NATIONAL INSTITUTE OF TECHNOLOGY
PATNA, INDIA, 800005

# Blockchain-Based Smart Healthcare System

Submitted By:
Bharath Veera 2106187
Manoj Kumar 2106111
Ganipudi Yugesh 2106140

Under the supervision of:
Dr. Piyush Kumar (project supervisor)
Assistant professor, Department of CSE

# Outline:

- Introduction
- Motivation
- Literature Survey
- Problem Statement
- Methodology
- Work done so far
- Evaluation
- Conclusion

# Introduction:

- The introduction of Electronic Medical Records (EMRs) revolutionized healthcare data management, enabling efficient storage and retrieval of patient information
- However, traditional EMR systems are not immune to security vulnerabilities such as data breaches and unauthorized access
- EMRs are widely used and exhibit significant benefits in reducing healthcare cost, improving quality of clinic, and reinforcing disease surveillance
- At present, EMRs are core elements of a smart healthcare system, since they are convenient for transmission, sharing, and exchanging between doctors and cross-hospital healthcare and diagnosis in an open network

# Introduction(cont.):

- Therefore, it is important to build a secure and reliable transaction frame- work with attribute based privacy-preserved mechanism.
- Because it need to meet the requirements of a smart healthcare system for individual-centric EMR collection, sharing, and exchanging in an open network.

# Motivation:

**Decentralized data storage:**

- Blockchain decentralizes data storage by distributing copies of the EMR database across a network of nodes.
- Each node maintains a complete copy of the blockchain ledger, ensuring redundancy and resilience against single points of failure.
- By eliminating the need for a central authority to control the data, blockchain enhances the security and availability of EMR systems.

# Motivation(cont.):

**Access Control in EMRs:**

- Blockchain enables fine-grained access control through the use of cryptographic techniques and smart contracts.
- Smart contracts can define access rules and permissions for different users or entities based on predefined criteria.
- For example, a patient may grant access to specific healthcare providers or researchers for a limited time or purpose, and this permission is recorded on the blockchain.
- Access to patient records is granted only to authorized parties with the corresponding cryptographic keys or permissions, ensuring data privacy and security.

# Literature Survey:

| TITLE | AUTHOR: | YEAR: | EXPLANATION: |
|---|---|---|---|
| Electronic health record system using Blockchain | B. Harshini | 2020 | The data is encrypted by the algorithm known. as SHA-256 which is used to encrypt all the data of the patients into a single line 256 bit encrypted text .<br>Cons : Less secure due to its 256 standards. |
| Electronic health record using Blockchain Technology | Arlindo F.da | 2019 | propose the implementation of a large-scale information architecture to access Electronic Health Records (EHRS) based on Smart Contracts as information mediators .<br>Cons : Health Record validation delay and false sense of security. |
| Analysis of Blockchain in the Healthcare sector:Application | Dsv madala | 2022 | Investigate how blockchain technology can be applied to improve the overall performance of the healthcare sector.<br>Cons : low scalability and less transaction. |

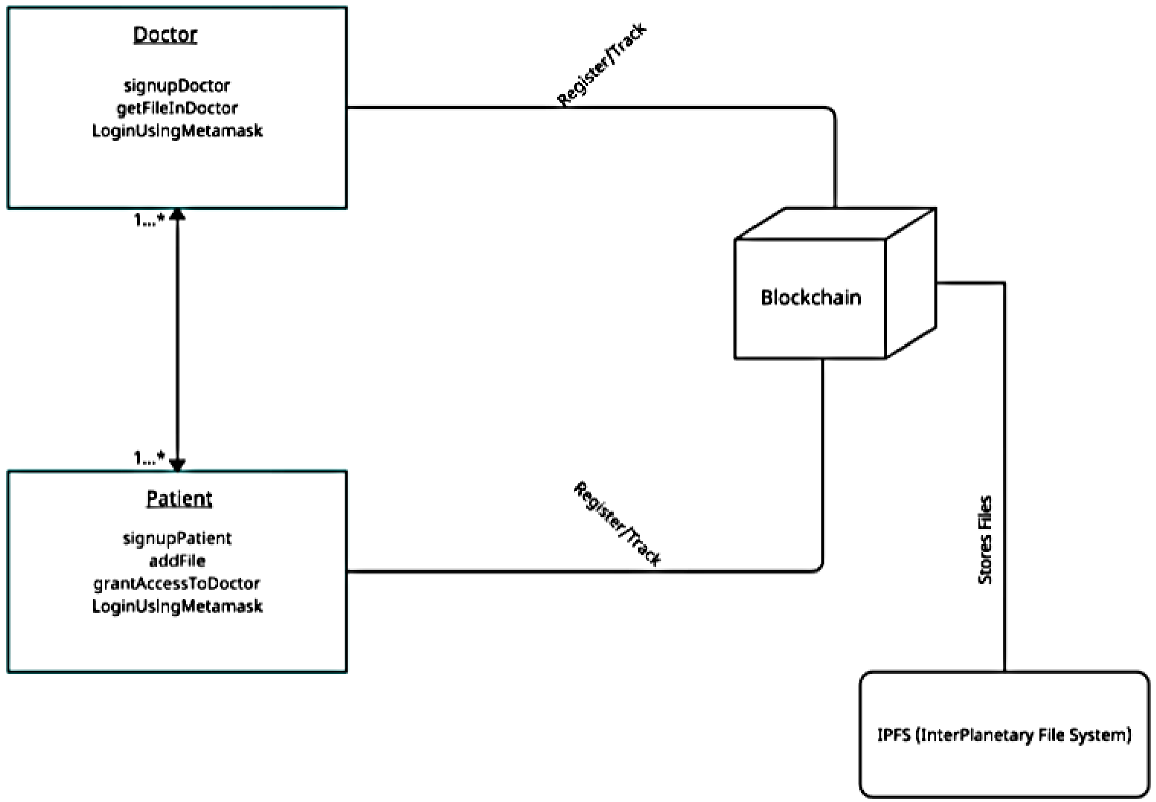
# Literature Survey(cont.):

| TITLE: | AUTHOR: | YEAR: | EXPLANATION: |
|---|---|---|---|
| Electronic health records and blockchain requirements : a scoping review | Suzanna Schmeelk | 2022 | We conducted a literature search in the OVID databases (Medline and Embase) on terms blockchain, implementation, interoperability, EHRs, security, and standards .<br>Cons: False sense of security due to frequent |
| Blockchain-based Electronic Health Records Management A comprehensive Review and Future research | Mamun, Abdullah Al | 2022 | The study examined 99 papers that were collected from various publication categories. The deep technical analysis focused on evaluating articles based on privacy, security, scalability, accessibility, cost, consensus algorithms .<br>Cons: No Specific solution proposed to overcome the issues. |

# Problem Statement:

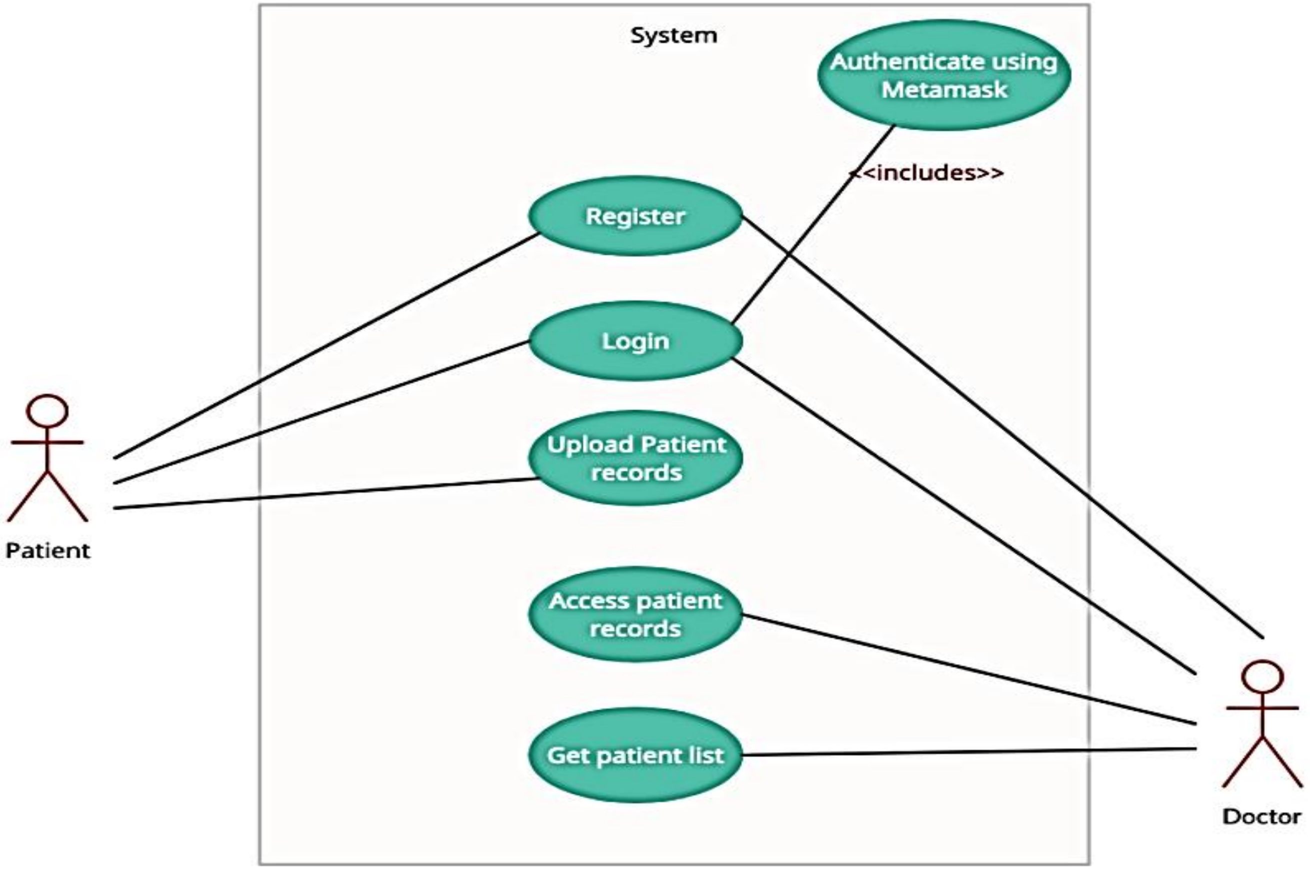
- Controlling access to sensitive patient information is crucial to safeguarding privacy and preventing unauthorized disclosure or misuse of data. Traditional access control mechanisms in EMR systems may be vulnerable to insider threats or external attacks.
- SOLUTION: Blockchain can control the access of attributes by dividing attributes into three categories.
- EMRs are centralized database. This centralized model poses several problems, including a single point of failure, susceptibility to cyberattacks and lack of transparency.
- SOLUTION: Blockchain has decentralized database structure.

# Methodology:



**BLOCK DIAGRAM**

# Methodology (cont.):



**USE-CASE DIAGRAM**

# Work done so far:

## LAUNCHING THE PROJECT

### Ganache

- Open Ganache and click on settings in the top right corner.
- Under **Server** tab:
  - Set Hostname to127.0.0.1 –lo
  - Set Port Number to 8545
  - Enable Automine
- Under **Accounts & Keys** tab
  - Enable Autogenerate HD Mnemonic

### Metamask

- After installing Metamask, click on the metamask icon on your browser.
- Click on **TRY IT NOW**, if there is an announcement saying a new version of Metamask is available.
- Click on continue and accept all the terms and conditions after reading them.
- Stop when Metamask asks you to create a new password. We will come back to this after deploying the contract in the next section.

# Work done so far (cont.):

## Smart Contract

Compile Contracts using truffle compile

## Starting your local development blockchain

- Open the new terminal and deploy contracts using truffle migrate
- Copy deployed contract address to src/app.js
- If you change the contents of any contract, replace existing deployment using truffle migrate –reset.

## Running dApp

### Connecting Metamask to our local blockchain

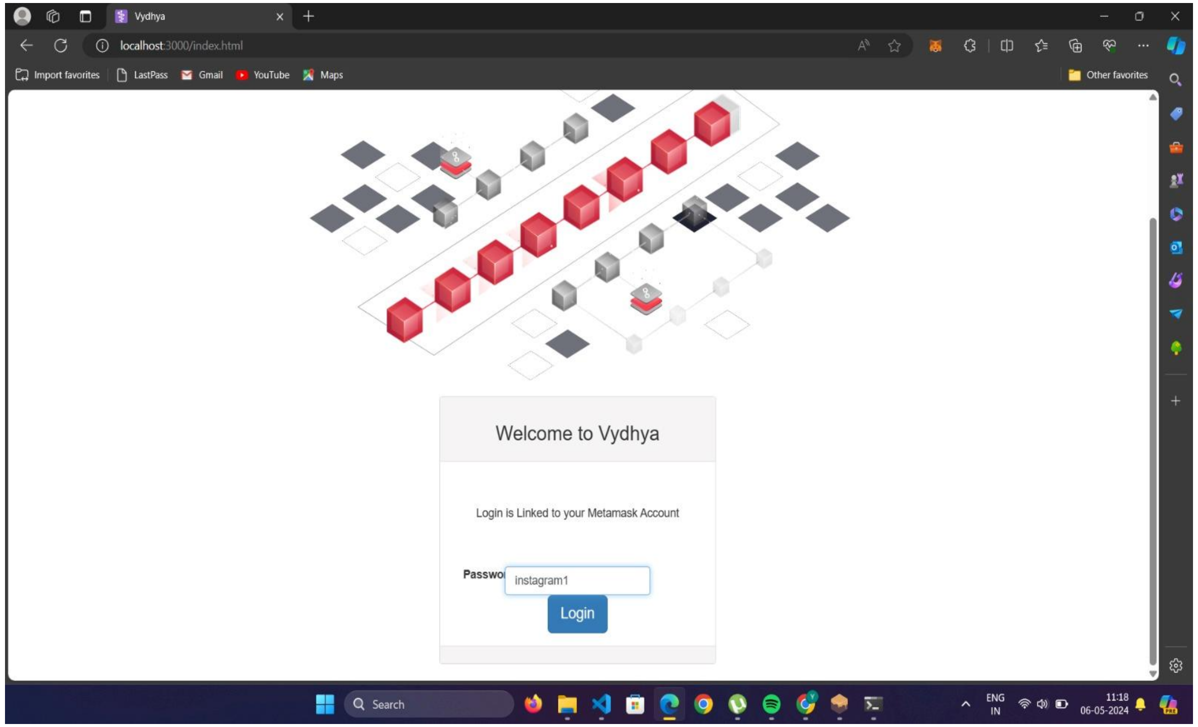
- Connect metamask to localhost:8485
- Select any account from ganache and copy the private key to import account into metaMask

## Start a local server

- Open a new terminal window and navigate to /YOUR_PROJECT_DIRECTORY/app/.
- Run npm start.
- Open localhost:3000 on your browser.

# Work done so far (cont.):

## IMPLEMENTING PROJECT



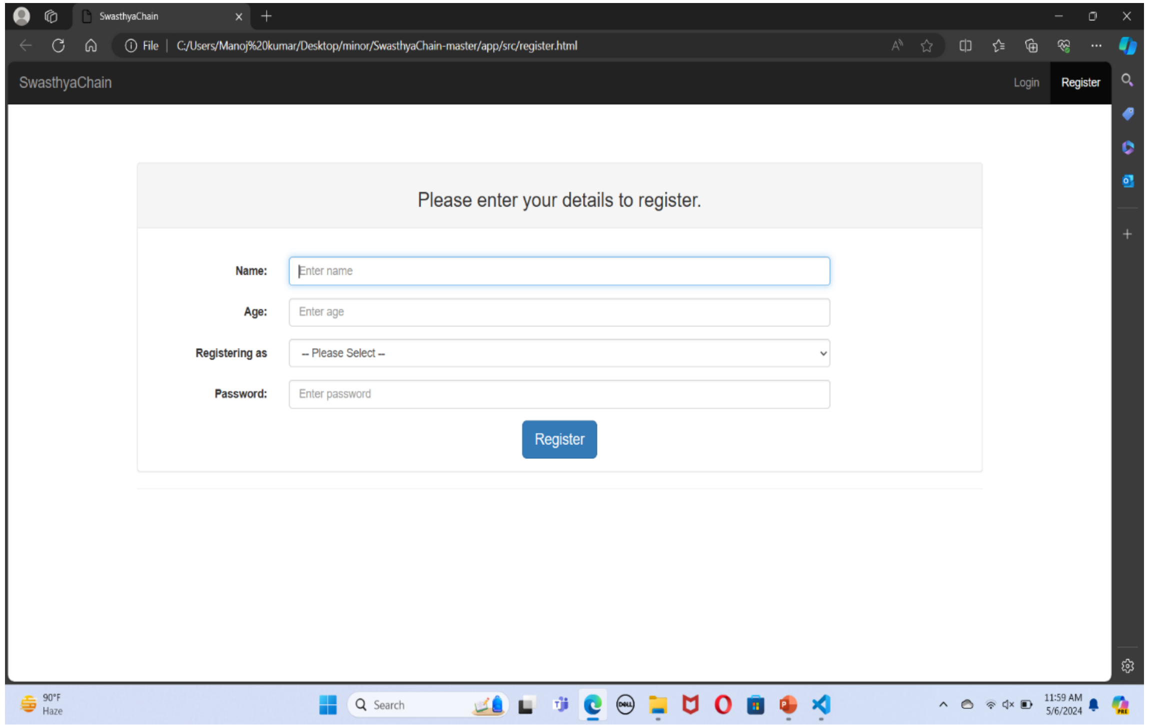
Welcome to Vydhya

Login is Linked to your Metamask Account

Passwo: instagram1

Login

LOGIN PAGE


SwasthyaChain
File | C:/Users/Manoj%20kumar/Desktop/minor/SwasthyaChain-master/app/src/register.html
SwasthyaChain
Login
Register
90°F
Haze
Search
11:59 AM
5/6/2024

Please enter your details to register.

Name: Enter name

Age: Enter age

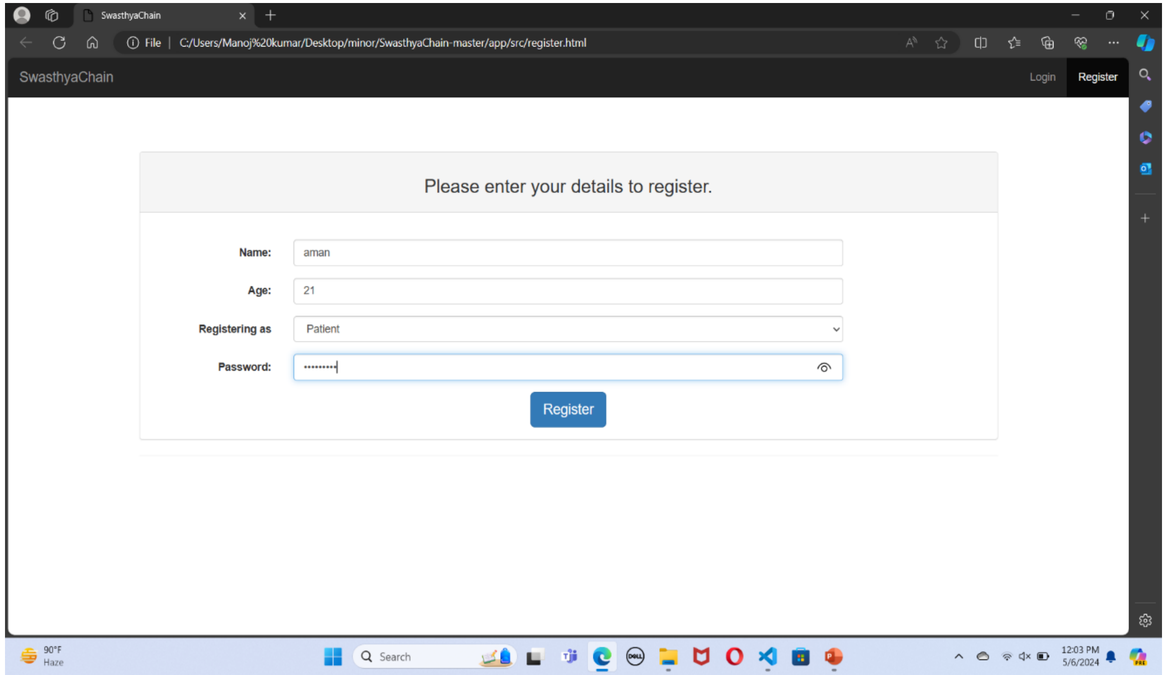
Registering as: -- Please Select --

Password: Enter password

Register

REGISTER PAGE

# Work done so far (cont.):


SwasthyaChain
File | C:/Users/Manoj%20kumar/Desktop/minor/SwasthyaChain-master/app/src/register.html
SwasthyaChain
Login
Register
90°F
Haze
Search
12:03 PM
5/6/2024

Please enter your details to register.

Name: aman

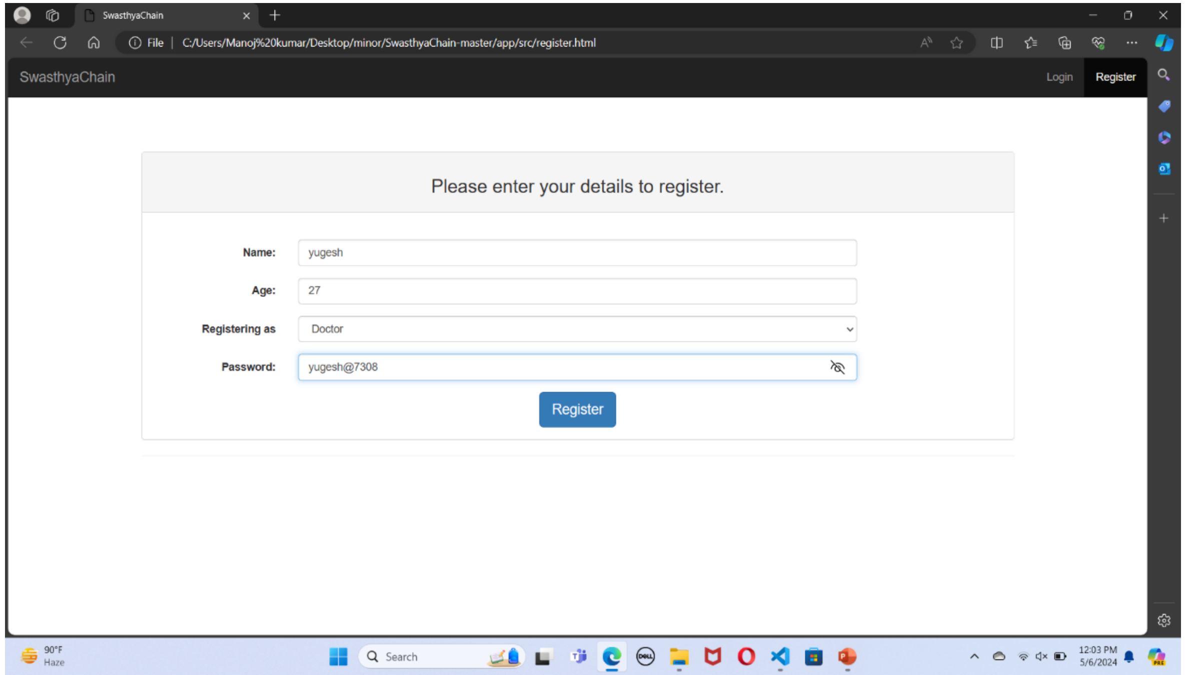
Age: 21

Registering as Patient

Password: •••••••••

Register

PATIENT LOGIN


SwasthyaChain
File | C:/Users/Manoj%20kumar/Desktop/minor/SwasthyaChain-master/app/src/register.html
SwasthyaChain
Login
Register
90°F
Haze
Search
12:03 PM
5/6/2024

Please enter your details to register.

Name: yugesh

Age: 27

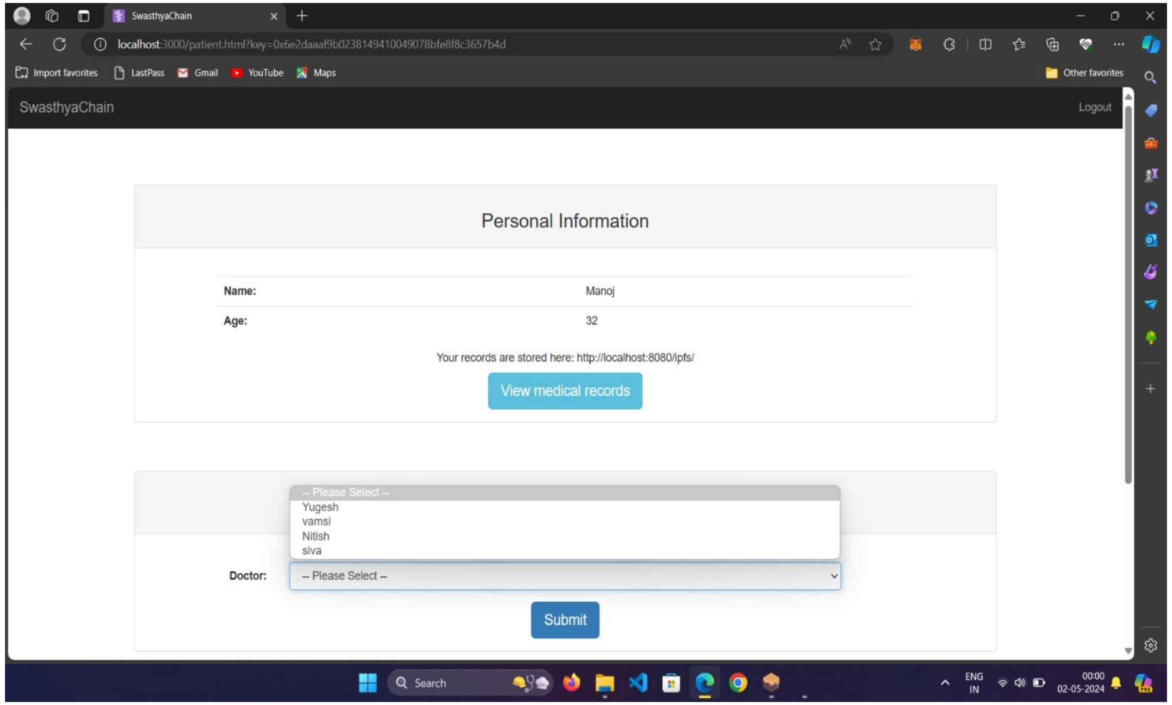
Registering as Doctor

Password: yugesh@7308

Register

DOCTOR LOGIN

# Work done so far (cont.):



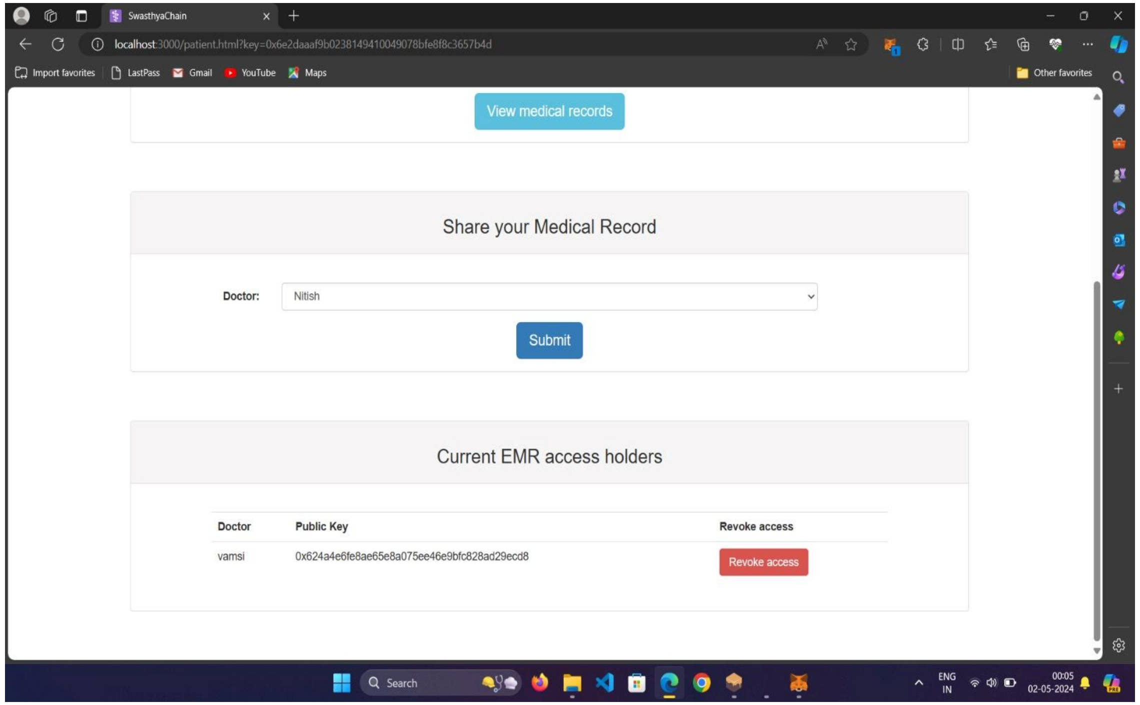
Personal Information

| | |
|---|---|
| **Name:** | Manoj |
| **Age:** | 32 |

Your records are stored here: http://localhost:8080/ipfs/

**Doctor:** -- Please Select --

-- Please Select --
Yugesh
vamsi
Nitish
siva



Share your Medical Record

**Doctor:** Nitish

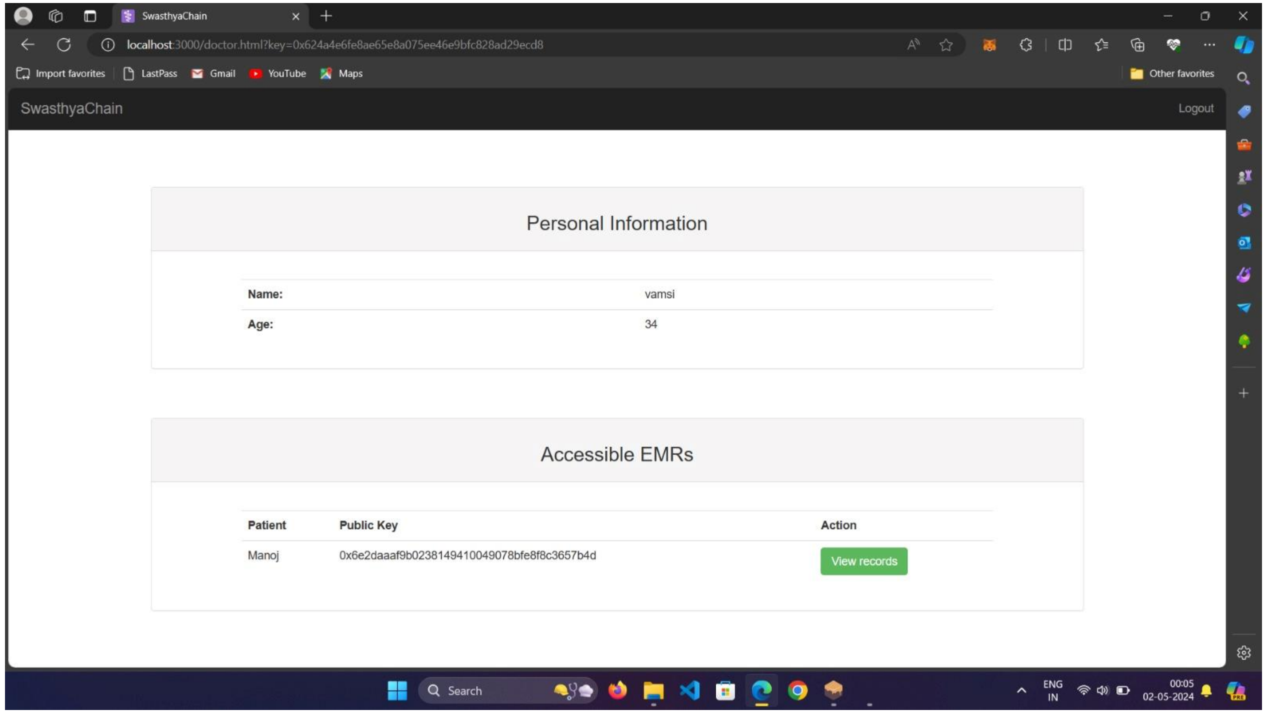
Current EMR access holders

| Doctor | Public Key | Revoke access |
|---|---|---|
| vamsi | 0x624a4e6fe8ae65e8a075ee46e9bfc828ad29ecd8 | Revoke access |

PATIENT DASHBOARD

1. Can give access to selected doctors
2. Can revoke access from permitted doctors

# Work done so far (cont.):



SwasthyaChain

Personal Information

| | |
|---|---|
| **Name:** | vamsi |
| **Age:** | 34 |

Accessible EMRs

| Patient | Public Key | Action |
|---|---|---|
| Manoj | 0x6e2daaaf9b0238149410049078bfe8f8c3657b4d | View records |

DOCTOR DASHBOARD

Can view patient record whose access is permitted by patient

# Evaluation:

ATTRIBUTE BASED PRIVACY PRESERVING:

- For high-level privacy attribute I, we use SHA265, instead of practical ID, so that an attacker cannot obtain a real ID of a participant in a transaction.
- For medium-level privacy attribute P, we design an LDP-based disturbance. This design can ensure a requester not to infer an individual information distribution from the collected data, for the reason that each bit in the collected vector is randomized with probability p, q.
- Finally, we design smart contract to implement dynamic access control over low-level privacy C, as well as the total EMRs.

ACCURACY:

- We measure accuracy through the rate of number of successful transactions and number of total transactions.

$$\text{Accuracy} = \text{o}\frac{Number\ of\ successful\ transactions}{Number\ of\ total\ transactions}$$

- Out of 25 transactions that performed, we had 23 successful transactions . Hence accuracy score of our model is 92%.

# Conclusion:

- we present a blockchain-based privacy preserved smart healthcare system, aiming to provide dynamic access control and fine-grained privacy protection for personal EMR exchanging and sharing.
- We design multi-level smart contracts in a blockchain platform to conduct dynamic access control between publishers and requestors
- We classify EMR attributes into different privacy levels, and configure corresponding privacy budgets of LDP to achieve the goal of attribute-based differential privacy protection.
- In the future, we plan to enhance the flexibility of access control principle by considering security, privacy and complex workflow of IoMT issues simultaneously.

# References:

[1] Guangjun Wu, Shupeng Wang, Member, IEEE, Zhaolong Ning, and Bingqing Zhu, “Privacy-preserved electronic medical record exchanging and sharing: A Blockchain-Based smart health care system”, IEEE J. Biomed. Health Informat., Vol. 26, No. 5,2022.

[2] Y. Zhuang, L. R. Sheets, Y. W. Chen, Z. Y. Shae, J. J. P. Tsai, and C. R. Shyu, “A patient-centric health information exchange framework using blockchain technology,” IEEE J. Biomed. Health Informat., vol. 24, no. 8, pp. 2169–2176, 2020.

[3] G.Cormode, S. Jha, T. Kulkarni, N. Li, D. Srivastava, and T. Wang, “Privacy at scale: Local differential privacy in practice,” in Proc. Int. Conf. Manage. Data, 2018.

# References(cont.):

[4] M. Muzammal, Q. Qu, and B. Nasrulin, “Renovating blockchain with distributed databases: An open sourcesystem,” Future Gener. Comput. Syst., vol. 90, pp. 105–117, 2019.

[5] C. Ge, Z. Liu, and L. Fang, “A blockchain based decentralized data security mechanism for the Internet of Things,” J. Parallel Distrib. Comput., vol. 141, pp. 1–9, 2020.