Management of Case Wise Medical Record Using Block Chain

Pengshu

April 5, 2018

Medical devices in IoT generates sensitive information private to patients, such data requires permission management, and the content of data requires hiding. We use block chain technology to manage the permission to data, and apply one-time-key cryptography to protect the data privacy of patients. Upon such convenient and secure way of accessing medical data, we propose methods to break the data barrier between medical institutes and ethically share patient data for medical research.

1 The Problem Statement

It is difficult for patients in eastern Asia, especially China, to access their own medical data. Also, there is data barrier between medical institutes. Such nonavailability of medical data causes redundant examinations, jeopardizes the relationship between patients and medical workers, and is developing into a social problem.

In the light of IoT technology, it is possible that various medical devices joins a network to provide convenient medical data access for patients and medical institutes, immensely improving the data availability.

Note a point to bear in mind is, medical data contains sensitive personal information about patients, not everyone should have the permission to view any piece of medical data on the network. Medical data of a patient should only be accessible under the request of the patient himself or responsible medical workers. Block chain based solution to manage permission to medical databases has been put forward by Azaria et al.[1], and can be extended to managing data generated by IoT medical devices.

Another problem is leakage of medical data, which may occur during an attack on medical database or IoT medical devices. Statistics have shown that these event are not uncommon. IoT medical devices are particularly vulnerable due to limited computing power. Block chain itself is not enough for ensuring data security at the lower level of storage provider, as is clarified by Azaria et al.[1]. A solution which does not requires extensive computing power while keeps the data safe is favorable for IoT medical devices.

2 Existing Method of General Medical Record Management using Block Chain

Azaria et al.[1]implemented a system using block chain and smart contract to manage the access and permission off-chain medical data. In their model, the central identities involved are Provider and Patient, who collaborate to manage the medical data of Patient. Provider provides the physical storage space for the medical data of Patient, while Patient makes queries to the Provider in order to retrieve his/her medical data.

A private block chain is deployed in the system, Provider and Patient acts as nodes in the block chain network. There interaction between Provider and Patient on chain are achieved my manipulating 3 types of smart contracts.

1. The issuing of virtual ID to Providers and Patients is managed by **Registrar Contract**
2. The establishment of collaboration between Provider and Patient, and access verification to a certain piece of medical data is managed by **Provider-Patient-Relationship(PPR) Contract**
3. The activities of updating medical data, and querying medical data, is recorded and managed by **Summary Contract**

The medical data of Patient is stored in offchain database managed by Provider. Updating the medical record of Patient works as follows:

- Update of medical data of a particular Patient is received by Provider, say the doctor uploads the latest medication of Patient to Provider.
- Provider updates the entry for Patient in the offchain database.
- Provider resolves the Provider-Patient relationship onchain, and posts transactions on block chain to update the Summary Contract and PPR contract.
- The Summary Contract fires a signal to Patient, notifying the update.

Querying the medical record of Patient works as follows:

- Patient send a digitally signed query request to Provider, using an offchain communication channel.
- Provider checks onchain the accessibility of the sender of query request.
- If the sender of the query request has the permission level to access the query content, Provider retrieves the corresponding query content from offchain database, and return the content to Patient.

A few remarks to make:

NO medical data is stored on block chain in this model.

The block chain only manages the accessibility of users to medical data, , and the Patient-Provider-Relationship, in a highly secure way.

The actual medical data is stored offchain, the data format is only dependent on the structure of offchain database, therefore the content and formatting is not restricted.

The block chain CANNOT deal with information leakage from user end. Both Patient and Provider are responsible for the data admin in their local storage, and their offchain communication.

3 Case Wise Medical Data Management

We want to record in fine detail the treatment on Patient during a particular medical case, e.g. a cardiovascular operation.

We want the record to be always retrievable by Patient.

We want the record not temper-able once completed.

(The use of block chain is more like a log of treatment.)

The Patient should have their privacy over the record, the treatment log shall not be accessible to outsiders.

(So it is more likely to be a private block chain. It should be a private block chain for each medical case.)

We expect the doctor to update the log honestly, as frequent as possible.

References

[1] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman. 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.