Threat Model – Slaughterhouse System

1. Scope and Assets

- Animal & product registration data
- Recall functionality
- Operations of each station (must continue even if the network is down)

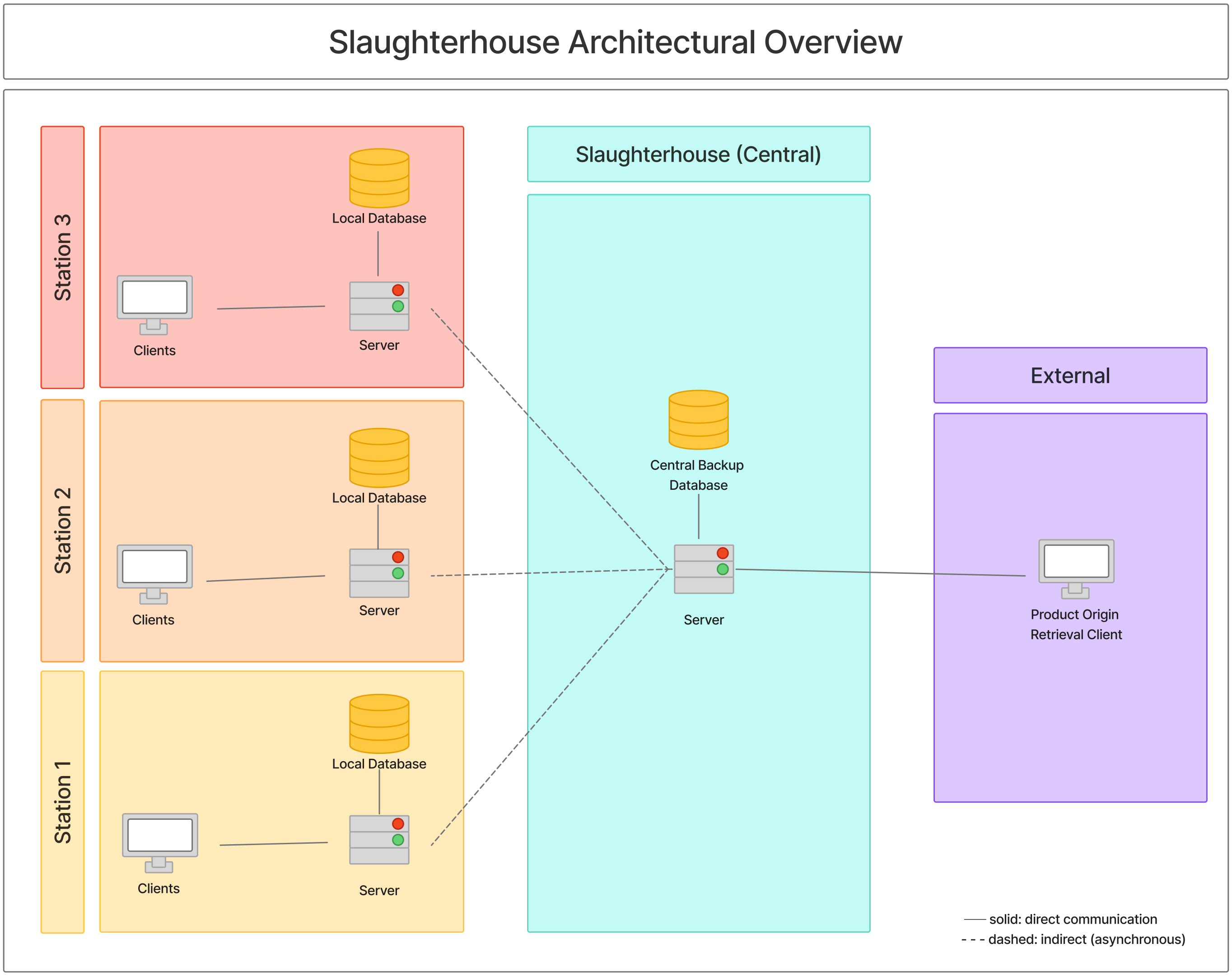
2. Actors

- Station Operators (Clients at Station 1-3)
- External Recall Client (Supermarket or Authority)
- Maintenance Staff
- Malicious Outsiders

3. Trust Boundaries

- Internal network boundary – encloses Station 1–3, internal services and database.
- External boundary – separates external recall client from the internal network.

4. Architecture & Data Flows



At each station, the staff operating the client machines of the system will be able to upload animal and product registration data to the local server.

The local server will store the data in the local database and try to synchronize the data with the central database.

The external recall client will be able to send recall requests to the recall service, which will then propagate the recall request to all stations through the internal message bus. In case the network is down, the central server will be able to use the central backup.

In case a station needs to operate with data of another station, and that other station is not reachable, the local server will be able to use the central database backup (as long as it has any access to the central server).

5. STRIDE-Based Threat Analysis

Component/Flow	Category	Threat Example	Mitigation
External recall API	Spoofing	Fake recall request by unauthorized party	Authentication and authorization to access the system
Synchronization process / Recall	Tampering	Alter recall instructions in transit	Encryption
External recall API	Denial of Service	Flooding recall endpoint	Rate limiting and monitoring
Database	Tampering	Unauthorized changes to product/animal records	Role-based access control, audit logging, backups
Database	Repudiation	Operator denies having changed a record	Signed audit trails
Staff	Information Disclosure	Leakage of sensitive product trace data	Encrypt data at rest, least-privilege access
Inter-station communication	Denial of Service	Network outage halts workflow	Local buffering, asynchronous queues
Inter-station communication	Elevation of Privilege	Compromise of admin credentials	Multi-factor authentication, strong password policies

6. Mitigation Summary

- Use authentication and authorization to access the system.
- Encrypt data in transit and at rest.
- Implement rate limiting and monitoring to prevent DoS attacks.
- Use role-based access control, audit logging, and backups to protect data integrity.
- Implement signed audit trails to prevent repudiation.
- Use local buffering and asynchronous queues to ensure operational continuity.