Report of Biometrics

Professor: Dr. Lamiaa Said

TA(s): Eng. Hossam Eldin Abdelhamed

Team Member:

Naira Gamal Badry	ID :202301234
Basma Sameh Mohamed	ID :202301148
Mariam Wael Mohamed Gamaleldin	ID :202302146
Nourhan khalid Elfakharany	ID :202303319
Shaimaa Mohi Gaber	ID :202300897
Yasmin Abdelaziz Ramadan	ID :202400477

Report of Biometrics

Project Report: Advanced 2FA Biometric & RFID Access Control System

1. Introduction

This project implements an advanced **Two-Factor Authentication (2FA)** Security System. Unlike standard security systems, this solution integrates **Biometric Identification (Fingerprint)** with **Radio Frequency Identification (RFID) technology**.

The system is designed to provide high-level security for restricted areas. Access is only granted if the user possesses a valid RFID tag and provides a matching fingerprint. An **I2C LCD screen** has been integrated to provide real-time user guidance, replacing the basic Serial Monitor dependency.

2. System Architecture & Design

The system logic follows a sequential security flow:

1. **Stage 1 (RFID):** The system waits for an **RFID card**. If the card is an **"Admin Card",** it opens a management menu. If it's a "User Card", it proceeds to the next stage.
2. **Stage 2 (Biometrics):** After card validation, the user must scan their fingerprint.
3. **Final Action:** If both factors match, the **system grants access**, triggers a green LED, and sounds a success beep.

Hardware Components Communication

- **Arduino UNO**: The central processing unit.

Report of Biometrics

- **R307 Fingerprint Sensor:** Communicates via **SoftwareSerial** (Pins 2 & 3).
- **RC522 RFID Reader**: Communicates via **SPI Protocol** (Pins 9, 10, 11, 12, 13).
- **I2C LCD (16x2):** Communicates via **I2C Protocol** (Pins A4 & A5) to display status.
- **Buzzer & Dual LEDs:** Provide audio-visual feedback on pin 8 (Buzzer), 11 (Green LED), and 12 (Red LED).

3. Circuit Diagram & Wiring Documentation

Connections Used:

Component	Arduino Pin	Purpose
Fingerprint TX/RX	D2 / D3	Biometric Data Transfer
RFID (SDA / RST)	D10 / D9	SPI Chip Select & Reset
RFID (SCK/MOSI/MISO)	D13 / D11 / D12	SPI Data Bus
LCD (SDA / SCL)	A4 / A5	I2C Communication
Buzzer	D8	Audible Alerts
Green / Red LEDs	D11 / D12	Status Indicators

4.Algorithm & Logic Flow

Admin Mode (Management)

- Triggered by a specific **Admin UID** (Hardcoded in Flash memory using PROGMEM to save RAM).
- Allows the administrator to **Enroll** new fingerprints or **Delete** existing ones via the Serial Monitor.

User Mode (Authentication)

1. **Scan RFID Card:** System reads UID.

2. **Fingerprint Prompt:** LCD displays "Place Finger".
3. **Verification:** System searches the sensor's database.
4. **Result:** LCD show

Memory Management

Fingerprint templates are stored locally on the sensor's flash memory, while the Admin UID is stored in the Arduino's flash memory to save RAM.

5. Software Implementation

- **Memory Optimization:** The code uses F() macro for strings and PROGMEM for static data to minimize RAM usage.
- **State Machine:** The system uses an enum (SystemMode) to switch between scanning, enrolling, and verifying modes efficiently.
- **Timeout Mechanism:** An **Admin Timeout (30 seconds)** is implemented to automatically exit admin mode if the system is left idle, enhancing security.

6.Testing & Results

- **Scenario A (Valid Card + Valid Finger):** Access Granted immediately.
- **Scenario B (Valid Card + Unknown Finger):** Access Denied; LCD displays "Not Registered".
- **Scenario C (Invalid Card):** System remains in "User Mode" or rejects the card before reaching the fingerprint stage.
- **Scenario D (Admin Access):** Successfully entered the management menu to add/remove users.

7. Creativity & Innovation

- **2FA Integration:** Moving from a simple password to a more secure "What you have" (RFID) and "Who you are" (Fingerprint) system.

- **Hardware Evolution:** The project was upgraded from a Keypad-based design to a more modern, contactless RFID and LCD interface.
- **Stand-alone Capability:** The system can operate without a PC once initial enrollment is complete.

8. Final Demo & Operation Guide

The final prototype demonstrates a fully functional standalone security system. The demonstration covers the following operational phases:

A. System Initialization

- Upon powering the Arduino via USB or external power, the **I2C LCD** initializes and displays "Fingerprint Sys".
- The system performs a self-check on the fingerprint sensor. If successful, the green LED blinks, and the LCD prompts: "**Scan RFID Card**".

B. Admin Management (via Serial Monitor)

- **Accessing Menu:** When the pre-coded **Admin RFID Tag** is scanned, the LCD displays "Admin Access Granted".
- **Enrollment (Mode 1):** The administrator uses the Serial Monitor to assign an ID (1-127). The LCD guides the user through "Step 1/2" and "Step 2/2" of the fingerprint scan.
- **Deletion (Mode 3):** The administrator can remove specific users by entering their ID in the Serial Monitor.

C. Two-Factor Authentication (User Access)

1. **Card Verification:** The user scans their RFID tag. If valid, the system moves to the second factor.

2. **Biometric Scanning:** The LCD prompts "Place Finger".
3. **Validation:**
    - **Success:** If the fingerprint matches the database, the **Green LED** lights up, the **Buzzer** emits a high-pitched success tone, and the LCD displays "Verified!".
    - **Failure:** If the fingerprint is unrecognized, **the Red LED** lights up, a low-pitched error tone sounds, and the LCD displays "Not Found".

D. Security Features Demonstrated

- **Admin Timeout:** If the admin menu is accessed but no action is taken for 30 seconds, the system automatically logs out and returns to "Scan RFID" mode to prevent unauthorized access.
- **Visual & Audio Feedback**: Every action (scanning, success, error) is confirmed by a specific LED color and Buzzer frequency.

Future Work

- **IoT Integration:** Connecting the system to Wi-Fi (using ESP8266) to send mobile notifications when someone tries to access the system.
- **Database Expansion:** Adding an SD card module to log every entry attempt with a timestamp (Date and Time).
- **Physical Actuator:** Connecting a **Solenoid Door Lock** or a Servo Motor to physically open a door upon successful verification.
- **Mobile App:** Developing a mobile application to manage users (add/delete) remotely instead of using the Serial Monitor..