WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Preserve Sharing of Medical Data Robustness Testimony in Cloud Server Framework

[1]Aravinth , [2]Sanjay Bharathi, [3]Sankar, [4]Assistance Prof Anand Raj

[1]E.G.S Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, India
E-mail:aravinthproj@gmail.com
[2]E.G.S Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, India
E-mail:sanjaybharathi90@gmail.com
[3]E.G.S Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, India
E-mail:sankarselva2111@gmail.com
[4]Associate Professor E.G.S Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, India
E-mail:anandraj@egspec.org

A B S T R A C T

Electronic Health Records (EHRs) are digitally stored health information electronically . EHRs are commonly shared between health partners and power outages, data misuse, and scarcity .The path to privacy, security, and audit. Blockchain, on the other hand, is a twentieth revolutionary invention Provides a distributed and decentralized system for communication between nodes in the list of networks Without federal authority. It addresses the limitations of EHR management and provides a secure, secure, And the decentralized environment for the exchange of EHR data. Three types of blockchain-based potential Solutions have been proposed by researchers to handle EHRs. EHRs: Ideological, exemplary and implemented. This review focuses on a systematic literature review (SLR) and analyzes submitted articles Theoretical or implemented to manage EHRs using blockchain. SLR finds that blockchain technology guarantees decentralization, security and privacy Traditional EHRs are often absent. Furthermore, the results obtained from extensive studies will provide the possibility Researchers with blockchain type for future research. Finally, future research directions, in the end, Direct enthusiasm for incorporating new blockchain-based systems to properly manage EHRs.

.

1.INTRODUCTION

One of the most common forms of data reduction processes works by comparing data fragments to find duplicates. To make that happen, an identification is assigned to each piece of data, which is computed by software that typically uses cryptographic hash functions. In many processes, Although this may not be true in all cases due to the pigeonhole principle, it is assumed that if the identification is identical, the data will be identical; Other processes do not assume that two data sets with the same identifier are identical, but check that the data with the same identifier is actually identical. If the software assumes that the given identity already exists in the deductible namespace or actually verifies the identity of the two batch of data, it will replace that duplicate piece with a link. Once the data has been copied and re-read the file, wherever a link is located, the system simply replaces that link with the specified piece of data. The detection process should be transparent to end users and applications. Storage-based data reduction reduces the amount of storage required for a given set of files. This can be very useful in applications where multiple copies of identical or identical data are stored on the same disk - a surprisingly common situation. In the case of data backups that are routinely made to protect against data loss, most of the data in a given backup will remain unchanged from the previous backup. General backup systems try to use this by avoiding unchanged files or saving & nbsp differences

*Aravinth: *Phone*.no: +919150833431
E-mail address: aravinthproj@gmail.com

between files. However, no approach likes all redundancies. Hard linking does not help large files that have only been converted in small ways, such as the email database; Differences should only be found in redundancies in subsequent versions of a file, and the logo image should be removed and re-inserted into a section or multiple documents.

2.METHODOLOGY

Step 1:The health system provides services to a patient and stores patient data (physician Write a note on an existing health information technology system or a pharmacist may prescribe medication. Later, the Data fields and the patient's public ID are redirected to the blockchain via APIs.

Step 2:Transaction completed and uniquely identified: Each transaction is encrypted and gives an identifier stored in the blockchain Patient's public (unidentifiable) ID.

Step 3: Healthcare companies and organizations may request blockchain directly: To request data, healthcare organizations and organizations submit and use their queries through APIs

Step 4:Patient's public ID in blockchain to retrieve encrypted data. Patient information is like that
(E.g. age, gender, disease, physician) can now view and analyze to find new insights.

Step 5:Patients can specifically authorize any individual to access their medical information: The patient's private key links their identity to blockchain data. This private key can be shared with health organizations, which can use it to decrypt the patient's data. Thus, data remains unidentifiable to those without the key.

3.MODELING AND ANALYSIS

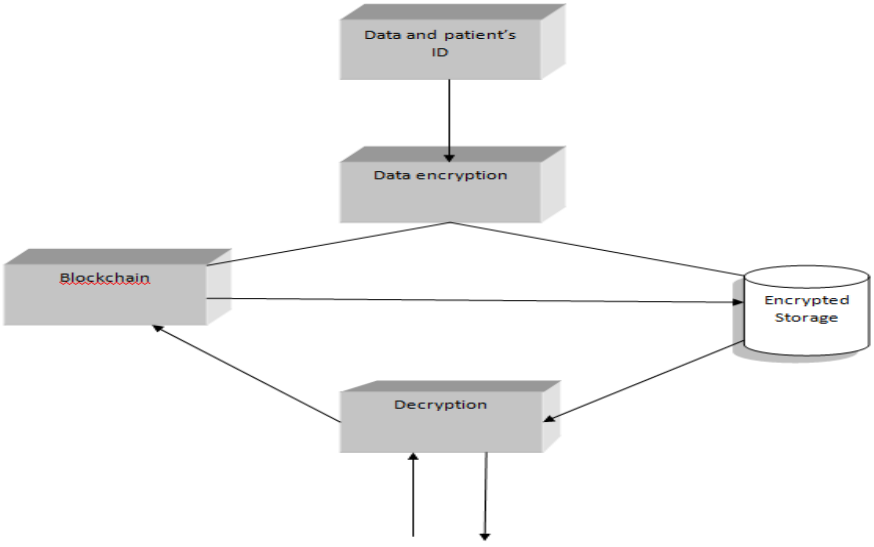

Figure1: Data Flow.

4.RESULTS AND DISCUSSION

Testing a decentralized system (as well as any system with different autonomy Components) is a challenging task for a number of reasons: it takes time and attention to come up with components and start on different machines; When Death Penalty, Communication links may be broken; Different areas may present failures Only with a specific sequence of functions, it often happens when something fails It is necessary to analyze the history and connections of all the components connected. In particular, it tests the performance and security of the blockchain network .The literature presents

additional challenges as we discuss the delegate Indicators and test kits are still incubating. Literary approach Security is generally based on modeling, , Belief assumptions and theoretical evaluations because test verification is not always complete .On the other hand, performance analysis creates new challenges because it is necessary to write test cases that reach all the components and recreate the real situation .Where all the components are placed under pressure.

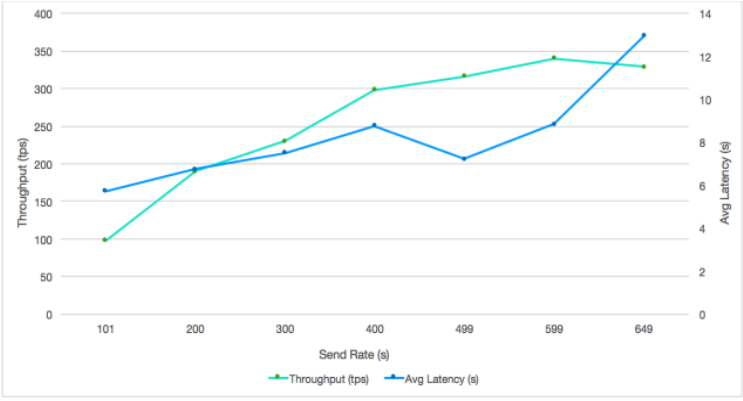

Figure 2: Throughput and latencies, write operations, normal scenario.

5.CONCLUSION

In this article we will discuss how to use blockchain technology to handle EHR (Electronic Health) and we propose an architecture that can be used to improve the current EHR .The challenges behind its widespread adoption. We chose the Ethereum framework to enable Ledger Proposed views. From these studies, it is clear that the medical record is high .A detailed record of a person's identity must be kept and handled in a secure manner. Because Blockchain cannot change or delete encrypted information, It is full integrity and commitment Protection from the first day of using medical records. Therefore, to enable reliable access to medical data, Patients will be at the center of their health care data and may have any access or withdrawal The other company that needs access to their information. Blockchain and distributed infrastructure .Technology is one of the most exciting developments in the field of healthcare. It has to be a part of it Strategic design for business process modernization of a company concerned about issues Security, mobility and privacy. Therefore, medical information covers medicine Records, pictures, documents and laboratory reports that require considerable storage space. Ideally, every member included in the chain should have a complete copy of the entire medicine The record of each individual and this amount may exceed the storage capacity of the current Blockchain technology.

6.REFERENCES

[1] Zuo, Cong, et al. "Fine-grained two-factor protection mechanism for data sharing in cloud storage." IEEE Transactions on Information Forensics and Security 13.1 (2017): 186-196.

[2] Chen, Jinchuan, and Yunzhi Xue. "Bootstrapping a blockchain based ecosystem for big data exchange." 2017 IEEE international congress on big data (bigdata congress). IEEE, 2017.

[3] Zhao, Yanqi, et al. "Machine learning based privacy-preserving fair data trading in big data market." Information Sciences 478 (2019): 449-460.

[4] Raman, d., and j. Sujatha. "Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage." system 6.04 (2019).

[5] Liang, Kaitai, Willy Susilo, and Joseph K. Liu. "Privacy-preserving ciphertext multi-sharing control for big data storage." IEEE transactions on information forensics and security 10.8 (2015): 1578-1589.

[6] Alderman, James, Christian Janson, Carlos Cid, and Jason Crampton. "Access control in publicly verifiable outsourced computation." In Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, pp. 657-662. 2015.

[7] G. Rathi, Abinaya. M, Deepika. M, Kavyasri. T," Healthcare Data Security in Cloud Computing"International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 3, March 2015 Copyright to IJIRCCE

10.15680/ijircce.2015.0303089 1807

[8] R. Josephius Arunkumar 1 , R. Anbuselvi2, "Enhancement of Cloud Computing Security in Health Care Sector ", International Journal of Computer Science and Mobile Computing A Monthly Journal of Computer Science and Information Technology ISSN 2320–088X IMPACT FACTOR: 6.017 IJCSMC, Vol. 6, Issue. 8, August 2017, pg.23 – 31.

[9] Kushan Shah, Rui, and Ling Liu. "Security for Healthcare Data on Cloud." In Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, pp. 268-275. IEEE, 2010.

[10] Raval, Divya, "Cloud based Information Security and Privacy in Healthcare." International Journal of Computer Applications (IJCA), ISSN (2016): 0975-8887.