Reference Model for Health Data Security Management Supported in a Blockchain Platform

Walter Espíritu[1[0000-0001-7952-2132]], Christian Machuca[1[0000-0003-2265-5625]], Daniel Subauste[1[0000-0003-1131-1384]]

[1]Universidad Peruana de Ciencias Aplicadas, Lima, Peru

{u201213869, u201214881}@upc.edu.pe

daniel.subauste@upc.pe

Abstract. Several problems in health care come from the complex network of intermediaries. Currently, medical health data is fragmented and isolated, there are communication delays and workflow tools are different due to lack of interoperability, which negatively affects research and health services. For these reasons, health entities and their patients need to securely protect their data. However, for the privacy of patients, the danger of having such information on the network and due to the vulnerability of traditional authentication systems, a reference model is proposed to manage the health data security based on Blockchain. Blockchain allows access to complete medical records that are stored in fragmented systems anonymously and securely. Our reference model uses the concepts of an information security management system such as: policies, risks and controls. This allow private or public entities in the health sector to implement Blockchain. On the other hand, our reference model was developed by researching and comparing existing Blockchain platforms in the health sector, with the purpose of guiding qualified information security personnel when they decide to implement Blockchain in a health sector organization.

Keywords: Reference Model, Blockchain, Healthcare, Data Management, ISMS.

1 Introduction

The health industry is one of the largest industries in the world, since it consumes more than 10% of the gross domestic product (GDP) of the most economically developed countries with a high standard of living [1]. In addition, the process of allowing the exchange of data between multiple parties, although it is beneficial for the patient, still lacks transparency and control. Patients have expressed concern about the possibility of their medical data being used by for-profit entities [1]. Patient data is dispersed in different entities of the health industry known as data silos; data sharing is prone to a multilevel permit control process [1]. Because of this, many times, crucial data is not accessible and is not available at the time of an emergency.

Blockchain can solve this problem with the exchange of health information by acting as a secure decentralized database. Blockchain is a revolutionary technology that can help solve the challenges of medical care by providing security and trust. Access to a patient's medical history can be enabled for all health care providers prior to patient registration and authorization. The access control system in Blockchain puts patients in control of their data; consent and access rights may be granted to third parties to a subset of your medical records. It is possible to write custom laws and agreements through smart contracts which are equivalent to real-world contracts [2].

Smart contracts can be used in various processes within medical care, including billing and insurance, which helps automate the process and reduce costs. To unify the compression of Blockchain technology and its security, a reference model is proposed that allows us to provide a series of controls based on possible risks that may occur within the Blockchain platform and affect the privacy of patient health data. For this reason, we investigate the different Blockchain platforms for the health sector where it was decided what properties we consider for our analysis. We will use the information collected and analyze the similarities and differences between the platforms.

2 Literature Review

2.1 Research protocol

This research is carried out from the perspective of health care to build our reference model and, therefore, we are considering the following property. Platforms: We are considering Blockchain technology implementations that introduce different approaches to privacy and smart contracts [2].

- Public Blockchain: All records are visible to the user and everyone can participate in the consensus process [3].
- Private Blockchain: It has centralized permission for a governing organization [3].

2.2 Selected Blockchain platforms

Blockchain technology platforms can be divided into two groups, as illustrated in Table 1. For our study, we have selected a Blockchain platform from each group.

They can be characterized as follows:

Table 1. Types of Blockchain (Platforms)

Public	MediChain	MediBloc
Private	Patientory	Medicalchain

MediChain: It is a Blockchain solution for the storage and distribution of medical data that allows patients to have control over their own medical information [7].

- Advantage: It allows the exchange of medical records between the patient and their doctor, as well as research institutions protecting the confidentiality and security of the data.
- Disadvantage: It is open source and does not offer a backup system in case of data loss, it does not allow to work with pharmaceutical entities.

MediBloc: It is the combination of a social need with a technological enabler, it is a system that prioritizes patient data, providing a transparent and accessible view of the medical history [6].

- Advantage: It is associated with the use of "smart contracts", which allow the exchange of information through an intermediary who oversees executing complex transactions.
- Disadvantage: It is a network without permission and the user pays a 10% commission when exchanging their health information.

Patientory: It is a distributed application based on Cybersecurity Blockchain that provides users with access to their health data. Creates smart contracts that can be executed in relation to the continuous cycle of medical and patient care. Centralize all patient medical data in one place to manage, share and track medical care [4].

- Advantage: It helps healthcare organizations create personalized smart contracts for those healthcare organizations that adopt and use the Patientory Blockchain network.
- Disadvantage: It works as a private network and is not open source, uses proprietary algorithms and does not allow modifications to the source code.

Medicalchain: It allows doctors, hospitals, laboratories, pharmacists and health insurers to request permission to access a patient's record-to-record transactions in a distributed ledger [5].

- Advantages: Provides the patient with full access and control over their data, ability to provide different levels of access to various users, assigning a set of access permissions and designating who can consult and write data on their Blockchain.
- Disadvantage: It is a private Blockchain that is not open source and does not allow external developers to show their applications within the ecosystem.

3 Theoretical Foundation

3.1 Reference model:

Reference models are reusable representations of abstract knowledge for a given application domain. Also, they are relevant representations for a purpose of an information system designed through a construction process. They provide a useful means to reduce the information modeling effort. They are developed with the objective of being reused for different scenarios of similar applications and are used as a starting point for the construction of specific project models [8].

3.2 Blockchain:

It is one of the technologies behind Bitcoin, an open peer-to-peer value transfer network (p2p). Cryptocurrencies are analogous to money currencies such as the USD or the EUR that facilitate the exchange of value but use cryptographic protocols as the basis of governance instead of relying on a central authority such as banks [9]. In Blockchain, a transaction represents a change of state. When a new transaction is created, it is transmitted to the network where a mining node (computer) collects the transaction and composes a block by combining one or more transactions and broadcasts the block to the network [10].

3.3 Smart contracts:

A smart contract represents a piece of self-executing, self-verifiable and tamper-resistant code with a programmable programming application logic that resides and runs on Blockchain [3]. Formalizes transaction rules and relationships between entities and assets in Blockchain and provides the flexibility to write the logic of the custom application that becomes a law imposed by the Blockchain itself without relying on trusted intermediaries [11]. As an example, Ethereum it is a platform based on smart contracts [12].

3.4 Health data management:

The management of health data that includes storage, access control and data exchange is an important aspect of the health industry. Proper management of health data improves results and allows a comprehensive view of patients, personalized treatments and efficient communication. Confidence problems and lack of profit incentives are the main obstacles to the exchange of health data [13]. Blockchain technology can solve both problems by acting as a layer of trust, introducing profit mechanisms such as tokens (digital assets) that are used as a reward [12]. With the Blockchain incentive and trust structure enabled, there is a promise of a global health information exchange [12]. However, by establishing a series of guidelines focused on an information security management system based on ISO / IEC 27799: 2016, the exchange of health data will be safer compared to the traditional process of medical history of a health entity.

4 Case Study

4.1 Organization:

The model was implemented in a clinic specialized in providing health care services for institutions and companies (public or private), has a large team of specialized professionals, with extensive experience in health and medicine. The local clinic did not carry out risk management on a continuous basis, due to the time it may require and because it did not have a specialized information security staff to carry it out.

4.2 Implementation:

The implementation of the reference model is carried out in the medical history registration process, since it is the central process of the clinic, in which all information related to this must be protected. The selected work team is composed of the process owner, the head and coordinator of the systems area, as well as the authors of this article.

Phase 1: Validation of the risk matrix: We need the clinic information and IT information as inputs. Following our proposed model, in phase 1, for the traditional scenario, ten risks were found, classifying them as two High risks, eight Medium risks and zero Low risks. This meant that there are certain deficiencies on the part of the systems area, as they did not contemplate such risks that could affect the integrity of the clinic. Once the traditional system scenario has been analyzed, the risk matrix prepared based on the analysis that was made using the Ethereum platform consisting of a decentralized Blockchain is shown, finding a series of risks that could occur outside the Blockchain where a total was found. Of 11 risks classifying them as 0 High risks, 8 Medium risks and 3 Low risks.

This means that there is still a risk on users who have to adapt to use this technology, since within the Blockchain the information is secure; the problem comes when it is outside of this. Finally, the risk exposure of the traditional system is compared to a scenario using Blockchain technology. For this, a heat map was made where the codes of the risks found are placed and classified according to the result obtained.

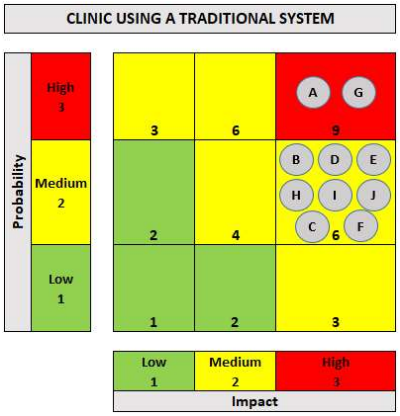

Fig. 1. Heat Map - Traditional System.

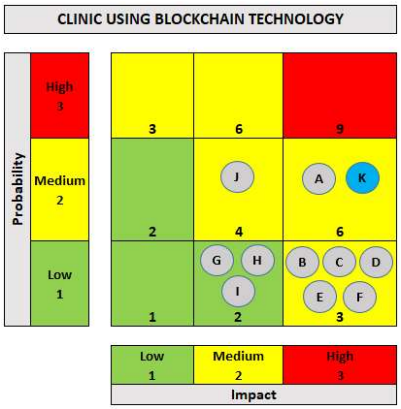

Fig. 2. Heat Map - Using Blockchain Technology.

The results obtained were calculated based on the sum of the metrics of the risks found and classified on the maximum metric (90). Obtaining a risk level of 67% (Fig. 1.) in a traditional system scenario and 41% (Fig. 2.) in a scenario where Blockchain technology is used. concluding that there is a higher risk exposure in a traditional system, while using Blockchain technology the risk exposure is reduced by 26%.

Phase 2: SoA Validation (Statement of Applicability): Once the results of the assessment of the identified risks have been obtained, the SoA template is used as a reference for the implementation of information protection measures, as well as to verify that no necessary security measures are being set aside.

They had not been considered inside the clinic. Next, we will see the results obtained in the traditional system scenario where the validation of this document was carried out.

It can be seen that the vast majority of the sections of controls their level of compliance is below 20%, which indicates that there is a large breach of information security quite exposed. The average result obtained gives us 11% compliance, this means that there are no controls established within the clinic to ensure and protect the information of their patients against cyber-attacks.

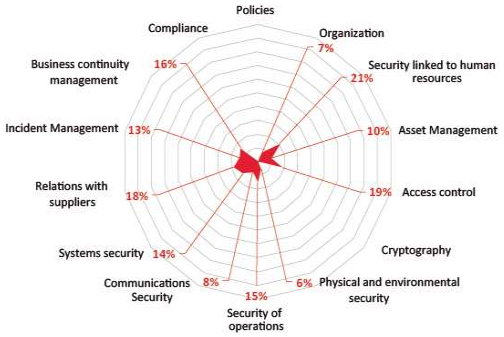

Fig. 3. SoA Matrix - Traditional System.

Once the results on compliance with SoA document controls were analyzed, the same controls were validated, but this time on stage using Blockchain technology. Next, we will see the results obtained using Blockchain technology in any health sector organization.

Most controls meet more than 20% of the criteria necessary to carry out proper management information security. As well, the average result obtained gives us a total of 44% compliance, this means that when using Blockchain technology, the controls established within the clinic are more robust and meet the criteria necessary to carry out a correct management of information security, in order to guarantee and protect patient information against possible attacks.

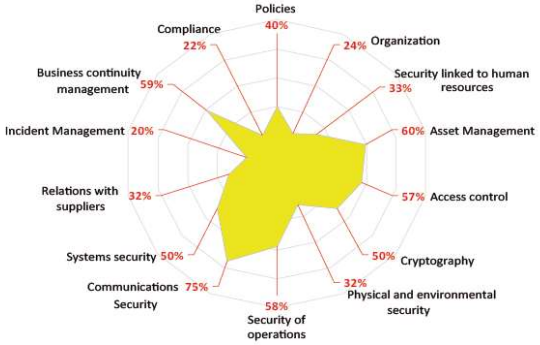

Fig. 4. SoA Matrix - Blockchain Technology.

Once the analysis of both scenarios is completed, a graph is prepared with the results obtained to make a comparison and see the compliance status for each of the sections proposed in the SoA template. The results obtained indicate that there is a 33% improvement in overall compliance when using Blockchain technology compared to a clinic with a traditional system.

Phase 3: Validation of asset inventory: The inventory of information assets was measured by the criticality obtained by its final classification level where the confidentiality presented 9 high level, 16 medium level and 0 low level. On the part of the integrity, 6 of high level, 11 of medium level and 8 of low level were presented. Finally, I present 5 high level, 16 medium level and 4 low level availability.

Finally, together with the total distribution by the classification of the levels and turning it into a percentage, the following results were obtained: High Level = 32%, Medium Level = 52%, Low Level = 16%. With these results we can conclude that the highest percentage of classification is given by the average level, which indicates that the information assets are mostly of medium to high importance for the clinic where the classification of the inventory of information assets.

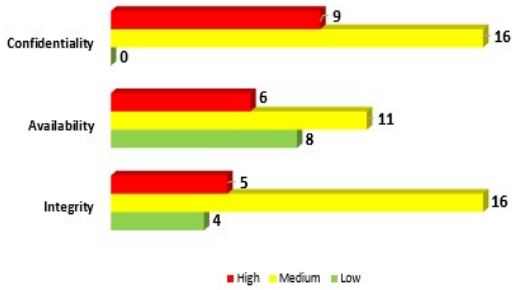

Fig. 5. Classification of Assets.

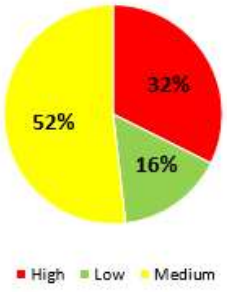

Fig. 6. Total Distribution by Classification.

5 Conclusions

The model was validated at a local clinic (Lima, Peru) and compared in a simulation scenario using Blockchain technology. In the results of the implementation of the model, it is observed that the level of risks would be reduced by 26%, compliance with the controls would increase by 33% when the proposed controls are applied in a scenario with Blockchain.

The proposed reference model will allow knowing the status of compliance with policies and controls based on the ISO / IEC 27799: 2016 standard of any health center. Based on the results obtained, the clinic was shown that it is ideal to have knowledge about its risks, controls and assets that are the most critical and to consider a risk analysis to make decisions about the safety of each of them.

With the implementation of the reference model, the health centers will have a detailed vision about the possible risks that could occur, avoiding legal problems such as lawsuits imposed by patients or financial sanctions by the regulatory entity.

The costs of implementing mitigating controls are high compared to using a Blockchain technology that mostly minimizes security breaches. When using Blockchain technology, a new risk appears which is: the use of the private key, consider that if a

user loses their private key, they automatically lose all their information stored in the Blockchain.

Our future plans regarding the research carried out is to be able to help hospitals and clinics to choose the best Blockchain platform alternative, since at the end of the day migrating the medical information of their patients to Blockchain will be a reality in the future that benefit the health sector.

References

1. Gajendra J. Katuwal, Sandip Pandey, Mark Hennessey and Bishal Lamichhane. Applications of Blockchain in Healthcare: Current Landscape & Challenges, December 10, 2018.
2. Chibuzor Udokwu, Aleksandr Kormiltsyn, Kondwani Thangalimodzi, Alex Norta. The State of the Art for Blockchain-Enabled Smart-Contract Applications in the Organization, November 8, 2018.
3. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE International Congress on Big Data (BigData Congress) (pp. 557-564). IEEE.
4. Chrissa Mcfarlane, Michael Beer, Jesse Brown, and Nelson Prendergast. Patientory - Whitepaper. (May):1–19, 2017.
5. Medicalchain Whitepaper 2.1, 2018(accessed November 6, 2018). https://medicalchain.com/MedicalchainWhitepaper-EN.pdf.
6. Allen Wookyun Kho and Eunsol Lee. Medibloc – Whitepaper. (March): 1-15, 2018.
7. Rouhani, S., Butterworth, L., Simmons, A. D., Humphery, D. G., & Deters, R. (2018, July). MediChain TM: A Secure Decentralized Medical Data Asset Management System. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 1533-1538). IEEE.
8. Jorg Becker and Patrick Delfmann. Reference Modeling: Efficient Information Systems Design Through Reuse of Information Models, July 14, 2007.
9. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.
10. Beck, R., Stenum Czepluch, J., Lollike, N., & Malone, S. (2016). Blockchain–the gateway to trust-free cryptographic transactions.
11. Yang, Z., Yang, K., Lei, L., Zheng, K., & Leung, V. C. (2018). Blockchain-based decentralized trust management in vehicular networks. IEEE Internet of Things Journal, 6(2), 1495-1505.
12. Tikhomirov, S. (2017, October). Ethereum: state of knowledge and research perspectives. In International Symposium on Foundations and Practice of Security (pp. 206-221). Springer, Cham.
13. Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways; found healthcare intelligence on blockchain with novel privacy risk control. Journal of medical systems, 40(10), 218.