Role-Based Access Control (RBAC) in a Distributed Web System

Project developed by:

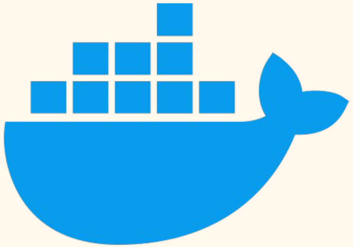
- Francisco Cardoso (up202108793)
- Ruben Esteves (up202006479)
- Artur Oliveira (up202108663)

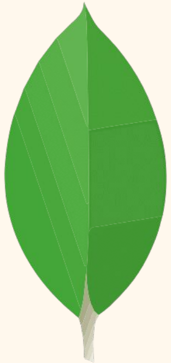
Project Presentation

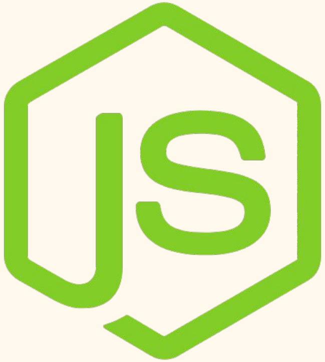
Overview

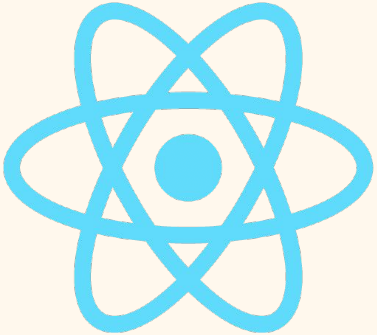
Design and implement a secure distributed system where users authenticate through a central authorization server. The system enforces **Role-Based Access Control (RBAC)** to restrict access to service operations, using **JWT tokens** for authorization and **TLS certificates** for secure communication between services.

Tech Stack







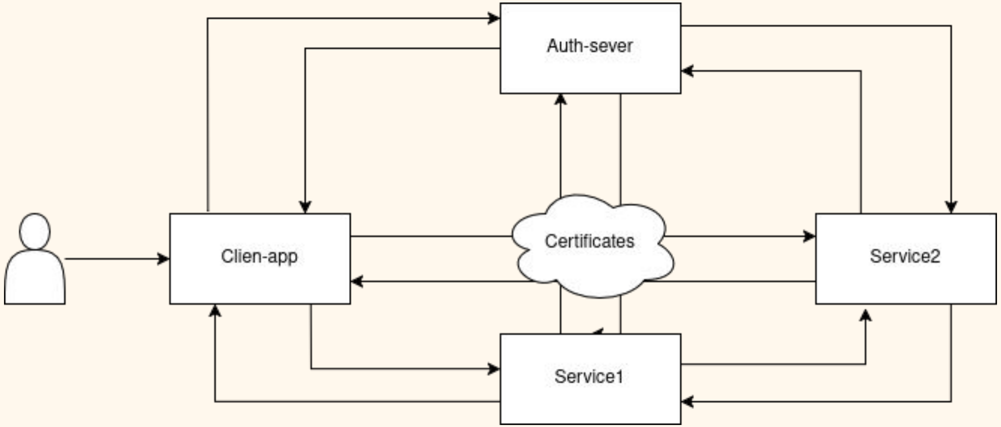


System Architecture

Diagram of the system:

- Client App (React)
- Auth Server (Node.js)
- Service 1 (Node.js REST API)
- Service 2 (Node.js REST API)

All communication over HTTPS/TLS



Roles and Users

Admin

All Operations From both Servers

Manager

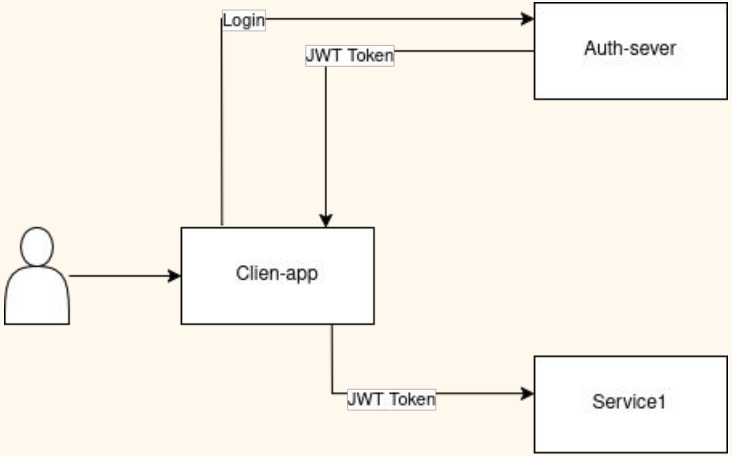
All Operations From Server 1

User

Some Operations from Server 1

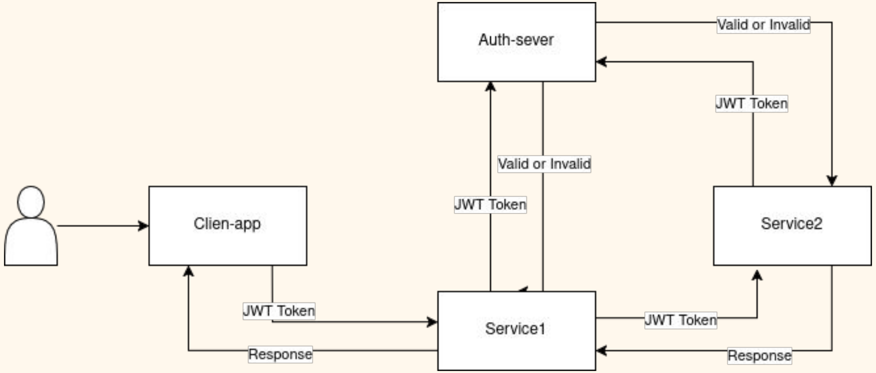
Authentication & Token Flow

1. User logs in via client app
2. Auth server verifies credentials
3. Auth server generates:
    - ○ JWT Token (signed with private key)
    - ○ Public key (sent to services)
4. Client stores token, sends it with requests



Authorization Enforcement

1. Role and permissions checked on each service request
2. Nested calls (e.g., service1 → service2) only succeed if user is allowed
3. Unauthorized access → 403 error



Certificates & Root CA in the System

1 - 🏛️ Root Certificate Authority (CA)

- A custom Root CA is created to act as a trusted authority.
- It is used to sign all service certificates.
- Ensures trust and authenticity between services.

2- 📄 Certificates for Each Service:

- Each service (auth-server, service1, service2, client-app) has:
  - A private key
  - A certificate signed by the Root CA

3- 🔄 Trust Chain

- Services trust each other because:
- All certificates are signed by the same Root CA
- Each service has access to ca.pem to validate peers and know to trust the authority of certificates that are signed with it

Demo