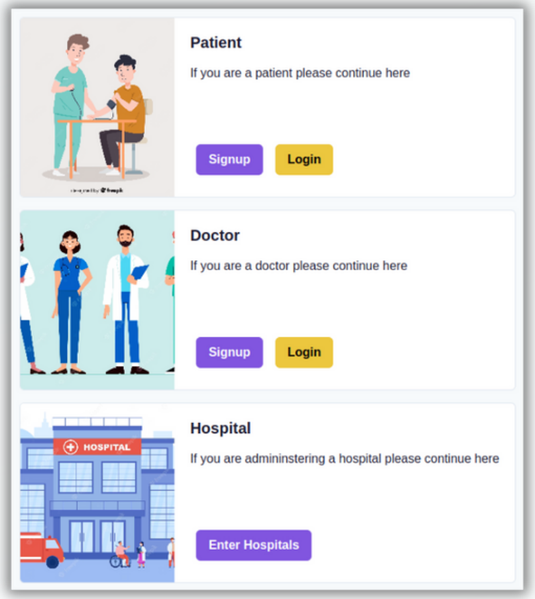

HEALTH RECORD MANAGEMENT(HRM) TEZOS

DIZZYN

Pranay Pandey

PROBLEM TO SOLVE:

Limitations of the current Electronic Health record system:

Data Interoperability: Current EHR systems struggle to communicate due to differing data formats, hindering effective data sharing.

Fragmented Patient Information: Patient data is scattered across systems, leading to incomplete medical profiles and compromised care.

Inconsistent Data Formats: Lack of standardization makes data exchange complex and requires manual integration efforts.

Security and Privacy: EHRs face challenges in maintaining data security and patient privacy, raising concerns about unauthorized access and breaches.

PROPOSED SOLUTION

Objective n° 1

Use Tezos blockchain to store the information for patients and doctors and hospital.

Objective n° 2

The information on blockchain will be publicly visible so we will incorporate encryption for security.

Objective n° 3

Each information (Patient info, patient aadhar, patient Diagnosis) will be encrypted by AES algorithm.

Objective n° 4

Each patient and doctor will also have a unique public/private key which will be used for communicating this AES key with each other through RSA algorithm.

Objective n° 5

All info of one patient is encrypted using a single AES key and this key is passed (in encrypted manner) only to those whom we want to share our information.

Objective n° 6

IPFS is utilized to store the diagnosis documents and its hash is also encrypted in the diagnosis information.

Objective n° 7

Use our back-end for identity management to authenticate the user and also to encrypt and decrypt information.

EMPOWERING HEALTHCARE

Privacy

Utilizing robust encryption methods, patient diagnosis data is safeguarded against unauthorized access. AES encryption ensures confidentiality, while RSA encryption facilitates controlled sharing of AES keys with authorized doctors. IPFS storage and encrypted hashes enhance patient data privacy.

Leveraging Tezos blockchain, the platform offers standardized storage for medical records, fostering data interoperability. Encryption ensures security and seamless sharing among medical entities. IPFS streamlines document access, promoting efficient information exchange and collaboration.

Interoperability

WORKFLOW

Since there is storage on the blockchain, we are encrypting the information from the frontend and then uploading the information

Registration

The patient registers entering his details like aadhar, age, sex etc.

FRONTEND

A unique AES encryption is generated for this patient. A public/private RSA pair is also generated and the information is encrypted

BACKEND

The encrypted information is uploaded on the smart contract

CONTRACT

Diagnosis

The patient enters the diagnosis/appointment details

FRONTEND

The encrypted AES key is fetched from contract storage, is decrypted and the information is sent to entry point after encrypting with the AES key

BACKEND

Info Viewing

The doctor gets the encrypted AES passed as message from patient

The doctor decrypts the encryption key and uses it to read the diagnosis, similar to how the user reads the encrypted information

Doctor may enter diagnosis details for the patient after encypting

FUNCTIONALITIES

The robust system assigns a unique public-private key pair to each user, ensuring a secure and distinct digital identity.

USER AUTHENTICATION AND ENCRYPTION

Empowering users, the platform facilitates the secure upload of encrypted medical diagnoses onto the blockchain, ensuring data integrity.

DIAGNOSIS UPLOADS

Users exercise precise control over their data by selecting the specific recipients with whom they wish to share their information

CONTROLLED DATA SHARING

For heightened privacy, the platform encrypts the AES encryption key, strengthening the layers of security for sensitive information

ENHANCED PRIVACY THROUGH KEY EXCHANGE

FUNCTIONALITIES

Recipient doctors are granted access to shared data by securely decrypting the encrypted AES key, enabling effective collaboration

RECIPIENT DATA ACCESS

Furthermore, recipient doctors can contribute seamlessly by sharing encrypted URLs of documents, fostering a secure information exchange.

ENCRYPTED DOCUMENT LINKS

A user-centric approach empowers individuals with complete autonomy to retract shared information, thereby ensuring data sovereignty and control

DATA MANAGEMENT AND DELETION

THANK'S FOR WATCHING

You can interact with the application from the following link - https://hrm-chi.vercel.app/