Secure Authentication & Threat Detection System

Aaron Tsang

December 2025

Contents

Document generated by ChatGPT

1 Overview

This document provides a complete system design for a Secure Authentication & Threat Detection Service. This backend web service manages user authentication, logs all authentication events, and performs rule-based analysis to identify suspicious activity such as brute-force attempts, unusual login locations, or impossible-travel logins. The system includes admin endpoints to retrieve logs and alerts and can optionally include a frontend dashboard.

2 System Architecture

The system architecture consists of the following components:

- Frontend
- Backend API
- PostgreSQL database
- Redis cache for rate limiting and ephemeral data
- Threat detection engine

3 Core Features

- Secure user signup and login
- Password hashing (bcrypt/argon2)
- JWT-based access and refresh tokens
- Role-based authorization
- Logging of authentication attempts
- IP and device tracking
- Redis-based rate limiting
- Rule-based threat detection
- Admin endpoints for logs and alerts

4 API Endpoints

Endpoint	Method	Description
/auth/signup	POST	Create a new user account
/auth/login	POST	Authenticate user and issue tokens
/auth/refresh	POST	Refresh access token
/auth/me	GET	Retrieve authenticated user profile
/admin/logs	GET	Retrieve login attempts
/admin/alerts	GET	Retrieve suspicious activity alerts

5 Database Schema

5.1 users Table

- id (PK)
- email
- password_hash
- role
- created_at
- updated_at

5.2 login_attempts Table

- id (PK)
- user_id (nullable)
- email_entered
- ip_address
- user_agent
- success (boolean)
- timestamp

5.3 alerts Table

- id (PK)
- type
- description
- user_id (nullable)
- ip_address
- created_at
- resolved (boolean)

6 Threat Detection Logic

Threat detection is performed using rule-based evaluation.

- 3+ failed attempts from the same IP address
- Logging in from an new location
- Successive logins from differing locations
- Multiple account access from tthe same IP

7 Project Structure

```
secure-auth-threat-detection/
    backend/
        src/
            controllers/
            middleware/
            services/
            models/
            routes/
        tests/
        Dockerfile
        docker-compose.yml
    frontend/
        src/
            users/
            admin/
```

8 Deployment

- Local Docker-based development
- Cloud hosting on Render
- GitHub Pages for documentation and frontend only