Medical Apllications of Blockchain

Swapnil Kole

Email: b118060@iiit-bh.ac.in

***Abstract*—one of the biggest problems in healthcare today is that organization hold multiple and fragmented health records about patients. With the dramatic increase in the Internet of Things (IoT), remote monitoring of health data and automation of health data to achieve intelligent healthcare solutions has received great attention recently. Due to the limited computing power and storage capacity of IoT devices, users' health data are generally stored in centralized third-party applications, such as the hospital database or cloud databases, and make users lose control of their health data, which can easily result in privacy leakage and single-point bottleneck of getting the data erased, mutated or deleted. In this paper, I propose Doctel, a large-scale health data application based on blockchain technology, where health data are stored with different levels of access controls and privacy policies to give the best benefits. Theoretical analysis and experimental results show that the proposed Doctel is applicable for smart healthcare systems. This system is ready to be highly scalable and can be massively adopted and what is proposed in this paper is just a prototype of the same.**

'Blockchain,EHR,Smart contract,Healthcare system, Internet of Things(IOT), cloud database, access control'

I. Introduction

Blockchain has been around for several years, and we see initiatives to use it for purposes other than Bitcoin on a regular basis. Wherever a transaction (financial or non-financial) requires security, confidentiality, transparency, and authenticity. Since its beginning, blockchain technology has gained significant acceptance, due to its exceptional characteristics such as immutability and transparency. These characteristics have made it an incredible solution to numerous issues in many industries, including supply chains, finance, banking, insurance, social media, as well as energy, and the healthcare sector is no exception. Blockchain is simply a distributed database in which each node maintains a ledger of transaction history. Blockchain technology is making significant strides in industries all over the world in terms of efficiency, convenience, and safeguarding business processes. Everyone in today's digital world is worried about the privacy and security of their data, including in health care. The healthcare industry, which is one of the most complex and flourishing, may also profit from the incorporation of blockchain technology into its business operations. The healthcare ecosystem is complicated, with several participants and fragile, sophisticated relationships. This causes data difficulties, privacy concerns, and operational inefficiencies. Ownership of administrative data and medical information, as well as trustworthy access to it, are critical, but the processes must be made more simpler and less expensive. Traditionally, healthcare records were kept on paper, which was easily broken and altered. Therefore, increased transparency in medical information is required to preserve patients' privacy and minimize the risk of security breaches. As a result, a new secure system is required to improve the data-access process in accordance with government privacy and security requirements in order to assure accountability and monitoring of medical usage data. Blockchain technology has the unrivalled potential to transform these complex healthcare procedures and difficulties by placing the patient at the core of the healthcare ecosystem while also increasing the security and privacy of health data. As a dependable, secure, and transparent Distributed Ledger Technology (DLT), Blockchain has significant promise for overcoming the aforementioned challenges and may thus be utilised for patient' EHR management and RPM system security.

A. Use Cases of Blockchain in Healthcare

There are several ways in which blockchain might assist to cover up loopholes in today's healthcare industry. In this section, we discussed blockchain use cases in healthcare. Data security is a critical concern in the healthcare business. Data security has become a major problem for patients worldwide, with the amount of data breaches growing every year. The security concerns associated with online accessing, storing, and maintaining healthcare information include fragmented and disjointed health data, interoperability problems, data security, privacy, and scalability.

Blockchain technology is a decentralised, immutable ledger of records. Because of the blockchain's high security features, any information stored on it is almost impossible to hack or change. Any changes to the infor-

mation are clearly visible because of the transparency feature, so there is no possibility of altering with the data.

II. Related Works

Many researchers developed a solution based on blockchain technology in medical healthcare that will not only safeguard data from tampering but will also prevent data leakage. This technique has the potential to preserve data and ensure consistency.

This study [1]offers i-Blockchain, which employs a blockchain which is permissioned to enhance the individual's data sharing experience and protect the privacy of patient health data by using different levels of access control. To prevent malicious activities, it only permits qualified users and Service Providers [Healthcare] to join the network. In addition to a public key and a private key for safe exchange of data, it employs hot storage functions as storage where temporarily users store data that is requested and off-chain storage in the form of off-chain storage.

Nguyen et al. [2]proposed an Electronic Health Records sharing scheme based on a mobo-cloud platform. They created an access control system for doctors, patients, and healthcare providers which is way far reliable efficient. They had protected the patient's sensitive information from malicious activities. They have used the Ethereum mainnet blockchain to share real-time data on a mobile application.

Kai Fan et al. [3] proposed MedBlock, a blockchain-based information management solution, to handle patients' information. MedBlock's distributed ledger allows for quicker Electronic Medical Records access and retrieval in their proposed architecture. Their proposed MedBlock provides a high level of information security because of the combination of their strategic symmetric encryption and access control methods. Their method avoids the disclosure of the patients' identity information, which has the same effect as the ring signature. They improved the efficiency of information retrieval by using bread crumbs on the ledger. They developed a reliable and effective hybrid consensus technique to reduce unnecessary energy use and power centralization.

Aujla and Jindal [4] proposed a lightweight private blockchain-based method for healthcare data protection (Privacy of Health Records). It was proposed to use end devices to securely share health data with cloud servers. For the prevention of data redundancy, a "tensor train decomposition model" was provided for storing health data on cloud servers. Blockchain technology was employed for data security as well as to protect the healthcare data privacy. Registration, block generation, validation, data generation, and updates on block were some of the steps in their proposal. The proposed scheme used some Layer 2 solution for optimality ie. zero-knowledge proof (ZKP) protocol to confirm the authenticity of two persons without revealing any confidential information.

Researchers [5] presented a blockchain-based infrastructure in the healthcare system for remote patients. Every patient has wearable devices (sensors in their watches like heart rate monitor) that obtain health data at regular intervals as specified in their architecture. The blockchain stores the information after it has been preprocessed by the system. A miner mechanism is employed for the generation of blocks. The miner technique is not the same as the miner concept in bitcoin. In the proposed system, only one miner works to generate the hash value of the current block. In the bitcoin system, multiple miners work together to generate current block's hash value. However, The patient agent chooses an appropriate miner based on a set of criteria (eg, reliability and previous experience of miners). For the sharing of health information across health practitioners, the suggested approach used a patient-centric model.

Adarsh Kumar et al. [6] has designed a smart healthcare system using Ethereum blockchain framework and healthcare 4.0 processes. In their smart healthcare system, they used an Ethereum virtual machine to run their contracts, meta-mask as a wallet (gateway to the blockchain and do transactions), remix as IDE (to write and test smart contracts), Geth (command-line interface) as Go-Ethereum, Ganache for account creation and running a local blockchain and Athena as a web interface to analyze the performance of the system. To validate the data accessibility they used statistical simulation optimization methods and algorithms. Their proposed smart healthcare system's advantages are that the system can protect from central authorities approach and rather applies a decentralized approach system, data security, and data management.

The researchers [7] offered a conceptual approach for sharing personal continuous ever-changing health-related info using blockchain. They used Ethereum as a development framework for their system. Cloud storage is used in conjunction with this method to get scalability. The authors recommended employing hashmaps to the location in the storage to tackle the challenge of sharing dynamic, continuously changing, large-sized data while merging blockchain and cloud storage as they came up that hashmaps are the most optimal data structure to accomplish this task. Large quantity of data may be kept

on cloud in an encrypted format, but only metadata and transaction's data can be preserved and shared on the blockchain as the data is on the cloud and the retrieval link is put in the blockchain.

Chattu et al. [8] discussed disease surveillance system using blockchain technology. They discussed about how blockchain can be used in advance identification of threats and sending reports to healthcare organizations so that preventive measures can be taken. They used ML algorithms to create a disease surveillance system.

The researchers [9] employed data masking technology to preserve a patient's privacy by transforming and disguising sensitive data into virtual data using masking algos that specialized algorithms. They also employed the InterPlanetary File System to create a secure Electronic Medical Record system, as IPFS connects all nodes to the same file system and prevents file manipulation and duplication. It is important that IPFS not only stores files in several formats, but it also returns the hash of the persistent file. Following hash value and data concealing , the user (a patient or a doctor) distributes medical record data on the blockchain network for storage. This concept addresses the problem of data readily being changed and disappearing throughout the medical record exchange process.

In this [10] proposal, researchers suggested a blockchain framework system named BiiMED. Ethereum blockchain is getting used as a framework. Its usage is to maintain and verify data that is shared between medical service providers who store health data in the cloud and exchange patients' Electronic Health Records. This method introduced the Trusted Third Party Auditor, which is based on blockchain technology and handles validating of the transferred data. While exchanging EHR, the proposed approach maintains data interoperability and integrity. To identify and authenticate users, the proposed system employs an access management module. As a result, secrecy is ensured. Furthermore, based on scalability analysis, the suggested system supports an enormous population of patients.

The researchers [11] of this study developed a decentralized storage system by merging Ethereum blockchain, Inter-Planetary File System, and attribute-based encryption technologies to improve data privacy and availability on clouds. To provide fine-grained access control on cloud data, a data owner distributes a secret key to users and encrypts his data using a predetermined access policy. The smart contracts are meant to provide keyword search in de-centralized storage systems, which solves the issue of conventional cloud storage not delivering accurate search results.

Omar et al. [12] presented a patient-centric data management system for healthcare. A Private Accessible Unit (PAU) is used in this system for safe interaction between users. After registering on the system, users receive a unique Identification (ID), which they may use to securely retrieve data stored on the blockchain.

The authors [13] mentioned that healthcare data is an important and valuable asset and that there is an urgent need to efficiently preserve it using safe methods. Due to data in healthcare being fragmented the researchers faced a lot of difficulties. As a result, this must be resolved. They believed that by combining blockchain technology and the cloud environment, they might solve the problem to some extent. They presented a blockchain-based network for storing and managing massive amounts of healthcare data with security, accuracy, and convenience. At the moment, all data related to healthcare is kept on centralized systems. The researchers presented a design that ensures decentralization. This places the data in a dispersed context, which improves interoperability. The data are fragmented in this system, and every transaction is kept on multiple nodes. The proposed architecture uses cryptographic methods to verify the user's identity after a user requests a transaction. The system adds a new block to the current blockchain regarding the transaction when the user has been validated by the system.

The authors [14] of this research suggested MedChain, a blockchain-based session-based healthcare data exchange system. The proposed system allows patients' Electronic Health Records as well as physiological information obtained from the internet of medical things (IoMT) devices linked to their bodies to be managed and shared. Although MedChain ensures data integrity and confidentiality, it has significant limits in terms of availability and scalability. The availability of the sharing service is dependent on the patient's availability to execute these acts due to manually sharing data and uploading data manually to blockchain which can become a disadvantage.

Garg et al. [15] suggested a model called BAKMP-IoMT an authentication key agreement protocol that uses the Elliptic curve encryption algorithm, signatures, and blockchain to safeguard transmitted data and enable anonymity in an unsecured channel. In their proposed model the cloud servers keeps track of the entire healthcare data on a blockchain. To authenticate between the communicating nodes, they included the identity of the trusted authority as an extra security parameter. The

model uses Automated Validation of Internet Security Protocols and Applications (AVISPA) tool for security verification against the different types of possible malicious attacks.

III. Proposed Work

In this paper, I propose DocTel, a blockchain health data application, for storing health data with different levels of access controls and privacy policies to give the best benefits. In DocTel admins (hospital management) or IoT devices can regularly update the users' health data or add new data. Doctors and AI health analyzers can anywhere and anytime diagnose these data and this data will build up all the historical data of that particular user and will be connected by a unique identification number (Aadhar no.) to every patient across the whole country who are part of or can become part of this system. The data will continuously keep on growing as more and more patients get added with them more data will be coming in and blockchain is incapable of storing huge amounts of data as the resource requirements will become too high and complexity will increase to maintain, search and verify the health data. The optimal solution at this point will be to use the InterPlanetary File System (IPFS), a content-addressable (having hash maps that directly maps from the hash to the file location or in simple terms the hash is the location of the file) distributed file system to store data. The data is distributed over different nodes in the network as there is no central server. Even if some nodes are disconnected still the data is accessible from other running nodes and it can distribute large amounts of data without duplication. After uploading file to IPFS it returns a hash string which is unique and can be used to retrieve the file from anywhere. In the DocTel application, most of the data is stored in the IPFS and that particular hash of that file is stored in the blockchain and helps in data integrity verification and link data in ipfs storage. The health data has to be accessed by the doctors and health analyzers so access control is added to the application so only specific groups of people can access the sensitive health data.

In the next section, there is a flow chart and then explaining the whole workflow. Parties involved in this project are as follows:

Patient: A person who is having to go to the hospital. Should have a unique identification no. such as aadhar number which is already provided by the government to all its citizens.

Doctor: A doctor who can treat patients and is associated with a hospital or is isolatedly having his own clinic.

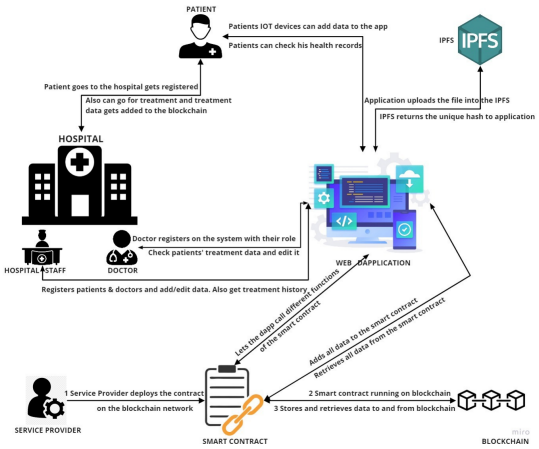

Fig. 1. Proposed blockchain system architecture

Hospital Staff: A hospital staff helps in the process of registering patients and doctors on the application. Helps in the retrieval of health data of patients and doctors also add treatment for patients.

Figure 4 shows the detailed model of the proposed system. Currently I'm using a local blockchain known as ganache which works exactly as Ethereum blockchain so that all transactions run very fast it is also running on rinkeby ropsten network of ethereum to which everybody involved in the system can get connected but is not compulsory and the only difference it has from the ethereum mainnet is that it only requires fake money and not the real one. I developed a smart contract written in Solidity language to manage all these activities. This smart contract is running on the "Code is law" protocol i.e. the functionality under all circumstances will follow whatever is written in the code. This contract is deployed on ganache blockchain, rinkeby and ropsten testnets of Ethereum network also. I created a web dapplication using React.js [A javascript library for building user interfaces] for the frontend creation for all the user interfaces and functionality that can be leveraged for this application, Web3.js [a library that allows you to interact with local or remote Ethereum node using HTTP, IPC, or Websocket] connected with blockchain backend using Metamask[an extension for accessing Ethereum enabled distributed applications, or "Dapps" in your browser] extension that allows you to cover for the gas fees and transaction cost. It is used to be an interface for all the involved parties to access the blockchain network and carry out various activities in the DocTel system. The system strictly follows the decentralized aspects of

a private blockchain with a consensus mechanism of entities for every transaction. The detailed steps involved in our proposed Blockchain system are depicted by fig. 1 as follows:

Mining Continuously: The process of block production in blockchain is known as mining and is carried out by miners who validate all transactions and check the legitimacy of all functions getting called in the smart contract. In our platform, the mining is continuous in the blockchain and smart contract written in solidity language accomplishes code is law where the functions runs exactly as it is coded in the contract. The service provider can deploy the contract[once and for all] and start mining. The access control is not at the mining level rather it is in the contract layer. So the mining is continuous but the transactions can only be done by a particular agent and the smart contract's validates all transactions before sending them to the blockchain.

Users Registry: This step is to collect all the information about the involved parties, which can be achieved by the registration of all the parties such as hospital staff, doctors, and patients into the platform. The registration can be carried out with a government identity proof(Aadhar number)of the parties and their registration details get stored in Blockchain. While registering the patients all health data is added to the blockchain and ipfs [and the link is sent into the blockchain] which lets the blockchain store only hashes and ipfs storing all the bigger files which might take a lot of storage.

Adding Treatment: Whenever a patient comes for any type of treatment at the hospital, the hospital staff adds a new treatment [the details of all the treatment] and it gets connected to the patient's unique no. [aadhar no.] and the set of doctors doing the treatment also gets connected to that treatment. So everything in this system is strongly interleaved with each other and can be retrieved very easily only by concerned parties.

Changing Treatment Stage: Treatment status can only be advanced to next steps and done by only hospital staff and doctors and it tracks the history of the treatment as the history cannot be mutated or deleted in blockchain. We solve the purpose of losing or getting records manipulated. At each stage new doctors might get added, new reports and prescriptions also get added and can be tracked anytime. The system is made robust enough to handle all these.

IV. Technology Implemented

The main technologies implemented in this project are: Blockchain, Inter-Planetary File System, Ethereum, Smart Contracts, Ethereum Virtual Machine, Solidity, React Javascript, Ganache, Metamask, AWS Amplify, Github, Consensus Algorithm, and Hashing Algorithm. A brief description of all these technologies follows

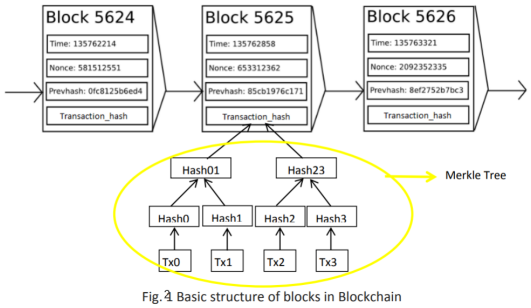

Fig. 1 Basic structure of blocks in Blockchain

Fig. 2. Basic Structure of blocks in blockchain

A. Blockchain:

It is a distributed ledger-based technology that uses consensus-based decisions to come to a single point of truth. It involves three main technologies which are private key cryptography, peer-2-peer network, and Blockchain protocol. The data once entered becomes immutable and hackproof. Blocks in blockchain contain groups of valid transactions that are encoded into a Merkle tree structure and hashed at each step of the merkle tree generation. Each block contains the hash of the parent block in the blockchain, linking the two together so that they cannot be tanmpered. The linked blocks form a chain. This repeatative process confirms the integrity of the parent or previous block, all the way back to the genesis block. Each block also has a timestamp and a nonce associated with it **fig-2**

B. Inter-Planetary File System:

The Inter-Planetary File System[IPFS] protocol is a peer-2-peer network for sharing and storing data in a distributed system of files. For uniquely identifying each file it uses content addressing in a global namespace in which all computing nodes are connected in a decentralized manner. It uses content-based addressing and Merkle Directed Acyclic Graph data structure **fig-2**.

A Merkle-DAG is a Directed Acyclic Graph structure where each node has an identifier and this is the result of hashing the contents of the node. So to get the hash of the any node the children nodes are hashed together and the new hash that comes is the hash of the parent node. The hashing is done using a cryptographic hash function like SHA256.

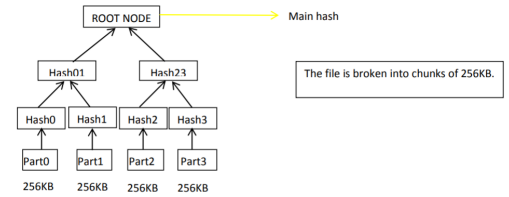

Fig 2: Storing strategy in IPFS via Merkle-DAG

Fig. 3. Storing strategy in IPFS via Merkle-DAG

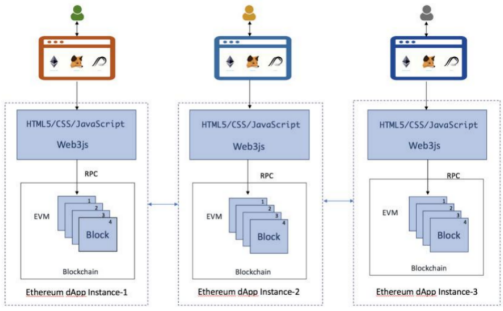

Fig 4: EthereumDapp instance

Fig. 4. Ethereum Dapp instance

C. Ethereum:

Ethereum is a platform based on Blockchain technology that enables anyone to build and deploy smart contracts and connected decentralized applications. Ethereum's coding language solidity helps write smart contracts. Its native currency is Eth. It was founded by Vitalik Buterin.

D. Dapplication:

A decentralized application **fig-3** is a computer application that runs on a distributed computing system. They have distributed ledger [DLT] based technology. It has a web-front in any javascript libraries, smart contract running on blockchain as backend and web3, or some kind of RPC pipelines to connect both of them together as a middleware.

E. Solidity:

Solidity is a contract oriented language. It is used mostly for Ethereum Virtual Machine. It is statically typed language so you have define types for each data and functions, supporting inheritance, libraries and complex user defined types. Almost all the applications of solidity are for writing smart contracts.

F. Github:

It is a version control software used for versioning and hosting of software, codebases and applications. It offers the distributed version controlling and project code management functionality. In this project github is purely used for version control and first step in CI/CD pipeline.

G. AWS Amplify:

AWS Amplify is a set of purpose-built tools and features that lets frontend web developers build full-stack applications, with the flexibility to leverage the breadth of AWS services. In this project it is used for the CI/CD pipeline and hosting the web application.

H. React.js:

React is a front-end open-source JavaScript library for building user experience and interfaces based on small components. In this project it is extensive used for the creation of front end and UI

I. Ganache:

Ganache is a copy of Ethereum Blockchain which can be used as a mock for personal use and is used to test and deploy smart contracts , develop applications, run tests and perform other functionalities free of cost. It is used in this project as the blockchain running locally.

J. Metamask:

MetaMask is a cryptocurrency wallet for interacting with the Ethereum blockchain. It enables users to access their Ethereum wallet through a mobile app or browser extension, which can then be used to interact with decentralized applications. In this system it acts as a gateway to the blockchain world and to carry on all the transactions.

Algorithm: A voting mechanism where all the nodes connected to a network vote on the validity of a block only then the block is confirmed over the blockchain. The consensus algorithms that can be used for this project are Practical Byzantine Fault Tolerance, Proof of Work and Proof of stake.

K. Hashing Algorithm:

It plays a crucial role in the blockchain process and also in the integrity of the transaction and confidentiality of data. It transforms and maps an arbitrary length of input arbitrary data value to a unique fixed-length value. The algorithm should be one-way and collision-free. Some majorly used hashing functions are SHA-256 and Keccak.

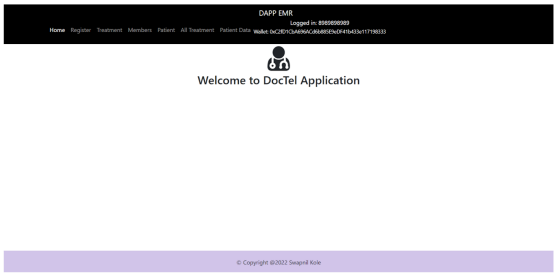

Fig. 5. Screenshot of Homepage

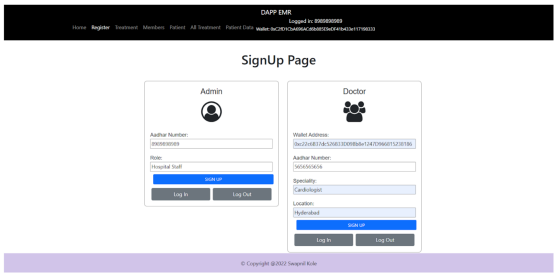

Fig. 6. Screenshot of Admin Registration Page

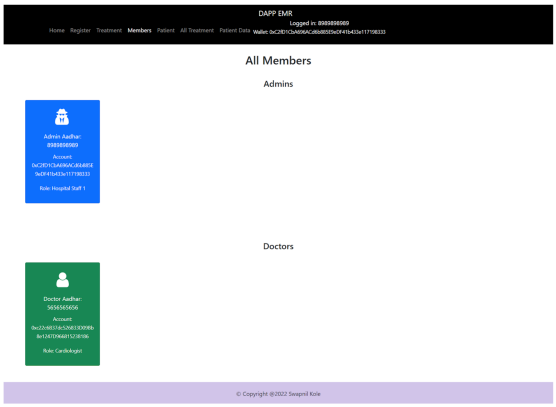

Fig. 7. Details of All Members page

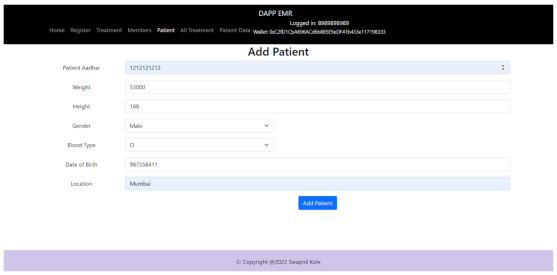

Fig. 8. Screenshot of Patient Registration page

V. Implementation

The implementation is done in the form of a small working prototype application. A detailed explanation with the help of screenshots follows for each webpage of my system.

Fig-5 is a very basic homepage I have made just to show that the web application exists and can be customized a lot to make it more professional. The homepage moving forward will have some more features and will have a help center where people will get to know how to use this application.

Fig-5 is the registration page where the admin can signup/login/logout and they require a wallet to be connected to do all these transactions. The admin can join and input his aadhar no. and role in the system and his wallet should be connected to get the account address of the admin. If the admin clicks on "Sign up" button all these admin data will go into the blockchain as a transaction and this admin will be registered into this system. With the same inputs the admin can click on "Log In" and the header will reflect the wallet and logged-in aadhar no. of that admin. If he clicks on "Log Out" his account gets disconnected from the current log in. A doctor can sign up on his own or the hospital staff can make the sign up for him. The doctor has to provide his wallet address, aadhar number, his specialty, and his location and he/she will be registered into the system. The Log In and Log Out works the same for him as well.

Here in **fig-6** we have the member list and only the hospital staff can access it. They can see the details of all the hospital staff as in for now only the wallet address and aadhar no. but later the details can be increased also. In addition to this even the doctors' details namely aadhar number, wallet address, and role can be seen.

This page in **fig-7** is exclusively for patients' registration into the system for the first time and later on it can be updated and each time there is a new treatment. In this registration, the patient has to give his aadhar no., weight (in grams), height (in cms), gender, blood group, date of birth in epoch time, and location. After the hospital staff or the doctor enters this data it will go into the blockchain as a transaction. There is a validation for kind of extreme values for each field. If the value deviates from general values by a lot its going to throw an error statement. For example the Height cannot be more than 300 cms so we have the error handler on

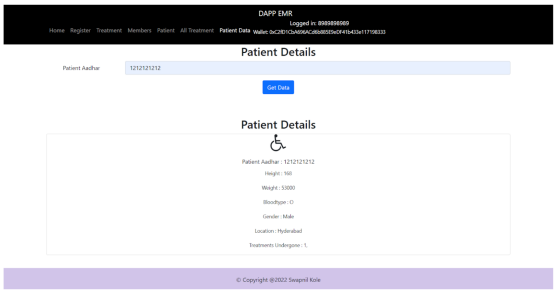

Fig. 9. Screenshot of Patient Details page

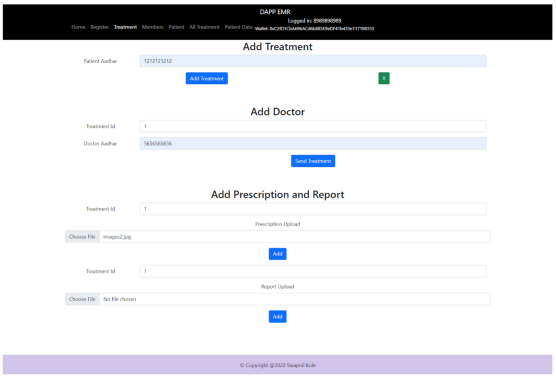

Fig. 10. Add Treatment Reports page

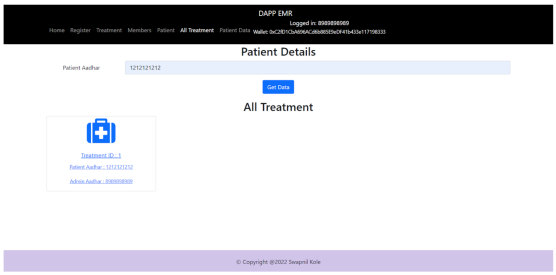

Fig. 11. Treatment Details page

it which throws an error statement anytime somebody enters values exceeding the limit.

In this page **fig-8**, the hospital staff, doctor or the patient can retrieve the patient's data by putting his aadhar no. in the search box and clicking on "Get Data" and all the details will show in the below section. The patient's aadhar no., height, weight, bloodtype, gender and location is shown. In this section there is "Treatments Undergone" which will show all the treatments Id this patient has gone through.

This is the page **fig-9** where hospital staff or doctors can add treatments. They should start by adding the patient's aadhar when he arrives at the hospital for some treatment. Once the add treatment is clicked a treatment is generated in the blockchain which has the treatment Id, the patient's aadhar no. and the logged in user's aadhar no. (hospital staff or doctor whoever did the transaction). Whenever this treatment is assigned to a doctor the "add doctor" form should be used in which the treatment id and doctor's aadhar no. should be added who is going to do the treatment and this data will go to the blockchain and also an event will be emitted in the blockchain to make this doctor addition immutable. Next during the whole process of this treatment any prescription or reports can be added just by adding the treatment Id and uploading the file for the same (any format) and then click on add. This file is first uploaded to Ipfs from where ipfs gives back a hash through which the file can be accessed. This hash is then sent to the blockchain to save up on space by keeping just hash rather than whole file.

This page in **fig-10** shows all the treatments in the system. It shows just basic data namely the treatment Id, Patient's aadhar and the admin's aadhar who added this treatment. There is a search bar in which when a patient's aadhar no. is put and searched for it will return only that particular patient's treatments. Every single treatment when clicked routes to a Treatment details page which is shown in the next image.

This is the Treatment History/Details page in **fig-11** it firstly shows the treatment Id, Patient's aadhar and the admin's aadhar who added this treatment. Then in the events section it gives all the history of this treatment since when it was added and timestamp of each of them. In this particular example it shows when the treatment was added. It shows that a doctor was added to the treatment and his aadhar no. following a prescription and report was added and shows the time of it. The picture is a small version of the actual picture which can be viewed by clicking on this image and this image is getting retrieved from the ipfs by taking the hash from the blockchain. Also the hash is shown in the same card.

This is Ganache application in **fig-12** where I'm currently running a local blockchain and it functions exactly the same as the ethereum blockchain just with fake money and I'm using it for testing the application, seeing logs, having accounts and funds in them.

This is my terminal in **fig-13** which is running a node for the ipfs to get connected with the ipfs and send and

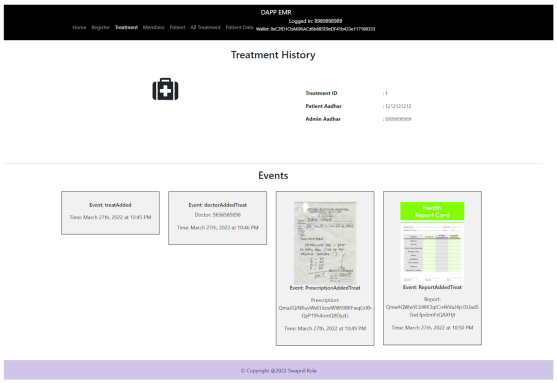

Fig. 12. Treatment History page

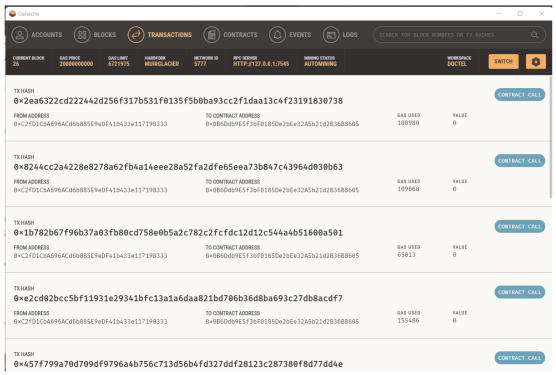

Fig. 13. Ganache Application

receive data. It is running on 5001 port and without running this the ipfs files neither can be retrieved nor uploaded.

This screenshot in **fig-14** is from my github repository which I'm using as a version control system and keeps my codes safe from getting deleted or modified.

This screen in **fig-15** is from Amazon AWS Amplify where I have hosted my website for this application and it helps in the whole CI/CD pipeline as everytime I push my code to github repository amplify will pull the changes and start with the deployment stages as provision, build, deploy and then verify. After these 4 steps, the website is live at a website from amplify having SSL certificate.

A detailed view of each step in CI/CD pipeline in **fig-16** is given here with logs of each step.

VI. Result Discussion

The application is already able to achieve all the objectives that were mentioned before making this proposal.

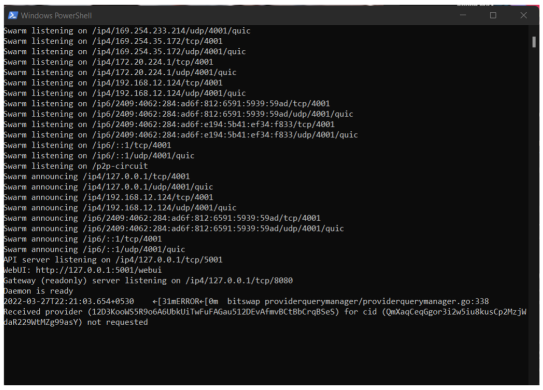

Fig. 14. Terminal Page

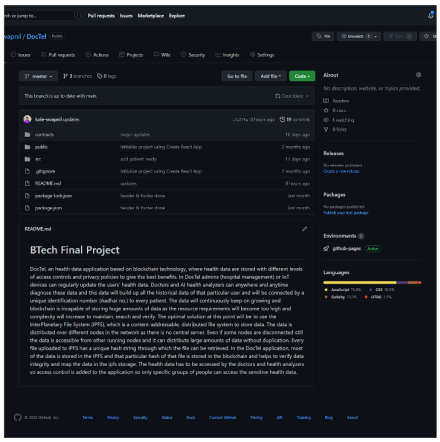

Fig. 15. Github Repository

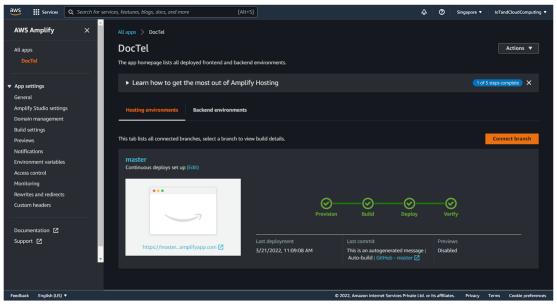

Fig. 16. Amazon AWS Amplify

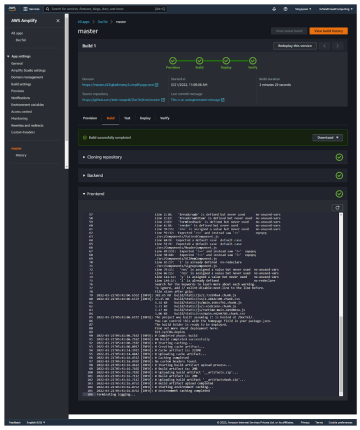

Fig. 17. CI/CD pipeline build

The Medical records cannot be mutated, deleted, or tampered with anymore as the database is decentralized with the help of blockchain. Nobody at a later stage can show different results as once written on blockchain nothing can be changed but later on new reports can be added, as you might have seen in the application every operation is having a timestamp. Each health record is connected to a user's unique identification number or Aadhar no. and we can get a unified decentralized database all across the country. Easily all the health records of a patient can be retrieved by searching by his aadhar no. and is way faster and more reliable for patients' moving from place to place. A lot of reliability as well as well as robustness is added to the application. Its rather simple, functional User interface makes it easy for all the users to like and use it.

VII. Conclusion

I can conclude that this application after using the latest and the top technologies has a lot of potential and a large-scale implementation of this application is worth the efforts behind it. Also, the system once in production will be very reliable, efficient, and user-friendly. It drives today's medical records applications to all new levels and this application can have many more integrations so that other applications can be easily integrated into this application and they will become decentralized very easily. Decentralization is the new future and making applications decentralized is the first step into it. Blockchain as an emerging technology will take everything into the decentralized world.

VIII. Future Works

A lot can be improved in the user interface (UI) and user experience (UX) to make it more user-friendly. A lot of applications (currently used in Healthcare) can be integrated or some major features can be added to make this application an all-in-one application for all healthcare-related tasks. The IoT part of the applications is also what will be incorporated next to take the application to a whole new dimension. New extensions will be added to the application to make it interoperable for diverse medical usage.

References

[1] K. Ito, K. Tago, and Q. Jin, "i-blockchain: A blockchain-empowered individual-centric framework for privacy-preserved use of personal health data," in *2018 9th International Conference on Information Technology in Medicine and Education (ITME)*. IEEE, 2018, pp. 829–833.

[2] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure ehrs sharing of mobile cloud based e-health systems," *IEEE access*, vol. 7, pp. 66 792–66 806, 2019.

[3] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "Medblock: Efficient and secure medical data sharing via blockchain," *Journal of medical systems*, vol. 42, no. 8, pp. 1–11, 2018.

[4] G. S. Aujla and A. Jindal, "A decoupled blockchain approach for edge-envisioned iot-based healthcare monitoring," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 491–499, 2020.

[5] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A patient agent to manage blockchains for remote patient monitoring," *Stud Health Technol Inform*, vol. 254, pp. 105–115, 2018.

[6] A. Kumar, R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover, and E. Hossain, "A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes," *IEEE Access*, vol. 8, pp. 118 433–118 471, 2020.

[7] X. Zheng, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Mere, "Blockchain-based personal health data sharing system using cloud storage," in *2018 IEEE 20th international conference on e-health networking, applications and services (Healthcom)*. IEEE, 2018, pp. 1–6.

[8] V. K. Chattu, A. Nanda, S. K. Chattu, S. M. Kadri, and A. W. Knight, "The emerging role of blockchain technology applications in routine disease surveillance systems to strengthen global health security," *Big Data and Cognitive Computing*, vol. 3, no. 2, p. 25, 2019.

[9] S. Wu and J. Du, "Electronic medical record security sharing model based on blockchain," in *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, 2019, pp. 13–17.

[10] R. Jabbar, N. Fetais, M. Krichen, and K. Barkaoui, "Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity," in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*. IEEE, 2020, pp. 310–317.

[11] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *Ieee Access*, vol. 6, pp. 38 437–38 450, 2018.

[12] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "Medibchain: A blockchain based privacy preserving platform for healthcare data," in *International conference on security, privacy and anonymity in computation, communication and storage*. Springer, 2017, pp. 534–543.

[13] H. Kaur, M. A. Alam, R. Jameel, A. K. Mourya, and V. Chang, "A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment," *Journal of medical systems*, vol. 42, no. 8, pp. 1–11, 2018.

[14] B. Shen, J. Guo, and Y. Yang, "Medchain: Efficient healthcare data sharing via blockchain," *Applied sciences*, vol. 9, no. 6, p. 1207, 2019.

[15] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. Rodrigues, and Y. Park, "Bakmp-iomt: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment," *IEEE Access*, vol. 8, pp. 95 956–95 977, 2020.