System Design - End Term - Yerlan Dias

Github repo link

TASK 6

Functional requirements:

1. Register recipients using biometric data
2. Record each aid distribution event with:
    - Recipient ID
    - Timestamp
    - Volunteer ID
    - Aid type
    - Geolocation
3. Offline functionality: queue and store unsynced transactions locally until reconnected.
4. Data sync: synchronize data with nearby devices or local nodes via peer-to-peer
5. Digital wallet for recipient
6. Generate anonymized audit reports showing distribution patterns, fairness metrics, and discrepancies
7. Role management: volunteers, managers, auditors, recipients

Non-functional requirements:

1. Aid claim and eligibility verification must complete in < 200 ms on field devices
2. Registration operations (biometric scan, DID issuance, data write) may take up to 500 ms
3. UI response times (tap to feedback) must remain < 150 ms on supported hardware
4. Aid claim and registration transactions must be atomic
5. System must ensure eventual consistency across nodes after offline operation

6. Each node must support ≥ 250 GB HDD, replicated on at least 3 nodes for resilience

7. Minimum 16 GB RAM required for regional/local edge servers or sync hubs
8. Mobile field devices must operate with ≤ 2 GB RAM, optimizing memory footprint
9. Personal data encryption at rest and in transit
10. System should handle up to 2,000 concurrent connections per regional server (volunteers + NGO staff)
11. Each server must support minimum 8 vCPUs to manage concurrent sync, signing, and verification tasks

Trusting the Source: Digital Signatures are Like Personal Seals

Imagine every volunteer has a unique, unforgeable digital "seal" or signature tied only to them and secured on their device.

When a volunteer registers someone or hands out aid, the app automatically puts their unique digital seal on that record right there on the spot.

Why this builds trust: You know exactly which volunteer recorded that specific action, and you know the record hasn't been messed with since they sealed it. It’s like a signed delivery confirmation – you trust who signed it and that the details are what they wrote down at that moment. There's accountability right from the start.

Trusting the Information: Verifiable Credentials are like Official Digital Badges

Instead of just putting info into a big database, we create specific digital "badges" or credentials for recipients (like "Registered by Red Cross," "Received Food Pack - Oct 10th"). These badges are also digitally signed, usually by the volunteer/NGO making the claim.

Why this builds trust: Recipients can hold onto these badges (digitally). When they need aid from another program, they can show just the relevant badge. The other NGO can instantly verify the badge is real and issued by a trusted partner without needing to call back to some central office or access a giant, shared file on everyone. It compartmentalizes information and makes it verifiably true on its own.

Trusting the History: The Shared, Tamper-Proof Notebook

This is the big one – replacing the single central database. Imagine a special kind of shared digital notebook (this is the "Distributed Reconciliation Layer"). Crucially, this notebook isn't owned or controlled by just one NGO. Instead, several participating NGOs and UN agencies each hold a copy and work together to maintain it using agreed-upon rules.

When a volunteer's signed records eventually sync up, they're proposed to be added to this shared notebook. The participating organizations' systems automatically check the digital seals (signatures) and follow the rules they all agreed on (like "don't let the same person be registered twice," or "don't give out two food packs the same day to the same person").

Only when a consensus is reached among these organizations does the record get permanently added to all copies of the notebook.

Why this builds trust:

No Single Boss: No one organization can secretly change the records or control the history. Cheating the system would require multiple independent organizations to collude.