A blockchain-based system for patient data privacy and security

Article *in* Multimedia Tools and Applications · January 2024

DOI: 10.1007/s11042-023-17941-y

Isma Masood

19 PUBLICATIONS **403** CITATIONS

SEE PROFILE

Ali Daud
Rabdan Academy

173 PUBLICATIONS **3,288** CITATIONS

SEE PROFILE

Yongli Wang
Nanjing University of Science and Technology

160 PUBLICATIONS **4,202** CITATIONS

SEE PROFILE

Ameen Banjar
Jeddah University

53 PUBLICATIONS **570** CITATIONS

SEE PROFILE

Multimedia Tools and Applications
https://doi.org/10.1007/s11042-023-17941-y

A blockchain-based system for patient data privacy and security

Isma Masood[1] · Ali Daud[2] · Yongli Wang[1] · Ameen Banjar[3] · Riad Alharbey[3]

Received: 14 May 2023 / Revised: 2 December 2023 / Accepted: 17 December 2023

Abstract
The integration of wireless body sensor networks with cloud computing introduces numerous challenges in ensuring the privacy and security of patient data, including access control, scalability, privacy, data confidentiality, authorization rights management, multiple access control policies, audit control, and the availability of personal health information (PHI). Traditional sensor-cloud infrastructure (S-CI) architectures, typically reliant on a single trusted authority, struggle to address these multifaceted challenges. Recognizing the evolving landscape and the need for robust security measures, Blockchain technology has emerged as a promising solution, showcasing significant advancements in various domains, especially healthcare. This study presents a detailed examination of the complex challenges within the S-CI paradigm and propose a comprehensive blockchain-based system designed to enhance the privacy and security of patient data. Our approach surpasses conventional architectures by introducing an innovative Blockchain-Based Access Control Model (BBACM). This model is specifically tailored to effectively manage authorization rights for accessing both patient physiological parameters (PPPs) and PHI. To validate the practicality and effectiveness of proposed BBACM, a real use case scenario involving a paralysis patient is implemented. Experimental results showcase that our model significantly improves fine-grained access control, security, privacy, scalability, and availability of PHI. By leveraging the decentralized and tamper-resistant nature of blockchain, our system provides a robust framework for addressing the identified challenges in S-CI. The introduced BBACM establishes a foundation for secure and privacy-preserving healthcare data management, offering a promising solution to the intricate security and privacy issues associated with the integration of wireless body sensor networks and cloud computing.

Keywords Blockchain · Access control model · Patient data privacy · Security · Sensor-cloud infrastructure

1 Introduction

The healthcare domain adopts wireless body sensor networks (WBSNs) to facilitate patients for real-time monitoring and early medical aid. The dedicated WBSNs are providing high-quality healthcare services for elderly ill paralyze children, Epilepsy, Alzheimer's,

Extended author information available on the last page of the article

Published online: 05 January 2024

and Parkinson's disease. These WBSNs produce a huge amount of medical data and lack in terms of resource infrastructure [1]. Therefore, sensor data migrated to cloud storage infrastructure for fast computation, efficient energy performance, massive storage, communication power, and memory [2]. This amalgamation of WBSNs with cloud computing technology as Sensor-Cloud Infrastructure (S-CI) is providing early and at the time medical aid. According to the National Institute of Science and Technology (US NIST), cloud computing defines as follows: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". The definition indicates that cloud computing is hired by a third party on demand. The Healthcare domain hires cloud servers (usually private) for S-CI. Therefore, distributed nature of S-CI is more vulnerable to patient data privacy and security (PDPS).

Nowadays, blockchain technology shows a significant application in cryptocurrencies (e.g. Bitcoin) for ensuring trust, transparency, and accountability across the network. In addition, blockchain allows data isolation, confidentiality, and a shared channel-specific ledger for authenticated peers in the network. As an alternative to a traditional intermediate trusted entity or central authority in brokerage firms and banks, blockchain technology introduces a consensus mechanism on a distributed network [3, 4].

The consensus mechanism ensures trust, transparency, and accountability across the network. Distributed blockchain applications have also gained the attention of researchers to overcome the problem of a single point of failure [5–7]. Apart from that, data can easily be tempered in a centralized environment, hence distributed blockchain infrastructure can significantly improve the security of data [6]. In short, "The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value". Trust is not only the key concept of the economic and financial system but also an important element to building a good relationship between doctor and patient. According to Frank Somnenberg "Trust is like blood pressure. It's silent, vital to good health; and if abused can be deadly"[8]. Some other studies are also performed related to General Data Protection Regulation (GDPR) for compliant data processing [48] and compliant information confidentiality preservation [49] and data anonymization with application to machine learning processes [50–53].

Especially, the Internet of things (IoT) and wearable devices use for patient medical services produce a large amount of sensitive and confidential data. Typically, S-CI architecture has a rich storage entity named as a trusted authority (TA) for bootstrap the whole system in the initialization phase [9–12]. TA generates public/private keys, certificates, secret key parameters, and privacy policies for authorization. Relying on a single entity for access control means a bottleneck of the whole framework in case of failure. Therefore, TA is not suitable for the healthcare domain as it requires management, reliability, and availability of a large amount of memory. Figure 1 shows the traditional S-CI architecture with TA.

Recently, the potential benefits of blockchain technology for the healthcare domain gains a lot of attention in both the industry and academia. The application of blockchain technology in the field of healthcare can bring significant reforms in the industry in terms of providing increased access to data and patient medical records and by enabling device tracking throughout the life cycle of that device in blockchain structure [13]. Along with several benefits provided by blockchain infrastructure, several requirements are not being provided in many of these experiments and need to be explored [14]. Also, there are numerous research as well as functionality-based challenges that are required to be met for the integration of blockchain technology with the current electronic health record systems

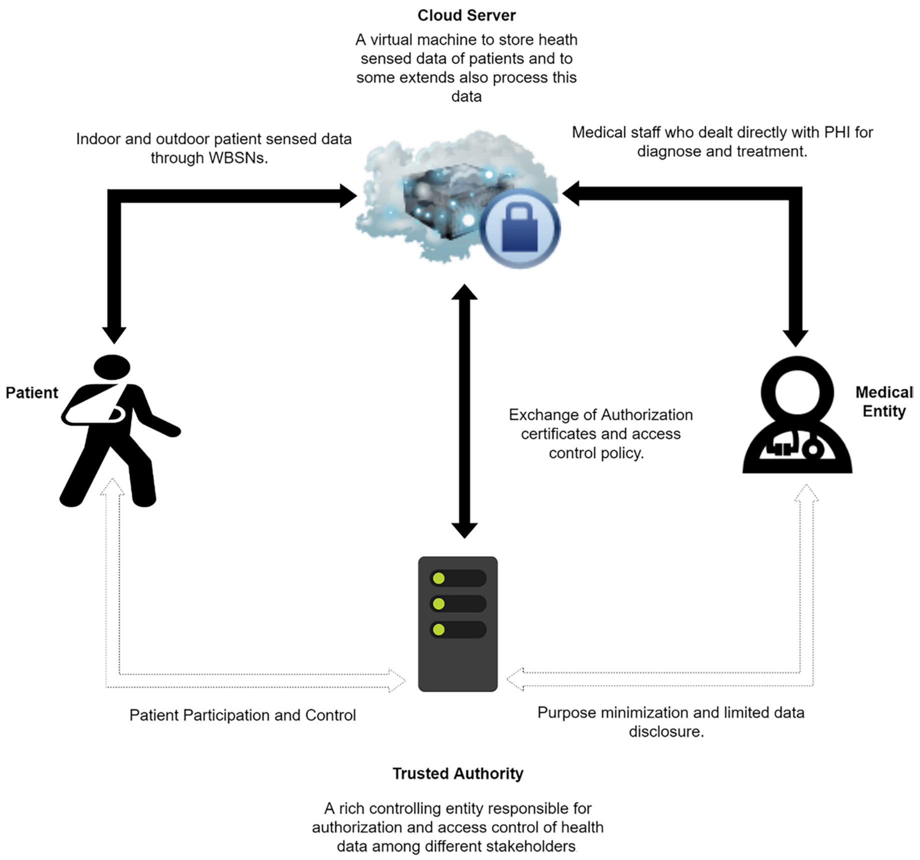

Cloud Server
A virtual machine to store heath sensed data of patients and to some extends also process this data
Indoor and outdoor patient sensed data through WBSNs.
Medical staff who dealt directly with PHI for diagnose and treatment.
Patient
Medical Entity
Exchange of Authorization certificates and access control policy.
Patient Participation and Control
Purpose minimization and limited data disclosure.
Trusted Authority
A rich controlling entity responsible for authorization and access control of health data among different stakeholders

Fig. 1 Traditional S-CI Architecture

[13, 15, 16]. The healthcare services can be more secure and trustable with blockchain technology like cryptographic techniques for authentication and access control in a distributed, secure and scalable manner [17–19].

There is an urgent need to develop blockchain-based methods to manage the patient privacy of health data stored in cloud-assisted WBANs. With the help of blockchain infrastructure, healthcare data can not only be studied and analyzed but can also be shared in a way that ensures security and privacy preservation [5, 18]. Therefore, Liang et al. [20] proposed an innovative mobile-based patient-centric Personal Health Information (PHI) sharing solution with permissioned and decentralized blockchain technology. Similarly, Ichikawa et al. [21] proposed a trustable and accountable decentralized network for PHI name as a temper resistance mHealth-based system using blockchain technology. Dubovitskaya et al. [22] proposed another blockchain-based framework to share and manage electronic medical records (EMR) of cancer patients. The fine-grained access control is used to reduce the turnaround time for EMR sharing cancer patients. Xia et al. [23] proposed a MeDShare system to deal with medical data sharing in the trust-less environment. The system used blockchain technology to provide auditing, provenance tracking, and access control in cloud repositories. In S-CI, multiple indoor and outdoor patients equip with

WBSs for real-time monitoring. There is a central cloud server where all sensed PPPs are stored after an equal interval of time. Multiple medical entities from cloud servers access PPPs in the hospital for the real-time monitoring of their patients. Usually, medical entities have authorization rights over PPPs to read, write, copy or transfer to a 3rd party [24]. Typically, S-CI has a central TA to implement data access policies, security parameters, generate public/private keys for authorization and certificates. Relying on the single entity for access control and authorization means a bottleneck of the whole framework in case of failure. The TA is not sufficient to manage PDPS of S-CI there is a need for improved access control of PPPs without comprising patient privacy.

Instead of relying on central TA, Blockchain technology used a consensus mechanism for the network. Blockchain technology allows data isolation, confidentiality, transparency, accountability, immutability, and channel-specific ledger for authentication of peers in the network. Following two research questions are investigated here.

> **RQ1.** *How is patient data privacy and security managed without relying on the single trusted entity in sensor-cloud infrastructure?*
> **RQ2.** *How patient PPPs can be accessed by multiple medical entities with blockchain technology in sensor-cloud infrastructure?*

Therefore, a BBACM to manage PDPS in S-CI is proposed. To achieve the solution to the aforementioned problem. However, there is no single study available to address the PDPS in SCI by using blockchain technology. In this study, a new blockchain-based system with an access control model is proposed to manage PDPS. Following are the main contributions of this work:

- Innovative blockchain-based architecture for S-CI without relying on a single TA.
- A blockchain-based access control model for sharing PPPs in multiple medical entities.
- Implementation of the real use case scenario to validate our access control model.

Despite these advancements, the traditional S-CI architecture relies on a central TA for data access policies, security parameters, and key generation, creating a potential bottleneck. To address this limitation, our proposed Blockchain-Based Access Control Model (BBACM) aims to manage PDPS in S-CI without relying on a single TA. The BBACM facilitates secure sharing of patient physiological parameters (PPPs) among multiple medical entities through a blockchain-based architecture.

The main contributions of this work include the introduction of an innovative blockchain-based architecture for S-CI, eliminating the dependence on a single TA, and the development of a BBACM for secure sharing of PPPs among multiple medical entities. To validate the effectiveness and practicality of the proposed model, the implementation of a real use case scenario involving a paralysis patient is presented. Through experimental results, it is shown that proposed BBACM significantly improves fine-grained access control, security, privacy, scalability, and availability of PHI in the context of S-CI. This study establishes a foundation for secure and privacy-preserving healthcare data management, paving the way for further advancements in blockchain technology for healthcare applications.

The rest of the paper is organized as Section 2 presents related work, Section 3 defines the research method of the study, Section 4 presents our blockchain-based system, Section 5 discusses performance and security analysis, and finally, the conclusion in Section 6.

2 Related work

In this section, exiting S-CI architectures with TA and figure out some important challenges to PDPS in S-CI are reported. Furthermore, how blockchain technology is facilitating the healthcare sector is discussed. Table 1 shows the summary of related studies with PDPS challenges.

2.1 Sensor-cloud infrastructure with trusted authority

A two-fold framework was proposed by [25]. In which the inter-sensor communication was secured by a multi-biometric key generation scheme and secured the storage of EMRs on a hospital community cloud to preserve patient privacy. A central TA server claimed to secure patient privacy by balancing administration rights and roles. Where the multi-biometric scheme is used as a combination of biometric and two PPPs values (ECG and EEG). A wireless sensor networks and cloud computing technique (WSNCC) was proposed with TA to manage access to sensor-cloud data for efficient communication and security of patients. This architecture was based on hash algorithms such as SHA-224, SHA-256, SHA-384, and SHA-512 for message integrity. Meanwhile, for electronic healthcare, Chen et al. [26] proposed a number theory research unit (NTRU) based scheme. It was used to secure PPPs sharing from wearable sensors to cloud servers. Antony et al. [27] proposed a novel technique with Integrated Secure Authentication (ISA). This application used TriMode Algorithm as compared to traditional cryptographic approaches for authentication of the e-health based cloud system. In 2017, Shynu et al. [28] also proposed an e-health cloud storage system to handle multiple users for sensitive data sharing. The patients were monitored through WBANs continuously and health data were collected in Electronic Health Records (EHRs). First, users registered with the cloud server and obtained a pair of cryptographic keys and smartcard. In the next step, a mutual authentication process took place. Health Service Provider (HSP) was responsible for the secure connection between the data owner and the data user. HSP issued an attribute certificate to the trusted entities. After this, the HSP enforces access policies (read, write) for data access and data encryption. Here, the system utilized the attribute-based searchable encryption (ABE) technique. During the whole process, a trapdoor function calculated for every patient. Table 1 summaries the selected studies of S-CI with TA.

2.2 Blockchain-based de-centralized techniques

In the healthcare domain, Yue et al. [32] proposed an application for patients named Healthcare Data Gateway (HDG). The main objective of this App was to allow patients to share their data without violating privacy. The blockchain-based platform enabled purpose-specific storage and access control of patient data. The shared data ensured purpose specification and patient control without violating PDPS. Similarly, Azaria et al. [33] proposed MedRec's first functioning prototype in which the system utilized Ethereum smart contracts for intelligent representation of EMRs on nodes of the blockchain network. MedRec was able to manage accountability, data sharing, authentication, and confidentiality of EMRs. However, MedRec used proof of work (POW) and permissionless blockchain, which is quite expensive in terms of the transaction fee. However, Ichikawa et al. proposed Temper Resistant Mobile Healthcare System (TRMH) with blockchain technology. Initially, EHRs collected through patient smartphones and directly send to blockchain networks without any intermediate storage server. The validating peers of the hyper ledger fabric verify the

Table 1 Summary of SC-I Techniques with TA

Technique	Application Area	Main idea	Findings	PDPS Challenges
M-BKG [29]	M-Health	The confidence of remote –healthcare system users can increase with patient privacy and communication security	A secure mobile healthcare framework for an inter-sensor communication of patient data	Source Authentication
WINCC [30]	M-Health	Cloud-based sensor data need reliable and fast communication	A model to manage sensor data for fine-grained access control, efficient communication, and security	Data Confidentiality, Fine-grained Access Control, Message integrity, and Availability
NTRU [26]	e- Health	Wearable devices that produced sensitive medical data for cloudlet cause a threat to patient privacy	To protect the patient privacy of medical data, a cloudlet-based data sharing system	Patient privacy, Data confidentiality
ISA [27]	e-Health	In WBANs spoofing attacks are easy to compute for authentication	ISA application to prevent spoofing attack in sensor-cloud-based e-healthcare system	Spoofing Attack
ABE scheme [28]	M-Health	The existing techniques are patient-centric and do not provide security with fine-grained access control	An ABE technique with a trapdoor function to avoid unauthorized access control for cloud-based health data	Fine-grained Access Control
IoT [31]	e- Health	Old aged people can get feasible medical aid from embedded devices with cloud servers	An IoT-based secure scheme for real-time monitoring of old age people	Data confidentiality

member and allow the transaction without compromising faults. Meanwhile, Dubovitskaya et al. [21] proposed a secure and trustable framework (STEMR) for sharing cancer patients' EMRs. StEMR was a blockchain-based on healthcare data management between different healthcare providers. The prototype of the framework ensured availability, privacy, security, and access control. The evaluation showed improved decision-making for medical aid and cost reduction. Shafagh et al. [35] proposed a blockchain-based design for IoT devices access control and data management in the distributed network. A detailed systematic review has been conducted by Agbo et al. [26] in which they have discussed numerous cases of application of blockchain in healthcare systems. They identified that the effectiveness of these proposed use cases has not been studied and characterized satisfactorily by prototyping. Table 2 summarizes the blockchain-based studies in healthcare.

2.3 Blockchain and IOT

In recent years, many patients' remote monitoring systems proposed to enforce access control policy with blockchain-based implementation and transactions. Zhang et al. [36] proposed a framework based on smart contracts. The proposed framework comprises one judge contract, one register contract with multiple access control contracts to control distributed and secure access control for IoT systems. To validate the system a case study based on Ethereum was implemented to attain access control. Xu et al. [37] proposed BlendCAC a decentralized blockchain-based access control for IoT devices. BlendCAC aimed to provide access control and information security at largescale IoT devices. The implementation demonstrated fine-grained access control, scalable, decentralized, and lightweight technique for IoT systems. Similarly, Novo [38] proposed an innovative blockchain-based architecture for privileges and attribute-based roles for IoT Scenarios. The experimental result of the proposed architecture revealed that blockchain technology provides scalable access management for IoT scenarios. In another study, Outchakoucht et al. [39] proposed a mechanism for access control of IoT context. The technique particularly provides a dynamic and optimized security policy.

The studies discussed reveal the reliance on TAs in existing architectures, such as the multi-biometric key generation scheme [25], Wireless Sensor Networks and Cloud Computing technique (WSNCC) [25], and the Integrated Secure Authentication (ISA) application [27]. These approaches utilize cryptographic techniques, hash algorithms, and attribute-based searchable encryption (ABE) for secure communication, access control, and data protection. However, the limitations of these techniques include challenges related to source authentication, data confidentiality, fine-grained access control, spoofing attacks, and the need for patient privacy. Transitioning to blockchain-based decentralized techniques, the review highlights various applications, such as Healthcare Data Gateway (HDG) [32], MedRec [33], Temper Resistant Mobile Healthcare System (TRMH) [21], and Secure and Trustable Framework for Sharing Cancer Patients' EMRs (STEMR) [22]. Blockchain technology addresses accountability, data sharing, authentication, and confidentiality concerns in the healthcare domain. However, challenges like transaction fees in permissionless blockchains and the need for further validation of proposed use cases are acknowledged [33]. The detailed examination of blockchain technology in healthcare showcases its potential in overcoming existing challenges but emphasizes the need for more comprehensive studies and characterizations of its effectiveness. Additionally, the integration of blockchain with the Internet of Things (IoT) is explored. The studies by Zhang et al. [36], Xu et al. [37], Novo [38], and Outchakoucht et al. [39] propose blockchain-based access control mechanisms for IoT devices, addressing issues of decentralized and secure access control, fine-grained

Table 2 Summary of Blockchain Technology in Healthcare

Technique	Application Area	Main idea	Findings	Challenges
HDC [32] 2016	M- Health	Personal health data should be owned by patients as assets to avoid privacy risks	A blockchain-based application for patients to share their healthcare data without privacy risks	Patient control and participation
MedRec [33] 2016	M- Health	EHRs are sensitive handle in the healthcare domain	A permission-less blockchain-based system for access to EHRs	Accountability, confidentiality, authentication
TRMH [21]	M-Health	Accurate and safe digital healthcare data sharing	A blockchain-based tamper-proof system for mobile-based health data	Tamper Proofing
STEMR [22]	Healthcare Data Management	EMRs are extremely critical and sensitive while sharing in a different hospital	A blockchain-based framework for sharing cancer patient data	Availability, security, privacy, and fine-grained access control
IOT [34]	Healthcare Data Management	Cloud-storage architecture for IoT leads to health data management	A blockchain-based architecture for IoT devices used for access control and data management	Access control

access control, scalability, and optimized security policies. However, the literature recognizes the necessity for further validation and experimentation to assess the scalability and effectiveness of these proposed architectures in real-world IoT scenarios.

This study introduces a novel approach to address the limitations of traditional S-CI architecture by proposing a Blockchain-Based Access Control Model (BBACM). Unlike the conventional S-CI, which relies on a central Trusted Authority (TA) for critical functions, the BBACM eliminates this single point of dependency. The key innovation lies in the use of a blockchain-based architecture to manage Patient Data Processing Systems (PDPS) securely. The BBACM enables the secure sharing of patient physiological parameters (PPPs) among multiple medical entities. The contributions of this work include the introduction of the innovative blockchain-based architecture for S-CI, the development of the BBACM for secure PPPs sharing, and the validation of the model through a real use case involving a paralysis patient. The experimental results demonstrate significant enhancements in fine-grained access control, security, privacy, scalability, and availability of Personal Health Information (PHI) within the S-CI framework. This study establishes a robust foundation for advancing secure and privacy-preserving healthcare data management, showcasing the potential of blockchain technology in healthcare applications.

3 Method

In this section, a brief description of the blockchain network and Hyperledger fabric composer used for our proposed model is provided. Meanwhile, a detailed description of the case scenario was selected for the implementation of our model.

3.1 Blockchain network

The blockchain is used to record business trades, promises, transactions, or simply assets for transparency and immutability. Blockchain technology consists of four main key concepts to revolutionize the business in terms of privacy and pre-permission identities in the network [40]. Following are the four main key concepts:

Shared Ledger:—As compared to a bilateral entry in the traditional ledger, blockchain introduced a new concept of distributed shared ledger. This shared ledger means an immutable record shared among all the participants of the network[40].

Permission:—Blockchain can be divided into two type's: permission and permissionless. Bitcoin and Ethereum are examples of permissionless blockchain networks [41]. However, permissioned blockchain facilities participants of the network with a unique identity, which enables access, control policies for transactions details. Therefore, permissioned blockchain network is more suitable for sharing PHI. Permissioned blockchain for PDPS in S-CI is also utilized.

Consensus:—All participants of the blockchain network are trusted and identifiable. Therefore, the transaction of the shared ledger can be committed and verifiable through a consensus mechanism (agreement). Some common consensus mechanisms are proof of stake, multigeniture, and practical Byzantine fault tolerance (PBFT) [40].

Smart Contract:—A smart contract is a set of rules used to manage the transaction of a network automatically. These contracts are based upon many contractual conditions that are partially or fully self-enforcing and self-executing [40].

3.2 Hyberledger fabric

Hyperledger is an open-source software to improve collaborative efforts for the advancement of cross-industry with blockchain technology. Hyperledger hosted by Linux foundation collaborating for globalization in the supply chain, IoT, banking, spanning finance, manufacturing, and technology. The fabric is a distributed network from peer to peer where, each peer contained a replicated copy of consistent blockchain data structure, records of the transaction on the network with chain codes. The fabric is a hyperledger project that provides a platform for blockchain-based implementation and application development.

The hyperledger composer is used to simplifying the application development in hyperledger fabric. Hyperledger composer provides a framework for development used to step up an application on top of the blockchain network. This framework starts from a business level and is used to model the basic components of the network. Model files in the hyperledger composer portray the “Assets, Participants, Transactions and Events” of the network. For data sharing and privacy, “Access Control List” defines the rules at runtime. However, “Transaction Processors Functions” are used to implement the additional requirements [41]. Figure 2 shows the general structure of the composer. Following are the detail of composer files:- The Model file is responsible for outlining the structure of the network. Three main components: assets, participants, and transactions. Assets are often the variables stored in the network. Participants are the nodes of the network and can interact with assets and other participants through transactions. Transactions are the functions of the network and are invoked to update the network (e.g., transferring an asset). The script file defines the various transaction functions in the network. It is written in JavaScript handles the transaction logic, including which types of participants interact (different categories of participants have different levels of access in the network) and which kinds of assets are transferred. The access control file delineates the specific scopes of access users have in the business network. In this file the role of the user (participant) is described, determining their role in creating(C), reading(R), updating(U), or deleting(D) elements of the network. The query file defines the structure and function of queries from this network. Queries can be set to extrapolate transactions from the historian, which is a ledger of all past transactions in the system.

Once the network is defined, it can be exported as an archive, downloaded, and run on another machine. A network card is used to connect to the system. Network cards can take the form of a participant type or admin. Participant cards generally have a more controlled scope of access in the network, while the admin can perform more high-clearance functions such as adding new participants or deleting participants. This card type defines the node that uses the card to connect to the network and, thus, outlines what kind of role the node plays.

4 Blockchain-based system

In this section, proposed blockchain-based system to facilitates the access of PPPs among multiple medical entities of a hospital is explained. Proposed blockchain-based system provides scalability to store a large number of PPPs collected through WBANs. Since PPPs are highly sensitive to PHI, BBACM is proposed to ensure the PDPS in S-CI by implementing a real case scenario of a paralysis patient. Unlike, traditional TA-based S-CI system; our system is secure, transparent, and auditable for data owners and data requesters. Figure 3 shows proposed blockchain-based system architecture applied to achieve the aforementioned objectives.

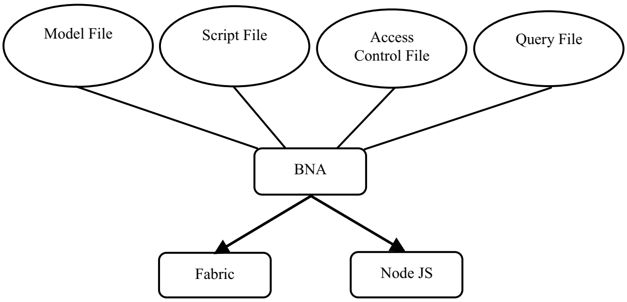


Fig. 2 General Structure of Fabric Composer

4.1 System entities

Our proposed system consists of four system entities. Following are the five main entities:

1) ADMIN

The admin is responsible to register patients and medical entities for our system. This entity can add, update and delete the patient and medical entities from the system.

2) PATIENT

In our system, there are two categories of patients a) indoor patient (Pi) and b) outdoor patient (Po). Both types of patients are equipped with wireless body sensors for PPPs collection. These PPPs are then uploaded to the cloud server through their device.

3) MEDICAL ENTITY (ME)

These are multiple medical entities like a doctor, a nurse, and a medical secretary. These multiple entities have authorization rights (read, write, copy or transfer) to access PPPs according to their patient's treatment and diagnosis. The medical entity can request to access PPPs from the cloud server.

4) CLOUD SERVER (CS)

It is an outsourcing cloud computing service to provide storage for WBANs. PPPs are uploaded and accessed according to the authorization rights defined in the blockchain network. Access to PPPs is secure, confidential, traceable, and accountable.

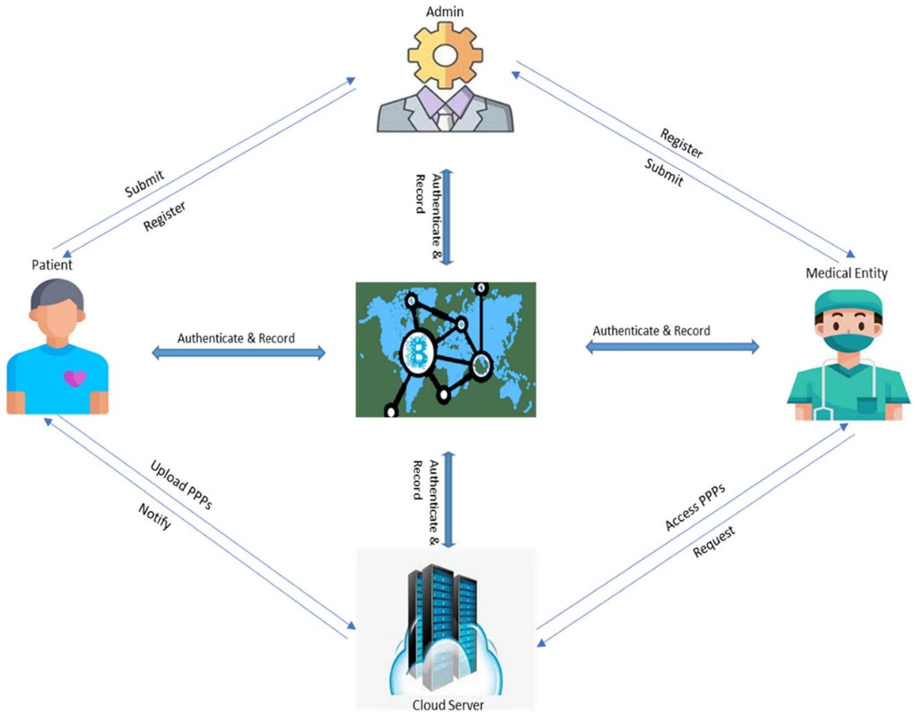


Fig. 3 Blockchain-Based System Architecture

5) BLOCKCHAIN NETWORK (BN)

The blockchain network used for PDPS of PPPs in S-CI. This network has an umbrella role throughout the process. From PPPs uploading to PPPs access all transactions appended to the blockchain network. Blockchain provides a data access policy based on authorization rights for PDPS. At first, the Pi or Po visits the hospital, and the admin is responsible to register both types of patients on the network. The concerned ME uploads PHI at CS(HIS) with unique patientrecordid. Moreover, PPPs can be uploaded from WBANs at CS. Then the authorized ME can access PHI with an updated version of PPPs through BN. However, each participant's transactions are logged and updated at the shared ledger of BN. However, once the record is logged in BN cannot be tempered or lost.

4.2 Case study

4.2.1 Paralysis patient case scenario

In this section, a real case scenario of a paralyzed patient from a local Medical Hospital is considered for implementation. This hospital hired a private server cloud for their patients, which requires frequent visits for constant monitoring. However, the hospital is quite concerned about patient data privacy and security. Therefore, they did not share the real names of the patient and so anonymous names are used for the patient and the medical staff. A use case scenario of a patient suffering from paralyzes requires constant healthcare monitoring (see Fig. 4). Paralysis is caused by trauma (fall or car accident) in which damage to the spinal cord needs lifetime monitoring and long-lasting treatment.

The patient is 35 years old young man. His spinal cord was badly affected in a road accident when he was 5 years old. His body is 40 percent paralyzed. For the last thirty years, he is in constant medical observation at the local general hospital. His PHRs used in several different places like a general physician, surgical department, gastrology department, neurology department, lab, etc. He has to visit the hospital every month for regular checkups. He is suffering from occasional fits attacks for the last 6 months. Meanwhile, he is suffering from shortness of breathiness. The main motivation to choose this real case is the maximum utilization of PHRs across different departments of the hospital. Meanwhile, the patient is dependent on the hospital and family for his privacy.

4.2.2 The internal medicine physcian (specialist)

Our simple scenario was extracted from the interview with the internal medicine physician. Patient family member makes an appointment for his regular monthly checkup. Dr. Isma is responsible for the general examination. His nurse records specific physiological parameters to check his current condition and update his PHI. If the patient is diagnosed with

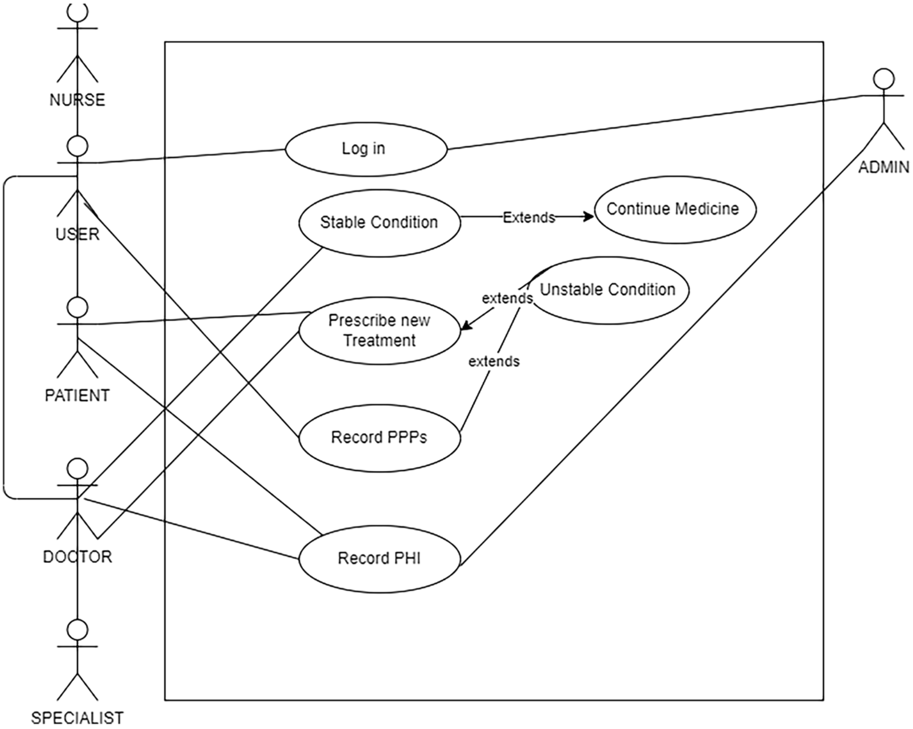


Fig. 4 Use Case Model

an unstable medical condition Doctor recommends encountering some new physiological parameters and if needed recommend new treatment or refer to the concerned department for a new physician. The marked terms were utilized later in the implementation (see Table 3). Following is an extracted phrase from Doctor's interview:

> *"When my[1] patient[2] arrives[3] for regular checkup[4] in internal medicine department (IMD) [5], I recommend recording[6] his physiological parameters like body temperature, blood pressure, and heart beat[7], etc. These parameters are documented[8] in the his[9] medical record (PHI)[10], which my[11] nurse[12] and I can access[13] from hospital information system (HIS) [14].*

From the internal medicine physician scenario, the patient data can be divided into two types for implementation of BBACM. Following are two types of patient data:

1) PERSONAL HEALTH INFORMATION

This data is maintained from the initial visit of the patient at the hospital. Medical entities with proper authentication rights can access the PHI of patients from HIS. Data items like patient id, patient name, address, contact no, medical diagnoses, medical treatments, surgeries, and drug allergies, etc. are commonly maintained in PHI.

2) PATIENT PHYSIOLOGICAL PARAMETERS

This data type contained the PPPs recorded and saved with PHI in HIS. These PPPs are used for real-time monitoring to assess the medical condition of the patient. In this scenario, PPPs like Bp, Bt, and Hb are commonly recorded. From the patient medical history of the use case scenario, we can extract two medical conditions for real-time monitoring.

Stable Medical Condition: The recording of PPPs show stable medical condition, and the current treatment plans or medications are according to patient care.
Unstable Medical Condition: The recording of PPPs show unstable medical condition, and the current treatment plans or medications are not enough for patient care. However, details about PPPs readings, treatment plans, and medication details of the patient are not investigated, as it is out of the scope of this study.

4.3 Experimental setup

To test the proposed system, Ubuntu 14.04 version LTS, OS type 64-bit with Intel core i7, and Docker engine 17.03 is used. Hyperledger composer is used to modeling. Hyperledger's Modeling Language used for access control list,.cto file model design and stored on the chain.

As HF is a permission-based network, restrict services for particular users. Our blockchain-based system incorporated two fundamental parts (1) off-chain storage (cloud server), and a (2) blockchain network. The Business Network Archive (BNA) is created through HC which decides the capabilities and characteristics of our model. Besides, the HC deploy runtime version of the BNA on HF instance.

HC creates three basic files as A Script document, A Model Document, and the Access Control List. Participants are the main actors of the network for the exchange of data with transactions. In our model, three main participants are involved (Admin, Patient, and

Table 3 Extracted Concepts for Implementation

Category	Marked no	Role	Meaning
Participants	1, 11	Doctor	It represents the role of the doctor as a participant in the network
	2, 9	Patient	It represents the role of the patient as a participant in the network
	12	Nurse	It represents the role of the nurse as a participant in the network
Assets	7	Bp	It represents the role of the PPPs as an asset in the network
	7	Bt	It represents the role of the PPPs as an asset in the network
	7	Hp	It represents the role of the PPPs as an asset in the network
	10	PHI	It represents the role of the PHI as an asset in the network
Transactions	6	Recording	It represents the role of the access of PPPs for write/read authorization rights in the network
	8	Documented	It represents the role of the access of PPPs for write authorization right in the network
	13	Access	It represents the role of the access of PPPs for reading/copy authorization rights in the network
Events	3	Arrives	It represents the role of the arrival as an event in the network
	4	Regular checkup	It represents the role of the regular checkup as an event in the network
Location	5	IMD	It represents the role of the IMD as a physical location in the network
	14	HIS	It represents the role of the HIS as physical storage in the network

Medical Entity). Description of the participants is in the Model file of HC. New participants can be generated or added to the participant registry. HC needs blockchain identities as credentials and mapping characters for participants to store in the identity registry. Admin control all identity management services for deployment of a blockchain network.

In our model, at any point, new participants (Doctor, Nurse, Patient) with their access control list can be added to the network. While, access control list, type of transactions, and attributes for each participant are defined in "permissions.acl" file. "permissions.acl" file. For example, in our model authorization rights to a doctor are controlled by the patient. Assets of our model (PHI, PPPS) are saved in the asset's registry of the HC. Transactions are operations to exchange assets by participants within the network. Our model implantation consists of five main functions for Add new Patient, Read Access of PHI, Updated PHI, Delete, and Transfer rights. These functions are triggered by the participants of the network.

4.4 Hyberledger business archive network (HBAN)

After the extraction of the terms from the scenario, the following components for the hyberledger business archive network are created:

1) PARTICIPANTS

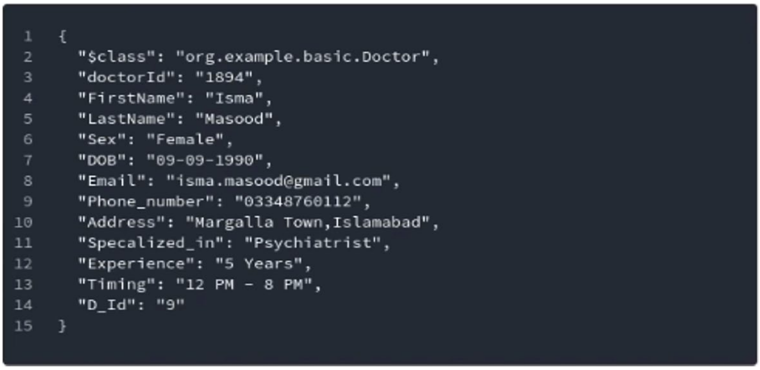
In the proposed HBAN, five participants for the network are created (Table 4). The admin is responsible for registering other participants on the network. Meanwhile, the admin also has the right to control the transactions of other parties. In the beginning, the patient consults for monitoring with a relevant medical entity (doctor, nurse, specialist). Once the patient gets consultation his/her PHI or PPPs record is updated on the network. In the future, these records only be shared with authorized participants according to the access control list. Figure 5 shows an example to add a doctor as a participant for HBAN.

2) ASSETS

Anything that value is called an asset. In proposed HBAN, three assets PHI, MEI, and PPPs are considered. The assets are responsible for the transaction of data. Table 5 shows a list of assets involved throughout the lifecycle of the system. PHI is an asset that contains all basic medical information about the patient, while PPPs asset is linked to PHI by patiendrecodid attribute. PPPs assets contain vital signs of a patient. The recorded PPPs values in real-time will be updated at a specific interval of time in this asset. However, admin is responsible to add or delete any specific parameter from this record. The MEI asset maintains information about any particular entity like doctor nurse and specialist. Figure 6 shows PHI assets on HBAN.

Table 4 List of Participants for HBAN

No	Participants
1	Admin
2	Patient
3	Doctor
4	Nurse
5	Specialist



```
{
  "$class": "org.example.basic.Doctor",
  "doctorId": "1894",
  "FirstName": "Isma",
  "LastName": "Masood",
  "Sex": "Female",
  "DOB": "09-09-1990",
  "Email": "isma.masood@gmail.com",
  "Phone_number": "03348760112",
  "Address": "Margalla Town,Islamabad",
  "Specalized_in": "Psychiatrist",
  "Experience": "5 Years",
  "Timing": "12 PM - 8 PM",
  "D_Id": "9"
}
```

Fig. 5 Add Doctor

Table 5 Assets in HBAN

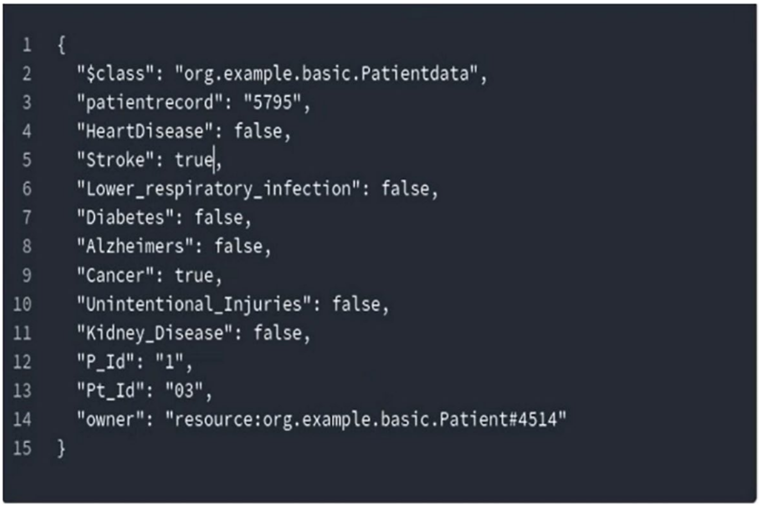
No	Assets	Key Fields
1	PHI	patientrecordid, name, gender, dob, address, contact_no, email, allergies, referedby, heartdisease, stroke, lower_respiratiory_infection, diabetes, cancer, Alzheimer's, unintentional_injuries, kidney_disease, other
2	MEI	medicalentityid, name, gender, dob, designation, department, specialized_in, experience, affiliation
3	PPPs	Patientrecordid, BP, BT, Pulse, EEG, EEC, Heart_rate,

3) TRANSACTIONS

The participants of the HBAN perform their processes on the network by transactions. These transactions are responsible to change the value of assets on the network. The participants of HBAN can perform a total of four transactions UploadPHI, AccessPHI, UpdatePHI, and TransferRights throughout the lifecycle. Each interaction with the PPPs is logged as transactions in the blockchain network. Participants associated with the relevant transaction can view these transactions on the network. Figure 7 shows some interactions on the network with data, time, and participant records.

In *UploadPHI* transaction there are three main participants of the transaction such as patient, doctor, and nurse with assets PHI and PPPs. In *AccessPHI* transaction there are two main participants doctors and specialists with assets PHI and PPPs. Similarly, two participants admin and doctor can make a transaction in *UpdatePHI* with asset PHI. However, doctors can perform only *TranferRights* on asset PHI. Table 6 list the details of all four transactions in our system with pseudocode.

To ensure the access control of the PPPs, chain code defines the functionality of authorization rights for the participants of the blockchain network. Hyperledger Fabric contains ACL, which defines the access control policy for the items of the domain model. CTO. By defining access control rules for the authorization rights (for medical entities) in ACL, one can control the assets of the participants in proposed blockchain network.



```
{
  "$class": "org.example.basic.Patientdata",
  "patientrecord": "5795",
  "HeartDisease": false,
  "Stroke": true,
  "Lower_respiratory_infection": false,
  "Diabetes": false,
  "Alzheimers": false,
  "Cancer": true,
  "Unintentional_Injuries": false,
  "Kidney_Disease": false,
  "P_Id": "1",
  "Pt_Id": "03",
  "owner": "resource:org.example.basic.Patient#4514"
}
```

Fig. 6 PHI Asset on HBAN

5 Discussion

Previous studies with TA-based approaches to access PHI and PPPs in HIS were more vulnerable to patient data privacy and security breaches. In TA based system the access control policy depended on one entity for the whole network. Meanwhile, different parties involved in the exchange of patient data were not known. In our system the access control policy is manned by.acl on the network therefore, there are zero percent chances of the bottleneck. Meanwhile, a real-time ledger of the blockchain maintains the access details of every participant. As aforementioned, to the best of our knowledge, this is the first novel approach for access to PPPs based on blockchain as compared to other TA-based techniques. Therefore, the difficulty level of mining of each block, scalability of the network, and availability of the system is focus.

The difficulty level of each block depends upon the mining network concerning time. Suppose, the expected time to mine a single block is 10 min. Then the average speed of mining the last 2000 blocks in 8 min. Hence, the new difficulty level calculated as follows:

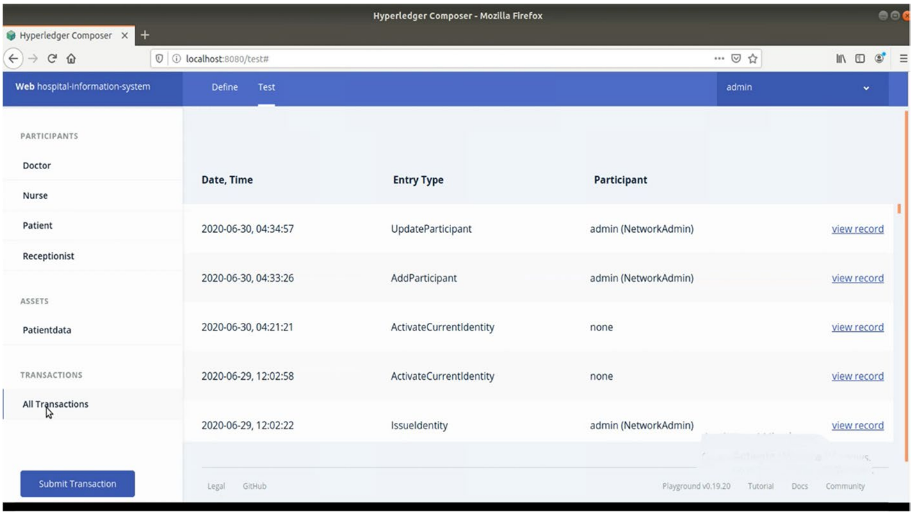
Let, Difficulty level = DL, New Difficulty = ND, Old Difficulty = OD, Fixed no. of previous blocks = Fpb.

Time in minutes = tm

$$DL = ND = OD\_Fpb\_tm \tag{1}$$

(The average time of mining Fpb) ND = OD * (2000 blocks * 10 min)/ (the average time of mining last 2000 blocks). If the average time is > 10 min the factor will be less than one and the next difficulty level will be decreased for 2000 blocks.

The current estimated difficulty level is 4,022,059,196,164 in scientific notation: 4.2e12. Minimum difficulty level = 232 = 4.3e9 hashes (for 1 block). So, average of 4.2e12 *4.3e9 = 1.806e22 hashes required to mine 1 block. Our system with Core i7 26000 CPU performed 2.3e7 hashes per second (based on ASCI hardware code).



Date, Time	Entry Type	Participant	
2020-06-30, 04:34:57	UpdateParticipant	admin (NetworkAdmin)	view record
2020-06-30, 04:33:26	AddParticipant	admin (NetworkAdmin)	view record
2020-06-30, 04:21:21	ActivateCurrentIdentity	none	view record
2020-06-29, 12:02:58	ActivateCurrentIdentity	none	view record
2020-06-29, 12:02:22	IssueIdentity	admin (NetworkAdmin)	view record

Fig. 7 Transactions on HBAN

Hence, 1.806e22 / 2.3e7 = 7.8521739130435e14 average seconds required to mine one block in our system. This will be approximately 2 million years.

Scalability Scalability is one of the major challenges for S-CI [42–44]. As patient data sharing needs scalability [43] based upon the number of access requests and stakeholders. Bitcoin network is the first application of blockchain network on the average process seven transactions per second (tpsec) [45]. An average online transition through visa = 2000 tpsec, the bitcoin blockchain size increased over GB as compared to other online transactions. For example, the number of transactions processed through Visa at peak of time is 2000 topic.

An average online transition through visa = 2000 tpsec, the bitcoin blockchain size increased over GB as compared to other online transactions. For example, the number of transactions processed through Visa at peak of time is 2000 tpsec. Similarly, 15,000 tpsec was processed by Twitter at peak time. However, 500,000 to 2,100,000 tpsec were processed by trading, email, and advertising networks.

$$Scalability = Requested\ Transactions \times (Block\ size \times Time^{*}) \tag{2}$$

Time in seconds, minutes, hours, and days.

In our system, the number of requests to access PPPs in real use case scenario of our case study adopted as user transactions per second. For example, assume system consist with maximum 100 tpsec with block size 650 MB. The estimated size of blockchain network as follow:

Table 6 List of Transactions

No	Participant	Transaction	Pseudocode
1	Patient Doctor Nurse	UploadPHI	*Upload Patient Health Information with Parameters* *Patient uploads encrypted PPP (asset) on the ledger with the private key* *Patient grants access of asset to Doctor* *The doctor's ID added to the Patient's asset available on the ledger* *Patient's ID added to the Doctor's asset authorized on the ledger* *The symmetric key for the PPP decrypted with the patient's private key* *Symmetric Key encrypted with Doctor's public key*
2	Doctor Specialist	AccessPHI	*Access Patient Health Information with Parameters* *Doctor requests Patient's PHI (asset) on HIS with the private key* *Doctor's ID added to the Patient authorized asset* *The patient's ID was added to the Doctor authorized asset* *The doctor's private key is used to decrypt the symmetric key for Patient PHI (assets)* *Symmetric key encrypted with Patient public key*
3	Admin Doctor	UpdatePHI	*Update Patient Health Information with Parameters* *Doctor requests Patient's PHI (asset) on HIS with the private key* *Doctor's ID added to the Patient authorized asset* *The patient's ID was added to the Doctor authorized asset* *The doctor's private key is used to decrypt the symmetric key for Patient PHI (assets)* *Symmetric key encrypted with Patient public key*
4	Doctor	TransferRights	*Doctor Transfer Rights to Nurse* *Doctor updated authorization rights to allow Nurse to access Patient PHI (asset)* *Chaincode verify Doctor's rights on the Patient asset* *The doctor's private key is used to decrypt the asset's symmetric key* *Nurse public key used to encrypt the symmetric key* *Nurse's ID added to the Patient's authorized assets* *Patient's ID added to the Nurse authorized asset*

100(650 X 1) = 65,000 bytes = 520 KB per second
100(650X 60(1)) = 3,900,000 bytes = 31.2 MB per minute
100(650X36X102(1)) = 238,680,000 bytes = 1.9 GB per hour
100(650X864X102(1)) = 5,728,320,000 bytes = 45.82 GB per day

Security: PHI stored in HIS (a private cloud server) encrypted with asymmetric key pair of a 2048-bit RSA. The patient as a data owner can only share encrypted keys and set a control access policy to maintain confidentiality. The PPPs uploaded from the patient interface and PHI shared from HIS are secured on the network with the hash algorithm. The hash of the data objects is stored on the shared ledger and digitally signed transactions to ensure data integrity.

Availability: The availability of the PHI is guaranteed by storing it in a private cloud server. A role-based APIs on the network to query or invoke the chain code. Whereas, in loss of credentials off-chain and on-chain stored data is still recoverable.

Since this is the first effort to use a blockchain network instead of TA in S-CI it is very hard to compare our work with other related works. Thus, comparison is done with other techniques proposed for PDPS in S-CI. A two-fold mobile healthcare-based framework was proposed using WBANs. The security of patient data is maintained with 1) inter-sensor communication secured by a multi-biometric key generation scheme; 2) secure storage of EMRs. The framework used dynamic reconstruction of metadata for PDPS. In contrast, Zhou et al. [46] used body symmetric structure for their scheme. The symmetrical structure of the patient body was adopted for key generation extracted from ECG, EEG, and privacy maintained with similar social groups. Similarly, the "wireless sensor networks and cloud computing" (WSNCC) technique used Hash Algorithms such as SHA-224, SHA-256, SHA-384, and SHA-512 for access control and secure communication in S-CI. Constant availability and confidentiality of patient data symmetric key cryptography.

Recently, Huang et al. [43] proposed mobile healthcare social network (MHSN) scheme and provided fine-grained access control through the fusion of health and social data. MHSN used identity-based broadcast and attribute-based encryption for PDPS. Similarly, Li et al. [47] used chaotic maps in S-CI for secure and continuous real-time monitoring of patients. As compared to the aforementioned work, our model only requires two messages on the blockchain network1) the transaction for access of PPPs and 2) the response of the blockchain network. Message integrity on the network is maintained by hash and symmetric key encryption. However, the response time of our model depends upon the type of blockchain network.

This study underscores the novelty and advancements brought by our proposed Blockchain-Based Access Control Model (BBACM) in contrast to traditional Trusted Authority (TA)-based approaches for accessing Patient Health Information (PHI) and Patient Physiological Parameters (PPPs) in Health Information Systems (HIS). TA-based systems have historically posed vulnerabilities to patient data privacy and security, relying on a single entity for network-wide access control policies. In our BBACM, the access control policy is managed by an.acl on the network, eliminating the potential bottleneck associated with TA-based architectures. Additionally, the real-time ledger of the blockchain maintains detailed access records for each participant. To the best of our knowledge, this study presents the first innovative approach to access PPPs based on blockchain, distinguishing it from TA-based techniques. The evaluation focused on the mining difficulty, scalability, and system availability. Mining analysis revealed that our system, based on a Core i7 26,000 CPU, would take approximately 2 million years to mine one block, emphasizing the robustness of the proposed approach. Scalability considerations showed the potential for efficient processing of access requests, surpassing limitations observed in other Scalable-Cloud Infrastructure (S-CI) systems. Furthermore, the security measures, including encryption and hash algorithms, ensure the confidentiality and integrity of PHI, while the availability of data is guaranteed through role-based APIs and recoverable off-chain and on-chain stored data. Comparisons with existing PDPS techniques in S-CI demonstrate the superiority of our model in terms of efficiency, requiring only two messages on the blockchain network for access transactions and response.

6 Conclusion

This research introduces an innovative access control model, BBACM, leveraging the inherent properties of blockchain technology to establish a robust access control policy for medical entities. The model's effectiveness is demonstrated through the implementation of a real-use case scenario involving a paralysis patient in the internal medicine department, wherein BBACM efficiently manages authorization rights for patient data within the S-CI framework. Our blockchain-based access control model encompasses routine patient physiological parameters (PPPs) such as body temperature, heartbeat, and blood pressure, providing a secure and streamlined mechanism for access across multiple medical entities. Notably, BBACM addresses and mitigates threats to patient data privacy and security (PDPS), ensuring real-time monitoring and control over PPPs access. The evaluation of BBACM on the Hyperledger Fabric platform underscores the success of our fine-grained access control coupled with symmetric key encryption. The performance and security analyses reveal a marked improvement in scalability, security, and availability, substantiating BBACM's efficacy in facilitating secure PPPs access. Looking ahead, BBACM holds promising potential for extension into emergency management and access control for intricate use case scenarios. As we continue to refine and expand the scope of BBACM, its application in diverse healthcare settings is poised to contribute significantly to the advancement of secure and efficient patient data access and management.

In future work, one may aim to further enhance the versatility and applicability of BBACM by extending its capabilities to address emergent challenges in healthcare. Our focus will include refining the model for seamless integration into emergency management systems, allowing for rapid and secure access control in critical situations. Additionally, we plan to explore the adaptation of BBACM to more complex use case scenarios within the healthcare domain, broadening its scope and impact. Continuous refinement and expansion of BBACM will be guided by a commitment to advancing secure and efficient access control for patient data, ultimately contributing to the ongoing evolution of healthcare information management systems.

Data availability Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Sajid A, Abbas H (2016) Data privacy in cloud-assisted healthcare systems: state of the art and future challenges. J Med Syst 40(6):1–16 (in English)
2. Li J, Zhang Y, Chen X, Xiang Y (2018) Secure attribute-based data sharing for resource-limited users in cloud computing. Comput Secur 72(218):1–12
3. Zhang P, White J, Schmidt DC, Lenz G, Rosenbloom ST (2018) FHIRChain: applying blockchain to securely and scalably share clinical data. Comput Struct Biotechnol J 16:267–278
4. Ullah I et al (2021) Global context-aware multi-scale features aggregative network for salient object detection. Neurocomputing 455:139–153
5. Benarous L, Kadri B, Bouridane A (2020) Blockchain-based privacy-aware pseudonym management framework for vehicular networks. Arab J Sci Eng 12:1–7
6. Khalid S, Maqbool A, Rana T, Naheed A (2020) A blockchain-based solution to control power losses in Pakistan. Arab J Sci Eng 18:1
7. Kudva S, Badsha S, Sengupta S, Khalil I, Zomaya A (2021) Towards secure and practical consensus for blockchain based VANET. Inf Sci 545(2021):170–187
8. Boysen GN, Nystr M, Christensson L, Herlitz J, Sundstr BW (2017) Trust in the early chain of healthcare: lifeworld hermeneutics from the patient's perspective. Int J Qual Stud Health Well-being 12(1):1–12
9. Khan MA, Salah K (2018) IoT security: review, blockchain solutions, and open challenges. Future Gener Comput Syst 82(2018):395–411
10. Masood I, Wang Y, Daud A, Aljohani NR, Dawood H (2019) Towards smart healthcare: patient data privacy and security in sensor-cloud infrastructure. Wirel Commun Mob Comput 2018:1–23
11. Ramya A, Anandh A, Muthulakshmi K, Janani S, Gayathri N (2022) Blockchain-powered healthcare information exchange systems to support various stakeholders. In: EAI/Springer Innovations in Communication and Computing Cham, Ed. (EAISICC). Springer, pp 189–206
12. Zaabar B, Cheikhrouhou O, Jamild F, Ammie M, Abida M (2021) HealthBlock: a secure blockchain-based healthcare data management system. Comput Netw 200:108500
13. Tanwar S, Parekh K, Evans R (2020) Blockchain-based electronic healthcare record system for healthcare 4.0 applications. J Inf Secur Appl 50:102407
14. McGhin T (2019) Blockchain in healthcare applications: research challenges and opportunities. J Netw Comput Appl 2019(135):62–75
15. Shi S, He D, Li L, Kumar N, Khan MK, Choo KK (2020) Applications of blockchain in ensuring the security and privacy of electronic health record systems: a survey. Comput Secur 15:101966
16. Rajput AR, Li Q, TalebyAhvanooey M, Masood I (2019) EACMS: emergency access control management system for personal health record based on blockchain. IEEE Access 7:84304–84317
17. Zyskind G, Nathan O, Pentland AS (2015) Decentralizing privacy: using blockchain to protect personal data. In: Proceedings of the 2015 IEEE Security and Privacy Workshops (SPW 2015). San Jose, CA, USA, pp 180–184

18 Farouk A, Alahmadi A, Ghose S, Mashatan A (2020) Blockchain platform for industrial healthcare: vision and future opportunities. Comput Commun 154:223–235

19 Aggarwal S, Kumar N (2021) Basics of blockchain. Adv Comput 121:129–146

20. Liang X, Zhao J, Shetty S, Liu J, Li D (2017) Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In: The 28th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (IEEE PIMRC 2017), Montreal, Quebec, Canada. IEEE, pp 1–5

21 Ichikawa D, Kashiyama M, Ueno T (2017) Tamper-resistant mobile health using blockchain technology. JMIR Mhealth Uhealth 5(7):1–10

22. Dubovitskaya A, Xu Z, Ryu S, Schumacher M, Wang F (2017) Secure and trustable electronic medical records sharing using blockchain. In: AMIA 2017 Annual Symposium Proceedings

23. Xia Q, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M (2017) MeDShare: trust-less medical data sharing among cloud service providers via blockchain. IEEE Access 5(2017):14757–14767

24 Masood I, Wang Y, Daud A, Aljohani NR, Dawood H (2018) Privacy management of patient physiological parameters. Telemat Inform 35(4):677–701

25. Hammi MT, Hammi B, Bellot P, Serhrouchni A (2018) Bubbles of trust: a decentralized blockchain-based authentication system for IoT. Comput Secur 78(2018):126–142

26. Chen M, Qian Y, Chen J, Hwang K, Mao S, Hu L (2016) Privacy protection and intrusion avoidance for cloudlet-based medical data sharing. IEEE Trans Cloud Comput PP(9):1–9

27. Rani AAV, Baburaj E (2016) An efficient secure authentication on cloud based e-health care system in WBAN. Biomed Res-India 27(2016):S53–S59 (in English)

28. Shynu PG, Singh KJ (2017) An enhanced ABE based secure access control scheme for E-health clouds. Int J Intell Eng Syst 10(5):29–37

29. Khan FA, Ali A, Abbas H, Haldar NA (2014) A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks. 9th International Conference on Future Networks and Communications (Fnc'14) / the 11th International Conference on Mobile Systems and Pervasive Computing (Mobispc'14) / Affiliated Workshops, vol 34, no 2014, pp 511–517 (in English)
30. Saha S (2015) Secure sensor data management model in a sensor– cloud integration environment. In: Applications and Innovations in Mobile Computing (AIMoC)
31. Hu J-X, Chen C-L, Fan C-L, Wang K-H (2017) An intelligent and secure health monitoring scheme using IoT sensor based on cloud computing. J Sens 2017:1–11
32 Yue X, Wang H, Jin D, Li M, Jiang W (2016) Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. J Med Syst 40(10):1–8 (in English)
33. Azaria A, Ekblaw A, Vieira T, Lippman A (2016) MedRec: using blockchain for medical data access and permission management, presented at the IEEE 2016 2nd International Conference on Open and Big Data
34. Shafagh H, Burkhalter L, Hithnawi A, Duquennoy S (2017) Towards blockchain-based auditable storage and sharing of IoT data. Presented at the CCSW'17
35. Zhou J, Cao Z, Dong X, Xiong N, Vasilakos AV (2015) 4S: a secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks. Inf Sci 314(2015):255–276
36. Zhang Y, Kasahara S, Shen Y, Jiang X, Wan J (2018) Smart contract-based access control for the internet of things. arXiv preprint arXiv:1802.04410
37 Xu R, Chen Y, Blasch E, Chen G (2018) BlendCAC: a blockchain-enabled decentralized capability-based access control for IoTs. 1804.09267v1 [cs.NI] 24 Apr 2018
38. Novo O (2018) Blockchain meets IoT: an architecture for scalable access management in IoT. IEEE Internet Things J 5(2):1184–1195
39. Outchakoucht A, Es-Samaali H, Leroy JP (2017) Dynamic access control policy based on blockchain and machine learning for the internet of things. Int J Adv Comput Sci Appl 8(7):417–424
40. Laurence T (2023) Blockchain for dummies. John Wiley & Sons
41. Cachin C (2016) Architecture of the hyperledger blockchain fabric. In: Workshop on distributed cryptocurrencies and consensus ledgers (vol 310, no. 4, pp 1–4)
42. Maitra T, S Roy (2017) SecPMS: an efficient and secure communication protocol for continuous patient monitoring system using body sensors. In: 9th International Conference on Communication Systems and Networks (COMSNETS). IEEE
43. He H, Zhang J, Gu J, Hu Y, Xu F (2017) A fine-grained and lightweight data access control scheme for WSN-integrated cloud computing. Cluster Comput 2017(20):1457–1472
44 Huang K, Zhang X, Mu Y, Rezaeibagh F, Due X (2021) Scalable and redactable blockchain with update and anonymity. Inf Sci 546:25–41
45 Luu L, Narayanan V, Baweja K, Zheng C, Gilbert S, Saxena P (2015) SCP: a computationally-scalable byzantine consensus protocol for blockchains. IACR Cryptol ePrint Arch 1168:1–16
46. Zhou J, Cao Z, Dong X, Lin X (2015) PPDM: a privacy-preserving protocol for cloud-assisted e-Healthcare systems. IEEE J Sel Top Signal Process 9(7):1332–1344
47. Chunlin L, Jingpan B, Zhao W, Yang X (2019) Community detection using hierarchical clustering based on edge-weighted similarity in cloud environment. Inf Process Manag 56(1):91–109
48. Desiato D et al (2018) A methodology for GDPR compliant data processing. Proceedings of the 26th Italian Symposium on Advanced Database Systems, Castellaneta Marina (Taranto), Italy, June 24–27, vol 2161
49. Caruccio L et al (2020) GDPR compliant information confidentiality preservation in big data processing. IEEE Access 8:205034–205050
50. Caruccio L et al (2022) A decision-support framework for data anonymization with application to machine learning processes. Inf Sci 613:1–32
51. Cauteruccio F et al (2019) Short-long term anomaly detection in wireless sensor networks based on machine learning and multi-parameterized edit distance. Information Fusion 52:13–30. https://doi.org/10.1016/j.inffus.2018.11.010
52. Calimeri F et al (2019) A logic-based framework leveraging neural networks for studying the evolution of neurological disorders. Theory Pract Logic Program 21(1):80–124. https://doi.org/10.1017/s1471068419000449
53. Malik HAM, Shah AA, Muhammad A, Kananah A, Aslam A (2022) Resolving security issues in the IoT using blockchain. Electronics 11:3950. https://doi.org/10.3390/electronics11233950

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Authors and Affiliations

Isma Masood[1] · Ali Daud[2] · Yongli Wang[1] · Ameen Banjar[3] · Riad Alharbey[3]

✉ Ali Daud
alimsdb@gmail.com

Isma Masood
isma_masood@hotmail.com

Yongli Wang
yongli.wang@nust.edu.cn

Ameen Banjar
abanjar@uj.edu.sa

Riad Alharbey
ralharbi@uj.edu.sa

[1] School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210000, China

[2] Faculty of Resilience, Rabdan Academy, Abu Dhabi, United Arab Emirates

[3] Department of Information Systems and Technology, College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia