**Biometric Integration Design**

**Objective:**  
Incorporate biometric authentication and attendance mechanisms to improve security, accountability, and streamline workforce monitoring.

**Detailed Components:**

* **Supported Modalities:**
  + Fingerprint scanning (via device-native APIs like Android BiometricPrompt, Apple Touch ID/Face ID).
  + Facial recognition for newer smartphones with TrueDepth cameras or IR sensors.
* **Hardware Interfacing:**
  + Integration with external biometric scanners (USB/Bluetooth-enabled) for low-end or shared devices using vendor SDKs (e.g., ZKTeco, Suprema).
* **Enrollment Workflow:**
  + Capture, verify, and store biometric templates linked to employee ID securely.
  + Storage either in device's secure enclave or encrypted cloud repository with consent logs.
* **Authentication Use Cases:**
  + System login, attendance check-in/out, and sensitive operations (e.g., approvals, data modifications).
* **Security & Compliance:**
  + No raw image storage — only hashed/templated biometric data.
  + Full compliance with GDPR, HIPAA (if applicable), and local labor/biometric data protection laws.
* **Fallback Methods:**
  + PIN/password fallback for accessibility and edge-case scenarios.