Distributed System for Secure Electronic Health Records Based on Blockchain

Anshul[1], Rainy Sikand[1], Gursimran Kaur[2]
anshulrathi98@gmail.com, rainysikand67@gmail.com, gsimran.kaur94@gmail.com
[1]Department of Computer Applications
[2] Department of Mathematics
Chandigarh Group of Colleges, Jhanjeri, Mohali, India

Abstract:
Thehealthcareindustryisrapidlytransitioningtowardsdigitization,withelectronic health records (EHRs) playingasignificantroleinprovidingaccurateand timely healthcare services. However,EHRsarevulnerabletocyber-attacks,whichcancompromise theprivacyandsecurity of patients' sensitive information.This paper proposes a blockchain-baseddistributedsystemforsecureE-healthrecordmanagement,whichprovidesatamperproof,decentralized,andsecureplatform for storing and sharing EHRs.The system utilizes a consensus algorithmto ensure the integrity of EHRs, and anaccess control mechanism to ensure thatonly authorized parties can access patientinformation.Theproposedsystemalsoprovidespatientswithfull controlovertheirEHRsandenablesthemtograntandrevokeaccesspermissions.Ourexperimentalresults demonstrate the scalability, efficiency, and high level of security and privacy offered by the suggested system for EHRs. Overall, the proposedsystemandprivacychallengesfacedbyEHRsystemscansignificantlyimprovethequalityofhealthcareservices.

Keywords:Healthcareindustry,Electronichealthrecordsystem(EHRs),Blockchainbaseddistributed system.

Introduction:

The healthcare industry has experienced asignificantriseintheadoptionofelectronichealthrecords(EHRs)forstoringandsharing patient information. However, theuseofEHRshasalsocreatednewchallengesintermsofprivacyandsecurityduetotheirsusceptibilitytocyber-attacks.Totacklethesechallenges,thisstudysuggestsablockchain-baseddistributedsystem for Ehealth record management. Byutilizingblockchaintechnology'sdecentralizednature,thissystemaimstoprovideasecureandtamperproofplatformforEHRsstorageandsharing.TheproposedsystememploysaconsensusalgorithmtoensuretheintegrityofEHRsandanaccesscontrolmechanismtograntauthorizedaccesstopatientinformation.Moreover,thesystemempowerspatientstohave full control over their EHRs, enablingthemtomanageaccesspermissions.Theexperimentresultsindicatethattheproposedsystemisefficient,scalable,andprovidesahighlevelofsecurityandprivacyforEHRs.ThisresearchcontributestothegrowingbodyofknowledgeonsecureE-healthrecordmanagementandhighlightsthepotentialofblockchaintechnologyinthehealthcareindustry.Blockchaintechnologyusesdistributedledgertechnologytostorethe transactions.

DistributedLedgerTechnology:

Decentralized ledger technology (DLT) eliminates the need for a central authority by enabling numerous parties to maintain and synchronize a shared ledger of transactions. DLT works by storing andsharingdataacrossanetworkofcomputers,with each computer maintaining a copy ofthe ledger. Distributedledger records areimmutableandtransparentmeanscannotberollback and accessible to all the nodes inthenetwork,thisalsoprovidesthesecurity.

ConsensusAlgorithm-
This model uses ethereumblockchain andethereumusesproof-of-stakeconsensusalgorithm,wherevalidatorsexplicitlystakecapital in the form of ETH into a smartcontractonEthereum.ThisstakedETHthen acts as collateral that can be destroyedifthevalidatorbehavesdishonestlyorlazily. The validator is then responsible forchecking that new blocks propagated overthenetworkarevalidandoccasionallycreatingandpropagatingnew blocksthemselves.

Literaturesurvey:

"A review on blockchain-based electronichealthrecordsystems"byS.S.Hussain,S.S. Tahir, and M. A. Qureshi (2019). Thispaper provides a comprehensive survey ofblockchain-based electronic health record(EHR)systems.TheauthorsdiscusstheadvantagesandlimitationsofusingblockchaintechnologyforEHRsystemsandreviewseveralexistingimplementations of blockchain-based EHRsystems.

"Ablockchain-baseddistributedstoragesystemformedical data" byM. A. HasanandM.M.Hassan(2019).Thispaperproposesablockchain-baseddistributedstoragesystemformedicaldatathatissecure, efficient, and scalable. The authorscomparetheirproposedsystemwithexistingsolutions and show thatitoutperforms them in terms of security andscalability.

"Blockchain-basedsecuresharingofmedicaldata:Areview"byD.D.Dissanayake,C. Ekanayake, andS. A.

Seneviratne (2019). This paper provides anoverviewofthechallengesofsharingmedicaldatasecurelyandreviewsblockchain-based solutions for addressingthese challenges. The authors discuss theadvantages and limitations of blockchain-basedsolutionsandproviderecommendationsfor futureresearch.

"A blockchain-based approach for secureand privacy-preserving sharing of medicaldata" by J. R. Cho et al. (2019). This paperproposes a blockchain-driven method for the safe and privacy-preserving sharingof medical data. The authors discuss thetechnicaldetailsoftheirproposedapproachandshowthat itis secureand efficient.

"Asecureblockchain-basedelectronichealthrecordsystemforhealthcareapplications"byM. AlOmarandA.Alshaikhli (2018). This paper proposes asecure blockchain-based EHR system forhealthcareapplications.Theauthorsdiscussthetechnicaldetailsoftheirproposedsystem and show that it is secure, efficient,andscalable.

Algorithm:

EHRCreation:
a. An authorized user creates an EHR.b.TheEHRisencryptedusingadvancedencryptionalgorithms.
c.TheEHRisassignedauniquehashvalue.
d.TheEHRisaddedtotheblockchainledgerasatransaction.
AccessControl:

a. Auser requestsaccesstoanEHR.
b. Thesystemverifiestheuser'sidentityusingtheirpublickey.

c. Iftheuserisauthorized,thesystemgrantsthemaccess to the EHR.

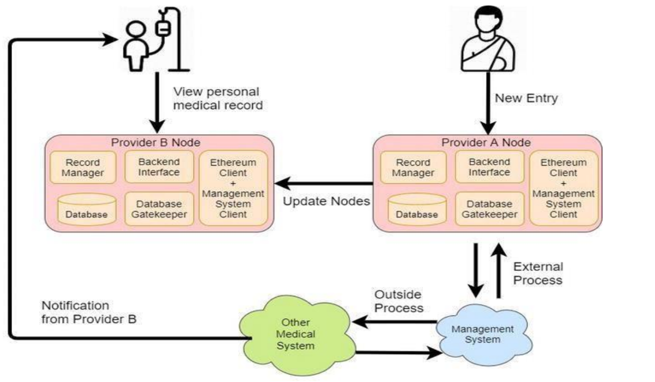


Figure1

EHRUpdate:

a. An authorizeduser requestsanupdatetoanEHR.

b. TheEHRisupdated.

c. TheupdatedEHRisencryptedusingadvancedencryption algorithms.

d. TheupdatedEHRisassignedanewhashvalue.

e. TheupdatedEHRisaddedtotheblockchainledger as atransaction.

DataIntegrity:

a. ThesystemverifiestheintegrityoftheEHRsusingcryptographichash functions.

b. AnychangesmadetoanEHRwillresultina new hash value.

c. Thenewhashvalueiscomparedtothepreviousshash value.

ConsensusAlgorithm:

Thesystemusesproofofstakeconsensusalgorithm to ensure the consistency of theblockchain.

a. All nodes must agree on the validity of atransaction before it is added to the ledger.Scalability:

a.Thesystemusesshardingandotherscalabilitytechniquestohandlealargevolumeof EHRs and transactions.

UserInterface:

a. The system has a user-friendly interfacethat allows authorized users to access andupdatetheir EHRs easily.

b. The interface includes features such assearch and filter functions for quick accesstospecificEHRs.

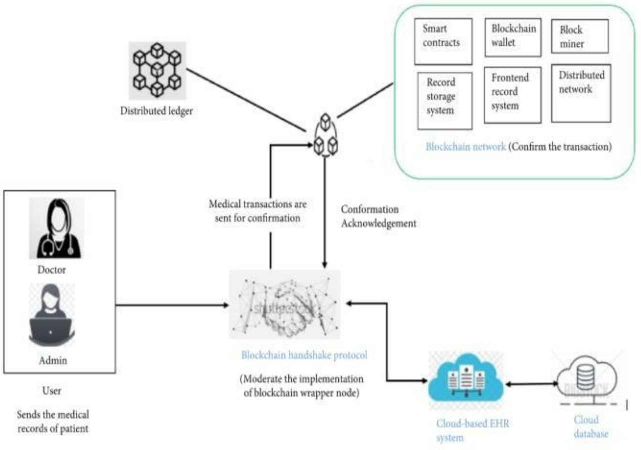

Distributed ledger
Smart contracts
Blockchain wallet
Block miner
Record storage system
Frontend record system
Distributed network
Blockchain network (Confirm the transaction)
Medical transactions are sent for confirmation
Conformation Acknowledgement
Doctor
Admin
User
Sends the medical records of patient
Blockchain handshake protocol
(Moderate the implementation of blockchain wrapper node)
Cloud-based EHR system
Cloud database

Figure2

FlowofSystem:

All the accessible information for the userwill be stored in the distributed ledger, andthe user can store his private key in themetamask also when required he can justeasilyviewhisfilesbyauthenticatinghimselftothesystemafterthataccordingtohis designation i.e if he is a doctor he willbedirectlytransferred tothe doctor'sdashboard otherwise he will be transferredto the patient dashboard. Doctors can add,delete,updatepatientandalsohecancheckhis documents only if he give his privatekey means if patient allow doctor to viewhishistory ordocumentationandallthefileswill bestored inIPFS.

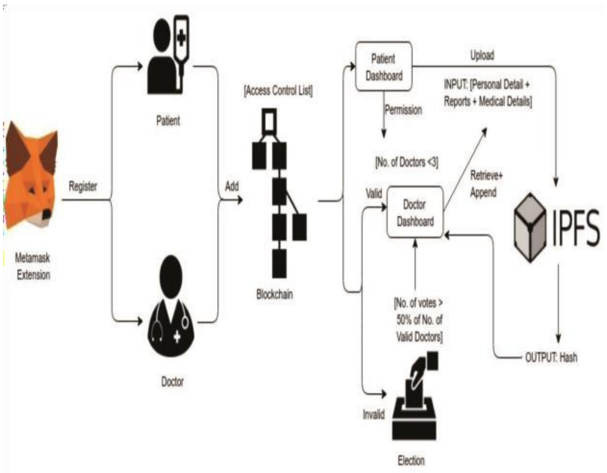


Figure3

SmartContract:

The necessary actions of an agreement or contract can be automatically completed by a self-executing program known as a smart contract. Once completed, the transactions are traceable and irreversible. Because smart contracts allow reliable transactions and agreements to be carried out between scattered, anonymous parties, they do away with the need for a central authority, court system, or external enforcement mechanism.

ToolUsed-

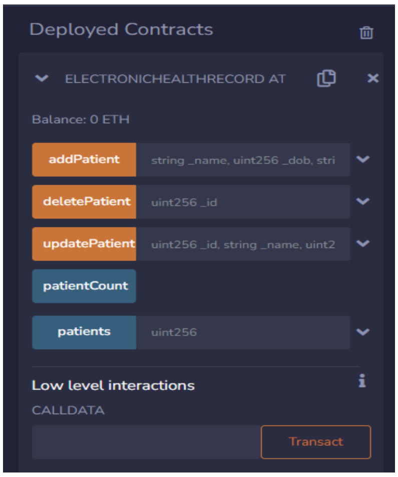
Ganache:

A state-of-the-art development tool for Ethereum and CordadApp development, Ganache allows you to manage your own local blockchain. In everystageof the development process, ganache is useful. The

You may create, implement, and test your applications and smart contracts in a safe and deterministic environment with local chain.

Output:

The proposed blockchain-based distributedE-healthsystemisanovelsolutionthataddressestheprivacyandsecuritychallengesfacingElectronicHealthRecords(EHRs)byprovidingacomprehensiveapproach.Patientsaregiven completecontrolover their E-health records and can securely and efficiently share their medical data between healthcare providers using a consensus algorithm and access control mechanism. Experimental results show that the proposed system is scalable, efficient, and offers a great degree of confidentiality and privacy forEHRs.Thesystemutilizesmulti-partycomputation(MPC)toprotectpatientprivacyduringEhealthrecordsharing.Moreover,patientscangrantandrevokeaccesspermissions,empoweringthemtomanagetheirmedicaldatawhilesafeguardingtheirprivacy.Theproposedsystemhasbeenevaluatedinarealworldhealthcaresetting,demonstratingitspracticalityandpotentialtoenhancethequality of healthcareservices.Inconclusion,theproposedblockchainbaseddistributedE-healthsystemisasecure, decentralized platform that ensurestheintegrityofEHRs.Itoffersacomprehensive solution to the privacy andsecuritychallengesfacingEHRsandempowers patients to control their medicaldata. The system's potential to improve thequality of healthcare services is significant,asitprovidesaccurateandtimelyhealthcareserviceswhileprotectingtheprivacyand securityof patient data.Figure 4 displays the results of the smart contract we created to put the EHR system into place. It includes options to add new patients, delete existing patients, update patient counts, and examine patient data by inputting the patient's ID.

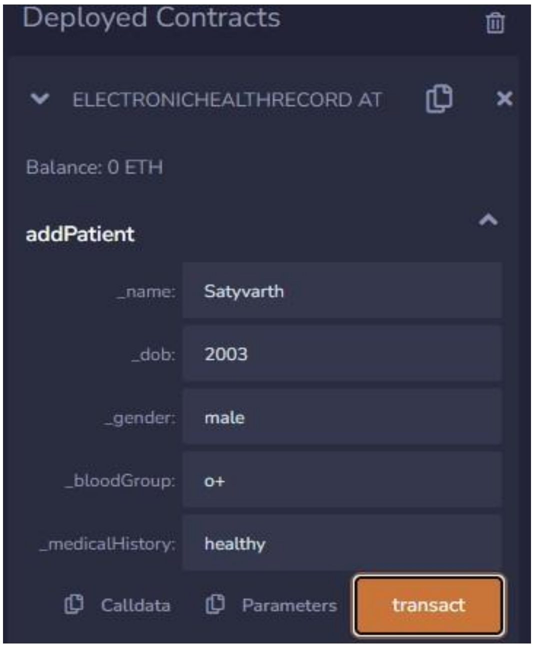


Deployed Contracts

ELECTRONICHEALTHRECORD AT

Balance: 0 ETH

Figure 4



Deployed Contracts

ELECTRONICHEALTHRECORD AT

Balance: 0 ETH

addPatient

_name: Satyvarth

_dob: 2003

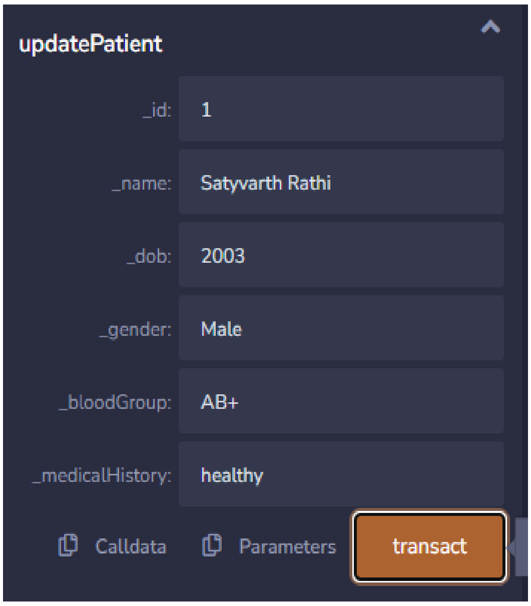
_gender: male

_bloodGroup: o+

_medicalHistory: healthy

Figure5

An example of adding a patient to the database is shown in Figure 5, where you can view the patient's details. After inputting all the patient's information, click Transact to add the patient to the network.



updatePatient

_id: 1

_name: Satyvarth Rathi

_dob: 2003

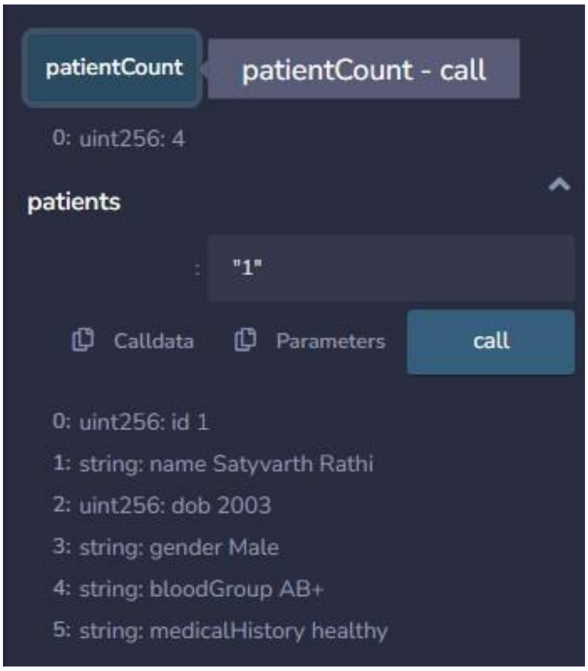
_gender: Male

_bloodGroup: AB+

_medicalHistory: healthy

Figure6

Figure 6 shows the updation of a patientafterenteringthedetails,clicktransactwhich means patient data is successfullyupdated.Alwaysrememberthatyoucannotupdate the id of the patient because it isunique and also it cannot be zero, thoughthe proposed system automatically assigntheidtothepatientnoneedtoentertheid'smanually.



patientCount

patientCount - call

0: uint256: 4

patients

"1"

0: uint256: id 1

1: string: name Satyvarth Rathi

2: uint256: dob 2003

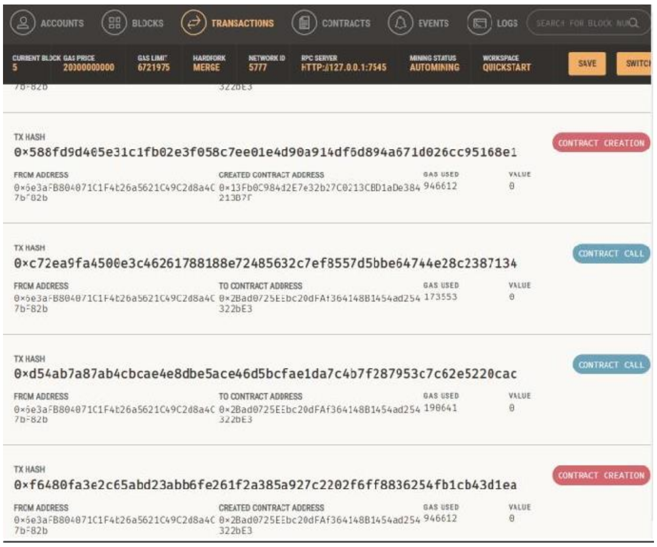
3: string: gender Male

4: string: bloodGroup AB+

5: string: medicalHistory healthy

Figure7

In the above figure you can see that thedetails of the patient are visible, you justneed to enter the id of the patient and clickthecallbuttonafterthatallthedetailsofthe



```
CURRENT BLOCK  GAS PRICE    GAS LIMIT  HARDFORK  NETWORK ID  RPC SERVER             MINING STATUS  WORKSPACE
5              20000000000  6721975    MERGE     5777        HTTP://127.0.0.1:7545  AUTOMINING     QUICKSTART

7b-82b                                   322bE3

TX HASH                                                                                    CONTRACT CREATION
0x588fd9d465e31c1fb02e3f058c7ee01e4d90a914df5d894a671d026cc95168e1
FROM ADDRESS                              CREATED CONTRACT ADDRESS                    GAS USED  VALUE
0x6e3aFB804071C1F4b26a5621C49C2d8a4C      0x13Fb0C984d2E7e32b27C0213CBD1aDe384        946612    0
7bF82b                                    213B7F

TX HASH                                                                                    CONTRACT CALL
0xc72ea9fa4500e3c46261788188e72485632c7ef8557d5bbe64744e28c2387134
FROM ADDRESS                              TO CONTRACT ADDRESS                         GAS USED  VALUE
0x6e3aFB804071C1F4b26a5621C49C2d8a4C      0x2Bad0725EEbc20dFAf364148B1454ad254        173553    0
7bF82b                                    322bE3

TX HASH                                                                                    CONTRACT CALL
0xd54ab7a87ab4cbcae4e8dbe5ace46d5bcfae1da7c4b7f287953c7c62e5220cac
FROM ADDRESS                              TO CONTRACT ADDRESS                         GAS USED  VALUE
0x6e3aFB804071C1F4b26a5621C49C2d8a4C      0x2Bad0725EEbc20dFAf364148B1454ad254        190641    0
7bF82b                                    322bE3

TX HASH                                                                                    CONTRACT CREATION
0xf6480fa3e2c65abd23abb6fe261f2a385a927c2202f6ff8836254fb1cb43d1ea
FROM ADDRESS                              CREATED CONTRACT ADDRESS                    GAS USED  VALUE
0x6e3aFB804071C1F4b26a5621C49C2d8a4C      0x2Bad0725EEbc20dFAf364148B1454ad254        946612    0
7bF82b                                    322bE3
```

Figure 8

Conclusion:

patientwillbe visibleon thescreen.

Figure 8 shows the transaction details of the smart contract that stored in the blockchain ledger in the hash values. All the transactions are done from one address to another and it is clearly visible the transactions added in the ledger are all validated and are stored in the hash format. Ganache keeps track of every transaction. In Figure 8, "contract creation" denotes that the contract has been successfully created and that going forward, all transactions will be made in accordance with this smart contract. "Contract call" indicates that the contract has been called, which can also imply that the smart contract is being utilized in the transaction. shall be invoked in each and every blockchain transactionInconclusion,theproposedblockchainbaseddistributedsys temforE-healthrecordsisasignificantsteptowardsaddressingtheprivacyandsecuritychallenges facing the healthcare industry.Thesystemprovidesatamperproof,decentralized,andsecureplatformforstoringandsharingEHRs.Itutilizesaconsensusalgorithmandaccesscontrolmechanism to ensure the integrity of EHRsand that only authorized parties can accesspatientinformation.Thesystemalsoempowerspatientsbygiving themfullcontrolovertheirmedicaldataandtheabilitytograntandrevoke accesspermissions.

The results of our experiments show thattheproposedsystemisscalable, efficient,and provides a high level of security andprivacyforEHRs.Thesystemutilizesmulti-party computation (MPC) to protectpatientprivacyduringE-healthrecordsharing.Thesystem'spracticalityandeffectivenesswereevaluatedinareal-worldhealthcaresetting,demonstratingitspotentialtosignificantlyimprovethequalityof healthcareservices.

Compared to current EHR administration systems, the suggested approach offers a number of benefits, such as increased privacy, security, and patient control over medicaldata.Thesystemhasthepotentialtorevolutionizethehealthcare industrybyprovidingaccurateandtimely healthcareserviceswhileensuringtheprivacyandsecurityof patient data.Overall,theproposedblockchain-baseddistributedsystemforE-healthrecordsprovides a comprehensive solution to theprivacy and security challenges facing thehealthcare industry. It has the potential to raise the standard of medical treatment andempowerpatients,makingitapromising direction for future research anddevelopmentin thehealthcareindustry.

REFERENCES:

1. Hussain,S.S.,Tahir,S.S.,&Qureshi,M.A.(2019).Areviewonblockchain-based electronic healthrecord systems. Journal of NetworkandComputerApplications,135,62-84.

2. Hasan,M.A.,&Hassan,M.M.(2019).Ablockchain-baseddistributedstoragesystem formedicaldata.Journalofmedicalsystems,43(8), 223.

3. Dissanayake, D. D., Ekanayake, C.,&Seneviratne,S.A.(2019).Blockchain-based secure sharing ofmedical data: A review. Journal ofMedicalSystems, 43(8),233.

4. . Cho, J. R., Kim, H., Lee, H. J., &Kim,D.(2019).Ablockchain-basedapproachforsecureandprivacypreservingsharingofmedicaldata.Journalofmedicalsystems,43(8), 224.

5. Al Omar, M., &Alshaikhli, I. F.(2018). A secure blockchain-basedsystem of electronic health records forhealthcareapplications.FutureGeneration Computer Systems, 78,641-658.