MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data

Conference Paper · December 2017

DOI: 10.1007/978-3-319-72395-2_49

4 authors:

Abdullah Al Omar
University of Alberta
20 PUBLICATIONS **1,015** CITATIONS
SEE PROFILE

Shahriar Rahman
University of Liberal Arts Bangladesh (ULAB)
52 PUBLICATIONS **1,440** CITATIONS
SEE PROFILE

Anirban Basu
Hitachi, Ltd.
85 PUBLICATIONS **2,126** CITATIONS
SEE PROFILE

Shinsaku Kiyomoto
KDDI R&D Laboratories Inc.
272 PUBLICATIONS **2,789** CITATIONS
SEE PROFILE

MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data

Abdullah Al Omar[1(✉)], Mohammad Shahriar Rahman[2(✉)], Anirban Basu[3], and Shinsaku Kiyomoto[3]

[1] University of Asia Pacific, Dhaka, Bangladesh
omar.cs@uap-bd.edu
[2] University of Liberal Arts Bangladesh, Dhaka, Bangladesh
shahriar.rahman@ulab.edu.bd
[3] KDDI Research Inc., Fujimino, Japan
{basu,kiyomoto}@kddi-research.jp

Abstract. Healthcare data are grabbing the interest of cyber attackers in recent years. Annihilating consequences of healthcare data could be alleviated through decentralization. A peer to peer (P2P) network enables the property of decentralization, where different parties can store and run computation while keeping the sensitive health data private. Blockchain technology leverages decentralized or distributed process, which ensures the accountability and integrity of its use. This paper presents a patient centric healthcare data management system by using Blockchain as storage to attain privacy. Pseudonymity is ensured by using the cryptographic functions to protect patient's data.

Keywords: Blockchain · Decentralization · Healthcare data
Pseudonymity · Privacy · Security

1 Introduction

Healthcare and Information Technology have recently attracted a lot of works in an amalgamated manner, which bring a lot of changes in healthcare. These changes not only affect treatment process of the patient but also require a careful data processing. With data processing data security and privacy issues arise simultaneously, as healthcare is completely dependent on data for treatment. Privacy of health data refers to the fact that the data of individual patient will be processed privately or authorization will be needed to access the data. And security refers to the fact of keeping sensitive data safe from eavesdroppers as well as from the intruders.

In the process of healthcare data preservation authenticated parties get the access to store it into and retrieve it from the system. Interaction between patient and the system needs to be in a secured way. In this interaction a patient could lose imperative data due to lack of security, as there are a lot of intruders in the network to access these valuable personal data. But losing healthcare data may

G. Wang et al. (Eds.): SpaCCS 2017 Workshops, LNCS 10658, pp. 534–543, 2017.
https://doi.org/10.1007/978-3-319-72395-2_49

be proved very detrimental in some instances. By recent attacks on healthcare systems, different countries [2,3] had devastating data loss. These attacks could steal the sensitive personal health data successfully as those were kept in server without encryption. Cyber-attackers sometime intrude into the data preserving system and make personal private data insecure. Let's assume one scenario, where a patient keeps her data in any [1,4,5,14] electronic health record (EHR) system for preservation and also for further access. EHR systems help the patient to share personal data with the doctors or healthcare organizations. Suppose a patient is keeping her data in a system [1] where data being preserved with Blockchain. Personal data need to be shared with the system then the system will preserve it to the Blockchain. Accountability of data is system centric here. Sharing of the data with doctors or healthcare organizations will also be maintained by the systems, as a result the system will be responsible for patients personal data loss.

In our framework we resolve above discussed problems by storing the encrypted data in the system. If system loses control over the Blockchain the data will be safe as patient herself is accountable for it. Also data sharing is managed by the patient. By using cryptographic function with Blockchain technology our framework resolves the data preserving vulnerabilities. Our proposed framework addresses the aforementioned vulnerabilities related to data storage. However, data would be safe because our system will be holding the encrypted personal data and if the system gets attacked the stolen data will make no sense to the attackers as data would be encrypted. Such use of encryption will also help us to attain pseudonymity. Although there is no identifier for anonymized dataset [6] but it could be managed by encryption keys.

So **accountability**, **integrity**, **pseudonymity**, **security** and **privacy** of healthcare data must be maintained by the systems. Nowadays patients are loosing their interest in electronic health record systems as privacy and security are threatened in EHR systems. So integrity and accountability of EHR systems are also being questioned. Pseudonymity of patient is imperative as personal healthcare data are sensitive.

We briefly describe each of the security and privacy properties in the context of our system below.

- Pseudonymity: No entity will be able to identify any party of our system, even through data it will not be possible to identify any party.
- Privacy: Only registered parties will be able to interact with the system. Even Registered parties will not be able to get the private raw data of other party.
- Integrity: Only authenticated parties will be able to store private data.
- Accountability: Parties will hold their individual block-id without which no entity will be able to interact with that particular block.
- Security: Only encrypted data will be kept by the parties in the system which adds an extra level of security in our system.

1.1 Related Work

Some national level frameworks based on cloud for electronic medical system have been proposed in [4,5,9]. Patra et al. [9] proposed a model which is cloud-based dealing with patients private data. A system was built by Patra et al. to ensure cost effectiveness, and this national level information system was designed for rural areas where cost plays an immense role. Through the framework medical professionals and policy makers could serve the patients remotely with a cloud-based model which includes all the imperative data in a single cloud. The patients were encouraged to share their data in the cloud so that they could get the medical service from the professionals. Disease diagnosis and control could be possible by this remote treatment. Data collection and data delivery are the key points in symptom analysis. Rolim et al. [11] proposed a framework where the system processes data in the steps of data collection and data delivery. In this model sensors play the role of collector. The collector collects the data and sends directly to the system to store and work with this data further. Sensors are proposed to be attached with the medical equipment. These data would be accessed by the medical professionals. Yin et al. [15] introduced cloud based patient centric system. This model includes three layers: data collection layer, data management layer and data service layer. A Blockchain based access control manager for heath data for enhancing the interoperability was proposed in [7]. Their proposal involved the use of public Blockchain as an access control manager of health data which would be stored in off Blockchain mechanism.

Controllability and traceability are two key topics of privacy preserving systems. Xiao et al. [14] proposed a model which is based on Blockchain to help patients to own, control and share their personal data easily and securely with privacy preservation. This application based model also deals with Secure Multi-party Computing (MPC) and Indicator-Centric Schema (ICS). Simic et al. [12] showed a case study where the study concludes with the illustration of significant benefits of IoT and Blockchain in a combined manner. In their work the IoT devices are used as collectors of the private health data of the patient, and the real time data of patient could be saved in Blockchain. They also describe controllability and traceability capabilities of Blockchain. Scalability of the Blockchain in case of Big data has also been tested in their study. Ekblaw et al. [1] proposed a prototype named 'MedRec' which uses Blockchain as a backbone and tried to find the security issues solution for electronic health records (EHR). They tried to achieve integrity, authenticity, auditability and data sharing through Blockchain.

The backbone of our work is Blockchain. The pseudonymity of our secured mechanism lies on only cryptographic function that is to be used to encrypt the data. Blockchain technology is popular for its application in Bitcoin cryptocurrency [10], which is a public ledger to hold and maintain the transaction data and integrity [13]. One of the reasons for using Blockchain technology in cryptocurrency is its decentralized digital ledger property, which was presented by Nakamoto [8] in his Bitcoin cryptocurrency framework. Blockchain's data structure has been modeled by linearly sequenced blocks. Each block contains the

cryptographic hashes corresponding to the previous and current block to ensure continuity and immutability of the chain. Chaining mechanism ensures integrity of this secured data structure.

1.2 Our Contribution

Our platform returns the control of the patients' private data to themselves. The main idea of this work is to keep the sensitive health data on the Blockchain to attain accountability, integrity and security. Patients will have the overall control over those blocks where their data will be kept. Present healthcare systems lack in pseudonymity but our platform gives the pseudonymity of patients. 'MediBchain' will regain the interest of patients in this vulnerable circumstance of EHR systems and will retain accountability, integrity, pseudonymity, security and privacy which are being lost in EHR systems. Analyses of these attributes are discussed in Sect. 3.

Organization of the paper: The remainder of the paper is organized as follows: Sect. 2 describes the protocol model. In Sect. 3, we analyze the protocol formally. We give some concluding remarks in Sect. 4.

2 MediBchain Protocol

In this section we present the architectural as well as the design view of our mechanism. Table 1 describes the Notations that is used in this section.

Table 1. Terminology table

Notation	Description
ID	ID of the User
PWD	Password of the user
U_D	Encrypted user data
U_{id}	Block number, where user data will be saved
ID_X	ID of the User X
PWD_X	Password of the user X
U_{DX}	User X's Encrypted data
U_{idX}	Block number, where user X's data is saved

2.1 Overview of Our Protocol

Figure 1 shows the high level view of our platform. The following entities and their roles are described briefly here.

Data sender is the patient, who will send her personal health data to the system. Data sender plays the vital role in case of data preservation. It must be ensured that the data that would be sent to the system are not wrong. However,

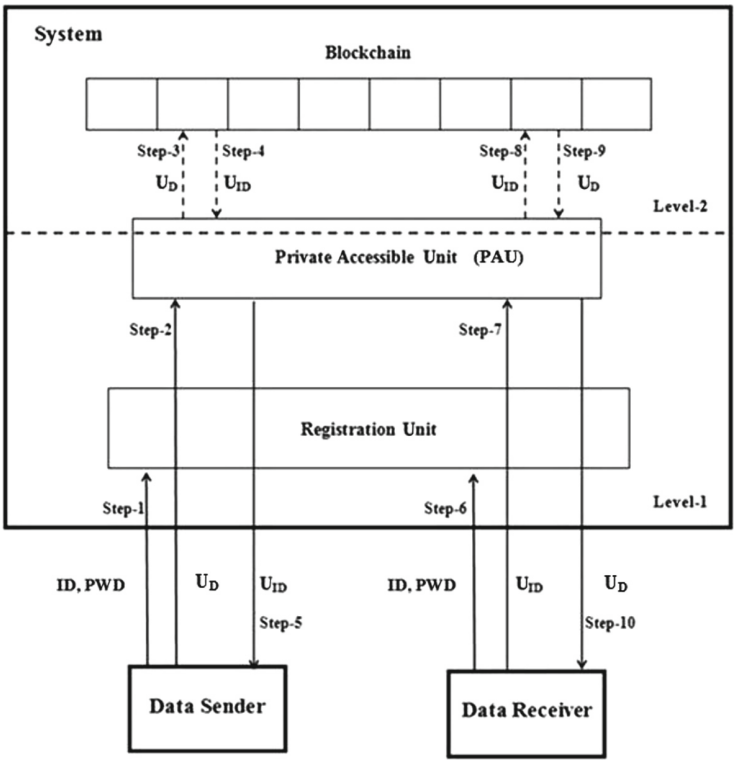

Fig. 1. High level view of this system.

our system will take the encrypted data from the user. Encryption of data will be done in user end.

Data receiver will request for the data after authenticating itself and accessing the system.

Registration Unit will act as an authenticator. When any party will come for the first time to take the service of the system; it will save their ID and PWD to be used further. Each party will have to register for once and need to preserve the ID and PWD. Further they just have to log in and access through secured channel for transaction of their private data.

Private Accessible Unit (PAU). Both the parties of the system will be able to interact with PAU after authentication. It needs a secured channel to interact with registration unit because through PAU they will send their data to the system. It is the intermediary unit of our system through which the element of one level could interact with the other.

Blockchain will hold the data of our users. Each transaction in the Blockchain will return an identifier. This transaction identifier will help the users to access the data further.

For better understanding our system is divided into two levels. Level-1 is Graphical User Interface (GUI). User will interact with our system through this level. Elements of level-1 are: Registration Unit and PAU. PAU is an important element of Level 1, as it interacts with both level 1 and 2. Level-2 is the backend of our system, which interacts with low level elements of this system through PAU. Element of level-2 is: Blockchain. Blockchain is being used as a repository of health data in our system. Our platform uses permissioned Blockchain which will require authentication to access.

Steps in the system: Steps of our system could be defined from Fig. 1.
Step-1: Data sender will request with the ID and PWD for accessing the system.
Step-2: Upon accessing the system in step-2, Data sender will send data to PAU for storing.
Step-3 & 4: Step 3 & 4 will take place in level-2 of our system, where PAU will send U_{ID} to Blockchain and it will return U_{ID} for future access to the Blockchain and also for finding the exact Block where the data were saved.
Step-5: In this step PAU will return the U_{ID} to the Data sender which was given by Blockchain.
Step-6: All the steps from this step onwards are related to Data receiver. As step-1, this step also requires sign in process. After this Data receiver can request for the data.
Step-7: In this step Data receiver will request for the data to PAU along with the U_{ID}. PAU will receive the U_{ID} for further use.
Step-8 & 9: Step 8 & 9 are same as step 3 & 4 but the data are not same for this steps. In step-8 PAU will request the Blockchain along with the U_{ID} and in Step-9 Blockchain returns it.
Step-10: This is the final step where PAU send the private data to the Data receiver.

2.2 Formal Description of Protocol

In this section we will define how Data sender, Data receiver, and our system work altogether in case of sending the data and receiving. For any kind of data transmission in our system, parties need to go through a step called registration. After confirmation of the Registration Unit that party can access the PAU.

Protocol Between Data Sender and System: Figure 2 shows the low level view of sending protocol. A patient will play the role of a data sender in this protocol. Data will be sent in encrypted form. These ciphertexts are generated from a function known as encryption function. *Enc(x,y)* is the function for encryption. Below we will see how this function works,

$$Enc(key, Data) = U_{\mathrm{D}} \tag{1}$$

By providing key and the health data to this function data sender will get U_{D} and will send it to the system. Public key encryption technique (e.g., Elliptic Curve Cryptography (ECC)) will be applied for encrypting private data.

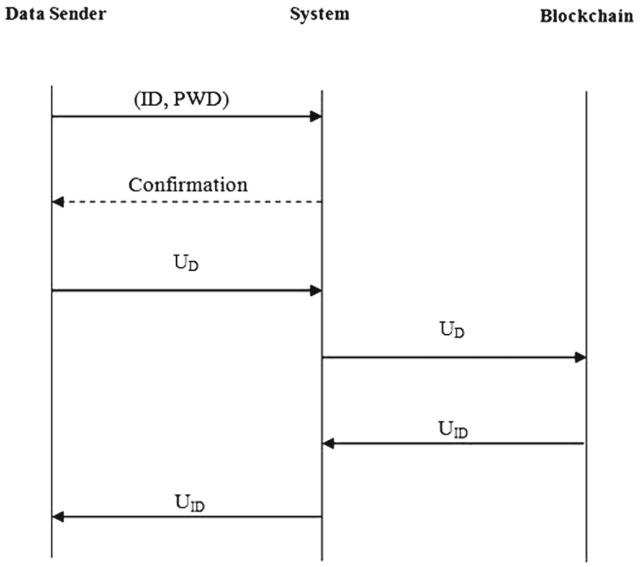

Fig. 2. Low level view of Sending Protocol

Suppose **X** is a Data sender of our system. At first X will request for getting into the system by providing the ID_X and PWD_X. Our system will send the confirmation to X if she provides the right ID and PWD. If X could sign in to the system properly and gets the confirmation then X will send U_{DX} to PAU through a secured channel. Secured channel will provide the security to X. In this stage PAU will interact with Blockchain. This interaction with the Blockchain will be done by the smart contract of our system.

Smart contract has been designed in such a way that Blockchain will return the number of the block. These block-ids will be used as U_{id} of a specific patient. Each time any patient will send a data through our system PAU will get the U_{id} for X it will be U_{idX}. PAU will send the U_{DX} to the Blockchain. Then Blockchain will return the special id for X that is U_{idX}. After that PAU will send the U_{idX} to X and end the protocol. X has to store this U_{idX} otherwise next time X will not be able to access personal data.

Getting the U_{idX} is the confirmation for Data sender X. Which means that the data has been kept to the system and then X could log out and end the secured channel transmission with the system.

Protocol Between Data Receiver and System: Receiving in our system will take two layers of authorization. Because after registering or signing into our system parties have to provide the U_{id} to get their data back through the secured channel. In the second phase if they fail to submit the U_{id} then they will not be able to access the data. U_{id} is the key to receive the actual data. It must be kept secured from sending phase. Figure 3 shows a low level view of receiving protocol.

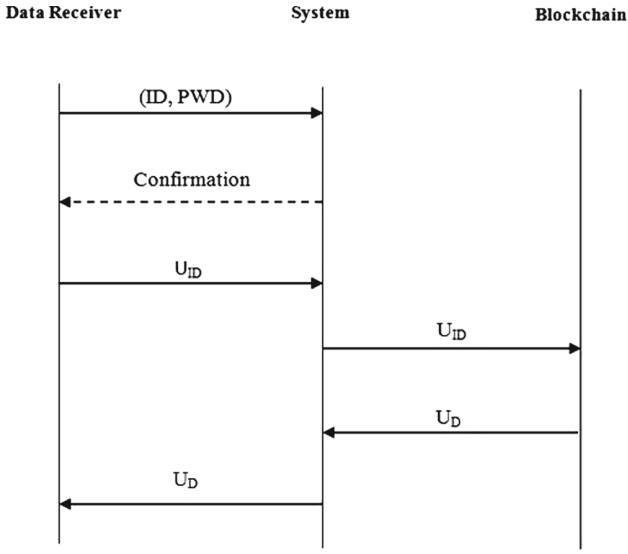

Fig. 3. Low level view of Receiving Protocol

Suppose user **X** wants to retrieve the data that has been kept in the system by X in the sending phase. As like sending phase this phase is also controlled by the authentication or Registration unit where X has to sign in first before accessing our system. This sign in required the ID and PWD of the user which was given in the registration phase. If X provides appropriate ID and PWD only then the system will send confirmation. After getting the confirmation X will be able to interact with the system through a secured channel. In this interaction with the system, X has to provide the U_{idX} that was given in sending phase. After getting the U_{idX} system will interact with Blockchain. This interaction will take place in level-2 of our system. Only PAU can interact with Blockchain, here the smart contract of our system will be the medium.

Smart contract will send the U_{idX} to Blockchain for retrieving the data of X from it. U_{idX} will be converted to the hash of that block in our designed smart contract. 256 bit hash of the corresponding block number will be checked in the smart contract, when the hash will be matched with any block then it will continue the process to retrieve the data. Otherwise this exception will be handled in our designed smart contract.

Suppose the hash of any block is,

`0xe3b1c14298fc1c149afbf4c8196fb92427ae41e4649b934ca495991b7852b811`

If the hash of U_{idX}'s corresponding block is same then X will be able to get data. For that purpose X needs to provide the correct U_{idX}. Blockchain will return the U_{DX} to X. By this returning function our system will end the session of data retrieval.

From the request X will have U_{DX} which has to be decrypted to get the actual data or plaintext. For decrypting user need to use *Dec(x,y)* function.

$$Dec(key, U_D) = plaintext \tag{2}$$

X will use Eq. 2 with key and U_{DX} to get the actual data that was encrypted by X in sending phase. ECC will be applied for decrypting.

3 Protocol Analysis

- **Pseudonymity:** Only encrypted data will be kept by the parties in our system, which will provide pseudonymity to them.
- **Privacy:** Registration Unit of our system will ensure the privacy of parties, and encrypted data will provide the privacy too.
- **Integrity:** Only authentic party's interaction will be ensured by the Registration Unit.
- **Accountability:** By using the Blockchain technology we attain accountability.
- **Security:** If the block-id of user is somehow been leaked the attacker won't be able to get the raw data as the data would be encrypted.

4 Conclusion

This paper presents a privacy preserving mechanism for the health care data. By analysis of the protocol we showed the strengths of this platform. The overall intention of this paper is to develop a distributed system and divert the web platform in a distributed manner for the patients. The concern over anonymity has also been addressed in this paper. In our future research we will deploy this whole system.

References

1. Ekblaw, A., Azaria, A., Halamka, J.D.: A case study for blockchain in Healthcare: MedRec prototype for electronic health records and medical research data. In: IEEE Open & Big Data Conference (2016)
2. FoxNewsHealth. 'Ransomware' Cyberattack Cripples Hospitals Across England. Associated Press, May 2017
3. Glaser, A.: U.S. hospitals have been hit by the global ransomware attack - Recode (2017). https://www.recode.net/2017/6/27/15881666/global-eu-cyber-attack-us-hackers-nsa-hospitals
4. Gul, O., Al-Qutayri, M., Yeun, C.Y.: Framework of a national level electronic health record system. In: Cloud Computing (2012)
5. Hendrick, E., Schooley, B., Gao, C.: CloudHealth: developing a reliable cloud platform for healthcare applications. In: IEEE 10th Consumer Communications and Networking Conference (CCNC) (2013)

6. Kiyomoto, S., Rahman, M.S., Basu, A.: On blockchain-based anonymized dataset distribution platform. In: 2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA) (2017)
7. Linn, L.A., Koo, M.B.: Blockchain for health data and its potential use in health it and health care related research. healthit.gov (2016)
8. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008)
9. Patra, M.R., Das, R.K., Padhy, R.P.: CRHIS: cloud based rural healthcare information system. In: Proceedings of the 6th International Conference on Theory and Practice of Electronic Governance (2012)
10. Raval, S.: Decentralized Applications: Harnessing Bitcoin's Blockchain Technology (2016)
11. Rolim, C.O., Koch, F.L., Westphall, C.B.: A cloud computing solution for patient's data collection in health care institutions. In: International Conference on eHealth, Telemedicine, and Social Medicine (2010)
12. Simic, M., Sladic, G., Milosavljević, B., et al.: A case study IoT and blockchain powered healthcare (2017)
13. Swan, M.: Blockchain: blueprint for a new economy (2015)
14. Yue, X., Wang, H., Jin, D., Li, M., Jiang, W.: Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. J. Med. Syst. **40**(10), 218 (2016). https://doi.org/10.1007/s10916-016-0574-6. ISSN 1573-689X
15. Zhang, Y., Qiu, M., Tsai, C.W., Hassan, M.M., Alamri, A.: Health-CPS: healthcare cyber-physical system assisted by cloud and big data. IEEE Syst. J. **11**(1), 88–95 (2017). https://doi.org/10.1109/JSYST.2015.2460747. ISSN 1932-8184