Blockchain Based Electronic Healthcare Record (EHR)

Bipin Kumar Rai, Akanksha Tyagi, Bhawana Arora, and Shivani Sharma

Abstract The nature of medical system is viewed as perhaps the main factor of a nation. Currently Electronic Health Record (EHR) is being used to store the patient's medical data. However, EHR faces some issues like interoperability, security, privacy. All such issues leads to the decreased quality of medical system and also to an increase in healthcare costs because data is being shared between different medical facilities over different places. The management of medical data also include some different challenges such as access to data and the way that data is often accessed at different places other than the medical facility. Blockchain technology can help in improving current healthcare system. The objective of this research paper is to show how EHR can be implemented into healthcare sector for maintaining patient's data using blockchain technology i.e. how the data can be gathered, uploaded and accessed. Blockchain provide the way to efficiently handle the medical data.

Keywords EHR · EMR · Privacy · Security · Blockchain · Pseudonymization · Depersonalization

1 Introduction

Technology employed in healthcare sector can help in efficiently operating of organizations to meet growing demand in order to deliver better patient care. All such advantages are provided by Electronic Health Record (EHR). EHRs are an information system that digitally maintains all medical records of a patient. It contains different sorts of health related data of a patient and understands the outline or integration of various electronic health data and fulfil the management related needs of the hospitals [1, 2].

Security and Privacy Issues: We need to handle the following security issues in a proper way while accessing EHR.

B. K. Rai (✉) · A. Tyagi · B. Arora · S. Sharma
Department of IT, ABES Institute of Technology, Ghaziabad, Uttar Pradesh 201009, India

A. Kumar and S. Mozar (eds.), *ICCCE 2021*, Lecture Notes in Electrical Engineering 828, https://doi.org/10.1007/978-981-16-7985-8_19

1. **User Authentication**: Only approved users will have the option to get access to the health record.
2. **Confidentiality and Integrity**: It is associated with the protection of medical data from unauthorized access and reliability of physical computer and network systems.
3. **Access Control**: It's been a fundamental security issue wherever healthcare data keeps in databases and traded with the help of heterogeneous documenting system.
4. **Data Ownership**: It is additionally a significant issue associated with ability to access of medical data. Obligations of information possession ought to be handled straightforwardly [3].

Using blockchain technology is the most efficient way to provide security to the data stored in an EHR. Advantages like storage of medical data electronically, management of appointments of patients with the doctor, bill management and storage of laboratory tests are all provided by EHR system [4].

2 Related Work

The process of data management and de-identification by which we can restore in person specifiable data by artificial identifiers or pseudonyms is known as pseudonymization [5]. Individual data can be identify and distinguish from related data using the process known as depersonalization [6–8]. Algorithms for calculating the pseudonym can depend upon encryption or hashing strategies [9–11]. According to Kerckhoff's principle algorithm which is applied to the system is accessible by anyone but we need to keep the keys secretly [12, 13]. Thielscher et al. [14] proposed a system in which decentralised keys are kept on smart cards. Two different methodologies were proposed by Pommerening et al. [15, 16], which were each kind of like the system proposed by Thielscher et al. Their system design is a blend of a hashing and an encryption method. Similarly, Peterson [17] came up with the approach which is dependable on centralised table used for reidentification motive. This centralised table also faces issue that a centralized list can be attacked from inside and outside of the system. In 2001, Schmidt et al. [18] also projected some other architecture. Yue et al. was first to implement blockchain technology into healthcare system. Xia et al. [19] proposed a blockchain-based methodology for the sharing of medical records of a patient using cloud-based solutions. They proposed the system for sharing medical records called as Medshare with the goal to provide various advantages such as access control and enhanced security of medical records. Liang et al. [20] using blockchain technology drafted a mobile-based application to share medical data. This secure user centric approach uses channel formation plan in order to provide privacy and access control. Jiang et al. [21] blockchain based approach is based on exchanging healthcare data. Ichikawa et al. [22] utilize a non-public blockchain to make sure the integrity and convenience of medical data which is stored in the system. They

construct an application called as mHealth with the help of smartphone. A medical insurance storage system i.e. MIStore was given by Zhou et al. [23]. Wang and Song [24] came up with two approaches which are a blockchain based EHR system and an attribute based crypto system.

Current pseudonymization algorithms and parameters by a non-expert person are difficult to understand and to realise privacy guarantees. Hence using blockchain technology to provide better and efficient platform to the users.

3 Blockchain for Ehealth Care

Blockchain is about enabling peer to peer transfer of digital assets without any intermediaries. Shortly this technology was getting used in several different industries, such as finance, healthcare and manufacturing [4, 25]. Blockchain does the work of establishing trust among unknown peers and record the transaction in an immutable distributed ledger [26, 27]. Data is distributed across many different nodes over the network and method of encryption is used to maintain the quality of the stored data [28, 29]. Blockchain technology provide us with different advantages like enhanced security, secrecy and integration of data without the interference of any third party. All such advantages prove that blockchain technology is a correct option for the storage of a patient's medical data.

4 Proposed Solution

4.1 Entities Involved

4.1.1 Patient

A patient is the one who generates the medical history and is the owner of the health data. For sharing of resources a patient usually pass his medical data to the distributed storage in encrypted form. Patient is the one who builds up and keeps up the smart contract and also generate and supply characteristic private key to the user in order to access medical data.

4.1.2 User

User can be any of the hospital, doctor, lab, insurance organizations. The user node can access the data of a patient as per the rights given to them.

4.1.3 Blockchain Database

This is used to keep encrypted health data of a patient and keyword indexes related to this data is forwarded to the database by that patient. Various kinds of users hold pre-defined rights for accessing the medical data of the patient.

4.2 System Design

The proposed system consists of users: patients, doctors and administration.

4.2.1 User Layer

Users perform essential tasks of creating, reading, updating and deleting the medical data. The users would get to the framework's usefulness by a browser called DApp browser.

4.2.2 Blockchain Layer

- **Blockchain Assets**: Transactions in blockchain are referred as assets. Assets are the piece of data that can be shared with some other user over the network or simply can be stored for different purposes.
- **Governance Rules**: Blockchain technology operates over some rules, it utilizes Proof of Work (PoW) consensus algorithm.
- **Network**: In the blockchain network all the nodes are associated as peers. So, all these associated nodes have equivalent status and rights.

4.2.3 Transaction

The framework incorporates following transactions:

Add Records: This process includes the creation of medical records of a patient through DApp browser. It is comprise of various fields such as ID, name, Blood group and IPFS hash.

Algorithm Add Account (Name, email, category, password)
assign ID;
Patient Id = = Pid;

Add Data:

Add Patient Record (Name, Address, Disease, Blood Group, Contact No, Age, Gender, City)

Add Doctor Record (Name, Qualification, Specialization, Gender, Contact No)
If (m.sender == doctor) **then**
add data to particular patient's record
else Abort session
else if
retrieve Data;

Update Records: This is the process of updating of patient's medical records.

Algorithm Update Data:
If (m.sender == doctor) **then**
If (id == patient id && name == patient name) then
Update data to patient particular patient record
else return fail

View Records: This allows a user to see patient's medical data which is stored within the DApp browser. Both the patient and the doctor can view medical records.

Algorithm View Patient Record (Patient Id)
If (m.sender == doctor || patient) then
Retrieve data from specified patient (Id)
Return (patient record)

Delete Records: This allows a user to delete medical records of any patient.

Algorithm Delete Patient Record (patient id)
If (m.sender == doctor) **then**
If (id == patient id && name == patient name) then
Delete particular patient's record
return success
else fail

Grant Access: Users should have access to perform any above mentioned transactions. Medical records of a patient can only be added or updated by the doctor or nursing staff.

4.3 Work Flow

4.3.1 Process of User Registration

In this process, users have to submit their personal information, then a set of key pairs representing a user's identity will be generated by the EHR platform. Also the hash value will be created which would be a unique identifier of that user. Figure 1 represents the user registration process and validation of a user's identity related data. Whenever a user join the EHR system, a unique identifier and key pairs for that user would be created.

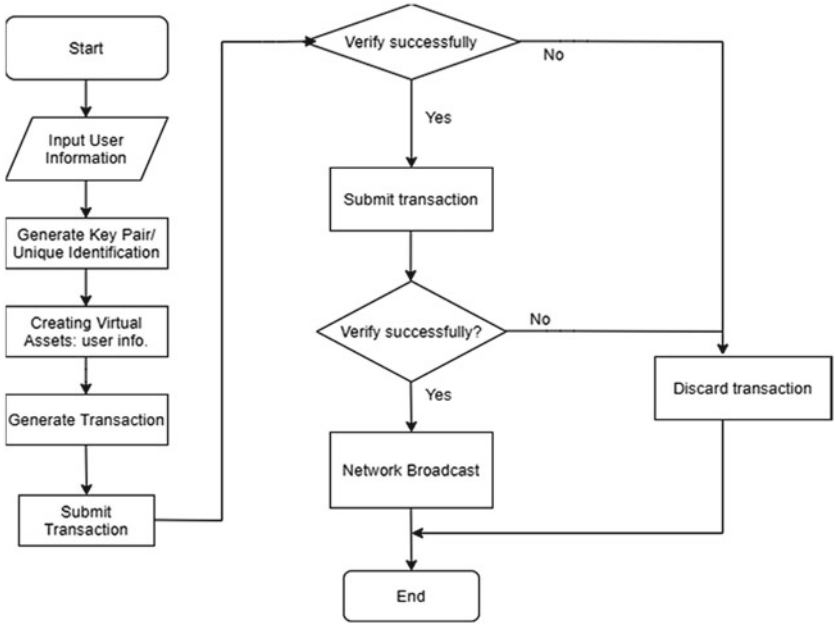

Fig. 1 User registration process

4.3.2 Process of Uploading Health Record

Doctor needs to get the patient's approval prior to uploading that patient's medical record to the blockchain database. Figure 2 represents the process of uploading health records. The EHR at the user node would be encrypted using the private key only if the user approve it. A transaction would be sent arbitrarily to a medical node in order to begin consensus and needs to decrypt the received transaction with the help of public key provided by the user. Decoded content must be fully matched in order to encapsulate transaction content into some new block and then that block gets added to the blockchain.

4.4 Smart Contract Implementation

See Fig. 3.

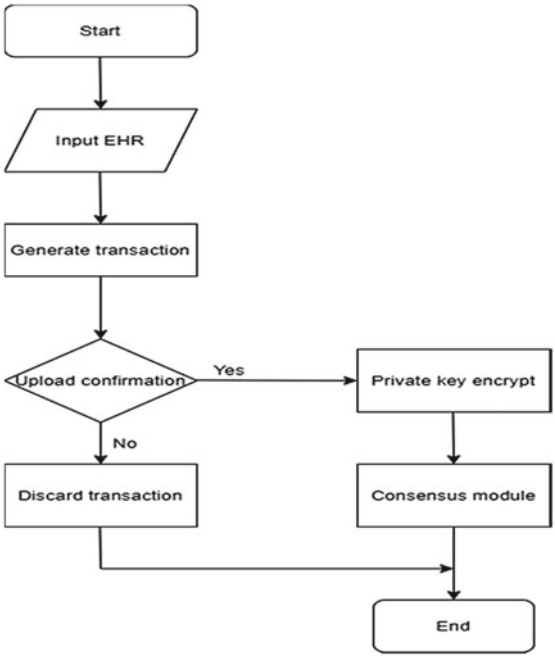

Fig. 2 Uploading health records

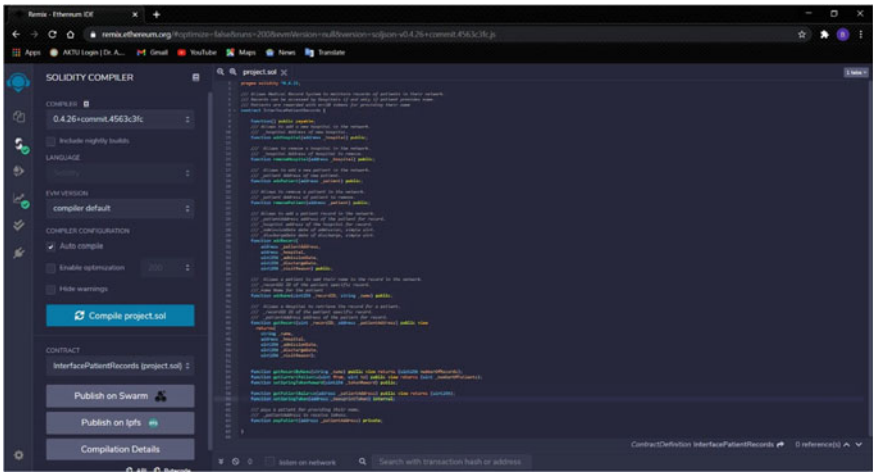

Fig. 3 Code for implementation of smart contract

5 Conclusion

In this paper we discussed the use of blockchain technology in healthcare sector and how it can be used for implementing EHR. Using blockchain technology can

provide solution to all the issues faced by EHR platform. Our proposed work provides with access rules to medical records as well as secure storage to those records. This proposed framework get rid of the central authority and security is accomplished using immutable ledger as the system become temper-proof. After having all such benefits it can be concluded that blockchain can be next revolutionary technology in healthcare sector.

6 Future Work

Blockchain technology provides secure way to share health data and also provide improved healthcare transactions. At present blockchain technology is not considered as of much importance in healthcare industry, however soon it will from numerous points of view as it is a definitive resource tracker. This kind of blockchain technology based way to deal with healthcare industry would allow users to transfer medical data in a protected way. This also provide users a way to anonymously share their medical data for the goal of medical research. Those systems which are empowered by blockchain technology have the capability of significantly decreasing the expense and the grating of current intermediates.

References

1. Tang FEI et al (2019) An efficient authentication scheme for blockchain-based electronic health records
2. Gaurav D (2020) Blockchain for EHR. Edinburgh Napier University Edinburgh, Scotland
3. Rai BK et al (2014) Security and privacy issues in healthcare information system. Int J Emerg Trends Technol Comput Sci (IJETTCS) 3(6)
4. Ayesha S et al (2009) Using blockchain for electronic health records. https://doi.org/10.1109/ACCESS.2019.2946373
5. Rai BK et al (2018) Real-time de-identification of healthcare data using ephemeral pseudonyms. Int J Emerg Trends Technol Comput Sci (IJETTCS) 7(2). ISSN 2278-6856
6. Rector A et al (2003) Clef-joining up healthcare with clinical and post-genomic research. In: Proceedings of UK e-Science all hands meeting, pp 203–211
7. Rai BK (2020) Pseudonymization based mechanism for security & privacy of healthcare. LAMBERT Academic Publishing, Germany. ISBN 978-620-0-78791-0
8. Rai BK et al (2016) Pseudonymization techniques for providing privacy and security in EHR. Int J Emerg Trends Technol Comput Sci (IJETTCS) 5(4). ISSN 2278-6858
9. Rai BK et al (2017) Patient-controlled Pseudonym-based mechanism suitable for privacy and security of electronic health record. Int J Res Eng IT Soc Sci (IJREISS) 07(2). ISSN 2250-0588
10. Lysyanskaya A et al (1999) Pseudonym systems. In: Proceedings of the sixth annual workshop on selected areas in cryptography (SAC '99)
11. Rai BK et al (2017) Prototype implementation of patient-controlled pseudonym-based mechanism for electronic health record (PcPbEHR). Int J Res Eng IT Soc Sci Impact Factor: 6.452, 07(07). ISSN 2250-0588
12. Hendry M (2001) Smart card security and applications, 2nd edn. Artech House, Norwood
13. Rankl W et al (1997) Smart card handbook. Wiley, New York

14. Thielscher C et al (2005) Patent: data processing system for patient data. International Patent, WO 03/034294 A2
15. Pommerening K et al (2004) Secondary use of the electronic health record via pseudonymisation. In: Medical and care compunetics 1. IOS Press, pp 441–446
16. Pommerening K (1994) Medical requirements for data protection. Proc IFIP Congress 2(1994):533–540
17. Peterson RL (2003) Patent: encryption system for allowing immediate universal access to medical records while maintaining complete patient control over privacy. US Patent US 2003/0074564 A1
18. Schmid V et al (2001) Patent: Verfahren zum be- oder verarbeiten von daten. German Patent, DE 199 25 910 A1
19. Xia Q et al (2017) Trust-less medical data sharing among cloud service providers via blockchain
20. Liang X et al (2017) Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In: Personal, indoor, and mobile radio communications (PIMRC), 2017 IEEE 28th annual international symposium
21. Jiang S et al (2018) A blockchain-based platform for healthcare information exchange. IEEE International conference on smart computing (SMARTCOMP)
22. Ichikawa et al (2017) Tamper-resistant mobile health using blockchain technology. JMIR Mhealth Uhealth 5:e111
23. Zhou et al (2018) A blockchain-based medical insurance storage system. J Med Syst 42:149
24. Wang H et al (2018) Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. J Med Syst 42:152
25. Rai BK et al (2018) A review paper on regulating bitcoin currencies. Int J Res Appl Sci Eng Techno (IJRASET) 6(4). ISSN: 2321-9653
26. Rabah et al (2017) Challenges & opportunities for blockchain powered healthcare systems: a review. Mara Res J Med Health Sci
27. Hölbl M et al (2018) A systematic review of the use of blockchain in healthcare. Symmetry
28. Esposito C et al (2018) Blockchain: a panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput
29. Engelhardt et al (2017) Hitching healthcare to the chain: an introduction to blockchain technology in the healthcare sector. Technol Innov Manag Rev