IoT-ENABLED BIOMETRIC AND OTP-BASED SMART VAULT SECURITY SYSTEM

SUGANTH S.N, THAMEEN ANSARI. A, VIDYADHEESHA.M.PANDURANGI, YESHWANTH. R - B.E ECE
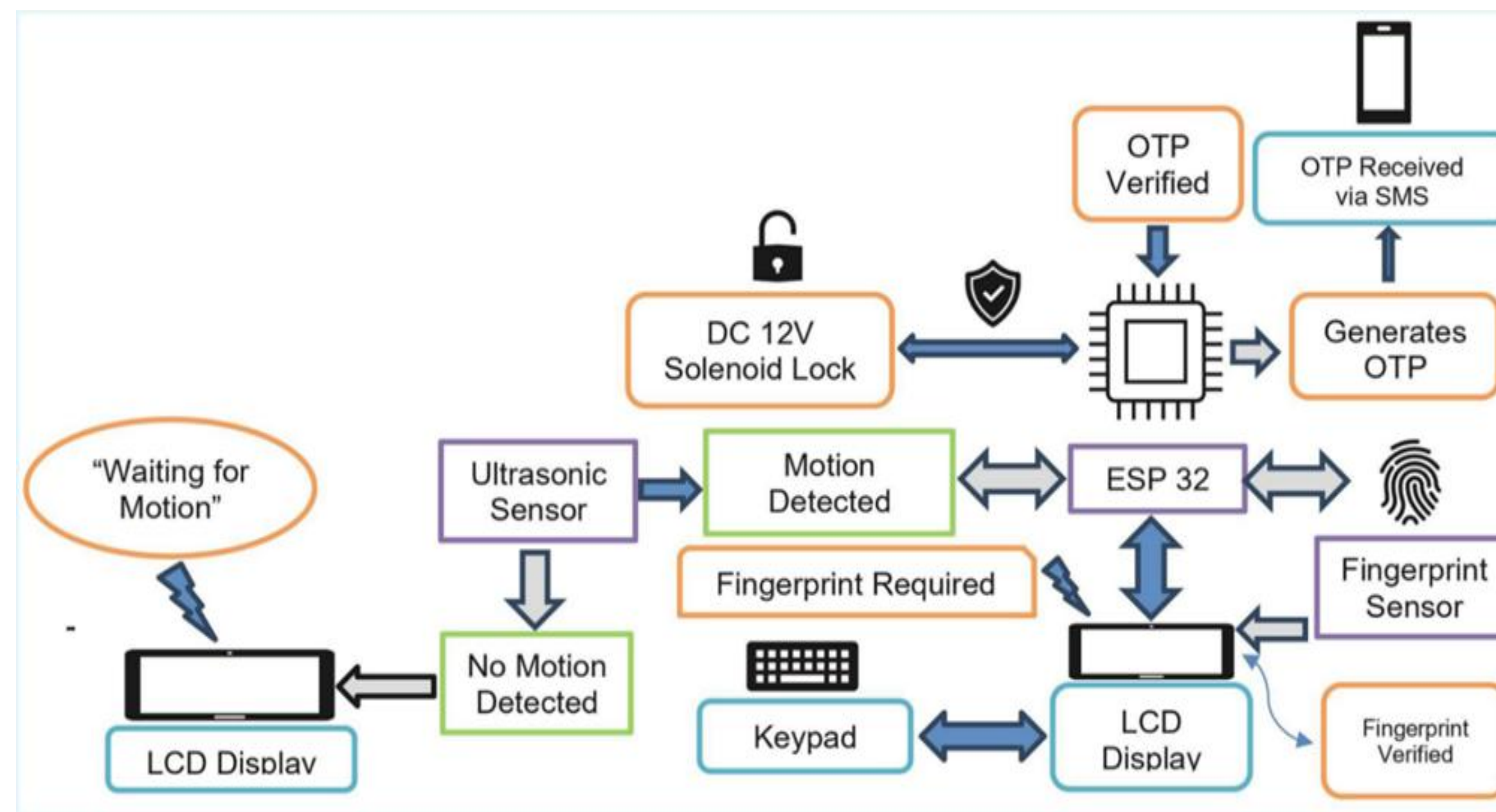### DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING
ADHIYAMAAN COLLEGE OF ENGINEERING [AUTONOMOUS] ,HOSUR – 635 109

OBJECTIVE

- To design a smart vault system using fingerprint and OTP authentication.
- To provide dual-layer security for preventing unauthorized access.
- To enable IoT-based monitoring and OTP transmission via Wi-Fi.
- To control a solenoid lock automatically using relay switching.
- To develop a low-cost, reliable, and scalable smart security system.
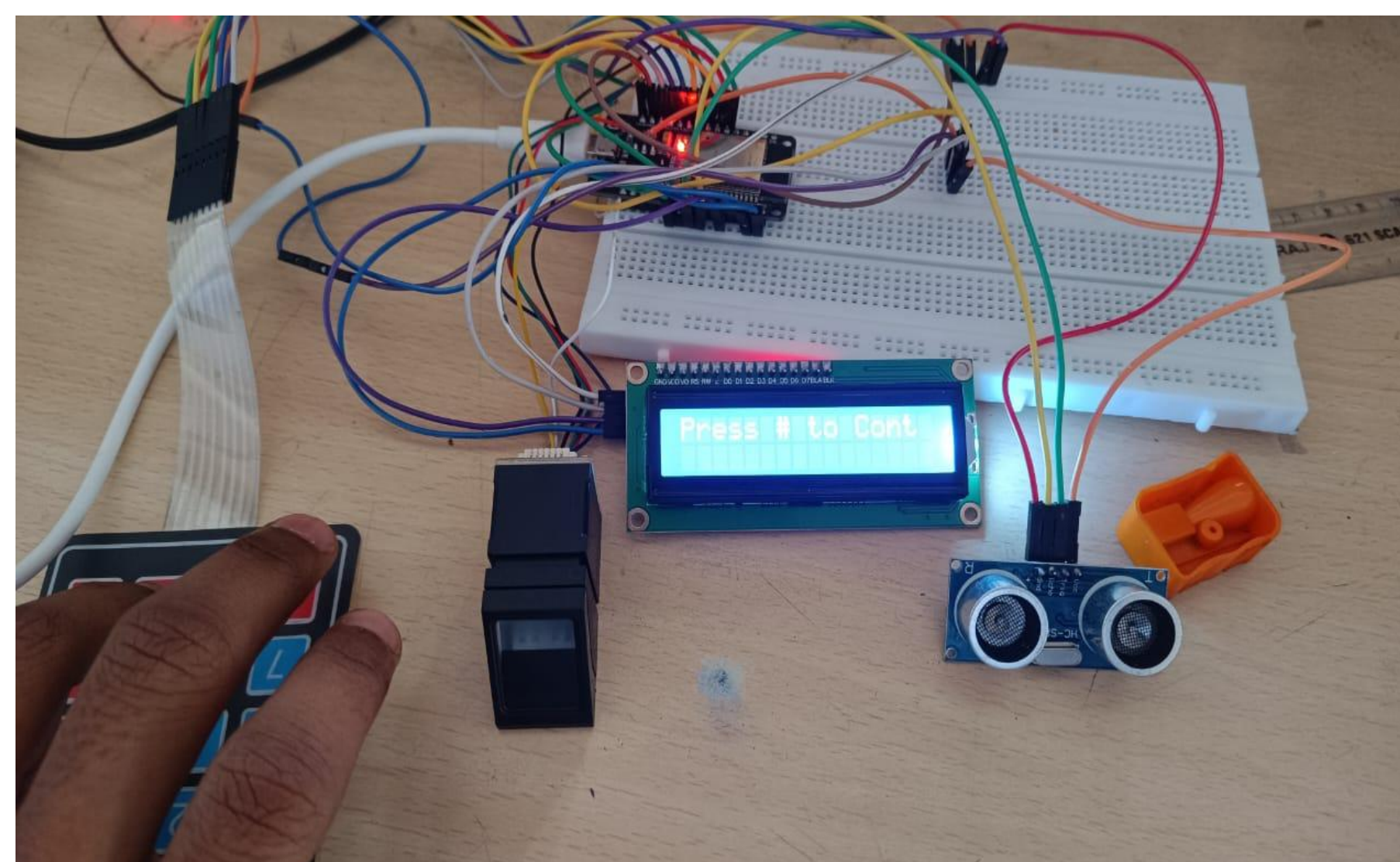
BLOCK DIAGRAM

WORKING PRINCIPLE

- **Object Detection:** The ultrasonic sensor detects a person or object within a fixed distance (e.g., 20 cm) to activate the system.
- **Fingerprint Authentication:** The user places their finger on the R307 sensor for biometric verification.
- **OTP Generation:** If the fingerprint matches, an OTP is generated and sent to the registered mobile number via Wi-Fi using the Twilio API.
- **OTP Verification:** The user enters the received OTP using the 4×4 matrix keypad for secondary authentication.
- **Lock Operation:** Upon successful OTP verification, the relay activates the solenoid lock to unlock the vault.
- **System Standby Mode:** When no object is detected by the ultrasonic sensor, the system remains in standby mode to save power.
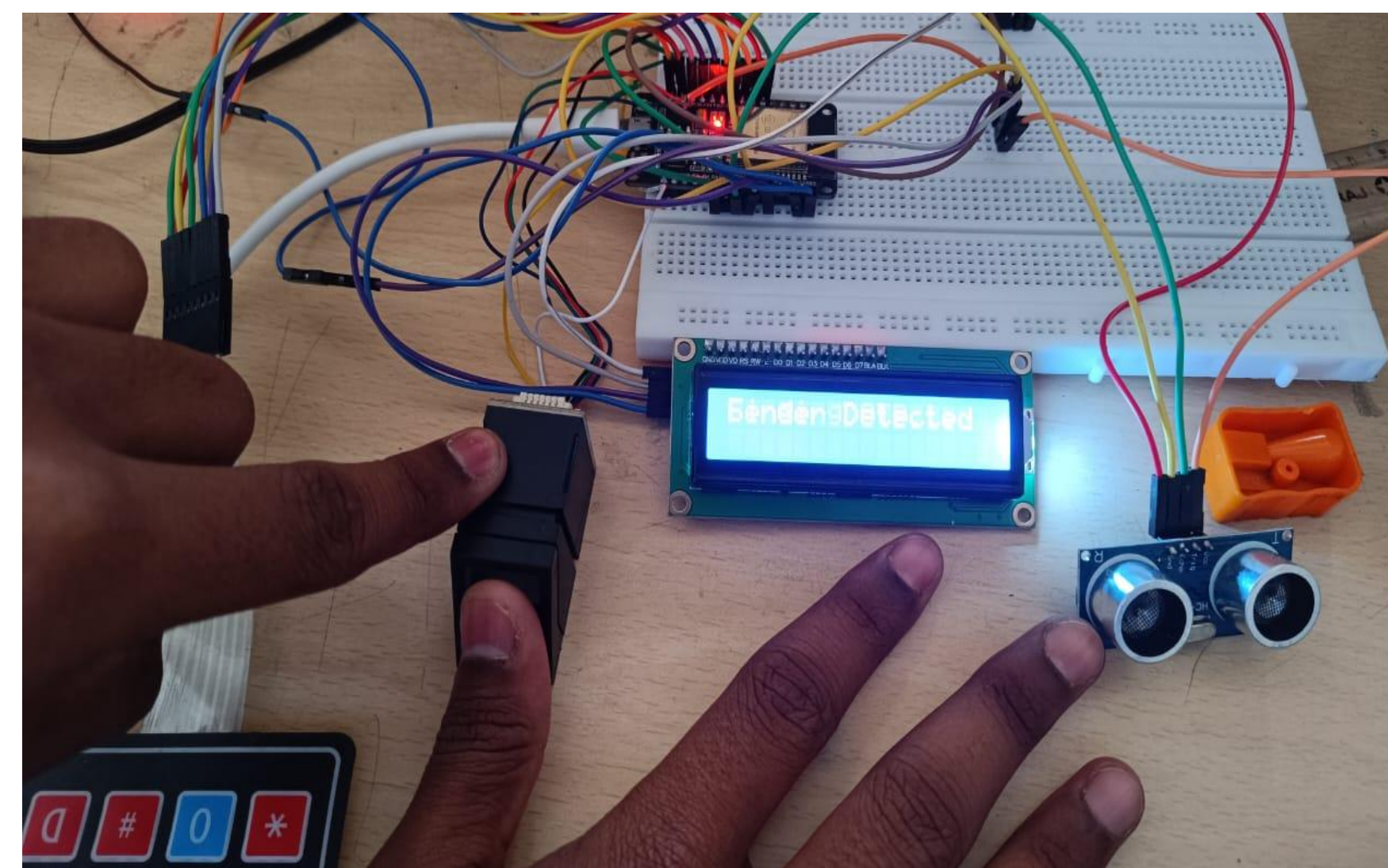
EXPERIMENTAL SETUP

- The ESP32, R307 & HC-SR04 sensor, I2C 16×2 LCD, keypad, relay, and solenoid lock are mounted on a breadboard.
- A 5V supply powers the ESP32, sensors, and LCD, while a 12V adapter powers the solenoid lock.
- The fingerprint sensor connects via UART pins, LCD via I2C, ultrasonic via TRIG and ECHO pins, keypad to GPIOs, and relay to a control pin.
- Wi-Fi credentials are set in the code for OTP transmission through the Twilio API.
- Fingerprints are enrolled using the keypad, and the ultrasonic sensor activates the system when an object is detected within 20 cm.
- After OTP verification, the relay activates to unlock the solenoid lock.
- The LCD displays the process status, and the serial monitor helps in debugging and observation.
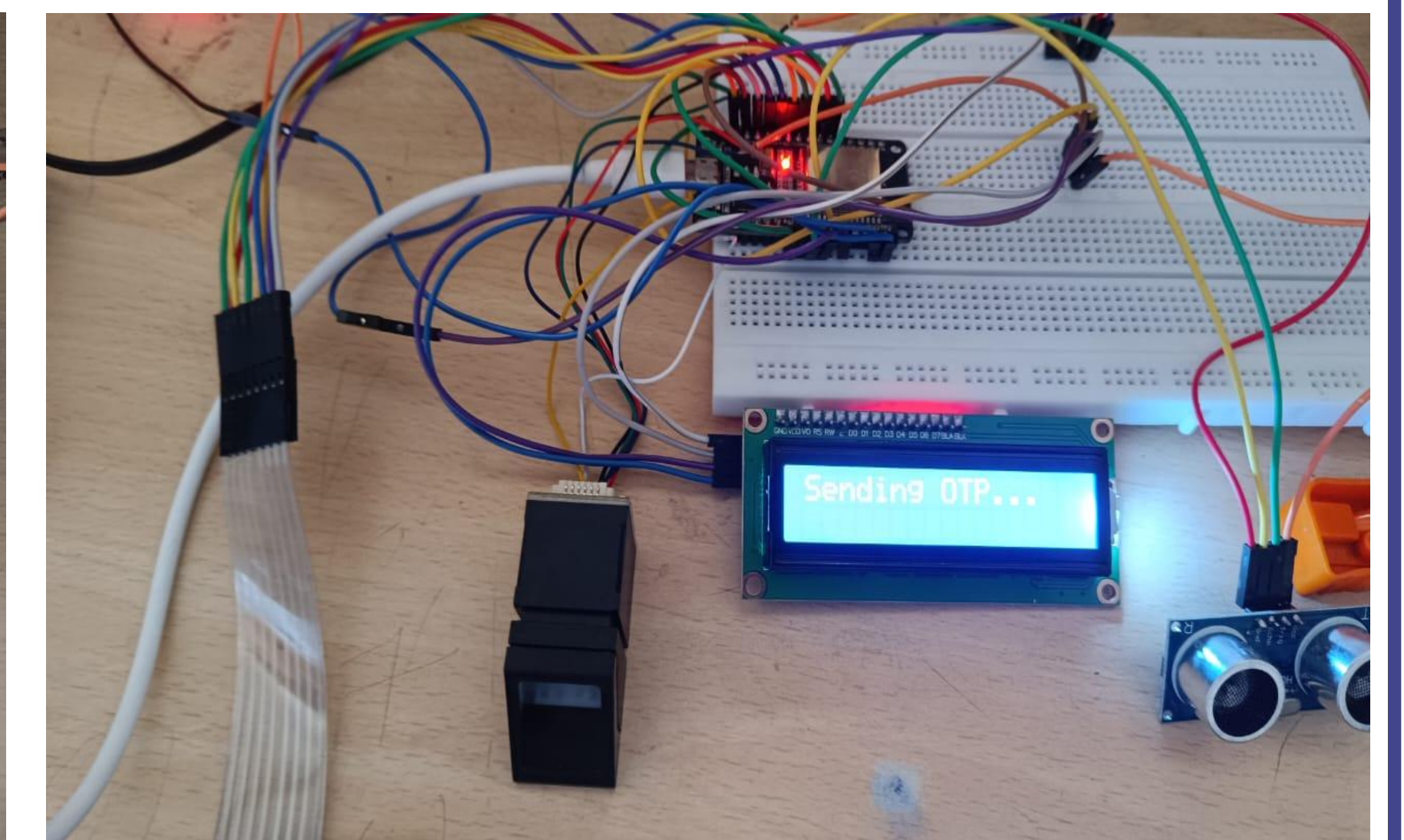
EXPERIMENTAL RESULTS

Press # to verify the Fingerprint

Placing the Fingerprint to verify

Verifying the OTP to unlock the door

LIST OF PUBLICATIONS

[1] J. Kook, "Design and Implementation of an OTP-Based IoT Digital Door-Lock System," Int. J. Eng. Res. Technol. (IJERT), vol. 12, no. 11, pp. 112–118, 2019.

[2]W. Yang, X. Hu, J. Guo, N. Yan, and L. Wu, "Biometrics for Internet-of-Things Security: A Review," Elsevier / PMC, pp. 1–15, 2021.

[3] S. R. Patel and G. Mehta, "Dual Authentication Method for Secure Access Using Biometrics and OTP," Int. Journal of Computer Applications, vol. 182, no. 32, pp. 18–24, 2022

[4] M. K. Hussain and A. Kumar, "IoT-Based Smart Locker with Biometric and OTP Authentication System," IEEE Int. Conf. Electronics, Communication and Control Systems, pp. 85–90, 2022.

[5] R. Paneru, S. Shah, and P. Paneru, "An IoT Based Smart Security Locker System with OTP Verification," in Proc. Int. Conf. Adv. Comput. Tech., pp. 245–250, 2023.

CONCLUSION

The IoT-Enabled Biometric and OTP-Based Smart Vault Security System successfully integrates fingerprint authentication, OTP verification, and IoT technology to ensure high-level security. The system provides dual-layer protection, preventing unauthorized access and improving reliability over traditional locking methods. Using the ESP32 microcontroller with Wi-Fi connectivity enables real-time OTP transmission and remote monitoring. The combination of biometric verification and OTP ensures both user convenience and data safety. The designed prototype proves to be cost-effective, efficient, and scalable for smart lockers, home vaults, and industrial applications. Overall, the project demonstrates an innovative approach toward modern, secure, and intelligent vault systems using IoT.

SUPERVISOR : Dr. S. SUMATHI