ISSN : 2347 - 2243

Indo - American Journal of Life Sciences and Biotechnology

www.iajlb.com
Email : editor@iajlb.com or iajlb.editor@gamil.com

Indo-American Journal of Life Sciences and Biotechnology

Vol. 9, Issue. 2, June 2021

Data Sharing and Privacy Preserving of Medical Records Using Block chain

Sungulurukirankumar[1],N.VamsiPraveen[2]

ABSTRACT

Because of privacy concerns and the fear that others may gain an advantage from the exchange of information, transferring medical records from one facility to another has traditionally been a difficult operation for the healthcare industry. This is changing, however.

Health care organisations are unable to get long-term patient information because of inconsistent policies and permissions granted. When it comes to detecting medical conditions, the ability to share electronic health records will aid in improving diagnostic accuracy. Blockchain technology is recommended in this system in order to improve patient data security and prevent medical records from being lost or manipulated. Block chain for healthcare is a method of securely sharing and preserving medical records with other organisations without the risk of them being tampered with, and the purpose of this survey is to learn more about how the technology works and how it may be used in this context (smart contracts and concept of mining).

Keywords:-Members of the mining community are also known as "miners" in this context.

INTRODUCTION

In systems where security and privacy are a concern, electronic health data exchange will help to improve the accuracy of categorization.

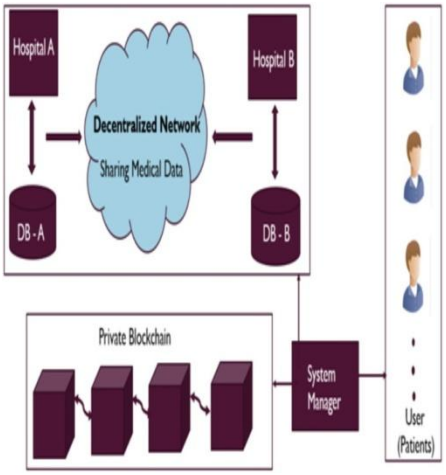
Recently, block chain has been considered a viable solution to achieve the exchange of personal health information (PHI) while maintaining security and privacy, due to its immutability characteristics. Block chain-based data sharing schemes for e-Health systems are proposed in this paper. The block chain will include everything of the patient's medical history, including previous and current therapies, as well as a history of medical problems in the patient's family. This will ensure that no medical records are ever lost or altered since they will be made permanent, transferrable, and easily available. As a promising new distributed architecture for amplifying and supporting the integration of health care data across a

[1]M.techStudent,DepartmentofECE,SiddharthInstituteOfEngineeringAndTechnology,PutturEmail:kirankumar.yits@gmail.com

[2]AssistantProfessor,DepartmentofECE,Siddharthinstituteofengineeringandtechnology,putturEmail:vamsipraveen7@gmail.com

variety of purposes and stakeholders, block chain will take control. Access to electronic health records may be made easier with the use of block chain technology, which provides frictionless connection backed by sound contracts and reliable permission. The original signed note may be compared against a tamperproof ledger of hashes to confirm that it had not been changed.

1. That degree of security cannot be provided by standard information technology. It



is a block chain-based application. Hospital systems from throughout the country have worked together to improve interoperability by exchanging information with each other. However, patient-centered ability carries with it fresh and critical issues and demands surrounding security and privacy, technology, incentives, and governance that must be solved in order for this form of data sharing to function at a large scale. Block chain technology may be able to assist in this transformation by providing mechanisms such as (1) digital access rules, (2) digital data aggregation, (3) data liquidity, (4) patient identification, (5) data immutability. After that, we'll look at obstacles to patient-driven interoperability offered by block chains, including the number of clinical data transactions, privacy and security, and appointment scheduling for patients. While patient-driven ability is an exciting trend in care, given these constraints, it has to be seen whether block chain can aid the move from [7] Institution-centric to patient-focused data exchange, we conclude by adding. There will be three distinct effects of the health care block chain technology. Because of the way these centralised systems interact with one another, patient data ends up dispersed over several locations. Sluggish user interfaces and a lack of trustworthy information might be disastrous. As a result, a block chain-based system must be implemented to store clinically relevant patient data and allow for instant access from anywhere.

2.

3.In a secure local network, only those who have been medically cleared to use the network may access patient information, ensuring that the privacy of patients is protected at all times. Digital patient data prevent medical centres from dispensing medication.

4.Instead of relying on centralised servers to store data from various locations, we can store it locally on each facility's computers. As seen by the recent ransomware attacks on NHS hospitals in the United Kingdom, they are a primary target for hackers. Even if there are no known security threats, there remains the issue of fragmentation. As a result, there has been a recent push toward patient-driven capabilities, in which patient-mediated and patient-driven health data interchange is becoming more commonplace. The following are definitions for words often seen in academic writing:

5.Blockchain: A block chain is a series of linked blocks, each of which holds valuable data

unmonitored by a central authority. It is safe and unchangeable using cryptography.
6.Because there is no central authority overseeing anything, blockchain is referred to be decentralised.
7.Decentralized networks may come to an agreement on some issues via the use of consensus mechanisms.
8. Miners: Those who mine for blocks using their computers' processing power.
9.For a variety of reasons, it's hard to create and maintain a public block chain [4].]

EXISTINGSYSTEM

As a result of the widely diverse and inconsistent data processing techniques used by hospitals and clinics, patient records are often incomplete or inconsistent. Authentication and secrecy are important considerations for health care programmes like MedRec, which make use of the blockchain to make data exchange easier. Due to privacy issues, the transfer of health care data from one institution to another has been a difficult undertaking.

Fear of allowing others to get an unfair advantage by providing information Health care institutions cannot get real-time access to patient data because of inconsistency in policies and agreements. The accuracy of diagnosis may be improved via electronic health record exchange, where security and privacy protection are essential considerations. Healthcare firms must be prepared to build the necessary technological infrastructure before blockchain can have a positive impact on the sector's operations. Block chain is expensive, there are questions about its integration with current technology, and there is a lot of conjecture about how it will be adopted culturally. It's clear that block chain has taken the healthcare industry by storm in the last year, with huge investments in the technology. With so many possibilities, it's no wonder that block chain is quickly becoming one of the most important cornerstones of the digital world's infrastructure. And maybe one day, the big data landscape will be transformed by it. New cost-effective analyses are now available to the public thanks to the release of accountable treatment data and insurance billing information. Auditable e-Health records are provided by our system, while patient privacy and security are also protected. The huge e-Health blocks are available to medical researchers, while government and regulatory organisations are granted extra identities for audit and conformity reasons, as well. Block chain technology will ultimately become widely adopted in e-Health due to a huge number of developers and significant levels of interest in the field. Our method is a decent effort to further enhance the efficiency and dependability inherent in the block chain's design. Additional tailored treatment is made possible by the comprehensive and consistent data blocks accessible to all service providers engaged when computational logics are implemented in e-Health block chains. The e-We're equipped to handle anything from security audits to regulatory compliance reporting to billing updates to notifications from test findings and drug occurrences.
Privateblockchainview

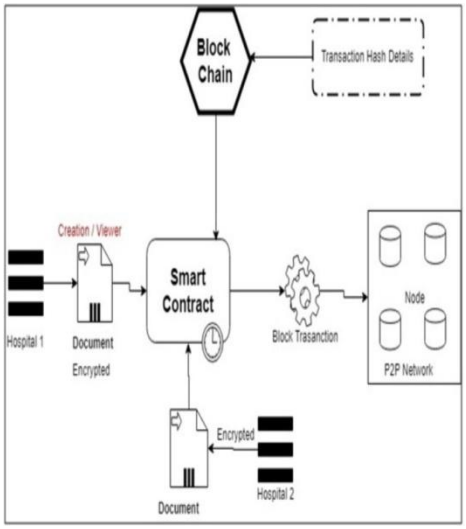
LITERATURESURVEY–

Research on healthcare blockchain began with the following articles.

Open Big Data, IEEE 2nd Int. Conf., p. 6, 2016, MedRec: Using Blockchain for Medical Data Access and Permission Management, Azaria, Ekblaw, Vieira, and Lippman. [1], four primary challenges are addressed by the MedRecblockchain implementation: Patients' agency; better data quality and quantity for medical research; sluggish and fragmented access to medical information. We create a blockchain ledger from a collection of references to various pieces of medical data. The breadcrumb trail of medical history may be traced back to these sources. Our
Individuals are given the opportunity to authenticate, audit, and share their own data

thanks to the system's on-chain permissioning and data integrity logic. For interoperability, we provide strong, modular APIs that may be integrated with the databases of current service providers. This paper has a lot going for it. Key encryption is accomplished via the usage of Public-Key Cryptography. Transactions may be monitored using Smart Contracts. There will be no disclosure of the patient's identity or private health information (PHI). There is no time limit for key access to viewing rights for third parties in this publication, which is a drawback.

TowardsSecure&Privacy-PreservingDataSharinginE-



healthSystemsviaConsortiumBlockchain,It's been published by Springer in June 2018 [2]: Aiqing Zhang XiaodongLin, published in June 2018 by Springer in 2018. Blockchains may be divided into two types, based on their data architecture and consensus mechanisms: private blockchain and consortium blockchain. The PHI is stored on the private blockchain, and the secure indexes of the PHI are recorded on the consortium blockchain. The PHI, keywords, and patient identities are all public key encrypted with keyword search to ensure data security, access control, and privacy preservation. To ensure system availability, block producers are needed to show evidence of conformity before adding new blocks to the blockchains. positive aspects of this work Metadata concerning record ownership and permissions is included in Smart Contracts. Private blockchains for individual hospitals and consortium blockchains for hospitals are both based on the token trapdoor concept. This document has a flaw. Due to the use of several blockchains, there is an increase in storage requirements.

There is also an increase in transaction publication time costs.

Towards Blockchain for Health-CareSystems-Public key cryptography and bilinear pairing technology are used in the work of Hsin-Te Wu and Chun-Wei Tsai, published in IEEE in June 2018 [3]. In order to avoid the identification of a specific patient, a set of anonymous IDs is produced together with a shared secret key. Wearable gadgets and an Android app are used to capture real-time data. This paper's main flaw is the lack of a system manager to track all of the keys. Centralized database administration is employed in private hospitals. A whole healthcare blockchain system has been developed. The database where the organization's medical records are housed contains all of such information.

SecureAttribute-BasedSignatureSchemewith Multiple Authorities for Blockchainin Electronic Health Records Systems R.GUO,H.SHI,Q.ZHAO,andD.ZHENG, Vol. 12, 2018 [4] of IEEE These EHRs have been encased in blockchain, and to ensure their authenticity, we provide an attribute-based signature system with additional proof other than his attestation. As a result, the escrow issue is avoided and the blockchain's distributed data storage method is adhered to by numerous authorities that produce and disseminate the patient's public/private keys. Corruption attacks from corrupted authorities can only be prevented by sharing the secret pseudorandom function seed with other authorities. This paper has a lot going for it. Multi-authority safeguards the confidentiality of data and the identification of patients. The problem with this study is that as the number of authorities and the attributes of the patient rise, so does the expense of the procedure..

AdvancedBlock-ChainArchitecturefore-HealthSystemsT.Mundie,w.liu,szhu,T.

In June 2017, Mundie was published in IEEE. It is described in [5] as a novel system solution for safe and efficient medical record exchanges on our blockchain architecture. Advancement in healthcare and changing social standards necessitated the development of Advanced Block-Chain (ABC). while yet protecting the privacy and security of patients, providing auditable e-health records Researchers in the medical field may access the enormous e-Health blocks, while government and regulatory organisations are granted extra IDs for audit and compliance reasons. If you need it, the e-Health Advanced Block Chain engine is ready to handle embedded security audits as well as reporting on regulatory compliance as well as billing changes and notifications from test findings and medication occurrences.

PROPOSEDSYSTEM

Smart contract-based blockchain-based P2P medical records sharing system diagram

When a customer seeks access to patient records, the system will begin mining the dataOnce they've been processed, the private data records may be exchanged directly between service providers and customers across a block chain. In order to protect the privacy of the patient, it is essential that the patient's identity be kept secret and that access to the patient's data is only permitted after the patient has given their consent. [3] [5]

There are three ways in which the health care block chain will be utilised:

The location of a patient's medical records in a Ledger.

2. Smart Contracts to identify who has access to the data in question.

To guarantee that only authorised parties have access to the data, key pairs are used.

The purpose of this research is to identify and analyse the pain spots in the healthcare industry, and then utilise the principles of blockchain to implement a solution. In addition to providing patients with a full, unalterable record of their medical history, it also makes it simple for them to access that data from many healthcare providers and treatment facilities. By using unique blockchain features, MedRec ensures that sensitive information is protected from tampering and unauthorised disclosure. Tokens may be created on blockchains, particularly Smart Contract-enabled blockchains like Ethereum ", it's a. For the sake of this discussion, we'll refer to tokens as "new digital currencies" whose laws are quite flexible. There is a token economy since those tokens may be traded for other tokens on the blockchain. It is possible to generate millions of dollars in only a few minutes via Initial Coin Offerings (ICOs), which allow anybody to launch an auction for tokens (or coins) they have developed. It's possible to specify restrictions for how the money may be used, and the smart contract itself enforces those rules. Because everyone is aware of how the contract will operate, there is more room for trust. Using'reputation systems' is another important feature of decentralisation "which may be implemented on a computer

Transparent use of blockchains. Medical researchers might be rewarded with tokens of reputation, based on the quality of their work, in a marketplace for medical research. Reputation-based diagnostics are a natural extension of this; a patient answers targeted questions and supplies his medical data, and a pool of trustworthy physicians delivers independent diagnoses and collaboratively agree on a diagnosis. Machine learning methods like DeepMind Health may be used to further improve this. Additionally, a healthcare prediction market might be developed where players who are more often than not accurate in their predictions are compensated openly for their work in the field.

CONCLUSION

Asymmetric key cryptography, public key cryptography, SHA 256, attribute-based encryption, and other approaches were studied in conjunction with blockchain principles and techniques. Medical records were typically

housed in the cloud or in an individual database, and exchanging them was time-consuming and vulnerable to assault. The system will be more secure than the current method since it uses blockchain technology to facilitate the transfer of medical data across companies. In order to further enhance the security of the system, other security approaches, such as encryption and cryptographic ones, will be investigated.

REFERENCES

MedRec: Using Blockchain for Medical Data Access and Permission Management" by Azaria, A. Ekblaw, T. Vieira, and A. Lippman, was presented at the IEEE 2nd International Conference on Open Big Data in 2016.

1."Secure Attribute-Based Signature Scheme with Multiple Authority for Blockchain in Electronic Health Records Systems" by R. GUO, H. SHI, Q. ZHAO, and D. ZHENG is published in the IEEE, vol. 12, 2018.

Online Medical Pre-Diagnosis Framework Using Nonlinear SVM for Efficient and Privacy-Preserving Online Medical Pre-Diagnosis," IEEE Journal of Biomedical and Health Information, vol. 12, H. Zhu et al

2.SupriyaThakurAras,VrushaliKulkarni, \BlockchainandItsApplications-ADetailedSurvey", International Journal of Computer Ap-plications(0975-8887)Volume180,No.3, December2017

Journal of Medical Systems Springer: "MedBlock: Secure and Efficient Medical Data Sharing through Blockchain," by Kai Fan, Shangyang Wang &YanhuiRen&Hui Li&Yintang Yang June 12th, 2018

3."HealthShare: Using Attribute-Based Encryption for Secure Data Sharing Between Multiple Clouds" by AntonisMichalas and Noam Weingarten "

4.International Symposium on Computer-Based Medical Systems, IEEE 1063-7125/17

5.This paper is titled "BMPLS: Blockchain-Based Multi-Level Privacy-Preserving Location Scheme for Telecare Medical Information Systems" and was written by Junwei Zhang, Jianfeng Ma, Chao Yang, Xin Yao, and YaxianJi ", a Springer Nature company june 18th, 2018

Ms. HarleenKaur, M. AfsharAlam, RoshanJameel, Ashish Kumar Mourya, and Victor Chang, A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment,' part of the Springer Nature series june 26th, 2018

6.There are ten authors listed in the paper titled "Blockchain-Based Data Preservation System for Medical Data," which was published in the Journal of the American Medical Informatics Association ", a Springer Nature 2018 publication.

7.Jiaping Lin, JianweiNiu, Hui Li, PCD: A Privacy-preserving Predictive Clinical Decision Scheme with E-Health Big Data Based on RNNs "Computer Communications, IEEE, 2017, 978-1-5386-2784-6.