IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 6, June 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006092 |

Electronic Health Record using Blockchain Technology

Prof.Raghu B R [1], Manasa K R[2], Meghana M N[3], Likhith P[4], Nachiketh M P[5]

Assistant Professor, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davanagere, Karnataka, India[1]

B.E Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davanagere, Karnataka, India[2]

B.E Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davanagere, Karnataka, India[3]

B.E Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davanagere, Karnataka, India[4]

B.E Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davanagere, Karnataka, India[5]

ABSTRACT: Institutions manage health records (HRs) rather than patients, which makes it difficult to get medical advice from multiple hospitals. It is imperative that patients regain control of their medical records and concentrate on the intricacies of their own treatment. Since blockchain technology is rapidly evolving, it is helping to advance public health by facilitating electronic storage of medical records and other patient data. This system gives patients full, unchangeable records and free access to HRs without service providers or treatment locations being involved. In this project, we make an attribute-based signature method with multiple authorities. A patient can support a message based on an attribute without giving any other information than the fact that he has signed it. To avoid the escrow problem and stick to the distributed data storage model of the blockchain, the patient's public and private keys are not made and given out by a single, trusted authority, but by a number of authorities. This protocol protects against a collusion attack from N compromised authorities by letting them all know about the secret pseudorandom function seeds. We also show that this attribute-based signature scheme is safe in the random oracle model.

KEYWORDS: Health Records, Healthcare, Blockchain, Attribute-Based Signature Scheme.

I. INTRODUCTION

1.1 Block Chain Technology

A "block" in a "chain" of databases linked by peer-to-peer nodes is what the term "blockchain" refers to in the context of blockchain technology. This kind of data storage is often referred to as a "digital ledger."
The owner's digital signature confirms each entry in this ledger. This serves as evidence of the transaction's validity and prevents it from being altered in any way. As a result, the digital ledger's information is very secure.
The digital ledger is like an online spreadsheet that can be accessed by multiple computers on a network and is used to keep track of purchases.

It's important to note that anyone can see the information, but they can't change it.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006092 |

In the last few years, Blockchain technology has been used by many businesses all over the world. A lot of people want to know how Blockchain works. Is this a big change or just a small one? Start learning about blockchain now, because it could be a big deal in the years to come. Blockchain is a mix of three of the world's most important technologies:

- Cryptographic keys
- A peer-to-peer network containing a shared ledger
- A means of computing, to store the transactions and records of the network

There are two kinds of keys in cryptography: private and public. This kind of key helps make sure that deals between two parties go as planned. These two keys are unique to each person and are used to connect to their digital identity in a secure way. Blockchain technology will protect your identity, so you can rest easy. This is called a "digital signature" in the bitcoin world, and it is used to authorise and keep track of transactions.
In this way, peer-to-peer networks and digital signatures are linked. The digital signature, among other things, is used by a large number of persons in control of transactions. A mathematical check ensures that the two parties connected to the network can perform a secure transaction when they agree to a trade. The peer-to-peer network is used by users who utilise Blockchain to conduct various digital transactions utilising cryptographic keys.

1.2 Features of Blockchain

These are the four parts of Blockchain that we'll talk about in depth:

1. We have a public ledger that works with a hashing encryption system.
2. The hash value of each block is like its digital signature.
3. On the Blockchain network, all transactions are approved and checked using a proof-of-work consensus algorithm.
4. The miners' resources are used by the Blockchain network. The miners' job is to check transactions in exchange for rewards.

1.3 Information on EHR

Health records may be easily stored in electronic health records (EHRs) since they are easy to access. They also make it simpler for patients to access their paper-based medical records online. EHRs may be created and shared by patients with their loved ones, friends, healthcare practitioners, and other authorised data consumers using this system. As long as medical researchers and practitioners can access EHRs from anywhere in the globe, the healthcare solution transition programme should be successful. Because of life events, patients' EHRs are distributed over the country. Essentially, this implies that the EHRs are moved from one database to another. Consequently, patients' access to their own medical records may be compromised, but the service provider often retains a greater degree of control [1]. Them have limited access to electronic health records (EHRs), and these information are difficult for patients to exchange with researchers or healthcare professionals. Sharing data in a high-performance manner is difficult because of interoperability issues across various providers, hospitals, research organisations, and so on. Uncoordinated data management and sharing results in fragmented, uncoordinated health records [2]. Fig. 1 illustrates

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006092 |

the benefits to the healthcare sector of allowing patients to safely and completely control and share their EHRs, whether for research purposes or to allow healthcare professionals to exchange information. The suggested solution accomplishes its purpose of encouraging collaboration between organisations by fostering deep trust between them, thanks to the use of blockchain technology.

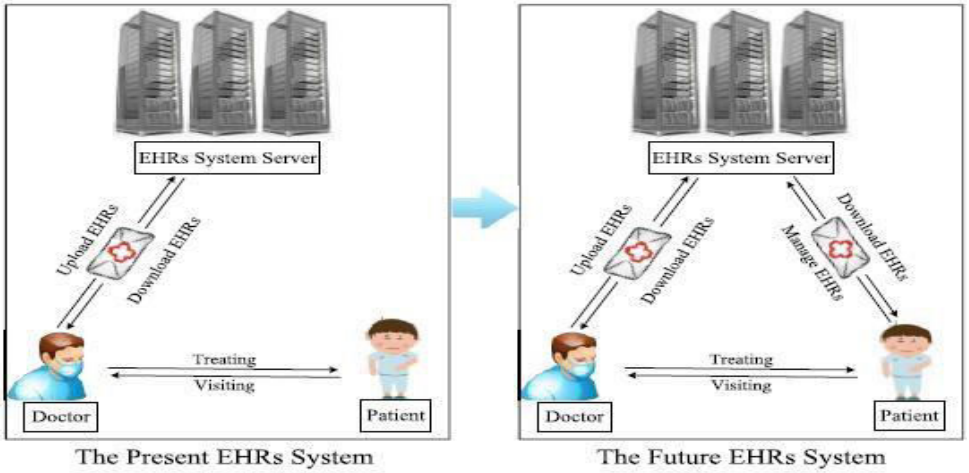

Figure 1. EHRs system in the present and future. The patient should have right to access hisEHRs for managing and sharing them independently.

Bitcoin was the first cryptocurrency to benefit from blockchain technology. When Nakamoto released the Bitcoin whitepaper in 2008, it served as an introduction to the public of the technology. This new technological revolution has been likened to steam engines or the Internet because it has had such a profound impact on society since its introduction. According to a 2015 World Economic Forum survey, 58% of participants believe that by 2025, blockchain technology will account for 10% of global GDP (GDP). [4] It used to be difficult to share large EHRs as a result of concerns about data security and the possibility of patients' confidential information being exposed. At the moment, hospitals and providers are in charge of EHRs, which means patients do not have the ability to take back ownership of their records. The blockchain of EHRs is constructed utilising blockchain technology, which sets rules for how to store data and manage identification. The audit trails of all transactions are also stored in an immutable distributed ledger using this technology. As a result, the exchange of data is conducted in a responsible and transparent manner. As a result, patients will be able to keep track of their own medical records and the results of diagnostic tests ordered by their physicians. As a result, medical errors are minimised and patient privacy is protected.

II. LITERATURE SURVEY

Data is stored in the cloud using cryptography-based access control, and attribute encryption is used to keep data safe and private. With PKE-based methods, it's common to encrypt a file with multiple user keys from different sets to limit access in small steps. The authors [1] look at five ways that blockchain technology could help make this change happen: (1) the rules of digital access; (2) the gathering of information; (3) the ease of finding new information; (4) the identification of patients; and (5) the fact that knowledge can't be changed. When we talk about block chain-enabled patient-driven capacity, we tend to talk about the number of clinical information transactions, privacy and safety, patient engagement and motivation, and the number of clinical information transactions. With these things in mind, we come to the conclusion that, even if patient-driven capacity is linked to a positive trend in treatment, it is important to find out how the block chain could help the transfer of information from hospital-centered to patient-centered.

[2] “Improving the interoperability of healthcare information system through HL7 CDA and CCD standards”

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006092 |

It is crucial to physicians in a certain manner to use the EHR (EHR). On the other hand, physicians are aware that they are unable to provide appropriate therapy. Modern EHR systems, on the other hand, are clunky, cumbersome, and slow clinicians down. Despite the benefits and drawbacks of electronic health records (EHRs), a list of how they handle issues may be found. The architecture that powers bit coin's crypto currency, the block chain, may hold the key to a solution.

[3] ”Blockchain Enabled Secure Electronic Health Records System Storage with Attribute

Based Signature Scheme” Journal in IJRASET Volume 7 Issue V, May 2019

Block chain EHRs are protected by a system where patients may approve messages based on an attribute, but they don't have to divulge any additional information beyond the fact that they've looked at them. Multiple authorities would be involved in this process. In addition, there are several authorities, but no one can be trusted to create and disseminate the patient's public and private keys. There is no need for escrow in this case, since data is stored on the blockchain. By allowing them to swap the seeds of the secret pseudorandom feature, this technique guards against collusion assaults from N 1's compromised authority. To demonstrate that an attribute-based signature system is secure in a randomised oracle system, we often utilise formal proofs to demonstrate that the theoretical bili ear Diffie-Hellman can be used. Using the suggested approach and other methods described in earlier research, the study demonstrates that they both work and have the same qualities as each other.

[4] “Privacy-preserving personal health record system using attribute based encryption” by

Master’s thesis, Worcester polytechnic institute 2011

Nowadays, practically all of the data on the cloud is stored and moved by storage providers, who are well-known and well-respected. The lack of data, high operational expenses, and lack of data security are only a few of the drawbacks of this system. This article explains how to utilise blockchain technology to create a secure, distributed data space for a keyword search engine. When a user uploads encrypted data, it will be encrypted before it is sent to cloud nodes and protected by cryptography. In this way, the individual who owns the data may provide others access to it. In the end, it will be able to search for a secret keyword in encrypted data sets.

III. EXISTING SYSTEM

These electronic health records (EHRs) may be accessed from anywhere in the globe by health care researchers and service providers. Health care transition programmes are meant to function like this. Life events, on the other hand, are causing patients to disperse their electronic health records in several locations. Essentially, this implies that the EHRs are moved from one database to another. Consequently, a person with access to their own health information may find themselves without it, although providers often retain it. Patients have relatively limited access to EHRs, and they can't readily share their data with researchers or healthcare practitioners.

Problem Statement

Health care professionals and patients alike would benefit from standardising issue lists in order to make it simpler for them to exchange information. Paper-based structures have no place in today's computerised environment.

Proposed Solution

The system's primary components are the Administrator and the User. There are two more groups of people who would use our proposed framework: physicians and patients. A member of the administrative staff of the hospital who is in charge of the system gives these users their jobs. The administrator is in charge of setting up access for the system's two main users, the doctor and the patient. So, the first thing the administrator would do is give out

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006092 |

responsibilities. This would have the User's Account Address and Role Name. Every person who used this system would get a role name and an account address. So, when an administrator gives a user a role, the name of the role and the user's account address are written down in a list called "roles." This step is taken so that validation can be done in later steps.

After the roles have been set up, if a user wants to do something on the proposed system, he must first ask for permission. The system would compare the user's role name and account address to the Roles List. If validation is successful, the user would have access to those services. After the functions are done, the system would send the data to the Ethereum Blockchain. The Ethereum Blockchain would then use the data to make transactions. The blockchain layer tells the system that the transaction was successful once it has been checked. This message can be seen by users on the DApp browser, which shows the whole proposed framework.

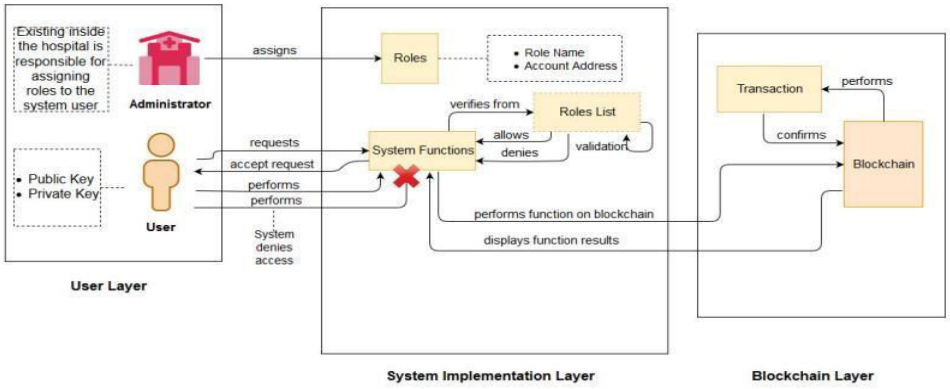

Fig.2 Dapp Architecture

IV. METHODOLOGY

The suggested framework or system consists of three components or modules, as seen in the image. When combined, these components would maintain our system operational. Concerning these things or modules, further concepts must be comprehended. The details are provided below. Users of the proposed framework may include patients, physicians, office personnel, and nurses. They were granted varying degrees of access to the system because they deserved varying degrees of control over it.

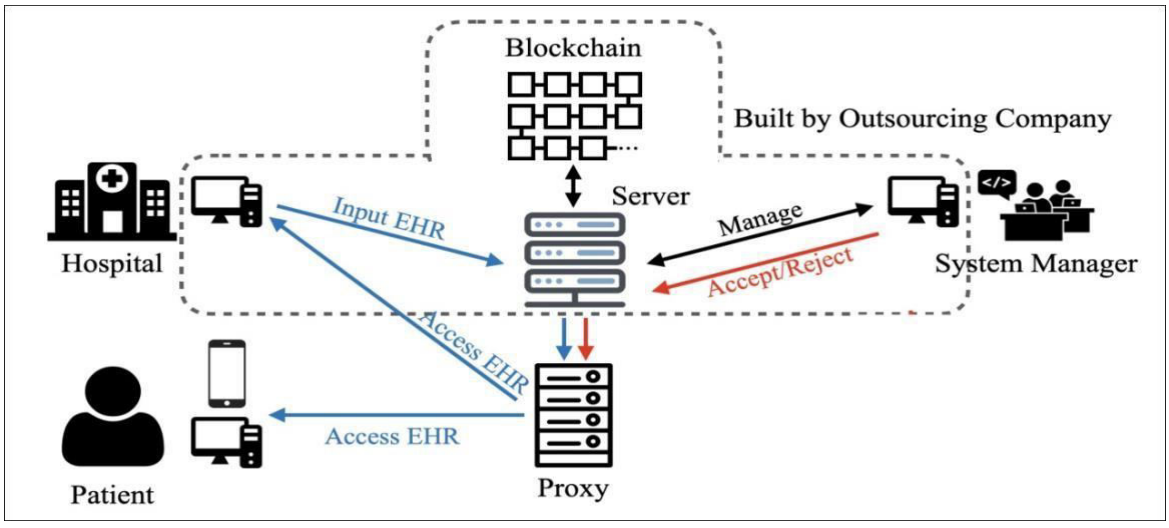

Fig .3: Phases of Project

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006092 |

1. User Layer

A person who uses a system and all of its resources well is called a user. Because a user has many roles and abilities on the system, the system can figure out who he is.

This system can be used by patients, doctors, office staff, and many other people. The main job of these users would be to communicate with the system and do basic things like create, read, update, and delete medical records. Users of this system would use a web browser to get to the system's features. Technically, this browser is called a DApp browser because it has the Graphical User Interface (GUI) of the DApp, which is our proposed system framework. All of the functions that a user can access are in the GUI. Depending on where the user is in the system, this GUI could be used to talk to the blockchain layer or the other system layer.

2. Blockchain Layer

The blockchain layer comes next in the system. This layer has the code or mechanism for how a user interacts with a blockchain-based DApp. This layer is made up of three different parts. They're:

- **Blockchain Assets:**A transaction is how a record or piece of information on the Ethereum blockchain network can be changed by a user from outside the network. The Ethereum blockchain sees these transactions as assets because they are pieces of information that users can give to each other or just store for later use.
- **Governance Rules:**Blockchain technology is based on a set of rules that everyone agrees on. These rules say how transactions are handled and how the totals are made. To do this, the blockchain needs ways to make sure it is secure and can't be changed. Proof of Work (PoW) is the way that Ethereum's blockchain comes to a decision. To make sure that the blockchain is run in a trustworthy way, all of the trusted nodes that are part of the blockchain network must agree on something.
- **Network:**The Ethereum blockchain uses the peer-to-peer network. In this network, each node is linked to every other node as a peer. Without a central node that controls everything and acts as the hub of the network. The network was used because the goal was to build a decentralised platform instead of a centralised one. So, the best thing this technology could have done is use a network where all connected nodes have the same status and rights.

Transaction

The system includes following transactions:

- When documents are added to the DApp, it will have a patient's medical records. It has the fields ID, name, co-morbid, blood group, and IPFS hash. The patient's basic medical records are kept with the IPFS hash that links to the patient's test results or other medical records file.
- The patient's medical records would be altered if records were altered. This cannot alter the IPFS hash, but it may modify the patient's fundamental information. IPFS hash cannot be altered, hence records are secure.
- View records would allow the user to view the stored medical records of a patient in DApp. Both physicians and patients use the "view records" feature. Before allowing a patient to see his own medical data, the system confirms the patient's identity. Therefore, the system utilises the patient's public account address to ensure that only relevant medical data are shown.
- This option would allow the user to erase any patient's record. Doctors are the users in this scenario, and they have the ability to erase any blockchain-stored patient information.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006092 |

• Allow access. Each of the aforementioned transactions should be restricted to certain users. For instance, only the physician or nursing staff may modify or add to a patient's medical records. Therefore, only these entities could add or modify records.

The patient may also see his medical records, but he cannot make any changes to them.

V. EXPERIMENTAL RESULTS

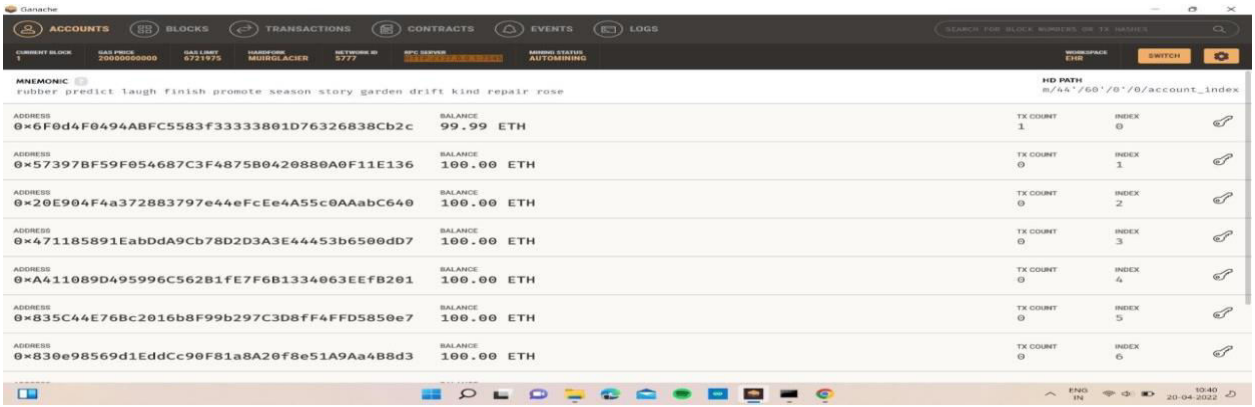

Fig: Ethereum wallet in ganache workspace

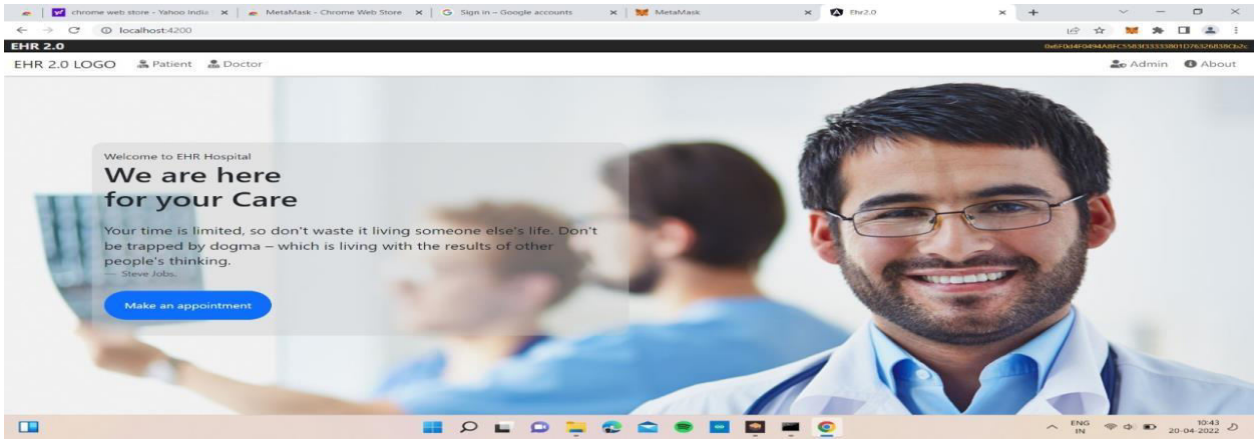

Fig: EHR homepage

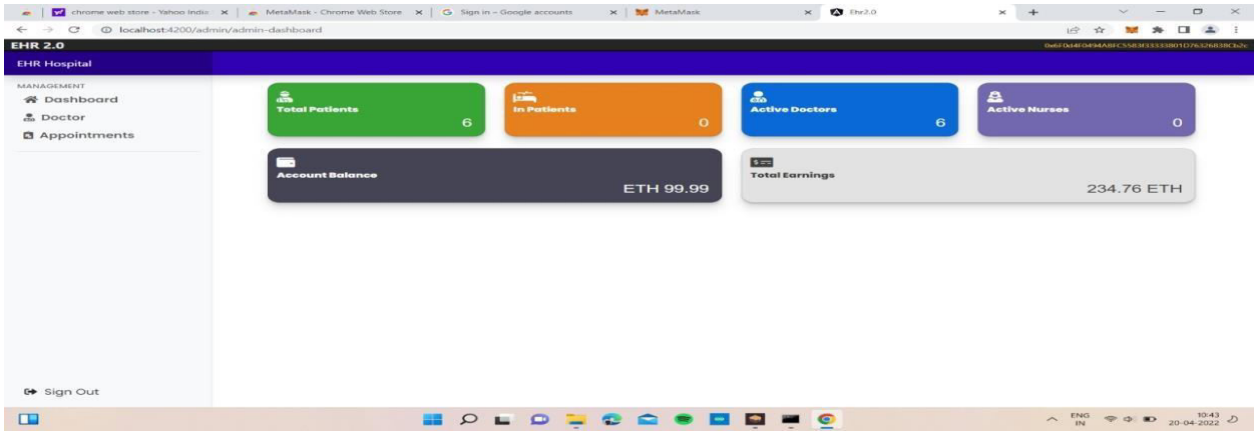

Fig: Admin Dashboard

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006092 |

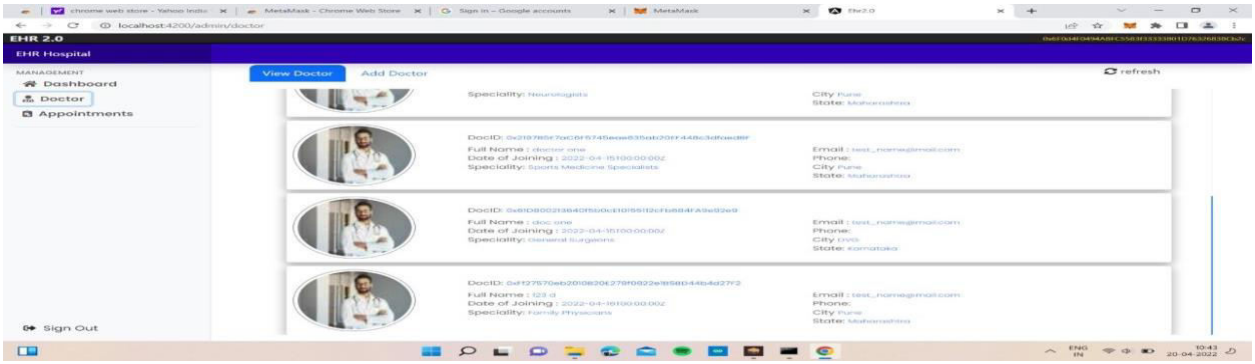

Fig: List of registered doctors

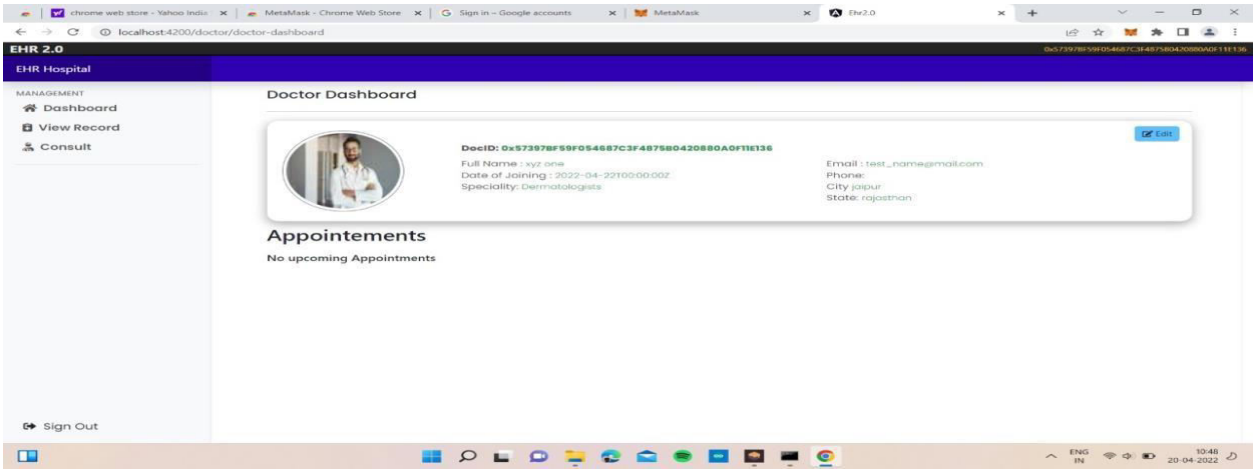

Fig: Doctor Dashboard

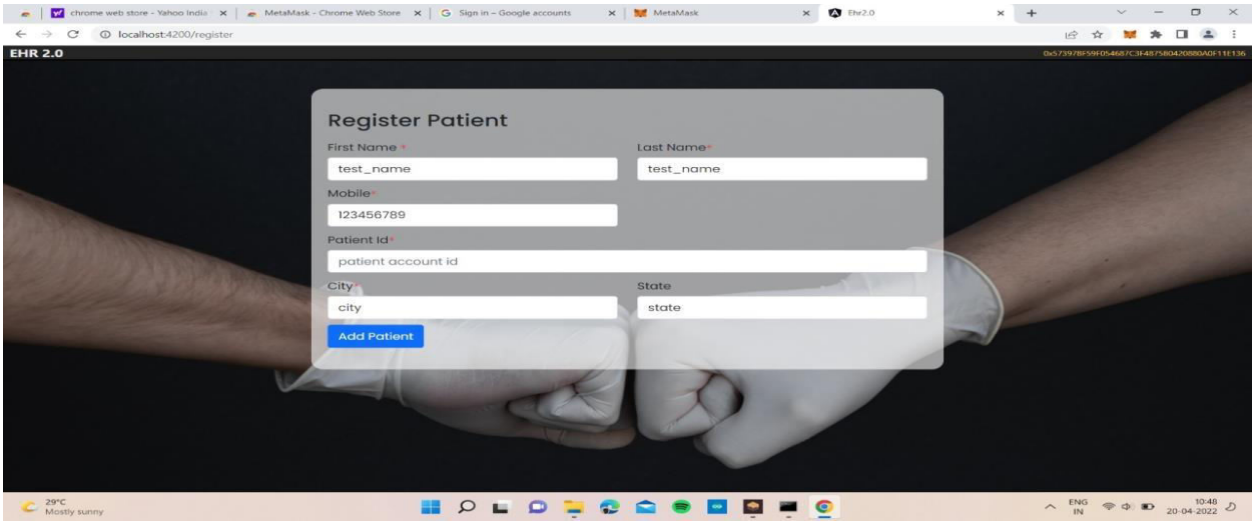

Fig: Patient registration

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006092 |

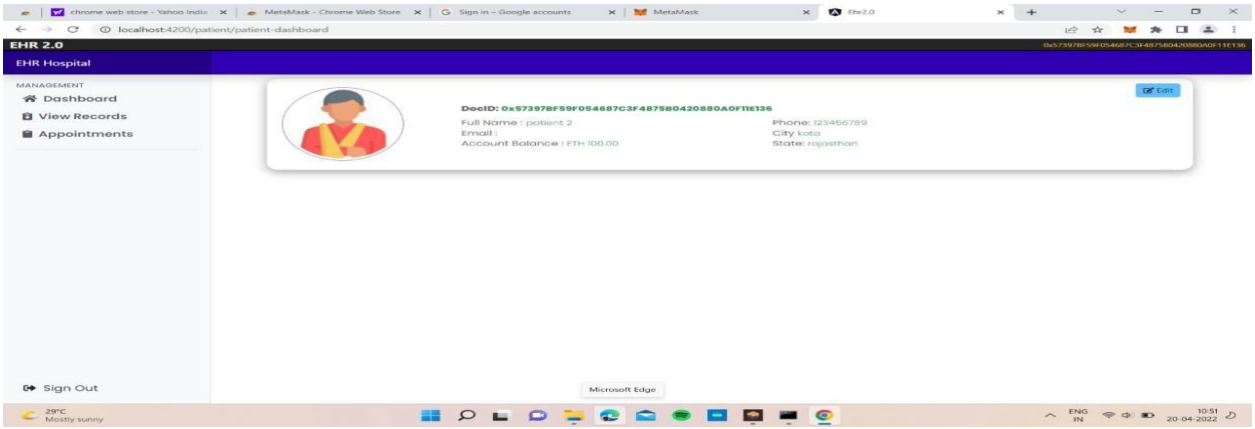

Fig: Patient Dashboard

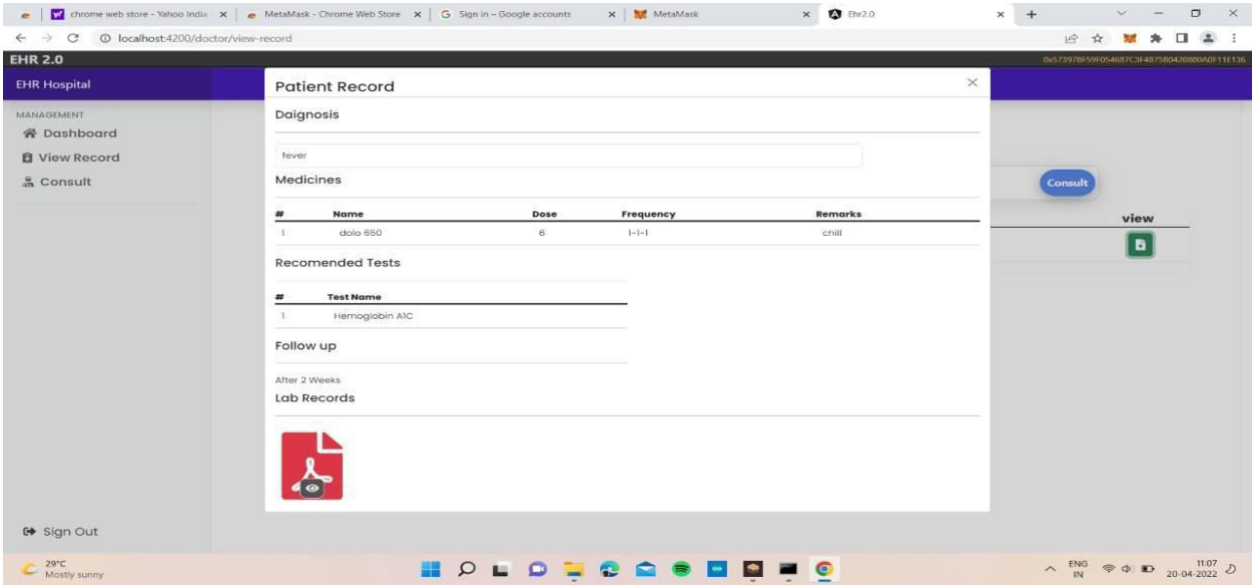

Fig: Patient record details

VI. CONCLUSION

From this, we can see how blockchain technology can help the healthcare industry and how it can be used for electronic health records. Even though the healthcare industry has grown and EHR systems have become more advanced, they still had some problems that this new technology, blockchain, fixed. Our proposed framework includes both a safe place to keep records and clear rules about who can see them. It makes a system that is easier for people to use and understand. Also, since the system uses IPFS's off-chain storage system, the framework suggests ways to make sure that the system solves the problem of where to store data. Role-based access is also good for the system because it makes sure that only trusted and related people can look at medical records. This also fixes the problem of the EHR system not having enough information for everyone. We hope to add the payment module to the framework we already have in the future. For this, we need to think about a few things, such as how much a patient would pay for a doctor's advice on this blockchain-based, decentralised system. We would also have to make policies and rules that meet the standards of the healthcare industry.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006092 |

REFERENCES

[1] Ming Li, Shucheng Yu, and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute based Encryption", IEEE Transactions on Parallel and Distributed Systems 2012.

[2] IEEE 2012 paper on "Improving the interoperability of healthcare information system through HL7 CDA and CCD standards".

[3] Madhusree N, kavitha G paper on "Blockchain Enabled Secure Electronic Health Records System Storage with Attribute-Based Signature Scheme" Journal in IJRASET Volume 7 Issue V, May 2019

[4]]"Privacy-preserving personal health record system using attribute based encryption, " Master's thesis, worcester polytechnic institute, 2011.

[5] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted personal health records in cloud computing," in ICDCS '11, Jun. 2011.

[6] Tatsuaki Okamoto, Katsuyuki Takashima, " Efficient Attribute-Based Signatures for NonMonotone Predicates in the Standard Model in " IEEE CLOUD COMPUTING, VOL. 2, OCTOBER-DECEMBER 2014

[7] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings, " in SecureComm'10, Sept. 2010, pp. 89– 106.

[8] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing, " in IEEE INFOCOM'10, 2010

[9] André Henrique Mayer, Cristiano André da Costa, Rodrigo da Rosa Righi," Electronichealth records in a Blockchain: A systematic review" Health Informatics Journal1–16, 2019

[10] Neha Agarwal, Shashikala Tapaswi," A Trustworthy Agent-Based Encrypted Access Control Method for Mobile Cloud Computing Environment" in Journal Pervasive and mobile computing, 2018.

[11] S. Narayan, M. Gagn´e, and R. Safavi-Naini, "Privacy preserving phr system using attributebased infrastructure, " ser. CCSW '10, 2010, pp. 47–52.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details