LEGAL AND TECHNICAL CONSIDERATIONS FOR MEDICAL DATA IN HYBRID DATABASE SYSTEM

Olga Siedlecka-Lamch

Department of Computer Science, Czestochowa University of Technology (Poland)

olga.siedlecka@icis.pcz.pl

EXTENDED ABSTRACT

Collecting, storing, and exchanging medical information is an essential aspect of modern healthcare. Relational database systems are extensively used for managing medical data due to their scalability and ability to store structured information. With the advent of blockchain technology, however, a new perspective on the storage and management of medical data emerges (Azaria et al., 2016; Farouk et al., 2020; Linn et al., 2016; Shahnaz et al., 2019).

This article focuses on a hybrid database model that integrates the benefits of relational data storage with the characteristics of blockchain technology. Particular attention will be paid to the legal facets of medical data and the ensuing technical challenges, such as ensuring the right to be forgotten (Rosen, 2011).

Important consideration must be given to the fact that data stored in a blockchain is, in theory, immutable. Existing legal regulations, such as the "right to be forgotten," continue to pose a challenge for medical system providers, who must guarantee the ability to delete data when necessary. In the remainder of the article, we will discuss techniques and strategies that can be effectively implemented in hybrid medical databases to address this issue.

In addition, we will investigate additional legal issues pertaining to medical data, such as privacy protection, compliance with data protection regulations, and controlled data sharing. In addition, we will investigate the technical aspects of implementing hybrid medical databases that facilitate effective data management and legal compliance.

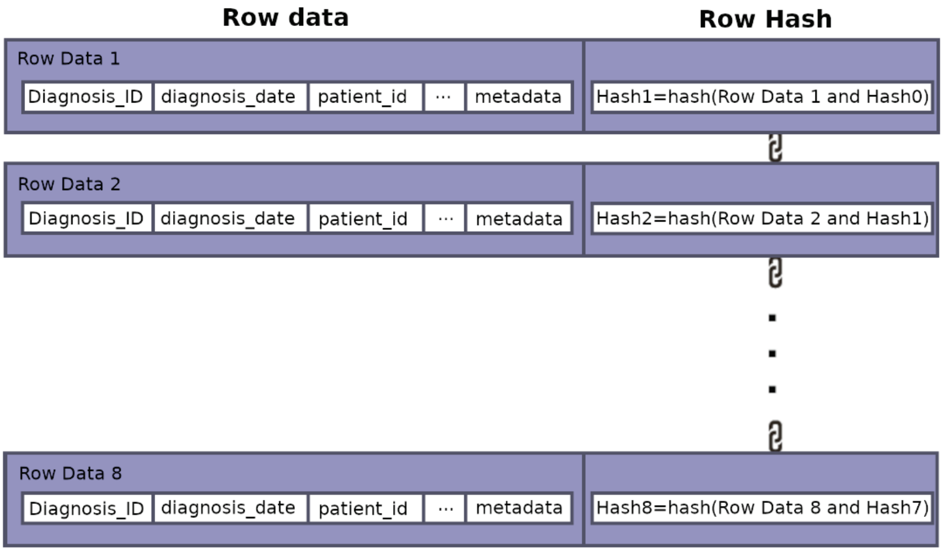
By delving into these issues, this article intends to provide readers with an understanding of the issues surrounding medical databases employing a hybrid model and guidance on the technical solutions that can be utilised to effectively manage medical data and meet legal requirements.

Hybrid model

Numerous researchers have been actively investigating the use of blockchain technology to store medical data for several years. The works of Azaria et al., 2016, Aguiar et al. 2020, Farouk et al., 2020, Linn et al., 2016, Shahnaz et al., 2019, and Yaqoob contain different approaches. Our solution is particularly novel because it enables many medical facilities to leverage existing relational systems by moving sensitive data portions to blockchain tables. This method ensures the immutability of diagnostic and treatment process events without incurring excessive costs associated with transforming entire systems or training staff. The addition of blockchain tables can be incorporated seamlessly, remaining imperceptible to end users and preserving the existing database logic.

We included patient information, medical staff information, visit history, medical leave records, test results, diagnoses, referrals, prescribed medications, disease codes, and their respective categories in our model. The treatment process-related data (test results, diagnoses, prescribed medications) should be stored in a blockchain tables (for example diagnosis table in Figure 1). This will result in an immutable, observable, and easily analysed sequence of events generated by each medical device. It will also be accessible to the patient, but only physicians with the appropriate certificates assigned to their profiles will be able to make changes.

Figure 1. Blockchain table for diagnosis information.



Source: self-elaboration based on Oracle documentation

Obviously, blockchain technology has both benefits and drawbacks, making it difficult to apply it to the entirety of the data (scalability issues, security concerns, certain elements being excessively transparent while others are inaccessible). This is why a combination of technologies can be a highly effective solution, as it combines the advantages of modern innovations with completely functional systems. In the case of our model, achieving legal conformance is the remaining obstacle.

Right to be forgotten

The right to be forgotten is a legal concept that allows individuals to request the removal of their personal information from organisations that acquire and process it. This is especially pertinent in the context of medical data, where the privacy and confidentiality of patient information is essential.

The General Data Protection Regulation (GDPR), which became effective in 2018, has strengthened the right to be forgotten in the European Union. Individuals have the right to request the deletion of their personal data under the GDPR if there are no longer any legal grounds for processing it, if the data is being processed in violation of regulations, or if the individual has revoked their consent for data processing.

Data immutability is the primary characteristic of a blockchain, which means that once transactions are added, they cannot be expunged or altered. In the context of the right to be forgotten and the erasure of medical records, there are a number of methods to overcome this obstacle. Here are some strategies to consider:

- Medical data can be stored off-chain, such as in external file systems or databases, while only the hashes or references to that data are stored in the blockchain. Thus, when the need to expunge the data arises, only the references in the blockchain can be updated or removed without compromising the blockchain's integrity.
- Smart contracts and special functions: Certain blockchains allow for the creation of smart contracts and special functions that supervise access to medical data. It is possible to implement mechanisms that enable controlled data deletion or restrict access to only authorised parties.
- The addition of an intermediary layer between the interface and the blockchain is also a viable alternative. This layer enables access control and administration of medical data, including deletion based on the fulfilment of certain conditions.
- Data anonymization: Instead of deleting data directly, identifying information can be removed using anonymization techniques. Thus, the data remains in the blockchain, but cannot be associated with particular individuals.

The first three techniques involve adding additional structures around blockchains. Storing the actual data off-chain raises the most concerns, as the purpose of putting them in a blockchain is to ensure their immutability. Placing them off-chain introduces the possibility of making changes and only complicates the structure. Smart contracts and special functions entail additional expenses, turning simple modifications into complex software solutions. The use of an intermediary layer has the same drawbacks—complexity, cost, and the potential loss of some advantages offered by the proposed solution. What seems to be the most reasonable approach for the hybrid model is data anonymization.

In this article, we examine a method for erasing patient data involving the encryption of identifying information and the ability to delete encryption keys. In addition to the aforementioned techniques, we will investigate the potential of blockchain tables that permit the eradication of particular information after an established amount of time and under specific conditions (subject to having the appropriate certificates).

Experiments

The database implementation phase utilised the Oracle server version 21c capabilities, including the blockchain table mechanism. The model has been implemented and populated with sample data. The anonymization process was tested through key deletion and direct deletion of partial data from the blockchain tables.

KEYWORDS: Healthcare hybrid database; Blockchains; Legal requirements for healthcare databases; Data Security.

REFERENCES

Azaria, A., Ekblaw, A., Vieira, T. , and Lippman, A. (2016). “Medrec: Using blockchain for medical data access and permission management,” in 2016 2nd international conference on open and big data (OBD). IEEE, 2016, pp. 25–30.

De Aguiar, E. J. , Faiçal, B. S., Krishnamachari, B. and Ueyama, J., (2020) “A survey of blockchain-based strategies for healthcare,” ACM Computing Surveys (CSUR), vol. 53, no. 2, pp. 1–27.

Farouk, A., Alahmadi, A., Ghose, S., and Mashatan, A., (2020) “Blockchain platform for industrial healthcare: Vision and future opportunities,” Computer Communications, vol. 154, pp. 223–235.

European Parliament and Council of the European Union. Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04

Linn, L. A., Koo, M. B. et al.,(2016) “Blockchain for health data and its potential use in health it and health care related research,” in ONC/NIST use of blockchain for healthcare and research workshop. Gaithersburg, Maryland, United States: ONC/NIST, pp. 1–10.

Rosen, J. (2011). The right to be forgotten. *Stan. L. Rev. Online*, *64*, 88.

Shahnaz, A., Qamar, U., and Khalid, A.,(2019) “Using blockchain for electronic health records,” IEEE access, vol. 7, pp. 147 782–147 795.

Yaqoob, I. ,Salah, K. Jayaraman, R. and Al-Hammadi, Y.,(2022) “Blockchain for healthcare data management: opportunities, challenges, and future recommendations,” Neural Computing and Applications, vol. 34, no. 14, pp. 11 475–11 490.