22MIC0181

ADVANCED PYTHON PROGRAMMING – CSI3007

NAME : P SURIYA KUMARI

REG NO: 22MIC0181

IOT – DEVICE APPLICATION

QUANTUM-RESILIENT SMART KEYCHAIN

IDEA

The Quantum-Resilient Smart Keychain is a next-generation IoT device designed to secure everyday interactions using *post-quantum cryptography*. It transforms a mundane daily object ,a keychain into an intelligent authentication companion that protects users even in a future where quantum computers can break today's encryption. The idea is to merge **PQC algorithms**, **low-power embedded systems**, and **short-range IoT connectivity** into a compact, portable form factor. This object enables secure unlocking, device pairing, access validation, and identity verification without exposing the user to modern or future cyber threats.

COMPONENTS

- **Microcontroller (ESP32-S3 / ARM M33)**
  Handles PQ operations, BLE communication, and sleep-wake logic.
- **Secure Element (SE / TPM-Lite)**
  Stores quantum-safe private keys and defends against tampering and physical extraction.
- **Connectivity Module**
  BLE 5.2 for low-energy communication, NFC for tap-based quick authentication.
- **Sensors**
  Touch button, motion sensor, and proximity detection to trigger secure operations only when needed.
- **Rechargeable Li-Po Battery + PMU**
  Provides stable 3.7V power, peak-current support for heavy crypto operations, and smart sleep modes.
- **Companion Mobile App**
  Used for setup, key registration, policy changes, and firmware updates.

WORKING

1. **Initialization:**
   The keychain generates a post-quantum keypair inside the secure element.
   The mobile app registers this identity and binds it to the user.
2. **Proximity Detection:**
   When the user approaches a phone, laptop, or smart lock, the keychain wakes using motion or BLE RSSI triggers.
3. **Post-Quantum Handshake:**
   The device performs a hybrid handshake using **Kyber-based key encapsulation** along with classical ECC.
   This ensures security even if quantum computers decrypt classical algorithms in the future.
4. **Session Establishment:**
   A quantum-safe symmetric key is generated and used to authenticate the user to the host device.
5. **Secure Action Execution:**
   The host device unlocks, grants access, or verifies identity.
   Logs and metadata can be synced to a cloud server for monitoring and future audits.
6. **Return to Deep Sleep:**
   After operation, the keychain minimizes its power use, extending battery life for weeks.

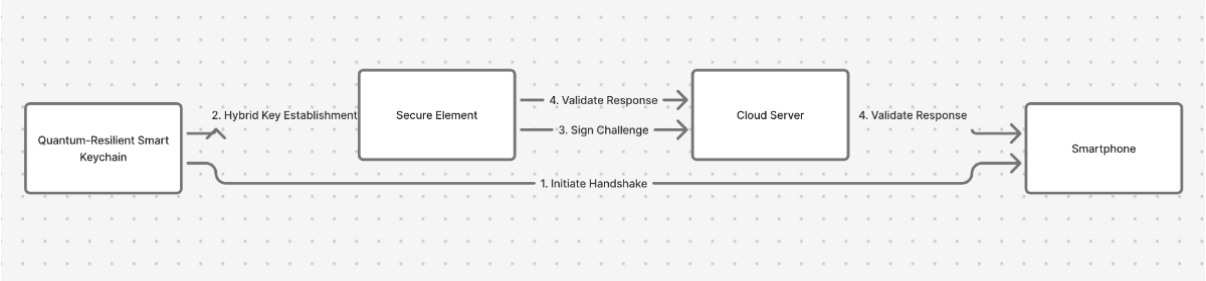

Fig.1 (Made using Figma)

CHALLENGES

- **Computational Load:**
  PQC algorithms require more memory and CPU cycles compared to classical encryption, demanding optimized firmware.
- **Power Efficiency:**
  Lattice-based operations cause temporary current spikes; managing these within a tiny Li-Po battery is complex.

- **Tamper Security:**
  Preventing physical key extraction requires secure elements, anti-probing detection, and zeroization mechanisms.
- **Interoperability:**
  Ensuring compatibility between classical systems and post-quantum systems requires hybrid crypto modes and cloud policy updates.

FRIENDLY (USE-CASE BENEFITS)

- **Everyday Carry:**
  Functions like a normal keychain but provides quantum-safe digital identity wherever the user goes.
- **Smart Lock Integration:**
  Unlock doors, vehicles, or laptops securely without passwords.
- **Future-Proof Security:**
  Protects sensitive data and access from future quantum attacks (harvest-now-decrypt-later threats).
- **Accessibility Friendly:**
  Tap-based NFC authentication supports elderly and differently-abled users with simple interaction.
- **Compact, Durable, and Wearable:**
  Waterproof, pocket-sized, and designed for daily use without requiring technical knowledge.