International Journal of E-Health and Medical Communications
Volume 13 • Issue 4

Blockchain-Enabled Electronic Health Records for Healthcare 4.0

Bipin Kumar Rai, ABES Institute of Technology, India*
https://orcid.org/0000-0002-9834-8093

ABSTRACT

Healthcare delivery is on the verge of a fundamental shift into the new era of smart and connected health care, termed Health Care 4.0. Sharing healthcare data is an important step in improving the healthcare system's intelligence and service quality. Healthcare data, which is a personal asset of the patient, should be owned and managed by the patient rather than being dispersed among several healthcare systems, preventing data exchange and jeopardizing patient privacy. EHRs (electronic health records) assist individuals by allowing them to combine and manage their medical data. On the other hand, today's EHR systems fall short of providing patients with traceable, trustworthy, and secure ownership over their medical data, creating serious security risks. In this article, the authors propose PcBEHR (patient-controlled blockchain enabled electronic health records) as a way for patients to have safe control over their data that is decentralized, immutable, transparent, traceable, and trustworthy. Decentralized interplanetary file storage (IPFS) is used in the suggested technique.

KEYWORDS

Blockchain, EHR, Ethereum, Healthcare, Smart Contracts

1. INTRODUCTION

At the moment, events are often covered in the public media, yet there is a lack of care regarding sensitive data. People, on the other hand, tend to feel more concerned when their personal healthcare-related data is at risk, owing to the ease with which they can envision reasons for abuse and comprehend the consequences of such misuse. Another apparent example is that almost everyone is presented with loan and insurance applications at some time in their lives. We can no longer dispute that privacy protection has a direct influence on both personal well-being and society as a whole. In fact, privacy is regarded as a basic human right. There are currently no particular entities in India that pay close attention to the necessity of getting informed consent from subjects. As a result, most hospitals and clinics are overly cautious when it comes to analyzing their material since they are aware that the implications of the information included are quite complicated; hence, there is a genuine risk that informed consent is really ill-informed consent. Research ethics and security rules compel research units to devote increasing money and effort to privacy and identity protection, yet restrictive regulations

DOI: 10.4018/IJEHMC.309438

*Corresponding Author

controlling the transfer of medical information may discourage research needlessly. Therefore, a patient-controlled mechanism is required.

EHR systems are extremely craved for the structured unification of all pertinent medical data of an individual and to exhibit the lifelong medical record. Various confidentiality threats of healthcare data are crucial which may be either from within the institution or outside by some intruder. Each healthcare unit, hospitals and clinic have their own information system for maintaining the patient's data. Therefore, standards for data exchange are required and electronic health records and data needs to be standardized, including semantic interoperability (standards for exchange of patient's data among EHR systems.

Most of the solutions don't provide full control to the patients (Al-Hamdani, 2010). Smart card healthcare systems developed in European countries are not strongly privacy preserving as anyone can access a patient's information from a health card without her/his consent. Indivo is the first patient-controlled web-based healthcare system which provide options to own a secure complete medical record, integrating EHRs of different health centers. In Serbia, the architecture of the healthcare system is a hybrid smart card-based solution (Vučetić et al., 2011).

The whole patient's experience of medical care is private. Hence providing confidentiality of medicine prescriptions is important one (Ateniese & de Medeiros, 2002). In smart-card based e-prescriptions system both patient and doctor have security concern with this e-prescription data as other parties are involved and some parties may use for their benefits like marketing etc. (Yang et al., 2004).

Access control mechanisms and applications related to e-prescription systems and other consumer related healthcare services requires a secure mechanism (Rai & Solanki, 2021). In the future, Blockchain technology seems to be more appealing in the field of healthcare(Mayer et al., 2020). We need to handle the following security issues in a proper way while accessing EHR (Rai & Srivastava, 2014).

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 healthcare information systems.
3. **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.
4. **Access Control:** The objectives of the access control are protecting any Information system from unauthorized access and the same time making available to authorized users. Electronic Health Record recommend that information systems need to develop a strong mechanism for protecting the unauthorized access of the data (Byers et al., 2002).

1.1 Novelty of the Manuscript

The novel contributions in this paper are summarized as follows:

- A patient-controlled blockchain enabled architecture is proposed which will be most suitable for health care information system.

2. RELATED WORK

Several mechanisms are available for ensuring security and privacy issues related to healthcare by pseudonymization technique (Neubauer & Kolb, 2009).

Pseudonymization is most suitable for healthcare information system which is similar to anonymization (Neubauer & Kolb, 2009; Rai & Srivastava, 2016). The only difference is identifying information is separated from the health records, referenced by pseudonym (which is a unique random number) but not permanently deleted. Therefore, pseudonymization is patient's controlled reversible process under specified circumstances. It is also applied in several applications like healthcare information system (Bruland et al., 2018).

Pseudonyms are secret random numbers that are commonly used as links between patients and health records, with the links only being recoverable when authorized (Amin et al., 2019).

Peterson approach (Peterson, 2003) ask users to register on a service provider's website. After registration, they are given a unique Global key (GK) and server-side key (SSID). A unique "personal encryption key (PEK)" and password must also be provided. GK is included on the ID card. By entering GK and PEK, the user retrieves data from the database.

(Slamanig & Stingl, 2008) proposed a hull architecture, here instead of storing the relation between patients and their dataset in centralized manner, all data are stored in two separate databases. One store plaintext pseudonyms and related medical datasets in plaintext for performance reasons. Another database is used to store the personal information of users as well as their encrypted pseudonyms.

Electronic health card (eGK) is a designed as service-oriented architecture (SOA)having some restrictions like local card access only, supported by Ministry of health, Germany (Zhang et al., 2009). Its architecture consists of five layers. first layer is Presentation layer which provide communication interface to user. Second layer to provide different services, third layer is Business layer which combine different services. Fourth layer, application layer manages data and user right. Last layer is infrastructure layer.

(Thielscher et al., 2005)proposed a solution in which "identification data" and medical record anamnesis data are stored in separate databases. In Pommerening (K & M, 2004) approach different ways for secondary use of healthcare data have been recommended. (Kushida et al., 2012) highlighted preventive steps for patient anonymity and untraceability.

(Bacelar-Silva et al., 2011) shows that different countries have different choices based on community needs, but most popular EHR solutions assert for patient-centered because it gives the patient total access rights. (Rai, n.d.) PcPbEHR system is patient-centered which combine pseudonymization techniques with an encryption mechanism to create an efficient mechanism for healthcare information system security and privacy.

Different firms are becoming familiar with the blockchain technology to enhance the manner in which they manage patient's data. Yue et al was first to implement blockchain technology into healthcare system. He came up with approach for the architecture of such application that can be used to share the patient medical record between various entities, but does not involve analysis of security and privacy. Jenkins et al. gives the idea of using blockchain technology for a multifaceted authentication in a particular research situation for example clinical huge data investigation with practical biomarkers.

(Clim et al., 2019) 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. Many blockchain research, in particular, have given numerous ideas and implemented them using prominent platforms like Ethereum and Hyperledger. Because of the size and cost of blockchain, the EHR system should consider that storing all EHR data in blockchain is difficult. As a result, if a sudden and unexpected need for storage and resources arises, blockchain-based EHR systems should be able to meet the demand.

(Ichikawa Daisuke and Kashiyama 2017) 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. This application was temper proof and used for sleeping disorder that permits psychological behavioural therapy. (Mayer et al., 2020; Passerat-Palmbach et al., 2019; Shahnaz et al., 2019) advoates the potential and suitability of blockchain for healthcare.

(Khezr et al., 2019) has done comprehensive review of the use of blockchain. (Gordon & Catalini, 2018) advocate patient-driven operability and possibility in healthcare using blockchain.

(Kim et al., 2020) came up with hybrid combination of cloud and blockchain based EHR system and an attribute based crypto system. In the current era, online administrations are turning out to be more information driven, they gather, process, examine and store huge amount of individual data as pseudonymized data sets. Such systems are developed to secure personal data as well as a user has full control over the data. However, 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(Mayer et al., 2020).

3. PRELIMINARIES

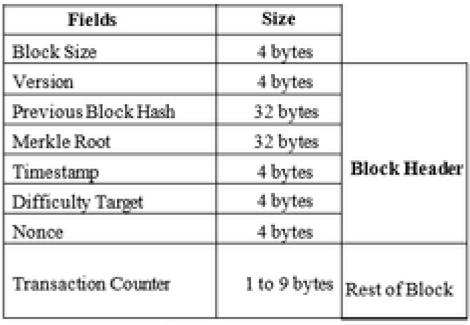
Blockchain technology could very well be the answer to data privacy and security. Blockchain provides robustness against failure and expose of data. Blockchain decentralized database, stores all transactional history. In the form of a chain, the blocks are connected to one another. The Genesis block is the initial block in the chain. A Block Header and a list of transactions are included in each block. It records data using a decentralised architecture. Figure 1 shows the construction of a block in the blockchain.

3.1 Consensus Protocol

The blockchain consensus process is utilised for the insertion of a block. In a permissionless architecture, any transaction is considered legitimate only after the system has proof that the authorised nodes have completed enough computational effort. Miners (who creates blocks) are continuously attempting to solve cryptographic problems known as Proof of Work (PoW) using hash computations. Mining is the process of adding a new block to the blockchain. A hash in the header identifies each block in the chain. The Secure Hash Algorithm (SHA-256) is used for generating hash code. The address (hash code) of the preceding block in the chain is included in each header [5]. A three-block blockchain is depicted in Figure 2. Each block contains data, a hash of the previous block's data, and a hash of this block's data. Except for the genesis block and every block in the blockchain, is connected to the one before it. If any data in a block is altered, the hash code of that block and subsequent blocks will be wrong.

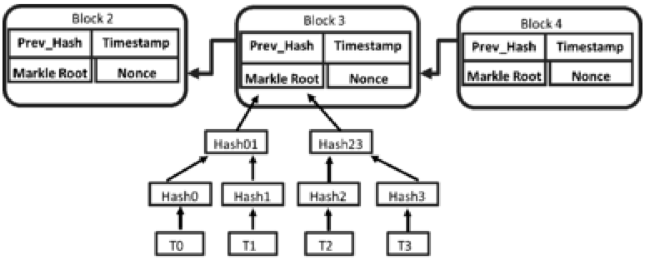
Because of the distributed nature of blockchain, every participant of the blockchain network has a copy of the chain and must make the same modifications in order for the entire blockchain to remain consistent, which is very unlikely. However, implementing blockchain in the context of EHR is not simple and comes with a slew of issues, including the need for a lot of computing power for PoW, limited scalability, and significant latency for transaction confirmation via the network. Paxos, Raft, BFT (Byzantine fault tolerance), and PBFT (Practical Byzantine fault tolerance) are some of

Figure 1. Structure of a block in the blockchain



Fields	Size	
Block Size	4 bytes	
Version	4 bytes	Block Header
Previous Block Hash	32 bytes	
Merkle Root	32 bytes	
Timestamp	4 bytes	
Difficulty Target	4 bytes	
Nonce	4 bytes	
Transaction Counter	1 to 9 bytes	Rest of Block

Figure 2. A simple blockchain with 3 blocks



the distributed system-based consensus mechanisms used in permissioned blockchain. PBFT is the most effective.

Blockchain technology can offer a feasible solution for medical sector because of its permission less, transparency and decentralized nature. Immutable nature of the blockchain technology can submerged as a significant alternative for medical services. It can provide various advantages like securing medical data, consequences of clinical preliminaries and guarantee administrative compliances. Utilization of smart contracts can demonstrate how blockchain technology can be employed to help continuous patient observing and clinical interventions. Such frameworks guarantee security of medical data of a patient while giving admittance to them. [26].

Blockchain technology allows for secure medical data exchange and provides patients complete ownership over their health information. Blockchain technology is emerging technology most suitable for development of a solution that not only securely stores and share medical information, but also ensures the privacy of each patient's data by granting individuals ownership of their health data. Aside from the benefits of blockchain for healthcare administration, its obstacles must be addressed ahead of time [29].

4. PROPOSED WORK (PCBEHR)

The blockchain is the most suited technology for the healthcare system because to its inability to erase or modify information within blocks. In this section detail design of the PcBEHR is described.

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 passes his/her 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 Architecture

The proposed PcBEHR system comprises of three different layers: user interface layer, blockchain layer, data access layer, as shown in the figure 3. Participants can interact with the system through any PC device. Members register through the customer application. A private key with a unique ID is generated by the admin in order to enlist the member. Various members have various parts in the framework and can just access data that they have consent to get to. Data can be added by a patient by summoning the chain code for the creation of a transaction to the network. At that point the transactions are dispersed over the network guaranteeing that each transaction is disseminated to each member and can't be altered or erased by unapproved members. As transactions are just added to the previous hash with a timestamp guaranteeing that the network is completely secure.

The proposed system consists of users: patients, doctors and administration. As shown in the fig 5, system consists of different layers.

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

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.

4.2.3 Governance Rules

Blockchain technology operates over some rules, it utilizes Proof of Work (PoW) consensus algorithm.

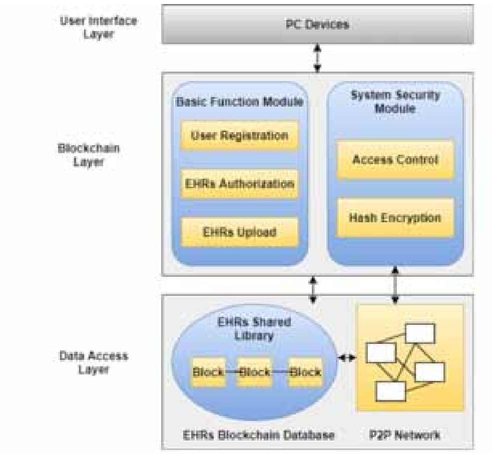
4.2.4 Network

In the blockchain network all the nodes are associated as peers. So, all these associated nodes have equivalent status and rights.

4.2.5 Transaction

The framework incorporates following transactions:

Figure 3. PcBEHR system architecture



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

```
Add Record (Name, email, category, password)
Patient Id == Pid;   // Assigning unique Patient ID
Add Patient Record (Name, Address, Disease, Blood Group, Contact
No, Age, Gender, City)
Add Doctor Record (Name, Qualification, Specialization, Gender,
Contact No)
If (doctor) then
   add patient data to his/her patient's record
else Abort session
```

Update Records: This is the process of updating of patient's medical records. By this only patient's basic information will be changed and not the IPFS hash.

```
 If (doctor) then
       If (Pid =patient id AND name = patient name) then
                      Update patient's 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.

```
View Record (PId)
  If (Authorized doctor OR patient) then
            Retrieve data from patient PId
     Return
```

Delete Records: This allows a user to delete medical records of any patient. Here, user would be doctor who have rights to delete medical records of a patient stored over the blockchain.

```
Delete Record (Pid)
If (doctor) then
    If (Pid = patient id AND name =patient name) then
        Delete 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.

5. IMPLEMENTATION OF PCBEHR

5.1 Tools Used

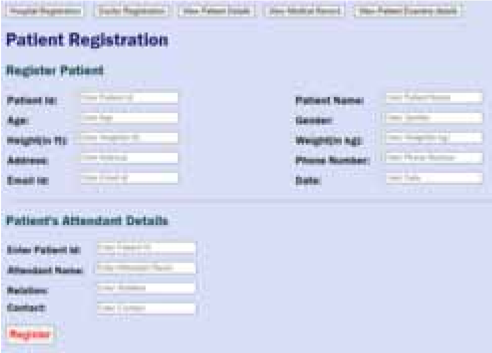
- **NodeJS:** NodeJS is a runtime environment that allows to launch both frontend and backend of web app using JavaScript.
- **Ganache:** Ganache is a personal Ethereum Blockchain used to test smart contracts which is used for deploy the contracts without any cost.
- **Remix:** Remix IDE is an open-source web and desktop application. It has modules for testing, debugging and deploying smart contract.
- **Ethereum:** Ethereum is a decentralized, open-source blockchain with smart contract functionality.

5.2 User Registration

Registration is mandatory to use PcBEHR system:

- **Patient registration:** Each patient has to register over the PcBEHR platform so that the information will be save for the future and for managing the data over the portal so that patient can access its record any time. In the figure 4, we can see that how the patient registers over the PcBEHR.
- **Doctor registration:** Each doctor has to register over the PcBEHR platform so that the information will be save for the future and for managing the data over the portal so that doctor can access its record any time and also available to the patients. In the figure 5, we can see that how the doctor registers over the PcBEHR.
- **Hospital registration:** Figure 6 shows registration of a hospital over PcBEHR platform.

Figure 4. Patient registration process



Patient Registration

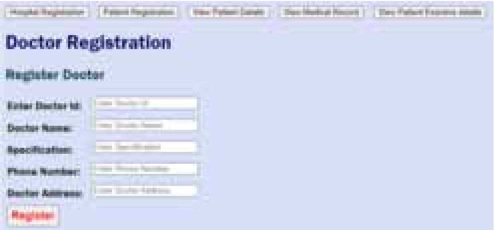
Register Patient

Patient Id:
Patient Name:
Age:
Gender:
Height(in ft):
Weight(in kg):
Address:
Phone Number:
Email Id:
Date:

Patient's Attendant Details

Enter Patient Id:
Attendant Name:
Relation:
Contact:

Figure 5. Doctor registration process

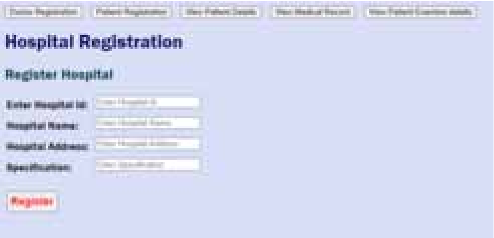


Doctor Registration

Register Doctor

Enter Doctor Id:
Doctor Name:
Specification:
Phone Number:
Doctor Address:

Figure 6. Hospital registration process



Hospital Registration

Register Hospital

Enter Hospital Id:
Hospital Name:
Hospital Address:
Specification:

5.3 Process of Deploying Smart Contracts

These are fundamentally lines of code that are kept on a blockchain and they get automatically executed whenever predetermined conditions are met. After programming, we will compile the code using EVM and then compiled program can be execute and deployed on the Ethereum. Utilization of smart contracts can demonstrate how blockchain technology can be employed to help continuous patient observing and clinical interventions. Such frameworks guarantee security of medical data of a patient while giving admittance to them.

In the figure 7, account information is showed. Each account has its own different address and a unique key which is known as PRIVATE KEY.

- **Smart contract for patient related process:** During the registration in the platform, it is very necessary to store all the information of patient so that it can be used in the future. It can be very beneficial for both the patient and hospitals. Here showing in the fig14, smart contract we have taken several parameters to store the patient record like patient name, patient age, patient gender, patient height, patient weight, patient address, patient emailed, etc.

```
function store_patient_details(uint256 patient_id,string memory
_patient_name,uint256 _age,string memory _gender,string memory
_height,uint256 _weight,string memory _patient_address,uint256 _
phone_no,string memory _email_id)public isOwner {
      p.patient_name=_patient_name;
p.age=_age;
p.gender=_gender;
p.height=_height;
p.weight=_weight;
p.patient_address=_patient_address;
p.phone_no=_phone_no;
p.email_id=_email_id;
       patientlist[patient_id] = p;
}
```

- **Adding Blocks to the Network:** In the figure 8, after successfully verifying [block:1 txIndex:0] and [block:2 txIndex:0] is added in the blockchain network. Now these bocks are verified and ready to store the patient information on the blockchain network. Information of patient is permanently stored in these blocks. This is what holds the safety of blockchain.

In the figure 9, information of patient can be stored. Here different parameters are used for storing the patient information such as, patient_id, _patient_name, _age, _gender, _height, _weight, _patient_address, _phone_no, _email_id, _date.

Figure 7. Account information

ACCOUNT INFORMATION

ACCOUNT ADDRESS

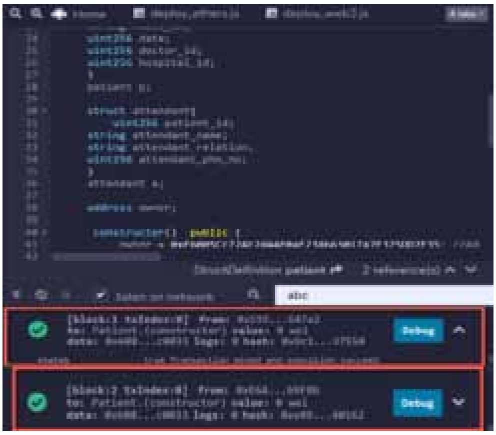
[illegible]

PRIVATE KEY

[illegible]

Do not use this private key on a public blockchain; use it for development purposes only!

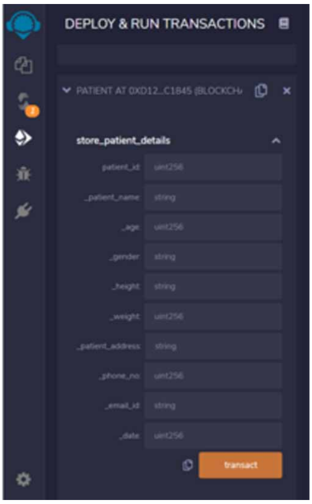
Figure 8. Adding blocks in the blockchain network



```
        uint256 data;
        uint256 doctor_id;
        uint256 hospital_id;
        }
        patient p;

        struct attendant{
            uint256 patient_id;
        string attendant_name;
        string attendant_relation;
        uint256 attendant_phn_no;
        }
        attendant a;

        address owner;

         constructor() public {
            owner = [illegible]
```

```
[block:1 txIndex:0] from: 0x[illegible]
to: Patient.(constructor) value: 0 wei
data: 0x608...c0033 logs: 0 hash: 0x[illegible]

[block:2 txIndex:0] from: 0x[illegible]
to: Patient.(constructor) value: 0 wei
data: 0x608...c0033 logs: 0 hash: 0x[illegible]
```

Figure 9. Storing information of patient for transaction



DEPLOY & RUN TRANSACTIONS

PATIENT AT 0XD12...C1845 (BLOCKCH

store_patient_details

patient_id	uint256
_patient_name	string
_age	uint256
_gender	string
_height	string
_weight	uint256
_patient_address	string
_phone_no	uint256
_email_id	string
_date	uint256

These files are immutable as IPFS has built-in security of hash. If user wants to retrieve the file, from the IPFS these files are only accessible to the authorized members. Another benefit of using hashes is avoid duplication. When multiple users try to upload the same file, it will only be accepted one, making the network efficient.

7. CONCLUSION

In this paper we discussed the use of blockchain technology in healthcare sector and how it can be used for implementing EHR. Advancement in technology can help healthcare sector to deliver better patient care. However, there are still few issues like privacy, information security, and authentication. Using blockchain technology can provide solution to all such issues. Our proposed work provides with access rules to medical records as well as secure storage to those records. The system is easy to understand and use for the users. The hash values after the encryption of healthcare records will be put away on the blockchain and their connected index set will be put away on the smart contracts.

Due to this, receiver would be able to verify the wholeness of the healthcare records. Our proposed framework get rid of the central authority and security of the proposed framework 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.

REFERENCES

Al-Hamdani, W. A. (2010). Cryptography based access control in healthcare Web systems. *Proceedings of the 2010 Information Security Curriculum Development Annual Conference, InfoSecCD'10*, (pp. 66–79). doi:10.1145/1940941.1940960

Amin, R., Islam, S. K. H., Gope, P., Choo, K. K. R., & Tapas, N. (2019). Anonymity Preserving and Lightweight Multimedical Server Authentication Protocol for Telecare Medical Information System. *IEEE Journal of Biomedical and Health Informatics*, *23*(4), 1749–1759. doi:10.1109/JBHI.2018.2870319 PMID:31283471

Ateniese, G., & de Medeiros, B. (2002). Anonymous E-prescriptions. *Proceedings of the ACM Conference on Computer and Communications Security, WORKSHOP*, (pp. 19–31). doi:10.1145/644527.644530

Bacelar-Silva, G. M., Vicente, C. M. O., David, M., & Antunes, L. (2011). Comparing security and privacy issues of EHR - Portugal, the Netherlands and the United Kingdom. *ACM International Conference Proceeding Series*. doi:10.1145/2093698.2093755

Bruland, P., Doods, J., Brix, T., Dugas, M., & Storck, M. (2018). Connecting healthcare and clinical research: Workflow optimizations through seamless integration of EHR, pseudonymization services and EDC systems. *International Journal of Medical Informatics*, *119*, 103–108. doi:10.1016/j.ijmedinf.2018.09.007 PMID:30342678

Byers, S., Rubin, A. D., & Kormann, D. (2002). Defending against an Internet-based attack on the physical world. *Proceedings of the ACM Conference on Computer and Communications Security, WORKSHOP*, (pp. 11–18). doi:10.1145/644527.644529

Clim, A., Zota, R. D., & Constantinescu, R. (2019). Data exchanges based on blockchain in m-Health applications. *Procedia Computer Science*, *160*, 281–288. doi:10.1016/j.procs.2019.11.088

Gordon, W. J., & Catalini, C. (2018). Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. In Computational and Structural Biotechnology Journal, 16. doi:10.1016/j.csbj.2018.06.003

Ichikawa, D., Kashiyama, M., & Ueno, T. (2017). Tamper-Resistant Mobile Health Using Blockchain Technology. *JMIR mHealth and uHealth*, *5*(7), e111. doi:10.2196/mhealth.7938 PMID:28747296

Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain technology in healthcare: A comprehensive review and directions for future research. *Applied Sciences (Switzerland)*, *9*(9), 1736. doi:10.3390/app9091736

Kim, M., Yu, S., Lee, J., Park, Y., & Park, Y. (2020). Design of secure protocol for cloud-assisted electronic health record system using blockchain. *Sensors (Switzerland)*, *20*(10), 2913. doi:10.3390/s20102913 PMID:32455635

Kushida, C. A., Nichols, D. A., Jadrnicek, R., Miller, R., Walsh, J. K., & Griffin, K. (2012). Strategies for De-identification and Anonymization of Electronic Health Record Data for Use in Multicenter Research Studies. *Medical Care*, *50*, S82–S101. doi:10.1097/MLR.0b013e3182585355 PMID:22692265

Mayer, A. H., da Costa, C. A., & Righi, R. (2020). Electronic health records in a Blockchain: A systematic review. *Health Informatics Journal*, *26*(2), 1273–1288. doi:10.1177/1460458219866350 PMID:31566472

Neubauer, T., & Kolb, M. (2009). Technologies for the pseudonymization of medical data: a legal evaluation. *2009 Fourth International Conference on Systems*, (pp. 7–12). doi:10.1109/ICONS.2009.48

Passerat-Palmbach, J., Farnan, T., Miller, R., Gross, M. S., Flannery, H. L., & Gleim, B. (2019). A blockchain-orchestrated federated learning architecture for healthcare consortia..

Peterson, R. (2003). *Encryption system for allowing immediate universal access to medical records while maintaining complete patient control over privacy*. Google Patents.

Pommerening, K., & Reng, M. (2004). Secondary use of the EHR via pseudonymisation. *Studies in Health Technology and Informatics, 103*, 441–446. http://europepmc.org/article/MED/15747953

Rai, B. K. (2022). Patient-Controlled Mechanism Using Pseudonymization Technique for Ensuring the Security and Privacy of Electronic Health Records. International Journal of Reliable and Quality E-Healthcare (IJRQEH), 11(1), 1-15. http://doi.org/10.4018/IJRQEH.297076

Rai, B. K., & Solanki, T. (2021). Access Control Mechanism in Healthcare Information System. *Cybersecurity: Ambient Technologies, IoT, and Industry 4.0 Implications*, *149*.

Rai, B. K., & Srivastava, A. K. (2014). Security and Privacy issues in healthcare Information System. *International Journal of Emerging Trends & Technology in Computer Science, 3*(6).

Rai, B.K. (2022). Ephemeral pseudonym based de-identification system to reduce impact of inference attacks in healthcare information system. Health Serv Outcomes Res Method 22, 397–415 https://doi.org/10.1007/s10742-021-00268-2

Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using Blockchain for Electronic Health Records. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 147782–147795. doi:10.1109/ACCESS.2019.2946373

Slamanig, D., & Stingl, C. (2008). Privacy aspects of eHealth. *ARES 2008 - 3rd International Conference on Availability, Security, and Reliability, Proceedings*, 1226–1233. doi:10.1109/ARES.2008.115

Thielscher, C., Gottfried, M., Umbreit, S., Boegner, F., Haack, J., & Schroeders, N. (2005). Patent: Data processing system for patient data. Int. *Patent, WO*, *3*(034294), A2.

Vučetić, M., Uzelac, A., & Gligorić, N. (2011). E-health transformation model in Serbia: Design, architecture and developing. *Proceedings of International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, (pp. 566–573). doi:10.1109/CyberC.2011.96

Yang, Y., Han, X., Bao, F., Deng, R. H., Yang, Y., Han, X., & Bao, F. (2004). A smart-card-enabled privacy preserving E-prescription system A smart-card-enabled privacy preserving E-prescription system Citation Citation A smart-card-enabled privacy preserving E-prescription system A Smart-Card-Enabled Privacy Preserving E-Prescription System. *IEEE Transactions on Information Technology in Biomedicine*, *8*(1), 47–58. doi:10.1109/TITB.2004.824731 PMID:15055801

Zhang, X. G., Li, J. S., Zhou, T. S., Yang, Y. B., Chen, Y. Q., Xue, W. G., & Zhao, J. P. (2009). Design and implementation of interoperable medical information system based on SOA. *Proceedings of IEEE International Symposium on IT in Medicine and Education*, 1074–1078. doi:10.1109/ITIME.2009.5236236