JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

BLOCKCHAIN BASED MEDICAL HEALTH RECORDSHARING APPLICATION

V. Punitha[1], Gokulakrishnan N[2],Ragavan R[2],Sudersan S[2],Vinoth Kumar M[2]

[1] Professor, Department of Information Technology, Saranathan College of Engineering, Trichy, India.
E-mail: punitha-it@saranathan.ac.in
[2]Department of Information Technology, Saranathan College of Engineering, Trichy, India.E-Mail:ragavankesavan2000@gmail.com[2]

Abstract: *Blockchain have been an interesting research area for a long time and the benefits it provides havebeen used by a number of various industries. Similarly, the healthcare sector stands to benefit immensely from the blockchain technology due to security, privacy, confidentiality and decentralization. Nevertheless, the Electronic Health Record (EHR) systems face problems regarding data security, integrity and management. In this paper, we discuss how the blockchain technology can be used to transform the EHR systems and could be a solution of these issues. We present a framework that could be used for the implementation of blockchain technology in healthcare sector for EHR. The aim of our proposed framework is firstly to implement blockchain technology for EHR and secondly to provide secure storage of electronic records by defining granular access rules for the users of the proposed framework. Moreover, this framework also discusses the scalability problem faced by the blockchain technology in general via use of off-chainstorage of the records. This framework provides the EHR system with the benefits of having a scalable, secure and integral blockchain-based solution.*

Keywords: Blockchain technology, Health records, Electronic health records, Decentralization, and scalability.

I. INTRODUCTION

The recent advent in technology is affecting all parts ofhuman life and is changing the way we use and perceivethings previously. Just like the changes technology hasoffered in various other sectors of life, it is also findingnew ways for improvement in healthcare sector. The main benefits that advancement in technology is offering are to improve security, user experience and other aspects of healthcare sector. These benefits wereoffered by Electronic Health Record (EHR) and Electronic Medical Record (EMR) systems. However, they still face some issues regarding the security of medical records, user ownership of data, data integrity etc. The solution to these issues could be the use of a novel technology, i.e., Blockchain. This technology offers to provide a secure, temper-proof platform for storing medical records and other healthcare related information.

Before the advent of modern technology, healthcare sector used paper based system to store the medical records, i.e., using handwritten mechanism. This paper-based medical record system was inefficient, insecure, unorganized and was not temper-proof. It also faced theissue of data- duplication and redundancy as all the institutions that patient visited had various copies of patient's medical records.

The healthcare sector faced a trend shift towards EHR systems that were designed to combine paper-based andelectronic medical records (EMR). These systems wereused to store clinical notes and laboratory results in its multiple components [1]. They were proposed to enhance the safety aspect of the patients by preventingerrors and increasing information access [2]. The goal of EHR systems was to solve the problems faced by thepaper-based healthcare records and to provide an efficient system that would transform the state of healthcare sector [3].

The EHR systems have been implemented in a numberof hospitals around the world due the benefits it provides, mainly the improvement in security and its cost-effectiveness. They are considered a vital part of healthcare

sector as it provides much functionality to the healthcare [4]. These functionalities are electronic storage of medical records, patients' appointment management, billing and accounts, and lab tests. They are available in many of the EHR system being used inthe healthcare sector. The basic focus is to provide secure, temper-proof, and shareable medical records across different platforms. Despite the fact that notion behind usage of EHR systems in the hospitals or healthcare was to improve the and didn't meet theexpectations associated with them [3]. A study was conducted in Finland to find the experiences of nursingstaff with the EHR, it was concluded that EHR systemsfaced the problems related to them being unreliable andhaving a poor state of user-friendliness [5]. The EHR system also faces some other problems which are as follows:

A. Interoperability

It is the way for different information systems to exchange information between them. The information should be exchangeable and must be usable for furtherpurposes. An important aspect of HER systems is itsHealth Information Exchange (HIE) or in general data sharing aspect. With a number of EHR systems being deployed in various hospitals they have a varying levelof terminologies, technical and functional capabilities which makes it to have no universally defined standard[6]. Moreover, at technical level the medical records being exchanged should be interpretable, and that interpreted piece of information could be further used [6].

B. Information Asymmetry

Today the greatest problem in healthcare sector definedby the critics is information asymmetry which refers toone party having better access to information than the other party. In case of EHR systems, or in general healthcare sector is suffering from this problem asdoctors or hospitals have access to the patient's records,thus making it central. If a patient wants to access his medical records he would have to follow a long and tedious process to access them. The information is centralized to only a single healthcare organization andits control is only provided to the hospitals or organizations.

C. Data Breaches

Data breaches in healthcare sector also calls for theneed of a better platform. A study [7] was done for analyzing the data breaches in EHR systems and itdepicted that 173 million data entries have been compromised in these systems since October 2009.Another study conducted by Argaw et al. [8], explainsthat hospitals have become a target of cyber-attacks andan increasing trend has been witnessed by theresearchers while conducting this study that a lot ofresearch work has been done in this domain [9]–[11]. Moreover, many EHR systems are not designed tofulfill the needs and requirements of the patients andface the issues related to inefficiency and pooradaptation of these systems [12]. The literature alsosuggests that use of EHRs have introduced negativeconsequences to information processing [2]. Theseproblems make it reasonable to find a platform thatwould be helpful in transforming healthcare sector tobe patient-centered, i.e., Blockchain. A platform whichis secure, transparent and it also provides data integrityto the medical records of the patients.

This paper proposes a framework that creates such a decentralized platform that would store patient's medical records and give access of those records to providers or concerned individuals, i.e., patient. We also intend to solve the scalability problem of blockchain, as it is not in the design of blockchain to store huge volumes of data on it. So, we would use off-chain scaling method that makes use of the underlying medium to solve the scalability problem by storing thedata on that medium. Moreover, our proposed work is intending to solve the above mentioned information asymmetry and data breaches problem faced by the EHR system.

This paper is organized as follows the section II of thispaper summarizes the basics of blockchain technologyand its dependencies; section III narrates the related work done in this domain. The section IV explains the design and architecture of the proposed framework andsection V explains the performance of this framework.The last section provides the conclusion and references.

II. BLOCKCHAIN TECHNOLOGY AND ITS DEPENDENCIES This technology was introduced by Nakamoto [13], for his popular work of digital currencyor crypto-currency, i.e., bitcoin. Nakamoto used blockchain technology to solve the double spending problem of bitcoin but soon this novel technology wasbeing used in many other applications.

Blockchain is a chain of blocks that are connected together and are continuously growing by storing transactions on the blocks. This platform uses a decentralized approach that allows the information to be distributed and that each piece of distributed information or commonly known as data have shared ownership. Blockchains holds batches of transactions that are hashed thus providing them security and they are managed by peer-to-peer networks. A blockchain has certain benefits such as security, anonymity, and integrity of data with no third party intervention.

These benefits make it a reasonable choice to store patient's medical records on it, because the innovation of technology in the healthcare industry has made the security of patient's medical data a top priority. A number of researchers have also identified that using blockchain technology in healthcare would be a feasible solution [14]–[16].

A. Architecture

To understand the blockchain architecture let us use thefollowing figure 1 that explains the whole process of a transaction being send from a user on the blockchain network.

1. A new transaction being sent by a user on the blockchain network suggests that a new block is created. A block in the blockchain is used for keeping transactions in them and these blocks aredistributed to all of the connected nodes in the network. That transaction placed inside a block isbroadcasted to all of the nodes in the network. Allthe nodes in the network have a copy of thecomplete blockchain that helps them in verification process. When a block containing theuser transaction is broadcasted to all of the connected nodes, they verify that the block is nottampered by any means. If this verification resultsin success then the nodes add that block in their own copy of blockchain.

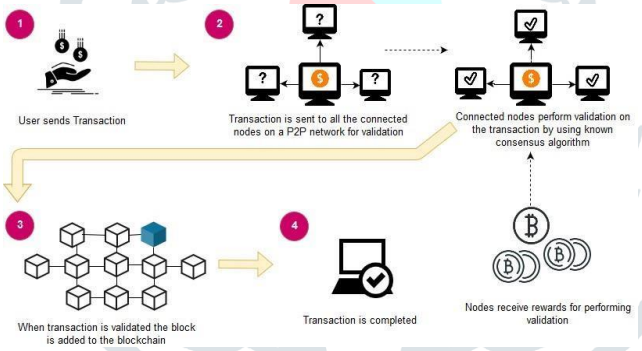


FIGURE 1. An overview of blockchain architecture.

2. This whole process of the block being added on the blockchain is done by the nodes reaching upona consensus where they decide which blocks are valid to be added on the blockchain and which arenot. This validation is performed by the connected nodes using some known algorithms toverify the transaction and to ensure that sender isan authenticated part of the network. When a nodesucceeds in performing the validation that node is rewarded with crypto-currency. This process of validating the transaction is known as mining andthe node performing this validation is known as miner.
3. After validation is done that block is added to theblockchain.
4. After the whole process of validation isperformed the transaction is completed.

Some basic concepts of blockchain technology can be understood in the following descriptions.

B. Block

As explained earlier blockchain are formed together bya number of blocks connected together in a peer-to-peer network thus making a decentralized application. The header of these blocks contains hashes of previous blocks in them. A block contains three things in it which are data, hash of current block and hash of previous block. The data could be anything as it depends on the type of blockchain. As in case of bitcoin, the data consists of coins that are

actually electronic cash [13]. The hash that is stored in these blocks contains a SHA-256 cryptographic algorithm which is used for unique identification of a block on thechain.

C. Consensus Algorithm

Each block that is added on the chain would need to follow some consensus rules for it to be added on the blockchain. For this purpose blockchain technology uses consensus algorithms. The most common consensus algorithm used is Proof of Work (PoW) algorithm and it was used by Nakamoto [13], in bitcoinnetwork. The basic working of this algorithm is that there are number of nodes or participants on a blockchain network so when a transaction is requested to be added on the network by any participating node itneeds to be calculated. This process is called mining and the nodes that are performing these calculations areminers [17].

D. Key Features of Blockchain

1) Decentralization

With blockchain the information is distributed across the network rather than at one central point. This also makes the control of information to be distributed and handled by consensus reached upon by shared input from the nodes connected on the network. The data thatwas before concentrated at one central point is now handled by many trusted entities.

DATA TRANSPARENCY

Achieving data transparency in any technology is to have a trust based relationship between entities. The data or record at stake should be secured and temper proof. Any data being stored on the blockchain is not concentrated at one place and is not controlled by one node but is instead distributed across the network. Theownership of data is now shared and this makes it to betransparent and secure from any third party intervention.

2) Security and Privacy

Blockchain technology uses cryptographic functions toprovide security to the nodes connected on its network.It uses SHA-256 cryptographic algorithm on the hashesthat are stored on the blocks. SHA stands for Secure Hashing Algorithm,these hashes provide security to theblockchain as data integrity is ensured by them. Cryptographic hashes are strong one way functions thatgenerate checksum for digital data that cannot be used for data extraction. This makes blockchain as such a decentralized platform made secure by thecryptographic approaches which makes it to be a goodoption for privacy protection of certain applications.

E. Challenges Faced by BlockchainTechnology

1) SCALABILITY AND STORAGE CAPACITY Storage of data on the blockchain causes two mainproblems, i.e.,confidentiality and scalability.The dataon the blockchain is visible to everyone that is presenton the chain this makes the data vulnerable which is nota desired outcome for a decentralized platform. Thedata stored on the blockchain would contain patientmedical history, records, lab results, X-rays reports,MRI results and many other reports, all of thisvoluminous data is to be stored on the blockchain thatwould highly affect the storage capacity of blockchain[18].

2) LACK OF SOCIAL SKILLS

The way the blockchain technology works is understandable by very few people. This technology isstill in its initial phases and is constantly evolving. Moreover, the shift from trusted HER systems to the blockchain technology would take time as hospitals, orany other healthcare institutes need to completely shifttheir systems to blockchain.

TABLE 1. Benefits and barriers of blockchaintechnology.

Benefits	Decentralized	The data or information stored on the blockchain is distributed across the network
	Data Transparency	Data stored on the blockchain is temper-proof
	Security and Privacy	Blockchain uses cryptographic algorithms to secure any information being stored on it
Barriers	Scalability, Storage Capacity	Storing huge volumes of data on the blockchain would cause storage and scalability problems
	Lack of social skills	As blockchain is an evolving technology and it is not a well understood technology so, it is quite challenging to shift the previously used systems on this technology
	Lack of universally defined standards	There are no defined standards and principles for blockchain technology that are universally applied which makes it difficult to enforce it throughout a specific domain

3) LACK OF UNIVERSALLY DEFINEDSTANDARDS

As this technology is still in the initial phases and is constantly evolving so there is no defined standard for it. Due to this the implementation of this technology inhealthcare sector would also take more time and effort.As it would require certified standards from international authorities that overlook the standardization process of any technology [19]. These universal standards would benefit in deciding upon thedata size, data format and type of data that could be stored on the blockchain. Moreover, the adaptation of this technology would become easier due to the defined standards, as they could be easily enforced in the organizations.

III. Related Work

Blockchain technology was designed by Nakamoto[13], the basic idea was to have a cryptographically secured and a decentralized currency that would be helpful for financial transactions. Eventually, this idea of blockchain was being used in various other fields oflife; healthcare sector also being one of them intends touse it. A number of researchers have carried out the research on this area, these research works focus on thefact that whether the idea of using blockchain for healthcare sector is feasible or not. They also identify the advantages, threats, problems or challenges associated by the usage of this technology. Some researchers also discussed the challenges that would be faced while actually implementing this on a largerscale.

A. Theoretical/Analytical Blockchain-Based Research

Gordon and Catalini [14], conducted a study that focused on the methods by which blockchain technology would facilitate the healthcare sector. Theyidentified, that healthcare sector is controlled by hospitals, pharmaceutical companies and other involved third parties. They specified data sharing as the key reason why blockchains should be used in healthcare. This study also identified four factors or approaches due to which healthcare sector needs to transform for usage of blockchain technology. These include way for dealing of digital access rights, data availability, and faster access to clinical records and patient identity. It also discusses the on-chain and offchain storage of data. The study also included the challenges or barriers faced by usage of blockchain technology these were huge volume of clinical records,security and privacy, patient engagement.

Eberhardt and Tai [18], conducted a study to understand possible approaches to solve the scalabilityproblem of blockchain and also to identify such projects that intend to solve this problem. They define blockchain as composition of various computational and economical concepts based on peer-to-peer system.The aim of this study was to find which data should bestored on-chain and what could be stored offchain. Thisstudy presented five patterns

for off-chain storage of data and also includes the basic ideas andimplementation framework of these patterns. The authors explain on-chain data is any data that is stored on the blockchain by performing transactions on it. While off-chain data storage is to place data elsewhere on any other storage medium but not on-chain and it also would not include any transactions.

Prototype/Implementation Blockchain-Based Research

Sahoo and Baruah [14], proposed a scalable frameworkof blockchain using Hadoop database. In order to solvethe scalability problem of blockchain, they proposed touse the scalability provided by the underlying Hadoop database along with the decentralization provided by the blockchain technology. They used the method to store blocks on the Hadoop database, the blockchain ontop of this framework includes all of the needed dependencies of blockchain but the blocks are stored onHadoop database to improve scalability of the blockchain technology. To tackle the scalability problem of blockchain platform this study offers to useHadoop database system, along with SHA3-256 for hashing used for transactions and blocks. The programming language used for this architecture was Java. This study, was helpful in understanding that blockchain can be used with other platforms that are scalable to improve or solve the scalability of thisplatform.

Kim et al. [16] proposed a system for management of medical questionnaires and the aim of this system is data sharing through blockchain technology. The authors explain that selection of data storage and sharing of medical questionnaire is to use this data for further medical and clinical research purposes. They emphasized that it would be helpful for developing diagnosis system, resolving terminologies being used inEHR systems and security issues associated with thesesystems was also a reason due to which authors selected blockchain technology for their proposed framework. This study contains two main functions, i.e., to create, store the data gathered by questionnaires and to share that data. Another benefit proposed by the system is thevalidation of the questionnaire being submitted in the system. The questionnaires that are added on this system are first validated to be correct specified formatand then are parsed to differentiate the personal data and specific data related to questionnaire results. This would ensure that data could be shared for future research purposes. The authors also address the scenario when a third party requests to access this questionnaire data, this would need the patients' permission that is asked by the doctor to let third partyview that data.

IV. Preliminaries

This section formally describes the preliminaries usedin proposed framework. It describes the software platform used for development of this framework andits advantages. Ethereum and IPFS being the most prominent and important for implementation of this framework are also discussed in the following section.

A. ETHEREUM

Ethereum is a distributed blockchain network that usesthe idea of blockchain that was previously used in the popular crypto currency Bitcoin [13]. Ethereum was formally introduced in year 2015 and the idea behind Ethereum was to create a trustless smart contract platform that would be open-source and would also hold the feature of programmable blockchain. Thistechnology also shares the peer-to-peer networking thatmakes it distributed. This platform also makes use of itsown crypto currency known as Ethers [17]. This cryptocurrency can be used for sharing it between accounts connected on Ethereum blockchain [18]. Ethereum alsoprovides the programmers a language in which they cancustomize their own blockchain, this language is known as Solidity. It was developed for smart contractsthat are the main feature of Ethereum.

B. Information Transaction

In Ethereum, transaction is the way external entity would interact with Ethereum. It can be used by external user to update the state of the record or information stored on the Ethereum blockchain network. An Ethereum transaction contains following elements [9]:

- **From –** message sender, having a 20-bytes address.
- **To –** message recipient, also having a 20-bytes address.
- **Value -** the fund amount (wei) transferred from sender to recipient
- **Data(optional)**–contains the message that is beingsent to the recipient
- **Gas –** For every transaction on the Ethereum blockchain the sender needs to pay some fees for performing that operation this fee is known as Gas.Every transaction contains the gas limit and gas price in it.

- **Gas Price:** that fee the transaction sender iswilling to pay for gas
- **GasLimit:** maximum gas that could be paidfor this transaction

C. Smart Contracts

Smart contract are known as the piece of code that is used to perform any task on the blockchain. This pieceof code is executed when the users send the transactions. They run on the blockchain directly thus making themselves secure from any kind of tampering and alterations. Smart contract commonly use solidity language and they can be used to program any kind of operation that a programmer wants to do on the blockchain. After programming the required operationsthe programmers can compile them by using EVM bytecode that would be explained in next section. And after compiling them it could be executed and deployedon the Ethereum blockchain [11]. The programming language of JavaScript and Python are encapsulated with the Solidity language provided by Ethereum to write code in smart contracts.

D. Ethereum Virtual Machine (EVM)

The key benefits that Ethereum platform offers includethe programmable blockchain. It provides its users withthe choice to create their own applications functioningon the Ethereum. The applications built using thisplatform are known as Distributed Applications(DApps). They contain a number of protocols that arepackaged together to create a platform for DApps.These DApps contain smart contracts that have codedefined by the user to perform some defined task of anapplication. That code is deployed and executed usingthe Ethereum Virtual Machine (EVM) [9]. Thus,the applications that are created using the smart contractare in actual being run on EVM.

E. Inter-Planetary File System (IPFS)

IPFS is a protocol that uses peer-to-peer network fordata storage. It provides secure data storage as datastored on IPFS is protected from any alteration. It usesa cryptographic identifier that protects the data fromalteration as any attempt to make change on the datastored on IPFS could only be done by changing theidentifier. All the data files stored on IPFS contains a hash value that is generated cryptographically. It is unique and is used for identification of stored data file on the IPFS.

This secure storage strategy of IPFS protocol makes it a favorable choice for storing critical and sensitive data. The cryptographic hash that is generated could be stored on the decentralized application to reduce the exhaustive computational operations over the blockchain.

IPFS protocol works using a peer-to-peer (P2P) network, this network contains a data structure known as IPFS object that contains data and link in it. Data is unstructured binary data and link consists of an array. The IPFS protocol works in the following way:

- Files stored on IPFS are assigned a uniquecryptographic hash
- Duplicate files are not allowed to exist on the IPFSnetwork
- A node on the network stores content and indexinformation of the node
-

V. System Design And Architecture

Therelated work section includes the work done in the domain of health care being implemented using blockchain technology. As mentioned they provided certain solutions for solving the prevalent problems in blockchain technology. The studies in discussion weremainly addressing the problems of scalability and datasharing through blockchain. They propose the solutionof using an underlying database, pertaining to some ONC requirements and any other defined standards to solve them. In contrast to those solutions our proposedframework offers to solve this problem of scalability byusing off-chain scaling mechanism of IPFS. Moreover,Ethereum is used for the overall implementation of theproposed framework. Ethereum and its dependencies are also discussed in the previous sections of this paper.

A. System Design

System design is the most important and vital part of any framework as it is used for the development of thesystem from its theory. This section includes the modules, architecture and various elements that are combined together to form the whole system's framework. As defined earlier the purpose behind this proposed framework is to create such a decentralized system that is temper-proof, secure and confidential blockchain-based system for electronic health records.

As visible in below figure 2, the proposed framework or system has three entities or modules. These modules when combined together would keep our system working. These entities or modules have further concepts that need to be understood they are explainedas follows.

The proposed framework consists of users that could bepatients, doctors, administration and nursing staff. They were given granular access as they should have varying level of authority on the system.

1) USER LAYER

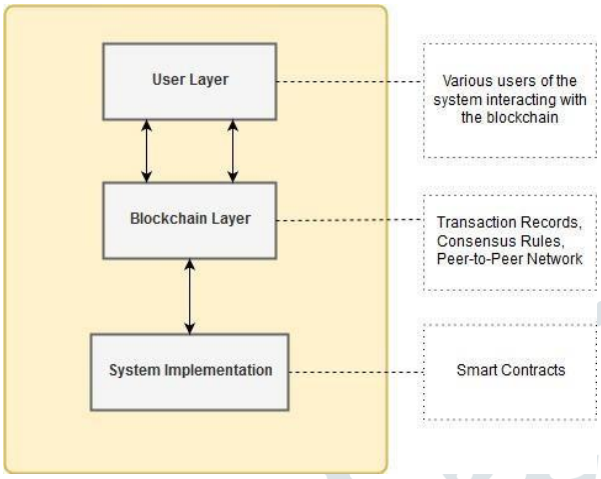


FIGURE 2. System design of proposed framework.

A user of a system is defined as an individual who makes effective use of the system and its resources. A user has various roles and features on the system, making him identifiable on the system. The users of thissystem could be patients, doctors and administrative staff etc. The main task of these users would be to interact with the system and perform basic tasks such as create, read, update and delete the medical records.

The users using this system would be accessing the system's functionality by a browser which in technicalterms we refer as DApp browser, as it is containing the GUI (Graphical User Interface) of the DApp, i.e., our proposed system framework. The GUI contains all the functions that could be accessed by a particular user. The user according to the assigned role could use this GUI for interacting with the other layer of the system, i.e., blockchain layer.

2) BLOCKCHAIN LAYER

The next layer on the system is the blockchain layer; this layer contains the code or mechanism for interaction of user with the DApp which is functioningon the blockchain. This layer contains three elements inside it. They are:

- **Blockchain Assets:** In Ethereum blockchain, transaction is the process by which external user can update the state of the record or information stored on the Ethereum blockchain network. Thesetransactions are treated as **assets** by the Ethereum blockchain as they are piece of information that user can send to another user or to simply store it for using it later.
- **Governance Rules:** Blockchain technology in general follows some consensus rules for its transactions to be done and computed. For this purpose it needs some consensus algorithms to keep the blockchain temper-proof and secure. Ethereum blockchain uses Proof of Work (PoW) consensus algorithm, the reason behind using it is also for ensuring that governance of blockchain ismaintained in a trusted manner which is through consent from all the trusted nodes attached to the blockchain network.
- **Network:** Ethereum blockchain uses the peer-to- peer network. In this network all the nodes are connected as peers.With no node acting as the central node controlling all the functions of the network. The reason behind using this network was because the idea was to create a distributed platform not a centralized. So, using a network where all the connected node shave equal status and right was the best choice this technology could have done.

TRANSACTION

The system includes following transactions:

- **Add records** would create patient's medical records in the DApp. It contains the fields of ID, name, co-morbid, blood group, and IPFS hash. Thepatient's basic medical records is stored along withthe IPFS hash that contains the file uploaded containing the lab results or other medical recordsof patient.
- **Update records** would update the medical recordsof patient. This can only change the basic information of the patient not the IPFS hash. IPFShash is non-updateable to ensure security of records.
- **View records** would let the user view the medicalrecords of a patient stored in DApp. The view records function is used both by doctors and patients. The patient can view his records by the system authenticating that patient views only his own medical records. For this purpose system usesthe public account address of the patient to ensurethat only the relevant medical records is shown to the patient.
- **Delete records** would make the user be able to delete record of any patient. The user here would be the doctors they are given this right to delete anypatient's record stored on the blockchain.
- **Grant access** for each of the above mentioned transactions, certain user would need to have access to them, i.e., only the doctor or nursing staffcan make changes in the records of the patient or add them. So, add and update records would only be accessible to these entities. Moreover, patient can view his medical records but won't be given the access to add or update them.

3) SYSTEM IMPLEMENTATION

As already explained in the previous sections, the system was implemented by using the Ethereum and its dependencies. This section explores system implementation in more detail to get an insight on the system various functions.

4) SMART CONTRACTS

As explained earlier, smart contracts are an important part of DApps as they are used for performing basic operations. Following contracts are included in this framework:

- Patient Records
- Roles

These contracts are used for giving access to the users on the DApp and performing CRUD operations on the records of patient. The Patient Records smart contract is made purely for implementing the functionality of the proposed framework.

It performs the CRUD operations along with the defining roles for access of these functions.

The second contract mentioned above, i.e., Roles is a predefined smart contract by the Open Zeppelin smart contract library. This library contains several smart contracts performing various functionalities that could be used for creatingyour own smart contracts. Thereason behind using this library was to make use of thebenefits it provides, i.e., tested and community reviewed code. The Rolessmart contract belongs to theAsset library, which is a sub-library of the OpenZeppelin library. The asset library containsvarious other contracts for defining the access rules butroles library provide a granular role definition mechanism which was the main reason behind selectionof this smart contract.

The algorithm for defining the Patient Records smart contract is given below. It defines all the operations thatare being performed in itand various conditions that areassociatedwith them. It also explains how the roles arebeing maintained for granting access to a particular functionality.

B. Usage Scenario for Algorithm 1

The Algorithm 1 explains the functioning of the smart contract for patient records. This algorithm has five functions that are to define roles, add, view, update anddelete records. These functions are used by the administrator and other users of the system. The first function of Algorithm 1 define roles, is to be performedby the administrator and it includes two variables new role and new account; these would be used for adding new role and account in role mapping list. This list would be used later on for accessing the roles of the users of the system. The second function is add patientrecord and it is performed by the doctor after they have been assigned this role by the administrator in

thedefine roles function. This function also keeps a checkthat this task is being performed by the authenticated public address of the doctor's account and not by any other third party. For this they use 'msg.sender' term which in programming language, i.e., Solidity languageused by Ethereum is used for identifying the address ofthe user. After this validity check is done the doctor canadd the records of patient and after doing so would endthe function by saving that record.

The third function is and it needs the patient id to be passed as the variable. This id would be used to by the system to look up the records of the patient and after doing so it would return those records to the account that requested to retrieve those records. This function also includes the validation for the assigned roles of patient or doctor. As only the patient and doctor wouldbe allowed to view the records. The fourth function is update patient records and is used for making anychanges in the saved records of the patient. The validation process is done once again to ensure that theauthenticated users are accessing this function. The lastfunction of Algorithm 1 is delete patient records whichas evident from its name is used for deletion of the records of a specific patient. This function takes the unique id of **Algorithm 1** Smart Contract for Patient Records

Assign Roles:

function Define Roles (New Role, New Account)add new role and account in roles mapping
end function Add Data: **function** Add Patient Record (contains variables to add data)
if (msg.sender == doctor) **then** add datato particular patient's record
else Abort session
end if
end functionRetrieve Data:
function View Patient Record (patient id)
if (msg.sender == doctor || patient) **then**
if (patient id) == true **then** retrieve data from specified patient (id) return (patient record) to the account that requested the retrieve opn **else** Abort session
end if end if
end function Update Data: **function** Update Patient Record (contains variables to update data)
if (msg.sender == doctor) **then**
if(id == patient id && name == patient name) **then** update data to particular patient's record return success
else return fail
end if
else Abort session
end if
end functionDelete Data:
function Delete Patient Record (patient id)
if (msg.sender == doctor) **thenif** (id == patient id) **then**
delete particular patient's recordreturn success
else return fail
end if
else Abort session
end if
end function

patient as input and after validating that the doctor is the one performing this function it would delete those records. This role based access would ensure that no third party is accessing these functions and only the authenticated users of the system would have access tothese functions.

C. Working Example for ProposedFramework

As mentioned in previous section, we have used Ethereum for implementation purposes and the expected block time for it is between 10 to 19 seconds.Here by block time we are referring to the amount of time taken by a new

block to be generated. For smart contracts the amount of time it takes for a transaction tobe confirmed is 38 seconds and this depends upon the gas price specified for the transaction. Unlike Bitcoin, Ethereum has no block size limit but instead it has a gaslimit, the terms gas price and gas limit are defined in the previous sections. The time taken for an append function of Algorithm 1, i.e., would be around 1-2 minutes depending upon the size of data. For the retrieval function such as Algorithm 1 function of ViewPatient Record would take 50 seconds.

InordertoexplainthefunctionalityofAlgorithm1inter ms of transaction size let us consider the following example.

Let,

Number of transactions per hour (Avg) = 31474Number of blocks per hour (Avg) = 269

Average transactions per block = Avg. number oftransactions per hour / Avg. number of blocks per hour

= 31474/269 =117

Average transactions size = Block Size / Averagetransactions per block

= 21.7KB / 117 = 0.19 KB

By the above calculations it is deduced that the average transaction size is 0.2 KB approximately. It should also be kept in mind here that these figures usedabove are real time values and are specifically forEthereum blockchain network.

D. Usage Scenario for ProposedFramework

The figure 3 below depicts the basic usage scenario of the proposed framework. Thesystem mainly has two entities,i.e., Administrator and User. Users are further divided into two categories for our proposed frameworkthey are doctor and patient. These users are assigned roles by the administrator of the system who is someonebelonging to the hospital's administrative staff. Here administrator is assigned the task of the defining the granular access to two main users of our system, i.e., doctor and patient.

So, the first activity would be that administrator assignsroles and this would include Role Name and Account Address of the user who is being assigned that role. Every user of this proposed system would have a role name and account address for using the system. So, after administrator assigns this user some role, that role name and account address is stored in a roles list forvalidation purpose required in later steps.

After roles are assigned, now when a user wants toperform some operations on the proposed system hewould at first request to perform them. The systemwould verify the user role name and account address from the Roles List and allows them accordingly toperform those functions after validation returnssuccess. After the functions are performed the system would store the information on the Ethereum Blockchain that would perform transactions for that information. Once the transaction is confirmed the system receives the message of success from the blockchain layer that users can view on the DApp browser on which the whole proposed framework is being visible.

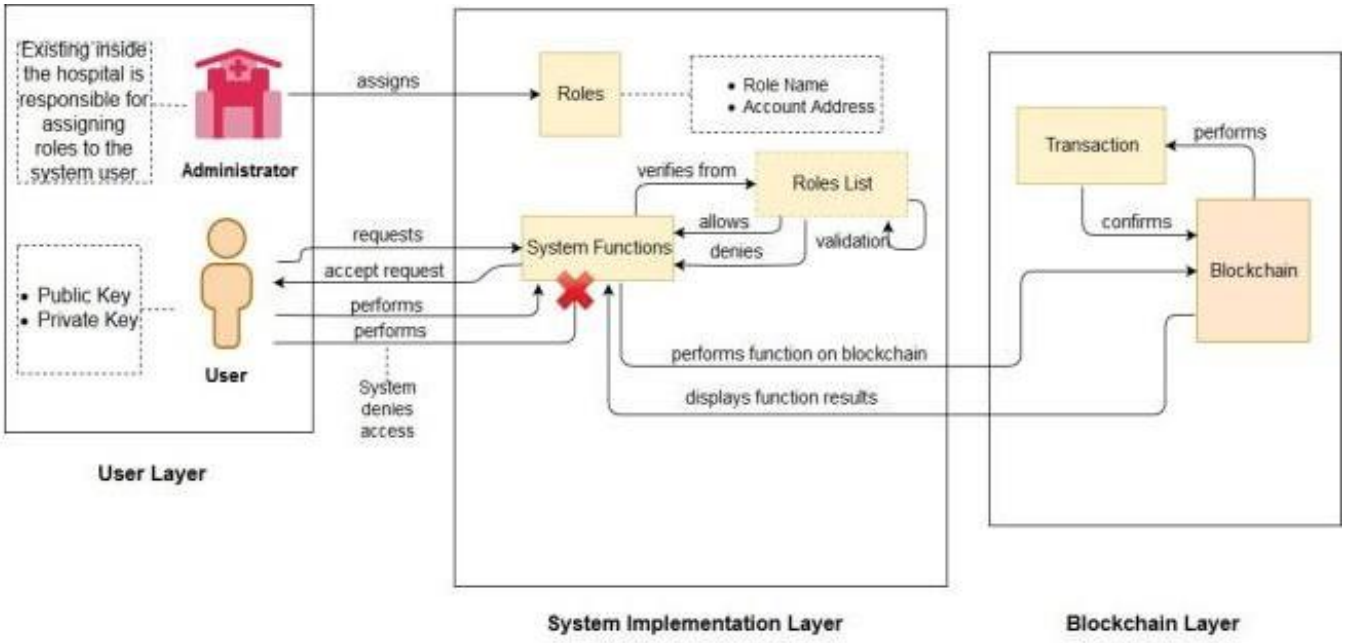


FIGURE 3. User interaction with DApp.

VI. Performance

In this section we evaluate the performance of the proposed framework. Byassessing theperformance wecan mitigatethe risks associated with this novel technology that is understandable by very few individuals.

A. Experimental Setup

For testing performance of the proposed framework we have conducted experiments by using the following configurations:

- Intel Core i7-6498DU CPU @ 2.50GHz 2.60 GHzprocessor
- And 8.00 GB of memory with Windows 64-bit OS(version 10)

We developed our proposed framework by using the Solidity which is programming language of Ethereum. JavaScript and Python are encapsulated in the Solidity language which is provided by the Ethereum to write code in smart contracts.

B. Data Collection for PerformanceEvaluation

This section explains what kind of data is used for evaluation of performance of the proposed framework.This section also discusses the metrics that are used to explain the results of this performance evaluation beingconducted.

1) TRANSACTION DATA

To evaluate the performance of the proposed framework following transaction data with its details are used.

- **Transaction Deployment Time (t_{x1})**

It is defined as the time when transaction gets deployed.In Ethereum, a smart contract is deployed using the transaction so this deployment time refers to that time.

- **Transaction Completion Time (t_{x2})**

It is defined as the time when the transaction is completed and confirmed by the blockchain which in this case is Ethereum.

2) EVALUATION METRICS

The metrics used for evaluation include the execution time, latency and throughput of the proposed framework. These are explained briefly as follows:

- **Execution Time** is defined as time duration (in seconds) between the transaction confirmation andits execution in the blockchain network.
  Mathematically, it is (max(t_{x2}) - min (t_{x1})).
- **Throughput** refers to the amount of data that could be transferred from one location to another in a unit amount of time.
- **Latency** is known as the delay that occurs when asystem component is waiting for another component of the system to respond to an action. In terms of time it could be referred as the difference of deployment and completion time of transaction.

C. Results

1) PERFORMANCE ASSESMENT

In order to understand how our proposed framework would perform in real-case scenario of various users performing different functions on the framework we conducted performance evaluation using Apache JMeter version 5.1.1 and Apache Version 2.00. ApacheJMeter is a desktop performance testing tool which is used for analysis and testing of applications [34].

A: Average Execution Time

The execution time increases with the number of transactions being increased. These transactions are performed for the various functions that are included inthe smart contract whose algorithm is defined in Section V. When there is only one user using the systemthe functions Assign Roles, Add Patient Records and View Patient Records would take 18.29 sec, 1 min 48 sec and 50 sec respectively for these functions to be executed. This time would increase when 100 users areusing the system simultaneously.

B: Throughput

Algorithm 1 explains various functions that are included in the smart contract of the proposedframework. By using JMeter we simulated number of users from 100 users to 500 users (with period of 10 to35), who are using the system and performing its various functions. In JMeter the throughput is represented in Data/time i.e. KB/sec units. While conducting the experiments we simulated the number of users as specified above and evaluated the performance of the system. These simulations are run on the proposed framework and at the end throughput is analyzed.

The following figure 4 shows the throughput of the proposed framework.

It is observed while conducting this experiment that as the number of users and requests increase the throughput of the system increased considerably in a linear manner. This

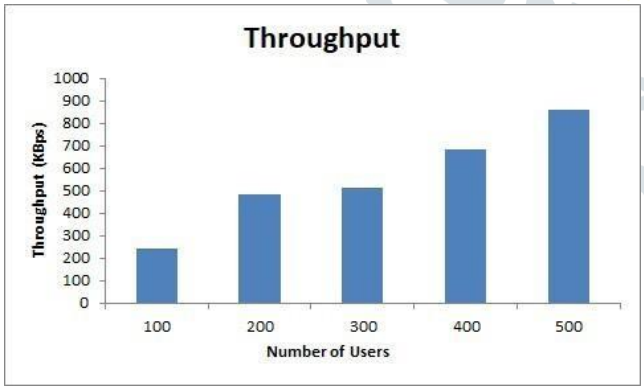


FIGURE 4. Throughput of the proposed framework.

linear increase in throughput indicates the efficiency ofthe proposed framework.

C: Average Latency

Latency as defined earlier is the delay or difference in time when one system component sends a request and a response is generated by any other system component.The difference between these two actions is defined aslatency. Here we have evaluated the average latency ofthe proposed framework by using JMeter. While evaluating the latency of the proposed framework we simulated the number of users by JMeter. In JMeter latency is measured in terms of milliseconds.

The following graph Figure 5 gives an overview of average latency of the system along with the throughputof the proposed framework. The highest recorded latency in this experiment is 14ms.

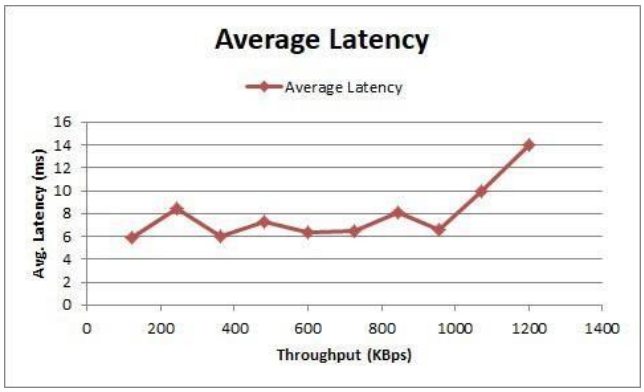


FIGURE 5. Average Latency of the proposedframework.

We also evaluated the performance of the proposed framework by assessing the size and cost of the transaction. Before assessing the transaction size we also analyze the transaction payload. This assessment isdiscussed in detail in the following section.

2) PERFORMANCE EVALUATION(TRANSACTION)

Every transaction on Ethereum contains a data payloadfield.

Data payload is included in that transaction which is meant to invoke smart contract functions. This data payload is in the hex-serialized format and has bytes associated with it. Here we would discuss two functionsfrom Algorithm 1 in order to understand the data payload included in the transactions being generated.

Data payload is the optional field of a transaction which is only used when there is some form of interaction with contract functions. It has two importantparts,

- Function Selector
- Function Arguments

The function selector are first 4 bytes of Keccak-256 hash, it is used for identification of the smart contract function which is being invoked. The function arguments include various static and dynamic element types which have different rules for encoding them in payload.

Let us now understand the payload of Define Roles function from Algorithm 1 to get an understanding as to how the data payload is generated. Firstly we wouldseparate the function selector and arguments. The function selector is actually the function signature which in this case is:

DefineRoles (string, address)

For the above function the Keccak-256 hash is asfollows,

0x6c0abd24edce8ce20a2dfb1cd2026179214 468cde47681e871b6e14bf9d39efd

The first 4 bytes of the generated hash (0x6c0abd24) are of the function selector which points to the functionbeing invoked from the contract. After function selectoris calculated let us now understand how the function arguments are encoded.

For this we encode the head part of two arguments, theaddress is the static type and string is the dynamic type.The static type is passed directly while for dynamic type the offset in bytes are used, it is also measured from the start of the value encoding. The first four bytescontaining the hash of function signature is not countedin it.

The encoding for dynamic type string with value ‘‘Doctor’’ would be as follows,

TABLE 3. Transactions size and fee for proposedframework.

Transaction	Size	Fee
TxF_{assign}	132 bytes	0.00006 ETH
TxF_{add}	548 bytes	0.0003 ETH
TxF_{view}	122 bytes	0.0004 ETH
TxF_{update}	420 bytes	0.00001 ETH
TxF_{delete}	132 bytes	0.0003 ETH

The encoding of this function with only its dynamictypes is as follows,

```
0x0000000000000000000000000000000000000000
0000000000000000000000000006
```

The number of elements or bytes is 6 and they are represented as seen above. Following is the string value‘‘Doctor’’ padded to 32 bytes on the right.

```
0x48976c7c7f2c20667f626c6421000000000000
0000000000000000000000000000
```

TABLE 2. Data payload of transactions used inproposed framework.

Data Payload	Contents Types	Size
Payload of F_{assign}	string, address	64 bytes
Payload of F_{add}	string, string, string, string, string, address	192 bytes
Payload of F_{view}	string, uint	64 bytes
Payload of F_{update}	string, uint, string, string, string	160 bytes
Payload of F_{delete}	string, uint	64 bytes

```
0x6c0abd24
  0x0000000000000000000000000000
  0000000000000000000000000000000000000006
    0x48976c7c7f2c20667f626c64210000000
  0000000000000000000000000000000
```

The static and dynamic type in this function would havesizeof32bytes.Thetotalbytesizeofthisfunctionis64bytes. In the same way we can calculate the data payload of other functions of the Algorithm 1. The following table2 represents the data payload size of various functions.

By using the data payload we can calculate the transaction sizes of various functions of our proposed framework. Table 3 represents the transaction sizes in bytes for these functions. Here it must also be kept in mind that the transaction size calculated in this sectionis from data payload perspective and is specifically calculated for various functions of Algorithm 1, whereas in Section V the transaction size was calculated fromblock size perspective and was calculated in ageneralized manner.

We can also calculate the fee or cost associated with various transactions of the proposed framework. In Ethereum the transaction fees is calculated in 'ETH' [29] which is Ethereum coin and it has certain units such as wei, gwei associated with it. The formula to calculate Ethereum transactions fee isalso discussedhere. The transaction fee for a transaction is the product of gas consumed and gas price. It could berepresented as follows,

Transaction Fee = gasConsumed × gasPrice

We can calculate the transaction fee by using the recommended figure for gas consumed which is 21000and is 21 Gwei for gas price. So,

Transaction Fee = 21000 × 21 = 441000 Gwei

And to calculate the transaction fee of 1ether we woulduse the following method,

1 Ether = 1000,000,000 Gwei Transaction Fee for 1 Ether = 441000/1000,000,000 Gwei = 0.00041 Gwei

The transaction fees for various functions of Algorithm1 are presented in table 3.

3) COMPARISON OF PROPOSED FRAMEWORK WITH RELATED WORK

We also discuss some parameters that are present in ourframework and are used for comparison with the relatedwork in this domain. While ensuring the presence of these parameters in the framework it is also consideredthat it would not compromise the security and privacy of the system. For this both security and privacy are discussed in each of the parameters discusses below.

A. SCALABILITY

Scalability in simpler terms refers to the ability of an information system to perform it functions well in suchsituations when the storage volume of the system increases or decreases. In case of blockchain technology scalability is an issue that needs some permanent solution. As data size or volume isincreasing on the blockchain. Our proposed system used the off-chain storage mechanism as the patient's data stored on the blockchain contains the basic information of patient along with the IPFS hash, i.e., theoff-chain scaling solution used in our proposed system framework. This solves the scalability issue mentionedas now huge volume of patient medical record is not stored on the blockchain. As, the data size being storedon the blockchain has now decreased the transactions could also be performed faster. As mentioned earlier, IPFS uses cryptographic hash which is stored in the decentralized manner using peer-to-peer network. This also ensures that while solving the scalability problemthe security of the framework is not compromised.

B. CONTENT-ADDRESSABLE STORAGE Content-addressable storage refers to the off-chain storage mechanism of IPFS used in the proposedframework [20]. The sensitive record of patient isstored on the IPFS, which ensures that a hash of thestored record is generated. That hash is now stored inthe blockchain and is accessed when needed by thedoctors and patients. The IPFS generates thecryptographically secure hash which ensures thesecurity of the data being stored on it. And this alsoensures security in our proposed framework.

TABLE 4. Comparison of proposed framework withrelated work.

	[24]	[25]	[26]	**Our Proposed system**
Blockchain-based	Y	Y	Y	Y
Scalability	Y	Y	N	Y
Content-Addressable Storage	N	N	N	Y
Integrity	Y	Y	Y	Y
Access Control	N	Y	Y	Y

C. INTEGRITY

Integrity of a system is measured by the trustfulness ofthat system and also that system storing that information is temper-proof and reliable. This blockchain-based system ensures that it does not compromise this feature. The information stored in thissystem is intact and is not changed by any unauthorizedchannel. Moreover, information is available to only theassociated parties that are doctors and patients. The users of the system and any third party do not have theright to make any changes in the smart contract as theyare not having any access to it. This is done by using the access rules which ensure that the private data or medical records of patients are not accessible and remain temper-proof. Moreover, using IPFS for storageof records also ensures the security of the medical records of the patients.

D. ACCESS CONTROL

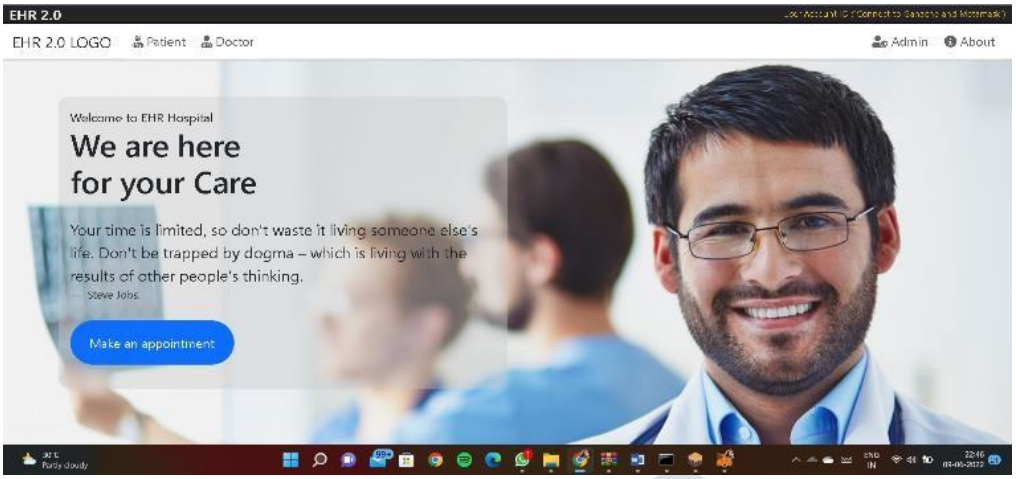
Using the Role-based access mechanism, this framework makes sure that every entity of the system is assigned a role. Any third party who is not authorizedto have access to the system would not be able to accessthe system. This system provides a two core security asfirstly blockchain technology in itself is secure and usescertain protocols and mechanism to keep itself secure from third-part intrusions. And secondly our system uses the Role-based access that also only allows the user shaving defined roles to have access to the systemand its functions. So, our system would not only ensuresecurity of patient records but would also make sure theaccess control of entities associated with it. This parameter also ensures that the security of the patient'spersonal medical data is not compromised and the access is provided to only the authorized users of the system.

VII. CONCLUSION AND FUTURE WORK

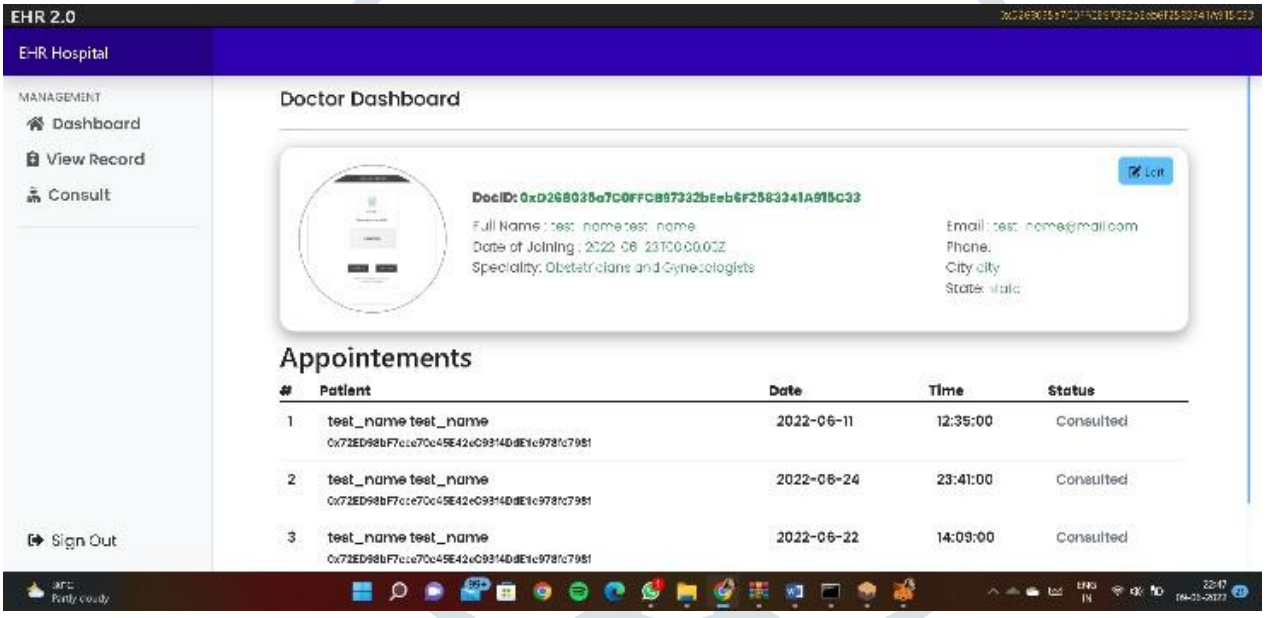
In this paper we discussed how blockchain technologycan be useful for healthcare sector and how can it be used for electronic health records. Despite the advancement in healthcare sector and technologicalinnovation in EHR systems they still faced some issuesthat were addressed by this novel technology, i.e., blockchain. Our proposed framework is a combinationof secure record storage along with the granular accessrules for those records. It creates such a system that is easier for the users to use and understand. Also, the framework proposes measures to ensure the system tackles the problem of data storage as it utilizes the off-chain storage mechanism of IPFS. And the role-based access also benefits the system as the medical records are only available to the trusted and related individuals.This also solves the problem of information asymmetryof EHR system. For the future, we plan to implement the payment module in the existing framework. For this we need tohave certain considerations as we need to decide how much a patient would pay for consultation by the doctoron this decentralized system functioning on theblockchain.

SCREENSHOTS

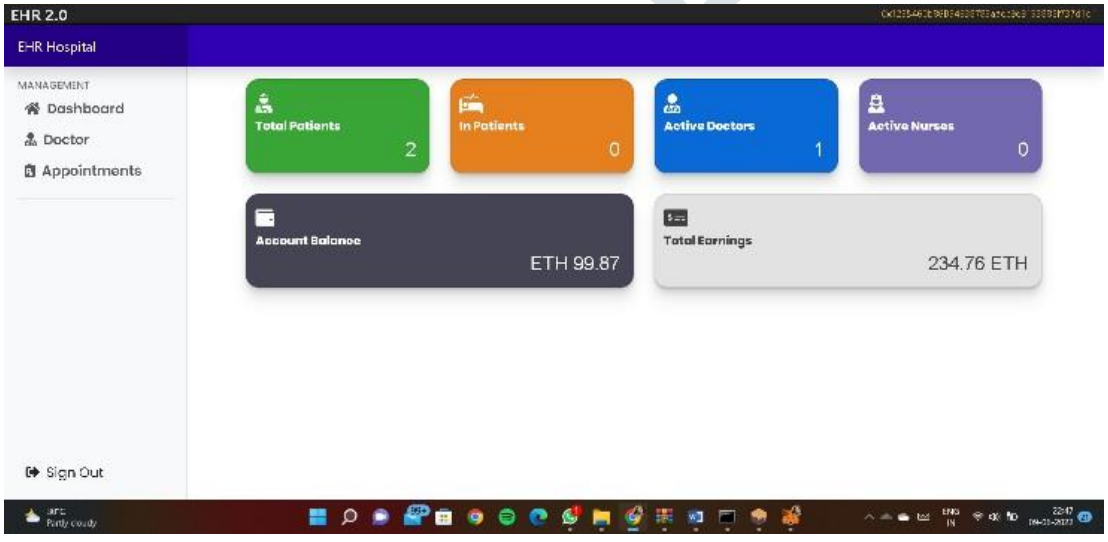
HOMEPAGE



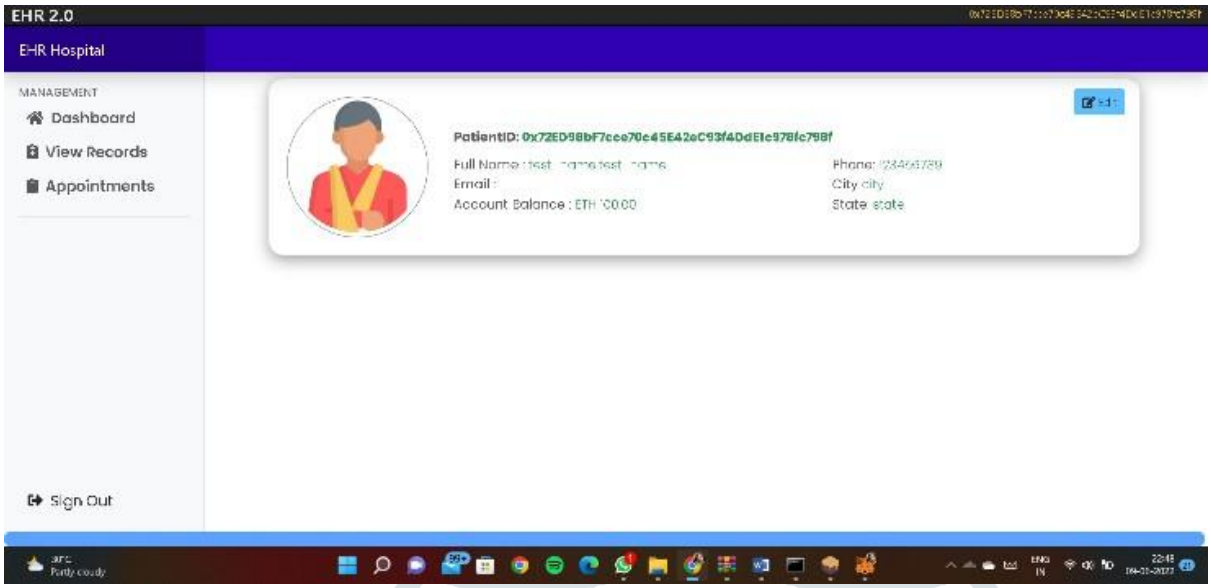
DOCTOR PANEL



ADMIN PANEL



PATIENT PANEL



REFERENCES

1. G. Jetley and H. Zhang, ‘‘Electronic health recordsin IS research: Quality issues, essential thresholds and remedial actions,’’ Decis. Support Syst., vol. 126, pp. 113–137, Nov. 2019.
2. K. Wisner, A. Lyndon, and C. A. Chesla, ‘‘The electronic health record’s impact on nurses’ cognitive work: An integrative review,’’ Int. J.Nursing Stud., vol. 94, pp. 74–84, Jun. 2019.
3. M. Hochman, ‘‘Electronic health records: A‘‘Quadruple win,’’ a ‘‘quadruple failure,’’ or simply time for a reboot?’’ J. Gen. Int. Med., vol. 33, no. 4, pp. 397–399, Apr. 2018.
4. Q. Gan and Q. Cao, ‘‘Adoption of electronic healthrecord system: Multiple theoretical perspectives,’’in Proc. 47th Hawaii Int. Conf. Syst. Sci., Jan. 2014, pp. 2716–2724.
5. T. Vehko, H. Hyppönen, S. Puttonen, S. Kujala, E.Ketola, J. Tuukkanen, A. M. Aalto, and T. Heponiemi, ‘‘Experienced time pressure and stress: Electronic health records usability and information technology competence play a role,’’ BMC Med. Inform. Decis. Making, vol. 19, no. 1, p. 160, Aug. 2019.
6. M. Reisman, ‘‘EHRs: The challenge of making electronic data usable and interoperable.,’’ PT, vol.42, no. 9, pp. 572–575, Sep. 2017.
7. W. W. Koczkodaj, M. Mazurek, D. Strzałka, A. Wolny-Dominiak, and M. Woodbury-Smith,‘‘Electronic health record breaches as socialindicators,’’ Social Indicators Res., vol. 141, no. 2,pp. 861–871, Jan. 2019.
8. S. T. Argaw, N. E. Bempong, B. Eshaya-Chauvin,and A. Flahault, ‘‘The state of research on cyberattacks against hospitals and available best practice recommendations: A scoping review,’’ BMC Med.Inform. Decis. Making, vol. 19, no. 1, p. 10, Dec. 2019.
9. A. McLeod and D. Dolezel, ‘‘Cyber-analytics: Modeling factors associated with healthcare data breaches,’’ Decis. Support Syst., vol. 108, pp. 57– 68, Apr. 2018. L. Coventry and D. Branley, ‘‘Cybersecurity in healthcare: A narrative review of trends, threats and ways forward,’’ Maturitas, vol. 113, pp. 48–52,Jul. 2018.
10. ‘‘The future of health care cybersecurity,’’ J. Nursing Regulation, vol. 8, no. 4, pp. S29–S31, 2018.
11. D. Spatar, O. Kok, N. Basoglu, and T. Daim, ‘‘Adoption factors of electronic health record systems,’’ Technol. Soc., vol. 58, Aug. 2019, Art. no. 101144.
12. S. Nakamoto, Bitcoin: A Peer-to-Peer Electrnic Cash System. 2008, pp. 1–9.
13. W. J. Gordon and C. Catalini, ‘‘Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability,’’Comput. Struct. Biotechnol. J., vol. 16, pp. 224– 230, Jan. 2018.
14. A. Boonstra, A. Versluis, and J. F. J. Vos, ‘‘Implementing electronic health records in hospitals: A systematic literature review,’’ BMC Health Services Res., vol. 14, no. 1, Sep. 2014, Art.no. 370.

15. T. D. Gunter and N. P. Terry, ‘‘The emergence of national electronic health record architectures in the United States and Australia: Models, costs, andquestions,’’ J. Med. Internet Res., vol. 7, no. 1, p. e3, Jan./Mar. 2005.
16. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, ‘‘An overview of blockchain technology: Architecture, consensus, and future trends,’’ in Proc. IEEE Int. Congr. Big Data (BigData Congr.),Jun. 2017, pp. 557–564.
17. C. Pirtle and J. Ehrenfeld, ‘‘Blockchain for healthcare: The next generation of medical records?’’ J. Med. Syst., vol. 42, no. 9, p. 172, Sep.2018.
18. A.A.Siyal,A.Z.Junejo,M.Zawish,K.Ahmed,A.Kha lil,andG.Soursou, ‘‘Applications of blockchaintechnology in medicine and healthcare:Challengesandfutureperspectives,’’Cryptography, vol.3,no.1,p.3,Jan.2019.