International Journal of Software Innovation
Volume 11 • Issue 1

Smart Contract-Based Secure Decentralized Smart Healthcare System

Anu Raj, Madan Mohan Malaviya University of Technology, India*
Shiva Prakash, Madan Mohan Malaviya University of Technology, India

ABSTRACT

Social distancing has been imposed to prevent substantial transmission of the COVID-19 outbreak, which is presently a global public health issue. Medical healthcare providers rely on telemedicine to monitor their patients, particularly those with chronic conditions. However, telemedicine faces many implementation-related risks, including data breaches, access restrictions within the medical community, inaccurate diagnosis, fraud, etc. The authors propose a transparent, tamper-proof, distributed, decentralized smart healthcare system (DSHS) that uses blockchain-based smart contracts. The authors use an immutable modified Merkel tree structure to hold the transaction for viewing contracts on a public blockchain, updating patient health records (PHR), and exchanging PHR to all entities. It is verified by a performance evaluation based on the Ethereum platform. The simulation results show that the proposed system outperforms existing approaches by enhancing transparency, boosting efficiency, and reducing average latency in the system. The proposed system improves the functionality of the SHS environment.

KEYWORDS

Blockchain, Ethereum, Healthcare, Merkle tree, Smart Contract, Telemedicine

INTRODUCTION

Nowadays, everyone in the modern world places more emphasis on improving their health. Several new hospitals have been established as a result of the increase in illnesses. Patients find it challenging to access past health information since they are fascinated by visiting multiple hospitals for treatment and spreading their health records around several hospitals during their lifetime. Patient engagement with health records is thereby fragmented, which leads to better management of health records. The current health crisis has acted as an accelerator, allowing for the quick passage of stages that ordinarily delineate the adoption cycle of innovation. Reducing the amount of time that professionals and their patients were exposed to the COVID19 virus was crucial. Patients can communicate with their healthcare providers over long distances using telemedicine, receive care in the comfort of their own homes while having their health continuously monitored, and allow doctors to monitor

DOI: 10.4018/ijsi.315742 *Corresponding Author

the hospitalization process while providing suggestions to patients and their doctors. Today, the most promising technology in the business and medical industries is IoT (Verma et al., 2022). One of the goals of IoT is to enable, share, and gather data anonymously from physical and intelligent devices, such as home appliances, cars, and other physical objects (Gaur & Prakash, 2021). This global network saw the addition of more than 8.4 billion devices in 2017, a 31% increase from 2016 (*ZDNet*, n.d.)(Verma & Prakash, 2021). Every action in the healthcare industry is difficult to complete on time, and integrating health records into the system is a challenging procedure. Because there are so many various types of health records, it can be difficult for providers to store, secure, and validate them. Another significant difficulty facing the healthcare industry is the high-quality recovery of stored health data in a time-sensitive situation (Azaria et al., 2016). Blockchain (BC) is an innovative architecture for digitizing clinical history, where it is challenging to cope with the problems of records and decentralized data protection (Siyal et al., 2019). To create a smart e-health system, Chelladurai et al.(Chelladurai & Pandian, 2022) presented a system for exchanging health data on a blockchain platform. The proposed system introduces health models, consisting of viewership contracts on the public blockchain network, immutable patient log creation, medical data interchange among various participating entities, and viewership contracts for storing securely and easy accessibility of medical records. The blockchain serves as a clinical data repository in this system, giving patients easy access to their EHR through healthcare professionals, and distributed ledger records consisting of information on all the events. However, it has previously been presented many blockchain-based security mechanisms for various types of IoT networks but still, there aren't any smart contract-based security approaches for the IoMT system. There is a need to do further work to design and develop security as well as access control techniques based on blockchain technology for these networks (Pelekoudas-Oikonomou et al., 2022). Fog computing appears to be the greatest option compared to cloud computing for setting up a real-time Internet of medical system scenario like telemedicine because it offers services with minimal latency, high mobility, and geographic distribution as well as temporary storage. The foundation of the internet of everything (IoE), which includes network intelligent systems, is essentially the internet of things (Raj & Prakash, 2018). There are various challenges related to IoT and WSN (Raj & Prakash, 2020). The main focus of this paper is on health data storage and security in the DSHS systems. The proposed system makes use of the idea of cloud computing to assure the distributed component required in remote patient health monitoring as well as blockchain-based smart contracts to provide access control that is dynamic, optimum, and self-adjusting (Bekr et al., 2021). The blockchain is a technology of a series of blocks in which each block depicts a series of transactions. A blockchain consists of several blocks that are irremovable in which each block consists of a block number, block hash value, digital signature, previous hash value, and nonce. In the medical industry, the patient's confidential information is handled by the domain and should be securely stored. Patient health information such as personal details, disease information, medical history, prescription details, medical test results, ECG, and scan reports, have not been able to be securely stored on the permissionless public blockchain. As a result, the proposed system presented in this paper describes a system for using smart contracts efficiently and securely transferring medical data among various healthcare entities in a public blockchain. The paper organization is in the following ways:

- Background study of pre-existing research on blockchain-based access control schemes
- Proposed framework and architecture design.
- Implementation part of the proposed DSHS system
- Results and performance analysis of the proposed framework
- Conclusion & future direction

RELATED WORK

In this section, a brief literature survey on the pre-existing work and blockchain technology advances for telemedicine data privacy and integrity has been provided.

To preserve anonymity, an author (Omar et al., n.d.) proposed Medibchain, a patient-oriented EHR framework that uses blockchain as data storage. In this case, pseudonymity is upheld by using cryptographic procedures to safeguard the patient medical information. Blockchain technology's decentralized Medibchain functionality eliminates data protection weaknesses while upholding privacy and security. Control Chain, a blockchain-based access control authorization system, was developed by Pinno et al. They demonstrate the viability of Control Chain using the E-Control Chain, an Ethereum network proof-of-concept. Finally, the authors used the Raspberry Pi as an IoT device to conduct a study of the E-Control Chain's performance and cost (Pinno et al., 2020). To enable dynamic access control by confirming the subject's behavior, smart contract-based access control for the IoT is presented in (Zhang et al., 2018) in combination with machine learning techniques. A judge contract, a registry contract, and various access control contracts (ACC) make up the system's architecture (RC). For a subject-resource pair, each ACC specifies an access control technique. The ACC contract contains a list of inappropriate behavior for each resource. When a subject calls for access, ACC is activated, and if it notices inappropriate behavior, it alerts the JC. To improve data management, Khatoon et al. (Electronics & 2020, n.d.) established some workflows for the healthcare industry. The Ethereum blockchain platform has been used to create and implement specific medical workflows. It comprises advanced medical techniques including surgery and clinical trials. A lot of medical data must be accessed and managed as part of this workflow. The basic architecture for Hyperledger Fabric was proposed by the researchers (Contin & 2021, n.d.). An enterprise-class open-source distributed ledger platform and source code are provided by the Hyperledger project, a collection of open-source blockchain initiatives. It is a neighbourhood-based project that offers a foundation for blockchain applications. For the Industrial IoT, the authors created an FC model based on the BC (Jang et al., 2019)so that data may be exchanged quickly and easily while maintaining low throughput and low latency. The researchers (Muthanna et al., 2019) proposed a model that deploys FC with the blockchain and software-defined network (SDN) and applications. In this architecture SDN controllers and manages, Fog, as well as IoT devices, are associated by the blockchain to deliver a high level of security to the proposed system. An author (Zaidi et al., 2021) developed Swarm and Interplanetary File System that integrate blockchain with IoT. The system does not require access control lists for every device. It increases the efficiency of access management. Additionally, we leverage blockchain technology for edge computing devices to record the characteristic, prevent data manipulation, and remove a single point of failure. IoT devices have power over both the user's environment and the gathering of his or her private data; as a result, privacy leakage could occur if the user's data is made available to unreliable private and public servers. Smart contracts are used to automate the system's data access, while Proof of Authority utilizes them to improve the performance of the proposed model and reduce gas usage. A blockchain-based smart contract framework was created by researchers (Griggs et al., 2018) to allow for the security monitoring and analysis of medical sensors in an IoT healthcare system. The sensors interact with the internet of things (IoT) devices that call smart contracts and log all actions on a peer-to-peer blockchain based on the Ethereum network. On the distributed storage (Benet, 2014), which can be connected to the blockchain using a hash value, the patient's record history may be kept. One of the most promising technologies for decentralized, transactional data sharing is blockchain technology. Blockchain enables electronic health records in the healthcare industry to balance privacy and accessibility. Table 1. shows the comparative analysis of existing work related to telemedicine-based on research description, technique, and their contribution to the research.

From table.1 we determined that a lot of authors worked on the innovative framework of the smart healthcare-based telemedicine system to improve its efficiency, and enhance security as well

Table 1. Comparative study of the pre-existing Research

Ref	Author	Description	Technique	Contribution
(Uddin et al., 2018)	Ashraf	Patient-Centric Agent uses Blockchain technology to store secure data when it transfers from body area sensors	Lightweight communication protocol	Data security through various segments of a real-time healthcare monitoring system
(Tahir et al., n.d.)	Tahir	The architecture uses random numbers in the authentication procedure that is associated with joint conditional probability.	Probabilistic model.	Mutual authenticity enhanced access control.
(Almaiah et al., 2022)	Amin Almaiah	The framework provides two levels of security and privacy using the blockchain-based deep learning method.	Variational Auto Encoder (VAE) technique	Provide security and privacy to every participating healthcare system using smart contract-based enhanced Proof of Work.
(Ali et al., 2022)	Aitizaz Ali	The approach substantially enhances security, anonymity, and user behavior tracking.	Unique deep-learning-based secured blockchain	Policies for secure key revocation and updates
(Iftekhar et al., 2021)	Adnan Iftekhar	Executable binaries and Docker images for the ARM64 framework	ARM64 framework based on Raspberry Pi 4 Model B using the Hyperledger Fabric	The main contribution was to generate executable binaries for the ARM64 framework.
(Zaidi et al., 2021)	Syed Yawar Abbas Zaidi	A model of IoT access control based on attributes.	Proof of Authority is utilized to improve system performance, whereas smart contracts are employed for data access.	Invocation storage and the development of smart contracts enable the tracing function.
(Rizzardi et al., 2022)	Alessandra Rizzardi	The combination of a permission blockchain within an IoT distributed middleware layer to improve access control management	It includes NOSs as well as sticky policy-based enforcement Architecture	It assures the manipulation resistance and decentralized, distributed synchronization of the Architecture
(Records et al., n.d.)	Ochchhav Patel	Address the security concerns with the IoT for a healthcare system in terms of confidentiality, integrity, and access control measures.	Kovan, binance smart chain, rinkeby, and matic blockchain networks	Patient data is generated by various IoT sensors and secured through cryptographic methods.
(Bekr et al., 2021)	Hideyat zerga	Smart contract-based access control methodology allows patients to be the real owners of their medical data and exchange them securely.	Combined Fog computing with Blockchain technology.	Provide access control that is dynamic, efficient, and self-adjusting.
(Abugabah et al., 2020)	Ahed Abugabah	Smart contracts-based framework to design an efficient, tamper-proof decentralized healthcare framework	Blockchain-based smart contract	Unlock the future of the healthcare sector
(Joshi et al., 2022)	Shashank Joshi	The smart contracts-based architecture depicts several interactions and transactions among the other entities.	Smart contracts-based framework	Transaction protocol to digitally facilitate to enforcement of the transaction and imitate a real-world contract.
(Majdoubi et al., 2021)	Driss El Majdoubi	Both IoMT data and EHRs are measured after combining data usage monitoring with data access control.	Hyperledger Fabric and collect encrypted health information with the help of IPFS	It tracks the execution of the service w.r.t patient preferences and privacy-preserving for patient data.
(Amir Latif et al., 2020)	Rana M. Amir Latif	Smart healthcare framework for Ethereum-based application	Blockchain-enabled smart contract for the medical industry	Enhance the performance of the healthcare environment.
(Haque et al., 2021)	AKM Bahalul Haque	Proposed an e-healthcare system to resolve the quality service and accessibility of this system.	Blockchain-based smart contracts	It provides a secure, decentralized, automated architecture that is accessible to authorized users.
(Lakhan et al., 2021)	Abdullah Lakhan	Framework ensure medical information consistency and validation with symmetric cryptography.	Blockchain-based Smart-Contract Cost-Efficient Scheduling Algorithm	It ensures the blockchain validity by storing distributed information and load balancing situation

as an effective database server. The majority of the authors offered numerous research works aimed at improving the technology they had employed, as well as their security and other characteristics. In the 21st Century, a lot of SHS systems, most of the proposed frameworks were adapted IOT, Big Data Machine Learning, Deep Learning, and Blockchain as the major design pillar.

PROPOSED DECENTRALIZED SMART HEALTHCARE SYSTEM (DSHS)

In this section, we provide a framework for telemedicine transactions that utilize blockchain-based smart contracts to monitor, supervise, and carry out transactions. Telemedicine promotes a virtual interaction between a patient and a doctor and allows for both remote healthcare monitoring using ECGs and X-rays as well as post-treatment assistance. Fig. 1 depicts the block diagram of the proposed decentralized smart healthcare system to secure health data using the smart contract.

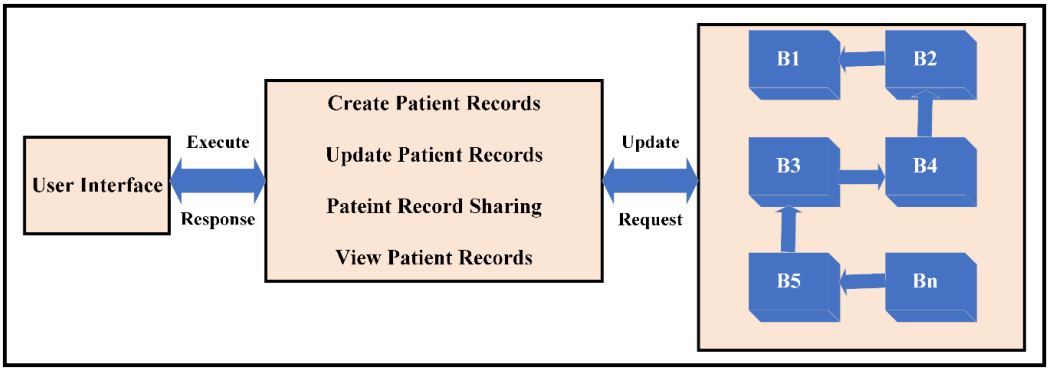
The proposed system utilizes a health blockchain, which maintains and distributes comprehensive patient records across a secure blockchain network. There are four models in this system the creation of immutable logs model, the sharing of the data model, the viewership, and the patient-provider models for modifying health records. The create module is responsible for the registration of patients including patient personal information, healthcare professionals' details, drug details, medical history, prescriptions, medical test reports, and other kinds of test reports including MRI, ECC, ECG, ECHO, MRI, CT scan, etc. The second module is accountable for updating patient medical records, the data sharing model is responsible for sharing health records among various providers in the blockchain network, and the view module provides owners of health records permission monitoring access. It is also possible to evaluate how well the patient is responding to the treatment. This system has made use of Ethereum smart contracts, which when performed cause events and let all authorized entities, including patients on the network, keep track of medical transactions. Transparency, interoperability, and data integrity can best be attained by adapting this proposed system.

System Architecture

In this subsection, Figure 2 illustrates the proposed model of a smart contract-based distributed smart healthcare system. Using blockchain-based smart contracts, the integrity of medical transactions will be ensured, lowering risks and enhancing scalability, tractability, and transparency. By compiling information from prescriptions, strategies, tests, and lab results, blockchain will allow clinicians to preserve a record of patient history when used in telemedicine. Additionally, our system focuses on using smart contracts to start events and enabling all associated entities to track all network transactions.

The main participating entities in DSHS are as follows:

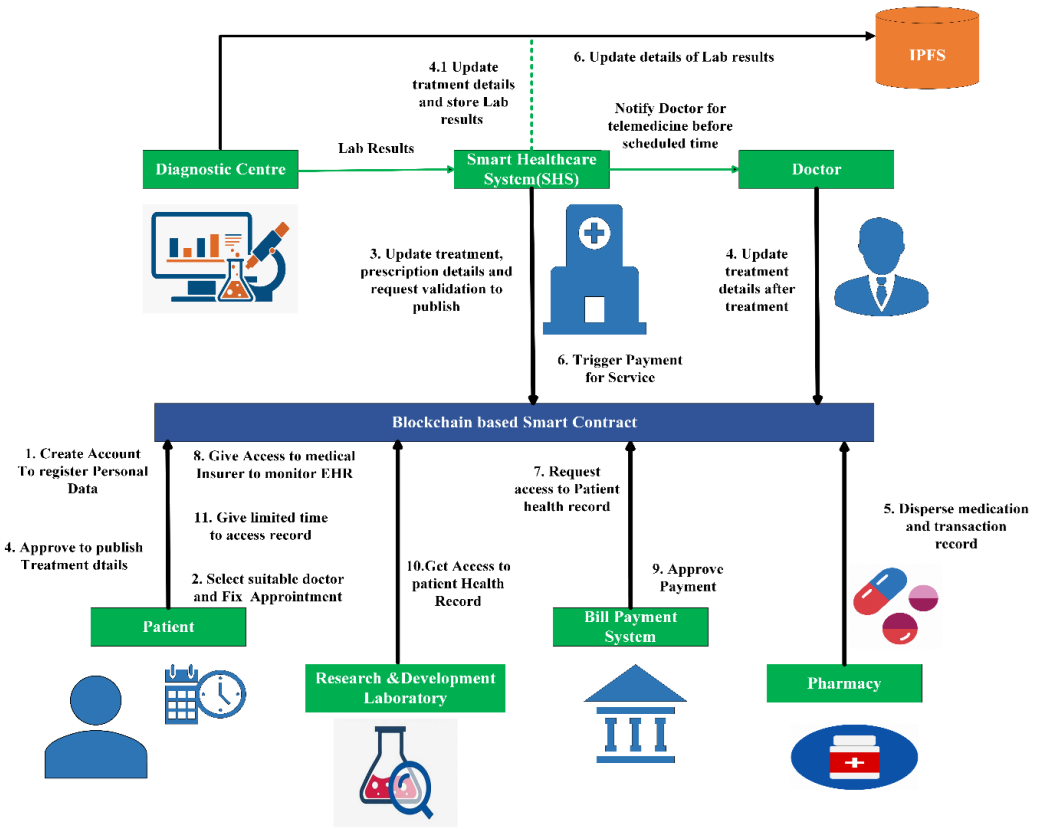
Figure 1. Block Architecture of the proposed system-DSH



a) Patient: It is the main entity in DSHS which creates and initiates the smart contract, and provide detail about herself/himself. All the transactions occurring within the blockchain are tracked by the patient.
b) Smart Healthcare System (SHS): Decentralized SHS is the most important entity among the all-participating entities which consists of authorized doctors and diagnostic centers that keep the record of all the medical tests on the patient. IPFS is a decentralized file system where medication details, health conditions as well as lab results are stored. The hash value of every transaction stored in the IPFS will be available to all the verified participating entities in the smart contract.
c) Pharmacy: The pharmacy provides the prescribed medications to the patient, updates the data on the smart contract, and keeps track of every transaction from their perspective.
d) Bill Payment System: Depending on the type of medical coverage inclusion, health insurance is a type of protection inclusion that covers a person's medical expenses. The event that prompts the insurer to cover the costs of the procedure or medical care once the treatment is complete is set off by the telemedicine center.
e) Research and Development Laboratory: Research institutions in the healthcare industry are important for providing market research and development laboratory services to the pharmaceutical and medical industries.

The healthcare provider is one of six entities in the proposed system, along with the EHR Manager, Blockchain repository, and doctors, caregivers, and clinical authorities. The registered patient in

Figure 2. System Architecture: A decentralized blockchain-enabled telemedicine



the proposed system can reach the healthcare provider in the peer-to-peer blockchain platform for additional reviews after the registration procedure has been verified. The accuracy of the data entered into the system must be ensured. The proposed methodology, however, uses the user's encrypted data. The user's computer performs data encryption. Every time a patient first goes for treatment, the healthcare professional completes the patient registration process, as well as the framework, and creates the patient's specific ID and password for future use. Additionally, users just need to check in to access their personal information through a secure channel for the transaction. In the same way, the healthcare professional or doctor must sign in to the system. A transaction identification has now been provided to each blockchain user. The users can obtain the data more easily thanks to this transaction identification. Blockchain is employed in the proposed framework as a database for health information. In this case, the patient initiates a smart contract only once established parameters have been agreed upon by all parties. This is done to protect the security of decentralized smart healthcare systems and smart contract-based medical data exchanges. The patient then schedules a visit with a healthcare professional at the DSHS service.

The doctor or healthcare professionals from the DSHS conduct a video consultation after the appointment, prescribes medications, update IPFS with treatment information, and keep the hash value within the smart contract. Once the patient has received all the medications, the pharmacy updates the contract with the detail of the transactions. The DSHS initiates the payment, and then the insurer is triggered. The medical insurance starts a process to gain access to the treatment, which the patient is informed of and consents to. The bill payment system gives healthcare the go-ahead to settle payments, and this information is disseminated to every participating entity by the events in the smart contract. He/she can grant access to the organizations conducting medical research so that they can conduct experiments and clinical trials. Additionally, as part of the telemedicine framework, the telemedicine center regularly consults with medical experts, particularly in cases of extreme complications.

IMPLEMENTATION

The implementations of smart contracts are shown in this section. The smart contract is an interface that enables coordinated transactions to be carried out by network participants. When automatically executed, smart contracts give network users the ability to carry out a set of conditions, terms, and circumstances governing a transaction. Every smart contract has a unique blockchain account and address. It then maintains its status and acquires ownership rights on the blockchain. The request and responses are also carried out using smart contracts.

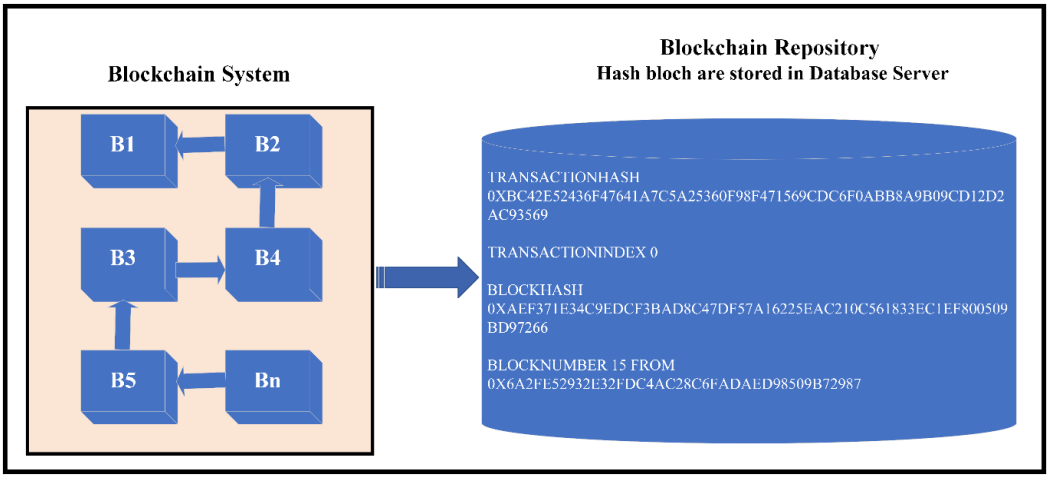
The proposed DSHS framework executes a set of blockchain-based smart contracts module which is as follows:

- Patient registration module
- Patient data update module
- Patient data sharing module
- Patient viewership module

Patient registration module

It is responsible for patient registration and keeps the medical records in the appropriate blocks. Blocks with hashes created by the system are directly kept in a database server. These blocks contain all transactions and the hash value. Figure 3 demonstrates how the patient registration contract generates patients' medical records, how those records are saved in blocks, blocks are kept in a database server and how the block's hash values are preserved.

Figure 3. Blockchain stored in the database server



Patient-provider update module

In this module, once a patient's health information is stored in the system, they can use this module to access their medical records and monitor the blockchain network through any doctor or healthcare provider. By using the Patient ID provided by the system, it automatically retrieves prior patient health records. No one can change the data because blockchain is an immutable system. The proposed approach enables the detection and prevention of changes to the patient's electronic health record (EHR). If any value is exceeded required, they will be developed by a team of pre-approved participants, which will also include the patient, the physician, and all other participating entities. The update contract module is used to implement this permission model.

Patient-provider data sharing module

The proposed system allows various healthcare entities to participate while preserving a degree of decentralization. A patient cannot choose to go to the same hospital for all aspects of treatment; rather, the patient prefers to travel to a different location to see a doctor as shown in figure 3. In that case, the doctor needs to see their previous treatment log to administer more care. The health blockchain has nodes that each includes, database blocks, smart contracts, and agreements.

Patient viewership module

The viewing contract is a module for ensuring the integrity of medical data that are maintained on record in the proposed system. Patients must have viewer permission to view any of their prior medical records. Doctors or physicians have administrator access to their patients' EHR, allowing them to make changes to monitoring threshold settings and treatment alterations. To do that, a viewership contract is immediately created, allowing patients to access viewership through the blockchain protocol.

The Remix IDE environment is also used to develop the smart contract in the Solidity programming language. The Ethereum addresses of the participating entities in our proposed system are used to identify them. By calling the smart contract's functionalities on a regular schedule, these entities make communication possible. Figure 4 represents the sequence diagram of a typical DSHS telemedicine situation and how medical treatments are delivered. We designed the telemedicine healthcare system in which patient has information about the medical data and data exchanging that occur in the blockchain environment. Patient ID, patient name, address of the medresearch_org, IPFShashEHR, number of requests from DSHS, number of approvals from SHS, and contState are

among the information provided by the patient when they create a smart contract. Depending on the type of medical expertise required, the patient selects the doctor they would choose to treat them after the contract has been created.

The telemedicine-based smart healthcare system requests the patient to publish his/her treatment records on the IPFS, and the hash value of the EHR is kept within the smart contract after the treatment completion. The patient approves publishing the medical records on the IPFS after confirmation of the relevant documents by analysing the hash value of the transaction kept. The drug store starts the dispersal of medicine to the patient followed by the completion of treatment. The DSHS initiates the payment request for medical services and treatments provided to the patient, and the event is broadcasted to all participating entities. The sequence diagram illustrates the association among various bill payment systems, patients, and medical research and development as shown in figure 5. Access to the patient's EHR is required by the medical insurer or bill payment system to issue payment for the rendered services. The patient grants access to their medical records at the insurer's request. Moreover, we've demonstrated in our system that the smart contract manages the data transfer and makes it possible to access the patient's information when a network-approved research organization requests temporarily restricted access to the patient's EHR records.

The proposed algorithms are as follows:

Algorithm 1: Smart Healthcare System contract

Input: Ethereum address of SHS, PatientID, patient name, IPFShashEHR, Ethereum address of the Research & Development Lab, No Requests By SHS, No of Approvals by Bill Payment System, and contractState.

contract state is ***NotReady***
the state of DSHS is ***ReadytoSubmit***
Bill Payment System state is ***SubmittedForPaymentApproval.***

The proposed system uses mapping to keep track of patients' addresses and approved results, which are shown as a key-value pair. Additionally, the system maintains a mapping to keep track of a list of

Figure 4. Diagram illustrating the association among various participating entities

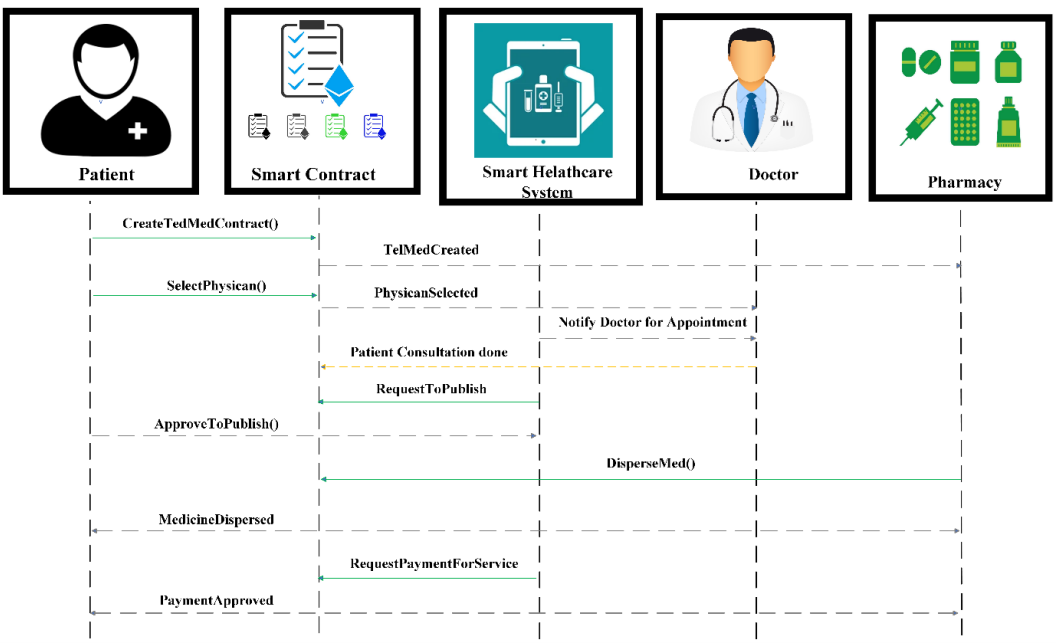
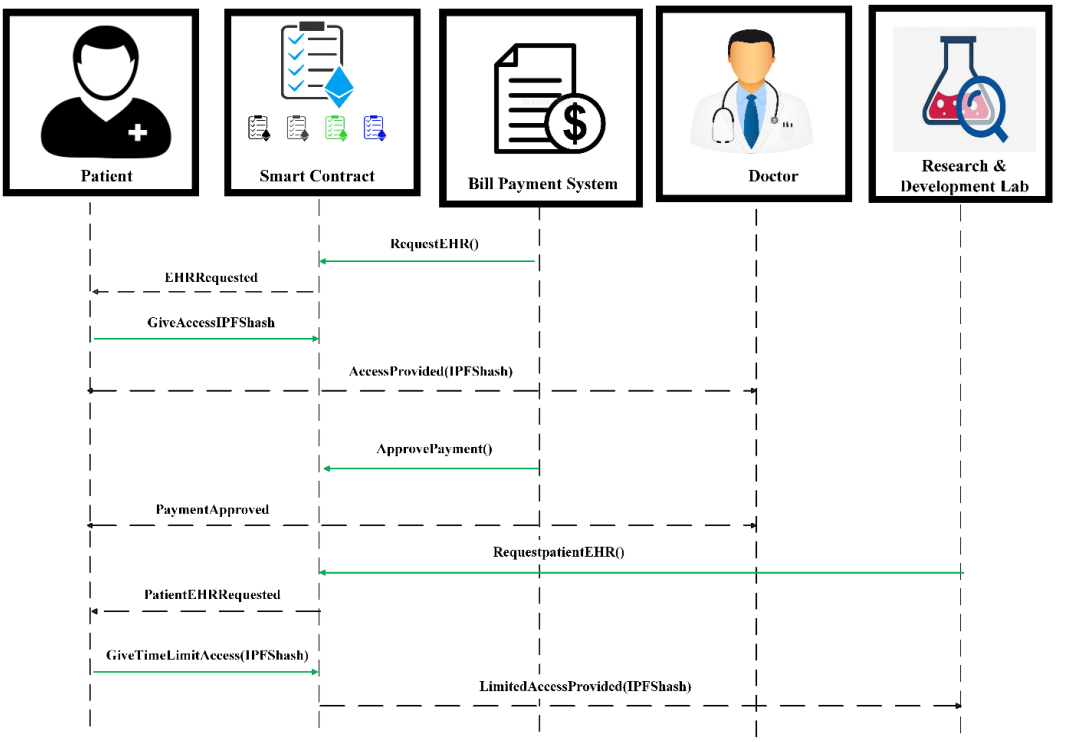


Figure 5. The association among bill payment systems, research lab, DSHS, and smart contract



insurance company approvals as well as the hash inputted by insurance companies during the approval procedure Algorithm 1 presents functions used in the implementation of the smart contract. PatientID, patientName, and notably IPFShashEHR, the IPFS hash of the EHR, are initialized in the constructor function of the smart contract. The hash value recorded in the functions of the smart contract is used to verify the integrity of the medical data whenever being accessed by different participating entities. At the initial stage, the contractState is Not Ready. The patient initiates the contract creation process by calling the contract. Create event and the CreateTelMedContract() function. As indicated by the no. of Approvals by BillPaymentSystem and the number of Requests by the smart healthcare system, the function also displays the initialization of the requests for approval by the bill payment system as well as the number of requests by the DSHS to publish their medical records.

```
Algorithm 2: Decentralized Smart Healthcare System request to
publish on IPFS
Input: Ethereum address of the DSHS, IPFShashof EHR
ContractState is PhysicanSelected
SHSState is ReadyToSubmit
Restrict access to only SHS
if address=address of authorizes SHS
    and document hash=IPFShashEHR then
    contract state changes to
    WaitingToApproveToPublish
    create a notification message stating the completion of
Treatment and Requesting
    patient approval for publishing the patient health records on
```

```
IPFS
                                end
                            else
    revert contract state and display an error message
             end
```

Algorithm 2 demonstrates that the DSHS system's request to publish EHR on the IPFS is RequestToPublish(). The SHS status changes to Ready to Submit and the contract state to doctor Selected. Only with the aid of the modifier, Not the patient can DSHS carry out the function due to its limitations. The SHS state is changed to Submitted for Approval, and the contract state is changed to Waiting to Approve to Publish. The DSHS triggers the event Requested for Approval and waits for the patient's consent before publishing the EHR on IPFS.

```
Algorithm 3: Patient provides approval to publish on IPFS
Input: Ethereum address of the SHS, IPFShashof EHR
Contract is WaitingToApproveToPublish
SHSState is SubmittedForAprroval
Restrict access to only Patient
if hash submitted by SHS matches the IPFShash of the EMR then
    contract state changes to Approved
    SHS state change to ApprovalSuccess
    NumberofApprovalbyPatient is increased by 1
    create a notification message from the patient's side for
approving to publish
    on IPFS
          end
     else
          contract state changes to ApprovalFailed
          SHS state change to FailedValidation
          create a notification message to provide the correct
details and to request again for Approval
       end
   else
     revert contract state and broadcast an error message
end
```

Algorithm 3 represents an algorithm for a patient giving the DSHS permission to publish patient medical information on IPFS. The DSHS is in a Submitted for Approval state, while the contract is in a Waiting to ApprovetoPublish stage. The contract state becomes approved after a successful approval, and the DSHS state converted to approval success. To demonstrate the successful approved state of all other authentic network entities, the event Approved success is published. If the validation fails, the contract's approval status is converted to Failed, and the validation status of DSHS is converted to Failed after that event Revise Content is broadcast to the DSHS to update the right information.

```
Algorithm 4: Patient Medical Record access to the Bill Payment
System
Input: Ethereum address of the bill payment system
Contractstate is WaitingForBillApproval
Paymentsyatem state is ApprovalRequested
Restrict access to only Patient
if hash provided by the PaymentSystem matches the IPFShash of the
original
    record of IPFS then
    contract state changes to Approved
```

```
    BillPaymentSystem state converted to ClaimSuccess
    create a notification for the treatment done
             end
        else
      contract state converted to NotCoverandFailed
    BillpaymentSystem state converted to FailedClaim
   create a notification message to instigate the patient      to
complete payment
      end
              else
 revert contract state and send an error message
          end
```

The operation represented by algorithm 4 is when the bill payment system is given access control to the patient medical information. The pharmacy entity activates the constructors to distribute medications to the affected patients as soon as the patient permits updating information on IPFS. The treatment and service provided by the DSHS must now be paid for by the medical insurer.

RESULTS AND PERFORMANCE EVALUATION

In this section, we describe how the Modified Merkle tree EMR data structure works and how the main smart contract works while testing transactions and interactions among entities of distributed smart healthcare systems. The proposed smart contract is developed on Remix IDE, and it is being executed and tested on Remix IDE, Ganache, and Nodejs. The web-based Remix IDE has several features that make it possible to evaluate smart contracts before delivering them. The code is written in the Solidity language and is tested on the Ethereum Network. The effectiveness of proposed blockchain smart contracts has been assessed through rigorous experimentation, and the results are provided in this section with several trials. Testing the smart contract ensured that the consent's advancement followed the necessary sequences based on its consent state and that the approvals and rejections of submitted endorsement solicitations were accurately tested. We consider the Ethereum addresses of smart healthcare system is 0x6A2fe52932e32fDc4ac28c6FadaeD98509B72987, address of the patient is 0x458A458A29ffe3ada8E0D13a0088d8f86EAe4e86 pharmacy 0x4D6ac664B918Bd90FaAEfC520E5CFa1587Bc919C, Bill Payment System, 0x62a0889475e1010042823f860Bb7aa25DE934340 and the research and development Laboratory are 0xA60D4A2F8C747EB7198A356E18d9a40ea95D6e98 respectively. We put the scenario where the SHS asks the patient to publish on IPFS to the test, as seen in Figure 6. The smart contract input is "Qma5jpgdqoXfSoUoxUb4FHH4RTGMU3R3dujMpTMDVcKYXQ," which is the IPFShash of the EHR. After the hash is confirmed, the event Permission Granted to Publish is published so that the concerned patient can read and review the records before broadcasting the event Approved Success.

On the Ethereum platform, we provided the fundamentals of a DSHS and described the various entities, their responsibilities, and their roles within the network. We tested the smart contract's functionality in a variety of scenarios for both success and failure. According to the results, there is a link between the industry's adoption of the proposed method as well as patients' access to more transparent and accurate data. The DSHS removes the requirement for a centralized administrator to control medical transactions and how the data integrity of EHR is preserved by utilizing the IPFS hash value in the decentralized network. The efficiency of the DSHS on sensitive healthcare records is examined using privacy accuracy against the number of patient health records.

Table 2 shows the comparison of privacy accuracy of the pre-existing framework against no. of the patient health records, from this table it is shown that using the proposed DSHS system, privacy accuracy increases up to 99.6% w.r.t 500 patient records which maximum as compared to other existing telemedicine frameworks.

Figure 6. Logs showing event Request for Approval triggered

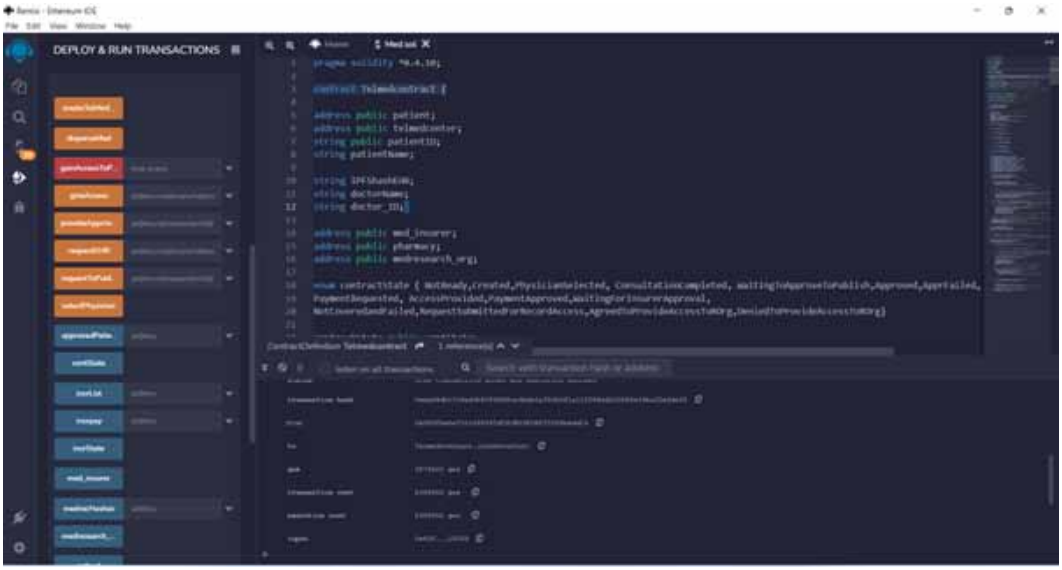


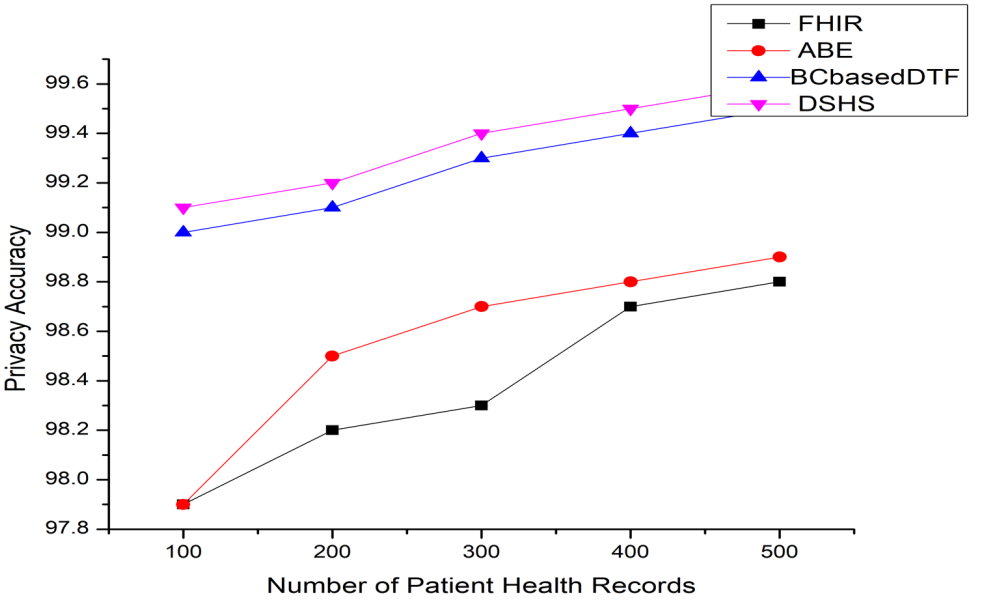
Table 2. Comparison of Privacy Accuracy with pre-existing models (in %)

No. of Patient Health Records	FHIRC	ABE	BCbasedDTF	DSHS
100	97.9	97.9	99	99.1
200	98.2	98.5	99.1	99.2
300	98.3	98.7	99.3	99.4
400	98.7	98.8	99.4	99.5
500	98.8	98.9	99.5	99.6

Figure 7 showed how the DSHS maintains high levels of security, privacy, and authentication accuracy. Five groups of patient health records are considered for system performance evaluation which consists of 100, 200, 300,400, and 500 patient health records. The effectiveness of the decentralized system is evaluated against several existing efforts, including the blockchain, attribute-based encryption (ABE), the FHIR Chain prototype (FHIRCP), and Blockchain-based decentralized Telemedicine Framework (BCbasedDTF). Telemedicine, the Internet of Things (IoT), and blockchain technology have all found use in the healthcare industry as a result of enhanced technological advancements. The results show that the confidentiality of the data is managed by a DSHS combined with blockchain technology. For patients who are in faraway locations, several of today's telecommunications technologies with video conferencing capabilities provide high-quality care. Despite this better technological advancement, there are not enough patients and it has not gained widespread acceptance. Poor video call quality due to technical glitches, a lack of dependable satellite networks, and slow or non-existent broadband networks are major concerns in remote parts of developing countries and may not be quickly resolved.

- System Throughput: The rate of storing the verified transactions of the proposed blockchain system within a given time frame is known as system throughput.
- Latency/Delay Latency is the amount of time it takes for a transaction effect that is used throughout the network.

Figure 7. Accuracy analysis



We used various patient groups, each of which consisted of a maximum of 500 patient medical records, to evaluate the various metrics of the proposed framework. Five patient group categories were established through testing the proposed approach and contrasting it with the current conventional system. 500 patients are examined for resource use throughout the investigation's initial phase.

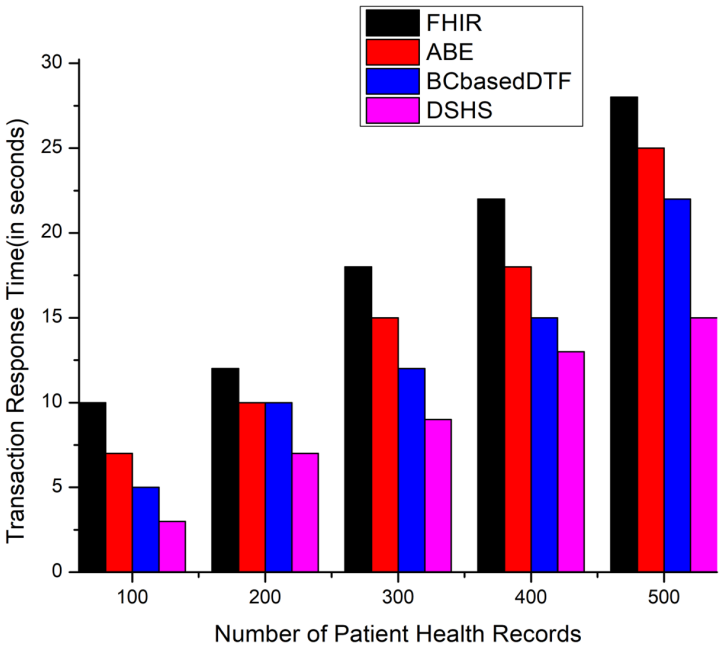
Table 3 represents the comparison of Transaction Response Time with the pre-existing framework w.r.t. to the no. of the patient health records, from this table it is shown that using the proposed DSHS system, Transaction Response time is 15 seconds w.r.t. 500 patient records which are minimum with other existing work.

A distributed ledger is used in the proposed DSHS system, and a replica of the information is kept in each participating node. It resolves the issue of delayed access and slow retrieval. A blockchain platform's transaction response time for a single patient request and response requires a minimum of 0 seconds, 5 seconds, 10 seconds, 15 seconds, 20 seconds, 25 seconds, and 30 seconds, and it varies depending on how the platform stores its records. For example, the transaction response time is measured for 500 patients at a minimum of 45 seconds. Figure 8 shows the transaction response time for requests and responses for various groups' health records. When compared to other existing systems, the blockchain platform's turnaround time, requests, and responses are

Table 3. Comparison of Transaction Response Time with existing work(in seconds)

No. of Patient Health Records	FHIR	ABE	BCbasedDTF	DSHS
100	10	7	5	3
200	12	10	10	7
300	18	15	12	9
400	22	18	15	13
500	28	25	22	15

Figure 8. Transaction response time



satisfactory. The proposed system's transaction latency is also measured using inputs such as the amount of time needed for a request to be sent and the time needed for results to become accessible. The overall amount of time needed for a transaction to take effect over the network is termed the transaction delay. The main challenge with the proposed approach is maintaining privacy as well as at each node. From the above result is it seen that our proposed System -DSHS outperformed the FHIR, ABE, and BCbasedDTF.

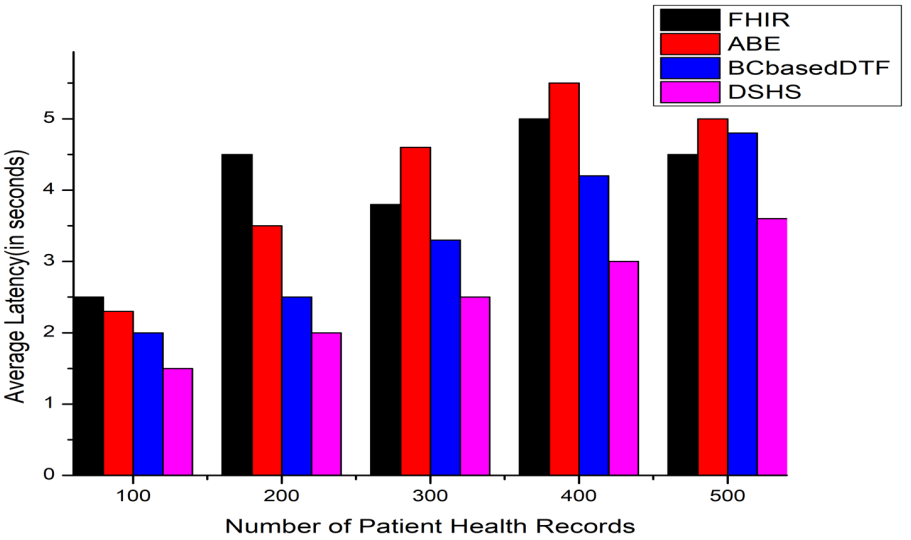
Table 4 shows the comparison of Average Latency with the pre-existing framework w.r.t. to the no. of the patient health records. Using the proposed DSHS system, the average transaction latency is 3.6 seconds w.r.t. 500 patient records which are minimum with other existing work.

The proposed system was evaluated with five groups of patients, and Figure 9 displays the average latency for each patient group. Each patient group has a different latency as the participant count rises, so does the system's latency. When a random delay is presented in existing systems, the latency is independent of the number of participants. The transaction response time for a single patient request and response requires a minimum of 0 seconds, 1 second, 2 seconds, 3 seconds, 4

Table 4. Comparison of Average Transaction latency against the No. of patient Hear Records (in sec)

No of Patients Health Records	FHIR	ABE	BCbasedDTF	DSHS
100	2.5	2.3	2	1.5
200	4.5	3.5	2.5	2
300	3.8	4.6	3.3	2.5
400	5	5.5	4.2	3
500	4.5	5	4.8	3.6

Figure 9. Average Transaction latency



seconds, 5 seconds, and seconds, and it varies depending on how the platform stores its records. For Example, if we take a group of 100 patient records FHIR has a maximum average latency of 2.5 and DSHS has a minimum of 1.7 seconds. If we take the group of 500p patient health records, ABE has the maximum average latency which is 4.9 while our proposed system has the least average latency of 3.8 seconds. From the above result is it seen that our proposed System -DSHS outperformed the FHIR, ABE, and BCbasedDTF on average latency.

CONCLUSION AND FUTURE DIRECTION

In this paper, a framework has been proposed for a decentralized smart healthcare system using blockchain-based smart contracts which ensure security, authenticity, and data integrity of medical transactions. Every participating entity can validate the transaction for secured health data exchange, and the smart contract regulates all transactions that take place between the various healthcare network participants. The research explores the design, implementation, and efficiency of the proposed blockchain-based DSHS system. It allows patients, doctors, healthcare providers, and bill payment systems to access, view, and share medical data with the patient's permission. This solution is intended to achieve privacy, security, and openness. This technology can also be used to control other remote non-medical assistance in the healthcare industry. The performance analysis is done to evaluate throughput, transaction response time, and the average latency of the DSHS system. The results show that the integration of SHS and blockchain enhances the system's throughput and performance while reducing latency and resource consumption.

In future work, the proposed hybrid approach can be extended to ensure content integrity. The extended work is based on the implementation of a new Modified Merkle Tree database system which will be helpful in the efficient storage and integrity of the patient medical data.

ACKNOWLEDGMENTS

Under the NET-NFSC scheme, the University Grants Commission is supporting the research work.

CONFLICT OF INTEREST

The authors of this publication declare there is no conflict of interest.

FUNDING STATEMENT

This research is funded by MHRD, Government of India.

REFERENCES

Abugabah, A., Nizamuddin, N., & Alzubi, A. A. (2020). Decentralized telemedicine framework for a smart healthcare ecosystem. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 166575–166588. doi:10.1109/ACCESS.2020.3021823

Al Omar, A., Rahman, M., & Basu, A. (n.d.). *Medibchain: A blockchain-based privacy-preserving platform for healthcare data.* Springer. https://link.springer.com/chapter/10.1007/978-3-319-72395-2_49

Ali, A., Pasha, M. F., Ali, J., Fang, O. H., Masud, M., Jurcut, A. D., & Alzain, M. A. (2022). Deep Learning Based Homomorphic Secure Search-Able Encryption for Keyword Search in Blockchain Healthcare System: A Novel Approach to Cryptography. *Sensors (Basel)*, *22*(2). doi:10 doi:.3390/s22020528 PMID:35062491

Almaiah, M. A., Ali, A., Hajjej, F., Pasha, M. F., & Alohali, M. A. (2022). A lightweight Hybrid Deep Learning Privacy Preserving Model for FC-Based Industrial Internet of Medical Things. *Recent Trends in Wireless Sensor and Actuator Networks.*

Amir Latif, R. M., Hussain, K., Jhanjhi, N. Z., Nayyar, A., & Rizwan, O. (2020). A remix IDE: Smart contract-based framework for the healthcare sector by using Blockchain technology. *Multimedia Tools and Applications*. doi: doi:10.1007/s11042-020-10087-1

Azaria, A. & Ekblaw, A. (2016). *Medrec: Using blockchain for medical data access and permission management.* IEEE. doi:10.1109/OBD.2016.11

Bekr, A., Tlemcen, B., Abou, U., Belkaid, B., Abou, U., Belkaid, B., Abou, U., & Belkaid, B. (2021). *A Smart Contract-based Access Control Architecture for Telemedicine During Covid-19*, 0–14. Research Square.

Benet, J. (2014). Ipfs-content addressed, versioned, p2p file system. *Arxiv.Org*. https://arxiv.org/abs/1407.3561

Chelladurai, U., & Pandian, S. (2022). A novel blockchain-based electronic health record automation system for healthcare. *Journal of Ambient Intelligence and Humanized Computing*, *13*(1), 693–703. doi:10.1007/s12652-021-03163-3

Contin, O. A.-C. M. (2021). A hybrid model using bio-inspired metaheuristic algorithms for network intrusion detection system. *Researchgate.Net*. https://www.researchgate.net/profile/Omar-Almomani/publication/350276313_A_Hybrid_Model_Using_Bio-Inspired_Metaheuristic_Algorithms_for_Network_Intrusion_Detection_System/links/605835ae458515e83460003d/A-Hybrid-Model-Using-Bio-Inspired-Metaheuristic-Algorithms-for-Network-Intrusion-Detection-System.pdf

El Majdoubi, D., El Bakkali, H., & Sadki, S. (2021). SmartMedChain: A Blockchain-Based Privacy-Preserving Smart Healthcare Framework. *Journal of Healthcare Engineering*, *2021*, 1–19. Advance online publication. doi:10.1155/2021/4145512 PMID:34777733

Electronics, A. K. (2020). *A blockchain-based smart contract system for healthcare management.* MDPI. doi: doi:10.3390/electronics9010094

Gaur, R., & Prakash, S. (2021). Performance and parametric analysis of iot's motes with different network topologies. *Lecture Notes in Electrical Engineering, 756 LNEE*, 787–805. doi:10.1007/978-981-16-0749-3_61

Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. *Journal of Medical Systems*, *42*(7), 1–7. doi:10.1007/s10916-018-0982-x PMID:29876661

Haque, A. B., Muniat, A., Ullah, P. R., & Mushsharat, S. (2021). An automated approach towards smart healthcare with blockchain and smart contracts. *Proceedings International Conference on Computing, Communication, and Intelligent Systems,* 250–255. IEEE. doi:10.1109/ICCCIS51004.2021.9397158

Iftekhar, A., Cui, X., Tao, Q., & Zheng, C. (2021). Hyperledger fabric access control system for the internet of things layer in blockchain-based applications. *Entropy (Basel, Switzerland)*, *23*(8), 1054. doi:10.3390/e23081054 PMID:34441194

Jang, S., Guejong, J., & Jeong, J. (2019). *Fog computing architecture-based blockchain for industrial IoT,* 593–606. Springer. doi:10.1007/978-3-030-22744-9_46

Joshi, S., Choudhury, A., & Saraswat, O. (2022). *Enhancing Healthcare System Using Blockchain Smart Contracts*, 1–12. http://arxiv.org/abs/2202.07591

Lakhan, A., Mohammed, M. A., Rashid, A. N., Kadry, S., Panityakul, T., Abdulkareem, K. H., & Thinnukool, O. (2021). Smart-contract aware of Ethereum and the client-fog-cloud healthcare system. *Sensors (Basel)*, *21*(12), 1–21. doi:10.3390/s21124093 PMID:34198608

Muthanna, A., Ateya, A. A., Khakimov, A., Gudkova, I., Abuarqoub, A., Samouylov, K., & Koucheryavy, A. (2019). Secure and reliable IoT networks using fog computing with software-defined networking and blockchain. *Mdpi*. doi:10.3390/jsan8010015

Pelekoudas-Oikonomou, F., Zachos, G., Papaioannou, M., de Ree, M., Ribeiro, J. C., Mantas, G., & Rodriguez, J. (2022). Blockchain-Based Security Mechanisms for IoMT Edge Networks in IoMT-Based Healthcare Monitoring Systems. *Sensors (Basel)*, *22*(7), 2449. doi:10.3390/s22072449 PMID:35408064

Pinno, O. J. A., Grégio, A. R. A., & De Bona, L. C. E. (2020). ControlChain: A new stage on the IoT access control authorization. *Concurrency and Computation*, *32*(12). doi:10.1002/cpe.5238

Raj, A., & Prakash, S. (2018). Internet of Everything: A survey based on Architecture, Issues, and Challenges. *5th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering*. IEEE. doi: doi:10.1109/UPCON.2018.8596923

Raj, A., & Prakash, S. (2020). Path discovery approach for mobile data gathering in WSN. *International Journal of Computer Applications in Technology*, *64*(2), 133–142. doi:10.1504/IJCAT.2020.111604

Records, I. H., Patel, O., & Patel, H. (n.d.). *Ethereum-based Blockchain Technology to achieve Confidentiality, Integrity, and Access control*, 1–31.

Rizzardi, A., Sicari, S., Miorandi, D., & Coen-Porisini, A. (2022). Securing the access control policies to the Internet of Things resources through permissioned blockchain. *Concurrency and Computation*, (February), 1–19. doi: doi:10.1002/cpe.6934

Siyal, A. A., Junejo, A. Z., Zawish, M., Ahmed, K., Khalil, A., & Soursou, G. (2019). Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. *Cryptography*, *3*(1), 1–16. doi:10.3390/cryptography3010003

Tahir, M., Sardaraz, M., & Muhammad, S. (2020). *A lightweight authentication and authorization framework for blockchain-enabled IoT networks in health informatics*. Mdpi. doi: doi:10.3390/su12176960

Uddin, M. A., Stranieri, A., Gondal, I., & Balasubramanian, V. (2018). Continuous Patient Monitoring with a Patient-Centric Agent: A Block Architecture. *IEEE Access: Practical Innovations, Open Solutions*, *6*(June), 32700–32726. doi:10.1109/ACCESS.2018.2846779

Verma, G., & Prakash, S. (2021). Emerging Security Threats, Countermeasures, Issues, and Future Aspects on the Internet of Things (IoT): A Systematic Literature Review. *Lecture Notes in Mechanical Engineering*, 59–66. doi:10.1007/978-981-15-9956-9_6

Verma, G., Shahi, A. P., & Prakash, S. (2022). A Study Towards Recent Trends, Issues and Research Challenges of Intelligent IoT Healthcare Techniques: IoMT and CIoMT. *Lecture Notes in Networks and Systems*, *376*, 177–190. doi:10.1007/978-981-16-8826-3_16

Zaidi, S. Y. A., Shah, M. A., Khattak, H. A., Maple, C., Rauf, H. T., El-Sherbeeny, A. M., & El-Meligy, M. A. (2021). An attribute-based access control for IoT using blockchain and smart contracts. *Sustainability (Switzerland)*, *13*(19), 1–26. doi: doi:10.3390/su131910556

ZDNet. (n.d.). *IoT devices will outnumber the world's population this year for the first.* Zdnet. https://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/

Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2018). *Smart Contract-Based Access Control for the Internet of Things*.

Anu Raj received the M. Tech degree in 2019 at Madan Mohan Malviya university of Technology, Department of information technology and computer applications, Gorakhpur, India. She is currently a Research scholar in the Madan Mohan Malaviya University of Technology, Department of information technology and computer applications. Her main research interests are the Internet of things, computer networking, wireless area network, computer-based applications, multimedia databases, metric learning and data gathering in WSN

Shiva Prakash has received M. Tech. degree in Computer Science & Engineering from MNNIT, Allahabad in 2006 and PhD degree in Computer Science & Engineering in 2013. Presently, he is working as a Professor (CSED), Chairman Campus Development Cell, Chairman SC/ST Cell, M.M.M. University of Technology Gorakhpur, UP, India. He has more than 20 years of teaching and research experience. He has shared responsibilities as Head of Department of CSE, Officer In-charge- Computer Centre, Officer In-charge Alumni Association, Convener of BOS of CSE, Coordinator NSS, and many more. He has published more than 117 papers in refereed international/national journals and conferences including IEEE, ACM, Springer conferences. He has organized many such conference in the capacity of conference Organizing Secretary, Technical Chair, and editor of conference proceeding. He has reviver of many National/International conferences and Journals. His publications are listed in Citeseer-x, IEEE, Elsevier, and Scopus. He is a life Member of Indian Society for Technical Education (ISTE), Member of IEEE and member of Computer Society of India (CSI). His many papers have been nominated as Best Paper Award at International Conference.