**International Academic Institute for Science and Technology**

International Academic Journal of Science and Engineering
Vol. 8, No. 2, 2021, pp. 6-10.

ISSN 2454-3896

**International Academic Journal of Science and Engineering**

www.iaiest.com

# A Healthcare Model Using Blockchain Technology to enhance Security and Data Sharing

Kavita Shenoy [a], Arvind Menon [b]

[a] *Quantum Computing Division, Chennai Institute of Technology, India*.
[b] *Quantum Computing Division, Chennai Institute of Technology, India*.

## Abstract

The exchange of Electronic Health Records (EHR) enhances medical quality and reduces costs, yet technical challenges persist despite the willingness of individuals and healthcare organizations to share information. These technical limitations encompass secrecy, privacy, connectivity, and integrity. This study proposes a blockchain - and MedRec-based methodology utilizing encryption and attribute-based verification to facilitate the safe exchange of medical information. This method enables: 1) Comprehensive viewing and safe storage of dispersed EHR components; 2) Verification of EHR genuineness; 3) Provision of flexible, granular access command; and 4) Maintenance of an unambiguous audit trail.

**Keywords:** Healthcare, Blockchain, Security, Data Sharing.



Received: 04 March 2021/Revised: 07 April 2021/Accepted: 3 May 2021/Published: 30 June 2021

## Introduction

In the provision of medical treatment, substantial quantities of data are generated and must be securely preserved for extended durations, frequently for a lifetime. A significant distinction between medical information and other forms of big data release is that Electronic Health Records (EHRs) (Kim et al., 2019) are typically highly confidential, potentially causing individuals and medical institutions to hesitate to share them. EHR sharing can benefit individuals and hospitals in several respects. Primarily, sharing information can enhance research in medicine by aggregating many clinical trials to foster improved knowledge and scientific breakthroughs. In addition, cooperation among various healthcare institutions, including cross-border situations, would be facilitated, such as physicians accessing clients' medical information and funding medical care in foreign countries (Bell et al., 2015). Lastly, legislation and standards to enhance secure EHR exchange will be established and reinforced, fostering more confidence among various medical institutions, ultimately providing patients with improved services, and advancing the field of medicine. Certain technical obstacles impede EHR sharing and complicate the process. A review of research papers from 2004 to 2015 identified eight primary safety concerns concerning EHR sharing, ranked from the majority to least concerning: safety, privacy, control over access, honesty, data genuineness, identification of users, audibility, and openness. Resolving these difficulties is crucial to facilitating safe EHR exchange (Subbian et al., 2021).

## Background

In the past few years, blockchain has been used in medical care to address security concerns related to data authenticity and reliability (Ali et al., 2021). A blockchain is a decentralized ledger utilized to document interactions between entities. Its distributed framework is one of its most intriguing attributes. Storing electronic health records on a centralized server may invite attacks from nefarious entities, and the collapse of a critical site is likely to result in service disruption or cessation. A distributed blockchain-based solution is expected to mitigate this difficulty, facilitating continuous service provision. A further benefit of blockchain is that altering transactions recorded in the chains is challenging owing to the security provided by the hashing algorithm and the Proof-Of-Work (PoW) mechanism (Duong et al., 2020).

There is a paucity of study findings about blockchain-based EHR sharing. A method for a health data exchange network is presented. There are two primary contributions. Initially, it proposes addressing the compatibility challenge through the semantics and format verification of EHRs to guarantee uniformity across all EHRs within the blockchain system. In addition, it offered a technique to randomly select the subsequent miner to conserve computational power and system assets.

The study proposes using blockchain to encrypt its privacy-preserving search for keywords and innovative contract technology to ensure anonymity and confidentiality, albeit it lacks specific methodologies (Bernabe et al., 2019). The MedRec medical system is constructed on contracts to facilitate the maintenance of EHRs. Users' identity strings correlate with Ethereum IP addresses in Registrant Contracts (RCs) to maintain user anonymity. Patient-provider relationship agreements (PPRs) delineate the management and accessibility of information; PPRs are cited through links in Summary Contracts (SCs) to consolidate a patient's medical information into a cohesive entity (Preeker & De Giovanni, 2018). The study fails to offer comprehensive strategies for addressing issues such as the encryption of individuals' EHRs, access protocols for registered users, user authentication methods, and maintaining an audit trail about EHR use. A blockchain-based application, Healthcare Information Gateway (Yue et al., 2016), has been created to help patients control and manage their medical information efficiently. All data is kept in the blockchain clouds and administered via the data management level. Accessibility to patient information is restricted to authorized individuals, and replicas must be deleted upon the expiration of the allowed period. The study examines the primary facets of health information and the benefits and drawbacks of employing blockchain for its preservation and recovery.

## Proposed Healthcare Model Using Blockchain

The structure of the suggested system, seen in Fig. 1, has six layers arranged as follows: The initial layer is the IoT physical level, comprising wearable health equipment such as blood pressure monitors, glucometers, and weight scales. They monitor patient health indicators in real-time, including respiration rate, blood pressure, pulse, and other essential metrics. The second level is the connection level, comprising an IoT gateway, an IoT computer, and communication protocols, including Constrained Application Protocols (CoAP) and Hypertext Transfer Protocols (HTTP). A Raspberry Pi, integrated with the Libelium e-Health toolbox, functions as an IoT gateway. The interface transmits the aggregated vital signs information to the medical IoT server.

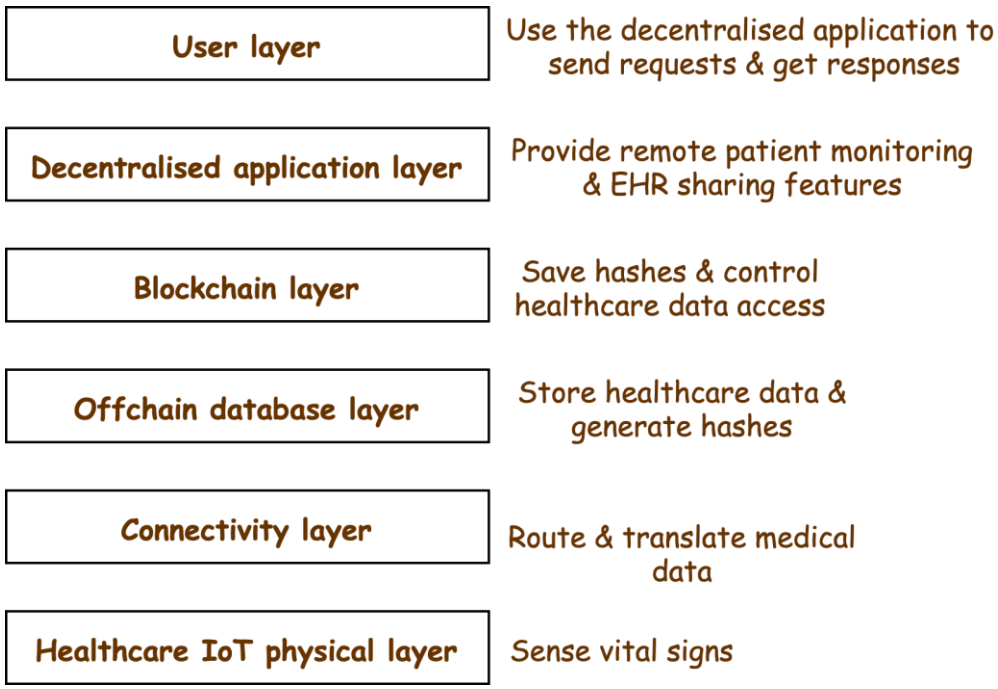



**Fig. 1: Architecture of the Proposed Model**

The cloud-based IoT client engages with the blockchain system and the distributed Offchain dataset. The IoT server secures the incoming data and stores it in a decentralized Offchain store. The medical IoT server transmits client-generated activities to acquire real-time vital sign data, device data, and gadget status.

The next tier is the Offchain database level, wherein the research proposes utilizing OrbitDB in conjunction with the Interplanetary File Systems (IPFS). OrbitDB is a peer-to-peer repository designed for the decentralized internet. IPFS is a peer-to-peer multimedia system employing content referencing to identify every file uniquely. IPFS computes the encryption key of the information stored in OrbitDB and transmits it to the blockchain databases.

The fourth tier is the network's security level, which employs a permission-based blockchain to limit access only to pre-approved users. The Hyperledger Fabric architecture oversees participant registering, registering wearable health gadgets, registering IoT gateways, and implementing access control measures.

A distributed remote monitoring of patients service has been suggested at the fifth tier, the application layer. This program operates on a peer-to-peer network and interacts with deployed intelligent contracts via program Programmer Interfaces (APIs). This decentralized program offers functionalities consumers can utilize, including authorizing the definition, maintaining patient health records, and surveillance.

The sixth level is the Users Section, which comprises people, doctors, pharmacies, and laboratory workers who engage with Health Block and derive advantages from its functions. A blockchain network manager is registered.

The administrator possesses the authority to build and join channels, deploy chain codes, and manage peers by adding, updating, or removing them. The research suggests an organization within the Ministry of Healthcare should serve as the administrative body. Each user constitutes a node within the blockchain system, and every node must fulfill a specific job, such as admins, rivals, orderers, members, or clients.

## Results

Fig. 2 depicts a random arrangement of machine utilization. The graph indicates that in the optimal case, read transaction speed markedly increases until it peaks, followed by a minor decline after the sending rate 2500, which is deemed the optimal situation. Transaction volume is assessed by adjusting the send frequency from 200 to 1400 operations per minute, as illustrated in Fig. 3. The graph indicates that the mean transaction speed rises with the send rate until it peaks at 1200 operations per send. The ideal condition for mean transaction speeds is 1200 operations per minute; thereafter, throughput declines as the sending rate escalates.

The mean transaction delay is evaluated by adjusting the transmit rate from 200 to 1400 operations per second. Fig. 4 illustrates that the median transaction delay of the suggested medical blockchain network experiences a minor rise up to a transmit rate of 1100 transactions per second (tps). As the volume of requests escalates beyond 1100 operations per minute, the response time of the blockchain system rises linearly. The ideal transmission rate for transactional delay is approximated at 1100 operations per minute.

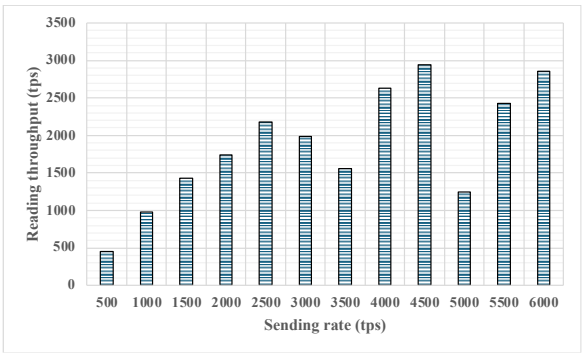



**Fig. 2: Reading Throughput Analysis**

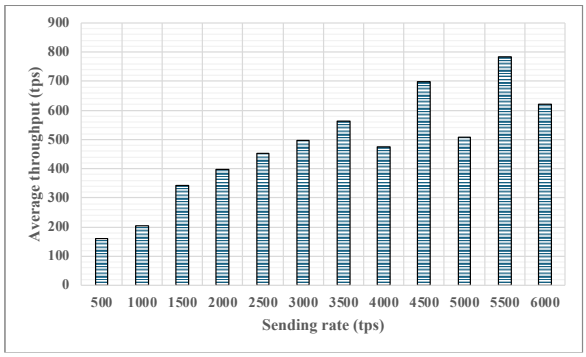



**Fig. 3: Average Throughput Analysis**

Similarly, in Fig. 5, the mean read activity delay is assessed by altering the transmit rate from 500 to 3000 operations per minute. The delay in read transactions exhibits a marginal increase until it reaches a sending rate of 2500 operations per second, which is deemed the ideal condition. However, the value of read delay escalates linearly beyond the perfect threshold of 2500 operations per minute as the volume of read requests rises.

Block mining typically requires 10 minutes, whereas executing transactions may take approximately one hour. Similarly, with Ethereum, the typical duration for block mining is approximately 24 seconds. The suggested medical digital currency is founded on a permissioned ledger system, wherein activities are conducted among authorized users under a governing framework. Likewise, the suggested permissioned blockchain architecture employs Practical Byzantine Fault Tolerance (PBFT), enhancing system efficiency by diminishing mining expenses. An authorized blockchain network diminishes the possibility of hostile actions in brilliant contract form. Given that the intended blockchain users are pre-registered and recognized, any actions, including event submissions and network setting adjustments, are tracked in the blockchain ledger state databases.

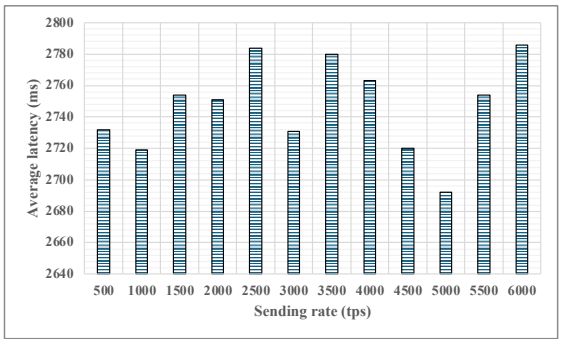



**Fig. 4: Average Latency Analysis**

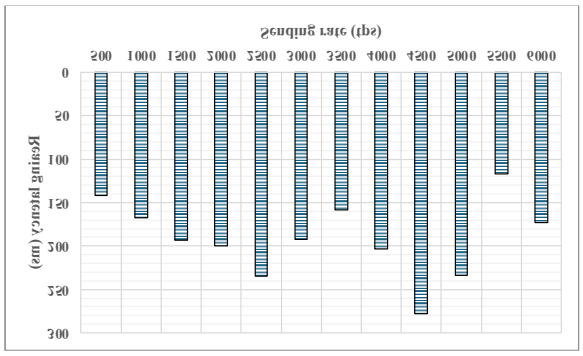


**Fig. 5: Reading Latency Analysis**

## Conclusion

This study proposes a blockchain-based method for establishing a decentralized medical system to share EHRs securely. The primary objective is to address safety concerns related to privacy, access control, anonymity, and auditability. Utilizing the MedRec framework, documenting any modifications to electronic health records on the blockchain safeguards medical records from tampering and facilitates accessible, integrated, and visible auditing data for clients. Encryption ensures the integrity of information. It offers a versatile method for accessing shared information, promoting a verifiable record of users seeking entry into patients' EHRs.

## References

Kim, E., Rubinstein, S. M., Nead, K. T., Wojcieszynski, A. P., Gabriel, P. E., & Warner, J. L. (2019). The evolving use of electronic health records (EHR) for research. In *Seminars in radiation oncology*, *29*(4), 354-361). WB Saunders. https://doi.org/10.1016/j.semradonc.2019.05.010.

Bell, D., Holliday, R., Ormond, M., & Mainil, T. (2015). Transnational healthcare, cross-border perspectives. *Social science & medicine*, *124*, 284-289. https://doi.org/10.1016/j.socscimed.2014.11.014.

Subbian, V., Galvin, H. K., Petersen, C., & Solomonides, A. (2021). Ethical, Legal, and Social Issues (ELSI) in Mental Health Informatics. *Mental Health Informatics: Enabling a Learning Mental Healthcare System*, 479-503. https://doi.org/10.1007/978-3-030-70558-9_18.

Ali, A., Rahim, H. A., Pasha, M. F., Dowsley, R., Masud, M., Ali, J., & Baz, M. (2021). Security, privacy, and reliability in digital healthcare systems using blockchain. *Electronics*, *10*(16), 2034. https://doi.org/10.3390/electronics10162034.

Duong, T., Fan, L., Katz, J., Thai, P., & Zhou, H. S. (2020, September). 2-hop blockchain: combining proof-of-work and proof-of-stake securely. In *European Symposium on Research in Computer Security* (pp. 697-712). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-59013-0_34.

Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T., & Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. *Ieee Access*, *7*, 164908-164940. https://doi.org/10.1109/ACCESS.2019.2950872.

Preeker, T., & De Giovanni, P. (2018). Coordinating innovation projects with high tech suppliers through contracts. *Research Policy*, *47*(6), 1161-1172. https://doi.org/10.1016/j.respol.2018.04.003.

Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *Journal of medical systems*, *40*, 1-8. https://doi.org/10.1007/s10916-016-0574-6.