Available online @ https://jjem.jnnce.ac.in
https: www.doi.org/10.37314/JJEM.SP0207
Indexed in International Scientific Indexing (ISI)
Impact factor: 1.395 for 2021-22
Published on: 08 December 2024

A secured Medical Data Sharing Using Blockchain Technology

Pavithra K A [1], Sampath Kumar S [2]

Student [1], Assistant Professor [2], Department of Master of Computer Applications
JNN College of Engineering, Shimogga

reddypavithra23junnu@gmail.com, sampathkumar@jnnce.ac.in

Abstract

File storage is perhaps the most well-known and frequently used cloud computing application in the modern world. Yet, if a document is saved in one place in the cloud and synchronized with a computer, it can be accessed by hackers and thus cannot be considered safe. Thus, there is no difference between blockchain and cloud storage and the simple way of looking at it is it can be considered as cloud storage with added security. It means that any node, which is involved in generation of resources, can form the associations with peers if connected to the Internet. This is because block chain information has to be copied and spread across nodes to make certain that agreement is reached and this helps in creating a set database that cannot be changed by nodes in the block chain. The new system will get a user's file, insure it based on IPFS (Inter Planetary File System) and then upload each file to many peers within the network. However, IPFS provides hash values that point to the direction of the file. This hash value will be included in the block chain together with other features of the block. These records are stored in the blockchain and IPFS cloud networks of the 'n' users. Specifically, when a user uploads a specific file to the system, the information is encrypted and uploaded on the IPFS. The file data will be stored in the blockchain and it will be secure and cannot be manipulated. Moreover, during the downloading of a certain version of the file, metadata associated with this file are obtained from the blockchain and used for encryption and the content delivery. The file information is retained and, at the same time, the smart contracts transfer the cryptocurrency (ETH) from the user's wallet to the peer's wallet. The Advanced Encryption Standard (AES) is an encryption technology that enhances protection of data that users store on the cloud.

Keywords: *Blockchain, EHR, Medical data, Security*.

1.Introduction

In the 2008, publication currency in the peer-to digital payment in cash system blockchain innovation was characterized as a periodic block add mechanism and a record for distinct operations conducted using bitcoin the distributed ledger is protected against tampering or damage by the encryption technique used by bit. It heavily utilizes distributed nodes and consensus-building techniques to produce and modify data and it makes extensive use of the database of the blockchain to verify and archive data all of which are safeguarded during transfer and access in addition to being a brand-new open-source computing environment chain is a framework for programming that enables the creation and modification of scripts including

smart contracts via the source code. Listed below represents a few of the features of the digital currency blockchain cryptocurrency removes the need for standard information centres and servers by storing every action on combined

records that are located on every network node the fact that each node is attempting to write to the record indicates that the current setup is dispersed trustworthy source of information the system doesn't need someone else to demonstrate its commonality because there are no obscure mathematical terms or steps everything is clear because the blockchain is autonomous anyone with an internet connection can use it from everywhere in the world however superblock activities will not combine to form composite interactions rather it will stay in the current state. among the reasons the digital currency uses string facts is that the system saves its contents in a time region with a bit value for the SHA 256 encryption technique however because of the fundamental principles underlying the process of consensus including encryption techniques controlling an infinite network is not possible keywords like agreement p2p interactive encryption and intelligent contracts can be used to describe some of the more innovative global computing platforms that use the field of blockchain on cloud servers metadata was intended to be kept for the reason of work scheduling. because several critical difficulties have been resolved the creation of digital file sharing or clinical file sharing systems employing digital currencies would preserve personal data while enhancing the credibility and effectiveness of healthcare offered since the application uses a digital ledger.

2.Related Work

V. L. Lemieux et al.,[1] They Proposed the health records durability safety distribution traceability and accessibility can all be improved with the introduction of blockchain based technologies figure 1 depicts several uses of cloud technology within the healthcare sector.

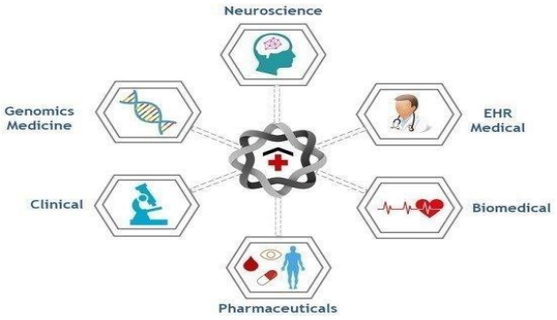

Fig 2. 1: Applications of blockchain in healthcare

A. Khatoon et al., [2] They bring forward the application of wise contracts in the healthcare sector was the primary subject of discussion asma displayed how blockchain determining and intelligent contracts can be used to run a healthcare care administration system she also provided justifications in her article for why centralized management in the health care ecosystem could result in lower transaction costs less administrative work and the elimination of middlemen.

D. Ichikawa, M. Kashiyama et al., [3] They present that primary goal was to be able to record health information in a secure manner based around the blockchain technology by use of appropriate APIs (Application programming interfaces) The Hyperledger fabric leaderboard platform provided us with the ability to transfer this medical data across many devices such as smart phones.

S. Rouhani, L. Butterworth et al.,[4] They suggested ways in which they might independently advance beyond both the classic centralized system represented by Ethereum and blockchain decentralization exemplified by bitcoin.

P. Zhang, J. White et al.,[5] They utilized blockchain software along with clever contracts they noted how they used blockchain computing throughout a broad range of health care applications while indicating out the

obstacles involved in promoting various such networks so that they can interact if superior methods to supply healthcare come into existence.

A. Panwar, V. Bhatnagar et al., [6] They deployed the solution on the IBM cloud using Kubernetes containers for the spotted strategy we recommend the use of the amazons web services with some serverless components paring with serverless means that the owner is charged only for what is used and when there is traffic variation the scalability of the application can be asked for as earlier discussed this leads to relatively stimulated performance this is as we shall find out in the findings section.

Naga Subramanian, G., Sakthivel et al., [7] It runs deploying a sort type ledger system called lockable fingerprints this sort in standardized implies treating medical assets as if they were standards this uniformity relates exclusively to the use of computer files for medical records.

Wang, Yong et al., [8] Ethereum innovation has developed an effective method for identifying boundaries this database within which something exists the right cut went to both informants and those who paid for them and the efficacy of the entire mechanism relied on both sides working together.

Mishra, Rahul et al., [9] This digital computing based technical wellness files is designed developed using great versatility adaptability reduced cost duties the ability to rethink the digitized medical documents has proposed searchable and confirmed blockchain-based e health documents.

Alrebdi, Alabdulatif et al., [10] This blockchain based ds chain paradigm is established over computer health that are electronic in this model the network offers services for confirmation maintenance and search as a result organized administration of technological health systems faces significant challenges because depend solely in one component is not enough to secure records from illegal access or attack.

Zhang et al., [11] These two agreed that using this strategy would allow them to save and classify all of the clients details they utilize the hospitals own network to store client medical details on its internal system yet other blockchain is made accessible outside to ensure their privacy.

Zaria et al., [12] This digital currency called blockchain are able then act to act as mediator in such different electronic welfare records so who they remain accessible even when clients shift from country or welfare insurance company were been working intensively on block chain technology in recent months exploring its potential applications in health care as well.

3.Proposed system

The suggested system for safe medical data sharing based on blockchain technology includes numerous important components that protect data integrity, anonymity, and accessibility. Initially, users, particularly patients, doctors, and healthcare professionals, can create an account or log in to the system using a strong authentication process that incorporates multiple authentication methods and role-based permissions. Only authorized individuals can upload medical files such patient records and evaluate the results using a secure interface, which collects metadata such as file type and upload timestamp. This information can also be obtained from a variety of sources, such as medical equipment and patient feedback. To preserve the confidentiality of health data, it is encrypted with modern encryption methods, and a hash of the secret data is generated and kept on the blockchain.

This ensures that any manipulation with the data is immediately recognized. To efficiently manage massive volumes of data, the real

encrypted data is stored in off-chain storage options such as the cloud. Access control measures are implemented to manage permits and make sure only authorized users have access to the data. Users can request access to particular medical data via a formal request process that involves an authorization mechanism to guarantee that access is granted correctly. Once a data request is accepted the system uses the blockchain hash to verify the data integrity and validity before decrypting it. Decryption is carried out utilizing secure key extraction techniques to make sure that the data is safeguarded throughout the process.

Finally, the decoded information becomes available for health tasks such as evaluation, therapy, and study via a simple interface to analyse tools. This solution takes advantage of blockchain technology's characteristics to provide an effective, open reliable system for transmitting clinical information, while guaranteeing client confidentiality patients while allowing permitted people to access data seamlessly.

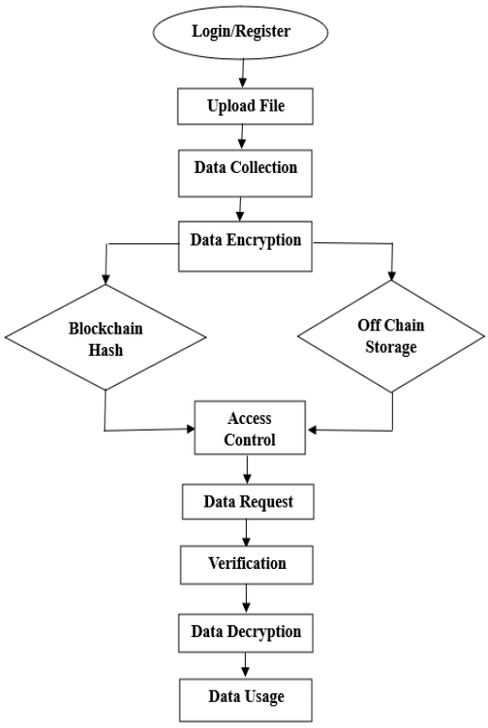

Fig 3.1: Flow Chart of Secured Medical Data Sharing

3.1.1 Existing system

The current solution for safe medical data sharing using the blockchain system generally uses a network of nodes to guarantee the honesty, anonymity, and reliability of data. Medical records are encrypted and kept on a blockchain, that is a public record handled by a collection of servers. Every node in the system stores a duplicate of the record, which is modified and linked using agreement procedures. These agreement techniques, known as proof of work (POW) or proof of stake (POS) assure that just approved payments are submitted to the distributed ledger prohibiting illegal entry and manipulation. Before being stored on the digital ledger, medical information is protected using powerful encryption techniques. The public key infrastructure (PKI) is extensively used with every user having a public and private key pair. The key that is publicly accessible is utilized for encoding and the private key for decoding. This guarantees that only those with permission receive access to the health information. Furthermore, access control techniques are used to set permissions and responsibilities, assuring that private information is only available to those with the correct authorization, such as medical experts and clients. Interoperability is another important aspect of blockchain-based medical data exchange platforms. Different healthcare systems can communicate easily by using smart contracts, which are automated agreements that carry out predetermined actions when certain circumstances are met. These smart contracts can simplify sharing information between various systems, making patient data available across several medical facilities while securing confidentiality and anonymity. In summary, existing blockchain-based medical data sharing solutions take advantage of blockchains decentralized structure to improve privacy, assure data integrity, offer visible audit trails, and allow interoperability across healthcare providers. This strategy tackles many of the

issues raised by traditional centrally managed systems, providing a more reliable and efficient option for performing and distributing private health information.

4.Results and Discussion

The blockchain-based system of sharing files has several advantages over the traditional methods of sharing of files. Following some of the major advantages associated with the same:

Security: Blockchain concerns itself with creating its decentralization platform for handling all kinds of information securely and reliably through cryptographic means. The chain consisted of all computers servicing the Internet.

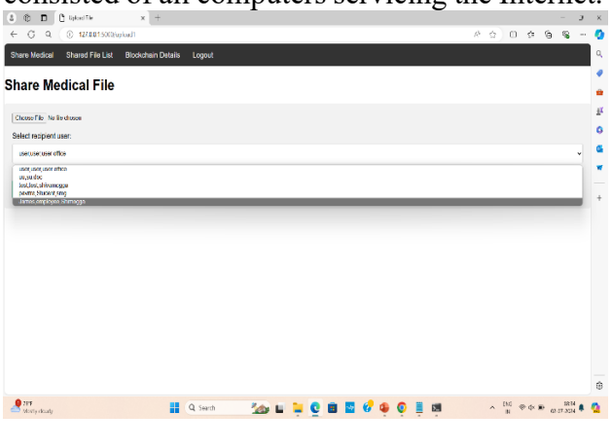

Fig 4.1: Upload File & Select Recipient User

That's because each block on the blockchain spreads out across all networked devices.

Decentralization: Blockchain file sharing can be achieved through decentralization. This makes the whole thing invulnerable against hacking attacks from outside but at the same time eliminates single points of failure within.

Transparency: It simply means that in principle every transaction recorded by the Blockchain must be publicly available so that everyone can find it if they want. This allows documents addressed to us to find their way through quicker if they have actually appeared in print somewhere and brings equality even if no one mentions them anywhere.

Cost-effective: In this regard, block chain technology proved itself extremely cheap compared to classical peer-to-peer systems because everyone shared their expenses.

Immutable: A file handed in at the safe storage facility via blockchain technology cannot ever go missing nor become corrupted. The system guarantees security against unauthorized access or tampering.

Cryptological techniques make it possible to exchange messages reliably between different computers without requiring additional effort. The application of cryptographic techniques allows one to share data between different subsystems by ensuring their authenticity without extra expenditure.

The above Fig 4.1 Shows that, before any data submit or exchange, users (patients, doctors, healthcare providers) must verify by themselves. This is typically done via a multi-factor authentication (also known as MFA) handle involving something the user recognizes (password), a concept the user has (smartphone for OTP), and a concept the user is (biometrics). Once authorized, the user can submit medical data files (e.g., medical records, test results). Before the file is submitted to the blockchain, it is encoded using strong secure algorithms. Usually, this involves: Symmetric Encryption and Asymmetric Encryption. The encrypted file is sent to a distributed storage system that is connected with the blockchain. Instances of such formats involve IPFS (Interplanetary File System). The file's hash (a unique identification) is generated and saved on the blockchain, preserving its confidentiality and allowing the computer to confirm that it has not been interfered with. When choosing a recipient user, the technology must confirm that the receiver has permission to access the specified medical data.

This involves: The system maintains an Access Control List (ACL) that specifies which users have access to which data. This list is recorded on the blockchain to prevent tampering. The sender encrypts the symmetric key used for file encryption with the receiver's public key, ensuring that the data can only be decrypted by the person who was intended.

Conclusion

The suggested method strengthens data security by decentralizing the data among a group of peers linked to the network while encrypting it for instance user data protection at the platform level utilizes the AES 256-bit technique following encoding the IPFS protocol is used to move and store information among various network partners our approach ensures maximum facility use by enabling peers to lease out their spare space in exchange for cryptocurrency addressing concerns about security and privacy associated with central cloud computing better information integrity will be offered by the suggested solution that spreads among many of the users in the system.

References

1. V. L. Lemieux, ―Trusting records: is Blockchain technology the answer? Records Management Journal, vol. 26, no. 2, pp. 110 139, doi: 10.1108/RMJ-12-2015-0042, Jul. 2016.
2. Khatoon, ―A Blockchain-Based Smart Contract System for Healthcare Management, ‖ Electronics (Basel), vol. 9, no. 1, p. 94, doi: 10.3390/electronics9010094, Jan. 2020.
3. D. Ichikawa, M. Kashiyama, and T. Ueno, ―Tamper-Resistant Mobile Health Using Blockchain Technology, ‖ JMIR Mhealth Uhealth, vol. 5, no. 7, p. e111, doi: 10.2196/mhealth.7938, Jul. 2017.
4. S. Rouhani, L. Butterworth, A. D. Simmons, D. G. Humphery, and R. Deters, ―MediChainTM: A Secure Decentralized Medical Data Asset Management System, ‖, doi: 10.1109/Cybermatics_2018.2018.00258, Jan. 2019.
5. P. Zhang, J. White, D. C. Schmidt, and G. Lenz, ―Design of Blockchain Based Apps Using Familiar Software Patterns with a Healthcare Focus, ‖ in Proceedings of the 24th Conference on Pattern Languages of Programs, in PLoP ’17. USA: The Hillside Group, 2017.
6. Panwar, V. Bhatnagar, M. Khari, A. W. Salehi, and G. Gupta, ―A Blockchain Framework to Secure Personal Health Record (PHR) in IBM Cloud-Based Data Lake, ‖ Comput Intell Neurosci, vol.2022, pp.1–19, doi: 10.1155/2022/3045107, Apr. 2022.
7. Naga Subramanian, G., Sakthivel, R.K., Patan, R. et al. Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Comput&Applic32, 639– 647 (2020).
8. Wang, Yong, et al. "Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain." IEEE Access 7: 136704-136719, (2019).
9. Mishra, Rahul, et al. "DS-Chain: A secure and auditable multi-cloud assisted EHR storage model on efficient deletable blockchain." Journal of Industrial Information Integration 100315, (2022).
10. Alrebdi, N., Alabdulatif, A., Iwendi, C. et al. SVBE: searchable and verifiable blockchain based electronic medical records system. Sci Rep12, 266 (2022).
11. A Q Zhang and X D Lin, “Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain,” J Med. Syst., vol.42, pp.140, 2018.
12. Azaeia, A., et al, MedRec: Using Blockchain for Medical Data access and Permission Management. In 2016 2nd International conference on Open and big Data (OBD). 2016.