Healthcare Privacy Approach Using Blockchain Technology

Vrushali Jalgaonkar, Mahesh Shirole, and Sunil Bhirud

Abstract Nowadays, with the advancement in information technology, great progress is seen in the healthcare domain. However, such advancement has also made healthcare data not only much bigger but also much more difficult to handle. Also, the data generated is in different formats and to access such largely scattered data is merely impossible. Health care today suffers from fragmented data, delayed communications, and disparate workflow tools caused by the lack of interoperability. Blockchain technology possesses key properties that can potentially address pressing issues in health care such as incomplete records at the time of care and difficult access to patients' health information in a secure manner. The proposed solution emphasizes on solving a current problem of storing the largely scattered healthcare information in a decentralized fashion and allowing the access of data by the authorized persons only. This application manages authentication, confidentiality, accountability, and data sharing while handling sensitive health information.

Keywords Blockchain · Healthcare data · Medical research centers · Data exchange

V. Jalgaonkar (✉) · M. Shirole · S. Bhirud
Department of Computer Engineering and Information Technology, Veermata Jijabai Technological Institute, Mumbai, India
e-mail: vrjalgaonkar_m17@ce.vjti.ac.in

M. Shirole
e-mail: mrshirole@it.vjti.ac.in

S. Bhirud
e-mail: sgbhirud@ce.vjti.ac.in

D. Patel et al. (eds.), *IC-BCT 2019*, Blockchain Technologies,
https://doi.org/10.1007/978-981-15-4542-9_5

1 Introduction

Health Information Technology (HIT) has evolved greatly, but even now, we do not have access to the entire patient's health history in a unified way. We still have different health records with diversified healthcare providers (i.e., healthcare professionals and healthcare organizations) that we interacted in our lifelong period [1, 2]. In a real scenario, a patient visits different doctors and different hospitals for treatment. At every medical appointment, the patient must have to tell his/her whole health history again, which may not be appropriate or accurate with losing time. Electronic Health Record (EHR) is a standardized information model, enabling integration among multiple healthcare providers, ranging from supporting medical prescriptions, improving disease management, and contributing in the reduction of severe medication errors while Personal Health Record (PHR) can receive data entered by patient like the patient's weight, blood pressure readings, etc. [3]. Some healthcare providers have been successful in communicating with patients using mobile technology (mPHR), which allows patient self-monitoring and managing his/her health status [4]. Thus, with such an advancement in healthcare technology, the healthcare data is becoming larger and even outdated.

Many health organizations use databases in a proprietary format. These databases are hosted in a data center inside the health organizations, with restricted access to internal health professionals. In some cases, for example, laboratory results, patients, and healthcare providers can have external access to health records in a restricted manner, only to be viewed or printed [5]. In many cases, the patient's data is not being shared by the healthcare providers and thus, they do not have up-to-date data when their patients are assisted by other healthcare providers. Moreover, these data are stored in different formats in different organizations. Being voluminous, healthcare records are either stored using cloud infrastructure to enable easy access and sharing of information among the different stakeholders or on local databases by the healthcare institutes. In addition, the security and privacy measure offered by the cloud increase the resiliency of data [6]. This brings difficulties for the exchange of healthcare data among the organizations. However, the use of cloud storage does not allow interoperability between different care providers. Also, the integrity and authenticity of the data cannot be guaranteed.

Other problems arise from the existence of duplicate and outdated data in the organizations and also the patient does not have a unified viewpoint of his data. A promising solution to these problems involves the application of blockchain technology, which provides "trustless" transactions via decentralization with pseudo-anonymity [7]. A blockchain system can be considered as a virtually incorruptible cryptographic database where critical medical information could be recorded. The system is maintained by a network of computers, which is accessible to anyone running into the network. Blockchain implements a ledger that validates the existence of digital assets (e.g., coins, as in the case of Bitcoin) and tracks where the control exists for each of them in the network. Such control is distributed, and the one (or ones) who has the control can change the state of the asset (e.g., its controllership) without permissions from any central authority [8]. The access control of heterogeneous patient's health care, records across multiple health institutions and devices needed to be carefully designed. Blockchain itself is not designed for the large-scale data storage system.

In the context of health care, a decentralized storage solution would greatly complement the weakness of blockchain in the perspective. The blockchain network as a decentralized system is more resilient as in that, there is no single-point attack or failure compared to centralized systems. Hence, by storing historical healthcare records of the patient, there will be no loss of data. Also accessing the patient data must be controlled, which can be achieved by blockchain technology.

The above observations of patient's data access and issues in the healthcare data interoperability motivate us to provide blockchain-based unified system. The paper discusses the healthcare records issues which face the problems of

- A single view of both PHR and EHR to be distributed, up-to-date and interoperable to patients, healthcare providers, medical research centers, and insurance companies,
- The historical healthcare data which is being stored in different formats and how to handle them in a unified manner.
- Validation of each peer on every access request.

The remainder of this paper is organized as follows: In Sect. 2, the related work and the existing system are discussed. Section 3 discusses the proposed system. Section 4 gives an overview of the implementation and results. Section 5 concludes the paper.

2 Literature Survey

Blockchain is a platform that alleviates the explicable on a single, centralized authority, yet still supports secure and "trustless" transactions directly between interacting entities [8]. It offers decentralization, immutability, and consensus via cryptography. This technology provides the foundations for several application domains, including cryptocurrency and Decentralized Apps (DApps) [9]. Smart contracts, as implemented in the Ethereum Blockchain [10], that provide code to directly control the exchanges of digital assets between two or more entities according to certain rules or agreements previously established between involved participants. Storing data objects and defining operations on that data can be done using smart contracts, enabling the development of DApps to interact with blockchains and provide seamless services to the application users.

In the healthcare domain, smart contracts are being applied to create secure and effective technical infrastructures to enhance care coordination and quality and thus improve the well-being of individuals and communities [7, 11]. A major problem in the production of healthcare systems today is the lack of secure links that can connect all independent health systems to communicate and establish an end-to-end reachable network while protecting healthcare information with some level of anonymity [6, 12, 13]. Although data standards like HL7 and FHIR [14] provide basic interoperability for data exchange between trusted systems, this level of interoperability is limited to the implemented standards and requires mapping of data between systems in most cases. Also, to achieve maintainability for these systems is difficult because an interface change on one system requires other parties in the trusted network to adopt the change as well. Startups like *Ujo* or *Peertraks* offer a new approach, such as how music rights can be administered and enforced using blockchain. At *Stampery*, for example, contracts, emails, and documents can be signed digitally and smart contracts can be settled [7].

The confidentiality and protection of individually identifiable health information that is transferred, received, handled, or shared by healthcare professionals and organizations must require Health Insurance Portability and Accountability Act (HIPAA) rules [15]. EHR is "information related or relevant to the wellness, health, and healthcare of an individual, in computer processable form and represented according to a standardized information model." PHR refers to a "representation of information regarding, or relevant to, the health, including wellness, development, and welfare of that individual" [3]. All systems and apps created to share health information must be HIPAA compliant. MedRec: a novel decentralized record management system [16] handles EMRs (electronic medical records), gives a comprehensive, immutable log, and easy access to patient's medical information across healthcare providers and treatment sites.

Permissionless and permissioned blockchain [17] can be helpful in managing and sharing electronic health and medical records to allow patients, hospitals, clinics, and other medical stakeholders to share data amongst themselves, and increase interoperability. In [18], a set of evaluation metrics is defined which can be used to assess DApps designed to address healthcare interoperability issues such as (1) Entire workflow is HIPAA compliant, (2) Framework employed needs to support turing complete operations, (3) Support for user identification and authentication, (4) Support for structural interoperability at minimum, (5) Scalability across large populations of healthcare participants, (6) Cost-effectiveness, and (7) Support of patient-centered care model.

By seeing all the related work, the disadvantages of the existing systems do not allow the patient's health data to be exchanged between different healthcare organizations. An efficient and effective solution is provided to store all the healthcare history of the patient in a decentralized fashion which can be accessed by different health institutes, medical researchers, and insurance companies by providing privacy on the data.

3 Proposed System

In the proposed work, we focus on the storage and controlling the access of both PHR and EHR data without any Trusted Third Party (TTP) in a distributed environment. The model's purpose is to carry out data integrity, confidentiality as well as to eliminate the inconsistency for the end-user while allowing a unified view of health records that are distributed in several health organizations. The model proposes a way in which healthcare data are organized hierarchically, encrypted, and distributed in chained data blocks on the network. These blocks store data that are located in different healthcare organizations and even in a patient-managed repository.

Figure 1, the entities involved in the system can access the patient's healthcare data which is stored in the IPFS cloud through blockchain [19]. The health data like laboratory analysis report which can be in text or image or a document format can be stored on IPFS because the data size is larger and the IPFS hash which is only of few tens of bytes is stored on the blockchain.

The major objectives of the proposed work are as follows:

- To design an approach for the healthcare domain where the system stores all historical data into the blockchain manner.
- To create a distributed environment hierarchy for parallel data processing for end-user applications.
- Validation of each peer on every access request.

The users involved in the system are

1. **Patient**—The patient's medical history is being stored which can be accessible by the authorized entities of the network. The ownership of the data is being managed by the patient.

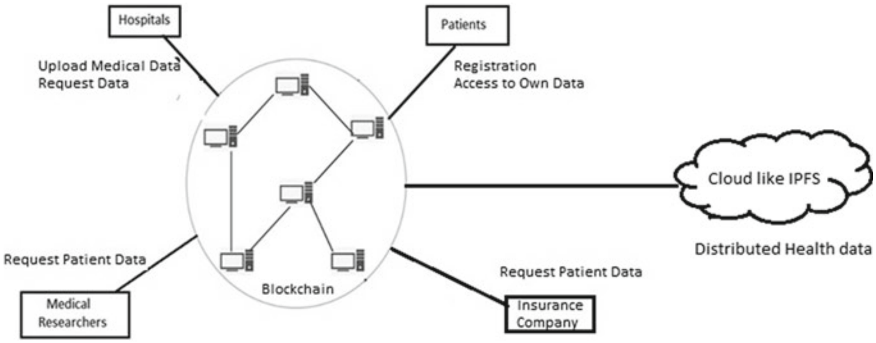


Fig. 1 System architecture diagram for the patient's storage and retrieval of information

Table 1 List of system actors with smart contracts

Actor	Contracts
Patient	1. Patient. sol (a) Patient registration (b) Permit request (c) View history
Hospital	2. Hospital. sol (a) Hospital registration
Doctor	3. Doctor. sol (a) Doctor registration (b) Update patient report
Medical researchers	4. Medical research. sol (a) Med research registration (b) Request patient data
Insurance company	5. Insurance company. sol (a) Insurance company registration (b) Request patient info

2. **Hospitals**—The doctor will treat the patient. The report generated after treatment will be uploaded to the network, thus maintaining the up-to-date healthcare information of the patient. This information would be useful by the other healthcare organizations where the patient would visit for health assistance.
3. **Medical researchers**—The patient's data should not be unknowingly accessed by anyone. The healthcare institutes would be restricted to give patient data to medical researchers without the knowledge of the patient.
4. **Insurance company**—While the patient seeks any health insurance or life insurance, the procedure to claim that benefits are time consuming. Thus, by providing request-based access to patient's health information would make the hectic insurance claiming process much faster and also reliable.

During the registration time, the new user is verified by the email verification. Once the user is verified, he/she would be considered as the verified entity of the blockchain network. Based on request access to the data, verification of the entity is done by the other blocks present in the network using a delegated proof of stake consensus mechanism algorithm. Thus, only validated entities of the network get a chance to access the healthcare information. The control access of uploading the patient's treatment report is being given to the hospital's staff, in which the authorized doctor would have all access to the health information while the other hospital staff, for example, nurse, is given access to the only view the data. The medical researchers and insurance companies can only view health data after the request is granted by the patient (Table 1).

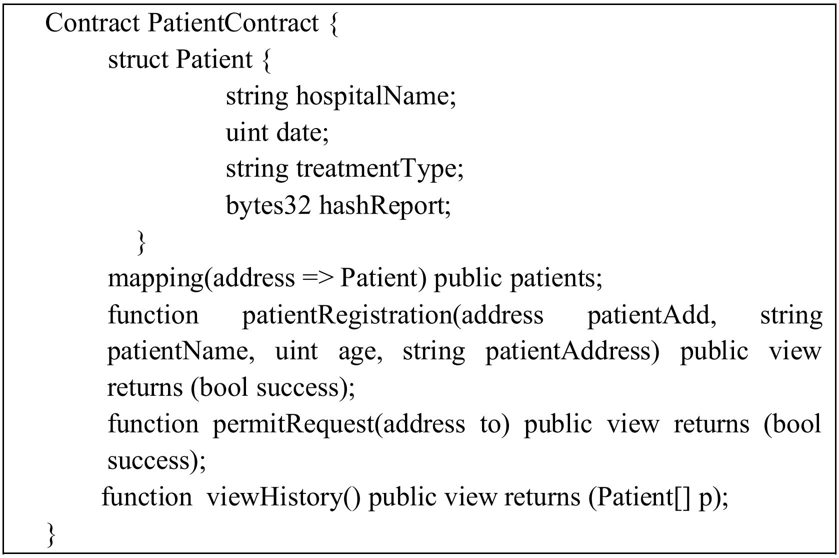
4 Implementation and Results

The contracts for the system are written in Solidity language using the truffle framework. Truffle is a development environment, testing framework, and asset pipeline for Ethereum. Metamask is an extension that allows you to run Ethereum DApps right in your browser without running a full Ethereum node.

Following is an interface contract declaring the required functions for the patient. The data structures used are structure and map. The contract's patient data structure will contain the following information.

- *hospitalName* will store the name of the hospital,
- *date* for storing the date during which the patient had reported to the hospital for the treatment,
- *treatmentType* declares the type of treatment which the patient had, it can be any medical checkup or any laboratory test like a blood test,
- *hashReport* stores the hash for the medical report which will be given during the treatment.

The patientRegistration(…) function is used to store the patient's details. The function permitRequest(…) takes the "to" address of the entity who wishes to access the patient's data. The patient's data is accessible by only those to whom the permission is granted. The function viewHistory() returns the historical patient data which the patient wants to view.



```
Contract PatientContract {
        struct Patient {
                        string hospitalName;
                        uint date;
                        string treatmentType;
                        bytes32 hashReport;
          }
        mapping(address => Patient) public patients;
        function   patientRegistration(address   patientAdd,   string
        patientName, uint age, string patientAddress) public view
        returns (bool success);
        function permitRequest(address to) public view returns (bool
        success);
       function  viewHistory() public view returns (Patient[] p);
}
```

Following is an interface contract declaring the required functions for the hospital. The data structures used are structures and mapping. The contract's hospital data structure will contain the following information.

- *hospitalName*, stating the hospital name
- *hospitalAddress*, the location address of the hospital

The hospitalRegistration(…) function registers the hospital.

```
contract Hospital Contract {
    struct Hospital {
            string hospitalName;
            string hospitalAddress;
      }
    mapping(address => Hospital) public hospitals;
    function hospitalRegistration(address hospitalAdd, string
    hospitalName, string hospitalAddress) public view returns (bool
    success);
}
```

Following is an interface contract declaring the required functions for the doctor. The data structures used are structures and mapping. The contract's doctor data structure will contain the following information:

- *doctorName*, takes the doctor's name who will be treating the patient.
- *Specialization*, specifies the highest qualification of the doctor.

The doctorRegisration(…) function registers the doctor into the network. The updatePatientReport(…) function uploads the hash generated of the medical report of the patient and a brief description of the medical report. This can be done as follows:

updatePatientReport (0×1111111111111111111111111111111111111111, "Blood test", QmYqSCWuzG8Cyo4MFQzqKcC14ct4ybAWyrAc9qzdJaFYTL)

"QmYqSCWuzG8Cyo4MFQzqKcC14ct4ybAWyrAc9qzdJaFYTL" is the hash of the medical report.

```
contract Doctor Contract {
        struct Doctor {
                string doctorName;
                string specialization;
          }
        mapping(address => Doctor) public doctors;
        function doctorRegisration (address doctorFrom, string
        doctorName, string specialzation) public view returns (bool
        success);
        function updatePatientReport (address patientAdd, string
        reportDesc, bytes32  hashReport ) public returns (bool success);
}
```

Following is an interface contract declaring the required functions for the Medical Research Center. The data structures used are structures and mapping. The contract's Medical Research data structure will contain the following information.

− *hashReport*, is the hash of the medical report which the medical research centers want to view.

The function medReseachRegistration(…) registers the medical researchers. The patient's data is requested using requestPatientData(…) function.

```
Contract MedicalResearchers Contract {
        struct MedicalResearch {
                bytes32  hashReport;
          }
        mapping(address => MedicalResearch) public
        medicalResearchers;
        function medReseachRegistration (address
        medResearcherFrom, string medResearchName) public view
        returns (bool success);
        function requestPatientData (address medResearcherFrom)
        public view returns (MedResearch[] M);
}
```

Following is an interface contract declaring the required functions for the insurance company. The data structures used are structures and mapping. The contract's insurance company data structure will contain the following information:

− *hashReport*, is the hash of the medical report which the medical research centers want to view.

The function insurance Company Registration(…) registers the insurance companies. The patient's data is requested using request Patient Info function.

```
contract InsuranceCompanyContract {
      struct InsuranceCompany {
                  bytes32 hashReport;
        }
      mapping(address => InsuranceCompany) public
      insuranceCompanies;
      function insuranceCompanyRegistration (address insComAdd,
      string insComName, string insComAddress) public view returns
      (bool success);
      function requestPatientInfo (address insComAdd) public view
      returns (InsuranceCom[] i);
}
```

The advantage of this system is that the historical data of the healthcare which is shared by the various medical institutes and by patients can be secured using blockchain technology. The data integrity and confidentiality can be maintained. The data can be shared between the entities in the network securely. Thus, providing an effective way to preserve the privacy of the patient's healthcare data.

We have implemented the system, while it is under test and yet not tested in the real environment.

5 Conclusion

In this paper, the distributed and scattered data of patients and hospitals are channelized using the proposed system. The system facilitates hospitals to use and interoperate healthcare data of the patients stored by different stakeholders seamlessly. Patients are capable of accessing the complete health record and authorize requesting parties to use and view their health records. The healthcare data appear to be centralized from the logical viewpoint of patient and healthcare provider, but in fact, they are physically decentralized. Usage of IPFS allowed to store a large volume of patient's data which are in different formats stored on the cloud. This data is accessible only through the blockchain; thus, reducing the misuse of the data. Thus, the model aims to support patients to take advantage of having their health history single access, as well as for healthcare providers to have their patients' health data up-to-date.

References

1. Gorp PV, Comuzzi M (2012) Lifelong personal health data and application software via virtual machines in the cloud. IEEE J Bio Health Inf 0(0)
2. Bourgeois FC, Nigrin DJ, Harper MB (2015) Preserving patient privacy and confidentiality in the era of personal health records. PEDIATRICS, 13(55)
3. ISO, Health informatics—Capacity-based ehealth architecture roadmap—Part 2: Architectural components and maturity model, Technical Report (ISO/TR TR14639-2). https://www.iso.org/obp/ui/#iso:std:iso:tr:14639:-2:ed-1:v1:en
4. Reeder B, David A (2016) Health at hand: A systematic review of smart watch uses for health and wellness. J Bio Inf
5. Kraan C.W., Piggott J.J.H., Vegt F.V.D, Wisse L.: ‘Personal Health Records: Solving barriers to enhance adoption ‘, July 2015
6. Divya T, Shanmugapriya L (2016) Two-level security in shared m-healthcare system using owncloud. IEEE
7. Matthias M, HSG MA (2016) Blockchain Technology in Healthcare. In: The international conference on e-health networking, applications and services (Healthcom), IEEE
8. Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system
9. Johnston D, Yilmaz SO, Kandah J, Bentenitis N, Hashemi F, Gross R, Wilkinson S, Mason S (2014) The general theory of decentralized applications, dapps. Github—.https://github.com/DavidJohnstonCEO/DecentralizedApplications
10. Buterin V (2013) A Next-generation smart contract and decentralized application platform. Ethereum white paper, GitHub repository
11. Leslie M.,: ‘A blockchain revolution sweeps into health care, offering the possibility for a much-needed data solution’, IEEE Pulse, June, 2018
12. Kim H, Song H, Lee S, Kim H, Song I (2016) A simple approach to share users. Own Healthcare Data with a Mobile Phone ICUFN, IEEE
13. Zhang Y, Qiu M, Chun-Wei T, Mohammad MH, Alamri A (2015) Health-CPS: Healthcare cyber-physical system assisted by cloud and big data. IEEE SYSTEMS JOURNAL, IEEE
14. Bender D, Sartipi K (2013) HL7 FHIR: an agile and restful approach to healthcare information exchange’, IEEE
15. H. Office for Civil Rights: standards for privacy of individually identifiable health information. final rule. Federal Register, vol 67, no 157, p 53181, 2002. https://www.nap.edu/read/12458/chapter/7
16. Azaria A, Ekblaw A, Vieira T, Lippman A (2016) MedRec: using blockchain for medical data access and permission management. In: 2nd international conference on open and big data
17. Alhadhrami Z, Alghfeli S, Alghfeli M, Abedlla JA, Shuaib K (2017) Introducing blockchains for healthcare’, international conference on electrical and computing technologies and applications (ICECTA)
18. Zhang P, Walker MA, White J, Schmidt DC, Lenz G (2017) metrics for assessing blockchain-based healthcare decentralized apps. In: IEEE 19th international conference on e-health networking, applications and services (Healthcom)
19. IPFS information. https://en.wikipedia.org/wiki/InterPlanetary_File_System