Full Smart Security System: AI-Driven Smartlock with Blockchain Logging

Overview

This project implements a **full-scale, AI-augmented, blockchain-backed smart security system** for access control in sensitive environments (e.g., ATS-secured rooms). It integrates **IoT, BLE communication, facial recognition**, **AI-based packet monitoring**, and **private blockchain logging** via **Chainlink + Hyperledger**, ensuring **traceability**, **security**, and **accountability**.

System Workflow

1. Smart Lock BLE Initialization

- The smart lock emits a unique `lockCID` over **Bluetooth Low Energy (BLE)**.
- The **Flutter mobile app** (used by authorized employees) scans for this BLE signal using Flutter's `flutter_blue` package.

---

2. Facial Recognition & Motion Verification

- Once the mobile app detects the BLE signal, the user is prompted for **facial verification**.
- Motion detection is used to prevent spoofing via static images.
- The face image is sent to an **AI service**, which uses **vector comparison (ML embedding matching)** to validate identity.

---

3. Access Logging on Blockchain

- Upon successful identity verification:
  - A **Redis pub-sub event** is triggered to a **Hyperledger gateway**, which logs the access event into a **Chainlink-powered private blockchain**.
  - This ensures **tamper-proof, trustless logging** without relying solely on centralized DB admins.

---

4. Door Control & Anomaly Detection

- The IoT lock opens.
- If the door **fails to close within 6 seconds**, it triggers:
  - An alert to the backend.
  - Event logging into **Supabase**.
  - Infrared sensor checks for physical obstruction.
  - Alert forwarded to the frontend interface for visibility.

Network Security: AI-Driven Packet Inspection

- IoT traffic is monitored using **packet tracing**.
- A **LangChain-powered ML model** analyzes incoming traffic:
  - Flags suspicious packets (e.g., from unusual IPs or DDOS attempts).
  - Automatically blocks malicious IPs.
  - Sends real-time alerts to the mobile app.

Mobile App Responsibilities

- **Employee-facing Flutter app**:
  - Scans for BLE signals.
  - Handles facial recognition & verification.
  - Displays login history, failed attempts, and notifications from the AI system.

Frontend Interface

- Real-time dashboard showing:
  - Smartlock status per room.
  - Logs of access attempts (synced via Supabase).
  - Alerts and suspicious activity.

- Integrated with the blockchain to **verify trust and access legitimacy**.

Why These Technologies?

Component	Purpose
Blockchain	Immutable logging of all IoT interactions; smart contract alerts.
Supabase	Cloud-native DB enabling microservice communication & real-time sync.
Microservices	Decoupled services increase modularity and scalability.
Redis	Lightweight pub-sub messaging for quick background event handling.
Flutter	Cross-platform mobile support for employee-facing access control.
LangChain + AI	Real-time anomaly detection for packet-level network security.

Links

- **Live Website**: https://envi-front.vercel.app/
- **GitHub Organization**: https://github.com/envirm