DataSafeHealth : Healthcare privacy system using blockchain Technology

Mrs. Samrudhi Bhadane,Assistant Professor, Department Of Information Technology,GHRCEM, Pune, India samrudhi.bhadane@raisoni.net

Vikram Kumar, 4rth Year B.Tech. Department Of Information Technology,GHRCEM, Pune. Pune, India vikramkumar225221@gmail.com

Rupesh Ghule, 4rth Year B.Tech. Department Of Information Technology,GHRCEM, Pune. Pune, India rupeshghule70@gmail.com

Manoj Chavan, 4rth Year B.Tech., Department Of Information Technology,GHRCEM, Pune. Pune, India manojchavan9918@gmail.com

Avinash Jadhav, 4rth Year B.Tech., Department Of Information Technology,GHRCEM, Pune, India avijadhav7420008080@gmail.com

Abstract **- The healthcare sector has become crucial for ensuring and privacy since it containssensitive patient data, research information and medical records. The old method of keeping patient data in the healthcare sector is exceedingly insecure and may result in patient health manipulation, which has emerged as a severe problem. Blockchain technology can be used to secure data in ever-evolving ways. Thus, the project seeks to design and implement a user-friendly and secure data storing platform, DataSafeHealth that provides data security, immutability and transparency of medical data. Thisapproach can possibly save survives and decreasehealthcare costs in the long run.**

Keywords : **Blockchain; Hash key.**

I. INTRODUCTION

DataSafeHealth will be based on a blockchain platform designed to securely store medical data from patients. The digitalization of health records has exposed patient data to cyber threats and unauthorized access, destroying trust in healthcare. This platform provides a dynamic space for patients to store their medical data and can grant access to authorized peers. It may affect the treatment you receive from the doctor and your health treatment. This project provides data security, immutability and transparency for medical data. Blockchain technology is found good for Decentralizing Privacy, it can protect personal data. Healthcare data privacy has become a paramount concern in the era of digital health information exchange. The advent of electronic health records (EHRs) and telemedicine platforms has revolutionized healthcare but also exposed patient data to various security risks. Blockchain technology, the backbone of cryptocurrencies and various decentralized applications, relies on cryptographic hashing for securing data and verify transactions. The United Nations-directed Maintainable Development Goal for Health (SDG) is particularly significant for India, considering the multiple obstacles that its huge and varied population faces, because this strategy hasthe potential to save lives and minimize long-term healthcare expenditures.

- Related Work : There have been various attempts to address these privacy issues. Ayushman Bharat HealthAccount (ABHA) is the government application for Health insurance under PM-JAY ‘Prime Minister’s People Health Scheme.

A. Background

The healthcare business has seen a major transition in recent years as a result of the digitalization of patient information, telemedicine, and the incorporation of technology into medical procedures. This digital revolution has brought remarkable benefits in terms of efficiency, accessibility, and the quality of healthcare services. However, it has also raised critical concerns regarding security and privacy of patient’s sensitive medical data.

B. Research Objectives

 DOI : 10.35291/2454-9150.2023.0245

This research paper aims to address the pressing issue of healthcare data privacy and explore the potential of blockchain technology as a solution. Healthcare data privacy is importance as it not only involves safeguarding patients' personal and medical information but also has far-reaching implications for the quality of care, trust in healthcare systems.

II. HEALTHCARE DATA PRIVACY

A. Importance of Healthcare Data Privacy

Healthcare data privacy is the foundation of patient trust and the cornerstone of ethical healthcare practice. It encompasses the safeguarding of individuals' personal and sensitive medical information. Ensuring the privacy of healthcare data is critical for several reasons:

- Patient Faith: Patients are more likely to share correct and detailed data with healthcare providers if they are confident their data will be kept private.
- Ethical Responsibility: Healthcare professionals have a moral and legal duty to protect patient confidentiality.
- Regulatory Compliance: In the United States, laws such as the Health Insurance Portability and Accountability Act (HIPAA) require the security of patient data.
- Data Integrity: Privacy breaches can result in data manipulation, leading to incorrect diagnoses or treatment decisions.

B. Current Challenges and Vulnerabilities

Despite its importance, healthcare data privacy faces several challenges:

- Cybersecurity Threats: Due to the high value of medical data, the healthcare sector is a popular target for hackers.
- Data Breaches: Incidents of data breaches and leaks have increased, exposing millions of patient records.
- Insider Threats: Healthcare employees with access to patient records may abuse their privileges.
- Data Sharing: Sharing data among multiple healthcare entities often lacks a secure, standardized framework.

III. BLOCKCHAIN TECHNOLOGY

A. Understanding Blockchain

Blockchain technology is a distributed and decentralized ledger that enables cryptocurrencies such as Bitcoin. It is made up of a series of blocks, each of which contains a list of transactions. Blockchain's key characteristics include :

- Decentralization : Data is not kept on a single central server but distributed across a network of nodes, making it resistant to a single point of failure.
- Immutability : Once a block is added to the chain, its data is cryptographically sealed and can't be altered, ensuring data integrity.
- Transparency : All participants in the network have entree to the same ledger, creating transparency and trust.
- Security: Strong cryptographic techniques and consensus mechanisms enhance data security.

B. Features Beneficial for Healthcare

Blockchain technology offers several features beneficial for healthcare data:

- Data Integrity: Cryptographic seals and immutability ensure the integrity of patient records, reducing the risk of tampering.
- Decentralization: Removes the need for a central authority, giving patients more control over their data.
- Smart Contracts: Self-executing contracts can automate data access and sharing based on predefined rules.

C. Blockchain in Healthcare

In the context of healthcare, blockchain can be viewed as a framework for improving data security, integrity, and accessibility. It addresses challenges in data sharing, security, and patient consent, making it a promising technology for healthcare data management.

III. How Blockchain Enhances Healthcare Data Privacy :

A. Immutability and Data Integrity

Through cryptographic sealing and immutability, blockchain technology protects data integrity. Once patient data is stored on the blockchain, it cannot be changed or erased without network consensus. This permanence decreases the possibility of illegal data tampering and ensures that medical records are accurate and trustworthy.

B. Decentralization and Data Ownership

Decentralization in blockchain removes the requirement for a central authority to control healthcare data. Patients gain greater ownership and control over their health records, allowing them to grant or revoke access to their information. This not only empowers

 DOI : 10.35291/2454-9150.2023.0245

patients but also limits the potentialfor data misuse.

C. Smart Contracts and Data Access Control

Smart contracts, self-executing code stored on the blockchain technology, enable automated and secure data access control. Patients can set rules for who can access their data and under what conditions. For instance, data can be automatically shared with a healthcare provider upon payment, enhancing privacy and ensuring that data is only used when explicitly permitted.

D. Security and Privacy

Health records can be securely and seamlessly shared across providers while maintaining privacy. This enhances coordination among healthcare professionals withoutcompromising patient data privacy.

IV. BLOCKCHAIN TECHNOLOGY AND ITS DEPENDANCES

This technology was developed by Nakamoto for his well-known work of digital currency or crypto-currency, bitcoin. Nakamoto employed blockchain technology to overcome bitcoin's double spending problem, but the emerging technology was soon used in a number of other applications. Blockchain is a chain of linked blocks that is constantly growing by storing transactions on the blocks. The platform adopts an approach that allows sharing of information, and all shared information, or information as it is known, is common property. Blockchain has some advantages such as security, anonymity, data integrity and no need for third-party intervention. These benefits make storing patient medical information a valuable option as the security of patient information increases as technology in the healthcare industry advances. Treatment is most important. Anumber of researchers have also identified blockchain technology as an achievable solution in healthcare.

A. Architecture :

To understand the blockchain architecture, consider Fig.1, which represents the entire process of a transaction being sent by a user on the blockchain network.

1. A new block is created when a user sends a new transaction request to the blockchain network. Blocks inthe blockchain are used to store transactions, and these blocks are distributed over all network links. Transactions put on a block are broadcast to the whole network. To aid in the authentication process, each node in the network has a copy of the whole blockchain. When the block containing the user's transaction is broadcast to all connections, they verify to ensure that the block has not been tampered with in any manner.

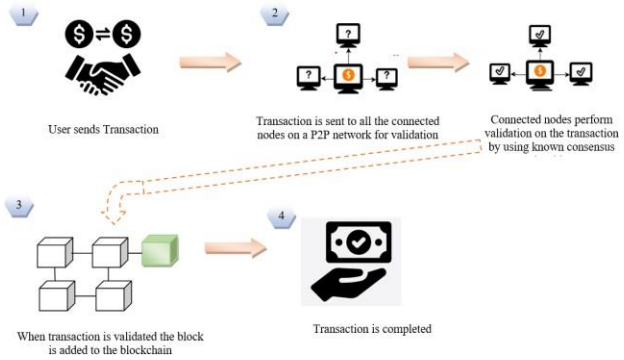


Fig. 1. Blockchain architecture

2. The Nodes handle the whole process of adding blocks to the blockchain until consensus is obtained; nodes decidewhich blocks can and cannot be added to the network. To validate the transaction and guarantee that the senderis a member of the network, several techniques known to the linked network are used. After passing verification, a node is paid with cryptocurrency. Mining refers to the process of validating transactions, andminers are the nodes that undertake this verification.

3. Once verification is complete, the block is added to the blockchain.

Once all verification procedures are completed, the transfer is completed. You can understand some concepts of blockchain technology from the following explanation.

B. Consensus algorithm

Before being added to the blockchain, each block must comply with specific agreements. Blockchain technology employs a consensus algorithm for this purpose. The Proof of Work (PoW) algorithm, which Satoshi Nakamoto used on the Bitcoin network, is the most frequently utilized consensus method. The operating idea of this method is that the blockchain network has many nodes or participants, thus when a member requests an extra transaction in the network, it must be counted. This is known as mining, and the nodes that do these computations are known as miners.

V. BLOCKCHAIN TECHNOLOGY'S CHALLENGES

A. Storage Capacity and Scalability

Storage Capacity and Scalability Data storage on blockchain represents two major issues: privacy and scalability. Information on the blockchain is available to everybody on the chain, leaving it subject to attacks; this is not what a decentralized platform requires. The data saved on the blockchain will comprise the patient's medical history, papers, laboratory findings, x-ray data, MRI results, and many more reports, all of which will influence the chain's storage capacity.

 DOI : 10.35291/2454-9150.2023.0245

B. Lack of social skills

Only a few people understand how blockchain technology works. The technology is still in its infancy, but it is continually evolving. The transition from old systems to blockchain would be time-consuming since it requires the total transformation of numerous healthcare companies.

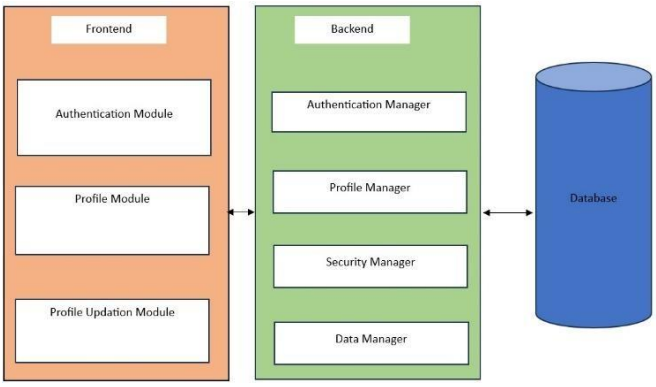
C. Lack of globally accepted standards

There is no concept of a global standard. Because technology is still in its early stages and continually developing, there are no set standards. As a result, using this technology in therapy takes more time and effort. Because it demands worldwide certification requirements while ignoring the technical procedure. The size, kind, and type of data that may be kept on the blockchain will be determined by this model. In addition, updating technology will be easier because standards have been established and it can be simply implemented in organizations.

Benefits	• Decentralized • Data Transparency • Security and Privacy	The blockchain stores data or information that is spread throughout thenetwork. The blockchain protects data against alteration. Blockchain uses encryption algorithms to protect the datastored in it.
Barriers	• Capacity, Storage andScalability • Insufficientsocial skills • a lack of universally defined standards	Large data quantities would result inscalability and storage problems when stored on the blockchain. Since blockchain is a revolutionary technology and goesagainst common sense,it is very difficult tochange the systems used for this technologyin the past. Blockchain technology does not have clear standards and principles for universal use, making it difficult to use it in specific projects.

Table 1. Profits and Blocks of blockchain technology.

VI. SYSTEM DESIGN AND ARCHITECTURE



Hash generator:

A hash generator is a tool or program that takes input data (such as a file, text, or any digital content) and processes itthrough a cryptographic hash function to produce a fixed- size string of characters, which is characteristically a hexadecimal number.

Information validator:

An information validator is a mechanism used to verify theaccuracy, authenticity, integrity, or validity of information, data, or content. Information validation is crucial in variouscontexts, such as data processing, content verification, security, and decision-making.

Recovery Center:

A Recovery Center for 'DataSafeHealth' using blockchaintechnology could serve as a crucial component in ensuringthe integrity, privacy, and security of patients' health information while also providing a backup and recovery mechanism. It can be a specialized node or set of nodes within the blockchain network.

Transaction initiator:

A "transaction initiator" typically refers to an entity or individual that initiates a specific action, update, or interaction related to a patient's health record on the blockchain network.

Report Generator:

A Report Generator can provide a secure and efficient wayto create, access, and share medical reports and patient information while ensuring data privacy and integrity.

Committing transaction:

In a blockchain-based system, "committing a transaction" typically involves the process of securely recording and validating a specific action or update within the blockchainnetwork.

VII. CONCLUSION

Due to the complexity of this field and the need for a stable and effective way to manage information, there are many studies demonstrating the use of blockchain technology in business transactions. Interoperable architectures will certainly play an important role in many business use cases that face similar data exchange and communication. More research on safe and effective software applications for the use of blockchain technology in business is needed to educatesoftware professionals and experts on the resources and methods of this new technology, its limitations, and whether existing blockchains can be used to create distributed applications.

 DOI : 10.35291/2454-9150.2023.0245

VIII. REFERENCES

[1] Anushree Tandon, Amandeep Dhir, A.K.M. Najmul Islam, Matti Mantymaki, 'Blockchain in healthcare: A review literature review, synthesizing framework and future research agenda', Computers in Industry publications, volume 122, November 2020.

[2] Kianoush Kiania, Seyed Mahdi Jameii, Amir Masoud Rahmani,'Blockchain-based privacy and security preserving in electronic heath: a systematic review, by in National Library of medicine which is national center for Biotechnology Information, PMCID: PMC9936121 | PMID:36811000.

[3] Jin Sun, Xiaomin Yao, Shangping Wang, Ying Wu, 'Blockchain-Based secure storage and access a=scheme for electronic medical records in IPFS, IEEE published in the volume 8, pages (59389- 59401), INSPEC Accession Number: 19499371.

[4] Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-Health systems via consortium blockchain", L. Med. Syst., Volume 42, no. 8, page number 140, August 2018.

[5] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao and S. Liu, "Blockchain-based data preservation system for medical data", J. Med. Syst., vol. 42, no. 8, pp. 141, Aug. 2018.

[6] G. Jetley and H. Zhang, ''Electronic health records in IS research: Qualityissues, essential thresholds and remedial actions,'' Decis. Support Syst., vol. 126, pp. 113–137, Nov. 2019.

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

[8] M. Hochman, ''Electronic health records: A ''Quadruple win,'' a ''quadruple failure,'' or simply time for a reboot?'' J. Gen. Int. Med., vol. 33, no. 4, pp. 397–399, Apr. 2018.

[9] Q. Gan and Q. Cao, ''Adoption of electronic health record system: Mul- tiple theoretical perspectives,'' in Proc. 47th Hawaii Int. Conf. Syst. Sci., Jan. 2014, pp. 2716–2724.

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

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

[12] S. T. Argaw, N. E. Bempong, B. Eshaya-Chauvin, and A. Flahault, ''The state of research on cyberattacks against hospitals and available best practice recommendations: A scoping review,'' BMC Med. Inform. Decis.Making, vol. 19, no. 1, p. 10, Dec. 2019.

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

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

[15] ''The future of health care cybersecurity,'' J. Nursing Regulation, vol. 8, no. 4, pp. S29–S31, 2018.

[16] Spatar, O. Kok, N. Basoglu, and T. Daim, ''Adoption factors of electronic health record systems,'' Technol. Soc., vol. 58, Aug. 2019,Art. no. 101144.

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

[18] W. J. Gordon and C. Catalini, ''Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability,'' Comput. Struct. Biotechnol. J., vol. 16, pp. 224– 230, Jan. 2018.

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

[20] T. D. Gunter and N. P. Terry, ''The emergence of national electronic health record architectures in the United States and Australia: Models, costs, and questions,'' J. Med. Internet Res., vol. 7, no. 1, p.3, Jan./Mar. 2005.

[21] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, ''An overviewof blockchain technology: Architecture, consensus, and future trends,'' in Proc. IEEE Int. Congr. Big Data (BigData Congr.), Jun. 2017, pp. 557–564.

[22] Pirtle and J. Ehrenfeld, ''Blockchain for healthcare: The next generation of medical records?'' J. Med. Syst., vol. 42, no. 9, p. 172, Sep. 2018.

 DOI : 10.35291/2454-9150.2023.0245