**Final Year Project Proposal Performa**

**Department of Computer Engineering**

Entry: 22-Computer

Date: \_\_\_/\_\_\_\_/\_\_\_\_\_

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Project Title:** | **Patient-Controlled Decentralized Electronic Health Record (EHR) System** | | | | | | | | | |
| **Intended number of students** | 4 | | | | | | | | | |
| **Industry Advisor Name (if any)** |  | | | | | | | | | |
| **Company Address (if any)** |  | | | | | | | | | |
| **DESIGN PROBLEM FORMULATION** | | | | | | | | | | |
| **Problem Statement:** | | Current EHR systems often suffer from centralized control, privacy breaches, and lack of patient consent management. This project addresses these challenges by enabling patients to control who can access their health records on a transparent, tamper-proof blockchain. | | | | | | | | |
| **Project Summary:** | | This project aims to develop a secure and decentralized Electronic Health Record (EHR) system that empowers patients with full ownership and control over their medical data. Unlike traditional centralized EHR systems—which are vulnerable to data breaches, unauthorized access, and lack transparency—this system leverages blockchain technology combined with decentralized storage solutions like IPFS. This ensures that patient records are securely stored in a tamper-proof manner and accessible only to authorized parties. Smart contracts are used to enforce strict access control, enabling patients to grant or revoke permissions to healthcare providers, insurers, or researchers with full transparency and an immutable audit trail recorded on the blockchain.  Cryptographic techniques safeguard patient privacy while enabling seamless and secure data sharing, improving healthcare outcomes through timely and accurate information exchange. By giving patients autonomy over their health data, this solution reduces the risk of misuse, supports compliance with data protection regulations like HIPAA and GDPR, and fosters patient-centric care. | | | | | | | | |
| **Aims & Objectives:** | | 1. To decentralize EHR data ownership using blockchain and smart contracts 2. To implement patient-managed access control over medical data 3. To securely store encrypted health data using decentralized storage (IPFS) 4. To log all access and modification events immutably 5. To enable healthcare interoperability between hospitals, labs, and doctors | | | | | | | | |
| **Tools:** | | **Blockchain**: Ethereum / Polygon (for smart contracts)  **Smart Contract Language**: Solidity  **Decentralized Storage**: IPFS or Filecoin  **Encryption**: RSA/AES for data encryption  **Identity**: Ethereum Wallet / Decentralized Identity (DID)  **Frontend**: React.js with Ethers.js or Web3.js  **Backend** : Node.js for IPFS and encryption helpers  **Wallet Integration**: MetaMask or WalletConnect | | | | | | | | |
| **Complexity Level**  **(description of WPs is given on next page)** | | WP1 | WP2 | WP3 | WP4 | WP5 | WP6 | WP7 | WP8 | WP9 |
| √ | √ | √ | √ | √ |  |  |  |  |

