Project: Secure Digital Lock with Encrypted SQLite User Management & FPGA Control

This project implements a smart digital lock system using an Android app for user authentication and an FPGA for access control. The Android app manages user accounts and stores credentials securely in an encrypted SQLite database, while the FPGA verifies the PIN and controls the lock mechanism.

---

FPGA (50%) – Custom VHDL/Verilog Implementation

✅ UART Receiver Module → Receives AES-encrypted PIN from the Android app over Bluetooth (HC-05).

✅ AES-128 Decryption Core → Decrypts the received PIN using a custom AES module in VHDL/Verilog.

✅ PIN Authentication Module → Compares the decrypted PIN against stored user PINs in FPGA memory.

✅ Lock Control System → If authentication is successful, generates PWM signals to rotate a servo motor (or activate a relay) to unlock the system.

✅ Status Feedback → Displays lock status (Locked/Unlocked/Error) on LEDs or a 7-segment display.

---

Android App (50%) – User Management & Secure Communication

✅ User Registration & Authentication → Allows users to create accounts, store their passwords and PINs, and log in securely.

✅ SQLite Database with AES Encryption → Stores user credentials locally using SHA-256 password hashing and AES-encrypted PINs.

✅ PIN Transmission with AES-128 Encryption → The app encrypts the PIN before sending it over Bluetooth UART (HC-05) to prevent eavesdropping.

✅ Bluetooth Communication (HC-05 Module) → Sends encrypted PINs to the FPGA and receives authentication feedback (access granted/denied).

✅ User Interface (UI) → A simple, intuitive app with options for login, new user registration, and lock status display.

---

Key Features & Enhancements

💡 Multi-User Support: Users have individual username/password/PIN combinations, all stored locally in the SQLite database.

💡 Secure Offline System: Works without an internet connection, ensuring low-latency access control and preventing cloud-based attacks.

💡 Hardware-Accelerated Security: AES decryption is done in hardware (FPGA) for enhanced security and performance.

💡 PIN Retry Limit & Lockout: Prevent brute-force attacks by blocking access after repeated failed attempts.

💡 Biometric Authentication (Optional): Use Android's fingerprint scanner for an extra layer of security before entering the PIN.