Journal of Positive School Psychology
2022, Vol.6, No.4, 3632-3638

http://journalppw.com

An Investigation On The Use Of Blockchain Technology In Electronic Health Records

G. Bhanu Prasad[1], M .Venkateswara Rao[2]

[1]Associate Professor, Department of Computer Science and Engineering, Malla Reddy Engineering College for Women, Maisammaguda, Hyderabad
[2]Professor, Department of Computer Science and Engineering GIT, GITAM DEEMED TO BE UNIVERSITY, Visakhapatnam

E-mail-id:bhanu.gorantla2020@gmail.com[1], venkateswararao.mandapati@gitam.edu2,

Abstract

Healthcare has benefited greatly from the use of electronic health records (EHRs). Patient safety, improved efficiency in healthcare, and increased access to health care services are all key functions of EHR in healthcare systems, as is the desire to decrease medical spending. To present current developments in the functions and uses of EHR in the healthcare system, this paper's primary aim was established. There are many ways in which EHR has shown to be beneficial in the healthcare system, including sharing and storing medical data via a decentralized peer-to-peer network in order to make it safer for healthcare workers to exchange health information. Patients, healthcare providers, and the general public have all been informed about blockchain-based healthcare apps and workflows developed for these groups. Data management for healthcare, the Internet of Medical Things, and a Blockchain model for health care are all aspects of blockchain technology that define healthcare, as well as the difficulties of using blockchain in health information exchange. In this paper we investigate the blockchain technology in electronic health records with different methodologies

Keywords: - Electronic medical records, Electronic Health Records, Trust, Healthcare Data Gateway, Blockchain technology.

1. INTRODUCTION

A patient's electronic health record (HER) [1-2] is a digital version of the patient's official health record that can be transferred quickly across institutions and departments in a safe manner. It contains all the information needed to get to know a patient, such as medical history, radiological pictures, diagnoses, medicines, vaccination dates, treatment plans, allergies, and test findings, among other things. It's critical in healthcare since it makes patient health records readily available for decision-making. since file-sharing is neither standardized or regulated, there is Healthcare providers must take EHR interoperability into account. Information exchange is complicated because of the challenges of establishing confidentiality and security. Because of low communication standards across different EHRs, increased integration costs, low patient participation in data sharing and the absence of patient identification throughout health information exchanges, EHRs and other organizations in the Health Information Technology sector are disorganized. A digital record of a transaction is what is meant by the term "blockchain." Blockchains is the name given to this

technology because of the way it is constructed. It has a collection of people's records in the form of connected blocks arranged into a single list called a chain. Each transaction is added to the blockchain after it has been authenticated by one of the validating nodes that are linked to it. DLT, or Distributed Ledger Technology, is used in Blockchain[5-10]. One system cannot contribute incorrect or unlawful blocks to the chain because of this dispersed computer node network. Every time a new block is added to a blockchain, a "cryptographic hash" generated from the contents of the previous block is used to link it to the others. Due to its immutability and use of cryptographic algorithms for secure communication, blockchain is well-suited for trustworthy EHR information exchange. As far as pandemic management is concerned, there are many possible use cases for blockchain-based EHRs. These include tracking down infected or recovered people and managing the supply chain for vaccines as well as other essentials. Other possible use cases include tracking down infected or recovered people.

Historically, all treatment records were kept on paper and filed by hand. Medical documents were also collected and filed from shelves that were specially built to hold the file folders for these records. Things began to change with the introduction of information technology, and records were transferred to a digital medium for storage and retrieval, giving rise to electronic healthcare records systems. Patient records may be readily connected to monitoring devices for collecting and analyzing patient data in the EHR thanks to automated record management. In rapid growth, the EHRs began to utilize production and huge quantities of medical data to maintain that were successful in epidemiological research[3-6]. Requirements for Electronic Health Records the EHR specifications are as follows: The degree to which devices and systems can transmit and translate shared data is referred to as interoperability in EHR. Security and privacy in healthcare are meant to offer patients control over their medical data by allowing them to provide authorizations for the use of such records. Distinguishing confidential information from private information refers to how well providers and patients can communicate or contract together. The medical records of patients must be kept strictly confidential. Medical information should only be available to authorized healthcare professionals and patients under certain circumstances. Patients should be able to control who has access to their data by providing it to themselves. Due to the fact that a patient's treatment is dispersed across many different health care providers, the data is shared with other medical institutions as well as with the government. Maintaining data efficiency and consistency is a key part of maintaining integrity. In EHR, it ensures that no unauthorized usage damages patient data.

EHR technology is helping to solve certain problems, but it's also creating new ones. When security measures aren't taken ahead of time, it's much easier for hackers to get into the system. In order to make advantage of this new method of storing data, employees will need training. Electronic health records (EHRs) store, share, retrieve, and cover a wide range of patient-related medical data that must be kept secure. Several various stakeholders, such as doctors, healthcare workers, pharmacies, insurance agencies, and researchers, must regularly maintain and exchange medical information to promote and improve the state of healthcare facilities. Data transfers need stringent confidentiality and accountability standards depending on the type of data transmission. In the area of healthcare productivity, Blockchain can revolutionize electronic health record exchanges by providing a secure method for medical data sharing via a dispersed peer-to-peer

connection. In order to make the process of comprehending distributed ledger technology easier, the Blockchain method is being suggested as a solution. Health data, insurance billing, and smart contracts will all benefit from advancements in this cutting-edge blockchain technology. Using blockchain technology in healthcare has many advantages, including better record interoperability, improved patient information access, and system monitoring throughout the full life cycle of a device in the blockchain substructure. For improved EHR solutions, blockchain may be utilized in conjunction with other cutting-edge technologies like as the Internet of Things (IoT) and Cloud computing. The security, dependability, immutability, and interoperability aspects of blockchain will be handled by the technology[7-9]. The ability to access patients' medical history is critical for making medication recommendations, and blockchain can provide this. It will be simple to make significant changes to the medical care delivery system's structure.

The structure of this paper is as follows: Section II goes into detail on the work, including the Process and Methods. Section III outlined the issues and offered a solution in the form of a method. Part IV, the last section, gives the conclusion

I. Related works

A blockchain security framework (BSF-EHR) is proposed by Abunadi, I, [11] to store electronic health records (EHRs) efficiently and securely. In addition to providing patients with easy access to comprehensive, consistent information and free use of EHRs, this framework safeguards their privacy and keeps EHRs up to date. The patient may manage, download, and distribute his EHRs autonomously using BSF-EHR. According to the findings of the experiments, BSF-EHR is capable of enabling safe data exchange between users. A key feature of this access control system is its ability to safeguard critical EHR data from outside threats. As an added benefit, the BSF-EHR architecture allows for faster EHR exchange than conventional centralized storage. Blockchain security framework has only been applied to healthcare sector in this case study. Various areas such as the supply chain, the Internet of Things, the education system, logistics and finance will all benefit from using this paradigm.Kim, M et al.[12] developed a secure framework for a blockchain-assisted cloud EHR system. Registration, authentication, uploading of smart contracts, storage of EHRs, EHR request, and uploading of log transactions were all specified in the proposed system. demonstrated that the proposed system protects against a wide range of threats and offers secure mutual authentication, anonymity, and complete forward secrecy to all parties involved. AVISPA simulation proved the proposed scheme's security against MITM and replay attacks. Established that the suggested strategy guarantees patient and medical server mutual authentication using BAN logic is secure. Compared the proposed scheme's security and performance against those of other systems. It's been shown that the suggested system is more efficient and safe than similar solutions. The proposed EHR system may be a good fit for the current healthcare system, since it is both safe and effective. To put the procedure to the test, a realistic collection of simulations must be created.

A new cryptographic primitive was proposed by Hussien, H.M et al.[13] by combining searchable symmetric encryption (SSE) with ciphertext-policy attribute-based encryption (CP-ABE). Smart contracts were also used to achieve efficient and secure control of outsourced encrypted data, data confidentiality by removing trusted private key generators, and multi-keyword searchability. SC-ABSE is protected against the chosen-keyword attack (CKA) and keyword secrecy (KS) in the standard model based on decisional bilinear Diffie–Hellman

hardness assumptions (DBDH) and discrete logarithm issues. Throughput and latency transactions will be evaluated using a common benchmark tool called Caliper under the proposed methodology. SC-ABSE offers a higher throughput and lower latency than conventional healthcare systems while also having longer network life.Medical data exchange has been made possible via the use of cloud storage and encryption, as suggested by Cheng, X, [14]. Create a medical data security storage model based on the blockchain's features. Because of this, an authentication method is developed based on the network entity model that does not overly depend on a trusted third-party center while yet meeting the security standards. An evaluation of the authentication protocol's formal security performance and computing cost was conducted. Need to pay attention to the scheme's security and efficiency.

Distributed ledger technology (DLT) and an Identity Mixer (IdM) are used in PREHEALTH, a privacy-preserving EHR administration system presented by Stamatellis, C et al (Idemix)[15]. The paper presents a Hyperledger Fabric permissioned blockchain implementation as a proof-of-concept. Patient records may be safely stored using the suggested method, and the data will remain anonymous and unlinkable at the same time. Observations of the scheme's efficiency and practicality show that it is both efficient and feasible for large-scale implementation. Idemix credentials of the most recent version must be used for this task.In order to conduct an efficient and secure integer comparison with numerous inner products for inner product encryption, Gaybullaev, T [16] developed a novel vector encoding method. They used the novel encoding technique to create a P2P energy trading system that preserved user anonymity. By thinking about rebidding for the leftover energy, they improved upon the prior procedure even more. We built a prototype consisting of a DSO, smart meters, and a private Ethereum blockchain to evaluate the system's viability, and the results were encouraging. Our research shows that the new encoding method enhances trading activities substantially. For example, gas costs may be further reduced by using the suggested system to handle many matches in a single block. Scalability can be evaluated with additional players and different security rules can be taken into account.

Song, J.G et all [17]but Song present a dynamic pricing model for a smart contract-based P2P energy trading system. To ensure precise execution of trade and maintain immutable transaction records, the smart contract is stored on a blockchain that is shared by all parties. Traditional server-based P2P energy trading systems need significant overheads and expenses to protect against hackers or manipulation. The smart contract keeps track of the current energy level to avoid a resale. Additionally, they develop a dynamic pricing model that allows the DSO to choose between convergence speed and the precision with which supply and demand are balanced inside a microgrid.. A testbed with five prosumers, five consumers, and the DSO serves as the basis for the virtual simulations. When compared to a well-known blockchain-based energy trading system based on bidding, the proposed method saves up to 78% on operating gas.A prototype blockchain and smart contract were used to a patient device–based personal health record system by Kim H et al. [18]. This ecosystem offers efficient and effective decentralized health data management and exchange activities. Authenticity of personal health record data may be verified not only at the overall resource level, but also down to the level of individual data elements and values. This was proven. However, in this prototype system, the block data are generated through an asynchronous on-chain process apart from off-chain transactions for health

data, meaning there are no delays in off-chain data transactions due to the proof-of-authority consensus algorithm's features, which causes a delay during block generation equal to the genesis block's setting. In addition, while validating the patient Avatar's personal health record data, the data verification and return time may be longer since a big message has been sent. Calculate the time needed to hash the data segment, as well as the data alignment technique provided in the DSV.PHRs were applied cross-country by Lee H. et al. (19). PHRs may be efficiently transferred and shared between companies with the help of this platform. It has been shown that the platform is appropriate for PHR sharing and exchange by many users in different countries in the AeHIN. Precision medicine data may be saved and further modeled in the architecture using this approach. Additionally, characteristics of blockchain technology like as distributed node consensus methods, data transfer encryption, and a decentralized network of smart contracts may help guarantee the confidentiality and privacy of PHRs. FHIR, for example, is a worldwide standard that will be needed to guarantee international compatibility of PHR contents The PHR platform is only a concept at this time. The platform is being tested by a select number of users. However, if the number of users increases, it will be necessary to extend the hardware design in order to keep the platform running smoothly. A global data standard like HL7 FHIR will be needed to enable seamless deployment of the PHRs since they would be exchanged and shared across nations and regions.

Chenthara S et al. [20] create a Blockchain-based health chain privacy-preserving architecture called Health chain that keeps e-health data secure, private, scalable, and uncorrupted. Hyperledger fabric is used to create the Blockchain, which is a permissioned distributed ledger system using Hyperledger composer and stores EHRs using IPFS. Additionally, IPFS data is secured using a proprietary cryptographic public key encryption technique to establish a secure blockchain for electronic health data. The study's goal is to provide the groundwork for the development of cybersecurity solutions against cyber-attacks by using the inherent blockchain characteristics and thus contributing to the robustness of healthcare information sharing settings. Results show that healthcare records cannot be traced to unauthorized access because the model only stores an encrypted hash of them, which proves its effectiveness in terms of data security, enhanced privacy, improved scalability of medical records and interoperability and data integrity while sharing and accessing medical records among stakeholders in the health chain network.

II. Challenges and Proposed Technique

The issue that health care systems confront is how to exchange medical data with known and unknown parties while maintaining data integrity and protecting patient privacy. The requirement to keep data secure means that separate electronic health record processes must be maintained. The need of trust is underscored by all of these processes. The medical community has a problem in building trust so that different practitioners may access, modify, and exchange patient data using an authoritative and up-to-date record of diagnoses, medicines, and services. An advantage of adopting blockchain technology is that data security is improved, but no one wants to keep sensitive health data as part of their blockchain implementation. Med Rec does not store' the record directly, but instead encrypts the information so that patients may safely access the records. Metadata like as ownership and authorization are stored in Med Rec, but the patient record is requested later. The need to cryptographically sign and encrypt data, store it in a public chain, and the replication requirements of a distributed

data store make storing vast quantities of data on a blockchain an expensive proposition, both financially and computationally. To understand how blockchain technology works and can benefit healthcare, there is a lot of work to do. As a result of the centralized nature of systems, businesses aren't yet able to fully integrate blockchain to support the new distributed data culture. When it comes to adopting blockchain, one of the biggest challenges businesses have is securing sufficient funding. Executing peer-to-peer blockchain transactions comes with a high cost in terms of speed and efficiency[21-24]. While blockchain technology comes with its own set of issues, it has the potential to play a major role in resolving the healthcare industry's current interoperability and security issues.

The medical and healthcare systems rely heavily on block chain technology. Block chain offers healthcare security as a result of its decentralized and distributed nature. Block chain technology. In the field of human service administration, block chain innovation focuses on providing safe information sharing, information interoperability, adaptability, and rapid charging to various partners. For a variety of reasons, blockchain research has lately piqued the interest of healthcare academics and practitioners. With the advent of BCT, the healthcare system has found practical answers to long-standing problems. Health care is awash with information. To store electronic medical records (also known as electronic health records), every hospital and doctor's office uses a different method. We're losing money, and it's causing burnout among our workforce. It's even costing people their lives. All of these puzzle parts can be put together in real time with the assistance of blockchain. Thus, health care professionals will be aware of the patient's entire medical history. To profit from a blockchain-based medical record in health care, The most difficult technological problems, such as security breaches and concerns with personal privacy, remain. When it comes to applicable medical areas where patients' personal health information is being handled via the network, this is an especially delicate topic. The Dynamic Chain medical blockchain solution we propose is built on top of web-based software for dealing with EHR that uses the flask programming language together with HTML5, CSS3, bootstrap 4, and mongodb It enables the administration, the doctor, and the patient to carry out their respective operations with ease. Cloud servers store the information, and blocks with hashes generated using medical record characteristics and holding prior Hashes and time stamps are formed from that block.

2. CONCLUSION

This study examined how blockchain technology may benefit the healthcare industry and how electronic health records can benefit from its usage. Secure record storage in conjunction with granular access restrictions for those documents make up the blockchain architecture. And the framework offers methods to guarantee that the system deals with the issue of data storage when it makes use of off-chain storage. The interoperability issues within the healthcare sector are exacerbated by blockchain technology. The health blockchain and health IT systems share data. The interoperability issues within the healthcare sector are exacerbated by blockchain technology. Studies have demonstrated that electronic health records play a critical role in the healthcare system and in its implementation. EHRs Patient safety, increased access to health care services, and lower medical expenses are all reasons for implementing EHR in the healthcare system. Patient safety is also a consideration.

3. REFERENCES

1. R. Klitzman, "“Patient-time”, “doctor-time”, and “institution-time”: Perceptions and definitions of time among doctors who become patients", Patient Education and Counseling, vol. 66, no. 2, pp. 147-155, 2007. Available: 10.1016/j.pec.2006.10.005.
2. T. Gunter and N. Terry, "The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions", Journal of Medical Internet Research, vol. 7, no. 1, p. e3, 2005. Available: 10.2196/jmir.7.1.e3.
3. S. Hufnagel, "National Electronic Health Record Interoperability Chronology", Military Medicine, vol. 174, no. 5, pp. 35-42, 2009. Available: 10.7205/milmed-d-03-9708.
4. R. Evans, "Electronic Health Records: Then, Now, and in the Future", Yearbook of Medical Informatics, vol. 25, no. 01, pp. S48-S61, 2016. Available: 10.15265/iys-2016-s006.
5. E. Bertino, R. Deng, X. Huang and J. Zhou, "Security and privacy of electronic health information systems", International Journal of Information Security, vol. 14, no. 6, pp. 485-486, 2015. Available: 10.1007/s10207-015- 0303-z.
6. J. Fernández-Alemán, I. Señor, P. Lozoya and A. Toval, "Security and privacy in electronic health records: A systematic literature review", Journal of Biomedical Informatics, vol. 46, no. 3, pp. 541-562, 2013. Available: 10.1016/j.jbi.2012.12.003.
7. M. Crosby, P. Pattanayak, S. Verma and V. Kalyanaram, Blockchain Technology. 2019.
8. G. Karame and S. Capkun, "Blockchain Security and Privacy", IEEE Security & Privacy, vol. 16, no. 4, pp. 11- 12, 2018. Available: 10.1109/msp.2018.3111241.
9. J. Yli-Huumo, D. Ko, S. Choi, S. Park and K. Smolander, "Where Is Current Research on Blockchain Technology?—A Systematic Review", PLOS ONE, vol. 11, no. 10, p. e0163477, 2016. Available: 10.1371/journal.pone.0163477.
10. Y. Tribis, A. El Bouchti and H. Bouayad, "Supply Chain Management based on Blockchain: A Systematic Mapping Study", MATEC Web of Conferences, vol. 200, p. 00020, 2018. Available: 10.1051/matecconf/20182000002
11. Abunadi, I.; Kumar, R.L. BSF-EHR: Blockchain Security Framework for Electronic Health Records of Patients. *Sensors* **2021**, *21*, 2865.
12. Kim, M.; Yu, S.; Lee, J.; Park, Y.; Park, Y. Design of Secure Protocol for Cloud-Assisted Electronic Health Record System Using Blockchain. *Sensors* **2020**, *20*, 2913.
13. Hussien, H.M.; Yasin, S.M.; Udzir, N.I.; Ninggal, M.I.H. Blockchain-Based Access Control Scheme for Secure Shared Personal Health Records over Decentralized Storage. *Sensors* **2021**, *21*, 2462.
14. Cheng, X., Chen, F., Xie, D. *et al.* Design of a Secure Medical Data Sharing Scheme Based on Blockchain. *J Med Syst* **44,** 52 (2020).
15. Stamatellis, C.; Papadopoulos, P.; Pitropakis, N.; Katsikas, S.; Buchanan, W.J. A Privacy-Preserving Healthcare Framework Using Hyperledger Fabric. *Sensors* **2020**, *20*, 6587.
16. Gaybullaev, T.; Kwon, H.-Y.; Kim, T.; Lee, M.-K. Efficient and Privacy-Preserving Energy Trading

on Blockchain Using Dual Binary Encoding for Inner Product Encryption. *Sensors* **2021**, *21*, 2024.

17. Song, J.G.; Kang, E.s.; Shin, H.W.; Jang, J.W. A Smart Contract-Based P2P Energy Trading System with Dynamic Pricing on Ethereum Blockchain. *Sensors* **2021**, *21*, 1985.
18. Kim H, Ku H, Yoo K, Lee S, Park J, Kim H, Kim K, Chung M, Lee K, Kim J Smart Decentralization of Personal Health Records with Physician Apps and Helper Agents on Blockchain: Platform Design and Implementation Study JMIR Med Inform 2021;9(6):e26230: 10.2196/26230.
19. Lee H, Kung H, Udayasankaran J, Kijsanayotin B, B Marcelo A, Chao L, Hsu CAn Architecture and Management Platform for Blockchain-Based Personal Health Record Exchange: Development and Usability StudyJ Med Internet Res 2020;22(6):e16748DOI: 10.2196/16748.
20. Chenthara S, Ahmed K, Wang H, Whittaker F, Chen Z (2020) Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. PLoS ONE 15(12): e0243043.
21. T. Salman, M. Zolanvari, A. Erbad, R. Jain and M. Samaka, "Security Services Using Blockchains: A State of the Art Survey", IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 858-880, 2019. Available: 10.1109/comst.2018.2863956.
22. M. Atzori, "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?", SSRN Electronic Journal, 2015. Available: 10.2139/ssrn.2709713.
23. J. Vora et al., "BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records", in 2018 IEEE Globecom Workshops (GC Wkshps), 2019.
24. Veeramani, Vijayakumar & Sabarivelan, K.M. & Tamizhselvan, J. & Ranjith, B. & B., Varunkumar. (2019). Utlization of Blockchain in Medical Healthcare Record using Hyperledger Fabric. International Journal of Research in Advent Technology. 7. 414-419. 10.32622/ijrat.74201922.