



Distributed Network for Health Diagnosis Using Blockchain for Early Analysis and Detection of Health Aliments

Sunil Balakrishnan¹, Rama Parvathy L²

¹Research Scholar, ²Professor

Department of Computer Science and Engineering, Saveetha School of Engineering,
Saveetha Institute of Medical and Technical Sciences, Chennai

*Corresponding Author E-mail: ¹sunilvihar@gmail.com, ²ramaparvathyl.sse@saveetha.com

Abstract

Information technology plays very important role in the healthcare sector and as new technology are introduced the potential of those technologies are tried out to see how better the healthcare sector could get advantage of these new technologies. From the time of internet age, the healthcare sector has undergone massive changes and with new technologies like Cloud Computing has brought enormous possibilities in having Personal Health Record (PHR) management. One of such latest technology which has been successfully tested and getting introduced is Blockchain. The growing interest in utilizing this technology into Health Sector especially for PHR due to its disturbed network model and the security design it has embedded in it.

Keywords: Blockchain, PHR (Personal Health Record), PHI (Personal Health Information) Cloud Computing, Security

1. Introduction

Blockchain first introduced by [1] and was used for crypto currency. Blockchain uses open ledger methodology where the data is stored in the form of blocks. Blockchain uses a P2P network model instead of standalone which helps in creating a distributed data set for the same data, the data is stored as data blocks whenever there a new transaction is recorded. These transactions are updated in the ledger books of all the participating organizations in the network without need of a centralized control. Any minute changes in the existing data blocks are recorded and gets updated in all the ledgers of the participating organization leaving a trail of transactions. This enables improved security features and leaving audit trail for transaction monitoring.

Current model of PHR is managed by individual hospitals or third party organization based on proprietary technology or based on standalone database. This has led to having multiple records of Personal Health Information (PHI) in various organization with no historical details available for the same individual. There has been lot of traction to this with the introduction of Blockchain methodology. The potential of such technology has been adopted and tried out as new model like OmniPHR [2]. However, these approaches do not address issues of how PHI could be used in early diagnosis of health alignments or such captured information could be used in clinical research without compromising the individual's identification.

This paper proposes a new approach to advance model of system using the Blockchain methodology to address the requirements of health professionals and clinical research requirements without compromising the individual's identity as laid out by HIPAA in Research Repositories, Databases and the HIPAA Privacy Rule [3][4]. A covered entity may de-identify PHI in one of the two ways.

The first way is "safe-harbor" approach method, by removing all 18 identifiers captured under section 164.51(b)(2) of the regulations. A set of data that has been de-regulated for the 18 identifiers, then an entity could not identify an individual unless the entity uses the de-regulated information along with other information to identification.

The second method is to have qualified statistician determining the usage of the information using generally accepted statistical and scientific principles and methods. The risk of using such information is very low.

Once the data is de-identified it could be used for clinical research without compromising the individual's privacy thus benefiting for both individual and hospitals at the same time.

2. Related Works/Literature Survey

In a non Blockchain world, healthcare organization typically follow three models to facilitate interoperability of medical data: view, pull and push. In a push mode, medical information is sent from one organization to another. In a pull model, an organization seeks another organization about information. Finally, in the view model, an organization looks at another organization's record. Moreover, in push model, if a patient has been transferred from one hospital to another hospital the new hospital may not be able to view data recorded in the first hospital. Major drawback of those kind of models are data is not audited. The lack of having audit trail means the data integrity cannot be guaranteed from the point of data generation to the point of data usage. [5]

The introduction of wearable medical devices and use of mobile medical applications has led to the easy availability of PHI. These PHI are available with different organization for different usage. The lack of clarity in storing and usage of such devices in many countries as there is no written consent from the individual on the usage of his data.

The latest trend in data hacking is reported to have millions of PHI being stolen and this has contributed to security and privacy concern in the health industry as well the lack of confidence among the individuals in protecting their own data.

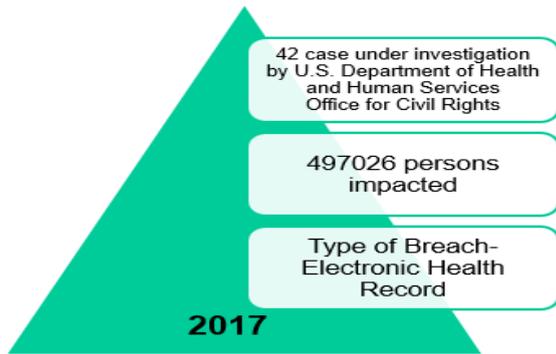


Fig. 1: Cases of data breaches in US for year 2017

Existing E-healthcare system has various issues with respect to security and privacy. Types of attacks on healthcare system such as jamming attack, data collision attack, data flooding attack, desynchronization attack, spoofing attack, selective forwarding attacks and Sybil attacks are identified as major type of cyber-

attacks [6]. These attacks are carried out with intention to misuse personal information for ransom or to bring dis-credibility to the health providers. These attackers can also the alter the existing data which could impact the individual's.

3. Framework

The proposal is to de-limit the individual details and extract critical information to create new data blocks which are based on diseases and clinical results in the form of distributed database using P2P network. This data blocks would assist health professional and clinical research organization and individuals in early detection of health ailments and provide new approach for providing early relief to individuals. This could be achieved without disclosure of individual's identification details at the same time having audit trails enabled to ensure transparency in usage of data blocks. The security features captured in the Blockchain methodology adds to the benefit of the individual's and health professional at same time without compromising the privacy of the individuals and enabling better security of the system used.

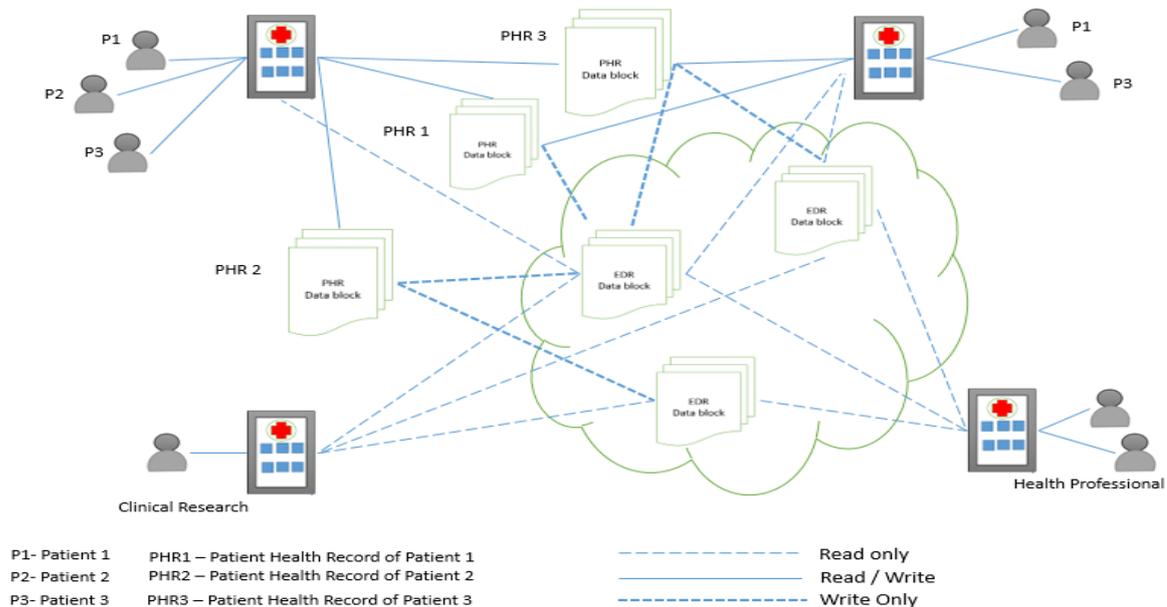


Fig. 2: Proposed two-layer architecture

a. Methodology/Implementation

This section discusses about the methodology which will be used for the development of the proposed architecture. The new trending technologies such as Cloud Computing along with Blockchain method would be used for creating P2P network and data blocks.

Cloud computing uses three models of service such as IaaS, PaaS and SaaS. These combined or separately could be used to have distributed network configured thus eliminating the need for standalone infrastructure. The use of virtualization technology helps in further reducing the need of dedicated platforms [7][8][9][10].

Blockchain typically uses cryptographic hash algorithm for transmission and storing of data which has better security features built into it. These help in data integrity leaving audit trail for future analysis [11].

Other technologies such as OpenPHR Standard which provides standards for clinical (HER) and demo demographic content model integrated with various standards such as SNOMED CT, LONIC DICOM and HL7 would support in identifying various health demographics [12].

PHI data sets need to be developed as part of implementation and testing for analysis of this model. Any existing PHI which could be integrated into the proposed model would be analyzed and used.

4. Discussions

This paper proposes two-layer architecture for creating data blocks using distributed network. This model proposes to use patient permission model for data access at the same time allowing to de-identify the PHI to remove 18 parameters as per HIPAA rule to create new data blocks as second layer. These data blocks in the second layer could provide new disease registries and medicinal registries to aid health professionals in early diagnosis of health alignments. These registries could also help clinical professionals and organization to use these data for their research without the need of individual's personal information as classified by HIPAA.

5. Conclusion

The article focused on the improving the data availability for health professional and clinical research without compromising data security and individual's privacy. Detailed analysis of various crypto algorithm needs to be evaluated before choosing the right one for the model. Integration of Cloud technology along with Blockchain needs to be tested to confirm the security standards mentioned by these technologies without compromising the individual privacy which add to the benefit of the proposed architecture model.

References

- [1] Satoshi Nakamoto, Bitcoin: Peer-to-Peer Electronic Cash System, page 1-9, www.bitcoin.org
- [2] Alex Roehrs, Cristiano André da Costa, Rodrigo da Rosa Righi, OmniPHR: A distributed architecture model to integrate personal health records, page 70-81, *Journal of Biomedical Informatics*, Elsevier, July 2017
- [3] Clinical Research and the HIPAA Privacy Rule, https://privacyruleandresearch.nih.gov/clin_research.asp
- [4] Research Repositories, Databases, and the HIPAA Privacy Rule, https://privacyruleandresearch.nih.gov/research_repositories.asp
- [5] NirKshetri, Blockchain's roles in strengthening cybersecurity and protecting privacy, page 1027-1038, *Telecommunications Policy*, Elsevier, November 2017
- [6] Security and Privacy Issues in Ehealthcare Systems: Towards Trusted Services, page 229-236, (IJACSA) *International Journal of Advanced Computer Science and Applications*, Vol. 7, No. 9, 2016
- [7] Dhanamma Jagli, Seema Purohit, Subhash Chandra, Knowledge Acquisition for Electronic Health Records on cloud, page 1909-1915, *Procedia Computer Science*, Elsevier, 2017
- [8] A. Galletta, L. Bonanno, A. Celesti, S. Marino, P. Bramanti and M. Villari, "An approach to share MRI data over the Cloud preserving patients' privacy," 2017 IEEE Symposium on Computers and Communications (ISCC), Heraklion, 2017, pp. 94-99
- [9] Al-Khanjari, Z, Al-Ani, A, Al-Hermizy, S, A PROPOSED SECURITY ARCHITECTURE FOR ESTABLISHING PRIVACY DOMAINS IN E-HEALTH CLOUD page 322-330, *European Scientific Journal*, June 2014
- [10] Ji-Jiang Yang, Jian-Qiang Li, Yu-Niub, A hybrid solution for privacy preserving medical data sharing in the cloud environment, Pages 74-86, *Future Generation Computer Systems*, Elsevier, February 2015
- [11] Dmitry Efanov, Pavel Roschin, The All-Pervasiveness of the Blockchain Technology, page 116-121, *Procedia Computer Science*, Elsevier, 2018
- [12] Dr. Koray Atalag PhD (New Zealand), Thomas Beale (UK), Dr. Rong Chen, PhD (Sweden), Tomaž Gornik (Slovenia), Dr. Sam Heard (Australia), Dr. Ian McNicoll (UK), openEHR A SEMANTICALLY-ENABLED, VENDOR-INDEPENDENT HEALTH COMPUTING PLATFORM, http://www.openehr.org/resources/white_paper_docs/openEHR_vendor_independent_platform.pdf