A Secure Framework for Health Record Management Using Blockchain in Cloud Environment

G Verma†, N Pathak‡, N. Sharma§

1†School of Computing, DIT University, Dehradun, INDIA, garimaverma.research@gmail.com
2‡Department of Information Technology, Bhagwan Parshuram Institute of Technology (BPIT), GGSIPU, Delhi, India. nitishforyou@gmail.com
3§Department of Computer Science and Engineering, Maharaja Agrasen Institute of Technology (MAIT), GGSIPU, Delhi, India, sharmaneelam2@gmail.com

*garimaverma.research@gmail.com

Abstract. Health records of any type should be confidential, but simultaneously they should be accessible to an authorized user. In the current conventional health care system, health records are processed in the local database. Only authorized hospital staff can have access to the patient health records kept in health centers. The flow of information in this kind of system is center-restricted. One technology that can potentially overcome this problem is Blockchain. Blockchain technology allows sharing of data in a distributed way with benefits like privacy-preserving and secure access control. To achieve secure access control and privacy of electronic healthcare data (EHD), a secure framework for distributed sharing of the health record is proposed. The use of blockchain will remove the requirement of a trusted 3rd party for data storage. The framework uses searchable key attribute-based encryption (ABE) for achieving fine-grain access control. The simulation results indicate that our scheme is quite effective and secure.

Keywords: Blockchain, Electronic health data, Attributed-based encryption, Security, Access control.

1. Introduction

With the fast and smart improvement of technology, most medical organizations such as hospitals, insurance companies are switching to electronic systems for the management of health records [1], [2]. This system generates huge medical data every day such as the medical history of the patient, lab test reports, medical prescriptions, etc. To decrease the patient cost and increase the hospital service quality, has gradually become the most concerning and important topic of research [3], [4]. The electronic management of medical information has carried a new challenge for hospitals and different medical institutions. The main challenge is centralized data management, which generates a concern of security, privacy, and access control [3], [5]. When the data is centrally managed and control by a particular hospital or medical institution there is always a problem in record transferring to other medical institutes. The use of EHD can help stakeholders to access medical records anywhere anytime [5]. Let’s, take a scenario if the patient has some medical history and was living in “A” city. Now if he is shifted to some other city “B”, he has to carry all the medical documents to the doctors of city B.
with the help of EHD can be stored electronically and whenever it is required to access can be accessed by the authorized user (Doctor, Patient or Hospital authority, etc.) But generally, the concept of EHD is implemented by some medical institutions, and it is not meant for data sharing.

The establishment of this kind of data center needs a very high cost of construction and professional information technology (IT) support. Cloud storage can provide a solution for this problem of cost and infrastructure. Cloud also provides the large storage, fast information transmission, and sharing property of anywhere anytime in a dynamic environment. Up to a very much extent, this solves the problem of remote data accessing and data sharing between different medical institutions. Also, remote institutions or doctors of different departments can provide the combined diagnosis to the patients. But the main problem with using cloud storage technology is trust and security issues. It is built on an untrusted network which raises various issues. Therefore it is required to handle EHD in such a way so it should be distributed, incorruptible, accessing to any authorized stakeholder, can be updated dynamically and changes should be accessible by all stakeholders of the EHD, no incompatibility issues, and finally, the patient should have full control on his data for ensuring privacy [6], [7], [8].

For addressing all the issues we have introduced a secure framework for health record management using blockchain. The above-discussed issues can be handled by blockchain as it provides the feature of auditing, immutability in records, and we can formalized contracts for accessing data [8]. Also, the framework will use ABE for providing fine-grained access control.

1.1. Our Contribution
- In this work we have analysed the some existing schemes [9], [10], [11], [12], [13], [14].
- Use of searchable keyword ABE for storing and retrieving medical records
- We have used blockchain technology to ensure no tempering of medical record.
- The system will provide the concept of interoperability between hospitals and other departments by the use of distributed ledger.

2. Related Work

To improvise the medical services and reduce the cost and effort of the patient treatment the electronic health record system is very important [11]. The robust healthcare system based on blockchain is discussed in [12]. The use of EHD can give lots of advantages such as – sharing of information, sharing of advice, tracking of disease, analysis of patient history, etc. The issue of security and privacy blocks the sharing of EHD to some extent. In the last few years, researchers are giving more attention to the security and privacy issue of EHD [11].

In 2019 [13], proposed a model called SEHRTB, that provides the (Electronic Health Record) EHR sharing between patients, doctors, service providers, and different medical institutions. The system gives the reduction in latency but there was no estimation of feasibility of the system given. In [14] they presented a system based on blockchain technology for the management of patient data. For maintaining the pseudonymity authors have used Elliptic curve cryptography (ECC). But the problem with the scheme was the issue of interoperability was not addressed.

In 2019 [15] proposed a secure model for healthcare management. The model used Ethereum blockchain for the management of distributed ledger and applied symmetric encryption technique to achieve security at the time of data access.

In 2020 [17], proposed a model of health data sharing scheme. The model was based on blockchain with the technology of proxy re-encryption. The use of proxy re-encryption ensures that the involved institutions in the model can decrypt the intermediate ciphertext. The scheme ensures confidentiality but the problem is no optimization of the process of implementation is given.

In 2019 [16,18], proposed a model for secure sharing EHR which combines the Interplanetary file system (IPFS) and blockchain technology. The model uses an access control mechanism using the Ethereum smart contracts. The model achieved the reliable and fast sharing of data using the mobile app but it requires the efficient management of EHR of the cloud.

3. System Model

The model is divided into two phases – storing of EHD and accessing of EHD. There are various types of entities are there in the model. Hospitals, Key generation center (KGC), Patient, Medical Institutes, blockchain, smart
contracts. The system model diagram is shown in Fig. 1. The steps of the working of different phases describes in Algo-1.

Algorithm-1 Steps of working

1. KGC starts the setup() phase. It takes security parameters as input and will generate the master key \( M_k \).
2. KGC also starts the keygeneration() phases, which generates the secret keys for hospitals, patients, and doctors as per requirements- \( S_k \).
3. Encryption is done by the patient by using Encryption(M, param, Pk), for generating the ciphertext, CT.
4. The authorization letter from KGC and the CT received by the hospitals for data sharing permission.
5. The hospital selects specific keywords from the original EHD data (such as – reported, adhar card no, data of birth, etc.), uses SHA256 as the key (K), generates \( k^i \) of the patient and encrypts the data by using encryption algorithm and then calculate the hash value.
6. The \( \{h_{data}, H_{addr}, \phi\} \) stored in blockchain and all the transactions will be stored in smart contracts.
7. The decryption of the document data will be done by entities Patient and Medical institutes, and doctors.
8. Every CU has its secret attribute key, and as per the access policy, the CU and CO can obtain the decrypted document.

End

3.1. Entities

**KGC** - generates system parameters and will deploy the smart contract. It also assigns attribute keys to the hospitals, patients, etc. KGC is also responsible to sends the respective secret key of the hospitals, patients, and doctors as per requirements.

It chooses \( p, G, G_T, g, g_1 \), and \( e \). In this \( p \) is a prime number, \( G \), and \( G_T \) are two multiplicative cyclic groups of order \( p \), \( g \) is a generator, \( e \) is a bilinear map and \( g_1 \) is a generator of \( G_1 \). Two random exponent values \( \alpha, \beta \in \mathbb{Z}_p \) and \( H, H_1, \) and \( H_2 \) are cryptographic hash functions, where \( H: \{0,1\}^* \rightarrow G, \ H_1: \{0,1\}^* \rightarrow G_1, \) and \( H_2: \{0,1\}^l \rightarrow G_2 \) (\( l \) means the minimum number of shares).

Mater Key \( M_k(\beta, g^\alpha) \)

Public key \( P_k = (g, g_1, H, w) , w = (g, g)^\alpha \)

Public parameters \( \text{param} = (p, G, g_1, G_2, g, g_1, H, H_1, H_2, \alpha, \beta, e, l) \).

\( S_k = (D = g^{(\alpha+r)/\beta}, \forall j \in A_i : D_j = g^{r_i \cdot H(j)}, D_j = g^{r_j}) \), where \( r \) is a random number. \( r, r_j \in \mathbb{Z}_p \) for the given attribute string \( A_i \).

**Patient** - Encryption is done by Patient, which uses an attribute access tree, plain text EHD, parameters, public key etc. to generate the cipher text (CT). The CT and authorization letter will be send to the hospitals from patient to authorize for data sharing.

Hospital- Hospital is responsible to upload the index of smart contracts. It uses cloud storage for storing ciphertext and uploads the transactions to make sure the credibility of data. The hospital selects specific keywords from the original EHD data (such as – reported, adhar card no, data of birth, etc.), uses SHA256 as the key (K), generates \( k^i \) of the patient and encrypts the data by using encryption algorithm and then calculate the hash value.

\( h_{data} = \text{SHA(data)} \). The CT and Ethereum transaction key will be stored by hospital in the cloud, and returns \( H_{addr} \) as a hash address. The \( \{h_{data}, H_{addr}, \phi\} \) stored in blockchain and all the transactions will be stored in smart contracts.
Keyword search- After the index and transaction ID uploaded on the cloud the Patient and other medical institutions can search required EHD by using keywords search. The Hospital selects $K_s$ as search key and stores encrypted keywords $\{kw_1, kw_2, kw_3, \ldots, kw_n\}$ in smart contracts. $F$ is a function that is used to calculate the tokens for searching the keywords in the smart contracts. $F = \{kw_1 || kw_2 || kw_3 || \ldots || kw_n\}$. Whenever the token is passed by the medical institutions, doctors, or Patient to the smart contracts the ID and location of the satisfied set are returned as a result.

Decryption of EHD- the decryption of the document data can be done by two entities Patient and Medical institutes, doctors, etc. Every CU has its secret attribute key, and as per the access policy, the CU and CO can obtain the decrypted document.

Validation of tempering of data- In view to verify the tempering of the original data the Patient or Doctors or medical institutes finds the $h_{data}$ from the Ethereum transaction ID and then recalculate the $h_{data} = SHA256(data_{received})$ and then compares both hash values if equal means data is not tempered else tempered.

![Fig. 1 System Model.](image)

4. Implementation and Performance Analysis

To estimate the performance of our scheme, we simulated all experiments on Intel (R) Core(TM) 10th generation i7-8750H CPU @ 2.20GHz 2.21 GHz, with RAM 4GB, using Ubuntu 14.04 LTS virtual machine.

4.1. Simulation

We have used the Ethereum test network using solidity language for the creation of a smart contract. The initial price of Gas was set to 9Gwei ($1Gwei=10^{-9}$ ether (ETH)). For testing purposes, personal data is being used for experiment and performance analysis. All the experiments are executed in a single threaded way. We implemented the system model on the blockchain environment using Ethereum TestRpc. This provides a simulated environment on the local system. The AWS cloud we have used as a medical cloud. The 120 W. power consumption is used. The efficacy of the proposed model is being compared with some existing state-of-art schemes [11], and [15].

4.2. Discussion

The plot in Fig. 2 shows the number of transactions and time taken for mining of new record. The figure shows very clearly that as the number of transaction increase the time also increases. Such as the scheme proposed by [11] takes approximate 870s for the 900 transactions, while [15] takes approximate 80s. The comparison shows that the proposed scheme is performing better than the other two. Fig. 3. Shows the plot between the access of records and time taken by the system for existing records. Which are stored on the cloud with a transaction ID on
blockchain. The time taken for searching is quite proportional to the number of records. The proposed scheme shows an improvement in comparison to the other schemes. For example if we take number of 30, then time taken by [11] and [15] is 2.7ms and 2.0ms respectively, while our scheme takes 1.7ms, which is surely less in comparison to other schemes taken for consideration.

5. Conclusion

The proposed framework uses the blockchain for EHD management. It uses the AWS, Ethereum smart contract, and searchable ABE technique for providing secure data accessing and storing on the cloud. The main benefit of using the ABE cryptography technique is the documents can be open by only those users if their attributes satisfy the given conditions of access policy, which is defined by the patient. The use of blockchain ensures the security, traceability, and non-tempering properties while storing and accessing data. The use of smart contracts removes...
the requirement of a third party for recording the transactions and consensus. This scheme can achieve sharing of documents at a low cost with required safety and security. In the future, we will use a public dataset for testing the model. Also, for real-time data collection, some smart devices can be introduced and the model can also be used for other medical institutes such as insurance companies, surgical instrument companies, pharmacy companies, etc.

References

[1] Barrows Jr, R.C. and Clayton, P.D., 1996. Privacy, confidentiality, and electronic medical records. *Journal of the American medical informatics association*, 3(2), pp.139-148.

[2] Vest, J.R. and Gamm, L.D., 2010. Health information exchange: persistent challenges and new strategies. *Journal of the American Medical Informatics Association*, 17(3), pp.288-294.

[3] Walker, J., Pan, E., Johnston, D., Adler-Milstein, J., Bates, D.W. and Middleton, B., 2005. The Value of Health Care Information Exchange and Interoperability: There is a business case to be made for spending money on a fully standardized nationwide system. *Health affairs*, 24(Suppl1), pp.W5-10.

[4] Krist, A.H., Peele, E., Woolf, S.H., Rothemich, S.F., Loomis, J.F., Longo, D.R. and Kuzel, A.J., 2011. Designing a patient-centered personal health record to promote preventive care. *BMC medical informatics and decision making*, 11(1), pp.1-11.

[5] Akinyele, J.A., Pagano, M.W., Green, M.D., Lehmann, C.U., Peterson, Z.N. and Rubin, A.D., 2011, October. Securing electronic medical records using attribute-based encryption on mobile devices. In *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices* (pp. 75-86).

[6] Namasudra, S., Deka, G.C., Johri, P., Hosseinpour, M. and Gandomi, A.H., 2021. The revolution of blockchain: State-of-the-art and research challenges. *Archives of Computational Methods in Engineering*, 28(3), pp.1497-1515.

[7] Croman, K., Decker, C., Eyal, I., Gencer, A.E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E.G. and Song, D., 2016, February. On scaling decentralized blockchains. In *International conference on financial cryptography and data security* (pp. 106-125). Springer, Berlin, Heidelberg.

[8] Ekblaw, A., Azaria, A., Halamka, J.D. and Lippman, A., 2016, August. A Case Study for Blockchain in Healthcare:“MedRec” prototype for electronic health records and medical research data. In *Proceedings of IEEE open & big data conference* (Vol. 13, p. 13).

[9] Yan, H., Li, X. and Li, J., 2014, November. Secure personal health record system with attribute-based encryption in cloud computing. In *2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing* (pp. 329-332). IEEE.

[10] Mhatre, S. and Nimkar, A.V., 2019. Secure cloud-based federation for EHR using multi-authority ABE. In *Progress in Advanced Computing and Intelligent Engineering* (pp. 3-15). Springer, Singapore.

[11] Wang, H. and Song, Y., 2018. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. *Journal of medical systems*, 42(8), pp.1-9.

[12] Mubarakali, A., 2020. Healthcare services monitoring in cloud using secure and robust healthcare-based BLOCKCHAIN (SRHB) approach. *Mobile Networks and Applications*, 25(4), pp.1330-1337.

[13] Mubarakali, A., Bose, S.C., Srinivasan, K., Elsir, A. and Elsier, O., 2019. Design a secure and efficient health record transaction utilizing block chain (SEHRTB) algorithm for health record transaction in block chain. *Journal of Ambient Intelligence and Humanized Computing*, pp.1-9.

[14] Al Omar, A., Bhuiyan, M.Z.A., Basu, A., Kiyomoto, S. and Rahman, M.S., 2019. Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future generation computer systems*, 95, pp.511-521.

[15] Andola, N., Prakash, S., Venkatesan, S. and Verma, S., 2019, December. SHEMB: A secure approach for healthcare management system using blockchain. In *2019 IEEE Conference on Information and Communication Technology* (pp. 1-6). IEEE.
[16] Mayank Singh and Viranjay M. Srivastava, 2019. Implementing Architecture of Fog Computing for Healthcare Systems based on IoT. *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 8, no. 4c, pp. 23-27.

[17] Huang, H., Zhu, P., Xiao, F., Sun, X. and Huang, Q., 2020. A blockchain-based scheme for privacy-preserving and secure sharing of medical data. *Computers & Security*, 99, p.102010.

[18] Nguyen, D.C., Pathirana, P.N., Ding, M. and Seneviratne, A., 2019. Blockchain for secure EHRs sharing of mobile cloud based e-health systems. *IEEE access*, 7, pp.66792-66806.