Cryptosystem For Securing Medical Data Sharing Using Blockchain Technology

Pratiksha M Javali[1], Gowrishankar[2]

[1] PG Scholar, Department of Computer Science and Engineering, BMS College of Engineering
[2] Professor, Department of Computer Science and Engineering, BMS College of Engineering

---***---

Abstract - In this digitalized world of healthcare, it is of the great importance that accurate knowledge distributed through medical services entities be used to further interpret information inside and out and to provide personalized medical services. Electronic medical data provide important preferences over paper-based health records in terms of capacity and recovery. In any case, the majority of currently available medical data sharing plans include risks of security, like being vulnerable to tampering with data and fraud, and will not promote the capability to confirm the trustworthiness of the source for information. Blockchain, as an open ledger characterized by its transparency, tamper-proofing, lack of confidence and decentralization, might give assistance in building a secure trade in patients in intensive care units.

Initially, medical data that has been encrypted is stored within the cloud, as well as address of storage and health records are stored in the blockchain, which will facilitate effective storage and reduce the risk of irreparable damage alteration of the information. Second, the proposed system incorporates Secure Hash algorithm (SHA-256) that ensures the in many communications, medical data is shared. Finally, it emerges from the review that this method meets the criteria for privacy and cannot be forged within the random oracle paradigm, which the proposed system provides more computational execution than different comparative plans.

Key Words: Electronic Medical data, Secure Hash Algorithm, signature key, confidentiality, Blockchain.

1.INTRODUCTION

In traditional publication, patient documents are kept in medical records like personal medical history, medications, immunizations, clinical reports, medical photos, and family history of hereditary diseases. However, sharing medical evidence on paper between two or more medical institutions was very difficult and time taking. The approach to this challenge is to share the medical records of the patient online. Medical records in digitalized format allows abiding storage and on requirement processing of medical data and can allow doctors to diagnose patients' diseases more accurately. However the growing volume of medical data needs expensive overhead storage. When electronic medical data is spread through an open network of various medical facilities, tampering and other types of attacks like surveillance and forgery can be easily carried out.

Cloud storage technologies can keeps large volumes of digitalized medical records with strong processing capacities and relatively inexpensive. Many number of users and medical institutions upload using the cloud for storage and distribution of medical data. This would lower the cost of storing medical information locally and allow individuals to access medical data that has been provided at any time and from any location. Numerous cloud-based approaches for the sharing of medical data have been introduced. To ensure data security, Cheng et al. implemented a method for breaking down big data into a series of structured data list and eventually storing them on a number of cloud servers. Shen et al. implemented a data storage technique that verifies the data, integrity and security of the data, which might identify whether the data has been tampered with before being accessed.

Blockchain is a decentralized internet database system that is still in development, accessibility and non-tamperability of records. In the case of blockchain technologies, we don't need to rely on other companies to store our data securely or to think about data which is not available. Therefore, security problems in the cloud will be avoided. A number of scholars have recently did research on the use of the medical profession, blockchain is being used. To ensure that medical data is shared in a secure manner, Peterson et al.[16] designed a consensus system blockchain - based technologies, but the overhead transmission of the high node consensus

The most sensitive details were provided by the driving force for the use of Blockchain in Healthcare. Digitization helps transfer paper records to a digital medium that will be convenient to store and archive. This digitalized health records are called the Electronic Health Record. It is likely that access and review to health information will be exchanged and in turn, will make it easier for healthcare professionals to view all the patient's medical documents and reduce the burden on patients who carry a handful of documents or test reports with them when they go to the doctor. While these documents have more benefits, there are certain items that need to be considered. These confidential data are the key focus for financial advantage from cyber-attacks. Current technologies cannot resolve the essential policies and technological components needed for national interoperability as identified by the ONC office, as they have limitations on stability, privacy, and interoperability. The usage of this brainstorm technology in the healthcare industry effectively nullifies patient privacy of Confidential Patient Records and the outcomes of clinical testing, unchangeable medical audits, eliminates uncertainty and costs, guarantees data protection and regulatory enforcement, facilitates trustless communication, and generates safe and immutable information.

Also, as result, in order to improve security protections to prevent data leakage, most hospitals and healthcare providers want to construct their networks in a protective boundary for a personal domain, for example, firewalls and vulnerability scanning are installed on a private network. This has contributed to the development of today's medical data silos, which are spread around numerous healthcare facilities, restricting collaborative healthcare and medical research. In this paper, it is open framework for the sharing of medical data utilizing the blockchain technology and cloud storage, which allows a large number of users to exchange and view medical information concurrently and fulfils the criteria for privacy, transparency, non-tamperability, confidentiality and verifiability at the same time.

2. STUDY ON MEDICAL DATA MANAGEMENT

A. Blockchain in Healthcare

Electronic Medical Records (EMRs) were not intended to manage a multi-hospital, lifetime medical data of patients. Patients leave data dispersed around various organizations as activities in life drive them away from one healthcare center to another. They will lose access to past records as a result of doing so. Patients interact with a variety of health-care professionals throughout their life, including physicians, specialists, dentists, dieticians, and others. They leave their medical records scattered amongst these many healthcare systems. Patients' confidential and sensitive healthcare data is stored in vast volumes by both public and commercial healthcare institutions. Individuals have no control on how their medical data is stored, utilized, or shared. Because blockchain fosters trust, it has the potential to improve healthcare data storage. Recently, usage of blockchain technologies becoming a mainstream a recent development in distributed computing, a vast number of researchers are now exploring using blockchain to protect the distribution and management of medical data. In addition, we divide these systems into two types: permissioned blockchain ways and permission less blockchain approaches. Christine V. Helliar explained barriers and transmitted drivers affiliated with illegal and approved blockchains, trying to decide if the obstacles and drivers are the same or new, and if they alter in the long run. The research was performed in two phases: (i) 2016 interviews exploring obstacles and diffusion drivers; and (ii) a research project for the year 2019of the approved blockchain of the wine business in Italy.

1.Permissioned Blockchain Approaches

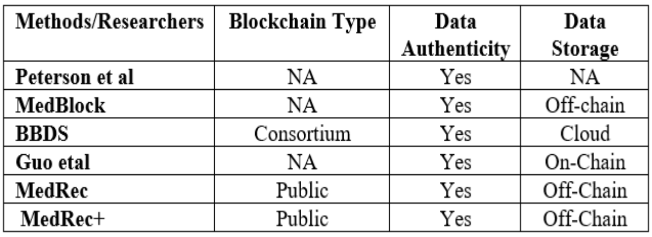
Denis Kirillov [2]. Due to exponential growth of technology based on distributed ledgers and their ability to address current issues, we suggest an updated protocol to the previously voting system, blockchain technology is added to that list to enhance participant's confidence in one another. The Permissioned Blockchain solution allows the simultaneous both votes are cast conventional traditional voting and electronic voting to be carried out. In this article, we define the architecture of this approach, explore its deployment on the Hyperledger Fabric network and demonstrate its features. The Chain [1] Anchor scheme offers anonymous identity authentication for individuals executing transactions in an approved blockchain. The method uses Improved Privacy ID (EPID) a evidence with zero knowledge scheme to show the secrecy and membership of the applicants. Fan et al. introduced MedBlock [3][4], a hybrid blockchain system for securing electronic medical records (EMRs), with nodes segregated into endorsers, orders, and committers. The PBFT Consensus Protocol is a subset of the Consensus Protocol. Although authors have not clearly stated whether or not third-party researchers would have access to medical records, Furthermore, their plan to use of encryption that is not symmetric methods to encrypt medical data does not appear to be a smart idea. choice given the efficiency of asymmetric encryption. Wang et al. [7] introduced a parallel healthcare system (PHS) in which artificial networks, statistical testing, and parallel executions are used to conduct descriptive, predictive, and prescriptive intelligence in healthcare. Under their system, a blockchain consortium comprising patients, doctors, health and government offices and researchers in medicine are being implemented. Smart contracts are placed in place to allow the exchange, analysis and examination of medical records. Xia et al. introduced BBDS [10] [12], a high-level blockchain system that enables data consumers and owners for accessing public registry medical information after successfully checking their identity and keys. The protocol for Identity-Based authentication and Key Agreement in [11] was used for the authentication of user membership. However, the safe exchange of confidential medical knowledge is restricted to invited and confirmed participants.

2.Permissionless Blockchain Approaches

These blockchains, sometimes referred to as private blockchains, might be regarded of similar to closed environments only that can be allowed by those who have been granted access. Any individual who wishes to approve transactions or evaluate information on behalf of the organization must get a central authority's approval. This is beneficial for businesses, banks, and organizations who are confident in their ability to comply with rules and are worried about maintaining total control over their data. Ripple is the epitome of with permission blockchain. Anyone may transact and participate as a verifier on these blockchains, which are commonly referred to as public blockchains. The information on these blockchains is open to the public, and entire replica of the ledgers are kept in various locations across the world. This makes these systems censorship and hacking are tough to get by. This blockchain is not controlled by anyone, and users may continue to exist largely anonymous because they do not need to identify themselves in order to obtain an address and conduct transactions.

In an unauthorized blockchain, transaction hashing blocks rely on the effort of a large number of anonymous miners who compete to solve difficult mathematical algorithms for transaction blocks through trial and error. Modelchain [5] was developed to apply blockchain to privacy-preserving machine learning in order to simplify medical research and promote quality assurance. In the architecture, the order of online machine learning is established by a proof-of-information algorithm at the top of the PoW Consensus Protocol to enhance performance and accuracy. Zhao et al. [13] suggested the use of fuzzy vault technologies to provide a simple backup and recovery system for keys for encrypting health signals gathered from body sensor networks (BSNs) and storing on a health blockchain. But the work proposed by them lacks information of how their wellness blockchain functions

Table 1: Surveyed Methods Metrics



Methods/Researchers	Blockchain Type	Data Authenticity	Data Storage
Peterson et al	NA	Yes	NA
MedBlock	NA	Yes	Off-chain
BBDS	Consortium	Yes	Cloud
Guo etal	NA	Yes	On-Chain
MedRec	Public	Yes	Off-Chain
MedRec+	Public	Yes	Off-Chain

B. Cloud and Cryptography in Healthcare

Considering that people and cloud services typically belong to separate managerial or security realms, the challenge of cloud-based sharing of data is determined on how much trust customers have in cloud service providers. Patient knowledge processing focused on cloud computing poses the same obstacles. Moreover, owing to Health Insurance Portability and Accountability Act [HIPAA's] protection and privacy laws, cross-institutional exchange of medical data becomes much more difficult and demanding. Allowing cloud providers to access keys may theoretically raise the risk of data theft so cloud operators have the opportunity to handle the keys and decrypt them further. Health Insurance Portability and Accountability Act-compliant clouds [6] such as Amazon, Google, and Microsoft, which have externally hosted clouds for the administration of medical knowledge, confront this problem.

Guo et al. [8] a signature based on multiple authorities attributes that combines blockchain technology to guarantee the preservation and access of medical health information. The Attribute Based Encryption signature only shows that the confirmed letter must be signed by a signatory whose characteristics match those requirements that prohibit when a receiver signs a message, their identity is revealed.

C. Through Anonymization Privacy Protection in Healthcare

Data privacy has gained a lot of attention recently, especially with data mining and analysis becoming the dominating technology trend in the big data era. To safeguard the confidentiality of transaction data publishing, the researchers devised a number of data anonymization methods, including generalization-suppressing diversity slices.

There are three distinct categories of privacy- preserving models in general such as K anonymity, L- diversity and T-closeness. In addition to the k -anonymity property, l -diversity is a stronger privacy protection paradigm that requires each sensitive characteristic to in the provided dataset, at least l well-represented values. The t -closeness model is yet another modification of the l -diversity model with privacy protection by decreasing the fineness of data representation, which considers attribute values distinctively by calculating the attribute's value distribution into consideration. It's a trade-off that leads in some data mining losses efficacy in order to gain some privacy.

Various methods aimed at improving these anonymization models have been presented based on these three models. [14] provide in-depth examinations of this topic. Differential privacy introduces noise to the data collection and, in contrast to data anonymization, prevents an attacker from knowing if a certain piece of data is included. To limit noise, Soria-Comas et al. [15] recommend the use of micro aggregate-based k-anonymization, which should be introduced to generate separate individual data sets.

In wireless medical monitoring contexts, Belsis and Pantziou anonymity based on clustering approach for sensor data gathering and aggregation. Loukides et al. provided a method for allowing data owners to communicate personal medical data without reveling their name and other details, incurring major data loss, or jeopardizing data value. Disassociation, a method for separating medical records into deliberately constructed sub records in order to hide diagnostic code combinations, is used in this strategy to manipulate data.

Anonymization of data is still a work in progress. However, a balance must be struck between anonymity and data value. At present, no combination of k-anonymity, l-diversity, or t-closeness can guarantee that no data is leaked while preserving a sufficient amount of data usefulness. In particular, k -anonymity and l -diversity will not preserve anonymity against all attacks [9]. T-closeness, on the other hand, provides perfect privacy but greatly impedes the correlations between key and secret properties.

3. BLOCKCHAIN FOR SHARING MEDICAL INFORMATION

The new framework must give importance to the protection and security of health records. Patients develop trust in their healthcare systems through a tamperproof mechanism that processes their medical records. The new framework should allow patients to manage a single profile in order to keep all their medical records at a minimum of difficulty. Such a method would not only help patients but also clinicians in order to properly assess the condition, since all hospital medical records are available for review.

The proposed method will solve the limitations of the EMR system and improve security by using SHA-256 hashing, AES encryption algorithms along with Blockchain. This device would allow patients to keep their medical records in a safe environment. The scheme would also ensure that only designated individuals have access to sensitive patient records.

The key goal is to ensure security with the "Blockchain Technology" victimization of patient medical records. Privacy or anonymity of patients is one of the key foundations of medicines required. Protecting the patient's personal information is not only a matter of professional respect, it is vital that trust be built between the doctor and the patient. When the patient sees the doctor, the diagnostic data is initially transferred to the EHRs. At the time of user development, AES private key and public key are created by the data owner and encrypted using the AES algorithm. The hash code is generated using the SHA256 algorithm and the hash code is stored in the block header. Previous block hash code is fetched and stored in a block header that allows authentication protocols and algorithms detect data tampering. The block that contains the individual data and the block header is generated.

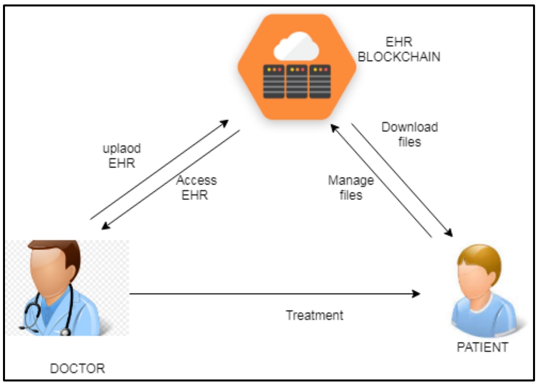


Fig 1: Flow of Medical Data Sharing

A connection is established between the local database and the operating network and the cloud storage server, and an FTP connection is established for file transfer. The created block is uploaded to the cloud storage facility. Ready access to a lot of all-inclusive, up-to-date patient details, fast, accurate and safe. Streamlining health records and efficient resources to take care of, enabling multidisciplinary team activities. Online call service tools, access to top treatments and easier access to doctor's guidance and identification experts. Reduced medical record processing, documentation, repetition and other forms – less time wasted locating unidentified notes, x-rays, admission or discharge preparation.

To protect sensitive information, the United States has adopted the Advanced Encryption Standard (AES) as a standard algorithm for encrypting and decrypting sensitive information. Gives a range of three separate keys, AES-128, 192, and 256 are three different types of encryption that can be 128, 192, or 256 bits. Based on the key length, the number of repetitions in the encryption method is decided, for example, the number of rounds is

- 10 for AES-128,
- 12 for AES-192 and
- 14 for AES-256.

AES uses 10, 12 and 14 rounds. After repeated transformation rounds, plain text is translated to cypher text. This makes information safer in the cloud.

SHA-256 is among the most efficient hash algorithms currently available, and it is one of the successor hash algorithms to SHA-1. SHA-256 is not any harder to write than SHA-1, and it has not been tampered with in any manner. It's a successful AES companion because of the 256-bit key.

The block is a formation that uniquely defines the block. This is accompanied by size of a block containing a block size. As with the Bitcoin header, the block header is hashed with sha256(sha256()). By preserving immutability, the block header is critical to the blockchain network. To spoof the block log, the attacker would have to alter all of the block headers starting with the genesis block. This greatly ensures network stability since there is complete certainty of the impossibility of accomplishing this mission. Mismatch of blocks alerts the device to a suspicious unfolding occurrence that activates data forensics

Table2: Comparison between Symmetric and Asymmetric Algorithms

	DES	AES	RSA	ECC
Factors Contributor	IBM 75	Rijman, Joan	Rivest, Shamir 78	Nal Kolitz, Victor S. Miller
Key Length	56-bits	128,192, and 256	Based on No. of bit in N = p*q	135 bits
Block Size	64-bits	128	Variant	Variant
Security Rate	Not enough	Excellent	Good	Less
Execution Time	Slow	Faster	Slowest	Faster

The 256-bit key makes it a successful AES companion. The header of the block includes the version number that shows the rules of validation to be followed. The prior block hash, which is really a sha256(sha256()) hash, is also included in the header. Its purpose is to make sure that no previous block header may be changed without also altering this one. Merkle root hash is included in the header to ensure that no blocks in the blockchain network may be altered without also altering the header. This is accomplished by adding the output of all occurrences in the blockchain network to the current block. The last performance is a sha256(sha256()). The header contains a time stamp for when the block was formed.

4. THE PROPOSED CRYPTOSYSTEM FOR MEDICAL DATA SHARING

The patient creates the hospital rule for controlling the authority and sends it to them. The patient then uses the Line Secret Sharing Scheme (LSSS) to create a signature of medical-related information. Finally, the patient transmits his or her signature as well as contributing to the data pool of medical information.

The Attribute Authority Organization (AAO) is primarily responsible for providing the patients, users of medical data, and the hospitals with the relevant attribute signature keys (SIKi), transformed key (tk), and private key (d). The CSP primarily stores medical data ciphertext and transmits the ciphertext's address to the blockchain. The data consumers have also given the CSP permission to finish a partially decrypted of the encrypted medical information. The health records cipher text, medical data and its signature are all stored in the blockchain data pool. The consortium blockchain is included into the system to increase the security of medical data. Medical data users, hospitals, and consumers of encrypted medical data are all members of the alliance, which ensures that the information on the blocks is to maintain the security of the blockchain ledger, the network of consensus uses the proof-of-stake (PoS) method in the consensus process. The consensus nodes use the PoS technique to choose the accounting nodes that will be able to actualize the blockchain's distributed consensus. The accounting nodes then transfer the medical information cipher text to the cloud, where they get the data access address. Furthermore, the accounting nodes update the blockchain with the location of cloud medical data storage ciphertext and health information. In the comparison to a distributed server, blockchain provides verifiability, decentralization, and immutability, all of which are important in the system.

Medical data users seek access to their data by providing a list of characteristics to the blockchain system. Data users receive the medical information cipher text address supplied by the node of accounting if the verification is successful. The address and modified key are then sent to the CSP, which is permitted to partly decode the medical data ciphertext. Then, the recovery key is used to completely decode the medical data ciphertext.

5. RESULTS AND DISCUSSION

In this section, we will analyze the cost of computation. The notations used are:

Table 3: Notations used for Computational cost

Notations	**Description**
E	Group G's exponential operations
E_T	Group GT's exponential operations
G and G_T	G and GT are two prime multiplicative cyclic groups p order
E_Z	ring EP's exponential operations
P	the operations of pairing

The computational cost for Encryption is:

$$(n+2)E+E_T$$

The computational cost for Decryption is:

$$P+E_Z+2E_T$$

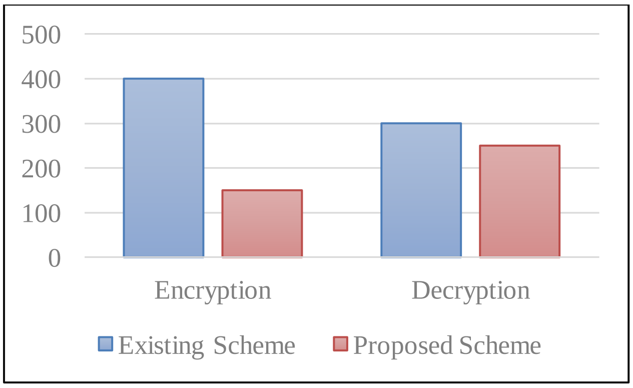


Fig 2: Time in each step is compared with existing system

In comparison to existing systems, the suggested method has lower computing overhead in the encryption and decryption stages, as shown in Fig. 2.

6. CONCLUSION

This paper provides a newesst sharing of health records method that integrates the benefits of cloud storage with the benefits of blockchain technology. Our approach makes use of a encrypted medical data will be stored on a cloud server and a blockchain system to keep track of the address of associated ciphertext for medical data and the data relating to health. As a result, the proposed method meets the immutability and unforgeability criteria. The confidentiality of medical information in the cloud may be protected, and the validity of the source of medical data can be confirmed, thanks to the attribute-based cryptosystem.

ACKNOWLEDGEMENT

This study and the analysis that went into it would not be feasible without Prof. Gowrishankar's invaluable assistance. His passion, expertise, and meticulous attention to detail were an inspirational and helped me stay on track with my job.

REFERENCES

[1] T. Hardjono and A. Pentland, Verifiable anonymous identities and access control in permissioned blockchains, 2019

[2] Kirillov D., Korkhov V., Petrunin V., Makarov M., Khamitov I.M., Dostov V. (2019) Implementation of an E- Voting Scheme Using Hyperledger Fabric Permissioned Blockchain

[3] K. Fan, S. Wang, Y. Ren, H. Li and Y. Yang, "MedBlock: Efficient and secure medical data sharing via blockchain", *J. Med. Syst.*, vol. 42, no. 8, pp. 136-146, 2018

[4] S. Wang et al., "Blockchain-powered parallel healthcare systems based on the ACP approach", IEEE Trans. Comput. Social Syst., vol. 5, no. 4, pp. 942-950, Dec. 2018

[5] T.-T. Kuo and L. Ohno-Machado, Modelchain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks, 2018

[6] Architecting for HIPAA Security and Compliance on Amazon Web Services, *2018*

[7] S. Wang et al., "Blockchain-powered parallel healthcare systems based on the ACP approach", *IEEE Trans. Comput. Social Syst.*, vol. 5, no. 4, pp. 942-950, Dec. 2018

[8] R. Guo, H. Shi, Q. Zhao and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems", *IEEE Access*, vol. 6, pp. 11676-11686, 2018

[9] M. Wang, Z. Jiang, Y. Zhang and H. Yang, "T-closeness slicing: A new privacy-preserving approach for transactional data publishing", *INFORMS J. Comput.*, vol. 30, no. 3, pp. 438-453, 2018.

[10] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa and X. Zhang, "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments", *Information*, vol. 8, no. 2, pp. 44, 2017

[11] L. Wu, Y. Zhang, Y. Xie, A. Alelaiw and J. Shen, "An efficient and secure identity-based authentication and key agreement protocol with user anonymity for mobile devices", *Wireless Pers. Commun.*, vol. 94, no. 4, pp. 3371-3387, 2017

[12] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du and M. Guizani, "MeDShare: Trust-less medical data sharing

among cloud service providers via blockchain", *IEEE Access*, vol. 5, pp. 14757-14767, 2017

[13] H. Zhao, Y. Zhang, Y. Peng and R. Xu, "Lightweight backup and efficient recovery scheme for health blockchain keys", 2017

[14] L. J. Vergara-Laurens, L. G. Jaimes and M. A. Labrador, "Privacy-preserving mechanisms for crowdsensing: Survey and research challenges", *IEEE Internet Things J.*, vol. 4, no. 4, pp. 855-869, Aug. 2017.

[15] D. Sánchez, J. Domingo-Ferrer, S. Martínez and J. Soria-Comas, "Utility-preserving differentially private data releases via individual ranking microaggregation", *Inf. Fusion*, vol. 30, pp. 1-14, Jul. 2016.