HEALTHCHAIN: A Patient Centric Blockchain Based Web Application For Maintaining Electronic Healthcare Records.

Purva Rumde[1], Rahul Doshi[2], Anushka Raval[3], Neeta Kadukar[4], Deepali Maste[5]

[1,2,3]*Department of Information Technology, Shri Bhagubhai Mafatlal Polytechnic, Mumbai, India*
[4] *Vice-principal, Department of Information Technology, Shri Bhagubhai Mafatlal Polytechnic, Mumbai, India*
[5]*Department of Information Technology, Atharva College of Engineering, Mumbai, India*

---***---

Abstract— Our web application "Healthchain: Your data our responsibility". This framework centers around creating privacy to patient clinical records utilizing 'Blockchain Technology'. Patient privacy or classification is one among the preeminent vital support points in medical services. Safeguarding the individual subtleties of a patient isn't only a question of moral regard, it's vital for bond trust between the specialist and patient. This blockchain based E-health record system will provide deep mutual trust between the doctor and patient. This project will permit patients to have the control of producing, overseeing and imparting EHR's to the approved care giver - Doctor. In addition, the medical care specialist and suppliers of medical care administration access these EHR's across the abroad, the progress program of medical care arrangement is relied upon to be accomplished.

Keywords—Healthcare, Blockchain, medical records, trust, security, privacy.

1. INTRODUCTION

As the world is evolving drastic changes in the healthcare system are widely seen and are equally being adopted by people around the globe. We can't deny the fact that the traditional healthcare system is quite extensively preferred by people who aren't that much aware about the latest technology. Especially the people living in the rural areas however favour the medical records on paper or done manually by the hospitals. The Revolutionary change in the Healthcare sector began in the mid 1960's conventionally known to all as Electronic Healthcare Records or Electronic Medical Records. E-Health Records (EHRs) offers a easy to access and handy medical record storage capability, which enhances traditional medical records of the patient which are available on paper to be electronically accessible on the web. An Electronic Health Record (EHR) is an electronic rendition of a patient's clinical history, and may incorporate every one of the key regulatory clinical information applicable to that individual's consideration under a specific specialist, including progress notes, issues, meds, past clinical history, vaccinations, lab

information and radiology reports. But since these EHRs are developed for hospitals they are considered to be centralised, as these EHRs are managed by a hospital management team. Every new technology or invention comes with pros and cons and the downfall of centralised EHRs is the storage facility, chances of the system being hacked and easily being vulnerable to illegal access by people outside the organisation. This is where blockchain in healthcare was brought into existence in 2012. And since then the concept of decentralised EHRs were introduced to all. Now coming to the reason for developing this web-based application named Heathchain, it is thought that health information technology, particularly electronic health records (EHR) will improve the healthcare facilities for both doctor and patient in a convenient and secure guarantee responsibility and transparency in the manner. The major rule of this project is to parade of information trade, reviewing trails in an unchanging way. To make it user friendly and efficient we have even added speech to text features in our web application.

A. Blockchain

Since the advancement of Bitcoin, a computerized digital currency, in 2008, Blockchain innovation has situated itself in the point of convergence of interest among a different scope of specialists and professionals. Blockchain is a decentralized record that stores all exchanges that have been made on top of a shared organization in a safe, certain and straightforward way. The fundamental benefit of Blockchain over the current innovations is that it empowers the two gatherings to make exchanges over the Internet safely without impedance of any mediator party. The exclusion of the outsider can decrease the handling cost while working on the security and effectiveness of exchanges. Blockchain is reforming different enterprises, going from finance, Internet of Things (IoT), medical services, notoriety frameworks, and production network the board.

It is worth focusing on that innovation organizations and monetary administrations put more than $1 billion just in 2016 into conveying Blockchain and it is very

unsurprising that this sum will be expanding drastically throughout the following not many years. The fast development of Blockchain innovation over the new years has opened up a lot of exploration holes and headings for the examination local area. Thus, an amazing measure of exploration tries have been directed inside the area of Blockchain as of late.[5]

B. Bigchain

BigchainDB[1] fills a hole in the decentralization environment: a decentralized data set, at scale. The BigchainDB configuration begins with a circulated data set (DB), and through a bunch of advancements adds blockchain attributes: decentralized control, unchanging nature, and creation and development of computerized resources. BigchainDB acquires attributes of present day conveyed data sets: straight scaling in throughput and limit with the quantity of nodes, a full featured NoSQL question language, productive questioning, and permissioning. BigchainDB is reciprocal to decentralized handling stages like Ethereum, and decentralized record frameworks like InterPlanetary File System (IPFS). Maybe than attempting to increase blockchain innovation, BigchainDB begins with a "major information" disseminated data set, and adds blockchain qualities. It evades the innovation decisions that plague Bitcoin, like full replication. Since the large information DB has its own implicit agreement calculation to endure amiable issues, we misuse that arrangement straightforwardly. We "move" of the calculation to allow it to choose which exchanges to compose, and what the square request is. We prohibit private, shared correspondence between the nodes with the exception of by means of the DB's underlying correspondence, for incredible investment funds in intricacy and for diminished security risk . This implies that noxious nodes can't send one message to part of the organization and distinctive message to other piece of the organization. Every time a node "talks," all the others can tune in.

C. IPFS

IPFS(Interplanetary File System)[2] gives a circulated record storage framework which works with association with the P2P network. The IPFS ascertains the special Hash of a record which is available to every one of the friends in the network. The hash gets altered each time the record gets refreshed. The IPFS is considered as the foundation of web 3.0 which gives a P2P decentralized record storage framework and content addressable method to get to the put away document. IPFS works with the appropriated hash table which is substantially more productive than BitTorrent, and Git document stockpiling framework. IPFS is otherwise called a form-controlled framework which guarantees the security, dependability, and versatility looked by the current

record stockpiling and sharing framework. A similar exchange has the very hash in the IPFS that guarantees the originality of the record. The IPFS hash gets dispersed to every one of the equals which likewise guarantees the consistency among the companions.

Interplanetary File framework gives high throughput content tended to obstruct capacity model which guarantees security of exchanges. IPFS gives a high throughput as far as access utilizing content-tended to impede capacity model, we additionally notice that capacity is another test in blockchain innovation attributable to the annex just highlights.

D. Express

Express[2]   is a trivial and versatile Node.js web application framework that gives a lively course of action of features to cultivate web and compact applications. It works with the quick advancement of Node based Web applications. Following are a portion of the center highlights of Express structure –

• Permits to set up middlewares to react to HTTP Requests.

• Portrays a coordinating table which is used to perform different operations subject to HTTP Method and URL.

 • Permits to powerfully deliver HTML Pages dependent on passing contentions to layouts.

E. MongoDB

One of MongoDB's essential objectives is to give prevalent execution, MongoDB can progressively fill the record, yet additionally preallocation of information documents to exploit extra space in return for stable execution. MongoDB utilizes as much memory as the reserve, attempting to naturally choose the right list for each question. To put it plainly, MongoDB in all parts of the plan is to guarantee his steady exhibition.[4]

MongoDB is quite possibly the most well known NoSQL data set, whose fundamental target is to overcome any issues between key-esteem stores with elite and adaptability and conventional RDBMS with rich administration, and take the benefits of both in one. MongoDB framework comprises of the customer application, the drivers, data set administration program Mongod, data set directing project A MongoDB framework holds a bunch of information bases, every data set holds a bunch of assortments, an assortment is a bunch of records, each archive is a bunch of fields, and a field is a key-esteem pair, key is the name of the field with the string type, esteem is the information of the field and can be any sort. MongoDB utilizes BSON as the information stockpiling and organization move design for archives. BSON is a parallel encoded serialization of

JSON-like records, which stores key-esteem pair in twofold byte with the way in to a string type and the worth to any kind including exhibit and report.[3]

2. PROBLEM STATEMENT

Patients face a vital need to emphasis in on the subtleties of their own medical care and reestablish the board of their own clinical information. As of now the majority of the medical care associations utilize a centralized technique for saving patient's data, indicative reports, and specialist's s prescription. Since it is an incorporated framework there are odds of information getting spilled or misused for different reasons as patients don't have power over their information and furthermore trading of the recorded information is tedious and an unpredictable interaction. The cutting edge medical services framework is involving computerized strategies for keeping up with patient's wellbeing records. Nonetheless, in current circumstance patients disperse their clinical information during life occasions, making their information move from one specialist/medical care association to another. Determined to manage these issues, we are making an application by changing the incorporated framework to a decentralized framework utilizing Blockchain innovation. The quick improvement of blockchain innovation advances medical services, including clinical records along with patient-related information.

3. LITERATURE REVIEW

Blockchain based EHRs have been implemented on a wider scale and are really brought into existence by a few companies. This section focuses on these healthcare applications and how well they have used blockchain to provide security and maintain the privacy of EHRs. Utilizing blockchain innovation, MedRec has shown how standards of decentralization may be applied to largescale information the board in an EMR framework. MedRec shows an inventive methodology for dealing with clinical records, giving auditability, interoperability and availability by means of a far reaching log. Intended for record adaptability and granularity, MedRec empowers patient information sharing and motivations for clinical analysts to support the framework. They anticipate formalizing an onboarding system for clinical examination "excavators", and investigating mining information financial matters. Soon, they expect to complete client studies to survey the attainability of the framework and to check patient and supplier interest. This might incorporate collaborating with nearby medical care bodies, and mimicking parts of framework proficiency in nature.[6] Another such framework that completely focuses on security is MeDShare a framework that highlights the issue of clinical information dividing between clinical large information caretakers in a trust-less climate. The framework is blockchain-based and gives information provenance, examining, and control for shared clinical information in cloud archives among enormous information elements. MeDShare supervises the information for malignant use from an information trustee organisation. In MeDShare, information changes and sharing from one person to the next, alongside all activities performed on the MeDShare framework, are recorded in a carefully designed way. The plan utilizes smart contracts and an entrance control tool to adequately follow the conduct of the information and renounce admittance to culpable elements on identification of infringement of authorizations on information. The presentation of MeDShare is tantamount to current state of the art answers for information dividing between cloud specialist organizations. By executing MeDShare, cloud specialist organizations and different information gatekeepers will actually want to accomplish information provenance and inspection while at the same time offering clinical information to individual like exploration and clinical organizations with insignificant danger to information security.[7]

BHEEM: Blockchain-based system for productive capacity and upkeep of EHRs. Here, the patient is provided the full control and responsibility for records and he can also check and monitor the exchanges that are attempted over it. Unapproved access by different entertainers is additionally limited and a feeling of decentralization while comprising certain hubs with an ad libbed authority is accomplished. This examination shown that it would be profoundly far-fetched to totally shroud all data and keep an open and interoperable framework, however by utilizing smart contracts to isolate data, the proposed system actually offers critical security protection and information trustworthiness.

BHEEM additionally infer that total encryption of the records and keeping up with convenience can't go connected at the hip and there is a compromise that should be taken into consideration by the organization administrator. In future, they might investigate the common sense of utilizing the differential security model and attempt to build up the connection between the clamor and size of blockchain.[8]
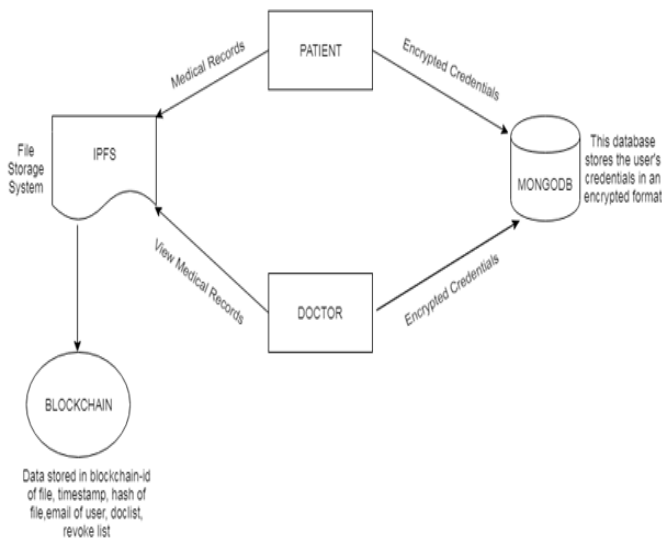
4. PROPOSED SYSTEM

a. System Architecture

Fig.1 System Architecture

Healthcare focuses on developing deep mutual trust between the doctor and the patient over sharing the Medical Records Digitally using Blockchain Technology**.**

The patient medical reports are stored in IPFS and the ID Hash Timestamp and Description generated of the file are stored in BigchainDB Blockchain Network. The database is used only to save the user information for the security of the cryptographic keys.

A transfer transaction will take place when the patient will give access, revoke access and when the doctor gives the prescription.

E-Healthcare consists of two modules:

1) Patient:

After the patient successfully logs in, the credentials (username/password) entered by the patient are stored in MongoDB. For security, after sign up a 2-Step Verification (OTP) will be sent on patient's entered Email Address. The patient will enter its personal medical details and upload the medical record which can consist of reports, images, pdfs, etc. The file uploaded will be stored in IPFS but the ID, Hash, Timestamp and Auto description generated will be stored in Blockchain BigchainDB. A doctors list will be available for the patient and based on the requirement the patient can choose one doctor and give access of its medical record to the doctor and hence a transfer transaction will take place. The file's encrypted hash will be stored in BigchainDB and decrypted view in IPFS. If a patient has previous medical history/records then it can view and

upload it if required. The patient has the flexibility to upload individual as well as multiple records at the same time.   The patient can then view the prescription uploaded by the doctor which will be stored in. Once the treatment is done, the patient will revoke access of the medical records and the record from the doctors list will enter into the revoke list in BigchainDB.

2) Doctor:

Once the doctor successfully logs in, a medical record list of access granted by the patient will be available for the doctor from which the doctor will select an individual patient record. Using the speech to text feature the doctor will give the prescription which will be encrypted and stored in BigchainDB and then a transfer transaction will take place. Before giving the prescription, the doctor can view patient profile details as well. If there is an emergency the doctor will send the mail to the patient's email ID and then the patient will get a mail along with an emergency give access of medical records page.

3) SHA-256

SHA-256 represents Secure Hash Algorithm – 256 bit and is a sort of hash work normally utilized in Blockchain. A hash work is a sort of numerical capacity which transforms information into a unique finger impression of that information called a hash. It resembles an equation or calculation which takes the info information and transforms it into a yield of a fixed length, which addresses the unique finger impression of the information. The info information can in a real sense be any information, regardless of whether it's the whole Encyclopedia Britannica, or simply the number '1'. A hash capacity will give a similar hash for a similar info in every case regardless of when, where and how you run the calculation. Similarly strangely, assuming even one person in the information text or information is changed, the yield hash will change. SHA-256 works in the way of MD4, MD5, and SHA-1: The message to be hashed is initial (1) cushioned with its length so that the outcome is a different of 512 pieces in length, and afterward (2) parsed into 512-cycle message blocks $M(1)$; $M(2)$;::::;M(N) . The message blocks are handled each in turn: Beginning with a fixed starting hash esteem H (0), consecutively figure $H(i) = H(i1) + CM(i) (H(i1))$; where C is the SHA-256 pressure work and + implies word-wise mod 232 expansion. H(N) is the hash of M.Figures and Tables.

B. Flowchart:

Flowchart of Data at Patient Side.

Once, the patient visits the Healthchain web application and either sign in or sign up if not visited earlier. After the whole sign in process, the patient has to go through

the two-step verification and enter the OTP he/she received on their email id. Then once the process is done, he or she can upload their medical reports in the form of pdf or image. Or simply view their past medical history if already they are using Healthchain. Patients can check the available Doctor's list for their treatment. Once that particular doctor is selected, patient can transfer single or multiple medical records to doctors for their opinions and prescriptions. During the treatment if the doctor sends the prescription via Healthchain to the patient's side, he/she can easily view the prescription and take the needed medication. As Healthchain is a patient centric healthcare application, the patient is completely in charge of his/her medical records and can revoke access from the doctor whenever, he feels the need to do so.

Healthchain application, he has to create his profile by entering all this educational and professional details.

Once the Doctor logs into his profile, he will see a list of patients that are interested in his treatment and have given access of their medical records to him. Here comes the Speech to text feature for prescribing the medications and giving treatment related opinion to the patient. The doctor can see his patient's profile and have access or his medical reports and even download them if required for the treatment procedure. We also have included a special feature that is the emergency feature. This feature comes in action when the doctor feels like there is an emergency for his ex patient and needs to have access over his medical record, he will then send an emergency to the patient's relative or whosoever concerned. A mail will be sent to that person asking him to grant access of the medical records to the doctor.
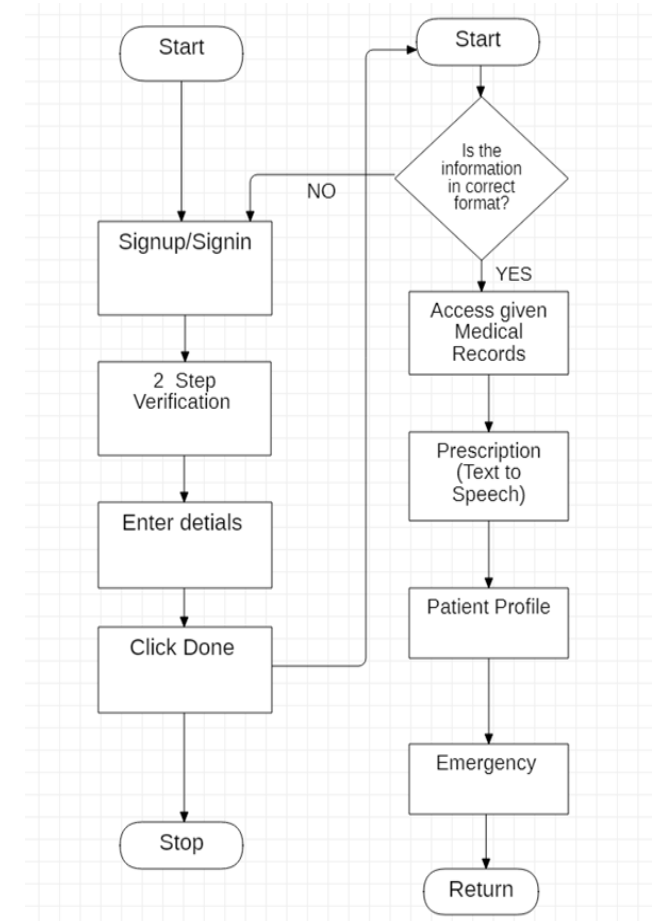

Fig. 2 Flowchart (Patient Side)

Flowchart of Data at Doctor Side:

Once, the doctor visits the Healthchain web application and either sign in or sign up if not visited earlier. After the whole sign in process, the patient has to go through the two-step verification and enter the OTP he/she received on their email id. If a new Doctor visits the

Fig. 3 Flowchart (Doctor's Side)

C. Use Case Diagram

Graphical view of how the patient uses Healthchain from their side.
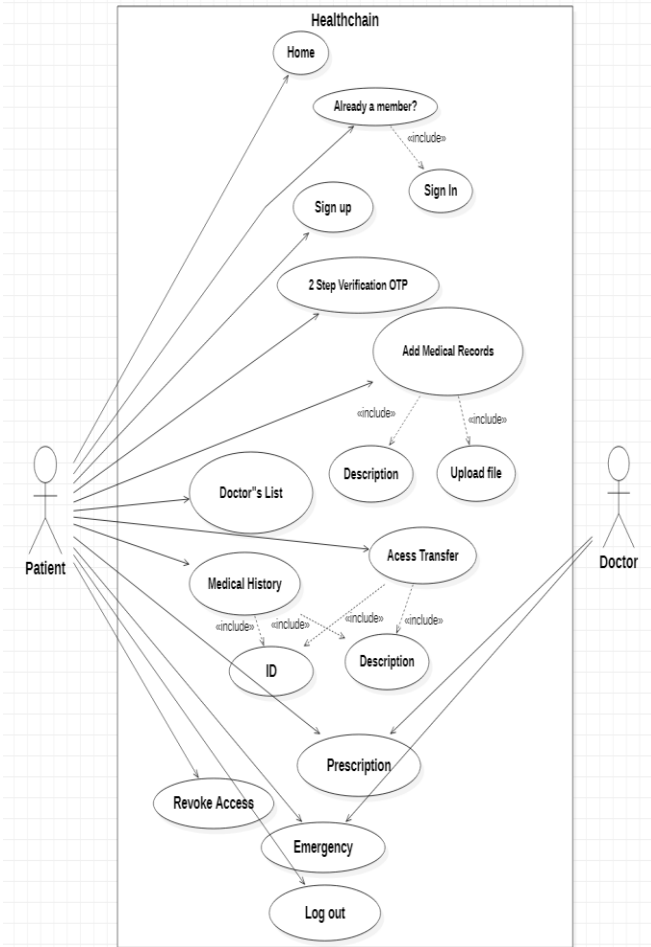
Fig 4. Use Case Diagram (Patient Side)

Fig 5. Use Case Diagram (Doctor's Side)

PATIENT'S SIDE

- First the user needs to signup/login on our platform.

- On login, user can upload their medical records on our platform.

- User will have various options like to find doctors on the platform or to view their medical record.

- Users can also give/revoke access of their medical records from/to a doctor.

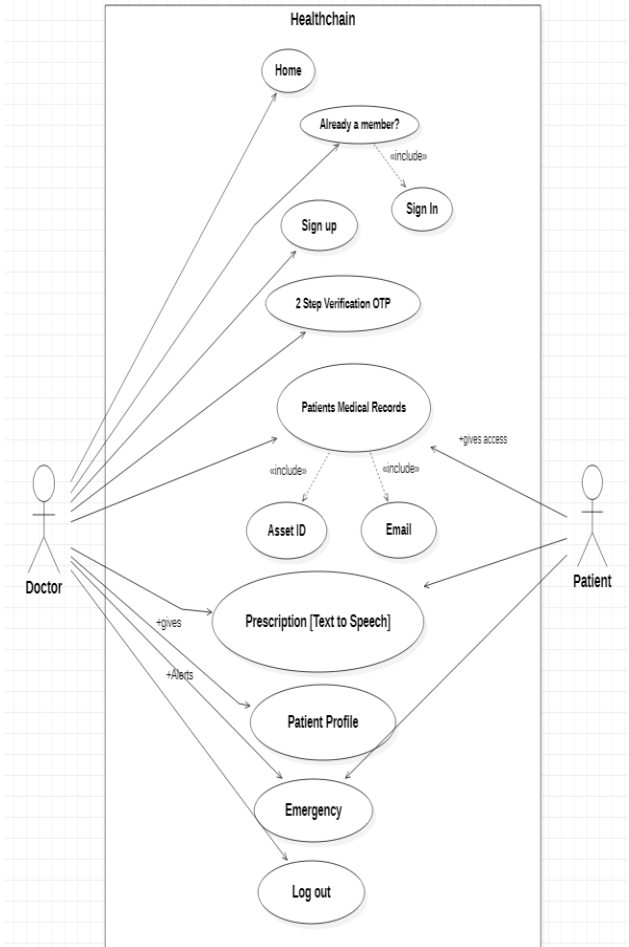- User can then view the prescriptions provided to them by the doctors.

DOCTOR'S SIDE

- First the user needs to login/signup on our platform.

- On login, doctors can see the patient's medical records and their history.

- Doctor can then send prescription (also use speech to text feature for simplicity purpose) to patients.

- In case of any emergency like accident, doctor can raise an emergency option which is present on our platform and the permission for accessing the medical history of patient will be sent to the patient's family members.
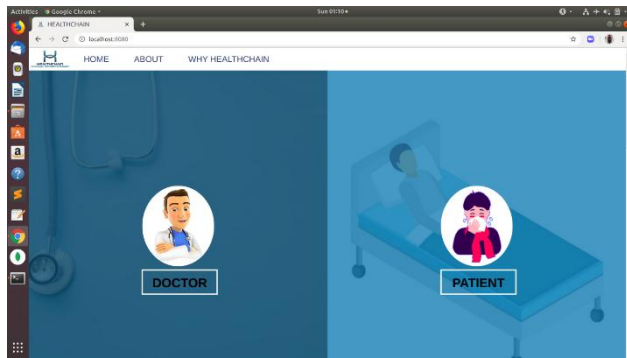
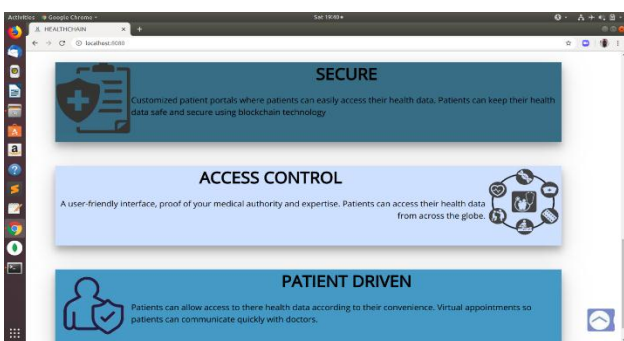**D. Screenshots:**

Fig 6.. Home Screen (Upper Part)
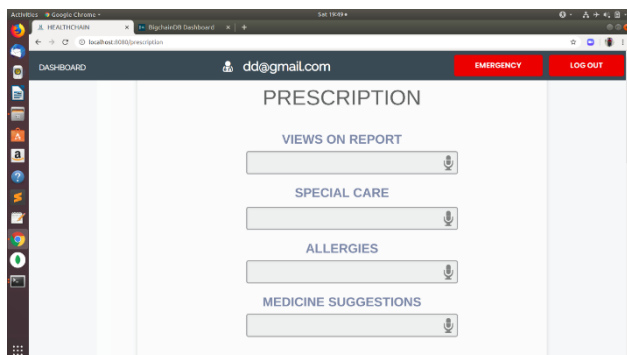

Fig 7. Home Screen (Lower part)

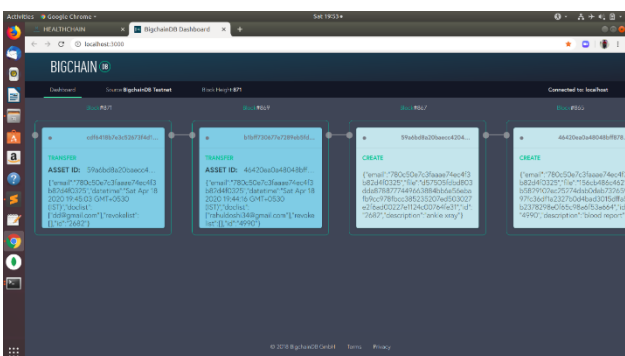Fig 8. Speech to text feature at the doctor's side for presciption.

Fig 9. BigchainDB (Medical Records Stored and access transfer details)
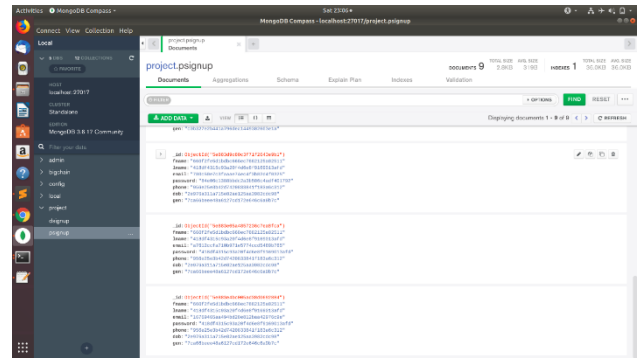

Fig 10. MongoDB (Local data)

5. SYSTEM REQUIREMENTS

H/W system configuration:

The project has been developed on HP Pavilion 15-cc19tx laptop. The laptop has the following specifications: -

1. Intel Core i5 5th generation processor @1.60GHz 1.80Ghz

2. 8GB RAM

Linux Operating System has been used with a version.

• RAM: 2GB+

• Secondary Memory: 1 GB+

• PC or Laptop with 2GHz+ or higher processor clock speed recommended (single or dual processor system)

• 1+ GB Graphic Card (1.40GHz Graphics Processor)

• 800x600 Resolution Display for Monitor.

S/W system configuration:

1. BigchainDB

2. Node.js

3. MongoDB

4. Express

5. NPM

6. IPFS

VI. CONCLUSION

The Paper Purposes An Electronic Health Record System Based On Blockchain Which Allows Users To Remotely And Securely Store Important Medical Records And Access It Anytime And Anywhere. Blockchain Helps Us To Achieve Scalability And Access Control In The Field Of Medical Records. The patient can permit or revoke access from the particular doctor anytime. This is how

we have aimed to keep the patient as the center of our application. Using healthchain the patient can easily find a specialist, take consultation and prescriptions there and there. Get second advice from other doctors as well. Lastly the emergency feature that we have incorporated can be considered as a game changer in the field of healthcare. Scope Of Electronic Health Record Includes Using Machine Learning Algorithms To Get A Quick Overview Of Patient's Medical History And Also Using Ai At The Doctor's End To Suggest Medicines And Precautions.

REFERENCES

1]Trent McConaghy, Rodolphe Marques, Andreas M¨uller, Dimitri De Jonghe, T. Troy McConaghy, Greg McMullen, Ryan Henderson, Sylvain Bellemare,and Alberto Granzotto, "BigchainDB: A Scalable Blockchain Database",Whitepaper ,2016, [Online] Available:https://git.berlin/bigchaindb/site/raw/commit/b2d98401b65175f0fe0c169932ddca0b98a456a6/_src/whitepaper/bigchaindb-whitepaper.pdf

2] Randhir Kumar, Rakesh Tripathi, Implementation of Distributed File Storage and "Access Framework using IPFS and Blockchain", 2019 Fifth International Conference on Image Information Processing (ICIIP)

3] Yunhua Gu1,Xing Wang,Shu Shen,Jin Wang,Jeong-Uk Kim, "Analysis of Data Storage Mechanism in NoSQL Database MongoDB", 2015 International Conference on Consumer Electronics-Taiwan (ICCE-TW), pp. 70-71

4] Li Liang,Ligu Zhu, Wenqian Shang,Dongyu Feng, Zida Xiao, "Express Supervision System Based on NodeJS and MongoDB ", CIS 2017, May 24-26, Wuhan, China, pp-607-608

5]Mohammad Dabbagh(Member, IEEE), Mehdi Sookhak(Member, IEEE), Nader Sohrabi Safa "The Evolution of Blockchain: A Bibliometric Study", 2019, pp-19212

6] Asaph Azaria, Ariel Ekblaw, Thiago Vieira and Andrew Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management", 2016, 2nd International Conference on Open and Big Data, pp.25-26

7]Qi Xia, Emmanuel Boateng Sifah, Kwame Omono Asamoah, Jianbin Gao, Xiaojiang Du, Mohsen Guizani, "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain", 2017, pp.1-7

8] Jayneel Vora, Anand Nayyar, Sudeep Tanwar, Sudhanshu Tyagi, Neeraj Kumar, M. S. Obaidat.,"BHEEM: A Blockchain-based Framework for Securing Electronic Health Records", 2018