Hospital Management System

Design and implement a secure authentication and authorization system for a Hospital Management System (HMS) using **JWT (JSON Web Token)**. The system should support three distinct user roles: **ADMIN**, **DOCTOR**, and **PATIENT**, each with specific access rights and functionalities.

1. **Authentication**:
   - Users must be able to register and log in.
   - On successful login, a JWT should be issued to the user.
   - The JWT should be required for accessing all protected endpoints.
2. **Role-Based Authorization**:
   - **ADMIN**:
     - Can manage (add/update/delete/view) doctors and patients.
   - **DOCTOR**:
     - Can view only their assigned patients and appointments.
   - **PATIENT**:
     - Can book new appointments and view their existing ones.
3. **Security**:
   - Protect endpoints based on user roles using Spring Security.
   - Ensure stateless session management using JWT.
   - JWT tokens must be verified on each request to access protected resources.
   - Token expiration and renewal strategy must be implemented.
4. **Endpoint Access Control (Sample)**:
   - /admin/** → Accessible by ADMIN only
   - /doctor/** → Accessible by DOCTOR only
   - /patient/** → Accessible by PATIENT only
   - /auth/** → Public (for login and registration)

🔐 **Objective:**

To ensure a secure and scalable architecture where access to system features is strictly controlled by JWT-based role validation, maintaining the confidentiality and integrity of patient and doctor data.