Health Record Management using Blockchain-Integrated Database

Objective

Develop a secure and tamper-resistant system to manage patient medical records using a hybrid architecture combining a relational database for data storage and a blockchain network for integrity verification through cryptographic hashes.

Tech Stack

Backend:

- Flask or Node.js

Database:

- PostgreSQL or MongoDB

Blockchain:

- Ethereum (using Ganache for local blockchain and Web3.js or Solidity for smart contract implementation)

Development Phases

1. System Design

- Design database schema with key entities:
    - Patients (basic details)
    - Visits (date, diagnosis, symptoms)
    - Medications (prescriptions)

    - Doctors (assigned professionals)

- Only SHA256 hashes of sensitive records are stored on blockchain to ensure privacy and immutability

2. Smart Contract Development

- Develop Solidity smart contract to:
    - Store SHA256 hashes of medical records
    - Allow verification of hash during record retrieval

3. Backend Integration

- Functions to:
    - Generate SHA256 hash for every patient record upon upload
    - Store the original data in the database and the hash on blockchain
    - On record retrieval, recalculate hash and verify against blockchain

4. UI Interface

- Build frontend to:
    - Upload and view patient records
    - Show real-time verification of record authenticity
    - Display verification results (valid/invalid tampering)

5. Security Measures

- Use JWT-based authentication for all users (doctors, patients, admins)
- Encrypt sensitive medical data at rest within the database

Expected Outcomes

- A trustworthy and secure medical record system
- Tamper-proof record verification through blockchain hash matching
- Enhanced patient data confidentiality and integrity without exposing raw data on blockchain