**Offline Sync & Conflict Resolution Architecture**

The traceability platform designed for Saint Lucia acknowledges the realities of remote, bandwidth-limited environments by incorporating robust offline-first capabilities. The **Offline Sync & Conflict Resolution** architecture ensures that essential operations-such as plant registration, batch tracking, and inventory updates-can be reliably performed by field operators even in the absence of consistent internet connectivity. This is especially critical in agricultural zones or regulated facilities with limited infrastructure.

**Mobile-First Data Collection with Local Persistence**

Operators interact with the system primarily via a cross-platform **Flutter-based mobile app**, which is equipped with**SQLite** as its embedded local database. This allows for full operational capability while offline. Users can register plant batches, enter growth or lab data, update inventory, or record waste disposal events-all of which are persisted locally on-device with encryption (via flutter\_secure\_storage).

Each action taken offline is stored as a discrete delta entry in the mobile app's **Sync Queue**, tagged with a timestamp, UUID, and contextual metadata. These queued entries represent the full sequence of state-changing events initiated during offline periods.

**Custom Sync Engine and Queued Delivery**

Once network connectivity is re-established-either via cellular or Wi-Fi-the app's **custom REST-based sync engine activates**. The sync process securely authenticates with the backend (using stored OAuth2 tokens from Keycloak) and pushes the queued deltas to the appropriate domain service endpoints (e.g., Cannabis Cultivation, Inventory, Waste Management).

The sync engine is designed to:

* Transmit changes in **chronological order**
* Batch similar operations for reduced network overhead
* Retry failed entries with exponential backoff
* Perform pre-sync validation to ensure the device and app version meet minimum requirements

**Conflict Detection and Resolution**

To ensure consistency and prevent overwriting valid data, the system employs **timestamp-based conflict resolution**. Each synced delta is compared against the server's canonical dataset. If a conflict is detected (e.g., two users updated the same inventory item with different data), the following resolution flow is triggered:

1. **Version Check**: The system checks the lastModified timestamp of the existing record versus the incoming update.
2. **Operator Priority Rule**: If the change originated from the same license-holder and is newer, it is accepted.
3. **Regulator Rule**: Regulatory changes always take precedence.
4. **Manual Review Trigger**: In ambiguous cases, a conflict flag is raised for manual review through the audit dashboard.

**Audit Logging and Blockchain Anchoring**

Every synced transaction-successful or conflicted-is **logged immutably** through the platform's **ELK-based audit stack**. Additionally, each accepted delta is **hashed (SHA-256)** and **anchored into the blockchain ledger** (Amazon QLDB or Hyperledger Fabric), ensuring tamper-evidence and full traceability. The blockchain commit includes:

* Record type and ID
* Event timestamp
* Hash of the delta content
* Operator ID and sync metadata

This provides regulators and auditors with cryptographically verifiable proof that offline activities were captured accurately and have not been manipulated post-hoc.

**User Experience and Security Controls**

Operators are guided via real-time UI indicators in the mobile app, which inform them of pending syncs, completed transactions, and potential conflicts. Sensitive credentials are never exposed-authentication is securely handled via OAuth2 token refresh with encrypted local storage.

All offline-synced data transmissions are protected using **TLS 1.3**, and SQLite databases are encrypted on-device using native mobile libraries.

**Benefits to RSA and Stakeholders**

This architecture ensures that **compliance, traceability, and operational efficiency** are maintained-even under adverse connectivity conditions. For regulators, it ensures complete visibility into activities as soon as the device reconnects. For operators, it ensures that critical business activities can proceed uninterrupted without fear of data loss.

Combined with automated conflict management, full auditability, and tamper-proof verification, the Offline Sync & Conflict Resolution mechanism stands as a core pillar of resilience and trust in the platform's architecture.