How Blockchain could Empower eHealth: an Application for Radiation Oncology

[Extended Abstract]

Alevtina Dubovitskaya[1,2], Zhigang Xu[3] Samuel Ryu[3], Michael Schumacher[1], and Fusheng Wang[4]

[1] University of Applied Sciences Western Switzerland (HES-SO), Sierre, VS, CH;
[2] École polytechnique fédérale de Lausanne (EPFL), Lausanne, VD, CH;
[3] Stony Brook Medicine, Stony Brook, NY, USA;
[4] Stony Brook University (SBU), Stony Brook, NY, USA

Abstract. Electronic medical records (EMRs) contain critical, highly sensitive private healthcare information, and need to be frequently shared among peers. Blockchain provides a shared, immutable and transparent history of all the transactions to build applications with trust, accountability and transparency. This provides a unique opportunity to develop a secure and trustable EMR data management and sharing system using blockchain. In this paper, we discuss our perspectives on blockchain based healthcare data management and present a prototype of a framework for managing and sharing EMR data for cancer patient care.

Keywords: eHealth, EMR, blockchain, radiation oncology

1 Introduction

Patient's healthcare data are often distributed among different actors of the Healthcare system. Patients need to share the data during the treatment, or for the purposes of medical research. Medical data are highly sensitive and when sharing or transferring them from one institution to another (for primary care and for research purposes), according to the legislation in Europe and USA a patient has to provide a consent where the access control policy is defined. Consents are usually not personalized standard forms, and it is not easy for the patient to express his access control policy. For example, when a patient wishes to receive an independent opinion about his condition from another medical doctor in the same medical institution, or prefers not to share some part of his medical history.

In case of the data aggregation for the research purposes, patients could be concerned about violation of their privacy and may not provide a consent to share their data as they are. An alternative to the consent collection is data anonymization. However, the privacy violation could happen in case of linking multiple datasets containing anonymized information about the same patient [6]. How to keep track of the shared information about the patient in a longterm perspective?

A patient with chronic disease or serious medical condition may need to keep track of his patient's record through his life, or may need to delegate the data management to his relatives due to the medical condition. Management of medical history, access control, prescriptions, medical expenses, insurance correspondence and payments is unavoidable notoriously time-consuming and bothersome for most of such patients. For example, treatment of a cancer patient may urgently require knowing the radiation dose received during the life-long treatment. Consent management and data transfer may delay a critical treatment. The goal of this work is to develop a framework that can be used by patients, medical doctors and other entities involved in healthcare processes for patient's data management. We present a solution that tackles the problems discussed above and ensures privacy, security, availability, and fine-grained access control over EMR data.

2 Potential applications of blockchain in eHealth

Background knowledge and related work. Blockchain – is a distributed ledger technology based on the principles of peer-to-peer network and cryptographic primitives (such as hash, asymmetric encryption and digital signature) [1]. Having access to a ledger - shared, immutable, and transparent history of all the actions (transactions) performed by participants of the network (such as a patient modifying permissions, a doctor, accessing or uploading new data, or sharing them for research) overcome the issues presented above. Based on how the identity of a user is defined within a network, one could distinguish between permissioned and permissionless blockchain systems. The potential of the applications built on top of the blockchain technology for healthcare data management has been recently discussed by researchers. MedRec is the first and the only functioning prototype that have been proposed recently [2]. Ariel et al. presented a system based on permissionless blockchain implementation. Our prototype presented further in this manuscript significantly differs from the framework in [2]. First, we have chosen to use a permissioned blockchian technology that provides better protection of the patient's privacy, do not involves transaction fees and "mining". Second, in [2] the patients data are stored locally at every node, which does not ensure availability of the data in case if the hospital node is temporary off-line.

Applications in eHealth. Blockchain provides a unique opportunity to support healthcare. Hereafter we discuss application of blockchain to support Connected health [4]. Sharing the ledger (using the permission-based approach) among entities (such as medical doctors, medical institutions, insurance companies and pharmacies) will facilitate medication and cost management for a patient, especially in case of chronic disease management. Providing pharmacies with accurately updated data about prescriptions will improve the logistics. Access to a common ledger would allow the transparency in the whole process of the treatment, from monitoring if a patient follows correctly the prescribed treatment, to facilitating communication with an insurance company regarding the costs of the treatment and medications. The network would be formed by the

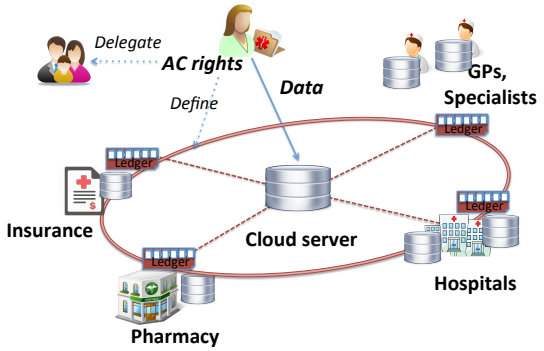

Fig. 1. Connecting different healthcare players for better patient care.

trusted peers. The peers will run consensus protocol and maintain a distributed ledger. The patient (or his relatives) will be able to access and manage the data through a web interface. The key management and the access control policy will be encoded in a chaincode, thus, ensuring data security and patients privacy.

In case of medical data aggregation for research purposes it is highly important to ensure that the sources of the data are trusted medical institutions and, therefore, the data are authentic. Using shared distributed ledger will provide tracebility and will guarantee patient's privacy as well as the transparency of the data aggregation process. Due to the current lack of appropriate mechanisms, patients are often unwilling to participate in data sharing. Using blockchain technology will facilitate the process of collecting patients data for research purposes.

3 Application in radiation oncology

We apply the blockchain technology to create a prototype of an oncology-specific clinical data sharing system. To present our solution, we take as an example an oncology information system, ARIA [5], which is widely used to facilitate oncology-specific comprehensive information and images management. ARIA combines radiation, medical and surgical oncology information and can assist clinicians to manage different kinds of medical data, develop oncology-specific care plans, and monitor radiation dose of patients.

Proposed framework. Hereafter we describe an architecture of the framework for radiation oncology data management. To develop a prototype we used Hyperledger Fabric – open source implementation of the permissioned blockchain technology [3]. Our architecture consist of a user interface and a backend that consists of the following components: membership service and certification authority, network of nodes (deployed in the medical institutions and connected to the database), load balancer to redirect a user to any of the trusted nodes in the network, separate cloud-based storages for patient's data and certificates.

Functionality of the prototype. The functionality of the prototype is the following. Patient can register in the system (via membership service), generate a secret key (AES), public/private key pair, receive a certificate from the certification authority. Then patient can login and create his record. In order to define access control policies he submits a transaction that will specify which doctor is able to access which type of the data within specified time interval. The patient could also upload the data to the cloud repository: after encrypting them with his own secret key and hashing to ensure the data integrity. The metadata will be stored on the blockchain: the transaction will contain the hash of the file, a URL of the file, id of the patient that uploaded the file. To provide an access to the data the patient's key has to be shared using the certificate of the doctor. A doctor also needs to register in the system and generate a public/private key pair and obtain a certificate from the certification authority. Similarly to the patients medical doctors are able to upload the data about the patient, access them but only based on the permissions specified by the patients.

4 Conclusion and Future Work

We proposed potential applications of blockchain technology in healthcare data management. Based on the requirements from medical perspective we implemented a prototype of a framework for data management and sharing in the oncology patient care. We are going to test our framework with the patients data in hospital environment. Extending metadata representations, adding new categories (e.g., images), evaluation and improvement of the user interfaces, introducing new actors (researchers, pharmacologists, insurances) are the next steps of our work. Using blockchain technology allows to ensure privacy, security, availability, and fine-grained access control over EMR data. The proposed work can significantly reduce the turnaround time for EMR sharing, improve decision making for medical care, and reduce the overall cost.

References

1. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system, 2008 [Internet]. Available from: https://bitcoin.org/bitcoin.pdf.
2. Azaria A, Ekblaw A, Vieira T, and Lippman A. Medrec: Using blockchain for medical data access and permission management. In *2016 2nd International Conference on Open and Big Data (OBD)*, pages 25–30, Aug 2016.
3. Cachin C. Architecture of the hyperledger blockchain fabric, 2016 [Internet].
4. Connected health [Internet]. Available from: https://en.wikipedia.org/.
5. ARIA Oncology Information System [Internet]. Varian Medical Systems [cited 9 March 2017]. Available from: https://www.varian.com/oncology/products/software/information-systems/aria-ois-radiation-oncology.
6. Baig MM, Li J, Liu J, and Wang H. (2011). Cloning for privacy protection in multiple independent data publications. *Proceedings of the 20th ACM international conference on Information and knowledge management - CIKM '11*, page 885.