International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 1s,2025
https://theaspd.com/index.php

Blockchain-Based Secure Storage Of Medical Records

Manish Nandy[1],Sarvaree Bano[2],Ritu Joon[3]
[1]Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India.
ku.manishnandy@kalingauniversity.ac.in;0009-0003-7578-3505
[2]Assistant Professor, Department of Chemistry Kalinga University, Raipur, India.
[3]Assistant Professor, New Delhi Institute of Management, New Delhi, India.;ritu.joon@ndimdelhi.org,
https://orcid.org/0009-0006-4319-6252

Abstract
In today's health organizations, electronic health records are essential. Concerns over reputation and privacy have grown recently in relation to the usage and storage of patient data. One example of social insurance and governance is the data exchanged through health and medical insurance. Patient privacy has been at risk during the last few decades due to a number of problems with the management of medical information. Protecting patient data is a primary concern in the field of intelligent healthcare apps. Blockchain technology may greatly increase security and transparency in medical applications, which is where it comes into play. A safe blockchain infrastructure created especially for handling medical records is suggested in this paper. Healthcare businesses can manage their data in a private and safe manner with this platform. To meet the demands of these institutions, it also recommends a safe method for storing electronic records, guaranteeing privacy and security while handling medical data.

Keywords: *Medical Records, organizations, secure storage system*

INTRODUCTION

The emphasis of the field of Telemedicine is creating various segments that require high-end technical treatments. In spite of the enormous advantages of telemedicine, there are several challenges such as patients' fear and unfamiliarity, inaccessibility, inefficiencies, and technical issues, and government support, including its utility and success [1]. Data breaches can cost organizations $380 per record, but current systems are susceptible to a variety of attacks. Security of the electronic health records (EHRs) and associated personal information is a prime concern in healthcare for hackers to identify correct identity details [9]. Evolving blockchain technologies will be the answer to significant security issues in healthcare. Characteristics such as decentralized storage, encryption and smart contracts equip organizations with infrastructure for strengthening the security of data, without losing accuracy and opening the door for unauthorized access or amendment of information concerning patients [3]. One blockchain can be illegal or legal. Blockchains are technically accessible to any user, without approval or public, but the proprietor will have to accept to become a member of an approved blockchain [2]. Since patient data is extremely sensitive, vetted blockchains are best for healthcare settings. This can lead to problems if permissions are not handled rightfully. Health care experts at present need to have convenient access to patient records, especially during emergencies. Non-uniform permissions can hinder access in situations of urgency, and it can be fatal to the patients [13]. Two transparent, stable solutions for permission management are employed in blockchain technology: Intelligent contracts offer access based on conditions agreed on by all parties involved in a contract. Such controlled access control type can be applied to make a variety of workflows automated [4].

Cryptographic keys put patients' access control under their control. Each patient is given a "master" key to "open" health information and may provide a copy of this key, if needed, to health practitioners or organisations. Activity might be limited to reading or writing content, and patients can cancel keys if a key is disabled. By permitting processes involving one or more middlemen to become automated, intelligent contracts and cryptography keys reduce human error risk and procurement-to-execution time on steps like insurance billing and payment.

REVIEW OF LITERATURE

Some technologies are resiliency-capable, but are in no way fully impenetrable. A never-used piece of code is as vulnerable as a never-published piece of code that has not yet been published. Furthermore, because it is typically accessed by people, information technology is subject to the most security risks, Because of this, the same reason, health technologies are also as concerned about information security as other applications and networks are. DLT is a decentralised ledger technology Distributed ledger technology (DLT) is a collection of replicated data across all nodes or computers in a network. No single authority governs the data; the data validate themselves. Data models like the conformity of transaction validation protocols, together with a ledger data structure determine what is written down in the DLT. It is not an asset ledger. Logic Assets are in transactions, but simultaneously the ledger records the facts regarding the assets. Other examples are: consequently, bitcoin transactions are added to a distributed ledger (as for any other currency exchange) A blockchain does not store single transactions linearly, but a chronological and consecutive block-by-block sequence is stored, one after another. We can also log advanced coding functions on the blockchain through the use of smart contracts. This can imply that one or more transactions would be received by the middleware. Transactions are capable of being grouped to enhance the transaction rate per second on a blockchain given a given block throughput. When every block's timestamp is written on the chain, a reference to the last block is added. Employing Merkle tree hashes: The hash tree of all the transaction hashes is Merkle root It is a hash value that signifies a one-time unique value Nonces are solved by miners to form a new block. The hashing function has been used on a few more numbers, and finds they sum up to the target amount needed. It is worth noting that this figure is linked with consensus algorithms. [5].

MATERIALS AND METHODS

This paper presents a secure blockchain platform for the healthcare records management system based on the design science methodology. Blockchain network, smart contracts, privacy key management, data encryption, and integration with medical IT comprise the five components of the proposed design. Increasing data security, interoperability, privacy, traceability, and accuracy are just some advantages of developing a secure blockchain platform for medical record management [11].

In the present healthcare systems, the health records are kept in centralized databases in silos and thus healthcare data become a highly vulnerable target for the attackers. Various existing research studies indicate that the storage of health information in centralized databases raises the risk of security threats and demands assistance from trusted third parties Saleh, I. K. (2022). Adaptive Disassembly Using Deep Reinforcement Learning Using Path Planning Communication Approach. *International Journal of Advances in Engineering and Emerging Technology*, *13*(2), 110–119. [10]. The centralized databases put us at risk of an attack, becomes escalated into cyber attacks and impedes the privacy and security of EHRs. Interoperability among healthcare service providers is yet another primary challenge for the healthcare sector due to differences in format and standards [8]. The health information in the widespread systems are in pieces and is difficult to transfer to healthcare providers or stakeholders [6]. It is hard to collect and analyze patient information. It also inhibits the effectiveness of EHR sharing during emergencies. There needs to be a tamper-proof system that everyone who is authorized can access.

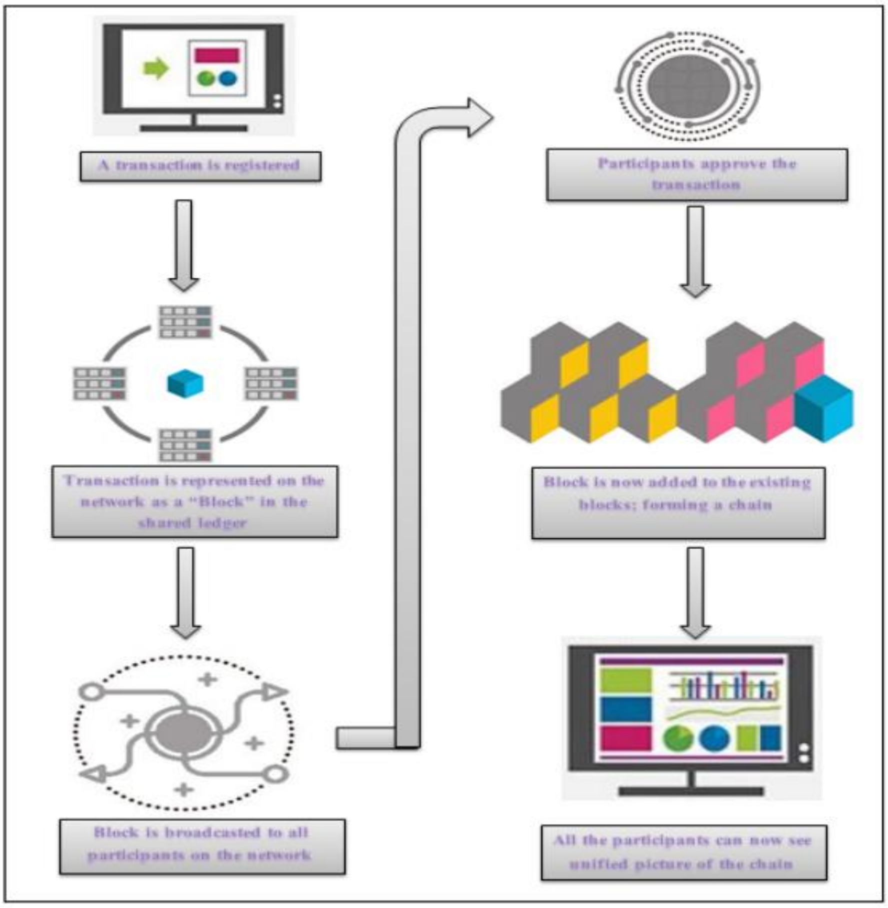

A transaction is registered
Transaction is represented on the network as a "Block" in the shared ledger
Block is broadcasted to all participants on the network
Participants approve the transaction
Block is now added to the existing blocks; forming a chain
All the participants can now see unified picture of the chain

Figure 1: Working of Blockchain

A conventional database system fulfills these needs partially and therefore other means of prevention from attacks need to be sought. Conditional access of patient records by doctors, pharmacies and laboratories instead of complete access is extremely important to maintain patient's health information privacy [7]. In addition, under the current system, patients have no complete control over the health records as it is handled by the hospital administration. Given the fragile character of healthcare data, effective data sharing among stakeholders in a public space is a complex and burdensome process. In spite of the wonderful attributes, the current healthcare sector is not capable enough to offer an effective means of storing, sharing and analyzing the health data in a globally consolidated manner.

RESULT AND DISCUSSION

A successful and happy life is based on leading a healthy lifestyle, and medical technology has greatly contributed to people's modern sense of fulfilment and enjoyment. Improvements in technology make it simpler to identify the issues influencing our health. Numerous patient medical records are maintained by the healthcare sector. [12]. In order for stakeholders to fully benefit from the special qualities of blockchains, the authors suggested a new architecture that would allow for safe sharing. It was discovered that the suggested design improved device security by encouraging data authenticity. An effective and interoperable method for carrying out transactions based on the consensus notion was provided by a consensus-based transaction system.

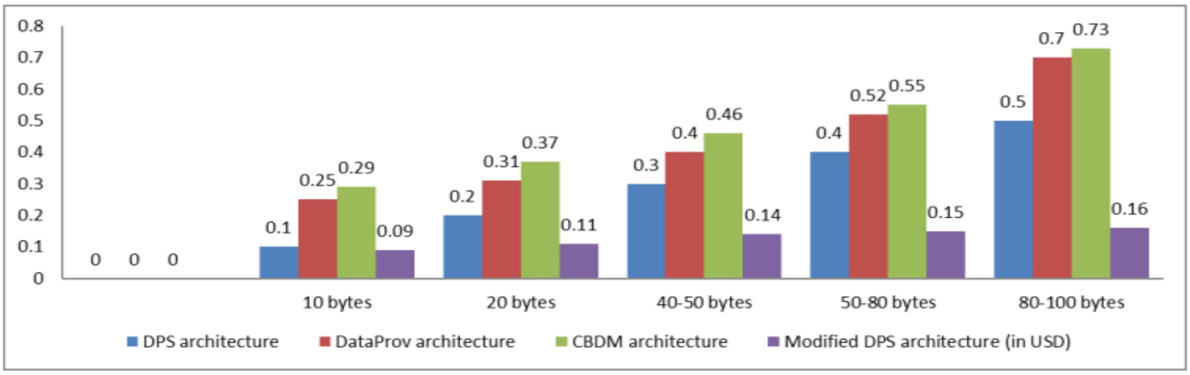


Figure 2: Cost Incurred to Preserve Files

The system was built upon a tripartite structure on numerous levels, such as a blockchain platform, application middleware, and smart contracts, to enhance cooperation between nodes across blockchain networks kept on the third level of the system. IoT suggests sharing healthcare networks to track patients.

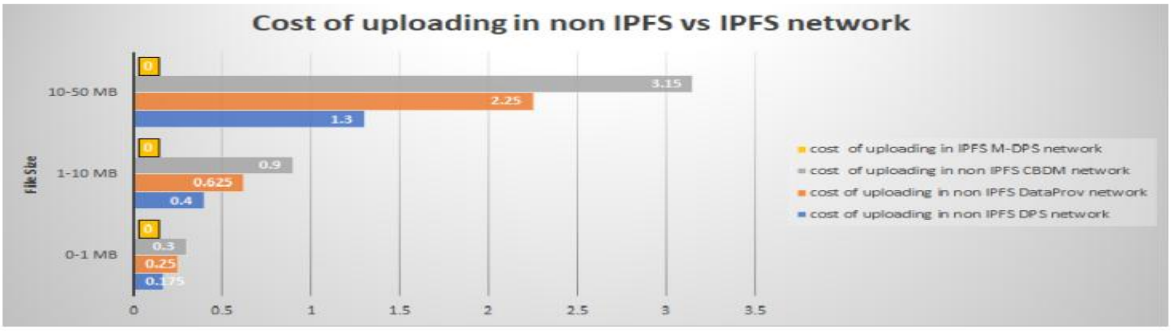
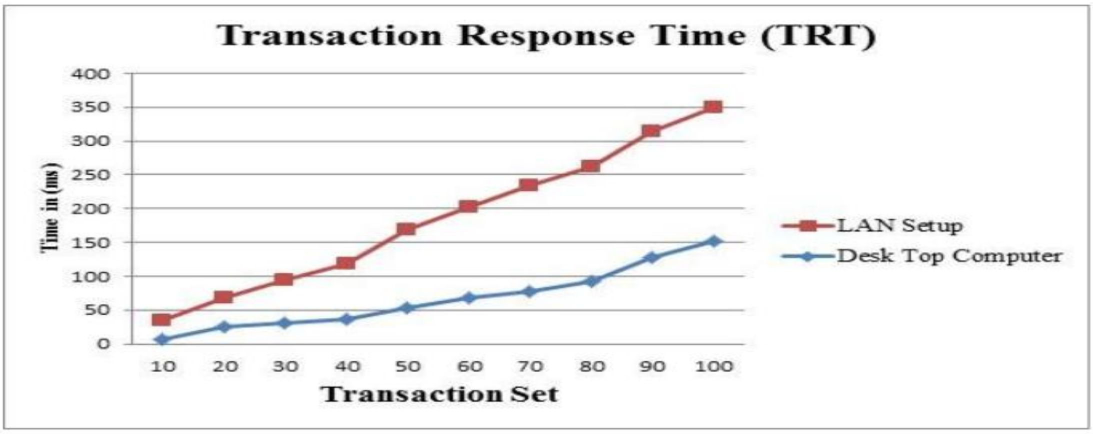


Figure 3: Fee Charged for Uploading Files in Non-Ipfs Vs. Ipfs Network

By isolating the data from intelligent, energy-efficient biosensors, their proposed method effectively transfers the data to microcontrollers and stores it in MySQL databases. Primary data and investigative information should be successfully screened, gathered, analysed, and documented for patients and medical practitioners globally. However, the authors failed to explore the proposed method's security measures.



The suggested protocol has been put into practice and tested with the EHR scenario health data network. The prototype implementation results testify that the suggested content encryption mechanism is safer and confidential to every individual of the e-Health system[14]. The privacy maintaining content encryption and decryption protocol encrypts all health assets and saves the hash values of every healthcare transaction in each block of the Blockchain. It is a possible method to guarantee confidentiality, privacy and security of the permissioned e-health Blockchain system[15].

CONCLUSION

With the advances in Information Technology, many healthcare organizations have converted conventional paper-based health records into Electronic Health Records. It consists of digitized information of patients' personal data, health data and health records. The digitized health data includes disease details, treatment history, prescriptions, drug summary, microbiological test reports and other imaging reports. The large amount of EHRs and extensive use of healthcare technologies in the big data era increase the role of the Internet and cloud network to store a large amount of health data and facilitate its access across the Network. The insecure nature of Internetwork, third-party maintenance with poor access to data and financial burdens besides privacy breaches lead to several attacks. Considering the vulnerable nature of Internetworking, there is a requirement for an immediate and effective mechanism that facilitates storage, security, sharing and accessing of health data across various stakeholders. Indeed a secured Patient Centric EHR management system is essential for managing the exponential growth in health records.

REFERENCES

1. Usman, Muhammad, and Usman Qamar. "Secure electronic medical records storage and sharing using blockchain technology." *Procedia Computer Science* 174 (2020): 321-327.
2. Zoitl, S., Angelov, N., & Douglass, G. H. (2025). Revolutionizing industry: Real-time industrial automation using embedded systems. SCCTS Journal of Embedded Systems Design and Applications, 2(1), 12–22.
3. Sun, Zhijie, Dezhi Han, Dun Li, Tien-Hsiung Weng, Kuan-Ching Li, and Xiaojun Mei. "MedRSS: A blockchain-based scheme for secure storage and sharing of medical records." Computers & Industrial Engineering 183 (2023): 109521.
4. William, A., Thomas, B., & Harrison, W. (2025). Real-time data analytics for industrial IoT systems: Edge and cloud computing integration. Journal of Wireless Sensor Networks and IoT, 2(2), 26-37.
5. Marichamy, V. Santhana, and V. Natarajan. "Blockchain based securing medical records in big data analytics." Data & Knowledge Engineering 144 (2023): 102122.
6. Arthur, L., & Ethan, L. (2025). A review of biodegradable biomaterials for medical device applications. Innovative Reviews in Engineering and Science, 3(1), 9–18. https://doi.org/10.31838/INES/03.01.02
7. Chen, Yi, Shuai Ding, Zheng Xu, Handong Zheng, and Shanlin Yang. "Blockchain-based medical records secure storage and medical service framework." Journal of medical systems 43 (2019): 1-9.
8. Alizadeh, M., & Mahmoudian, H. (2025). Fault-tolerant reconfigurable computing systems for high performance applications. SCCTS Transactions on Reconfigurable Computing, 2(1), 24–32.
9. De Oliveira, Marcela T., Lucio HA Reis, Ricardo C. Carrano, Flavio L. Seixas, Debora CM Saade, Celio V. Albuquerque, Natalia C. Fernandes, Silvia D. Olabarriaga, Dianne SV Medeiros, and Diogo MF Mattos. "Towards a blockchain-based secure electronic medical record for healthcare applications." In ICC 2019-2019 IEEE International Conference on Communications (ICC), pp. 1-6. IEEE, 2019.
10. Saleh, I. K. (2022). Adaptive Disassembly Using Deep Reinforcement Learning Using Path Planning Communication Approach. International Journal of Advances in Engineering and Emerging Technology, 13(2), 110–119.
11. Sun, Zhijie, Dezhi Han, Dun Li, Xiangsheng Wang, Chin-Chen Chang, and Zhongdai Wu. "A blockchain-based secure storage scheme for medical information." EURASIP Journal on Wireless Communications and Networking 2022, no. 1 (2022): 40.
12. Sun, Jin, Xiaomin Yao, Shangping Wang, and Ying Wu. "Blockchain-based secure storage and access scheme for electronic medical records in IPFS." IEEE access 8 (2020): 59389-59401.
13. Kumar, Anil, Ravinder Kumar, and Sartaj Singh Sodhi. "A novel privacy preserving blockchain based secure storage framework for electronic health records." Journal of Information and Optimization Sciences 43, no. 3 (2022): 549-570.
14. Sen, V., & Malhotra, N. (2025). A Critical Analysis of the Education for Sustainable Development. International Journal of SDG's Prospects and Breakthroughs, 3(1), 22-27.
15. Kapoor, P., & Malhotra, R. (2025). Zero Trust Architecture for Enhanced Cybersecurity. In Essentials in Cyber Defence (pp. 56-73). Periodic Series in Multidisciplinary Studies.