Analytical Study of Blockchain Enabled Security Enhancement Methods for Healthcare Data

Moumita Roy¹², Dr. Monisha Singh³

¹PhD Scholar, Department of Computer Science, Christ Deemed to be University, Bengaluru, India
²Assistant Professor, Department of Computer Application, CMR Institute of Technology, Bengaluru, India
³Assistant Professor, Department of Computer Science, Christ Deemed to be University, Bengaluru, India

moumita.r@cmrit.ac.in

Abstract. Healthcare data protection is very much required in the present time due to the rate of growth in data volume and sensitivity of the data. The data is collected through EHR, diagnostic image like scan or x-ray or IoT wearable devices which has sensors and shared with stakeholders who can analyse the data and use it for betterment of the processes. Benefits of medical data sharing among the entities makes it even more vulnerable. In this paper we have studied and analysed few blockchain based methods of securing healthcare data which is stored in cloud. The methods studied is successful in keeping the data safe from unauthorized access.

Keywords: Blockchain, Healthcare, Cloud, Ethereum, Hyperledger Fabric, EHR, IoT

1. Introduction

The healthcare industry has undergone a large-scale rapid-paced digitization transformation. This positive technological impact generated a massive load of electronic records like the Electronic Medical Report (EMR) or Electronic Healthcare Data (EHR) that needs to be managed and accessed by the stakeholders. Availability and security of these data sources is extremely important as it directly affects the health and lives of the patients and their treatment. Also, such data can be used for research–related work or analyzed to develop market strategies.

Cloud storage is a convenient solution for storing huge bulk of data in the present times. The ubiquitous, economic, scalable and on-demand features of cloud storage make it more efficient as a user data repository as compared to other traditional storage mechanisms. The concept of cloud computing can be further extended to decentralized idea of fog computing. Cloud/fog computing can work with other technologies, like IoT networks, at ease [1]. A major limitation of cloud storage is that the users cannot control the data they stored on cloud and they have to rely on the service providers for keeping the data secure. External dependency makes the data extremely vulnerable and the issues of user trust, data accessibility and security need to be solved [2].

Decentralized cloud solutions can be an answer to this data vulnerability issue. Smart contracts [3] along with blockchain [4] can create traceability and provide secure data access in cloud platforms [5].
A contract can be created, verified and applied between users, using rules of smart contract, to ensure the execution of a fair data transaction. Blockchain decentralizes the network, makes it more stable and stops any unauthorized mediatory intervention. That way, the data on the cloud platform becomes more secure. The merger of blockchain and cloud technologies have shown a lot of potential in the recent times in managing data access. The reason behind the success of the blockchain technology in enhancing security is its complexity [6]. A lot of effort is needed to understand the complex technology, create and implement a blockchain, and that makes it almost impossible to break it.

With the increase in the number of e-health services, volume of health-related documents being stored on cloud is also on a rise. Health records are confidential and requires secure storage. To mitigate the security challenges of cloud storage and provide uninterrupted and economic healthcare services, blockchain assisted cloud storage can be an excellent solution. We have identified few such research solutions which are quite promising and mature in their approach. Our study aims at analyzing and comparing them, bringing forward their strengths and weaknesses and also bringing to light the research gaps, if any.

2. Blockchain Technology

The blockchain concept was invented by Satoshi Nakamoto in the year 2008 for building cryptocurrency bitcoin [7]. Blockchain is a distributed public transaction ledger which keeps growing every time a new transaction takes place and a new record or block is added to the existing chain. The new block contains cryptographic hash of the previous block, time of its creation and other transactional data that are encoded into a Merkle tree. A record once added to a blockchain, cannot be modified.

The primary reasons that make a blockchain extremely secure are its de-centralized nature, immutability, data encryption and change transparency [8]. Traditional centralized systems like the client-server store all data in a centralized repository, making the system vulnerable to hacking. During maintenance or downtime, the entire system becomes unavailable and in worst case if the systems gets corrupt or fails beyond repair, all the data will be lost. Blockchain being a decentralized network, is almost not hackable. It has the benefit of not being controlled by any central authority or third-party controller. Blockchain is immutable means the data once stored in a blockchain becomes tamper proof. This can be achieved using cryptographic hash functions. Blockchain is transparent but it also protects the identity of the user. Transaction history will show each and every transaction performed but the username will be encrypted for protecting user’s privacy.

![Blockchain Architecture work-flow for a new transaction.](image)

**Figure 1.** Blockchain Architecture work-flow for a new transaction.

When a new transaction is initiated by a user, a new block is created containing the encrypted data and link to previous block. The information about the transaction is passed on to all users and the transaction is validated. The validated transaction block then gets connected to the existing chain of blocks. Fig. 1 depicts the flow of creation of a new block in a blockchain [9].

The use of blockchain started with the cryptocurrency Bitcoin but now it is being used for making smart contracts, creating supply chain, network security enhancement, banking and many more industry
sectors. Presently many blockchain platforms are widely in use, like Ethereum [10], Hyperledger Fabric [11] and IBM Blockchain [12].

Ethereum and Hyperledger Fabric are the two most commonly used public blockchain smart contract platforms. Ethereum technologies run on Ethernet Virtual Machine (EVM) and uses a public network. Each node in this network is identifiable by all other nodes. Ethereum users communicate with other nodes using smart contracts. The miner node solves the decryption puzzle (Proof of Work) and earns a reward (called Gas). Hyperledger Fabric is a permissioned blockchain in which nodes cannot publicly identify each other. Each node can be configured to perform specific tasks. An endorsing node sends transaction information to few or all other nodes. The endorsing node simulates the execution of the transaction and sends the result to the client node. The client node sends the result to the ordering node which creates the block for that transaction. For multiple transactions, node creation is done on first come first serve basis.

3. Healthcare and Technology

Healthcare now is of importance like never before, due to the increasing global population, the rise in the average age of the global population and the chronic and newer lifestyle disease that the world is getting affected with every day. Given the situation, more and more people will become old and suffer from chronic diseases and as a result basic healthcare will become super expensive and out of reach of common people. To get out of this deadlock, technological intervention is required.

Technological aid cannot reduce the rate of population aging or their getting sick with chronic illness, but can make the healthcare services affordable and accessible. Technology can provide with the following light-on-the-pocket healthcare advances which can save many lives:

- Monitoring a patient in the real-time and reporting any change in the status immediately.
- The end-to-end process of treating a patient can be automated making data flow from one equipment to the other with the help of wireless communication. That way the process will be much faster and error free.
- Data can be analyzed to generate reports directly, without storing the raw data. A lot of memory space will be saved.
- Devices can be configured to set alert to medical personnel for patients who need critical care or are on life support.
- Online medical consultations can be possible when the patient and the medical practitioner are geographically apart.
- Data collected can be used in research work and improvement of the future.

Technologies like Artificial Intelligence, Cloud Computing, Big Data and Internet of Things (IoT) are helping in automating healthcare processes by connecting the medical devices over a network and provide scalable virtual infrastructures for computation and storage of data and reports.

Figure 2. Growth in Digital Health Market in U.S. between 2014 to 2025. [9]
Across the globe, the use of technology in Healthcare domain is rapidly growing over the past decade. Fig. 2 shows the statistics of the rate of digitization in U.S.

4. Blockchain Based Healthcare Applications

![Blockchain implementation in Healthcare applications](image)

**Figure 3.** Blockchain implementation in Healthcare applications – the workflow.

After digitization of healthcare, a huge volume of medical data is getting generated. These data are critical and sensitive; critical as the data needs to be always available for the timely medical assistance of the patient and sensitive as the data can be very personal to the person involved. These data need to be protected and kept safe from any manipulation or loss.

Blockchain technology can be used to provide protected storage to the healthcare data generated due to digitization. Presently many healthcare applications have implemented blockchain in their system [13]. Such systems start with the generation of the data which after getting validated using a blockchain is send to the medical application through which the data reaches the concerned stakeholders. Raw data collected from primary sources like the patients, medical practitioners and staffs, pharmacies and pathological labs are gathered which becomes the starting point of the data management operation (example, Electronic Health Record). Blockchain technology secures this collected data using encryption and consensus algorithms. This secure data is accessed by the stakeholders like pharmaceutical companies, researchers, government authorities etc. through the healthcare applications. Fig. 3 shown the diagrammatic representation of the process flow.

In this paper, we will concentrate primarily on the data gathering, blockchain validation and storage of the healthcare data. The entire process of collecting and protecting the data, storing it and making is accessible is very much needed as the healthcare related data is critical and can be put to multiple and extremely important uses. Regarding security, as discussed, blockchain can provide a productive and robust solution.

4.1. Why sharing of medical data is important?

Traditional healthcare system requires a lot of human interference and judgement. If the system has to be automated with smart components, the system has to collect, store, learn from and manage a huge bulk of data. By doing so the practitioners can provide better care to the patients and collaboration among the stakeholders will improve the overall system. This sharing of information can happen in multiple levels and dimensions. A patient can share his medical history with doctor and insurance company, doctor can share data with pharmaceutical company and pathological laboratory, pharmaceutical company can interact with research centre and so on [14].

The types and formats of data shared are varied. The data can be in form of EHRs, medical images, data coming from personal wearable devices or XML files (CDA). These data can also be either static data or dynamic data. Static data are those that do not change much like patient’s name, address, height (for adults) etc. Dynamic data is more critical data like blood sugar level, level of oxygen in blood, blood pressure etc. [15]
Along with advantages, there are certain limitations of sharing data. Patients do not have access or control over the EHR after sharing and they do not get to know which unknown entities are using their data. As medical data contains lot of personal information, keeping it secure is very important.

4.2. Storage of Medical Data

As medical data cumulatively forms a huge bulk, cloud storage is mostly preferred due to its convenience. Cloud storage provides with a cost effective and virtually endless storage space with hindrance-free accessibility and fast transmission of data. With the invent of Mobile Cloud Computing (MCC) and its ability to fetch data from wearable medical devices, data can be analyzed very fast and timely reporting is possible [16]. The continuous flow of dynamic data can be accommodated in the storage system using several cloud environments like Amazon Web Services (AWS) or Google Cloud. The limitation with cloud storage is its data securing capabilities as dependency lies with third party service providers and unauthorized access of data cannot be avoided totally.

4.3. Securing Medical Data using Blockchain

Insecure medical data can be a loss of personal data to the patient and also can cause harm to a medical institute’s reputation and wealth. Blockchain can provide data security with its decentralized structure, applying cryptography and making data immutable. Consensus mechanism of blockchain can authorize the data requesting entity, securing the data from unauthorized access [14]. Also, the encrypted data will be meaningless to any intermediate entity except the data owner. Hacking and decrypting the data will be extremely difficult (almost impossible) owing to the complexity of blockchain technology [17]. The decentralized structure and use of smart contracts can also track the behaviour of the data elements and in case of any protocol violation, user access rights can be revoked [18].

5. Analysis

We have compared number of methods for securing healthcare data stored in cloud environment using blockchain technology. Table 1 contains a detailed comparison of those methods. Few methods used EHR as the input data source whereas few uses diagnostic images or reads input data from wearable medical devices or mobile devices. Majority of the methods are using Ethereum as the blockchain platform till date, but Hyperledger Fabric is slowly gaining popularity. Most of the methods using blockchain is also using cloud environment to store the data. Cloud platforms like AWS, Google cloud are preferred.

The methods we studied in this paper are all able to enhance data security by controlling access and stop unauthorized access using blockchain technology. Xia et al. [15] claimed that the proposed algorithm can keep track of the behaviour of the data and in case there is any protocol violation, the algorithm can revoke access rights for that data unit. This advancement can help keeping data secure as a continuous process. Kaur et al. [18] in their work could store both static and dynamic medical data in the blockchain, which is also a commendable advancement. But during data transmission, data loss due to leakage is a concern in this process.

**Table 1. Comparing Multiple Healthcare Data Management Methods Using Blockchain**

| Article | Input Data Format | Blockchain Platform | Other Technologies | Benefits | Drawbacks | Gap Identified |
|---------|------------------|---------------------|--------------------|----------|-----------|----------------|
| 13      | HER              | Ethereum            | AWS, IPFS          | Faster sharing of medical data over mobile cloud Can avoid | Not very scalable Poor network latency Compromised data privacy | Undefined |
| No. | HER | Ethereum | undefined | unauthorized data access while uploading |
|-----|-----|----------|-----------|------------------------------------------|
| 14  | Cloud Stored Medical Data | JMeter | Data access control | Higher data access communication cost |
|     | undefined | | Revoke data access on rule violation | The longer the data package, the more is the time cost to send transaction to blockchain |
| 15  | HER | undefined | undefined | Network Latency increases in proportion with number of requests from cloud service provider |
| 16  | HER | undefined | KSI, Jmeter | Data access cost compared to other existing solutions |
| 17  | Patient diagnostic data | ECC | Block ID generation cost is same for all input size | Interoperability among other medical stakeholders |
|     | undefined | | Successful privacy protection | Include techniques for key loss |
| 18  | HER | undefined | Cloud Environment | Securely stores heterogeneous data |
| 19  | Static and | Ethereum | AWS, Google Cloud | Divides input data into static |
|     | undefined | | | After the data transfer, any |
|     | | | | After the data |
dynamic personal health data and dynamic Data quality is maintained using machine learning data leakage while the data is stored or in use is out of scope.

| 20 | Medical Image | Custom-designed blocks | Undefined | Stronger data protection. Time taken does not depend on the number of keywords | Efficiency is slightly lower | Improved efficiency |

| 21 | Personal health data from wearable devices | Ethereum | Undefined | Improved efficiency | Transactions generated using simulators | Algorithm s to train the system for independent decision making in the real time Real transactions between devices |

| 22 | CDA Hyperledger Fabric XDS, FHIR | Secure immutable records Scalable | Undefined | Undefined |

6. Conclusion

Medical data volume is on a rise due to increase in the medical IoT devices and automation in the healthcare processes. Mostly these data are stored in form of EHR, EMR or diagnostic images. These data are extremely critical for timely treatment of the patient and also it contains personal and sensitive information of the patient. Due to the bulk, the data is mostly stored in cloud environments. Cloud is easy to access, virtually endless, always accessible, scalable and pocket-friendly; so, it has become the most convenient option for storing data. But cloud has security issues. To overcome this issue and keep the healthcare data safe from intruders, blockchain technology is used. Here we have studied few of the proposed solutions of recent times. The data security requirements are met, but the solutions have few limitations and gaps which require attention in the future.

References:
[1] M. Yannuzzi, R. Milito, R. Serral-Gracià, D. Montero and M. Nemirovsky, "Key ingredients in an IoT recipe: Fog Computing, Cloud computing, and more Fog Computing," 2014 IEEE 19th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Athens, 2014, pp. 325-329, doi: 10.1109/CAMAD.2014.7033259.

[2] A. Awad, A. Matthews, Y. Qiao and B. Lee, "Chaotic Searchable Encryption for Mobile Cloud Storage," in IEEE Transactions on Cloud Computing, vol. 6, no. 2, pp. 440-452, 1 April-June 2018

[3] N. Szabo, “Smart Contracts: Building Blocks for Digital Markets,” EXTROPY: The Journal of Transhumanist Thought, 1996.

[4] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”; http://bitcoin.org/bitcoin.pdf, 2008.

[5] D. K. Tosh, S. Shetty, X. Liang, C. A. Kamhoua, K. A. Kwiat and L. Njilla, "Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack," 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), Madrid, 2017, pp. 458-467, doi: 10.1109/CCGRID.2017.111.

[6] W. Zheng, Z. Zheng, X. Chen, K. Dai, P. Li and R. Chen, "NutBaaS: A Blockchain-as-a-Service Platform," in IEEE Access, vol. 7, pp. 134422-134433, 2019, doi: 10.1109/ACCESS.2019.2941905.

[7] Nakamoto, Satoshi. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Cryptography Mailing list at https://metzdowd.com.

[8] https://blockgeeks.com/guides/what-is-blockchain-technology/

[9] Mahrishi, M., Hiran, K. K., Meena, G., & Sharma, P. (2020). Machine Learning and Deep Learning in Real-Time Applications. IGI Global.

[10] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper 151.2014 (2014): 1-32.

[11] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacow Manevich, Srinivasan Muralidharan, Chet Murthy, Binh Nguyen, Manish Sethi, Gari Singh, Keith Smith, Alessandro Sorniotti, Chrysoula Stathakopoulou, Marko Vukolić, Sharon Weed Cocco, and Jason Yellick. 2018. Hyperledger fabric: a distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference (EuroSys '18). Association for Computing Machinery, New York, NY, USA, Article 30, 1–15. DOI:https://doi.org/10.1145/3190508.3190538

[12] Smith, Ben, and Konstantinos Christidis. "IBM Blockchain: An enterprise deployment of a distributed consensus-based transaction log." Proc. Fourth International IBM Cloud Academy Conference. 2016.

[13] D. C. Nguyen, P. N. Pathirana, M. Ding and A. Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems," in IEEE Access, vol. 7, pp. 66792-66806, 2019, doi: 10.1109/ACCESS.2019.2917555.

[14] Y. Wang, A. Zhang, P. Zhang and H. Wang, "Cloud-Assisted EHR Sharing With Security and Privacy Preservation via Consortium Blockchain," in IEEE Access, vol. 7, pp. 136704-136719, 2019, doi: 10.1109/ACCESS.2019.2943153.

[15] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du and M. Guizani, "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain," in IEEE Access, vol. 5, pp. 14757-14767, 2017, doi: 10.1109/ACCESS.2017.2730843.

[16] Nagasubramanian, Gayathri & Sakthivel, Rakesh & Patan, Rizwan & Gandomi, Amir & Muthuramalingam, Sankayya & Balamurugan, Balamurugan. (2018). Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Computing and Applications. 10.1007/s00521-018-3915-1.
[17] Omar, Abdullah & Bhuiyan, Md & Basu, Anirban & Kiyomoto, Shinsaku & Rahman, Shahriar. (2019). Privacy-friendly platform for healthcare data in cloud based on blockchain environment. Future Generation Computer Systems. 95C. 511-521. 10.1016/j.future.2018.12.044.

[18] Kaur, Harleen & Alam, Afshar & Jameel, Roshan & Mourya, Ashish & Chang, Victor. (2018). A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment. Journal of Medical Systems. 42. 156. 10.1007/s10916-018-1007-5.

[19] X. Zheng, R. R. Mukkamala, R. Vatrapu and J. Ordieres-Mere, "Blockchain-based Personal Health Data Sharing System Using Cloud Storage," 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), Ostrava, 2018, pp. 1-6, doi: 10.1109/HealthCom.2018.8531125.

[20] Zhang, Yu-lei & Wen, Long & Zhang, Yong-jie & Wang, Cai-fen. (2020). Deniably authenticated searchable encryption scheme based on Blockchain for medical image data sharing. Multimedia Tools and Applications. 10.1007/s11042-020-09213-w.

[21] Akkaoui, Raifa & Hei, Xiaojun & Cheng, Wenging. (2020). EdgeMediChain: A Hybrid Edge Blockchain-Based Framework for Health Data Exchange. IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.3003575.

[22] Margheri, Andrea & Masi, Massimiliano & Miladi, Abdallah & Sassone, V. & Rosenzweig, Jason. (2020). Decentralised Provenance for Healthcare Data. International Journal of Medical Informatics. 141. 104197. 10.1016/j.ijmedinf.2020.104197.