Healthcare Data Management Using Blockchain: MyHealthMyData (MHMD) and PharmaLedger

Galia Kondova[1], Amala Arockia[2]

1 School of Business, University of Applied Sciences and Arts Northwestern Switzerland FHNW, 4002 Basel, Switzerland

2 School of Life Sciences, University of Applied Sciences and Arts Northwestern Switzerland FHNW, 4132 Muttenz, Switzerland

ABSTRACT

Healthcare data is important in the development of new medicines as well as in disease prevention and health promotion. At the same time, there are significant barriers to sharing health data mainly due to privacy issues. Blockchain as a technology characterized by immutability, traceability, decentralization, and cryptographic security might provide feasible solutions to tackling challenges such as security concerns, data format inconsistency between health data providers, and data breaches caused by unauthorized access. International projects such as MyHealthMyData and PharmaLedger provide blockchain-based solutions addressing the privacy preserving issues associated with health data management. This paper provides an overview of the proposed innovative solutions of the two projects.

Keywords: eHealth, Digital Health, Data Management, Blockchain, Data Privacy, PharmaLedger, MyHealthMyData

INTRODUCTION

Healthcare data is crucial in the process of discovering new medicines and testing their safety and effectiveness in clinical trials. Healthcare data is a collection of data related to a patient's health collected from different resources. It includes health and treatment histories, symptoms, lifestyle choices, biometric data, etc. The digital storage of health data is also referred to as the Electronic Health Record (EHR).
At the same time, there are constraints to having health data readily available mainly due to privacy issues. MyHealthMyData and PharmaLedger are two projects that apply blockchain-based solutions to address privacy preserving issues associated with health data management. These two solutions are the focus of this paper.

Electronic Health Record (EHR)

Healthcare data could be stored in a physical or a digital format. The physical storage which includes papers and books faces requirements such as large storage spaces and a cumbersome retrieval of data. To overcome these issues, the healthcare industry has implemented the Electronic Health Record (EHR). EHR is associated with an enhancement of the safety of processing patient information by reducing mistakes and expanding data access (Yang and Li, 2018). EHR can be shared among various stakeholders facilitated by digital technologies in the health care system. Major stakeholders include hospitals, health professionals, insurance companies, health administrators, laboratories, and researchers. Hospitals could use the health data to assess and improve the quality of their services. Insurance companies could use the health data to develop new products and investigate potential fraud. Researchers study diseases, illness causes and symptoms by using health data. EHR data is also used for clinical research, health promotions, clinical audit, clinical governance, planning future services and national statistics etc. (Shah and Khan, 2020). EHR, being a central repository of hospitals, creates, transmits, and receives electronic documents using standard terminologies such as Continuity of Care Document (CCD) and Continuity of Care Record (CCR). This standardization enables connectivity and interoperability among authorized healthcare providers.

Health Information Exchanges (HIE)

The electronic exchange of health data among authorized healthcare providers takes place through Health Information Exchanges (HIE) (Ibrahim and Singhal, 2016). There are many varieties of HIEs such as regional, statewide, nationwide and vendor-to-vendor. HIE help facilitate care coordination, avoid repeating tests and procedures, move the burden of relaying medical histories from the patient to providers, and ensure that healthcare providers have more complete information. There are three forms of HIE, namely directed exchange, query-based exchange, and consumer mediated exchange (Ibrahim and Singhal, 2016). Table 1 presents an overview of the three forms of HIE.

Table 1: Forms of Health Information Exchange

(Patel et al., 2011)

Directed Exchange	Healthcare providers could send and receive information such as laboratory results, patient referrals, and discharge summaries to other healthcare providers over the internet. Also used for sending immunization data to public health organizations.
Query-based Exchange	Healthcare providers could find and request information on a patient from other providers. Often used for emergency care.
Consumer-mediated Exchange	Patients have the possibility to aggregate and manage their health information on the internet. Patients can transfer information between providers and track and monitor their own health data.

There are four common methods health organizations use to send and receive health data through a HIE:

- Transmission control protocol (TCP): TCP over Virtual Private Network (VPN). It allows computers to communicate over a secure private network and provides end-to-end connectivity. This is the interoperable way to exchange health data through a HIE. Health organizations can connect to a public HIE over VPN using an integration engine.
- Secured web services: HIE members send and receive patient data through secure communications over the internet. Using the secured web services, the HIE data is updated in real time based on trigger events.
- Secured File Transfer Protocol (FTP): Organizations can send patient data in batches, or one document at a time via secured FTP.
- Secure E-mail: Secure email is the direct transmission of patient data among HIE data provider. It is called the push method of HIE because the owner of the information pushes the data to another location (Lyniate, 2021).

However, there are some challenges to using HIE across organizations. These challenges include security concerns, data format inconsistency between health data providers, and data breaches caused by unauthorized access. Optimized processes in terms of security protocols, privacy configurations, electronic consent, and governance are on the agenda for further enhancing EHR interoperability. Blockchain as a technology characterized by immutability, traceability, decentralization, and cryptographic security might provide feasible solutions to tackling the above-mentioned challenges.

Blockchain

Blockchain combines a ledger with a peer-to-peer distribution, producing a decentralized, irreversible, and transparent history of transactions. The technology behind blockchain essentially aggregates data into blocks, which are sequentially added together to create a chain of data. The decentralized, distributed system means there is no central database vulnerable to manipulation. The existence of

multiple copies enhances the immutability characteristics. Blockchain also utilizes security keys for encryption, which can be further applied to verify users and create digital signatures.
There could be different blockchain applications to enable the creation of digitalized healthcare ecosystem for patients and healthcare service providers (HSP). These include privacy preserving platforms, medical data exchanges, mobile application architectures, record management systems, and data sharing networks (Zubaydi et al., 2019). The necessary requirements for these applications are interoperability, security, transparency, privacy, and cost effectiveness (Zubaydi et al., 2019).

Quantum Computing and Blockchain

The blockchain technology relies on the security of cryptography. In particular, the blockchain depends on two cryptographic primitives called hash functions and public key cryptography. These primitives are used to verify the unity of data and to check the ownership of data.
Every block in a blockchain includes a hash code to the previous block to avoid any modification of a block by attackers. A new entry to a block is done by verification of the data ownership through the public key cryptography. In the process of public key cryptography, a person signs data with their private key to create a signature and publishes this signature with public key. These cryptographic primitives are one-way functions. This means that it is not possible to access the private key through the public key nor the hash function input through the output (Rodenburg and Pappas, 2017).
The security of current cryptography is put under threat as quantum computers become more powerful. Quantum computers use quantum bits – qubits, which allow for an extremely fast performance. The fast computation power then threatens the security of the current encryption approaches. In particular, quantum algorithms such as Shor's algorithm and Grover`s algorithm pose a significant threat to blockchain. Shor's algorithm allows an attacker to break public key cryptography and thus blockchain digital signatures. Grover's algorithm provides a speedup when testing various inputs to a function, which can be used to reverse hash functions (Rodenburg and Pappas, 2017).
At the same time, the quantum computing threats could be counterbalanced through post-quantum cryptography and quantum-based cryptography. The most mature technology of quantum-based cryptography is Quantum Key Distribution to encrypt a secret message.

DATA PROTECTION AND PRIVACY PRESERVATION SOLUTIONS

Healthcare data is personal data and thus falls under the EU's General Data Protection Regulation (GDPR). Hence data security and privacy preservation should be addressed in every step of the data processing flow (Kondova, 2021).

The privacy preserving approaches of two EU Horizon 2020 projects in healthcare data management deserve special attention. These projects applying blockchain technology are MyHealthMyData (MHMD) and PharmaLedger.

MyHealthMyData (MHMD)

The MHMD project (MyHealthMyData, 2022) proposes a solution for a GDPR-compliant storage of sensitive personal data. In that model the private data is always stored in the data controller's facility and not on the blockchain. In permissioned blockchain, organizations define the policies for its access control layer for the various users.

Every organization in the healthcare ecosystem in MHMD runs at least one node in the blockchain network. Users communicate and interact with the system through the web server. Web server has the information related to user's authentication. It will not hold any sensitive data. Users' authentication information like username, password and organization is validated by the web server with the corresponding organization. The central web server is there to facilitate the interaction with the system and with the central catalogue (Koscina et al., 2019).

There is one local catalogue at every data controller. Local catalogues index the data from the data sources. Indexation process includes the generation of metadata from the actual data and the registration of metadata in the central catalogue. The indexation process ensures anonymization of the data so that the type of data is searchable on the central catalogue but not their owners.

Every organization has its own Certificate Authority (CA) with an API and a second API with the web server to handle the authentication of the users. Single sign on process is carried by the web server with the help of authentication API and connects CA API to perform the right mapping between user's credentials and public keys. Data exchange flows are enabled by smart contracts.

PharmaLedger

PharmaLedger aims to create a blockchain-based platform validated through use cases in supply chain, clinical trials and health data. Electronic Product Information (ePI) leaflet is the first pilot use case out of total eight use cases. ePI would enable the switch from paper to digital medicine information leaflets. The blockchain-based platform will facilitate the creation of trusted and secure content by the manufacturers, enable transparent and immutable review and approval of transaction records, facilitate trusted transactions between stakeholders, and allow interoperability with other digitally enabled services and systems (PharmaLedger, 2022).

In the case of the ePI use case, the user scans the GS1 Datamatrix Code (2D data matrix code) on the drug package from a phone application, and through a "resolver" on the blockchain the right eLeaflet is delivered to the user. Blockchain enables access to the eLeaflet and ensures that the eLeaflet data is correct, up to date, and authentic. This is made possible due to the decentralized and tamper-proof nature of blockchain as well as the deployment of smart contracts on it.

The technology based on distributed ledger technology/blockchain that is deployed in PharmaLedger is the OpenDSU (Open Data Sharing Units) (OpenDSU, 2021). Under the OpenDSU concept data subjects (individuals/patients

and companies/healthcare services providers) control their confidential data via smart wallets (digital wallets). The smart wallet manages data access and gives consent to Data Processors for accessing the confidential data stored in a secure container called DSU (Data Sharing Unit). Thus, the DSU contains data and code and is cryptographically secured and anchored in the blockchain. In addition, OpenDSU is blockchain agnostic, i.e., it supports any kind of programmable blockchain technology. Moreover, OpenDSU supports any kind of Self Sovereign Identities as well.

CONCLUSION

Healthcare data, being personal data, falls under the EU's General Data Protection Regulation (GDPR). Hence data security and privacy preservation rules should be in place along the data processing flow. The characteristics of blockchain technology such as decentralization and cryptographic security enable privacy preserving management of healthcare data especially around identity and access management. Two existing blockchain-based solutions for GDPR-compliant healthcare data management include MyHealthMyData and PharmaLedger that are briefly presented in this paper.
The discussed quantum computing threat to cryptographic security used in the blockchain technology could be counterbalanced through the advancement of post-quantum cryptography and quantum-based cryptography.

REFERENCES

Ibrahim, A., Singhal, M. (2016). A Simultaneous Key Generation Technique for Health Information Exchange (HIE) Based on Existing Patients' Credentials, in: Proceedings - 2016 IEEE 1st International Conference on Connected Health: Applications, Systems and Engineering Technologies, CHASE 2016. Institute of Electrical and Electronics Engineers Inc., 359–361.

Kondova, G. (2021). Blockchain-Based Healthcare Data Management: Current Practices and Opportunities Ahead. In: Kalra J., Lightner N.J., Taiar R. (eds) Advances in Human Factors and Ergonomics in Healthcare and Medical Devices. AHFE 2021. Lecture Notes in Networks and Systems, vol 263, 199–202.

Koscina, M., Manset, D., Negri, C., Kempner, O.P. (2019). Enabling trust in healthcare data exchange with a federated blockchain-based architecture. Proceedings - 2019 IEEE/WIC/ACM International Conference on Web Intelligence Workshops, WI 2019 Companion 231–237.

Lyniate. (October 24, 2021). FHIR: Shaping the Future of Health Data Exchange. Website: https://lyniate.com/resources/fhir-shaping-the-future-of-health-data-exchange/

MyHealthMyData. (January 14, 2022). MyHealthMyData. Website: http://www.myhealthmydata.eu/

OpenDSU. (October 23, 2021). Open DSU. Website: https://opendsu.com

Patel, V., Abramson, E. L., Edwards, A., Malhotra, S., & Kaushal, R. (2011). Physicians' potential use and preferences related to health information exchange. International Journal of Medical Informatics, 80(3), 171-180.

PharmaLedger. (January 14, 2022). Pharma Ledger. Website: https://pharma-ledger.eu

Rodenburg, B., Pappas, S.P. (2017). Blockchain and Quantum Computing. MITRE Technical Report. https://doi.org/10.13140/RG.2.2.29449.13923

Shah, S.M., Khan, R.A. (2020). Secondary Use of Electronic Health Record: Opportunities and Challenges. IEEE Access 8, 136947–136965.

Yang, G., Li, C. (2018). A design of blockchain-based architecture for the security of electronic health record (EHR) systems, in: Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom. IEEE Computer Society, 261–265.

Zubaydi, H.D., Chong, Y.-W., Ko, K., Hanshi, S.M., Karuppayah, S. (2019). A Review on the Role of Blockchain Technology in the Healthcare Domain. Electronics (8), 679.