Journal of Computer Applications and Information Technology
Vol. 2, Issue. 2, Jun 2026, pp. 24~33
ISSN: 3107-6424, DOI: 10.32595/v2i2.2026.33

Blockchain-Enabled Electronic Health Record System with Privacy-Preserving Data Sharing and Cloud Integration

Senthilkumar Moorthy[1], Ramesh Palanisamy[2]

[1]Assistant Professor, Department of Information Systems and Business Analytics, College of Business Administration, A'Sharqiyah University, Ibra, Sultanate of Oman.
E-mail: senthilkumar.moorthy@asu.edu.om
[2]College of Computing and Information Sciences, University of Technology and Applied Sciences, Ibra, Sultanate of Oman.
E-mail: ramesh.palanisam@utad.edu.om

Article Info

Article History:

Received Apr 05, 2026
Revised May 07, 2026
Accepted Jun 06, 2026

Keywords:

Blockchain,
Electronic Health Records,
Privacy-Preserving,
Cloud Computing,
Smart Contracts,
Healthcare Data Security,
Encryption

ABSTRACT

Health care data management comes with numerous barriers as a result of the use of different systems of record keeping, which are not compatible and increase the risks for data protection and privacy. Medical records are frequently distributed throughout various clinics and hospitals, and due to this it is hard to share information when patients are being treated. Centralized record systems bring unauthorized access to records and the problems related to the safety of data. In order to enhance the level of confidence of people and improve the level of transparency of health care data, advanced people choose decentralized technologies and uses cryptography for these purposes. Blockchain technology offers an unchangeable and decentralized ledger that guarantees safe monitoring of all information despite the presence of any centralized body. Coupled with sophisticated encryption methods, it provides the ability to limit access to private health information. In order to provide secure and respect privacy regarding medical data sharing, an Electronic Health Record (EHR) system powered by blockchain technologies is proposed. Patient record metadata is recorded on-chain while health data itself is stored on encrypted off-chain storage. In the realm of access management, smart contracts facilitate patients in designating by whom their records can be accessed and modified. The privacy of information is further strengthened by advanced cryptographic techniques like attribute-based encryption and zero-knowledge proofs. The system provides seamless interoperability among hospitals, laboratories, and telemedicine systems while ensuring high levels of security. The results of performance evaluation demonstrate that this method facilitates reliable transaction processing while providing better security, transparency and control than traditional centralized EHR systems.

Corresponding Author:

Senthilkumar Moorthy,
Assistant Professor, Department of Information Systems and Business Analytics,
College of Business Administration, A'Sharqiyah University, Ibra, Sultanate of Oman.
E-mail: senthilkumar.moorthy@asu.edu.om

1. INTRODUCTION

Information on health is an important asset for both those providing the services and the patients. Furthermore [1], it is essential to ensure the reliable exchange and preserving Electronic Healthcare Records (EHR). In the past few years, the centralization system was used in the EHR systems of health, whereby a cloud platform was used for sharing information on health between medical process participants [2], and thereby putting in danger the security of personal information. The EHR system has met difficulties in satisfying demands of various stakeholders. The task of integrating information from many registered sources has proven to be difficult [3], but electronic records can give an overall perspective of the exact information about patients. Although cloud technology was born due to the development in the field, the healthcare data storage is extremely vulnerable with all its advantages compared to traditional storage [4]. The healthcare industry is changing from paper to computer records and is undergoing important changes. Electronic Health Data (EHD), EHR, Electronic Medical Records (EMR), and Personal Health Records (PHR) are already in place. EHD stands for electronic health documentation, which is a modernized method of documentation utilized in lieu of conventional written records [5]. EHD comprises updated information about medical history, treatment, demographic details, data about immunization and other important information pertaining to the patient's health. The various advantages of EHD over paper-based records include decreased need for personnel [6], lower time investments and lesser physical space requirement.

With the increasing digitization of our world today, one of the solutions brought about by blockchain and cloud computing technologies is their merging together to form a new solution for data storage problems [7]. These days, the problem of storing data properly and safely is becoming even more urgent as the amount of data keeps growing and increasing fast. Blockchain technology is famous for its being decentralized and unchangeable ledger, in addition to that it can be used for protecting sensitive data in health. Blockchain uses data encryption and secure record keeping of transactions which guarantees that the data remains authentic and secure, allowing to avoid unauthorized access. In contrast, cloud storage provides a great deal of scalability and accessibility, enabling healthcare companies to store, analyze and process large volumes of data in an easy manner [8]. Besides, solutions that are based on the cloud allow flawless data sharing and collaboration among healthcare stakeholders and provide an opportunity to access important information in real-time and innovate care delivery processes. But the question of data security and confidentiality is still relevant owing to centralized nature of cloud storage.

The integration of the security of the blockchain with the functional cloud storage creates a possibility. The study aims to analyze the combined use of blockchain with cloud technologies in the management of medical data [9], taking into consideration issues of security, scalability, and interoperability. The synthesis performed allows improving the comprehension of the integration of these technologies, based on evaluation of the studies devoted to this subject. The analysis includes the overview of the works made by different scholars in this field. Our investigation concerns the technical dimensions of blockchain, its service models, security frameworks, and impact of this integration on the performance of cloud storage systems [10].

In the realm of healthcare data management, the combination of blockchain technology and cloud computing has great importance. Healthcare data entails being very sensitive in nature and therefore necessitates safe and at the same time flexible management options. The unchangeable and cryptographic nature of blockchain in conjunction with the scalability and affordability of cloud computing has the potential to change the way a healthcare system is managed. This combination will guarantee integrity in data, provide better protection, and establish

interoperability, which will allow healthcare stakeholders to exchange the data in an efficient manner and with full transparency. Using cloud analytics and machine learning systems, healthcare organizations will gain invaluable data concerning health outcomes of patients and the treatment results.

2. RELATED WORKS

[11] Proposes an innovative method that combines deep learning and blockchain technology for ensuring the confidentiality of electronic medical records. The provided dataset was analyzed and divided into normal and abnormal users via the convolutional neural networks approach. Then, by means of blockchain combined with a cryptocurrency-based federated learning module, the abnormal users were processed and removed from the database. The simulation was conducted in Python, and it appears that the classification results achieved are superior to those of the other existing techniques in terms of model performance.

[12] Designed a Patient's E-Healthcare Record Management System (PRMS) to provide a balance between latency and throughput. An extensive performance evaluation of PRMS is performed across different public and private cloud platforms to check its efficiency. In addition to this, PRMS is compared with blockchain technologies existing to this date like Hyperledger Fabric v0.6 and Etherium v1.5.8 with respect to latency and throughput performance by loading the workload upto 10000 transactions per second on respective platforms. PRMS is compared with secure and reliable healthcare blockchain (SRHB) system based on Yahoo Cloud Serving Benchmark (YCSB) on small bank datasets. Results showed that deployment of PRMS through Amazon Web Services improves its performance against both System Execution Time (SET) and Average Delay (AD) by upto 2.4 % and 15.26 % respectively. Moreover, deploying PRMS through Google Cloud Platform yields improvement in performance by upto 4.73 % related to SET and AD performance measures respectively.

[13] Propose a design utilizing blockchain technology that is able to verify the identity of users based on common cryptocurrency mechanism known as Proof of Stake (POS), and secured through use of cryptographic process called Secure Hash Algorithm (SHA256) for sharing electronic health record data between various electronic medical system. In addition, EHR recording device called Elliptic Curve Digital Signature Algorithm (ECDSA) was used to see if the described process generates valid data in the cloud. Based on the results, the process is much more efficient if compared to usual methods that make use of Proof-Of-Work (POW) algorithm, Secure Hash Algorithm called SHA-1, and Message Digest (MD5).

[14] Outlines a patient-centric, blockchain architecture that ensures privacy and confidentiality of patient information when such information is shared through EHRs. The Proof of Stake (PoS) consensus algorithm is proposed as an alternative to solve the scalability problems of conventional consensus algorithms. This technique is used together with smart contracts and cryptographic techniques so that the patients are provided with complete control over their data access. The proposed architecture has been developed to facilitate cooperation between different participants in the health care processes. Performance evaluation has been carried out using gas cost, transaction time, and comparison with the existing EHR systems.

3. METHODOLOGY

The proposed methodology merging blockchain technology, privacy-preserving encryption, and cloud computing, the proposed methodology provides secure and efficient management of Electronic Health Records (EHRs). Smart contracts are used in the methodology to enforce secure access, while encrypted patient records are maintained in the cloud ensuring data confidentiality and availability. The effectiveness of the proposed framework as a whole is determined by evaluating it using performance metrics including encryption time, data-sharing correctness, transaction throughput, and cloud access latency as shown in Figure 1.

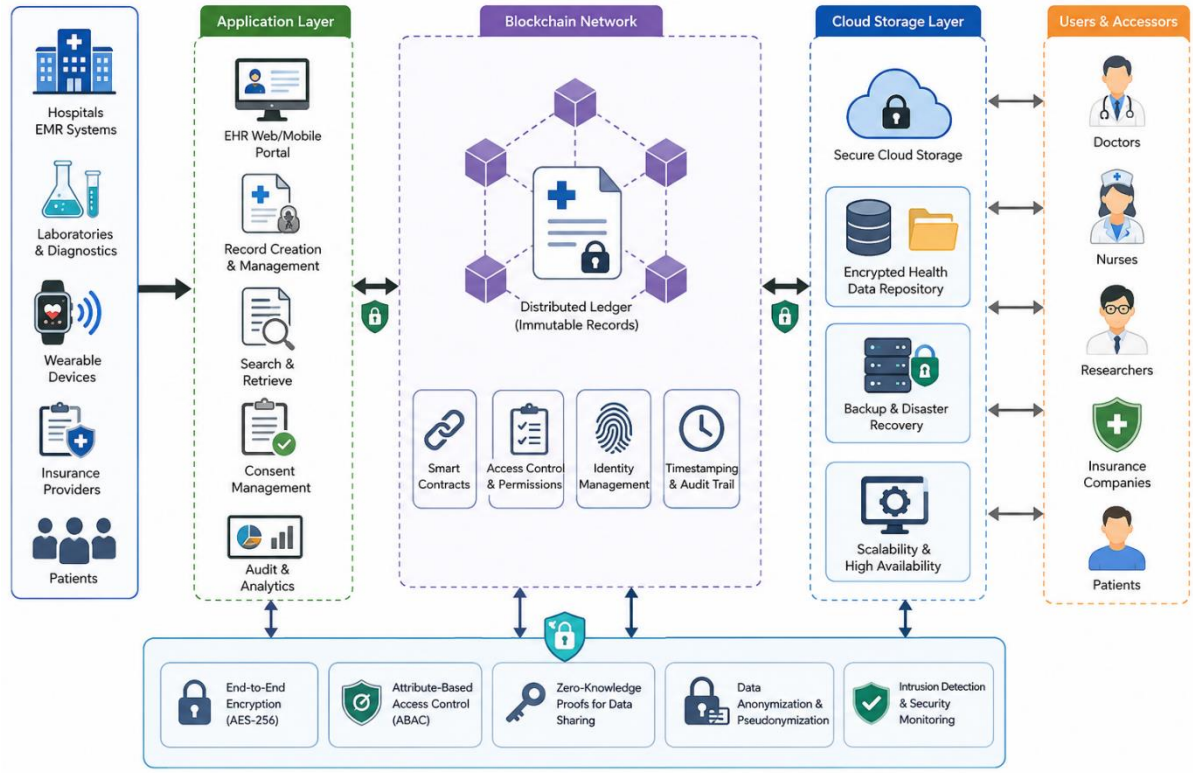

Figure 1. Working Process of the Proposed Model

3.1. Data collection

The research utilizes EHR data obtained through open-source data repositories like Kaggle, where fictitious patient details are present, including history of the patient, the diagnosis, treatment details, drugs involved, and access patterns. The datasets are constructed to mimic an actual clinical procedure and utilized as inputs to investigate the privacy-preserving strategy proposed in the paper. The information guarantees the implementation of encrypted storage, access control modeling and policy verification in numerous healthcare operations, such as those performed by doctors, nurses and top managers of a healthcare facility. Moreover, since the system allows the inclusion of fields that require a careful access, it can be verified if applying encrypted mechanism is feasible in the situation.

3.2. Data Normalization

Data cleaning is being utilized to address common issues with EHR data sets which include missing values, duplication, and outliers. Missing values can be handled either through imputation techniques such as mean/mode substitution or deleted altogether. To handle duplication, duplicates are removed to avoid redundancy. The statistical tests that are implemented to identify outliers. The

values of clinical tests can be determined through the use of certain equations that determine the existence of outlier values. Min-Max scaling is applied in (2) to standardize numerical information like age and test results.

$$X' = \frac{X - X_{\min}}{X_{max} - X_{\min}} \quad (1)$$

Let X be the raw quantity, and X' be the normalized value. Categorical variables (such as sex, diagnosis type, role) are converted in this approach using either label encoding or one-hot encoding in order to meet contractual requirements associated with role-based access permissions. Consistent formats for timestamps and units (e.g., vitals) ensure proper auditing of access and data comparisons.

3.3. Feature selection

Feature selection is meant to choose the most relevant features from electronic health records (like identification of patients, departments, diagnosis, and treatment), which can be utilized for both the purpose of access security and analytical work. Either a correlation study or a statistical test allows filtering out irrelevant and redundant features. Regarding quantitative data, Pearson correlation is used as follows:

$$r = \frac{\sum (X - \hat{X})(Y - \hat{Y})}{\sqrt{\sum (X - \hat{X})^2 \sum (Y - \hat{Y})^2}} \quad (2)$$

Where Xˆ and Yˆ represent the corresponding variables' mean values. This aids in the selection of sensitive features that need to be access-controlled and encrypted.

3.4. Cryptographic Mechanisms Design

This part reveals the essential cryptographic architecture that's intended to protect healthcare information in the Blockchain-based solution. The proposed framework adopts a combination of Encrypted RBAC and HE to achieve data confidentiality, access control and usability. Encrypted RBAC will apply the access control policy according to the roles assigned (doctor, nurse, administrator and others) and provide encryption of the roles and authorizations on the Blockchain ensuring their safety. Key features include: the role-based key pair composed of the public and private keys assigned for individual clients.

$$M : R \to P, \text{ where } P = \{p_1, p_2, \ldots p_m\} \quad (3)$$

This equation illustrates how each user identified by the role 'R' has been assigned its own unique key pairs P which facilitate the access of the encrypted data related to the role. For each role (doctor, nurse, etc.), a permission token is provided allowing a completely decentralized network or an access right based on a role.

$$C = AES_k(P) \quad (4)$$

In (4), the collection of access rights P has been encrypted with AES-256 symmetric encryption through K. The relevant ciphertext C is recorded on-chain, which makes sure the confidentiality of permissions based on the role is retained while providing an encryption speed of a high degree necessary for fast operation of healthcare. Each person utilizes a public-private key pair:

$$k_{pub}, k_{priv} \text{ such that : } C' = Enc_{kpub}(K) \quad (5)$$

In expression (5), the encryption process of the symmetric key K occurs with the help of the RSA public key of the user, k_ub. Thus, C^' is safely transmitting the encrypted key, which only the intended recipient with the k_priv private key can decrypt to receive the symmetric key K.

This way, contracts verify who has requested access by decrypting the role-based permissions and ensuring entitlement while concealing the identity and role.

$$\text{Veri } fy(U_i, R_j) = \{\text{GrantDeny if } R_j \in \text{AuthorizedRolesotherwise} \quad (6)$$

Smart contracts automatically confirm whether user U_i has a permitted role R_j If validated, access is provided. This enables permission enforcement while concealing the identity of the user and decrypting low-level data preserving the confidentiality and privacy of the system and roles as stated in (6).

4. EXPERIMENTAL RESULTS

The outcomes of the experiments show that the blockchain-enabled Electronic Health Record (EHR) system can successfully manage securely and efficiently health data while allowing for privacy preserving sharing of medical data. Compared to the existing cloud model, the proposed model requires shorter encryption time while ensuring comparable data sharing accuracy. The transaction throughput consistently improves as the number of patients' records increases, proving that the blockchain model is scalable. Cloud storage latency is kept under control to allow for timely access to encrypted medical records. Thus, it can be concluded that combining blockchain with cloud computing has a positive effect on safety, scalability, and performance of modern healthcare information systems.

Table 1. Experimental Performance Evaluation of the Proposed Blockchain-Enabled EHR System

Number of Patients	Encryption Time (s)	Traditional Encryption Time (s)	Data Sharing Accuracy (%)	Transaction Throughput (TPS)	Cloud Access Latency (s)
100	0.45	0.61	91.2	310	0.21
200	0.83	1.08	93.5	540	0.38
300	1.25	1.59	95.1	760	0.56
400	1.66	2.18	96.4	990	0.73
500	2.08	2.81	97.8	1180	0.92

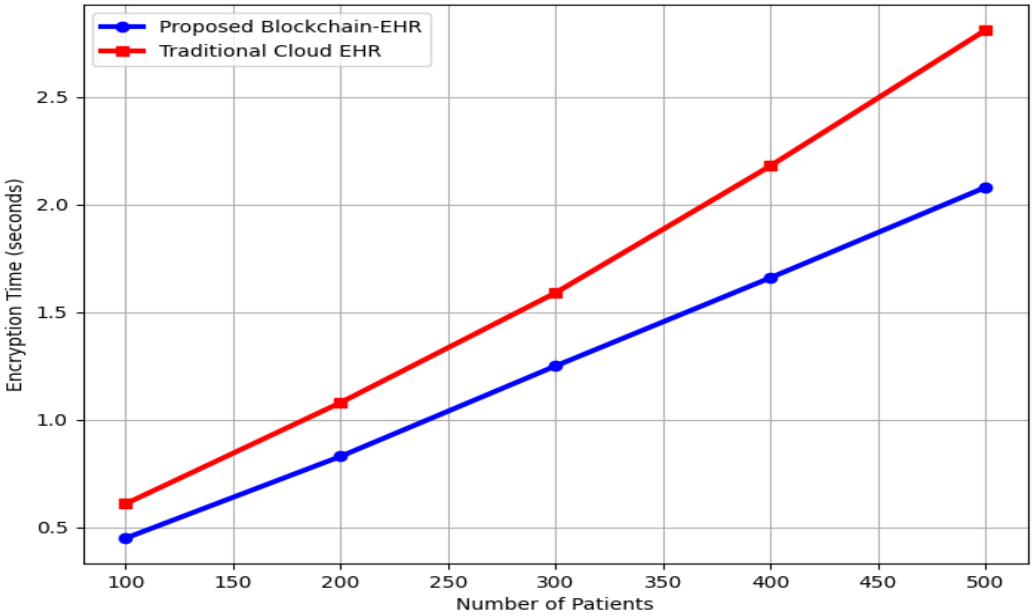

Figure 2. Encryption Time Comparison

The encryption times of the novel blockchain-based electronic health records system and the typical cloud-based electronic health records system have been compared in Figure 2 in relation to the number of patient records. The total number of 100 to 500 patients has been tested with respect to the time spent on encryption. While the encryption time for both electronic health records system models has increased with the increase in number of patients, blockchain technology has proved its effectiveness as a faster alternative to traditional encryption and cloud technology since it requires less encryption time as compared to cloud electronic health records.

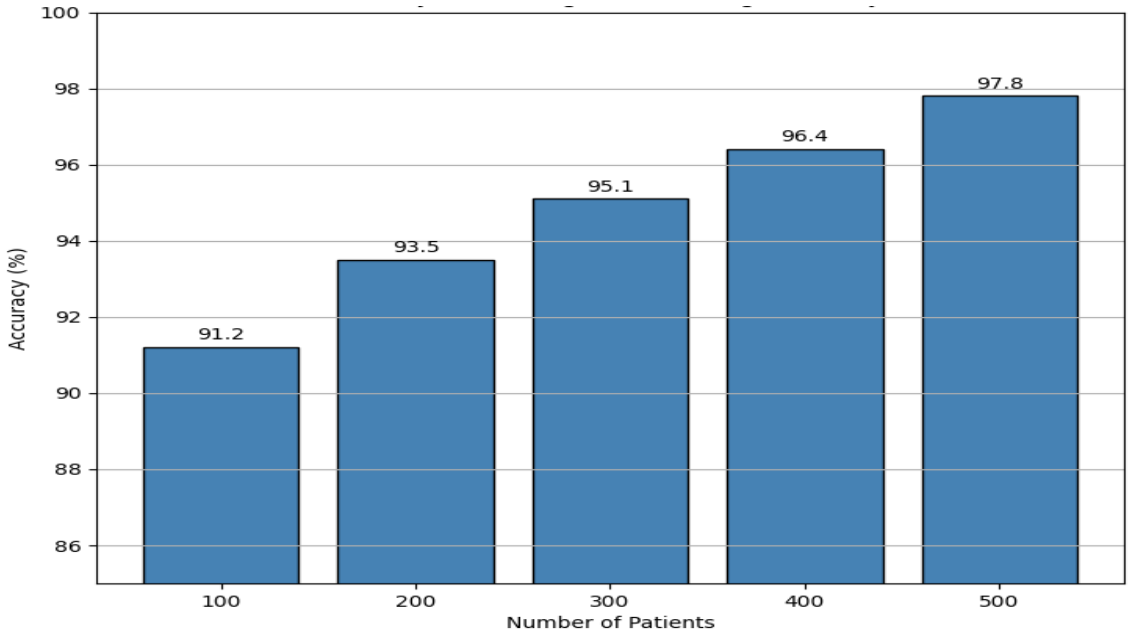

Figure 3. Privacy-Preserving Data Sharing Accuracy

Figure 3 depicts the correct sharing of data in the blockchain framework that we have created with privacy protection. The accuracy increases from 91.2% to 97.8% as the number of patient records increases, which suggests that the access control is effective and data sharing is secured. The results show that the proposed framework successfully protects the patients' privacy

and ensures the accurate and authorized sharing of electronic health records among different parties involved in healthcare.

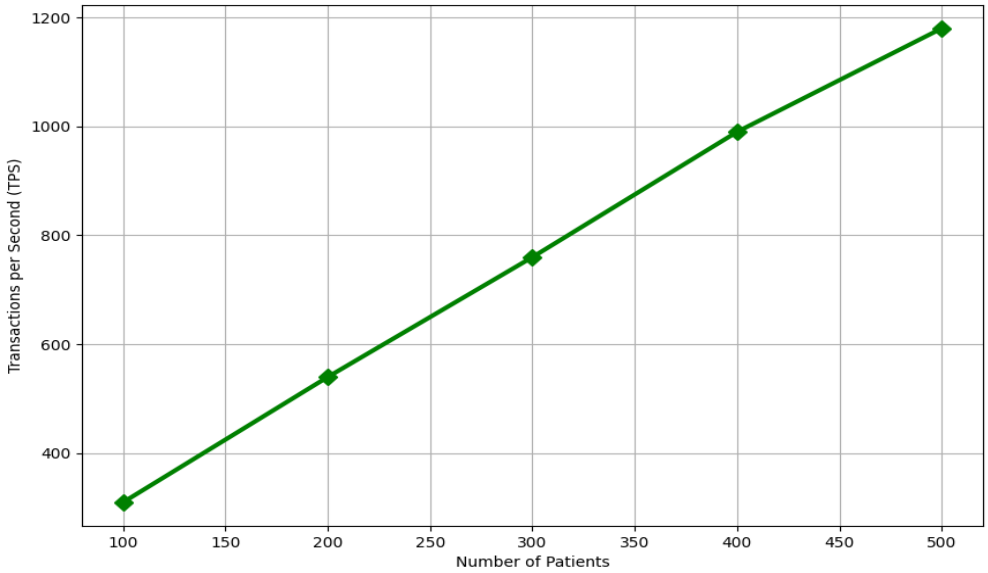

Figure 4. Blockchain Transaction Throughput

In Figure 4, the transaction throughput of the blockchain network at varying patient loads is exhibited. The throughput rises continuously from 310 TPS to 1180 TPS, showing that the blockchain network process an increasing amount of healthcare transactions satisfactorily well. Hence, it means that the results demonstrate the scalability of the discussed architecture regarding Electronic Health Record (EHR) transactions.

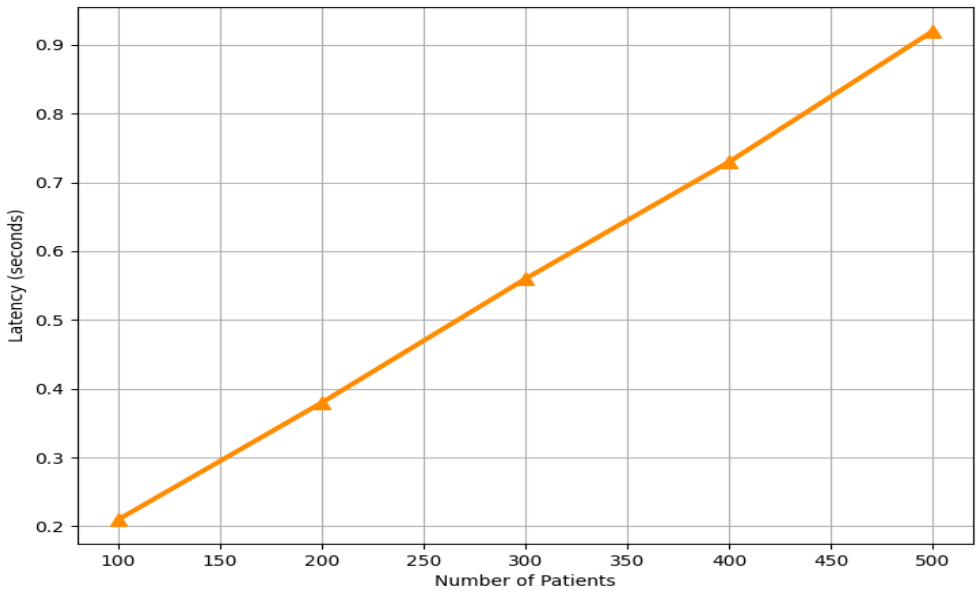

Figure 5. Cloud Storage Access Latency

The cloud storage access latency for the retrieval of encrypted medical records is shown in Figure 5. Even though latency rises slightly as the patient records increase, this latency remains lower than one second, which indicates that the communication between the blockchain network and cloud storage is effective. The outcomes suggest that the system allows timely access to health data as well as secure and privacy-preserving storage methods.

In conclusion, the experiments conducted reveal the superiority of the Blockchain-Enabled Electronic Health Record System over traditional cloud EHR systems when it comes to efficiency of encryption, privacy-preserving data-sharing, transaction throughput, and accessibility. The results appear to confirm that the proposed solution is a secure, scalable and reliable choice for modern healthcare information management.

5. CONCLUSION

In this study, we propose an Electronic Health Record (EHR) system powered by blockchain technologies to provide secure and respect privacy regarding medical data sharing. Patient record metadata is recorded on-chain while health data itself is stored on encrypted off-chain storage. In the realm of access management, smart contracts facilitate patients in designating by whom their records can be accessed and modified. The privacy of information is further strengthened by advanced cryptographic techniques like attribute-based encryption and zero-knowledge proofs. The system provides seamless interoperability among hospitals, laboratories, and telemedicine systems while ensuring high levels of security. The results of performance evaluation demonstrate that this method facilitates reliable transaction processing while providing better security, transparency and control than traditional centralized EHR systems.

REFERENCES

[1] Lopez, L.J.R., Millan Mayorga, D., Martinez Poveda, L.H., Amaya, A.F.C. and Rojas Reales, W., 2024. Hybrid architectures used in the protection of large healthcare records based on cloud and blockchain integration: A review. *Computers*, *13*(6), p.152.

[2] Nandanwar, H. and Katarya, R., 2025. Secure and Privacy-Preserving Data Sharing in 6G-Enabled Blockchain IoT Healthcare Systems. *Security and Privacy*, *8*(6), p.e70105.

[3] Marwa Ali Hamdan AL-Jabri and Nafisa Abul Ghafoor Othman AL-Ansari (2025) "A Review of Blockchain-Driven Access Control Frameworks for Secure Smart Contracts in Cloud Environments", *IIRJET*, 11(2). doi: 10.32595/iirjet.org/v11i2.2025.235

[4] Khan, A.R. and Jilani, A.K., 2024. Privacy-Enhanced Heart Disease Prediction in Cloud-Based Healthcare Systems: A Deep Learning Approach with Blockchain-Based Transmission. *Fusion: Practice & Applications*, *15*(1).

[5] Megha, S.A., Ranjith, J., Abhinand, B.V., Veeresh, K.M. and Kiran Kumar, V., 2026. Blockchain-Enabled Privacy-Preserving Framework for Secure Electronic Health Records Sharing and Diagnosis in Internet of Medical Things. *SN Computer Science*, *7*(2), p.201.

[6] Ezhumalai. P, Malarkodi. S and Jancy Rani. S (2022) "A Novel Privacy Preserving Localization Scheme based on Lateration for Mobile User Concentrated Networks", *IIRJET*, 2(Special Issue ICEIET). Available at: https://iirjet.org/index.php/home/article/view/244 (Accessed: 24 July 2026)

[7] Megha, S.A., Ranjith, J., Abhinand, B.V., Veeresh, K.M. and Kiran Kumar, V., 2026. Blockchain-Enabled Privacy-Preserving Framework for Secure Electronic Health Records Sharing and Diagnosis in Internet of Medical Things. *SN Computer Science*, *7*(2), p.201.

[8] Jakhar, A.K., Singh, M., Sharma, R., Viriyasitavat, W., Dhiman, G. and Goel, S., 2024. A blockchain-based privacy-preserving and access-control framework for electronic health records management. *Multimedia Tools and Applications*, *83*(36), pp.84195-84229.

[9] Fugkeaw, S., Wirz, L. and Hak, L., 2023. Secure and lightweight blockchain-enabled access control for fog-assisted IoT cloud based electronic medical records sharing. *IEEE access*, *11*, pp.62998-63012.

[10] Dong, Y., Mun, S.K. and Wang, Y., 2023. A blockchain-enabled sharing platform for personal health records. *Heliyon*, *9*(7).

[11] Alzubi, J.A., Alzubi, O.A., Singh, A. and Ramachandran, M., 2022. Cloud-IIoT-based electronic health record privacy-preserving by CNN and blockchain-enabled federated learning. *IEEE Transactions on Industrial Informatics*, *19*(1), pp.1080-1087.

[12] Zala, K., Thakkar, H.K., Jadeja, R., Singh, P., Kotecha, K. and Shukla, M., 2022. PRMS: design and development of patients' E-healthcare records management system for privacy preservation in third party cloud platforms. *Ieee Access*, *10*, pp.85777-85791.

[13] Amanat, A., Rizwan, M., Maple, C., Zikria, Y.B., Almadhor, A.S. and Kim, S.W., 2022. Blockchain and cloud computing-based secure electronic healthcare records storage and sharing. *Frontiers in Public Health*, *10*, p.938707.

[14] Singh, M.K., Pippal, S.K., Sharma, V. and Chakraverti, A.K., 2026. Blockchain-enabled Patient-Centric Privacy Preservation and Access Control for Electronic Health Record Sharing. *SN Computer Science*, *7*(4), p.317.