Advances in Parallel Computing Technologies and Applications
D.J. Hemanth et al. (Eds.)

doi:10.3233/APC210150

A Survey on Securing Medical Data in Cloud Using Blockchain

HariPriya K [a,1], Brintha NC [b] and Yogesh C K [c]

[a] *Research Scholar, Department of Computer Science and Engineering Kalasalingam Academy of Research and Education, Krishnankovil, TamilNadu, India*

[b] *Associate Professor, Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education Krishnankovil, TamilNadu*

[c] *Assistant Professor, Department of Computer Science and Engineering, Vel Tech Rangaraja Dr.Sagunthala R&D Institute of Science and Technology, Chennai,India*

Abstract. Security is a major concern in every technology that is introduced newly to facilitate the existing mechanism for better maintenance and handling. This is also the case in electronic health records. The data of the hospitals and the associated patients gets digital in the past few decades. The data is stored in the cloud for various reasons such as convenience of the participating entities to access it, easy maintenance. But, with this there also arises various security concerns. It has been observed from the reason studies that blockchain is used as the means of securing the healthcare data in the cloud environment.This study discusses the following. 1) Applications of blockchain in cloud environment, 2) Applications of blockchain in securing healthcare data 3) General issues and security concerns in blockchain technology and what features of block chain makes it suitable for securing health care a nd what features restricts it from using.This work helps the future researchers in getting a deep understanding of the in and out of applying blockchain in cloud and healthcare environment.

Keywords. Cloud environment, blockchain, healthcare data, security.

1. Introduction

Blockchain can be defined as the distributed data store[1] .the data can be anything such as events or records. This data are framed as blocks. Each block contains a hash value generated with the content in that particular block. Each block also contains its previous block's hash value also. These kinds of framework make the secure and tamper proof [2]. The following Figure 1 represents the basic structure of a block chain. The architecture of any blockchain process can be explained with the following Figure 2. The features of the blockchain that makes it suitable for applying in various domains for incorporating security are its distributed nature, the security it provides with the help of their cryptography algorithms and access permission methods, the transparency it provides, the method of deciding on whether a transaction is valid or not by all the nodes which is called as

[1] HariPriya K, Department of CSE, Kalasalingam Academy of Research and Education, Krishnankovil. E-mail: haripriyame@gmail.com

consensus algorithm and its flexibility. The transaction specified in the figure can be any operation done in a particular domain such as storing a health care data or modifying it.

Blockchain is used in various domains to provide security to the models developed in the respective domains. Studies have revealed that the major domains in which the blockchain technology such as Cybersecurity, Helathcare, Internet of Things[3]. This work concentrates on studying the various state of art models pertaining to the usage of the blockchain technology in Health care in order to improve the security in various means.It is also observed that there is a trend towards usage of healthcare data in the cloud environment. Hence, the survey made in this work is classified in to two groups.

- The works related to the application of blockchain in Healthcare both in with and without cloud context.
- The works related to the application of blockchain in cloud environment.

Both the study is made in perspective of the application of blockchain to resolve various security issues. In addition to this the various common security issues pertaining to the block chain is discussed along with the hurdles in implementing block chain technology in healthcare domain, The features of the blockchain that makes it suitable for the healthcare domain is also discussed along with this. The following Figure 3 represents the number of works discussed in both the above specified groups.

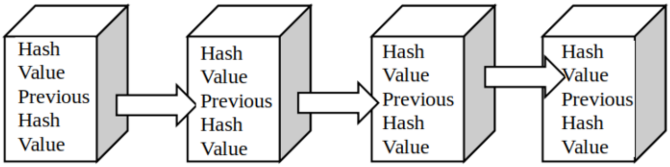
Hash Value Previous Hash Value
Hash Value Previous Hash Value
Hash Value Previous Hash Value
Hash Value Previous Hash Value

Figure 1. Structure of Blockchain

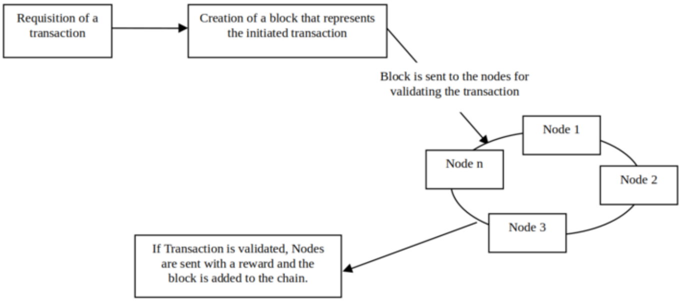
Requisition of a transaction
Creation of a block that represents the initiated transaction
Block is sent to the nodes for validating the transaction
Node 1
Node 2
Node 3
Node n
If Transaction is validated, Nodes are sent with a reward and the block is added to the chain.

Figure 2. Working of Blockchain

The organization of the paper is as follows. The second section specifies and shortly discusses the details of the works and the content provided that discusses the security vulnerabilities and the risks associated with the blockchain technology. It also discusses the general hurdles in implementing the blockchain technique in healthcare domain given in the literature. The third section explains how different features of blockchain technology make it suitable for securing health care applications. The fourth section in detail

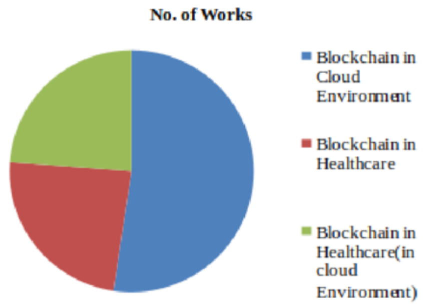

Figure 3. Summary of the work

explains the state of art models that uses block chain technology in cloud environment and addresses the various security issues related to the cloud environment. The fifth section explains the works that uses blockchain for addressing security issues in healthcare environment. The last and the sixth section give the conclusion and the inferences made.

2. Issues and Risks with the Blockchain Technology

As discussed in [4] , the general problems that occur with blockchain technology are shown in the following Figure 4 Since this work concentrates on studying the security concerns of the blockchain, only the issue pertaining to it is considered. In [5] various other security concerns of blockchain are considered. They are summarised in the following Figure 5.it also discusses in detail the various vulnerabilities with reference to these risks. [6] have specified a list of security concerns that may arise in the blockchain environment.

- There are possibilities that a user's identity is stolen
- Miners who are important players of the blockchain environment are the main targets of risk
- Due to the distributed nature of the blockchain environment, it is vulnerable to various risks such as the malicious code injection, leakage of transaction details from individual nodes. As per [7] the general hurdles in incorporating the blockchain technology in healthcare domain are given below.
- In case of the smart health care systems, it is observed that there is no rule of thumb to be followed in different activities such as the collection of data, sharing of data and the other associated communication mechanism.
- Since the model is user centralized, there are possibilities in certain cases that the users, in our case, patients are not in a position to grant access
- There are issues that might arise when the data are transferred from the Electronic Health record to blockchain Other general issues includes the unavailability of the government policies or government rules to govern the various aspects of blockchain such as the ownership of the data, issues related to legal aspects and punishments in case of any violations.

3. Benefits of using blockchain in healthcare

The [7] also gives a set of benefits of utilizing the blockchain model in the healthcare domain.

- Though there are certain security concerns with the distributed nature of blockchain, on the other hand, it also provides a secured means of storing the medical data of the patients as well as the clinical data.
- Since the blockchain model requires different participants of the model to authorize each transaction, patients can play an integral role in managing their data and even the system can be designed centred around them.
- The immutable nature of the blockchain model enables a trusted system and also it provides a better control over the system. Blockchain technology avoids the various shortcomings that arise in the centralised model.

It paves way for the secured means of sharing the data

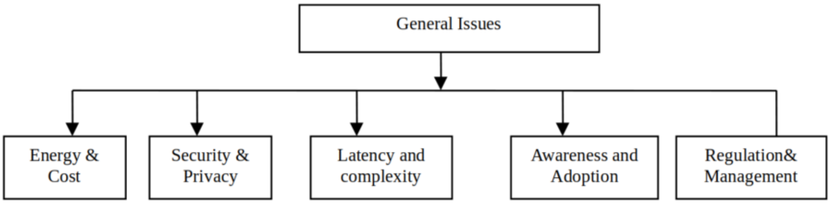

Figure 4. General issues with Blockchain

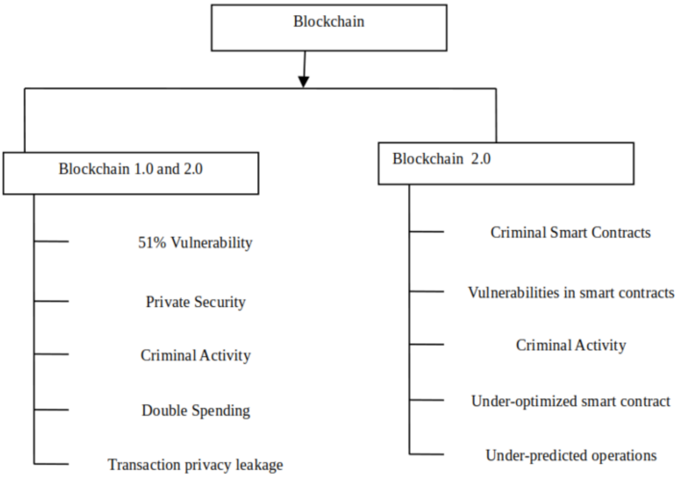

Figure 5. Risks in Blockchain models

4. Blockchain in Cloud Environment

The following is the summary of the various state of art models that uses blockchain technology in the cloud environment. There are various access control mechanisms that are in use in cloud storage environments. In [8] , a blockchain based access control mechanism, that can be used in the cloud environment is proposed. The various integrated processes of any access control mechanism such as the generation of keys, providing access to different requests, assigning access control policies, making changes in the access control policies, revoking the assigned policies and their corresponding logs are implemented with the support of the blockchain technology called as the decentralized ledger. The encryption model employed in the work is attribute based encryption. It is implemented with the etherum virtual machine. In cloud environment, the owner is not sure about the capabilities of making restriction on their data pertaining to the access control and maintains the integrity of the data. The main objective of the authors of the [9] is to design a blockchain enabled database suitable for the cloud environment. It is also helps in maintaining the integrity of the database. The model implements two layers of blockchain, the forst layer that uses the proof –of –work consensus algorithm and the second layer that employs the miners. The design approach proposed also addresses the various research questions pertaining to data integrity.

The security of the cloud environment in specific the data provenance is key element for addressing the various other security concerns, in [10], blockchain technology is used for meeting the requirements pertaining to the data provenance in the cloud environment. The authors after implementing the blockchain in cloud environment also concentrate on the security issues that would occur in the blockchain cloud. Particularly, the attack addressed in the model is the block without holding attack. Distinct pool rewarding mechanism is used for solving this issue and the various measurements and their impact are discussed and analysed [11,12]. In order to solve the data integrity issues in the environments such as cloud computing.[13] A technology based on mobile agents is used for creating a virtual machine agent, this helps in achieving the goal of verifying the trust of the data. This model helps in ensuring the reliability of the data. cloud environment, block chain technology is used in [14]. Verification of the trust of the data is an important task in The same mechanism can be used in ensuring the integrity of the in the blockchain mechanism. The authors have employed merkel key has for generating the hash values that are used for monitoring the smart contracts that are used for data change. In addition to ensuring the integrity of the model the other performance parameters measured and compared are construction cost and the reconstruction time.

Interoperability plays a key role in the personal cloud computing. It is the process that acts behind the sending and receiving the messages and securing them. In [15], the authors have proposed a blockchain based solution for ensuring the validity of the interoperability .in specific, the work concentrates on authentication. The mechanism of authentication and encryption of end to end data transfer is governed by JSON web tokens in this work where the activities are dependent on the central server. It is replaced with the blockchain technology. In case of [16] the authors concentrates on the implementation of the blockchain technology in the outsourcing services. The security issues considered are malleability attacks and the eavesdropping attacks. Blockchain implementation is made between the client and the service provider. The process consists of five phases. The phases ensure that the service provider provides the services that it has promised for.

This is ensured with the help of the challenging mechanism followed at the client end. Majority attack is a kind of attack that occurs in the blockchain environment due to the distributed nature of it. This kind of attack is also known as 51% attack. This is made by the miners. The threat model considered is based both on the one that occurs due to the user collisions and another that occur due to bad users. These problems are taken into consideration in [17] and a solution is provided based on block chain. The model provides secured mechanisms for document management and document modification. The various performance parameters considered and evaluated are Gas cost and time.

Monitoring and tracking of all the data objects in the cloud environment is a vital process to be followed in order to ensure the privacy of the data, accountability of the data. In [18] a novel architecture is provided based on blockchain . The architecture ensures that all the provenance data is verified by associating them with the blockchain. The security issue addressed with this model are reliability and privacy of the user. Three phases are employed by the authors that deal with the provenance data, one for collecting the data, one for storing the data and at last one for validating it. The limitations in the mobile devices such as the low storage capacity and the limitation in the computing power, is resolved with the help of the mobile cloud computing. In case of decentralized models in mobile cloud computing where, the resources such as the computational power and the storage are integrated together and used without the employment of the centralised server, there exists the problem of authenticating the mobile devices, in [19], and the authors have proposed a blockchain based model for mobile authentication. They ensure the proper authentication of the mobile devices that enters the mobile resource management network.

In case of the cloud computing, the users will store their files in the cloud storage. The cloud service providers might be vulnerable .this makes the users to encrypt their file and store in the cloud. The problem that arises with this is the overhead that arises with the transmission of the encrypted file. In [20], a block chain based approach is provided in order to split the data file in to number of chunks which are secured by means of encryption. The data is later placed in P2P network. Additionally, file block replica placement problem is also addressed with the help of genetic algorithm. The performance parameters considered are transmission delay and file security. In case of the cloud based models, both the cloud service providers and the clients depend on the third party auditor for ensuring the integrity of the data. In [21] it has been specified that availability of third party auditors is a question of concern in all the cases. The authors have proposed a blockchain based approach for replacing the third party auditor. The model concentrates on facilitating the auditing process of the cloud based models. The smart contracts designed for this purpose makes the cloud service providers to ensure it provides genuine service to its clients.

5. Blockchain in Addressing Security Issues in Health Care Domain

In [22] the authors have addresses two problems, former, the inability of the patients to access their records in certain cases and later the privacy of the data associated when the data is accessed by the stake holders. The framework proposed by the authors both the problems by means of blockchain technology. Six different contracts are designed and used. Service contract, owner contract, classification contract , relationship contract and consensus contract. All the operations such as addition of patients, manipulating access control permissions, working with records are done with the help of these contracts. Patient privacy is ensured with the help of encryption. In case of [23] two contracts are defined, one for performing the CRUD operations with the patient data and another for providing granular access control. A block chain is formed between the users and the implementation. The role contracts used by the authors are Rolesmart. It is a contract that belongs to the OpenZeppelin library. inorder to ensure that the blockchain in secure, consensus algorithm called as Proof of Work is employed. Every CRUD operation in the work is validated, authenticated and authorized. The addressed security issues in the paper are integrity, access control and confidentiality.

With an implementation of a private blockchain the authors of [24] addresses the security considerations of the health care data. In addition to this, a mechanism has been formulated which enables the patients with similar symptoms to communicate securely with a session key after authentication. Pairing based cryptography and openSSL libraries are used for implementation. The model also enables the doctors belonging to different hospitals to share the data securely between them. Proxy re-encryption is used for ensuring the security of the data during transit. Various other security issues are also addressed. The performance parameters that are evaluated are Computational cost, communication cost, security level.

Authentication and integrity are the major concerns of [25]. The authors uses keyless signature infrastructure for ensuring security of the digital signatures employed in the model and hence the associated authentication issues. The integrity of the data is addressed by the incorporated blockchain technology. In case of [26], patient driven interoperability is considered and the possibilities of applying the blockchain technologies to address the various issues pertaining to the specified interoperability is discussed. This is possible with the different kinds of features provided by the blockchain technology such as the immutability, identity, liquidity , aggregation and access rules. But in addition to specifying the possibilities of using blockchain technology in electronic health care domain, the authors have also specified the various barriers. In [27], blockchain technology is used in two places, first in case when the patients make their decisions on the authorization policies for their medical records and write the same in blockchain for further approval. In second case, when the node responsible for bookkeeping writes the description of the medical data to the blockchain. It also includes the location of the data in the cloud. Both these practice is included in order to ensure two security concerns namely the integrity of the data and traceability.

It has been specified by the authors of [28] that the centralized nature of cloud environment, leads to various security concerns such as data privacy. It has its impact in the transit of data also. The authors have proposed a protocol based on blockchain for sharing data. In this model, the authors have used the blockchain technology to store the keyword ciphertext. This keyword ciphertext is used for searching the data in the electronic healthcare records and also used for sharing the data. The security issues that are addressed are authorization, protection of identityand privacy. [29] have listed few issues related to the implementation of blockchain in healthcare systems. They are listed in the following Table 1. Though studies have specify that, solution to the above specified problems is in the form of storing the data outside the chain and the corresponding hash values in the blockchain these are the things to be considered in future researches with respect to the application of blockchain in healthcare. There are different security concerns that while outsourcing the electronic health care data in the cloud environment. The authors of [30] have designed a blockchain model for resolving various attacks such as forgery attacks,modification attacks and impersonation attacks.This is ensured by various aspects. First, an authentication mechanism is designed for ensuring that only the the authenticated users are allowed to outsource the data. The participants of the model, at any time can verify the integrity of the data.

Table 1. Few Blockchain Issues and Associated Problem

Issue	Property	Associated Problem
Integrity	Immutability	The Law of certain countries says that the personal data of individuals have to be erased based on the request.
Data Storage	Blockchain is suitable for storing transaction data and the associated backtracking	Medical data need more specific use cases such as the handling images, searching etc.

6. Conclusion and Inferences Made

The following were made from the study made. Though blockchain can be used in health care domain for addressing various security issues, Blockchain has its own security issues and General issues in terms of adapting it to Healthcare Domain. It is also observed from the study that though cloud is a centralised model, blockchain has its own applications in the cloud environment. Though there are only few studies that are related to the application of blockchain in securing health care records that are stored in the cloud environment, it addresses various security issue and still there are scope for future research.

References

[1] Blockchain definition [Internet]. [cited 15th June 2020]. Available from: https://*en.bitcoin.it/wiki/Block_chain*.

[2] Nofer M, Gomber P, Hinz O, Schiereck D. Blockchain. Business & Information Systems Engineering. Springer. 20 March 2017;59(3):183–7.

[3] Islam A, Shin SY. A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things. Computers & Electrical Engineering. 2020 Jun 1;84:106627.

[4] Meng W, Tischhauser EW, Wang Q, Wang Y, Han J. When intrusion detection meets blockchain technology: a review. Ieee Access. 2018 Jan 30;6:10179-88.

[5] Wang Y, Zhang A, Zhang P, Wang H. Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain. IEEE Access. 2019 Sep 23;7:136704-19.

[6] Niranjanamurthy M, Nithya BN, Jagannatha S. Analysis of Blockchain technology: pros, cons and SWOT. Cluster Computing. 2019 Nov;22(6):14743-57.

[7] Tripathi G, Ahad MA, Paiva S. S2HS-A blockchain based approach for smart healthcare system. In Healthcare 2020 Mar 1 (Vol. 8, No. 1, p. 100391). Elsevier.

[8] Sukhodolskiy I, Zapechnikov S. A blockchain-based access control system for cloud storage. In 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) 2018 Jan (pp. 1575-1578). IEEE.

[9] Gaetani E, Aniello L, Baldoni R, Lombardi F, Margheri A, Sassone V. Blockchain-based database to ensure data integrity in cloud computing environments. In 2017 Italian Conference on Cybersecurity 2017 Jan 20 (pp. 1-10).

[10] Wang H, Qin H, Zhao M, Wei X, Shen H, Susilo W. Blockchain-based fair payment smart contract for public cloud storage auditing. Information Sciences. 2020 May 1;519:348-62.

[11] Saranya MS, Selvi M, Ganapathy S, Muthurajkumar S, Ramesh LS, Kannan A. Intelligent medical data storage system using machine learning approach. In 2016 Eighth International Conference on Advanced Computing (ICoAC) 2017 Jan 19 (pp. 191-195). IEEE.

[12] Luo Y. Environmental cost control of coal industry based on cloud computing and machine learning. Arabian Journal of Geosciences. 2021 Jun;14(12):1-6.

[13] Selvakumar K, SaiRamesh L, Sabena S, Kannayaram G. CLOUD COMPUTING-TMACS: a robust and verifiable threshold multi-authority access control system in public cloud storage. In Smart Intelligent Computing and Applications 2019 (pp. 365-373). Springer, Singapore.

[14] Wei P, Wang D, Zhao Y, Tyagi SK, Kumar N. Blockchain data-based cloud data integrity protection mechanism. Future Generation Computer Systems. 2020 Jan 1;102:902-11.

[15] Faisca JG, Rogado JQ. Personal cloud interoperability. In 2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM) 2016 Jun 21 (pp. 1-3). IEEE.

[16] Zhang Y, Deng RH, Liu X, Zheng D. Blockchain based efficient and robust fair payment for outsourcing services in cloud computing. Information Sciences. 2018 Sep 1;462:262-77.

[17] Zhu L, Wu Y, Gai K, Choo KK. Controllable and trustworthy blockchain-based cloud data management. Future Generation Computer Systems. 2019 Feb 1;91:527-35.

[18] Liang X, Shetty S, Tosh D, Kamhoua C, Kwiat K, Njilla L. Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID) 2017 May 14 (pp. 468-477). IEEE.

[19] Kim HW, Jeong YS. Secure authentication-management human-centric scheme for trusting personal resource information on mobile cloud computing with blockchain. Human-centric Computing and Information Sciences. 2018 Dec;8(1):1-3.

[20] Li J, Wu J, Chen L. Block-secure: Blockchain based scheme for secure P2P cloud storage. Information Sciences. 2018 Oct 1;465:219-31.

[21] Tosh DK, Shetty S, Liang X, Kamhoua CA, Kwiat KA, Njilla L. Security implications of blockchain cloud with analysis of block withholding attack. In 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID) 2017 May 14 (pp. 458-467). IEEE.

[22] Gordon WJ, Catalini C. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. Computational and structural biotechnology journal. 2018 Jan 1;16:224-30.

[23] Shahnaz A, Qamar U, Khalid A. Using blockchain for electronic health records. IEEE Access. 2019 Oct 9;7:147782-95.

[24] Liu X, Wang Z, Jin C, Li F, Li G. A blockchain-based medical data sharing and protection scheme. IEEE Access. 2019 Aug 26;7:118943-53.

[25] Nagasubramanian G, Sakthivel RK, Patan R, Gandomi AH, Sankayya M, Balusamy B. Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Computing and Applications. 2020 Feb;32(3):639-47.

[26] Wang H, Song Y. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. Journal of medical systems. 2018 Aug;42(8):1-9.

[27] Vora J, Nayyar A, Tanwar S, Tyagi S, Kumar N, Obaidat MS, Rodrigues JJ. BHEEM: A blockchain-based framework for securing electronic health records. In 2018 IEEE Globecom Workshops (GC Wkshps) 2018 Dec 9 (pp. 1-6). IEEE.

[28] Li X, Jiang P, Chen T, Luo X, Wen Q. A survey on the security of blockchain systems. Future Generation Computer Systems. 2020 Jun 1;107:841-53.

[29] Esposito C, De Santis A, Tortora G, Chang H, Choo KK. Blockchain: A panacea for healthcare cloud-based data security and privacy?. IEEE Cloud Computing. 2018 Mar 28;5(1):31-7.

[30] Cao S, Zhang G, Liu P, Zhang X, Neri F. Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain. Information Sciences. 2019 Jun 1;485:427-40.