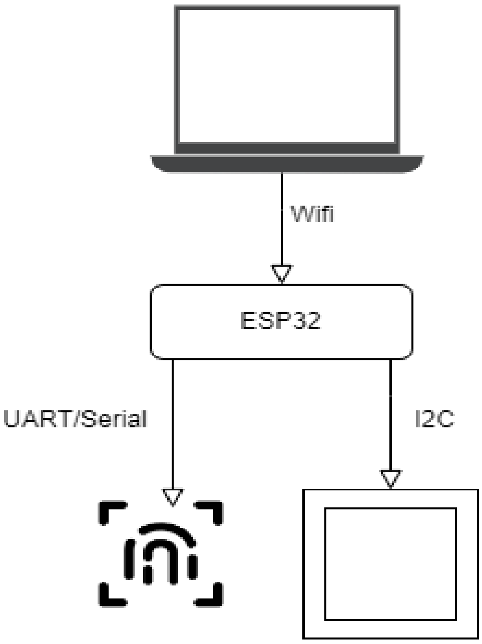

Fig. 1. *Hardware Diagram*

As illustrated in Figure 1, the overall hardware architecture highlights the main system components and their interconnections. The proposed system consists of an ESP32 microcontroller, a R307 fingerprint sensor, a 0.96-inch OLED display, and a web-based management platform integrated via Wi-Fi communication.

The ESP32 microcontroller was selected for its dual-core Xtensa LX6 processor, operating up to 240 MHz, its integrated Wi-Fi and Bluetooth capabilities, and 520 KB of SRAM, enabling efficient multitasking and real-time wireless communication under FreeRTOS [4], [10].

For fingerprint acquisition and recognition, the R307 fingerprint sensor was employed, offering 500 dpi resolution and the capacity to store up to 1000 fingerprints. Its high recognition speed and reliability make it ideal for secure access systems [5].

The OLED display (0.96 inches, 128×64 pixels, I2C interface) provides real-time feedback to users, indicating fingerprint scanning results and Wi-Fi connection status [2].

Components were interconnected via breadboard, enabling modular prototyping and easy upgrades without soldering.

3. Hardware Description and Electrical Schematic

The ESP32 was powered at 3.3V, as was the OLED display, while the fingerprint sensor was supplied with 5V, ensuring optimal operational stability.

The electrical schematic, illustrated in Figure 2 [3], shows the wiring connections between the ESP32, the fingerprint sensor (UART communication), and the OLED display (I2C communication). This modular configuration enhances system flexibility and debugging efficiency.

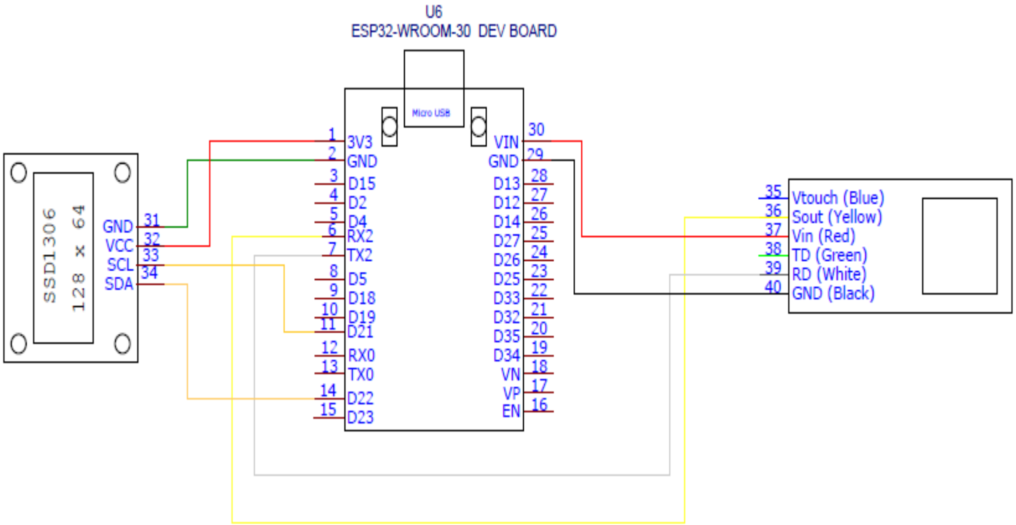

Fig. 2. *The electrical diagram was created using the Easy Eda platform [3], and it includes an ESP32, a fingerprint sensor, and an LCD*

4. Software Implementation and Task Management Using FreeRTOS

Software development was performed using Arduino IDE, utilizing ESP32-specific libraries for Wi-Fi and biometric functionalities [6]. Task scheduling and resource management were handled by FreeRTOS, ensuring efficient concurrent execution.

Two primary tasks were implemented:

- **FingerprintTask:** Responsible for fingerprint capture, processing, and authentication.
- **WiFiTask:** Responsible for maintaining Wi-Fi connectivity and transmitting authentication data to the remote server.

Synchronization between tasks was achieved using a binary semaphore, while access to shared resources such as the OLED display was protected using a mutex mechanism [7].

The software development process relied on several key tools. Arduino IDE was used for embedded C/C++ programming and deployment to the ESP32 microcontroller. XAMPP provided the backend environment, enabling Apache server and MySQL database simulation for local testing of the web-based platform. The user interface and server logic were built using HTML, CSS, and PHP, with Visual Studio Code facilitating modular development, version control, and debugging. This toolchain ensured a streamlined workflow and seamless integration between hardware-level fingerprint scanning and remote access management functionality.

This architecture ensures that fingerprint recognition operations are not disrupted by potential network instability and that resource conflicts are minimized.

5. Web Interface and Access Control System

To enhance functionality and scalability, a web-based interface was developed for remote management of the authentication system. The platform was built using an Apache web server, PHP scripting, and a MySQL database to store and manage fingerprint identifiers [6].

The authentication process operates as follows: the ESP32 captures the user's fingerprint, generates a unique identifier, and transmits it via HTTP POST requests to the server. The server verifies the identifier against records stored in the database. Upon successful validation, access is granted, and the event is logged for administrative review.

This approach enhances the system’s security and operational transparency, enabling real-time user registration, access logging, and assignment of role-based permissions through a secure web interface [8]. The interaction between the embedded system and the remote server is illustrated in Figure 3.

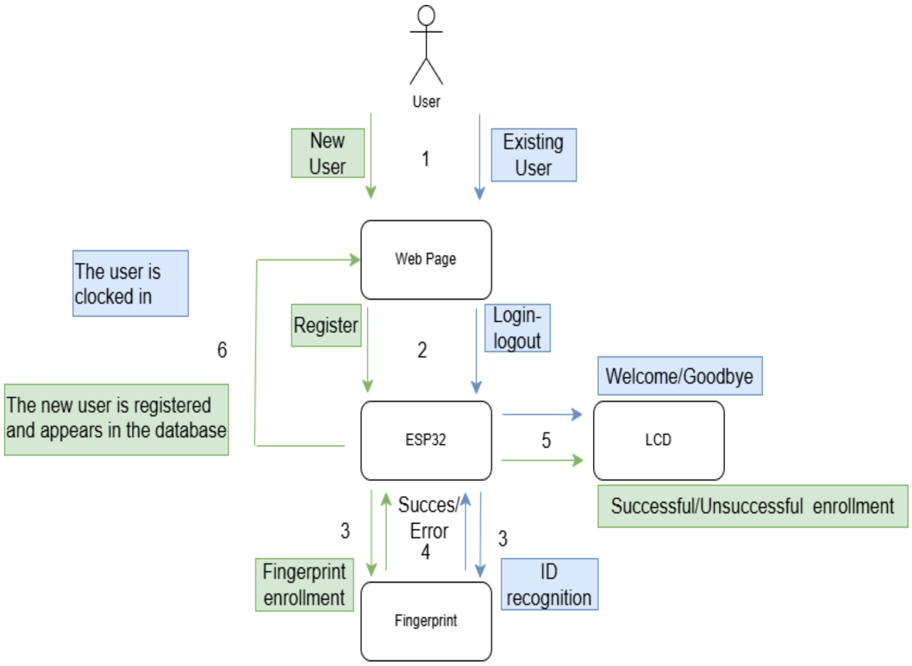

Fig. 3. *Software Diagram*

6. Performance Testing and Results

The system was evaluated based on fingerprint recognition accuracy, Wi-Fi stability, and power consumption.

6.1. Fingerprint Recognition Accuracy

Fingerprint recognition achieved 98% accuracy over 100 attempts. The detailed numerical results are summarized in Table 1.

Fingerprint acccuarcy Table 1

Number of Attempts	Recognition Time (sec)	Success Rate (%)
10	1.3	100
25	1.2	96
50	1.3	92

6.2. Wi-Fi Connectivity Stability Test

Wi-Fi stability tests demonstrated continuous operation over a 60-minute period without disconnection, as summarized in Table 2.

Stability test Table 2

Time (minutes)	Wi-Fi Connection Status
0-10	Stable
10-20	Stable
20-30	Stable
30-40	Stable
40-50	Stable

6.3. Power Consumption Analysis

The power consumption measurements are as follows:

- Idle Mode: 60 mA
- Scanning Fingerprint: 80 mA
- Wi-Fi Transmission: 100 mA

6.4. Resource Utilization and Reliability Test

Resource utilization was carefully measured to assess the system's memory management under FreeRTOS. Wi-Fi connection tasks consumed approximately 30% of available SRAM, fingerprint recognition processes required 40%, OLED display handling used 20%, and FreeRTOS background tasks utilized 10%, demonstrating efficient memory partitioning without resource overflows.

To validate system robustness, reliability tests were conducted under various environmental conditions. The authentication system achieved a success rate of 90% under high humidity, 85% under low temperature, 88% under high temperature, and 87% in dust exposure scenarios, confirming the system's stability and adaptability for real-world applications.

7. Finite State Machine (FSM) Authentication Flow

Authentication follows a Finite State Machine (FSM) model, ensuring reliable operation.

Initially, the system remains in an Idle state, awaiting a fingerprint scan. Upon fingerprint detection, the system transitions to Fingerprint Scanning, where the biometric data is processed. The next step is Verification, where the fingerprint is matched against stored database entries.

If the fingerprint is recognized, the system moves to Access Granted and transmits the confirmation data via Wi-Fi. If the fingerprint is not recognized, the system transitions to Access Denied and returns to Idle.

After successful data transmission during Wi-Fi Handling, the system resets to Idle, ready for the next authentication attempt.

This FSM structure ensures real-time decision-making, efficient resource management, and robust system behavior under normal and stressed operational conditions.

To enhance the security of data transmission between the ESP32 device and the web server, it is recommended to implement HTTPS communication protocols and server-side authentication mechanisms. These additional security layers help protect sensitive fingerprint data against potential interception or unauthorized access during remote operations. The authentication workflow is formally represented in Figure 4.

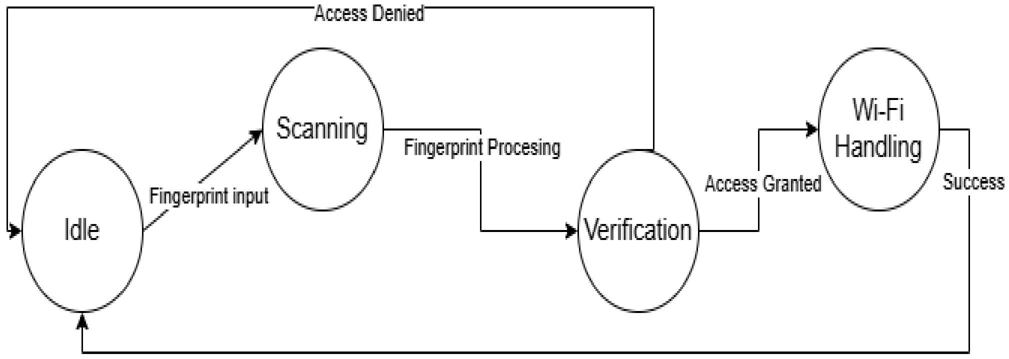

Fig. 4. *The FSM diagram illustrates the authentication process*

8. Conclusions

This study presented the development of an IoT-based biometric authentication system that integrates ESP32, fingerprint recognition, and web-based remote management. The use of FreeRTOS enabled efficient task scheduling and resource handling, ensuring continuous operation even under network instability.

Similar approaches and evaluations are discussed in the specialized literature. Experimental evaluations confirmed a 98% fingerprint recognition accuracy, stable Wi-Fi connectivity, and optimized power consumption, demonstrating the system's feasibility for real-world smart access applications.

The web interface enhances flexibility, allowing administrators to remotely manage users, permissions, and access logs.

Future improvements may include multi-factor authentication, cloud-based data storage, and mobile application integration, further enhancing system scalability and security. This work demonstrates the potential for combining biometric security and IoT technologies to deliver reliable, efficient, and scalable smart access control systems.

References

1. Bhattacharyya, D., Ranjan, R., et al.: *Biometric Authentication: A Review*. In: International Journal of u-and e-Service, Science and Technology 2 (2009), p. 13–28.
2. Da Xu, L., He, W., et al.: *Internet of Things in Industries: A Survey*. In: IEEE Transactions on Industrial Informatics 10 (2014) No. 4, p. 2233–2243.
3. EasyEDA: *EasyEDA Online PCB Design & Simulation Tool.* Available at: https://easyeda.com/ Accessed: 04.03.2025.
4. Espressif Systems: *ESP32 Datasheet. Espressif Systems*. 2018.
5. Li, L., Mu, X., et al.: *A Review of Face Recognition Technology.* In: IEEE Access 8 (2020), p. 139110–139120.
6. Maltoni, D., Maio, D., et al.: *Handbook of Fingerprint Recognition*. London. Springer, 2009.
7. Sicari, S., Rizzardi, A., et al.: *Security, Privacy and Trust in Internet of Things: The Road Ahead*. In: Computer Networks 76 (2015), p. 146–164.
8. Vincy, A. D., Sathana, S.: *Recognition Technique for ATM Based on Iris Technology.* In: International Journal of Engineering Research & Technology (IJERT) 7 (2019) No. 11, p. 1–5.
9. Yu, Y., Niu, Q. et al.: *A Review of Fingerprint Sensors: Mechanism, Characteristics, and Applications.* In: Micromachines 14 (2023) No. 6, p. 1253. https://doi.org/10.3390/mi14061253
10. Zanella, A., Bui, N., et al.: *Internet of Things for Smart Cities*. In: IEEE Internet of Things Journal 1 (2014) No. 1, p. 22–32.

11. Zheng, G., Wang, C.-J., et al.: *Application of Projective Invariants in Hand Geometry Biometrics*. In: IEEE Transactions on Information Forensics and Security 2 (2007), No. 4, p. 758–768.