Automated Access Control Gate System

GROUP 1:

KIONI ALLAN MUHORO

PETER MUNGAI

PAUL MUIGAI

JAMES WAINANA



Below is the updated detailed documentation for the project, reflecting the change from a servo‐driven gate to a solenoid lock mechanism. This document includes

1. the problem statement
2. proposed solution
3. system functionality
4. a list of required components (with additional information about the solenoid lock mechanism)
5. recommendations for large-scale deployment.

**Automated Access Control Gate System with Solenoid Lock**

**1. Introduction**

This project implements an automated access control system designed to secure entry through a physical gate that operates like a valve—allowing only one person to enter at a time. The system primarily uses fingerprint authentication for secure access and falls back on RFID and OTP (One-Time Password) verification if biometric authentication fails. Additional system management features include a restart prompt (secured by a PIN) and an assistance call function. In this version, the physical locking mechanism is implemented using a solenoid lock instead of a servo motor.

**2. Problem Statement**

**Security Challenge:**  
Many facilities require controlled access to prevent unauthorized entry and tailgating. Traditional systems may permit multiple persons to enter after a single authentication event, posing a significant security risk.

**Key Issues:**

* **Authentication Accuracy:** Ensure that each entry is individually authenticated using a robust biometric method.
* **Tailgating Prevention:** Guarantee that only one person enters per authentication event.
* **Redundant Verification:** Provide a fallback method (RFID+OTP) if the primary fingerprint sensor fails.
* **Physical Locking:** Implement a physical locking mechanism that effectively prevents unauthorized entry.
* **System Management:** Include secure methods for system restart (with PIN verification) and a means to call for assistance.

**3. Proposed Solution**

The proposed solution is an Arduino-based access control system that:

* **Primary Authentication:** Uses fingerprint data (input via Serial in simulation) to verify the user's identity.
* **Fallback Authentication:** After a set number of fingerprint failures, the system switches to RFID-based authentication. If a matching RFID is found, the user is prompted to enter an OTP using a keypad.
* **Physical Locking via Solenoid Lock:**  
  Instead of a servo motor controlling a gate, a solenoid lock mechanism is used. When activated (energized), the solenoid unlocks the door for a brief period, allowing one person to enter before it automatically re-locks.
* **User Feedback:**  
  An LCD display (non-I2C, 16×2) shows clear, scrolling messages to guide the user through the process.
* **System Management:**  
  Two buttons provide additional control:
  + **Button 1:** A short press initiates a restart prompt requiring a secure PIN (with a maximum of 3 attempts), while a long press cancels the prompt.
  + **Button 2:** Calls for assistance, alerting security personnel.
* **Debouncing:**  
  The Bounce2 library is used to ensure reliable button inputs.
* **Serial Debugging:**  
  Events are logged to the Serial monitor for troubleshooting and debugging.

**4. System Functionality**

**4.1 Standby and Primary Authentication**

* **Standby Mode:**  
  The LCD displays a scrolling “Scan Fingerprint” message. The system awaits fingerprint input via the Serial monitor (which simulates the fingerprint sensor).
* **Fingerprint Verification:**  
  When a fingerprint is received (prefixed with “FP:” via Serial), it is checked against a built-in user database.
  + If a match is found, the LCD displays a welcome message (e.g., “Welcome Alice”), and the solenoid lock is energized to unlock the door briefly.
  + If the fingerprint does not match, a failure counter increments. After five failed attempts, the system switches to fallback mode (RFID+OTP).

**4.2 Fallback Authentication (RFID + OTP)**

* **RFID Input:**  
  In fallback mode, the system listens for RFID data (prefixed with “RFID:” via Serial).
  + If a matching RFID is found, the LCD prompts the user to enter a 4‑digit OTP using the keypad.
  + If the OTP is correct (statically set as “7890” in this version), the solenoid lock is activated to unlock the door.
  + The RFID fallback is limited to 3 attempts, after which fallback mode is cancelled.

**4.3 Physical Locking Mechanism (Solenoid Lock)**

* **Solenoid Lock:**  
  The solenoid lock replaces the servo motor as the actuation mechanism. When activated, it energizes the solenoid to disengage the locking mechanism, allowing the door to unlock for a brief period. After a set delay, the solenoid is de-energized to re-lock the door, ensuring that only one person is admitted per authentication cycle.

**4.4 System Management via Buttons**

* **Button 1 (Restart):**
  + **Short Press:**  
    Initiates a restart prompt by displaying “Enter Restart PIN” on the LCD. The user must then enter a secure PIN via the keypad. A maximum of 3 incorrect attempts is allowed.
  + **Long Press:**  
    Cancels the restart prompt immediately if it is active.
* **Button 2 (Assistance):**  
  When pressed, the system displays “Calling Assistance” and logs a message via Serial. This alerts security personnel that help is needed.

**4.5 LCD Scrolling**

* **Scrolling Text:**  
  A helper function scrolls any text longer than 16 characters, ensuring that complete messages (e.g., “Welcome [User]” or “Use RFID+OTP”) are visible on the LCD.

**5. Components Required**

**5.1 Main Components**

* **Arduino Uno (or Compatible Microcontroller):**  
  Central controller for processing sensor inputs and controlling outputs.
* **Non-I2C 16×2 LCD Display:**  
  Used for displaying system messages. Uses parallel wiring (RS, EN, D4–D7).  
  *Example: LM016L or a similar character LCD.*
* **4×3 Matrix Keypad:**  
  For entering OTP and restart PIN.
* **Solenoid Lock Mechanism:**  
  Replaces the servo motor for physical access control. The solenoid lock is an electromechanical device that, when energized, disengages the lock to allow access. It then automatically re-engages after a set time.  
  *Additional Information:*
  + **Design:** The lock is designed to operate quickly, releasing the door for a short period before re-locking.
  + **Operation:** Typically controlled via a transistor or relay circuit with flyback diode protection.
  + **Photos/Diagrams:**



* **Two Push-Buttons:**
  + **Button 1:** Used for system restart prompt and cancellation.
  + **Button 2:** Used for calling assistance.
* **Fingerprint Sensor (or Simulation via Serial):**  
  For primary biometric authentication. In simulation, fingerprint input is provided via Serial with a prefix “FP:”.



* **RFID Reader (or Simulation via Serial):**  
  Serves as a fallback authentication method. In simulation, RFID input is provided via Serial with a prefix “RFID:”.



* **Bounce2 Library:**  
  For debouncing push-buttons reliably.
* **Keypad, LiquidCrystal, and Servo Libraries:**  
  For interfacing with the keypad, LCD, and controlling the solenoid lock (if using a relay/transistor interface, you might substitute the Servo library code with digital output control).

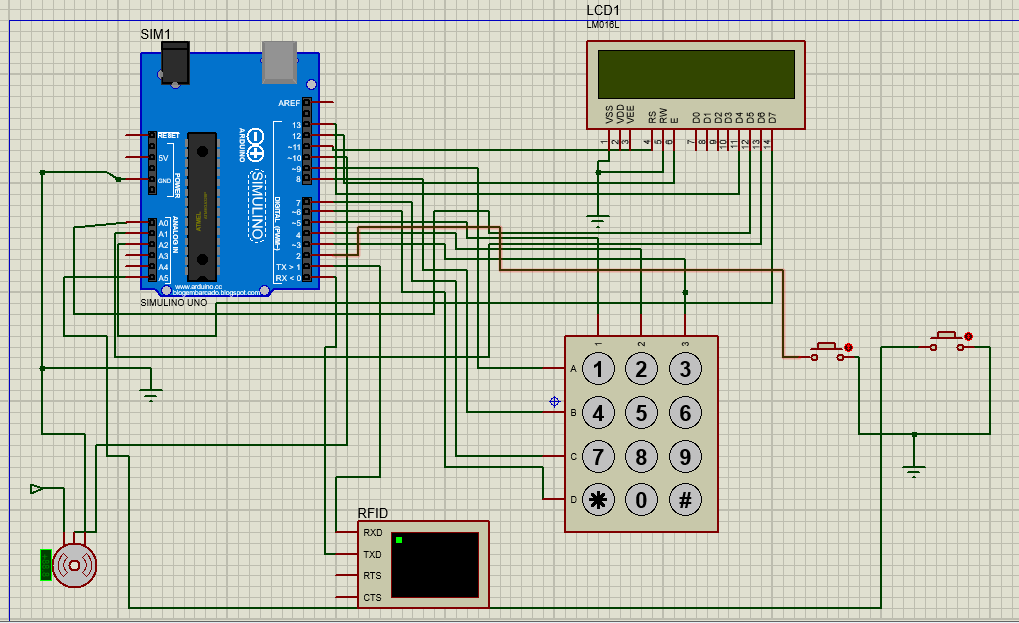
**5.2 Additional Components for Physical Deployment**

* **Power Supply:**  
  A stable power source (or battery pack) suitable for powering the microcontroller and solenoid lock.
* **Driver Circuit for the Solenoid Lock:**  
  Typically a transistor or relay circuit with a flyback diode to safely switch the solenoid.
* **Wiring, Breadboard/PCB, and Connectors:**  
  For making reliable electrical connections.
* **Enclosure:**  
  To house and protect the components.

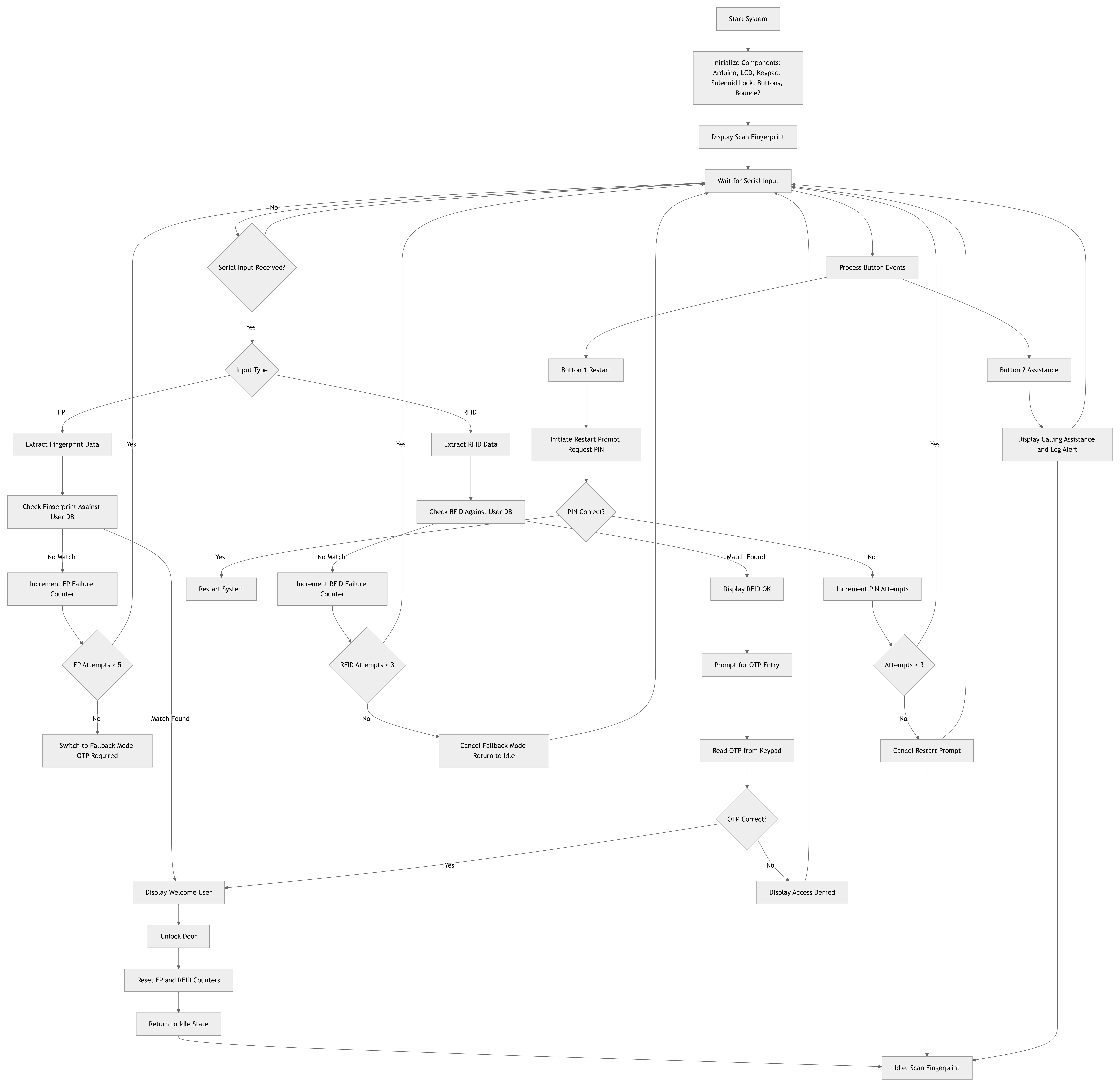


* **Valve-Like Gate System:**  
  A gate mechanism engineered to allow one person to enter at a time, mimicking a valve.  
  *Additional Information:*
  + **Design Considerations:** The gate system should physically block access until the solenoid lock is activated, ensuring that only one person can pass through before it re-locks.
  + **Photos/Diagrams:**.

**Circuitry Diagram**



FLOW CHART

****

**6. Large-Scale Deployment Considerations**

For a large-scale implementation (e.g., on a corporate campus or in a secure facility), several enhancements would be required:

**6.1 Centralized User Database**

* **Database Integration:**  
  Replace the internal user array with a centralized database (such as MySQL, PostgreSQL, or a cloud-based NoSQL solution) that stores user credentials (fingerprint templates, RFID IDs, names).
* **Remote Management Portal:**  
  Develop a web-based interface for administrators to add, update, or remove user information in real time.

**6.2 Networking and IoT Integration**

* **Network Connectivity:**  
  Equip each access control unit with WiFi, Ethernet, or cellular connectivity to enable remote monitoring, event logging, and firmware updates.
* **Cloud Services:**  
  Aggregate data from multiple access points in the cloud for centralized monitoring and analytics.

**6.3 Enhanced Hardware**

* **Industrial-Grade Components:**  
  For outdoor or high-traffic areas, use components rated for industrial use with appropriate weatherproofing.
* **Advanced Sensors:**  
  Incorporate additional sensors (e.g., door position sensors, motion detectors) to ensure the solenoid lock has fully engaged and to prevent tailgating.
* **Power Backup:**  
  Integrate UPS systems or solar power to maintain operation during power outages.

**6.4 Improved Software Architecture**

* **State Machine Implementation:**  
  Use a state machine to manage complex interactions and multiple authentication states.
* **Secure Communication:**  
  Encrypt data transmissions and use secure protocols (e.g., HTTPS, MQTT over TLS) to protect sensitive information.
* **Remote Diagnostics and OTA Updates:**  
  Allow remote troubleshooting, diagnostics, and firmware updates.

**6.5 Scalability and Maintenance**

* **Modular Design:**  
  Design the system in a modular way so that each unit (authentication, lock control, communication) can be independently upgraded or maintained.
* **Centralized Monitoring:**  
  Deploy centralized monitoring software that can alert administrators to potential issues across all access points.

**7. Conclusion and Future Improvements**

The Automated Access Control Gate System with a Solenoid Lock offers a robust solution for secure, single-user entry. It uses multi-factor authentication (fingerprint with RFID+OTP fallback) to ensure that only authorized individuals can access the facility, and it integrates system management features such as restart prompts and assistance calls.

For large-scale deployments, transitioning to a centralized user database, adding network connectivity, using industrial-grade hardware, and enhancing the software architecture will improve security, scalability, and maintainability.

This documentation provides a comprehensive overview of the project’s functionality, the problem it addresses, and the solution implemented—including a detailed list of required components and considerations for large-scale deployment.