**1. Projektbeschreibung**

Das Ziel des Projekts ist die Entwicklung eines sicheren, skalierbaren und MQTT-kompatiblen Backend-Servers zur Steuerung und Überwachung eines Raumüberwachungssystems. Das System sammelt Sensordaten (z. B. Temperatur, Luftfeuchtigkeit), verarbeitet Vorfälle (Incidents) und bietet eine WebSocket-Schnittstelle für Echtzeitkommunikation.

**2. Technologischer Stack**

| **Komponente** | **Technologie / Paket** |
| --- | --- |
| Programmiersprache | Python 3.x |
| Web-Framework | Flask |
| Authentifizierung | JWT (JSON Web Tokens) |
| WebSocket | Flask-Sock |
| Datenbank | SQLite |
| Messaging | MQTT mit paho-mqtt |
| Rate-Limiting | Flask-Limiter |
| Sicherheit | Passwort-Hashing mit Werkzeug |
| CORS-Unterstützung | Flask-CORS |
| Datenformatierung | JSON |
| .env-Verwaltung | Python-dotenv |

**3. Hauptfunktionen des Backends**

**3.1 Authentifizierung und Sicherheit**

* JWT-basierte Authentifizierung (/login, @jwt\_required)
* Passwort-Hash-Prüfung (check\_password\_hash)
* IP-basiertes Rate-Limiting mit Sperrfunktion bei zu vielen Fehlversuchen

**3.2 WebSocket-Unterstützung**

* WebSocket-Route (/ws) zur bidirektionalen Kommunikation
* Unterstützung für Live-Datenübertragung über MQTT an Frontend-Clients

**3.3 MQTT-Anbindung**

* Subscribed Topics:
  + RZ/data: Sensordaten (JSON)
  + RZ/config: Konfigurationen
  + RZ/incidents: Vorfälle/Alarme
* Dynamische Nachrichtenübertragung mit zufälligen msgIDs
* Verarbeitung von:
  + Echtzeitdaten (z. B. Temperatur, Türstatus)
  + Konfigurationsbefehlen (setConfig, getConfig)
  + Incidents (Alarme)

**3.4 REST API-Endpunkte (Auswahl)**

| **Route** | **Methode** | **Auth** | **Beschreibung** |
| --- | --- | --- | --- |
| /login | POST | ❌ | Benutzeranmeldung |
| /getConfig | GET | ✅ | Abrufen der Gerätekonfiguration |
| /setConfig | POST | ✅ | Setzen neuer Konfigurationen |
| /addAccessID | POST | ✅ | Generiert eine neue Zugangskarte |
| /data | GET | ✅ | Abruf von Sensorwerten |
| /incidents | GET | ✅ | Abruf von Vorfällen (Alarme etc.) |
| /user/profile | GET | ✅ | Aktuelles Benutzerprofil |
| /health | GET | ❌ | System-Gesundheitsstatus (MQTT Ping) |

**4. Datenbankstruktur (SQLite)**

**users**

| **Spalte** | **Typ** |
| --- | --- |
| id | INTEGER |
| username | TEXT |
| password | TEXT |

**dashboard\_data**

| **Spalte** | **Typ** |
| --- | --- |
| timestamp | TEXT |
| value | TEXT (JSON) |

**incidents**

| **Spalte** | **Typ** |
| --- | --- |
| id | INTEGER |
| timestamp | TEXT |
| type | TEXT |
| value | TEXT (JSON) |

**5. Sicherheitskonzepte**

* **Tokenbasierte Authentifizierung:** JWT mit Ablaufzeit.
* **Rate-Limiting:** Pro IP-Adresse max. 10 Fehlversuche → Sperre für 5 Minuten.
* **Passwortsicherheit:** Speicherung gehashter Passwörter mit werkzeug.security.
* **Passwortgesicherter MQTT Broker**

**6. Visualisierung Backend**