Volume 11, Issue 4
August 2022

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

A Secure Blockchain-based Framework for Healthcare Management System

[1]Gajala Praveen, [2]Piyush Kumar Singh and [3]Prabhat Ranjan

[1]Department of Computer Science, Central University of South Bihar, Gaya, India

[2]Department of Computer Science, Central University of South Bihar, Gaya, India

[3]Department of Computer Science, Central University of South Bihar, Gaya, India

E-mail: [1]gajalapraveen@cusb.ac.in, [2]piyush@cusb.ac.in, [3]prabhatranjan@cub.ac.in

ABSTRACT

Healthcare information systems have progressed in terms of electronic healthcare data management. An electronic health record (EHR) is a digital record of a patient's health information. Patient-centric data allows an authorized user to access the information at any time and from any location. E-healthcare offers more social advantages, better healthcare, and fewer medical errors. The combination of smart healthcare and blockchain is having a huge impact on the global development of health and medical services. The medical system will be more efficient as a result of decentralization and faster access to information. In this paper, we show how blockchain is being used in the healthcare industry to safeguard and manage electronic health records. A smart contract has been developed to create secure healthcare systems on the ethereum blockchain platform. In this work, we propose a secure blockchain-based framework for healthcare data storage. This paper explains the concept of blockchain, blockchain applications in healthcare, and the entire development process of frameworks for managing healthcare information sharing. Finally, the paper concludes with a discussion of future research opportunities.

Keywords: *Blockchain, Decentralization, Smart Contracts, Healthcare, Smart Health, Electronic Health Records.*

1. INTRODUCTION

Healthcare is a vital industry in which we maintain sensitive information such as provider and member information, which includes medical history, test results, service location, and service type. On a daily basis, all of this information must be processed, saved, and accessible. Many businesses in the healthcare sector have begun to transmit their data digitally. The EHR information will be used and transmitted between various systems, with the expectation that each interaction and transmission will be secure and trustworthy. Data leaks, interoperability, and information asymmetry are some of the difficulties in smart health care. To address these difficulties, blockchain eliminates the need for a middleman and provides a trustworthy, secure, and efficient mechanism for data exchanges. Because the blockchain is decentralized and open-source, any network participant can access it. But no one can change or erase data once it has been placed onto the blockchain. The data that is saved via blockchain is always visible.

The electronic medical record (EMR) is a computerized reproduction of paper-based health documents. EMR has further evolved into EHR, which allows many stakeholders to quickly communicate medical information. When systems are meant to have health information, the difficulty in healthcare is usually security concerns. Information security is included in the system. [1, 2]. The following are the most important considerations when it comes to the security of an EHR system: Confidentiality: One of the most important responsibilities of a healthcare provider is maintaining confidentiality. Health information is private and must be safeguarded against unwanted access [3]. Integrity: In medical services, data integrity is essential. It provides accurate and unaffected health data and also ensures the accuracy, consistency, and reliability of data [4].

Authorization: Medical service organizations are responsible for authorization. External users are excluded from the authorization process. The system must establish who has access to eHealth data [5]. Accessibility: The availability of a record is a feature that necessitates the use of a framework to allow authorized users to open, utilize, and access it. It means that customers can access information at any time if requested by an authorized user [6]. Paper Organization: The organization of this paper is as follows: An overview of blockchain in healthcare is described in section 2. In section 3, a full analysis and discussion of the linked works is provided. Section 4 discusses the preliminaries like smart contract and ethereum. The proposed framework and its factors definition are presented in section 5. Section 6 highlights the implementation details. The experimental outputs are discussed in section 7. Finally, section 8 brings the paper to a close.

2. OVERVIEW OF BLOCKCHAIN IN HEALTHCARE

Satoshi Nakamoto, a researcher who worked on the cryptocurrency bitcoin, was the first to introduce blockchain [7]. Figure 1 depicts a list of blocks linked by cryptographic hash. We constructed three blocks in the diagrammatic model, and each block was given some data. The blocks are arranged in order of when they were created. Every block contains a list of transactions that are linked to one another using a cryptographic hash like SHA256 [8]. It ensures safe and unchangeable records.

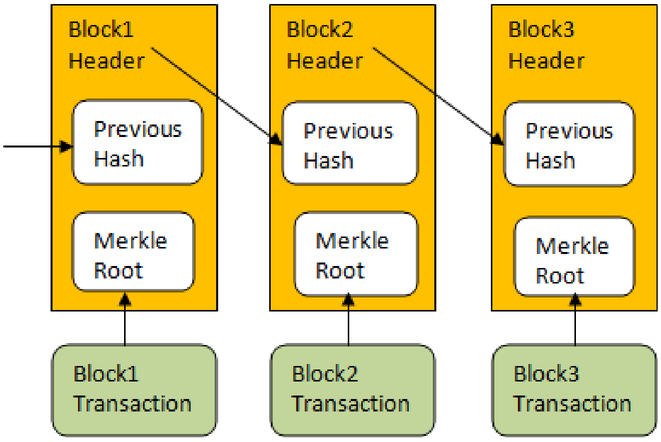


Figure.1. Blocks creating a chain using hashes

Nowadays, we are seeing a lot of data breaches in the healthcare industry. In comparison to other industries, it has risen at a quick rate because health insurance needs legal health records. Every citizen must have insurance because it is mandated in the majority of countries. Sharing data between healthcare organizations is difficult due to security and privacy concerns, although each hospital uses distinct terminology, employs different methodologies, and may have varied functional capabilities.

However, medical information shared between them should be interoperable. Blockchain has emerged as a prospective role in the medical industry for overcoming these challenges in electronic health records. For the EHR, we used blockchain to keep the patient's health data safe. The concepts of blockchain in the healthcare field have been discussed with their benefits and drawbacks [9].

2.1. DISTRIBUTED NETWORK FOR EHRS

EHRs are used to store medically sensitive data, which includes medical history, laboratory results, etc., in a digital format. These facts will be collected, stored, and managed electronically by authorized service providers. It will enhance the speed of data transfer between doctors and patients, and also save costs by eliminating the middleman between patients and doctors. The doctor sends digital information about their patients, such as medical information and test results, to the EHR database [10]. Only authorized people have access to the database's information [11]. Hospitals, doctors, patients, pathologists, and Admin can share data digitally without the involvement of a third party, as depicted in Figure 2. As a result of this, data duplication, information misuse, and information mismatches will all be reduced.

3. RELATED WORK

The use of blockchain technology to eliminate the middleman and secure the transaction is very popular. So it has been adopted by a variety of other industries, including healthcare. This section discussed the previous work to address the many features of blockchain in healthcare.

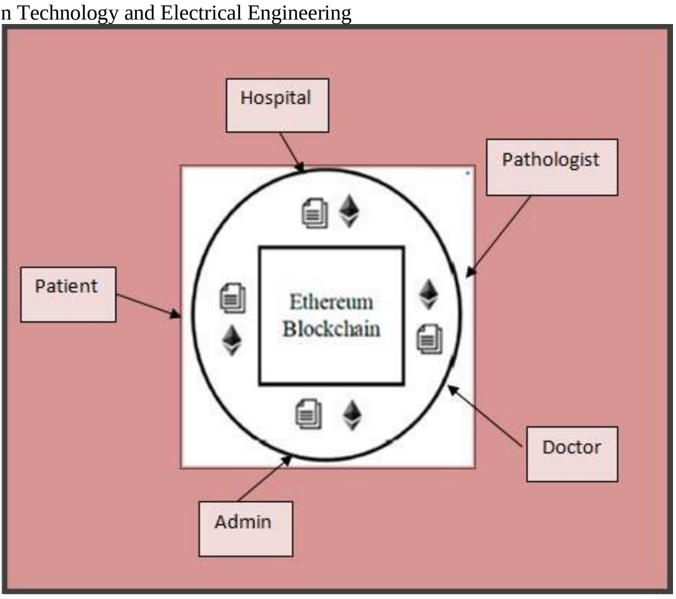


Figure.2. Health care distributed network

The MedRec [12] is a decentralized system that uses blockchain technology to store electronic management records. MedRec follows certain qualities such as data authentication, validation, and confidentiality when dealing with sensitive and critical information. The participants in this blockchain network are referred to as miners. Miners are the ones who make the blocks. Mining is a way to find legitimate blocks that all of the other network nodes must accept.

The members who validate or authorize these transactions are referred to as nodes. Participants in the network can share data that have the appropriate rights provided by the data owner.

Dagher et al. [13] presented the Ancile architecture, which uses smart contracts to improve access control and advanced cryptographic algorithms for securing the data. This framework provides data that is efficient and safe. The six types of contracts are used by the Ancile framework for operations. Patients can gain benefits such as enhanced utility and efficiency, as well as fewer data breaches, by using these contracts. Patients can control and view their private data via smart contracts, and they can provide authorization to other nodes to access their data. It also required many software modules for client usage and an architecture framework. The Database Manager component is responsible for generating hashes and connecting them to the blockchain. To ensure data integrity, hash values are utilized. It encrypts data with a symmetric key and protects it during distribution with the public key.

FHIRChain [14] is a blockchain-based concept proposed by Peng Zhang et al. for clinical information sharing. It demonstrates how to use FHIRChain to create and recover an entrance token. To create a model DApp, FHIR-Chain is connected. The application is coded in JavaScript, which has a blockchain-based interface called Ethereum. The author concluded with a case study of DApp to demonstrate the benefits of FHIR.

Rouhani et al. [15] describe the permission blockchain's access, which makes use of off-chain data storage. They also discuss the advantages and disadvantages of permissionless and permissioned blockchain. To control patient health data, they used a hyperledger platform for healthcare. Selfish Mining, Double Spending, and 51% are some of the security attacks discussed. They recommended more study in the direction of ZeroKnowledge to improve privacy and security.

Huynh et al**.** [16] provide an overview of the various aspects of blockchain security and protection. The common types of security attacks on blockchain and security upgrading arrangements were specifically given. The focus of the research was on existing solutions for safe blockchain protection, as well as the foundations for future investigation. In a blockchain organization, group signatures can be used to approve transactions, and zero knowledge can be used to ensure that transactions are legitimate.

Rouhani, S. and Deters, R. [17] study analyses the key ideas and offers the direction of continuing studies and improvements in the field of smart contracts in blockchain-based applications.

Johnson et al. [18] present a safe biomedical data sharing decentralized app, which is based on a real-world use case. An example is the iPhone's functioning framework (iOS) DApp.

The Jadhav and Moosafintavida [19] study is concerned with examining the potential applications of blockchain technology in present medical services frameworks, as well as the most important requirements for such frameworks. In addition, this research highlights the challenges that must be overcome before blockchain technology can be effectively implemented in medical care settings.

The authorized key issuer generates a public key and a private key for the user [20]. Every private key is linked to an access structure based on attributes. Doctors can enable data decryption using a private key, but they must follow the access policy during the decryption procedure. In the attribute-based encryption procedure, a monotonic access structure is maintained.

Non-monotonic access systems are possible for attribute- based encryption policy techniques. The doctor tries to gain access to the health record, which is encrypted. The encrypter has no way of knowing who will be able to decrypt the data. Encryption based on ciphertext characteristics has solved these concerns [21].

The patient's public key is used to encrypt the patient's health information. When the patient wants to see his or her medical records, he or she uses the private key that is linked to the public key to authenticate. This key is only used for a specific health record [22, 23]. The access policies of each health record are preserved using fine-grained encryption technology [24].

Despite the fact that patient data is encrypted and stored in the cloud using multiple methods [25]. In a centralized network, the single central node is the most significant part of the task [26]. However, cloud-based eHealth data is insufficient. In a decentralized system, nodes are dispersed and the distributed architecture provides a robust and highly usable system as well as a fault-tolerant method that eliminates the single point of failure problem, and it is done with blockchain.

The blockchain-based searchable encryption technique was proposed in the paper [27]. The ethereum technique is demonstrated in this work. It ensures data security while simultaneously lowering the cost of data transfer.

Gordon and Catalini [28] researched how blockchain technology could help the healthcare industry. This research also identified four aspects or techniques that the healthcare industry must change to use blockchain technology. It also goes over data storage on-chain and off-chain.

The authors found that using blockchain for this area has several benefits, including decentralization, the preservation of medical records, etc [29]. Confidentiality, speed, scalability, and the potential for malicious assault (51 % attack) have all been mentioned as drawbacks of blockchain technology. The authors propose storing sensitive medical data off-chain, encrypting data to preserve secrecy, and using VPNs (Virtual Private Networks) to protect against hostile assaults as solutions to these challenges.

4. PRELIMINARIES

The preliminaries used in the proposed framework are described in this section. It explains the software platform that was utilized to create this framework. The most important for the implementation of this framework are ethereum and smart contracts.

4.1. ETHEREUM SYSTEM DESIGN

Ethereum is not just a cryptocurrency. It is a distributed platform that facilitates the development of decentralized applications using smart contracts. It supports turing complete smart contract. It is so popular for creating smart contract-based decentralized applications like healthcare applications. The operation of smart contracts using ethereum is depicted in Figure 3.

The smart contract generates code in the form of byte operations and uploads the related transaction to the blockchain. For example, consider three Nodes: Node 1, Node 2, and Node 3. Node 1 starts the transaction and these transactions are validated by minor saved as block 1. If Node 2 wants to update the existing transaction, it will create a new transaction tx and the status of this transaction will be stored as block 2. When Node 3 wants to read information from the blockchain, it must be synchronized with Block 2 to see the changes caused by transaction tx.

Ethereum Virtual Machine (EVM): This made ethereum a completely distributed and decentralized computational system. It includes operations for computation and data storage. An operation performed in the EVM consumes gas. EVM Gas is a virtual fuel (ether) that powers the EVM. The gas required for a transaction is a fee for executing the code of the transaction. The gas consumed during transaction execution is transferred to the account of a miner. Miners are rewarded for the computational power invested in the execution of transaction code, such as the crypto currency ether [30, 31].

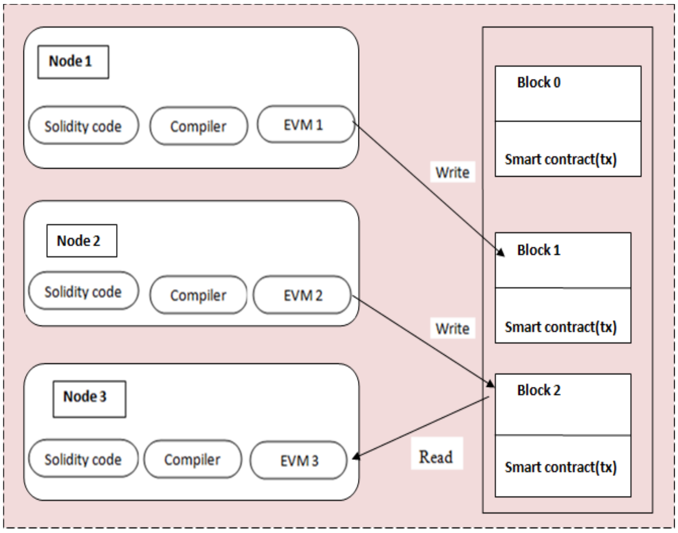


Figure.3. The Ethereum mechanism with a smart contract

DApps: An application running on such a decentralized peer-to-peer network is called a DApp. DApp is an abbreviation of the term “Decentralized Application”. Many DApps have been deployed in the main ethereum network. Ethereum is open-source and very developer-friendly. The ethereum implementation helps the developers with creating, testing, and deploying their DApps.

Solidity: Smart contracts are a set of instructions written in the solidity programming language and compiled to the Ethereum Virtual Machine (EVM), which is deployed to the blockchain via a local ethereum node. It is used to complete a specific task in the blockchain network. These little scripts are kept on each blockchain network's ledger. Typically a user can view the whole working process in a web browser and the smart contract code running on the blockchain. This configuration is called a distributed application, commonly termed “Dapp”.

4.2. SMART CONTRACTS

The phrase "smart contracts" was coined for the first time by Nick Szabo [32]. They are computer programs that execute automatically when particular conditions in the system are met. They are used to transfer any type of value between blockchain peers [33, 34]. A smart contract is a concept that supports the logic of business. Smart contracts are created in the Solidity programming language [35]. To apply for health insurance, the patient must go through a lengthy approval process. When a smart contract is used, the patient profile is automatically activated when the insurance policy is started.

5. SYSTEM DESIGN AND ARCHITECTURE

The proposed framework is implemented using the ethereum platform and its dependencies. This section contains the proposed architecture in detail.

The architecture consists of three layers: the user layer, the blockchain layer, and the implementation layer, as shown in Figure 4. These layers combine to provide the framework for the entire system, and our system will continue to function.

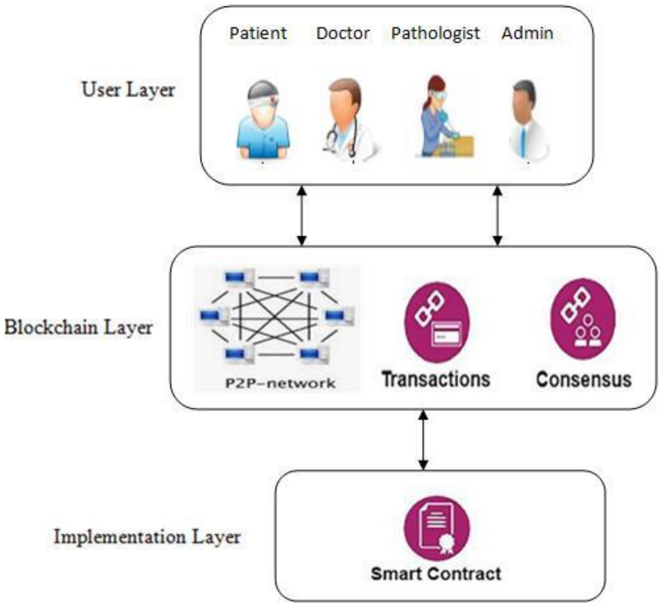


Figure.4. System Design of the Proposed Framework

5.1. USER LAYER

In the proposed framework, users include patients, doctors, administrators, and pathologists. A user can be identified on the system by his roles. These users' primary responsibility would be to interface with the system and execute basic functions such as creating, reading, and updating medical records. Users would utilize a browser to access the system's capabilities, which we refer to as a “DApp browser” in technical terms since it contains the DApp's GUI. The graphical user interface (GUI) contains all of the functionality that a given user has access to. This GUI could be used by the user to communicate with the blockchain layer, depending on their work.

5.2. BLOCKCHAIN LAYER

This layer consists of a mechanism that allows a user to communicate with a blockchain-based DApp.

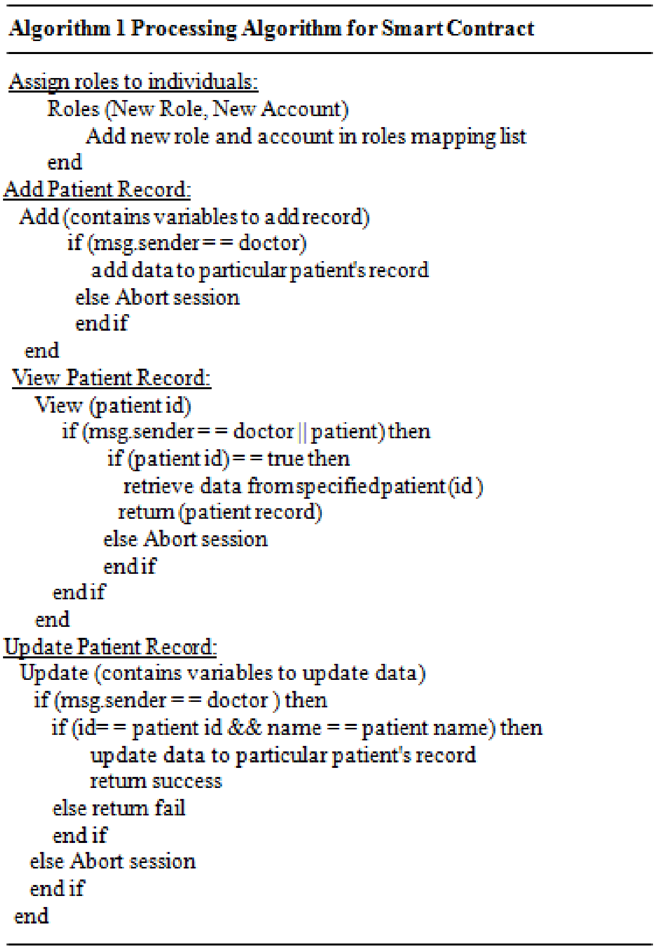
Peer-to-peer network: Ethereum blockchain uses the peer-to-peer network. Without a central server, blockchain operates on a peer-to-peer network over the internet. In this distributed blockchain network, all the connected nodes have equal rights to use this technology.

Transactions: The transactions on the blockchain are the records of events. They are pieces of information that a user might broadcast to another user or simply save for later use.

Consensus mechanism: Blockchain technology follows a specific consensus mechanism for transactions to be completed and computed. To do this, some consensus techniques are required. The Proof of Work (PoW) consensus algorithm is used by the ethereum blockchain.

5.3. IMPLEMENTATION LAYER

The system was implemented by using the smart contract. Smart contracts are an essential element of DApps because they are utilized to carry out basic tasks. These contracts are used to grant DApp users access. The smart contract processing algorithm is depicted in Algorithm 1.



Algorithm 1 Processing Algorithm for Smart Contract

```
Assign roles to individuals:
    Roles (New Role, New Account)
        Add new role and account in roles mapping list
    end
Add Patient Record:
   Add (contains variables to add record)
        if (msg.sender = = doctor)
            add data to particular patient's record
         else Abort session
         end if
   end
View Patient Record:
     View (patient id)
        if (msg.sender = = doctor || patient) then
            if (patient id) = = true then
               retrieve data from specified patient (id )
              return (patient record)
            else Abort session
            end if
       end if
     end
Update Patient Record:
   Update (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
```

The default role of admin is assigned to the first block ethereum address as admin deploys the smart contract. On the ethereum blockchain, each patient who registers will be assigned a new ethereum block address. Every new patient is assigned a unique hash code and a unique patient identity to ensure security and uniqueness.

In the ethereum blockchain, transactions are described as functions defined in a smart contract that is executed and altered state. Smart contract coding necessitates the implementation of many components in terms of transactions. The Algorithm describes how the smart contract for patient records works. This algorithm contains four functions: define roles; add; view; and update records.

The define roles function is performed by the admin to add new roles and accounts in the role mapping list. The second function is to add a patient record, and it is performed by the doctor. The 'msg.sender' term is used by ethereum for identifying the address of the user. The third function is to view patient records. The system will look for the patient's records using this id. The records would be accessible to both the patient and the doctor. The fourth function is to update patient records, which is used to make any modifications to the patient's saved records. To ensure that only authenticated users have access to this function.

6. APPLICATION DETAILS

In this section, we present an overview of the implementation of our proposed architecture. First, we'll go over the flow of the application. A new patient profile is established whenever a new patient enters.

6.1. FLOW OF THE APPLICATION

Flow diagram of the application is shown in Figure 5. In this project, a total of 3 users are available: patients, doctors, and lab persons.

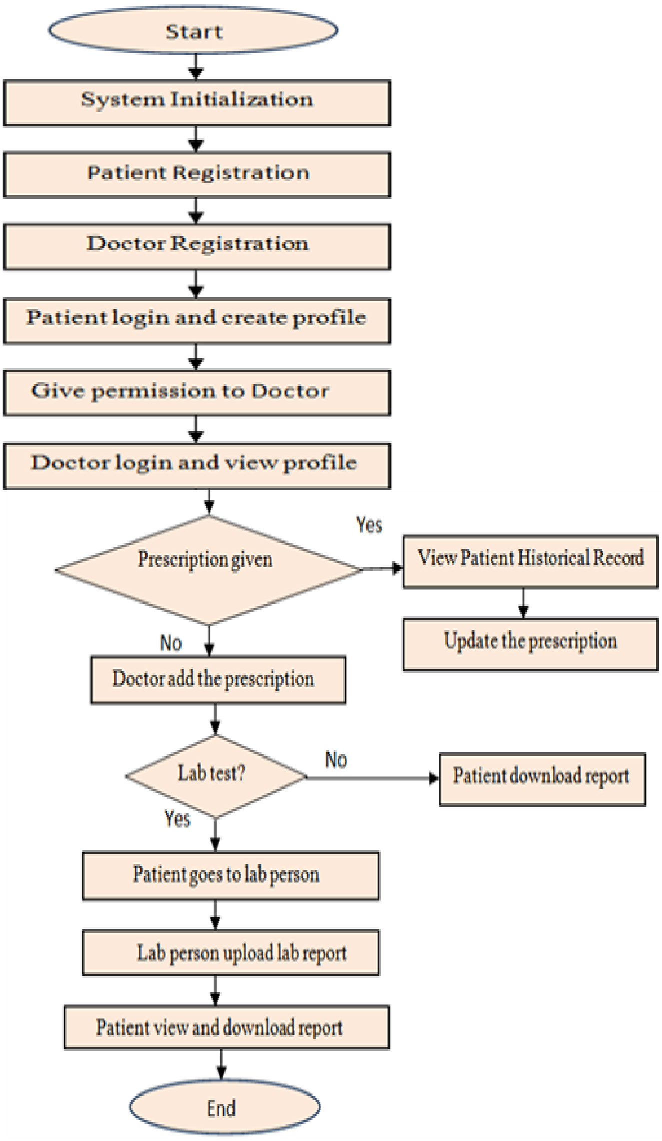

Start
System Initialization
Patient Registration
Doctor Registration
Patient login and create profile
Give permission to Doctor
Doctor login and view profile
Prescription given
Yes
View Patient Historical Record
Update the prescription
No
Doctor add the prescription
Lab test?
No
Patient download report
Yes
Patient goes to lab person
Lab person upload lab report
Patient view and download report
End

Figure.5. Flow diagram of the application

(i) Patients will build a profile and grant access to doctors after registering with the application.
(ii) Doctors will create an account with the application, log in, and gain access to all of the patients' records who have been permitted to this doctor.

(iii) The prescription will be added to the patient's profile by the doctor.
(iv) After logging into the application, the lab person will upload patient reports.
(v) Patients can log in and download or see reports using filters such as "All Reports" or "Reports by Date".

6.2. TECHNICAL SPECIFICATIONS

The technical specifications necessary for code implementation are listed in Table 1.

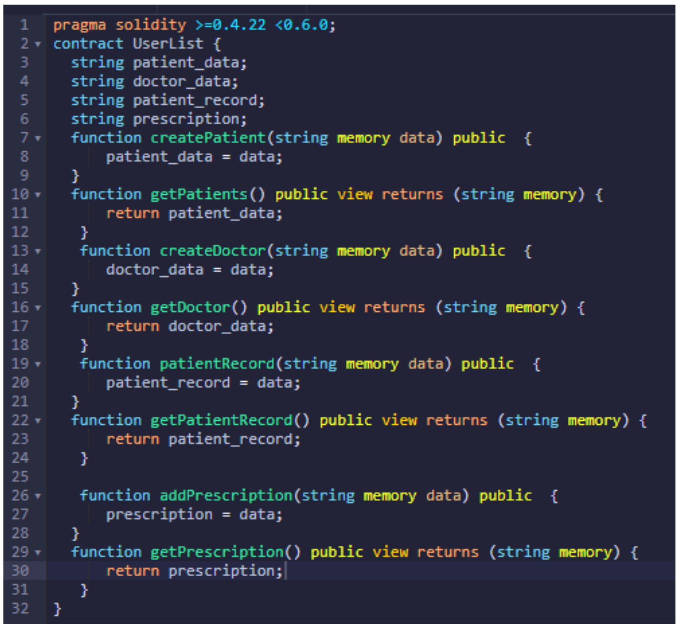
Blockchain Platform	Ethereum
Programming Language	Solidity
IDE	Remix.ethereum.org
Deployment Server	JavaScript Virtual Machine

Table.1. Technical specifications used in Implementation

Ethereum is a blockchain-based network. Solidity is a programming language in which JavaScript is encapsulated. Remix is used to write and compile smart contracts, which is a Solidity online text editor.

7. OUTPUT

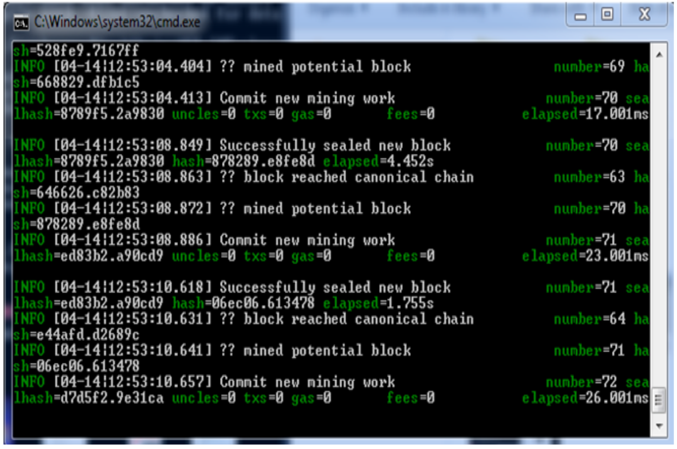
Some implementation steps and screen shorts are shared in this section. To store details we are using the blockchain ethereum tool and smart contract written in solidity program as shown in Figure 6.



```
pragma solidity >=0.4.22 <0.6.0;
contract UserList {
  string patient_data;
  string doctor_data;
  string patient_record;
  string prescription;
  function createPatient(string memory data) public  {
      patient_data = data;
  }
  function getPatients() public view returns (string memory) {
      return patient_data;
   }
   function createDoctor(string memory data) public  {
      doctor_data = data;
  }
  function getDoctor() public view returns (string memory) {
      return doctor_data;
   }
   function patientRecord(string memory data) public  {
      patient_record = data;
  }
  function getPatientRecord() public view returns (string memory) {
      return patient_record;
   }

   function addPrescription(string memory data) public  {
      prescription = data;
  }
  function getPrescription() public view returns (string memory) {
      return prescription;
   }
}
```

Figure.6. Solidity program

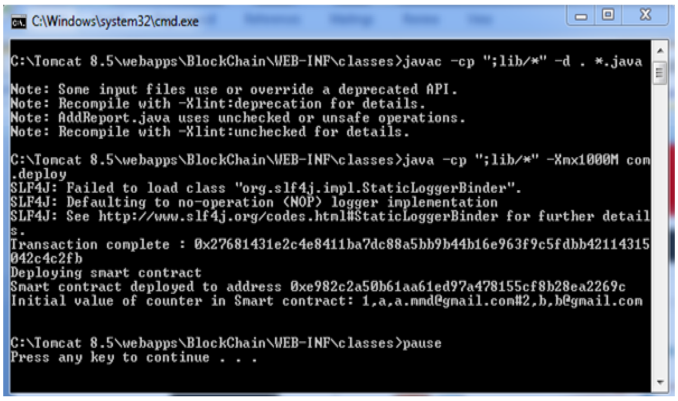
Initially, we have to start the blockchain ethereum server as shown in Figure 7.



```
sh=528fe9.7167ff
INFO [04-14|12:53:04.404] ?? mined potential block                  number=69 ha
sh=668829.dfb1c5
INFO [04-14|12:53:04.413] Commit new mining work                    number=70 sea
lhash=8789f5.2a9830 uncles=0 txs=0 gas=0       fees=0          elapsed=17.001ms

INFO [04-14|12:53:08.849] Successfully sealed new block             number=70 sea
lhash=8789f5.2a9830 hash=878289.e8fe8d elapsed=4.452s
INFO [04-14|12:53:08.863] ?? block reached canonical chain          number=63 ha
sh=646626.c82b83
INFO [04-14|12:53:08.872] ?? mined potential block                  number=70 ha
sh=878289.e8fe8d
INFO [04-14|12:53:08.886] Commit new mining work                    number=71 sea
lhash=ed83b2.a90cd9 uncles=0 txs=0 gas=0       fees=0          elapsed=23.001ms

INFO [04-14|12:53:10.618] Successfully sealed new block             number=71 sea
lhash=ed83b2.a90cd9 hash=06ec06.613478 elapsed=1.755s
INFO [04-14|12:53:10.631] ?? block reached canonical chain          number=64 ha
sh=e44afd.d2689c
INFO [04-14|12:53:10.641] ?? mined potential block                  number=71 ha
sh=06ec06.613478
INFO [04-14|12:53:10.657] Commit new mining work                    number=72 sea
lhash=d7d5f2.9e31ca uncles=0 txs=0 gas=0       fees=0          elapsed=26.001ms
```

Figure.7. Blockchain ethereum server initializing

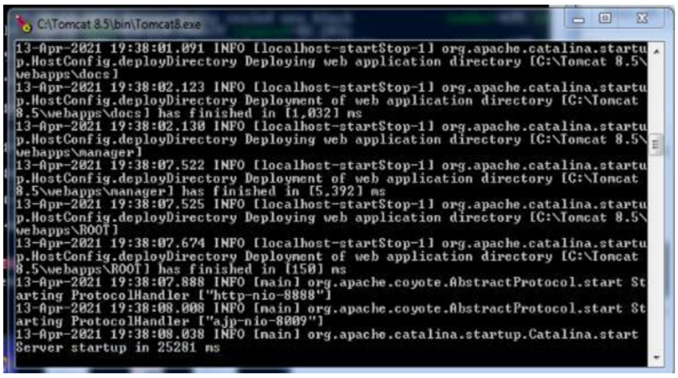
After that, we start the blockchain storage, and after running this file, we get the message as the smart contract deployed successfully, as shown in Figure 8.



```
C:\Tomcat 8.5\webapps\BlockChain\WEB-INF\classes>javac -cp ";lib/*" -d . *.java

Note: Some input files use or override a deprecated API.
Note: Recompile with -Xlint:deprecation for details.
Note: AddReport.java uses unchecked or unsafe operations.
Note: Recompile with -Xlint:unchecked for details.

C:\Tomcat 8.5\webapps\BlockChain\WEB-INF\classes>java -cp ";lib/*" -Xmx1000M com
.deploy
SLF4J: Failed to load class "org.slf4j.impl.StaticLoggerBinder".
SLF4J: Defaulting to no-operation (NOP) logger implementation
SLF4J: See http://www.slf4j.org/codes.html#StaticLoggerBinder for further detail
s.
Transaction complete : 0x27681431e2c4e8411ba7dc88a5bb9b44b16e963f9c5fdbb42114315
042c4c2fb
Deploying smart contract
Smart contract deployed to address 0xe982c2a50b61aa61ed97a478155cf8b28ea2269c
Initial value of counter in Smart contract: 1,a,a.mmd@gmail.com#2,b,b@gmail.com


C:\Tomcat 8.5\webapps\BlockChain\WEB-INF\classes>pause
Press any key to continue . . .
```

Figure.8. Smart Contract deployed successfully

After that, I will start the tomcat server as shown in Figure 9.



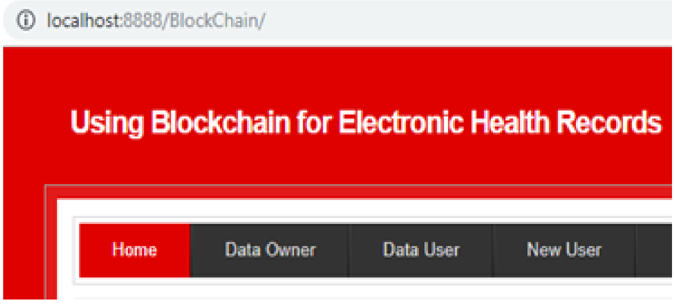
```
13-Apr-2021 19:38:01.091 INFO [localhost-startStop-1] org.apache.catalina.startu
p.HostConfig.deployDirectory Deploying web application directory [C:\Tomcat 8.5\
webapps\docs]
13-Apr-2021 19:38:02.123 INFO [localhost-startStop-1] org.apache.catalina.startu
p.HostConfig.deployDirectory Deployment of web application directory [C:\Tomcat
8.5\webapps\docs] has finished in [1,032] ms
13-Apr-2021 19:38:02.130 INFO [localhost-startStop-1] org.apache.catalina.startu
p.HostConfig.deployDirectory Deploying web application directory [C:\Tomcat 8.5\
webapps\manager]
13-Apr-2021 19:38:07.522 INFO [localhost-startStop-1] org.apache.catalina.startu
p.HostConfig.deployDirectory Deployment of web application directory [C:\Tomcat
8.5\webapps\manager] has finished in [5,392] ms
13-Apr-2021 19:38:07.525 INFO [localhost-startStop-1] org.apache.catalina.startu
p.HostConfig.deployDirectory Deploying web application directory [C:\Tomcat 8.5\
webapps\ROOT]
13-Apr-2021 19:38:07.674 INFO [localhost-startStop-1] org.apache.catalina.startu
p.HostConfig.deployDirectory Deployment of web application directory [C:\Tomcat
8.5\webapps\ROOT] has finished in [150] ms
13-Apr-2021 19:38:07.888 INFO [main] org.apache.coyote.AbstractProtocol.start St
arting ProtocolHandler ["http-nio-8888"]
13-Apr-2021 19:38:08.008 INFO [main] org.apache.coyote.AbstractProtocol.start St
arting ProtocolHandler ["ajp-nio-8009"]
13-Apr-2021 19:38:08.038 INFO [main] org.apache.catalina.startup.Catalina.start
Server startup in 25281 ms
```

Figure.9. Tomcat server startup

Users can view the whole proposed framework on the DApp browser. Open the browser and enter the localhost URL to get the homepage shown in Figure 10.

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

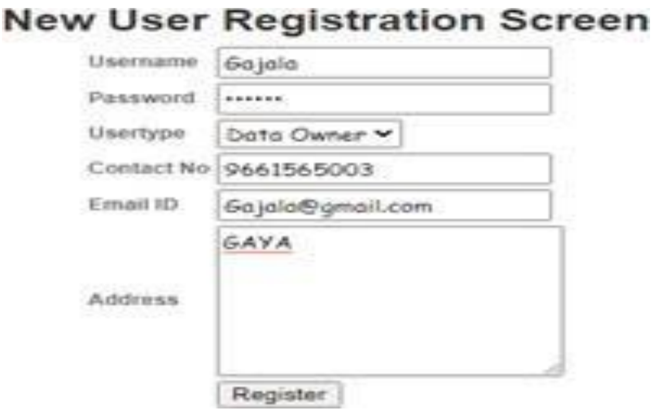


localhost:8888/BlockChain/
Using Blockchain for Electronic Health Records
Home
Data Owner
Data User
New User

Figure.10. Web app index page loading

There are the following steps for the successful application of the proposed framework.

(i) Patient Registration: After clicking on `New User' in above figure 10, I am adding here one patient detail and DataOwner will be considered as patient shown in Figure 11.



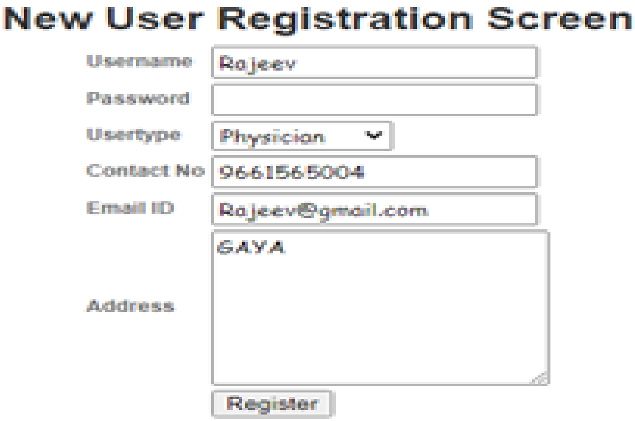
New User Registration Screen

Username: Gajala
Password: ••••••
Usertype: Data Owner
Contact No: 9661565003
Email ID: Gajala@gmail.com
Address: GAYA

Figure.11. Patient Registration

Patient input his/her details using a new block ethereum address.

(ii) Doctor Registration: Now go back to the 'New User' link again and add one doctor. I am adding one doctor's details and selected user type as 'Physician' as shown in Figure 12.

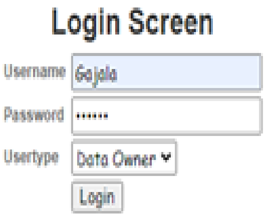


New User Registration Screen

Username: Rajeev
Password:
Usertype: Physician
Contact No: 9661565004
Email ID: Rajeev@gmail.com
Address: GAYA

Figure.12. Doctor Registration

(iii) Patient login: Now click on 'Data Owner' to login as a patient as shown in Figure 13.

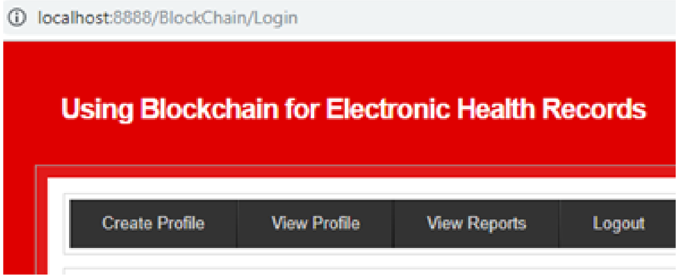


Login Screen

Username: Gajala
Password: ••••••
Usertype: Data Owner

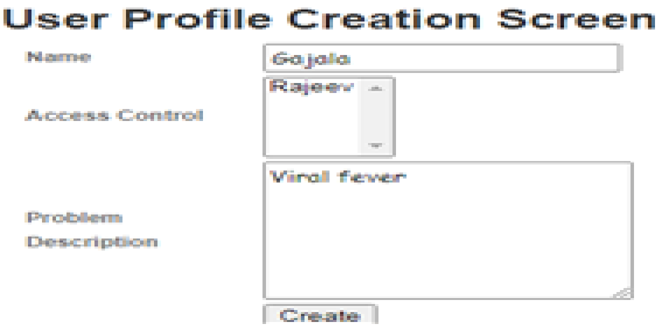
Figure.13. Patient login

After logging in, we will get the below screen.



localhost:8888/BlockChain/Login
Using Blockchain for Electronic Health Records
Create Profile
View Profile
View Reports
Logout

(iv) Patient Profile Creation:
In the above screen, click on the 'Create Profile' link and add profile details as shown in Figure 14.



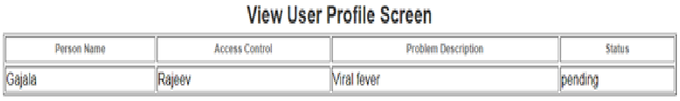
User Profile Creation Screen

Name: Gajala
Access Control: Rajeev
Problem Description: Viral fever

Figure.14. Patient Profile Creation

The patient will add his disease details and give access permission to the doctor by selecting the doctor's name from the drop-down list.

(iv) View profile: After adding disease details, we got a message as a profile was created successfully and now we click on the 'View Profile' link to get details as shown in Figure 15.



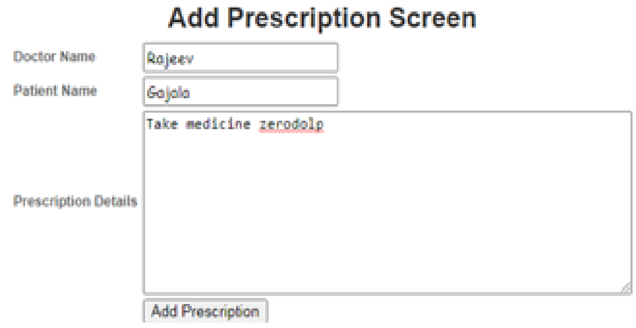
View User Profile Screen

Person Name	Access Control	Problem Description	Status
Gajala	Rajeev	Viral fever	pending

Figure.15. View Patient Profile

In Figure 15, I can see all the details, and in the last column, I got the message pending, which means no doctor has given any prescription. Now log out and log in as a doctor to give a prescription to this patient.

(v) Add Prescription: I logged in as a doctor and clicked on the "View Medical Profile" link to get all patient records. After that, the doctor will click on the 'Add Prescription' link to give a prescription to the patient as shown in Figure 16.

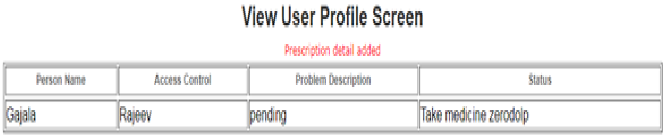


Add Prescription Screen

Doctor Name	Rajeev
Patient Name	Gajala
Prescription Details	Take medicine zerodolp

Figure.16. Doctor added prescription

(vi) View Prescription: The patient can view the prescription details as shown in Figure 17. If a test is mentioned in the prescription, then go to the lab for a test.



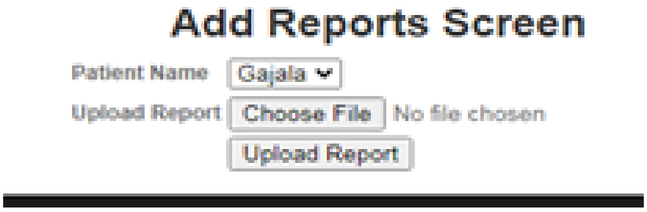
View User Profile Screen

Prescription detail added

Person Name	Access Control	Problem Description	Status
Gajala	Rajeev	pending	Take medicine zerodolp

Figure.17. Patient view prescription added by the Doctor

(vii) Pathologist login: Now Pathologist login to upload the report as shown in Figure 18. The lab person will select a patient's name and then upload a lab report.

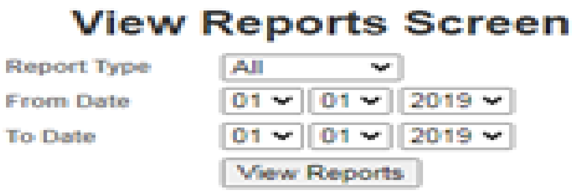


Add Reports Screen

Patient Name	Gajala
Upload Report	Choose File No file chosen

Figure.18. Login as a lab person and upload the report

(viii) View and download the report: Now patients can log in and access reports. The patient can select either option 'All' to get all reports or select all reports between two dates as shown in Figure 19.

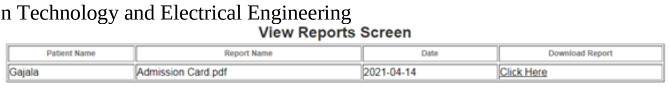


View Reports Screen

Report Type	All		
From Date	01	01	2019
To Date	01	01	2019

Figure.19. View report

The patient can click on the 'Click Here' link to download the report as shown in Figure 20.



View Reports Screen

Patient Name	Report Name	Date	Download Report
Gajala	Admission Card.pdf	2021-04-14	Click Here

Figure.20. Download report

8. CONCLUSION

Blockchain, an immutable distributed ledger technology, may be used to guarantee security and integrity for healthcare data management. The proposed blockchain-based framework describes how medical processes can be streamlined and illustrates the approaches used for establishing a blockchain-based reliable medical ecosystem. Smart contracts are proposed as a new solution to medical record administration. We have implemented blockchain technology in health data management and sharing systems. A patient-centric strategy has been created to provide a single copy of trusted health records that can be shared among healthcare organizations. The goal of this study is to suggest a practical solution and to put it into implementation. It is a complete code deployment research paper that includes all aspects of the technique and output. In the future, this solution could be expanded to make a full blockchain-based healthcare system that includes more healthcare stakeholders.

REFERENCES

[1] Samad, A., Shuaib, M., & Beg, M. R. (2017) "Monitoring of Military Base Station using Flooding and ACO Technique: An Efficient Approach", International Journal of Computer Network and Information Security, Vol. 9, No. 12, pp.36-44.

[2] Raghuvanshi, A., Singh, U. K., Shuaib, M., & Alam, S. (2021) "An investigation of various applications and related security challenges of Internet of things", *Materials Today: Proceedings.*, https://doi.org/10.1016/J.MATPR.2021.01.821

[3] Bigini, G., Freschi, V. and Lattanzi, E. (2020) "A review on blockchain for the internet of medical things: Definitions, challenges, applications, and vision" Future Internet, Vol. 12, No. 12, pp.1-16.

[4] Bokhari, D.M. and Alam, S. (2013) "BSF-128: A New Synchronous Stream Cipher Design"

[5] Shuaib, M., Alam, S. and Daud, S.M. (2021) "Improving the Authenticity of Real Estate Land Transaction Data Using Blockchain-Based Security Scheme", In book: Advances in Cyber Security, Second International Conference, ACeS 2020, Penang, Malaysia Springer, Singapore, Vol. 1347, pp.3-10.

[6] Bokhari, M.U., Alam, S. and Hasan, S.H. (2014) "A Detailed Analysis of Grain family of Stream Ciphers", International Journal of Computer Network & Information Security, Vol. 6, No. 6.

[7] Nakamoto, S. (2008) “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://bitcoin.org/bitcoin.pdf

[8] Shuaib, M., Alam, S., Shabbir Alam, M. and Shahnawaz Nasir, M. (2021) “Self- sovereign identity for healthcare using blockchain”, Materials Today: Proceedings, https://doi.org/10.1016/j.matpr.2021.03.083

[9] Aguiar, E.J., Faial, B.S., Krishnamachari, B., and Ueyama, J. (2020) “A Survey of Blockchain-Based Strategies for Healthcare”, ACM Computing Surveys (CSUR), Vol. 53, pp.1-27.

[10] Yue, L., Nortey, R.N., Adjeisah, M., Agbedanu, P.R. and Lui, X. (2019) “Blockchain Enabled Privacy Security Module for Sharing Electronic Health Records (EHRs)”, International Journal of Computer and Communication Engineering, Vol. 8, No. 4, pp.155-168.

[11] Ozair, F., Jamshed, N., Sharma, A. and Aggarwal, P. 2015 “Ethical issues in electronic health records: A general overview”, Perspectives in Clinical Research, Vol. 6, No. 2, pp.73-76.

[12] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016) “MedRec: Using Blockchain for Medical Data Access and Permission Management”, in 2nd International Conference on Open and Big Data (OBD), pp.25-30.

[13] Dagher, G.G., Mohler, J., Milojkovic, M. and Marella, P.B. (2018) “Ancile: Privacy-Preserving Framework for Access Control and Interoperability of Electronic Health Records Using Blockchain Technology”, Sustainable Cities and Society, Vol. 39, pp.283-297.

[14] Zhang, P., White, J., Schmidt, D. C., Lenz, G. and Rosenbloom, S. T. (2018) “FHIRChain: Applying Blockchain to securely and Scalably Share Clinical Data”, Computational and structural biotechnology journal, Vol. 16, pp.267-278.

[15] Rouhani, S., Butterworth, L., Simmons, A.D., Humphery D.G. and Deters, R. (2018) “MediChainTM: A Secure Decentralized Medical Data Asset Management System”, 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp.1533-1538.

[16] Huynh, T.T., Nguyen, T.D. and Tan, H. (2019) “A Survey on Security and Privacy Issues of Blockchain Technology”, International Conference on System Science and Engineering (ICSSE), pp.362-367.

[17] Rouhani, S. and Deters, R. (2019) “Security, Performance, and Applications of Smart Contracts: A Systematic Survey”, IEEE Access, Vol. 7, pp.50759- 50779.

[18] Johnson, M., Jones, M., Shervey, M., Dudley, J.T. and Zimmerman, N. (2019) “Building a Secure Biomedical Data Sharing Decentralized App (DApp): Tutorial”, Journal of Medical Internet Research, Vol. 21, pp.155-168.

[19] Jadhav, V.D. and Moosafintavida, S. (2020) “Blockchain in Healthcare Industry and Its Application and Impact on Covid 19 Digital Technology Transformation”, Mukt Shabd Journal, Vol. IX, No. IX, pp.479-487.

[20] Qian, H., Li, J., Zhang, Y. and Han, J. (2015) “Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation”, International Journal of Information Security, Vol. 14, No.6, pp.487-497.

[21] Shi, Y., Zheng, Q., Liu, J. and Han, Z. (2015) “Directly revocable key-policy attribute-based encryption with verifiable ciphertext delegation”, Information Sciences, Vol. 295, pp.221-231.

[22] Shen, W., Qin, J., Yu, J., Hao, R. and Hu, J. (2018) “Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage”, IEEE Transactions on Information Forensics and Security, Vol. 14, No. 2, pp.331-346.

[23] Sudarsono, A., Yuliana, M. and Darwito, H.A. (2017) “A secure data sharing using identity-based encryption scheme for e-healthcare system”, in 2017 3rd International Conference on Science in Information Technology (ICSITech), pp.429-434.

[24] Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M.D. and He, J. (2018) “BlocHIE: A Blockchain-Based Platform for Healthcare Information Exchange”, IEEE International Conference on Smart Computing (SMARTCOMP), pp.49-56.

[25] Tanwar, S., Parekh, K. and Evans, R. (2020) applications (2020) “Blockchain-based electronic healthcare record system for healthcare 4.0 applications”, Journal of Information Security and Applications, Vol. 50.

[26] Alam, S., Shuaib, M. and Samad, A. (2019) “A Collaborative Study of Intrusion Detection and Prevention Techniques in Cloud Computing”, in Lecture Notes in Networks and Systems, Vol. 55, pp.231-240.

[27] Chen, L., Lee, W.K., Chang, C., Choo, K., & Zhang, N. (2019) “Blockchain based searchable encryption for electronic health record sharing”, Future Generation Computer Systems, Vol. 95, pp.420-429.

[28] Gordon, W.J. and Catalini, C. (2018) “Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability”, Computational and Structural Biotechnology Journal, Vol. 16, pp.224-230.

[29] Kuo, T., Kim, H. and Ohno-Machado, L. (2017) "Blockchain distributed ledger technologies for biomedical and health care applications", Journal of the American Medical Informatics Association: JAMIA, Vol. 24, pp.1211-1220.

[30] Chohan, U.W. (2017) "Cryptocurrencies: A Brief Thematic Review", IRPN: Innovation and Finance (Topic).

[31] Gupta, S. and Sadoghi, M. (2019) "Blockchain Transaction Processing", Encyclopedia of Big Data Technologies.

[32] Szabo, N. (1997) "Formalizing and securing relationships on public networks", First Monday, Vol. 2, No. 9. [Online].Available: https://firstmonday.org/article/view/548/469

[33] Christidis, K. and Devetsikiotis, M. (2016) "Blockchains and Smart Contracts for the Internet of Things", IEEE Access, Vol. 4, pp.2292-2303.

[34] Wang, S., Yuan, Y., Wang, X., Li, J., Qin, R. and Wang, F. (2018) "An Overview of Smart Contract: Architecture, Applications, and Future Trends", IEEE Intelligent Vehicles Symposium (IV), pp.108-113.

[35] Atzei, N., Bartoletti, M. and Cimoli, T. (2017) "A Survey of Attacks on Ethereum Smart Contracts (SoK)", POST.

AUTHOR PROFILES

Gajala Praveen is pursuing her PhD in the Department of Computer Science at the Central University of South Bihar, Gaya, India. She received her M.Tech degree in Computer Engineering from Jamia Millia Islamia (a central university), New Delhi, India. Her research interests include blockchain technology, natural language processing, and distributed computing. She has published research papers in international journals, conference proceedings, and book chapters.

Piyush Kumar Singh is an Assistant Professor in the Department of Computer Science, Central University of South Bihar, Gaya, India. His research field interests are in image processing, wavelets, and blockchain technology. He has published research papers in national and international journals, conference proceedings, and book chapters.

Prabhat Ranjan is an Assistant Professor in the Department of Computer Science, Central University of South Bihar, Gaya, India. His research field interests are in big data, distributed systems, software engineering, and blockchain technology. He has published research papers in national and international journals, conference proceedings, and book chapters.