IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 16 July 2024, accepted 24 July 2024, date of publication 31 July 2024, date of current version 12 August 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3436075

RESEARCH ARTICLE

Secure Sharing Architecture of Personal Healthcare Data Using Private Permissioned Blockchain for Telemedicine

CH V. N. U. BHARATHI MURTHY AND M. LAWANYA SHRI
School of Computer Science Engineering and Information Systems, Vellore Institute of Technology, Vellore, Tamilnadu 632014, India
Corresponding author: M. Lawanya Shri (lawanyaraj@gmail.com)

This work was supported by the Vellore Institute of Technology, Vellore, Tamil Nadu, India.

ABSTRACT Blockchain technology has fascinated and significantly sparked research activities and industries due to its transparency in transactions and data sharing. The striking proliferation of blockchain technology is used to confront the challenges associated with trust, transparency, security, centralization, supply chain traceability, and regulatory compliance. The promising technology has the potential to enable several boons across diverse fields like healthcare, supply chain management, manufacturing, cross-border payments, finance, and energy trading. Telemedicine primarily aims to facilitate the transmission of healthcare data through electronic channels, enabling users to access medical services. It supports healthcare services around the globe, aids in early diagnosis and treatment, and assists with remote care by provisioning effective healthcare that is safe, secure, and reliable. However, there are challenges associated with Personal Health Records (PHR) due to lack of ownership of the data, accuracy, reliability, and data transaction security. The architecture presented in this work enables us to benefit from telemedicine and securely share PHR. The proposed model offers a permissioned network-based Hyperledger Fabric blockchain framework for secure PHR sharing amongst healthcare providers. The Byzantine Fault Tolerance consensus mechanism protects patient privacy, and the IPFS protocol is used to store the data off-chain. Additionally, the smart contract is utilized for providing patients with granular access control over PHR data. Hyperledger Caliper is used as a benchmarking tool to test this technology and determine the average latency rate for viewing and updating the PHR by healthcare providers along with analysis of CPU and memory utilization. As a result, our goals in telemedicine to improve secure sharing and give the patient access control are achieved.

INDEX TERMS Blockchain technology, data sharing, security, chaincode, IPFS, privacy, personal health record.

I. INTRODUCTION

Telemedicine refers to the delivery of health services and information via the use of telecommunications and electronic information technologies. It enables patient-to-clinician communication and suggests monitoring along with remote admissions. Soon, there will be an absolute need for a secure platform for telemedicine for storing, securing, and sharing the personal health records (PHR) of the patient [1], [2]. These services include the administration of access restrictions for patient information, preserving patient data from illegal access, and modification and deletion of stored data [3]. The paper [4] outlines the creation and implementation of a Patients' E-healthcare Records Management System (PRMS) with the objective of safeguarding privacy while utilizing third-party cloud platforms. PHR is vital and highly vulnerable health-related patient information for diagnosis and precise treatment. The amount of patient data stored in numerous health records is constantly and profoundly increasing due to the limited scope and accessibility of

The associate editor coordinating the review of this manuscript and approving it for publication was Peter Langendoerfer.

existing health records presented as fragmented information owned by individual hospitals [5]. The approach mitigates substantial privacy and security risks linked to the storage of sensitive healthcare data on cloud services. A crucial challenge in the healthcare industry is to ensure that health records are securely accessible and shared across many stakeholders [6], viz. hospitals, physicians, patients, and researchers [7], [8]. But it also raises the issues of privacy, security, and data tampering which may compromise patient care. In need of that, relying on current centralized systems leads to a high risk of data leakage and slow data processing. So, the proposed model uses Blockchain Technology to address the challenges associated with centralized systems. Blockchain technology has fascinated researchers due to its secure, decentralized data management and transparency. [9] propose a holistic framework that integrates IoT communication security protocols with sophisticated protection measures specifically designed for smart healthcare contexts, incorporating encryption techniques to ensure secure data exchange. The paper [10] focuses on significant privacy concerns and presents an innovative approach to improve the security and reliability of electronic health record (EHR) interactions by trust evaluation mechanisms and cryptographic techniques.

Blockchain is concerned with the secure sharing of information between network users and solving the interoperability of data [11]. The idea behind blockchain technology is to provide the current status of every transaction and store a huge amount of data in an organized manner. The updates carried out in the distributed ledger will be documented in the transaction history log of the blockchain network [12]. Blockchain also facilitates smart contracts that ensure trust and confidentiality in the form of a predefined set of code having access rights to medical information without the involvement of any third party [13]. Reference [14] provided test environments for smart health devices for security measures from attacks like Denial of Service and man-in-the-middle attacks.

In this work, the contributions are as follows:

- A private permissioned blockchain platform for the secure sharing of PHRs is proposed for Telemedicine applications
- Design of a multi-tier architecture based on blockchain with consensus and system workflows to secure the sharing of records with the off-chain data structure.
- Developed a model that facilitates smart contracts with different access policies and authentication rules to access the network.
- Implemented off-chain storage with the Interplanetary File System (IPFS) and provided encryption techniques for the data.

In this paper, section II provides the problem background and existing solutions; section III gives a brief introduction to Blockchain and Hyperledger fabric; section IV explains the proposed private permissioned blockchain for personal health records. Section V presents the implementation of the proposed system, and section VI presents the evaluation results.

II. RELATED WORK

Several contributions have been proposed to blockchain-based architectural design providing probable solutions to the existing bottlenecks of Electronic Health Records (EHR). The current trend is not focused on issues related to PHR. In [15], a novel permissioned distributed network is provided to the patients to collect, store, and maintain their PHR securely. In [16], the convergence of Agent-Based Modeling with blockchain smart contracts is proposed to improve participatory decision support systems [17]. The research [18] introduces a patient-centric healthcare framework reference architecture that aims to enhance semantic interoperability among different healthcare systems. The architecture utilizes blockchain, cloud computing, and the Internet of Things (IoT) to guarantee the secure, efficient, and compatible management and sharing of healthcare data.

In [19], a general blockchain with off-chain data storage using an IPFS system and Proof of work as a consensus mechanism is proposed. To protect patient confidentiality and privacy, patient-centric access control by the Hyperledger fabric platform is proposed in [20]. The platform provides privilege for peers to run blockchain code. In [21], a permissioned blockchain called Hyperledger Besu is suggested to assess its performance and use IPFS and Istanbul Byzantine Fault Tolerance (IBFT) to facilitate secure data sharing. The paper [22] suggests a hybrid framework that integrates blockchain and edge computing to effectively and securely handle Electronic Health Records (EHRs). The architecture incorporates attribute-based cryptographic methods to increase both privacy and access control. In [23], a Membership Service Provider in Hyperledger fabric with different chaincodes to handle the business logic among stakeholders is presented. An EHR management system powered by blockchain increases security, transparency, and interoperability while building trust amongst healthcare users because it does not require the participation of outside service providers [24]. In [25], patient medical data is stored in the form of a content-addressed hash value in the blockchain network. Each report in the IPFS version control system is associated with its corresponding hash value in the Distributed Hash Table (DHT). In [26], a patient's medical report can be acquired by the stakeholder by leveraging the hash value linked to the report and using a blockchain network to store a patient's health record hash value. In [27], a patient-centric agent (PCA) that uses blockchain technology to ensure the privacy of data among peers during communication is proposed. In [28], a vital key management technique was designed to guarantee the security of healthcare information, and it is accomplished by the utilization of the Advanced Encryption Standard (AES) algorithm. At the same time, the peers exchange data by using a cryptographic private key.

In [29], an architecture to store and share data using IPFS in the Ethereum blockchain and the Attribute-Based Encryption (ABE) technique is presented. In [30], a cohesive system-based model was suggested that combines off-chain and on-chain storage mechanisms by utilizing the consortium blockchain and IPFS. MedBlock is an extension of the Medclick application [31] that provides a single platform to save medical data and interact with medical organizations in which patients own full privileges over their health data. In [32], an architecture for the secure sharing of healthcare data is proposed by including privacy-preserved federated learning that enhances efficiency and accuracy. In [33], a Blockchain system for EHR is developed that requires authorization to access the Patient's data and transfer the data among stakeholders. MediChain [34] is a permissioned chain network proposed to work in trusted environments. In [35], a blockchain-based network called MeDShare is proposed to achieve secure sharing of data among cloud service providers. In [36], the Healthchain model based on blockchain is presented for preserving privacy using fine-grained access control. In [37], a novel architecture is proposed that facilitates storing and sharing the PHR in Hyperledger fabric, and it evaluates the performance using Hyperledger caliper with a limited set of peers. In [38], the RAFT consensus mechanism is utilized in Hyperledger fabric for healthcare data. The paper [9] emphasizes the significance of tackling ethical and regulatory considerations. These responsibilities encompass upholding patient independence, safeguarding data privacy, and ensuring the equitable availability of healthcare services. This showed solutions to robust authentication and provided a resilient design. In [39], the Hyperledger Caliper was utilized to assess performance improvement in terms of transaction latency, throughput, memory, and CPU utilization after implementing a patient-centric architecture on the Hyperledger Fabric.

Table 1 depicts the comparison between existing state-of-the-art blockchain-based frameworks related to the type of blockchain key technologies, key points, and their limitations. As mentioned in Table 1, the major limitations in the papers [6], [20], [24], [29] are lack of interoperability, scalability, security and in the papers [31], [33], [40] are low throughput, and access control issues. The current work mainly focuses on overcoming limitations of access control, interoperability, throughput, and scalability issues.

A. CASE STUDIES

The world is running at the pace of demand for our current needs in telemedicine. Gem Health is a blockchain network that connects businesses and healthcare industries. This business attempts to resolve the challenges associated with patient-centric treatment and operational efficiency. The solution is to develop a healthcare ecosystem connected to a universal data infrastructure utilizing blockchain technology. Identity management systems, data storage, and smart contract apps based on shared data infrastructure are all part of the Gem Health blockchain network. Many blockchain-based applications are used to allow several healthcare providers to access the same data through the Gem Health network. Coordination and communication between different healthcare professionals are hampered by closed medical record repositories and bookkeeping procedures [41].

Mediclaim is another emerging healthcare platform that makes use of blockchain technology for healthcare services. Mediclaim is a framework that encompasses two kinds of blockchains, such as Hyperledger Fabric, to facilitate accessibility to medical records, and Ethereum, to run all the platform applications and services. Since medical data is extremely sensitive in both social and legal contexts, permissioned blockchains like Hyperledger Fabric aid in maintaining the anonymity needed for such applications. Hyperledger Fabric is an optimal solution for overseeing access to health information due to its ability to provide many levels of authorization. This empowers data owners to determine the accessibility of different parts of their data selectively.

III. METHODOLOGY

A. BACKGROUND

A Blockchain is a decentralized system composed of a sequence of records called blocks, which are linked together using cryptographic methods. Each block includes transaction data, a timestamp, and a cryptographic hash value of the previous block. A blockchain inherently exhibits resistance to data tampering and permanently records transactions between two entities. In contrast to current centralized solutions, blockchain offers data integrity, security, and transparency.

Blockchain's primary attributes are decentralization, durability, accountability, autonomy, immutability, transparency, and traceability. Blockchain networks follow a consensus process to authorize the block intended for adding to the chain. A consensus mechanism in blockchain has an inbuilt fault-tolerant service to identify faulty blocks and to make arrangements among multiple agents in the network. The three categories of blockchains, such as Public (Permissionless), Private (Permissioned), and Consortium, are used for securing the block data. In a Permissionless blockchain, individuals enjoy unrestricted access to the network with an authorization process to examine transaction data. A permissioned blockchain is a limited network in which only authorized individuals or groups can access and control the data. In Consortium, only the selected member in advance can have the authority to choose the type of service. The remaining members can only access blockchain transactions, and those members cannot be part of the consensus process.

Figure 1 depicts the percentage of permissioned blockchain platforms that are being used in Healthcare Applications. More than 46 % of the applications use Hyperledger fabric for its security, availability, integrity, and confidentiality.

TABLE 1. Comparison table of literature survey.

Year & Citation	Approach	Blockchain Platform	Key Technologies	Advantages	Disadvantages
2017-[24]	EHR management system	Blockchain	NA	Improves transparency, interoperability, and security.	Lack of Confidentiality
2017-[35]	Private Blockchain-based data-sharing scheme	NA	NA	Three-layered scheme with centralized aspects. Requires registration and private keys.	Highly centralized system, Rigid.
2018- [6]	Integrated on-chain and off-chain storage using consortium blockchain and IPFS	Consortium Blockchain	IPFS	Model combining on-chain and off-chain storage	Lack of interoperability
2018-[27]	Patient-centric agent (PCA)	Blockchain	IoT, Encryption	Ensures data security in peer-to-peer communication. Cloud-based structure with third-party reliance	NA
2018-[28]	Key management scheme	Blockchain	AES	Secures medical data, data exchange using private key. Single key raises tampering concerns	Scalability issue
2018-[29]	Data storage and sharing with IPFS in Ethereum blockchain and ABE technology	Ethereum	IPFS, ABE	Proposed architecture for secure data storage and sharing	Lack of access control policies
2018-[34]	MediChain - Hyperledger-based Blockchain system	Hyperledger	Access control module, off-chain data storage, user interface	Manages medical data assets with off-chain storage and Blockchain hashing.	Limited interoperability, Centralized
2018-[20]	Patient-centric access control	Hyperledger Fabric	IPFS	Preserves patient security and privacy. Endorsing peers execute chain code	Low throughput
2019-[40]	Patient-centric access control	Ethereum	Blockchain, ABE	Single platform for saving medical data, patient control, and privacy protection	Lack of interoperability
2019-[32]	Patient-centred approach in a blockchain-enabled healthcare system	Hyperledger Fabric	Hyperledger Caliper	Addresses data privacy, authentication, and immutability. Deployment plan provided.	NA
2019-[36]	Blockchain-based private healthcare network	NA	IPFS	Secure system for sharing EHR from IoT devices.	High integrity and resilience but centralized.
2020-[33]	Permissioned Blockchain-based EHR system	NA	NA	Enables data sharing among patients, clinicians, and laboratories.	Assumes a known participant network, lack of access control
2020-[31]	A novel architecture for gathering, storing, and managing PHR in Hyperledger Fabric	Hyperledger Fabric	Hyperledger Caliper	Provides PHR management but lacks emphasis on data security	Lack of interoperability
2020-[39]	Patient-centric Framework on Hyperledger Fabric	Hyperledger Fabric	Hyperledger Caliper	Evaluates performance in terms of transaction metrics.	NA
2021-[17]	Private permissioned blockchain	Hyperledger Fabric	Smart Contracts	Suitable for secure health records	High Latency
2021-[23]	Membership Service Provider	Hyperledger Fabric	Different chaincodes	Manages business logic, and algorithm for chaincode working	Lack of data access control
2022-[21]	Permissioned blockchain	Hyperledger Besu	IBFT, IPFS	Secure data sharing, and performance evaluation	NA

Smart contracts are self-executing computer programs that operate on the blockchain without the need for middlemen. These programs define the protocols governing the operations and access privileges within a corporation, and a consensus process guarantees their precise implementation. Smart contracts, being integrated into a blockchain, offer the features of immutability and transparency. Smart contracts enable the enforcement of contract conditions and provide consequences for any violations of such provisions [31].

IPFS is a distributed P2P data storage protocol that avoids Censorship and Single-point failure. IPFS uses Content-based addressing for storing, retrieving and distributing the files. Every IPFS file possesses a distinct hash value that can be employed to retrieve the file, and the cryptographic hash functions are used to protect the stored file from modification. IPFS offers a dependable and protected approach to keeping confidential personal healthcare data. Moreover, in the blockchain system, the expense of storing the entire file is substantial, leading to detrimental impacts on the network's overall performance in terms of both delay and scalability. Storing data hashes in the blockchain and files on IPFS enhances the effectiveness of the system.

The transaction flow of any blockchain platform operates on two separate layers. On-chain transactions refer to transactions that are recorded and saved in the blockchain-distributed

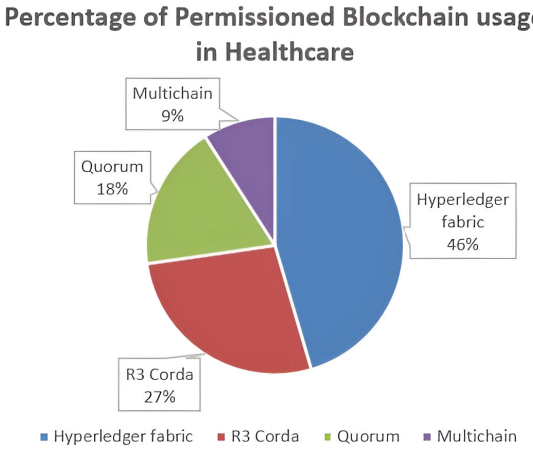

FIGURE 1. Percentages of permissioned blockchain platforms usage in healthcare applications.

ledger and Off-chain transactions that occur outside of the blockchain and are stored in a separate database like CouchDB or StateDB. The network's performance began to degrade as the large queue of pending transactions took significantly longer to execute. During On-chain transactions on the blockchain, there are substantial business and storage space costs involved, whereas Off-chain transactions do not store transactions for each node within the storage space. Off-chain storage can be used by any participant in the network who is willing to keep specific transactions. Off-chain improves computational efficiency; computations executed off-chain are deterministic and not consensus-based. So, these are the main reasons to use off-chain storage data in our proposed solution.

B. BLOCKCHAIN TECHNOLOGY FOR MEDICAL E-HEALTH RECORDS

Blockchain can bring a lot of changes and have a great impact on healthcare reports in which storing, securing, and maintaining medical data is crucial and expensive [33], [42]. The challenges associated with centralized systems, like security and reliability to uphold health data by third parties, are addressed by blockchain technology. Blockchain obviates the necessity of intermediaries and ensures that all participants in the network undergo verification. This is very useful for patients who visit different hospitals and need to save the history of all their medical reports. Such patients can access their data anytime they need using blockchain and the repetition of laboratory tests when shifted to another hospital can be avoided. The blockchain ensures that the data is stored securely and the data is available to the patients when it's required and enables the patients to share their authentic medical data for research purposes.

C. HYPERLEDGER FABRIC

Hyperledger Fabric is an open-source blockchain framework hosted by the Linux Foundation. Fabric networks are designed with permissioned access, ensuring that the

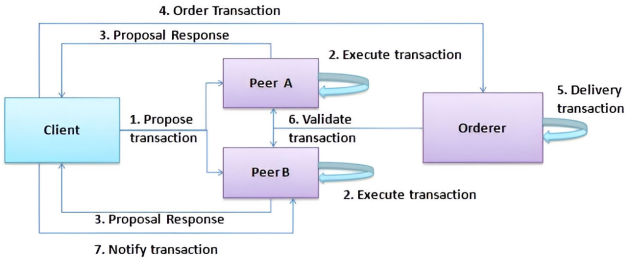

FIGURE 2. Hyperledger fabric transaction flow.

identities of all participants are both recognized and verified. Fabric introduces a distinctive blockchain framework that aims to provide robustness, adaptability, expandability, and confidentiality. Hyperledger Fabric is comprised of nodes to form a network. These nodes perform three roles:

1) Clients: These are the end-users that broadcast transactions for ordering, submit transaction proposals to be carried out, and help orchestrate the phase of carrying out transactions.
2) Peers: The individuals perform the tasks of executing, validating the transactions, and maintaining the ledger. Only endorsing peers have the right to perform the transactions.
3) Ordering service nodes: The nodes in Hyperledger Fabric that comprise the ordering service are responsible for achieving consensus.

Hyperledger fabric architecture adheres to a consensus called Ordering service that is divided into 3 phases: Endorsement, Ordering, and Validation. Hyperledger fabric transaction flow is illustrated in Figure 2:

1) Propose transaction: Client application proposes transaction to peers
2) Execute proposed transaction: Peers will execute the proposed transaction. They do not update the ledger. Each execution will capture a set of read-and-write (RW) data called RW sets
3) Proposal response: RW sets are returned to the application, which is assigned by each peer or endorser
4) Order transaction: The application submits a response as a transaction to be ordered
5) Delivery transaction: The Orderer delivers the transaction to the committing peers. They follow different ordering algorithms
6) Validate transaction: Committing peers validate the transaction
7) Notify transaction: Committing peers notify the transaction

Hyperledger Fabric utilizes chaincode having predetermined logical conditions that are automatically executed after the conditions are satisfied to write smart contracts. It provides a channel-based mechanism for supporting the transaction's confidentiality and integrity and also facilitates the establishment of communication channels among

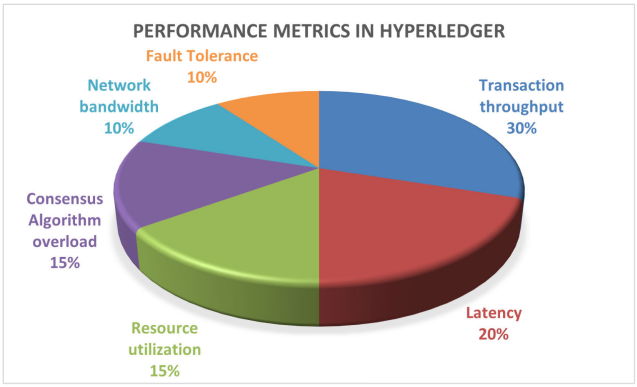

FIGURE 3. Percentage of performance metrics in hyperledger fabric.

various organizations to ensure privacy and security. Certificate Authority (CA) in Hyperledger Fabric is specifically designed for the Hyperledger Fabric distributed ledger architecture that offers features for registering identities, issuing Enrollment Certificates, and managing certificate renewal and revocation. CA functions as a system administrator and an authority for managing the organization. The role of CA is to remove the faulty nodes from the system and to maintain the system's health. It generates, distributes, and manages the digital certificates and also establishes the public-private key () for each Patient. The CA uses the Patient's private key to decrypt block data to maintain the state regulation of block information and medical research. The Membership Service Provider (MSP) is a component of Hyperledger Fabric that simplifies membership processes. The MSP encapsulates the protocols and cryptographic techniques that underpin user authentication, certificate validation, and issuance. Figure 3 depicts the percentage of considerable performance metrics of Hyperledger fabric leading by transaction throughput by 30 %, followed by latency by 20%, resource utilization by 15%, consensus algorithm overhead by 15%, network bandwidth by 10%, and fault tolerance by 10%.

IV. PROPOSED PRIVATE PERMISSIONED BLOCKCHAIN FOR PHR

Several contributions have been made to the discourse on blockchain-based architectural design which provides possible solutions to the constraints currently in Electronic Health Records. With the rise of demand for Tele-medical services, a need for a standard, secure, and trustable platform for PHR data sharing and storage systems that ensures patient privacy and confidentiality is increased. To fulfill the security measures, the proposed model uses a blockchain network that has great potential to carry out security issues in an effective manner.

The blockchain incorporates rigorous validation procedures to ensure that data is verified and approved before being incorporated into the transaction using consensus mechanisms. The absence of a single point of failure is ensured by the distribution of updated ledgers among the network nodes. The blockchain can authorize the network

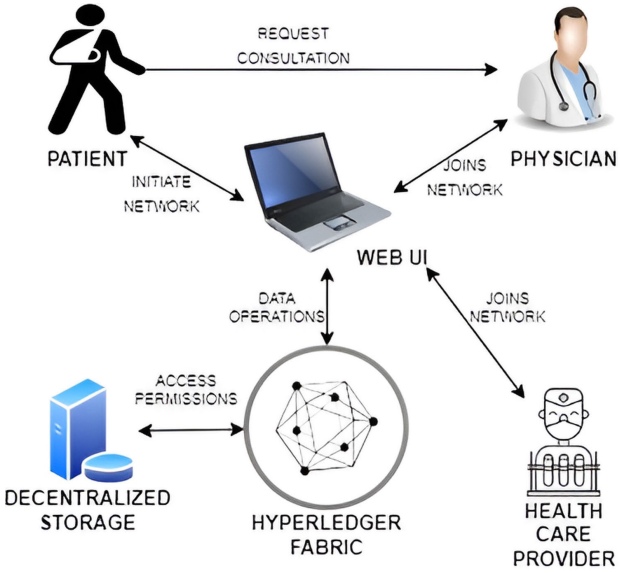

FIGURE 4. Private permissioned blockchain data workflow in telemedicine.

members and prevent the leakage of data to any untrusted parties. Private permissioned blockchain is the best choice for sharing PHR in the blockchain network to achieve patient data security, privacy, and confidentiality. The workflow of Private permissioned blockchain for PHR in telemedicine is outlined below steps and depicted in Figure 4:

1) The Patient requests an online consultation appointment, and once the appointment is fixed, the physician gets authorized and joins the Patient's network.
2) The Physician requests for patient medical history records by accessing into Patient's PHR network. The network needs to check the accessibility permission of the physician.
3) The Patient, who is the only owner of the data, grants access to the physician, and the blockchain network verifies the privileges and permissions.
4) Blockchain provides the data required by the physician based on the access privileges given by the Patient.
5) The Physician accesses and reviews the data to prescribe the medicines. The data accessibility will be revoked after a specific time allotted by the Patient.

A. PHR BASED ON HYPERLEDGER FABRIC

Hyperledger fabric platform is resorted as a Private Permissioned blockchain network as it provides optimal solutions for the challenges associated with healthcare data. It allows ledger data to be saved in multiple data formats and offers various access levels, access control, and running different channels. Hyperledger Fabric allows other members to request access to the data and makes it easy to interact. Every interaction is secure, transparent, and saved in the distributed ledger. The main components of Hyperledger fabric in telemedicine are:

TABLE 2. Summary of notations.

Parameters	
λ	Propagation Delay
T(t)	Transaction Delay
Q(t)	Queuing Delay
V(t)	Verification Delay
σ	Signature Generation and Verification
P(b)	Consensus mechanism to validate block
L(t)	Patient Health Leger at the time
NR	Number of Rounds
F(t)	Fault Detection and Recovery
PrK	Private Key
PuK	Public Key corresponds to PrK
D	Data

- Data Owner/Patient
- Healthcare providers
- Application
- Hyperledger fabric blockchain network
- Local storage system

In this Hyperledger fabric, the Patient is the owner, and the healthcare providers like Physicians and medical test laboratories can be peers with ordering services. Peers can generate or solicit data using a client application, which serves as a medium of communication with the blockchain network. Hyperledger Fabric utilizes smart contracts written in chaincode, which encompass logical instructions that are executed at any time a function is activated. The Hyperledger fabric utilizes a CA to grant authorization and issue certificates to the peers involved in the network, facilitated by a customized MSP. The creation of a private channel is to generate and maintain a separate ledger of transactions and it is made possible by Hyperledger Fabric during transactions. Only the active participants in the channel can access the ledger and the participants can actively participate in more than one blockchain network.

B. PROPOSED ARCHITECTURE FOR A HYPERLEDGER FABRIC BLOCKCHAIN SYSTEM FOR PHR

The proposed private permissioned blockchain network for PHR integrates with Hyperledger fabric and an off-chain IPFS storage model. Hyperledger fabric is efficient for healthcare data security in storing and sharing PHRs. As it is provided with different access levels, fine-grained access control over PHR is possible. Within this private permissioned network, every user is authenticated, enrolled, and linked via distinct channels to guarantee confidentiality and expandability.

1) LATENCY ANALYSIS OF BFT CONSENSUS

The proposed system uses the Byzantine Fault Tolerance (BFT) consensus algorithm for standard data communication. Fabric processes more than 3,500 transactions per second, making it far more efficient than existing public blockchains. Latency analysis of single channel fabric blockchain can be facilitated to assess the performance and efficiency of the consensus algorithm. Table 2 contains the summary of notations used in the proposed study.

Ensuring the integrity and authenticity of the data is of utmost importance, and hence, signature generation and verification play a vital role in data security. Signature Generation can be depicted as:

$$SG = Sign_{PrK}(D) \tag{1}$$

Equation 1 represents the process of generating a signature using the private key for the data D. The process of verifying a signature can be represented as follows:

$$Verify_{PuK}(D, SG) \tag{2}$$

The equation 2 denotes the verification algorithm applied to data D using the signature generated. So, the Signature Generation and Verification can be represented as:

$$\sigma = SG + Verify_PuK(D, SG) \tag{3}$$

The following aspects are considered for detecting the faults during the detection process.

- FD for Fault Detection
- T_detection for the time of fault detection
- T_failure for the time of node failure
- T_recovery for the time during which recovery is completed
- FR for Fault Recovery

Mathematically, fault detection time can be shown as:

$$FD = T_{detection} - T_{failure} \tag{4}$$

and Fault Recovery can be shown as:

$$FR = T_{recovery} - T_{failure} \tag{5}$$

Fault detection and recovery can be represented with the following:

$$F(t) = FD + FR \tag{6}$$

Consensus protocol typically involves steps like pre-processing, data communication, and post-processing. The consensus mechanism to validate the block in BFT can be represented as:

$$P(b) = P_{pre-processing} + P_{data} + P_{post-processing} \tag{7}$$

where

- P_pre-processing is time spent on pre-processing steps
- P_data is time spent on actual data communication
- P_post-processing is time spent on post-processing steps

Total latency in BFT consensus involves breaking latency analysis into various components with the sum of Propagation delay, Transmission delay, Queuing delay, Verification delay, Signature Generation and Verification, Block Ledger time, Consensus mechanism to validate block, Fault detection and recovery, and Number of Rounds is given in 8:

$$TotalLatency = \lambda + T(t) + Q(t) + V(t) + \sigma + P(b) + L(t) + F(t) + NR \tag{8}$$

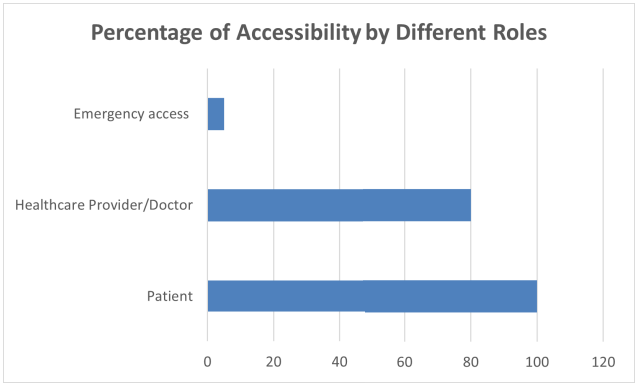

FIGURE 5. Percentage of accessibility by different roles.

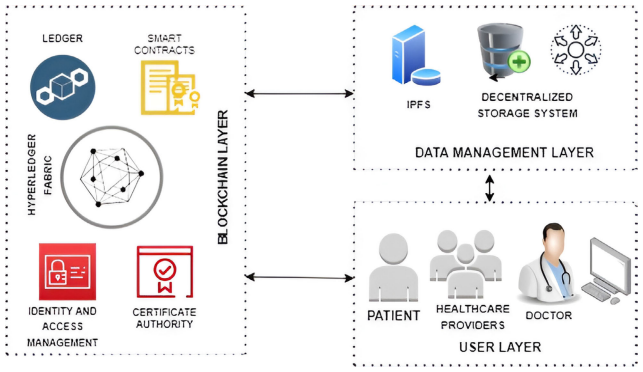

FIGURE 6. Layered architecture.

2) PROPOSED LAYERED ARCHITECTURE

The proposed work uses layered architecture to depict the process involved in securely storing, retrieving, and sharing the PHR's data among stakeholders. The proposed architecture has three layers: The user, the Blockchain, and the Data management layers. The user layer includes external users interacting with each other via web UI or decentralized applications. The blockchain layer consists of hyperledger fabric operations like maintaining metadata and smart contracts containing the permission management rules for sharing data. The data management layer consists of off-chain encrypted data and its hashes in the blockchain. Figure 6 illustrates different layers involved in the proposed architecture.

1. User layer: In this layer, users like patients, doctors, or healthcare providers interact with each other via web UI or decentralized applications. Each user will be given a unique blockchain ID to join the network.

2. Blockchain layer: In this layer, Hyperledger fabric is considered a private permissioned blockchain in which the nodes in this network are predetermined and assigned to the blockchain. Each node is responsible for validating and adding the data. Numerous smart contracts are essential for the consensual deployment of the blockchain.

In the Authorization contract, the hyperledger fabric issues authorized certificates to every user joining the network using CA. A list of the user's public key, the blockchain allotted RegID, and their role in the contract of the blockchain will be provided. This contract will be executed whenever there is a request for a transaction from any user and checks their authorized ID. After Authorization, the request will be sent to the accessibility contract.

In the Accessibility contract, the permission contract's request will initiate the execution of the accessibility contract. This contract outlines the logical rules that govern the allocation of various permissions to different roles within the blockchain. This also notifies the changes made by the owner to the ledger by healthcare providers. The list of access permissions in the system is shared in the table 3,4 below:

In Figure 5, the percentage of accessibility by different roles like Patient, Healthcare provider/Doctor, and Emergency access is shown. The Patient has the whole data accessibility, but the other roles have only limited access with fixed time slots. All the access operations in the blockchain will be stored in the hyperledger and also maintain the Patient's record and an encrypted pointer to the Patient's medical record. The record's pointer will undergo encryption and will be saved in the blockchain, while the Patient's health data and data access IDs will be stored off-chain in the Patient's local database. Cryptographic public and private keys are utilized for data encryption, decryption, and access control.

3. Data management layer: Data in this layer is stored in a distributed manner via the IPFS. IPFS is resilient to single-point failures and operates independently of third-party dependencies. The IPFS storage system bears a resemblance to blockchain technology.

C. WORKING OF PROPOSED ARCHITECTURE

Given that patients' data vary in the amount of information provided, it is advantageous to keep the data off-chain, outside of the blockchain. The data will undergo an encryption process and be stored in the Patient's storage system, while the reference to the hash value of each record will be recorded in the on-chain blockchain. On-chain storage data ensures the quality of being unalterable, while off-chain data ensures the confidentiality of the Patient. Using the off-chain data storage method addresses scalability, privacy, and efficiency concerns. The following steps give the workflow of the proposed architecture to join and add records to the blockchain network, and the process is depicted in Figure 7:

1) User/ Healthcare provider/ Doctor needs to join the network using individual RegID. To obtain RegID, healthcare providers must register with CA in the Hyperledger Fabric network using MSP.
2) Utilizing a Web-based user interface, a healthcare provider/user transfers the Patient's health report.
3) Using the Byzantine Fault Tolerance consensus approach, the uploaded reports are validated by ordering peers. The integrity of the network is maintained through the mining process.

TABLE 3. List of access permissions for Health Provider/Doctor Role.

Functionality	Description	Read	Write	Update	Delete	Special Permissions
Patient Records	Access to full patient history	Yes	Yes	Yes	No	Export, Share with other Providers
Diagnostic Test Results	Viewing test reports	Yes	Yes	Yes	No	Request Additional Tests
Treatment Plans	Managing treatment plans	Yes	Yes	Yes	No	Submit for Authorization, Modify Existing Plans
Appointment Scheduling	Managing scheduling calendar	Yes	Yes	Yes	No	Override scheduling conflicts, View availability
Prescription Management	Prescribing medicine	Yes	Yes	Yes	No	E-prescribe, Refill, Manage formulary preference
Consent Management	Handling patient concerns	Yes	Yes	Yes	No	Verify consent, Document patient refusal
Emergency Access	Access Critical data	Yes	No	No	No	Emergency Override

TABLE 4. List of access permissions for Patient Role.

Functionality	Description	Read	Write	Update	Delete	Special Permissions
Personal Information	Access to personal information	Yes	Yes	Yes	No	Request corrections
Medical Records	Viewing treatment records	Yes	No	No	No	Download, Share with providers
Appointment Scheduling	Scheduling and Rescheduling	Yes	Yes	Yes	Yes	Cancel appointments, Reschedule
Prescription History	Viewing Prescription	Yes	No	No	No	Request refills
Consent Management	Manage Consent	Yes	Yes	Yes	Yes	Revoke consent, Provide consent
Appointment Reminders	Receiving reminders	Yes	No	No	No	Set preferences for reminders
Emergency Contact	Manage or Update Contact	Yes	Yes	Yes	Yes	Update contact details

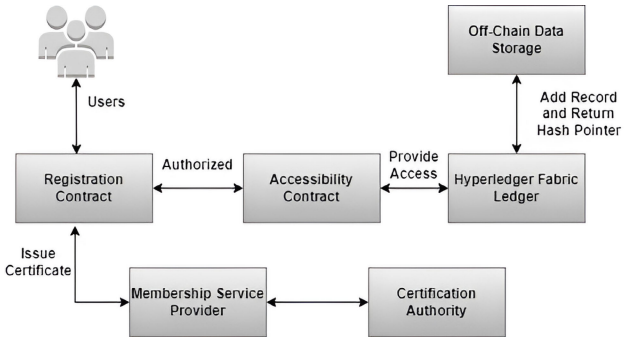

FIGURE 7. Data flow of proposed architecture.

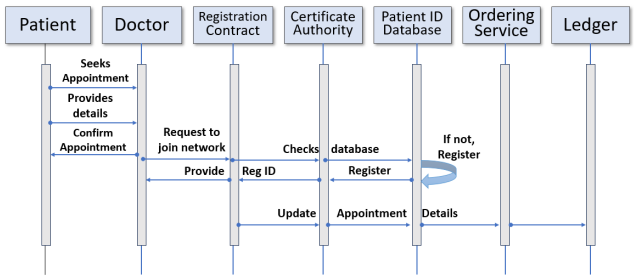

FIGURE 8. Process of appointment.

4) For the peers of the blockchain network to verify the transactions with their local copies and create the block, the orderer distributes the transactions to them.
5) The verified transaction is stored in the IPFS decentralized file system. The content-addressed hash value is created by IPFS and integrated into the blockchain network. Access to the list of transactions is restricted to registered peers within the network. Physicians must complete the registration procedure to become a member of the blockchain network.

V. TRANSACTION FLOW IN HYPERLEDGER FABRIC PHR ARCHITECTURE

The work sequence flow is used to show the operations involved in processing the appointment and for adding/updating the ledger data. Figure 8 depicts the sequence of steps followed by the network members for the appointment process. The appointment details will be stored on the blockchain network. At first, the Patient requests a teleconsultation appointment with a doctor by submitting the Patient's identification and public key. The doctor schedules the appointment and requests a registration contract to join the network using patient details. The doctor submits the public key to the CA to generate a unique ID. The generated ID is shared with the doctor, and the appointment details will be updated in the ledger.

In Figure 9, a sequence adhered to for adding or updating the record details in the ledger is shown. To go through teleconsultation, the Patient gets to verify the doctor's ID by the registration contract. Through the contract, the Patient checks the doctor's ID validity. They register and provide an ID with verification if it is not registered. To examine, the doctor requests access to patient medical data from the accessibility contract. This gives the response status whether the data access is granted or denied. The ledger provides patient data from storage to the doctor if access is granted. The doctor examines the Patient and updates or writes a medical report. The new report will be validated using the ordering service in the ledger. Upon validation, the report is sent to an off-chain storage system. The medical report is securely encrypted and saved off-chain. The blockchain ledger contains the hash pointer of the data that is stored on-chain.

A. SMART CONTRACT DESIGN

This section includes a smart contract design providing details of member registration and access permissions for the Patient, doctor, and healthcare provider. A smart contract is a set of a program written in logical code to adapt all the conditions needed by the parties in the network for trust and

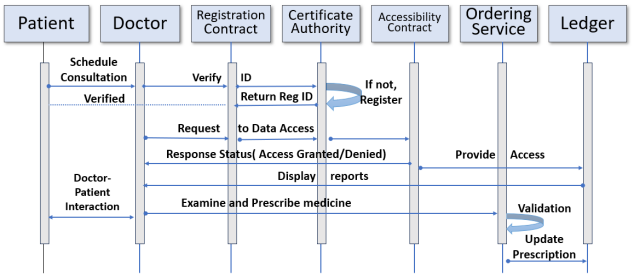

FIGURE 9. Adding or updating the ledger.

TABLE 5. Algorithm notations.

Notation	Description
P_k	Public key
Member ID	Registered ID
P_{id}	Patient ID
D_{id}	Doctor ID
HP_{id}	Healthcare provider ID
R_j	Record number

interoperability. The algorithm's notations are described in the table 5:

In Algorithm 1, the scenario for network member registration is presented whenever a member needs to join or access the data. The member provides their public key and role, and if they are already registered, they provide their registered member ID. The algorithm checks for ID validity. If an ID exists, it adds a member to the network. If not, it registers a member and returns the registered ID. This algorithm provides an example of logging as an existing member of the network or signing up as a new member for a particular network providing the role.

Algorithm 1 Algorithm for Member Registration

```
Input: P_k,Member ID, Role
Output: Authorization status
 procedure Member(ID)
  while(True) do
   if (ID is valid) then
     Add ID to blockchain network
     Print valid member
   else
     Register(P_k, Role)
     Return ID
   endif
  endwhile
 endprocedure
```

In Algorithm 2, the presentation illustrates the access rights for patient roles. Here, the individual submits a public key, patient ID, and the specific record ID they wish to retrieve. Upon validating the patient ID, the system verifies the record ID that the Patient has requested. If the record is present, the Patient can access and modify their personal health data. If no such record exists, the Patient can create and submit a new record. During the appointment session, the contract verifies the patient ID and doctor ID assignment. If the doctor's ID is valid, the Patient can authorize access to their Personal Health Record (PHR). Otherwise, they can revoke the doctor or healthcare provider's permission. Access to the data is restricted if the patient ID is invalid.

Algorithm 2 Accessibility to Patient Role

```
Input: P_k, P_id, R_j
Output: Access to R_j
 procedure Patient (P_id)
  while(True) do
   if (P_id is valid) then
    if (R_j exists) then
      Update(P_id, R_j)
      Read(P_id, R_j)
    else
      Write(P_id, R_j)
    elseif
    if appointment(P_id,D_id) then
     if (D_id is valid) then
      Grant(D_id, R_j)
     else
      D_id is invalid
     endif
    else
     Revoke(D_id, R_j)
    endif
   else
    P_id is invalid
   endif
  endwhile
 endprocedure
```

In Algorithm 3, the scenario of access permissions provided to a doctor or healthcare provider is presented. Firstly, they check the validity of the doctor or healthcare provider. If the ID is verified, the doctor gets authorization to access a particular patient record. The doctor can view or update the details in the report. If not, the doctor can create a new record and fill in the patient data. If the doctor's ID is not validated, they cannot get permission to access the patient data.

B. SECURITY ANALYSIS

In this sub-section, we conduct an informal analysis to evaluate the importance of the security efficiencies of the algorithm being suggested.

Resilient to an ID forgery attack In this forgery attack, the adversary creates a fake ID that mimics a P_id or D_id, following a predictable pattern without any appropriate signing key. To make any legal entity's communication process, adverse forces must extract the source parameters, such as P_id and H(R_j(data)). The certification authority forces the forged ID to undergo strong ID verification upon

Algorithm 3 Accessibility to Doctor/Health Provider Role

Input: P_k, D_{id}/ HP_{id}, R_j
Output: Access to R_j
  procedure Doctor (D_{id})
   whileTrue **do**
    if (D_{id} *is valid*) **then**
     if (D_{id} *is granted*) **then**
      if (R_j *exists*) **then**
       Update(D_{id},R_i)
       Read(D_{id}, R_j)
      else
       Write(D_{id}, R_j)
      elseif
      else
      D_{id} *is not granted*
      endif
     else
      Invalid D_{id}
     endif
   endwhile
  endprocedure

logging in, as the Membership Service Provider (MSP) generates the ID. You will lose access if you don't verify. Thus, the proposed algorithm is resilient to ID forgery attacks.

Resilient to Denial of Service Attack The adversary in this DoS attack aims to render a computer system or network service inaccessible to its intended users by flooding it with an excessive number of invalid requests. Our proposed scheme, which is a private blockchain network, provides a limited number of specialized services tailored to specific roles. It also enforces rigorous input validation to assure the legitimacy of requests.

Resilient to Improper Access Control The proposed algorithm strictly adheres to role-based access control, in which each role has its own specific and special permissions for accessibility. In the proposed method, the local node contains the actual patient data and follows the IPFS protocol. Every IPFS node can keep its logs for troubleshooting, monitoring performance, and managing local activities. The IPFS software running on that node normally manages these logs. In such a way, we can restrict access control for different roles to avoid improper access control.

VI. RESULTS AND PERFORMANCE EVALUATION

Hyperledger Fabric, along with its sandbox and Hyperledger Composer module, is utilized for the implementation of smart contracts on a virtual network. Docker is an operating system container that facilitates the creation, deployment, and execution of hyperledger-based apps within the container. With the use of docker, hyperledger fabric and composer can run inside the container. The proposed system used Hyperledger Caliper for benchmarking the performance metrics

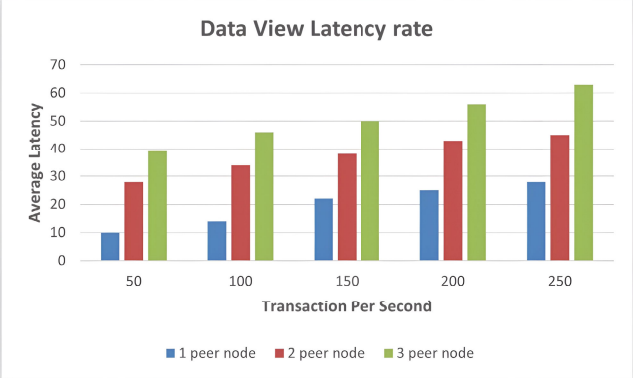

FIGURE 10. Average latency rate of viewing PHR data.

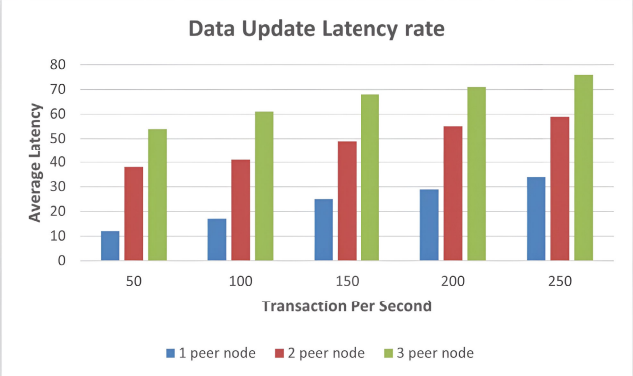

FIGURE 11. Average latency rate of updating PHR data.

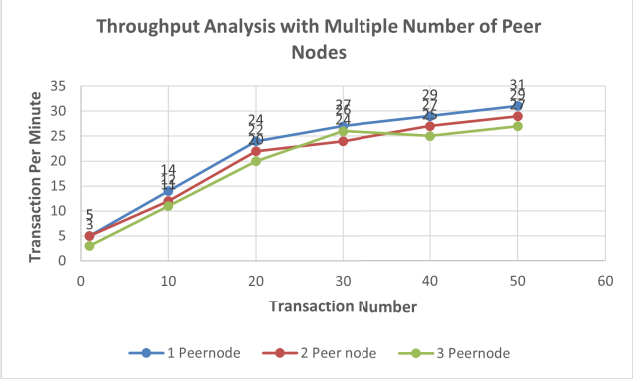

FIGURE 12. Throughput analysis with 1, 2, and 3 peer nodes in the same network.

in the blockchain network to calculate latency, resource allocation, and throughput analysis. The configuration details of the system to provide the implementation and produce the analysis are given in table 6.

A. RESULTS

When executing the Hyperledger Caliper to benchmark resource consumption, various parameters are considered, such as Average Memory Consumption, Average CPU Consumption, and the Amount of Data in and out. Table 7 shows the parameter values while running with a single peer network, two peers, and three peers with orderer CPU

TABLE 6. System configuration.

Component	Configuration
Operating System	Microsoft Windows 10 Professional (64-bit)
System Under Test	Hyperledger Fabric, Version 1.4.x, Blockchain Framework
CPU, Memory	Intel Core i5-1235U Processor, 4 Cores, 8 Threads, 16GB DDR4 RAM
Off-Chain Database	InterPlanetary File System (IPFS) for decentralized data storage
Test Language	Go Programming Language (Version 1.14.x) for smart contract and application logic development

TABLE 7. Resource allocation.

Type	Name	Memory (Avg)	CPU % (Avg	Data In	Data Out
Docker	1Org1peerFabric.example.com	250MB	3.00	3.4MB	2MB
	1Org2peerFabric.example.com	200MB	3.02	3MB	1.8MB
	1Org3peerFabric.example.com	100MB	1.12	2MB	3MB

consumption in the same network. Multiple peers with different incoming and outgoing traffic have been tested for average CPU consumption. In this, 1Org 3peer has the minimum CPU consumption with outgoing traffic of 3MB per second during the test showing that it has improved responsiveness with effective resource utilization.

Figure 10 shows the average latency rate for viewing the data of PHR considering the 1, 2, and 3 number of peer nodes in a network with 50, 100, 150, 200, and 250 transactions per second. This shows a slight increase in latency with the increase in the number of peer nodes along with the rise in transaction flow. In Figure 11, the graph displays the average rate of latency for updating data in the PHR by any user in the network. Considering 1, 2, and 3 number of peers in the network while increasing the transaction flow showed a significant increase in latency rate for the network with more peers. For a single peer network, the proposed work out-performs well and shows that the delay is low. In figure 12, the calculation of throughput is demonstrated by considering the number of transactions per minute in the network having different numbers of peer nodes with multiple sets of transactions. The throughput is elevated in the single-peer node even with the increase in number of transactions per minute. Through the experiment analysis, the latency rate remains low during the transaction of data with efficient utilization of CPU and Memory.

VII. CONCLUSION

PHR contains confidential, and private healthcare information of the Patient. The proposed work presented an architecture for the secure sharing of PHR by involving the Hyperledger Fabric network which is a private permissioned blockchain to store the data. This work also provides the mechanism in which data is accessible to the authorized members of the network according to their access levels defined by the Patient through smart contracts. The healthcare information is stored off-chain using IPFS protocol within the patient database, and its content-address hash is present on-chain in the hyperledger fabric. This work designed the process for teleconsultation for the Patient that is described in the algorithms. BFT is used as the consensus mechanism for the standard transfer of data, and CA, coupled with MSP, authorizes and issues certificates to the members of the network. Our proposed model comes across as an efficient model for the secure sharing of PHR, along with efficient CPU, memory consumption, and low latency rates.

REFERENCES

[1] J. S. Shapiro, D. Crowley, S. Hoxhaj, J. Langabeer, B. Panik, T. B. Taylor, A. Weltge, and J. A. Nielson, "Health information exchange in emergency medicine," *Ann. Emergency Med.*, vol. 67, no. 2, pp. 216–226, Feb. 2016.

[2] M. Swan, "Emerging patient-driven health care models: An examination of health social networks, consumer personalized medicine and quantified self-tracking," *Int. J. Environ. Res. Public Health*, vol. 6, no. 2, pp. 492–525, Feb. 2009.

[3] L. Chen, W.-K. Lee, C.-C. Chang, K.-K.-R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Future Gener. Comput. Syst.*, vol. 95, pp. 420–429, Jun. 2019.

[4] K. Zala, H. K. Thakkar, R. Jadeja, P. Singh, K. Kotecha, and M. Shukla, "PRMS: Design and development of patients' e-healthcare records management system for privacy preservation in third party cloud platforms," *IEEE Access*, vol. 10, pp. 85777–85791, 2022.

[5] J. N. Al-Karaki, A. Gawanmeh, M. Ayache, and A. Mashaleh, "DASS-CARE: A decentralized, accessible, scalable, and secure healthcare framework using blockchain," in *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2019, pp. 330–335.

[6] S. Kumar and M. Singh, "Big data analytics for healthcare industry: Impact, applications, and tools," *Big Data Mining Analytics*, vol. 2, no. 1, pp. 48–57, Mar. 2019.

[7] N. Zeinali, A. Asosheh, and S. Setareh, "The conceptual model to solve the problem of interoperability in health information systems," in *Proc. 8th Int. Symp. Telecommun. (IST)*, Sep. 2016, pp. 684–689.

[8] P. Antón, A. Muñoz, A. Maña, and H. Koshutanski, "Security-enhanced ambient assisted living supporting school activities during hospitalisation," *J. Ambient Intell. Humanized Comput.*, vol. 3, no. 3, pp. 177–192, Sep. 2012.

[9] F. J. Jaime, A. Muñoz, F. Rodríguez-Gómez, and A. Jerez-Calero, "Strengthening privacy and data security in biomedical microelectromechanical systems by IoT communication security and protection in smart healthcare," *Sensors*, vol. 23, no. 21, p. 8944, Nov. 2023.

[10] E. S. Babu, B. V. R. N. Yadav, A. K. Nikhath, S. R. Nayak, and W. Alnumay, "MediBlocks: Secure exchanging of electronic health records (EHRs) using trust-based blockchain network with privacy concerns," *Cluster Comput.*, vol. 26, no. 4, pp. 2217–2244, Aug. 2023.

[11] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. big data (BigData Congress)*, 2017, pp. 557–564.

[12] D. Li, D. Han, T.-H. Weng, Z. Zheng, H. Li, H. Liu, A. Castiglione, and K.-C. Li, "Blockchain for federated learning toward secure distributed machine learning systems: A systemic survey," *Soft Comput.*, vol. 26, no. 9, pp. 4423–4440, May 2022.

[13] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-enabled smart contracts: Architecture, applications, and future trends," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 11, pp. 2266–2277, Nov. 2019.

[14] A. Muñoz, C. Fernández-Gago, and R. López-Villa, "A test environment for wireless hacking in domestic IoT scenarios," *Mobile Netw. Appl.*, vol. 1, no. 1, pp. 1–10, Oct. 2022.

[15] T. B. D. S. Costa, L. Shinoda, R. A. Moreno, J. E. Krieger, and M. Gutierrez, "Blockchain-based architecture design for personal health record: Development and usability study," *J. Med. Internet Res.*, vol. 24, no. 4, Apr. 2022, Art. no. e35013.

[16] M. Laskowski, "A blockchain-enabled participatory decision support framework," in *Social Cultural and Behavioral Modeling*. Cham, Switzerland: Springer, 2017, pp. 329–334.

[17] H. S. A. Fang, T. H. Tan, Y. F. C. Tan, and C. J. M. Tan, "Blockchain personal health records: Systematic review," *J. Med. Internet Res.*, vol. 23, no. 4, Apr. 2021, Art. no. e25094.

[18] A. N. Gohar, S. A. Abdelmawgoud, and M. S. Farhan, "A patient-centric healthcare framework reference architecture for better semantic interoperability based on blockchain, cloud, and IoT," *IEEE Access*, vol. 10, pp. 92137–92157, 2022.

[19] R. Kumar, N. Marchang, and R. Tripathi, "Distributed off-chain storage of patient diagnostic reports in healthcare system using IPFS and blockchain," in *Proc. Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2020, pp. 1–5.

[20] T. Alshalali, K. M'Bale, and D. Josyula, "Security and privacy of electronic health records sharing using hyperledger fabric," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Dec. 2018, pp. 760–763.

[21] K. Shuaib, J. Abdella, F. Sallabi, and M. A. Serhani, "Secure decentralized electronic health records sharing system based on blockchains," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 8, pp. 5045–5058, Sep. 2022.

[22] H. Guo, W. Li, M. Nejad, and C.-C. Shen, "A hybrid blockchain-edge architecture for electronic health record management with attribute-based cryptographic mechanisms," *IEEE Trans. Netw. Service Manage.*, vol. 20, no. 2, pp. 1759–1774, Oct. 2022.

[23] M. Uddin, M. S. Memon, I. Memon, I. Ali, J. Memon, M. Abdelhaq, and R. Alsaqour, "Hyperledger fabric blockchain: Secure and efficient solution for electronic health records," *Comput., Mater. Continua*, vol. 68, no. 2, pp. 2377–2397, 2021.

[24] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *J. Amer. Med. Inform. Assoc.*, vol. 24, no. 6, pp. 1211–1220, Nov. 2017.

[25] Y. Chen, H. Li, K. Li, and J. Zhang, "An improved P2P file system scheme based on IPFS and blockchain," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2017, pp. 2652–2657.

[26] S. Chakraborty, S. Aich, and H.-C. Kim, "A secure healthcare system design framework using blockchain technology," in *Proc. 21st Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2019, pp. 260–264.

[27] Md. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "Continuous patient monitoring with a patient centric agent: A block architecture," *IEEE Access*, vol. 6, pp. 32700–32726, 2018.

[28] H. Zhao, P. Bai, Y. Peng, and R. Xu, "Efficient key management scheme for health blockchain," *CAAI Trans. Intell. Technol.*, vol. 3, no. 2, pp. 114–118, Jun. 2018.

[29] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *IEEE Access*, vol. 6, pp. 38437–38450, 2018.

[30] R. Kumar and R. Tripathi, "A secure and distributed framework for sharing COVID-19 patient reports using consortium blockchain and IPFS," in *Proc. 6th Int. Conf. Parallel, Distrib. Grid Comput. (PDGC)*, Nov. 2020, pp. 231–236.

[31] M. I. da Fonseca Ribeiro and A. Vasconcelos, "Medblock: Using blockchain in health healthcare application based on blockchain and smart contracts," in *Proc. ICEIS*, 2020, pp. 156–164.

[32] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4177–4186, Jun. 2020.

[33] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102407.

[34] S. Rouhani, L. Butterworth, A. D. Simmons, D. G. Humphery, and R. Deters, "MediChainTM: A secure decentralized medical data asset management system," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1533–1538.

[35] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.

[36] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, and N. Yu, "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8770–8781, Oct. 2019.

[37] A. Roehrs, C. A. da Costa, R. R. Righi, A. H. Mayer, V. F. da Silva, J. R. Goldim, and D. C. Schmidt, "Integrating multiple blockchains to support distributed personal health records," *Health Informat. J.*, vol. 27, no. 2, Apr. 2021, Art. no. 146045822110075.

[38] A. Alexandridis, G. Al-Sumaidaee, R. Alkhudary, and Z. Zilic, "Making case for using RAFT in healthcare through hyperledger fabric," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2021, pp. 2185–2191.

[39] A. P. Singh, N. R. Pradhan, A. K. Luhach, S. Agnihotri, N. Z. Jhanjhi, S. Verma, Kavita, U. Ghosh, and D. S. Roy, "A novel patient-centric architectural framework for blockchain-enabled healthcare applications," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5779–5789, Aug. 2021.

[40] A. Al Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," *Future Gener. Comput. Syst.*, vol. 95, pp. 511–521, Jun. 2019.

[41] G. Prisco, "The blockchain for healthcare: Gem launches gem health network with Philips blockchain lab," *BitCoin Mag.*, Apr. 2016. [Online]. Available: https://bitcoinmagazine.com/articles/the-blockchain-for-heathcare-gem-launches-gem-health-network-with-philips-blockchain-lab-1461674938/

[42] W. J. Gordon and C. Catalini, "Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 224–230, Jan. 2018.

CH V. N. U. BHARATHI MURTHY is currently pursuing the Ph.D. degree with VIT University, Vellore. She is an Assistant Professor (C) with the School of Computer Science Engineering and Information Systems, VIT University. She has published various research articles in international journals, published three patent applications, and conference proceedings. She is a Seasoned Researcher, with a focus on cloud computing, blockchain technology, and the Internet of Things.

M. LAWANYA SHRI has been an Associate Professor Senior with the School of Computer Science Engineering and Information Systems, VIT University, Vellore, since 2005, having more than 18 years of experience. She has published more than 40 research articles in international journals, published five patent applications, and more than 25 conference proceedings. She has published several book chapters, edited books, and two authored books. She has given various invited talks in the faculty development program. Her research interests include blockchain technology, artificial intelligence, cloud computing, machine learning, deep learning, and the Internet of Things. She serves as an Editorial Board Member for *Informatics in Medicine Unlocked* (Elsevier). She has organized and worked as the co-chair and the session chair at IEEE conferences.