INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 7, Issue 4 - V7I4-1390)
Available online at: https://www.ijariit.com

Electronic Health Records using Blockchain and Cloud computing

Sonia S. B.
sonia.sb@atria.edu
Atria Institute of Technology, Bengaluru, Karnataka

Amrutha D.
amruthadevaraj61@gmail.com
Atria Institute of Technology, Bengaluru, Karnataka

Bhavana C.
bhavanacgowda24@gmail.com
Atria Institute of Technology, Bengaluru, Karnataka

Ankitha J.
ankijairamnaidu@gmail.com
Atria Institute of Technology, Bengaluru, Karnataka

ABSTRACT

Blockchain technology eliminates the need for a central system to guarantee information integrity and custody of data, as well as to mediate transactions and the exchange of crypto assets, by allowing safe and pseudo-anonymous transactions and bilateral agreements between participants. It has crucial qualities like immutability, decentralisation, and openness that could help with pressing healthcare challenges including inadequate records at the point of care and restricted access to patients' own medical information. Interoperability software system and technology frameworks to interact safely and efficiently, share data, and utilize that data across healthcare organisations and application vendors, resulting in a more efficient and effective public health system. Due to a lack of interoperability, healthcare today suffers from compartmentalised and disjointed data, hindered communications, and fragmented work flow tools. In a safe and pseudo-anonymous manner, blockchain provides access to longitudinal, full, and adulterate aware medical records that are kept in fragmented systems. The goal of our suggested scheme is to first integrate blockchain technology for EHR and then to enable safe storage of electronic records for users of the framework by defining granular access controls. The following framework gives the EHR system the advantages of a blockchain-based solution that is extensible, secure, and integrated.

Keywords: *Blockchain, Health Records, Electronic Health Records, Decentralization, And Scalability*

1. INTRODUCTION

Technology's latest developments are touching many aspects of human life and altering the way the things are perceived. Technology is finding new methods to improve the healthcare industry, just as it has in many areas of life. The key advantages of technological innovation include enhanced safety, customer experience, and other aspects of the healthcare business [1]. Every patient's protected medical information is the most valuable asset in any healthcare sector. Blockchain technology provides an excellent and innovative solution to keep track of patient data that is scattered. The Electronic Health Record (EHR) is an unavoidable implementation of network architecture in the healthcare profession, and it contains a great deal of personal data. An Electronic Health Record (EHR) is a sophisticated system that collects and stores sensitive medical information and health data in a digital format. EHRs are patient-driven authentic records that securely deliver information to approved stakeholders as quickly as practical. Patients' personal and medical histories are stored in an EHR. The EHR paradigm aspires to go beyond typical clinical data collection in order to provide a more holistic perspective of health outcomes [2].As cloud storage technology has grown in popularity and as multiple benefits, the most common approach of EHR data exchange is for the end user to store the protected EHR information on to the cloud. Imagine that each and every EHR uploaded updates to an open-source, community-wide recognized register of prescriptions, concerns, and sensitivity lists, guaranteeing that modifications to medical information are well-understood and verifiable across enterprises. Instead of presenting data from a single repository, the EHR might represent information from any database linked to in the register.

The proposed framework incorporates Attribute-Based Signatures (ABS), a flexible primitive that allows a participant to sign a communication while preserving fine-grained command over identifying data. In ABS, a signer with a set of authorization credentials can sign a communication with a predicate that is in aggrievance with the authorization credentials. With the above proposed infra structure without manual user intercession, the result would be precisely balanced community-wide knowledge with guaranteed reliability from the perspective of data collection to the moment of demand.

2. LITERATURE SURVEY

The following paper discusses how distributed ledger technology can assist the healthcare sector and how it could be utilised for

electronic health records. Despite significant advances in the medical sector and technological advancement in electronic health records, the paper addresses the challenges encountered due to the novelty of blockchain technology. The proposed system combines protected record storage with sophisticated access control lists for such records. It establishes a structure that is easier to use and comprehend for the users. In addition, because IPFS uses an off-chain data warehouse, the framework proposes measures to ensure that the system solves the issues of data storage.

The following paper discuss the use of the Blockchain to distribute the HER addresses the major challenges of transparency and jurisdiction. The Blockchain makes it simple to retrieve data since it is available to anybody who has been given permission to do so. It can be accessible from everywhere since it is hosted on a distributed ledger. There are, nevertheless, a few problems that can be resolved in the future. Because the participants involved in the transactions can be identified, their anonymity and discretion may be jeopardised. While certain blockchains guarantee total anonymity, some confidential material should not be shared in this manner.

The following paper uses blockchain technology and cloud storage to store the indicator in element searchable encryption and the encrypted HER information independently, which solves the issue that the cloud provider has lower computational efficiency and is likely to cause privacy and security leakage in the attribute-based searchable cryptosystem. The key is encrypted at the very same time so it can be sent over the public channel. According to the conclusions of the performance monitoring, the encrypting and extraction time are independent of the concentration of attributes. The next phase would be to use a hidden access technique to achieve multi-keyword cipher text retrieval with a verifiable feature basis.

In this work, the author suggests an infrastructure that integrates blockchain technology into global HER systems to protect the validity of medical information while also enhancing the current systems' compatibility. It is interoperable with existing e-healthcare solutions and can be adopted by healthcare professionals without affecting record keeping efficiency. It enables chosen participants main responsibility for the blockchain technology maintenance, including the generation, validation, and attaching of new blocks, because the platform is basically a multiple access system and healthcare professionals separately maintain records.

3. METHODOLOGY

A new block is attached when a new transaction is transmitted by a participant on the blockchain network. A block would be utilized to maintain track of transactions, and all these blocks are transmitted to all of the network's linked nodes. This transactions, which is included within a block, is published to all nodes within the network. Every node in the network has a copy of the entire blockchain, which aids in the verification process. When a block comprising a client activity is disseminated to all network participants, they examine to see if it has been modified with in any way. If the validation passes, the nodes add the block to their personal version of the blockchain. This entire process of a block getting stored on the blockchain is finished by the nodes establishing an agreement on which blocks are legitimate for inclusion on the network and what is not. The connected nodes undertake this authentication using well-known techniques to authenticate the transactions and confirm that the originator is an authorized member of the system. When a node completes the verification successfully, it is awarded with crypto-currency.Mining refers to the process of validating a transactions, and the miner is the node that performs this validation.The block is added to the blockchain when it has been validated.The transaction is finished once the entire validation process has been completed[1].The following data flow is explained in the figure1.

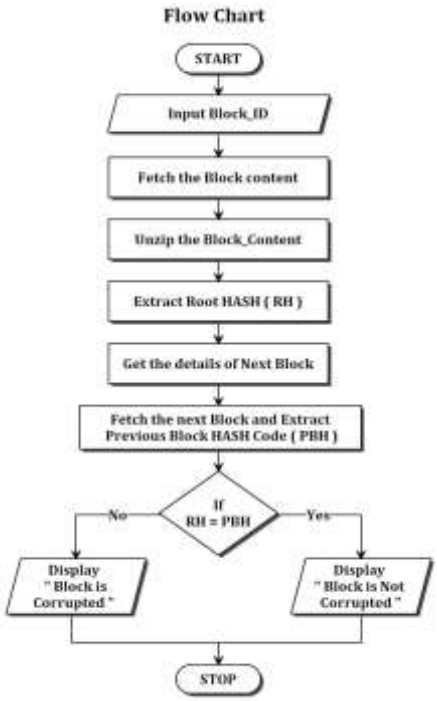

Figure1 – Block validation flow

Whenever a new transaction is made by the user the following flow is performed to store the data into the cloud by creating a new block. The WebApp's general hypermedia structure is explained by the System Architecture design. The structure of content items for presentation and navigation is referred to as content architecture. The way the application is structured to manage user interaction, handle internal processing duties, effect navigation, and present content is referred to as WebApp architecture. The architecture of a WebApp is defined in the context of the development environment in which it will be implemented, the main pillars of the architecture are admin, auditor, data owner. Admin is the main operator of the application and performs administrative roles. User receives the private key through a private channel shared by the data owner, the records is the securely stored on the cloud through block chain, the data is untampered here since each block is connected through the hash function and is encrypted using cryptographic algorithm , the auditor performs verification of the file and updates the status of the file. The architecture is shown in the figure 2.

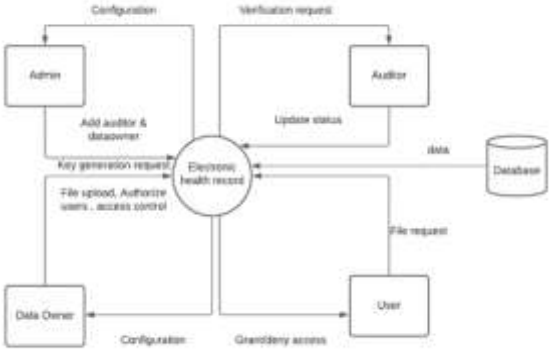

Figure2 - Architecture diagram

4. CONCLUSION

The paper examines how blockchain technology can benefit the healthcare industry and how it can be utilised for electronic health records in this article The approach proposed combines safe record storage with granular access controls for those documents. The Blockchain makes it simple to retrieve data since it is available to anybody who has been given permission to do so. It offers a system that is easier to use and comprehend for the users. The proposed system combines protected record storage with sophisticated access control lists for such records. It establishes a structure that is easier to use and comprehend for the users.

In addition, the framework suggests procedures to ensure that the system addresses the issue of data storage. The framework proposed uses blockchain technology and cloud storage to store the index in attribute present in searchable encryption and the encrypted Electronic health record data separately, with the attribute-based searchable encryption system, this solves the problem that the cloud server has low search efficiency and is simple to cause user privacy leakage .The key is encrypted at the same time so that it can be transferred through the private channel .According to the results of the performance analysis, the encryption and search times are independent of the amount of characteristics. There are, nevertheless, a few problems that can be resolved in the future. Because the participants involved in the transactions can be identified, their anonymity and discretion may be jeopardised. While certain blockchains guarantee total anonymity, some confidential material should not be shared in this manner.

5. REFERENCES

[1] **A. Shahnaz, U. Qamar and A. Khalid,** "Using Blockchain for Electronic Health Records," in IEEE Access, vol. 7, pp. 147782-147795, 2019, doi: 10.1109/ACCESS.2019.2946373.

[2] **V. B, S. N. Dass, S. R and R. Chinnaiyan**, "A Blockchain based Electronic Medical Health Records Framework using Smart Contracts," 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, pp. 1-4, doi: 10.1109/ICCCI50826.2021.9402689.

[3] **X. YANG, T. LI, R. LIU and M. WANG**, "Blockchain-Based Secure and Searchable EHR Sharing Scheme," 2019 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), 2019, pp. 822-8223, doi: 10.1109/ICMCCE48743.2019.00188.

[4] **Yang, Guang & Li, Chunlei & Marstein, Kjell.** (2019). "A blockchain-based architecture for securing electronic health record systems. Concurrency and Computation: Practice and Experience." 10.1002/cpe.5479.

[5] **G. Jetley and H. Zhang**, ``Electronic health records in IS research: Quality issues, essential thresholds and remedial actions," Decis. Support Syst., vol. 126, pp. 113-137, Nov. 2019.

[6] **K. Wisner, A. Lyndon, and C. A. Chesla**, ``The electronic health record's impact on nurses' cognitive work: An integrative review," Int. J. Nursing Stud., vol. 94, pp. 74-84, Jun. 2019.

[7] **M. Hochman**, ``Electronic health records: A ``Quadruple win," a ``quadruple failure," or simply time for a reboot?" J. Gen. Int. Med., vol. 33, no. 4,pp. 399-399, Apr. 2018.

[8] **Q. Gan and Q. Cao**, ``Adoption of electronic health record system: Multiple theoretical perspectives," in Proc. 47th Hawaii Int. Conf. Syst. Sci.,Jan. 2014, pp. 2716-2724.

[9] **T. Vehko, H. Hyppönen, S. Puttonen, S. Kujala, E. Ketola, J. Tuukkanen,A. M. Aalto, and T. Heponiemi**, ``Experienced time pressure and stress:Electronic health records usability and information technology competence play a role," BMC Med. Inform. Decis. Making, vol. 19, no. 1, p. 160,Aug. 2019.

[10] **M. Reisman**, ``EHRs: The challenge of making electronic data usable and interoperable.," PT, vol. 42, no. 9, pp. 572-575, Sep. 2017.

[11] **W. W. Koczkodaj, M. Mazurek, D. Strzaªka, A. Wolny-Dominiak, and M. Woodbury-Smith**, ``Electronic health record breaches as social indicators,"Social Indicators Res., vol. 141, no. 2, pp. 861-871, Jan. 2019.

[12] **S. T. Argaw, N. E. Bempong, B. Eshaya-Chauvin, and A. Flahault,**``The state of research on cyberattacks against hospitals and available best ractice recommendations: A scoping review," BMC Med. Inform. Decis.Making, vol. 19, no. 1, p. 10, Dec. 2019.

[13] **A. McLeod and D. Dolezel**, ``Cyber-analytics: Modeling factors associated with healthcare data breaches," Decis. Support Syst., vol. 108, pp. 57-68,Apr. 2018.

[14] **L. Coventry and D. Branley**, ``Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," Maturitas, vol. 113,pp. 48-52, Jul. 2018.

[15] ``The future of health care cybersecurity," **J. Nursing Regulation**, vol. 8,no. 4, pp. S2-S31, 2018.

[16] **D. Spatar, O. Kok, N. Basoglu, and T. Daim**, ``Adoption factors of electronic health record systems," Technol. Soc., vol. 58, Aug. 2019,Art. no. 101144.

[17] **S. Nakamoto**, Bitcoin: A Peer-to-Peer Electrnic Cash System. 2008,pp. 1-9.

[18] **W. J. Gordon and C. Catalini**, ``Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability," Comput.Struct. Biotechnol. J., vol. 16, pp. 22-230, Jan. 2018.

[19] **A. Boonstra, A. Versluis, and J. F. J. Vos,** ``Implementing electronic health records in hospitals: A systematic literature review," BMC Health Services Res., vol. 14, no. 1, Sep. 2014, Art. no. 370.

[20] **T. D. Gunter and N. P. Terry**, ``The emergence of national electronic health record architectures in the United States and Australia: Models, costs, and questions," J. Med. Internet Res., vol. 7, no. 1, p. e3, Jan./Mar. 2005.

[21] **Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang**, ``An overview of blockchain technology: Architecture, consensus, and future trends," in Proc. IEEE Int. Congr. Big Data (BigData Congr.), Jun. 2017,pp. 55-564.

[22] **C. Pirtle and J. Ehrenfeld**, ``Blockchain for healthcare: The next generationof medical records?" J. Med. Syst., vol. 42, no. 9, p. 172, Sep. 2018.

[23] **A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou**,``Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives," Cryptography, vol. 3, no. 1, p. 3, Jan. 2019.

[24] **J. Eberhardt and S. Tai**, ``On or off the blockchain? Insights on offchaining computation and data," in Proc. Eur. Conf. Service-Oriented Cloud Comput., Oct. 2014, pp. 1-45.

[25] **D. Vuji£i¢, D. Jagodi¢, and S. Randi¢**, ``Blockchain technology, bitcoin,and Ethereum: A brief overview," in Proc. 17th Int. Symp. INFOTEH-JAHORINA (INFOTEH), Mar. 2018, pp. -6.

