International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

IJISAE

ISSN:2147-6799 www.ijisae.org Original Research Paper

Privacy Preserving Cyber Security System Framework for Secure Cloud-based Medical Data Transactions

Sunil D. Kale[1], Sushanth Chandra Addimulam[2], K. Kiran Kumar[3], Vinay Avasthi[4], Surbhi Sharma[5], Arunava De[6]

Submitted: 04/02/2024 **Revised**: 12/03/2024 **Accepted**: 18/03/2024

Abstract: With the increasing adoption of cloud storage in healthcare, ensuring the privacy and security of medical data has become a critical concern. This paper presents a comprehensive framework for privacy-preserving cybersecurity to secure medical data transactions in cloud storage environments. The proposed framework focuses on preserving the confidentiality and integrity of medical data while facilitating secure transactions. It integrates encryption methods to safeguard sensitive data both at rest and during transmission, guaranteeing that only authorized individuals have the ability to access and decrypt the information. Access controls are implemented to enforce fine-grained permissions, restricting data access to authorized personnel based on roles and privileges. Additionally, the framework includes mechanisms for secure authentication and identity verification to prevent unauthorized access and mitigate the risk of data breaches. Compliance with regulatory requirements such as HIPAA and GDPR is also addressed to ensure that the framework meets the necessary standards for protecting patient privacy. By integrating privacy preservation principles with robust cybersecurity measures, the proposed framework provides a comprehensive solution for securely managing medical data in cloud storage, enhancing trust and confidence in digital healthcare systems.

Keywords: *Privacy preservation, Cybersecurity, Medical data, Cloud storage, Secure transactions*

1. Introduction

In recent years, the healthcare sector has witnessed a significant transformation with the widespread adoption of cloud storage solutions. This shift towards cloud-based infrastructure offers numerous benefits, including enhanced scalability, accessibility, and cost-effectiveness [1]. However, alongside these advantages come inherent risks, particularly concerning the privacy and security of medical data. As healthcare organizations increasingly rely on cloud storage to store and manage sensitive patient information, ensuring the confidentiality, integrity, and availability of this data has become a paramount concern [2].

To address these challenges, this paper presents a comprehensive framework for privacy-preserving cybersecurity in cloud-based medical data transactions. This framework is designed to mitigate the risks associated with storing and transmitting medical data in cloud environments while preserving patient privacy and confidentiality. Central to this framework is the integration of encryption methods, access controls, secure authentication mechanisms, and regulatory compliance measures, aimed at providing a holistic solution for securely managing medical data in cloud storage environments [3].

Smart healthcare frequently integrates Electronic Health Records (EHR) with cloud-based data, merging these EHR with mobile Internet of Things (IoT) technologies through the utilization of IoT devices and communication tools. This integration aims to advance medical and health services while enhancing administrative functions. Despite the rapid advancements in smart healthcare, security concerns persist [4]. Blockchain technology offers various features, including decentralization, Peer-to-Peer (P2P) networking architecture, confidentiality, tamper-resistance, and auditability. These attributes can prove effective for facilitating data sharing, transactions, and supply-chain management within the healthcare sector. In essence, the combination of EHR, cloud data, and IoT devices in smart healthcare holds promise for revolutionizing healthcare delivery and administration. However, the adoption of these technologies also introduces security vulnerabilities [5,6].

[1] *Department of Artificial Intelligence and Data Science, Vishwakarma Institute of Information Technology, Pune.*
Email: kalesunild@gmail.com
[2] *Sr. Infrastructure and Security Engineer,*
Applied Computer Techniques 28345 Beck Road STE 308, Wixom, MI-48393.
Email: sushanth93@gmail.com
[3] *Professor, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.*
Email:kiran5434@kluniversity.in
[4] *Professor, Dept. of CSE,*
Himalayan School of Science & Technology,
Swami Rama Himalayan University, Dehradun.
Email: vinayddun@gmail.com
[5] *Assistant Professor,*
ABES Engineering College, Ghaziabad-201009.
Email: surbhis676@gmail.com
[6] *Professor, Faculty of Information Technology,*
Gopal Narayan Singh University, Jamuhar, Rohtas, Bihar-821305
Email: arunavade@yahoo.com

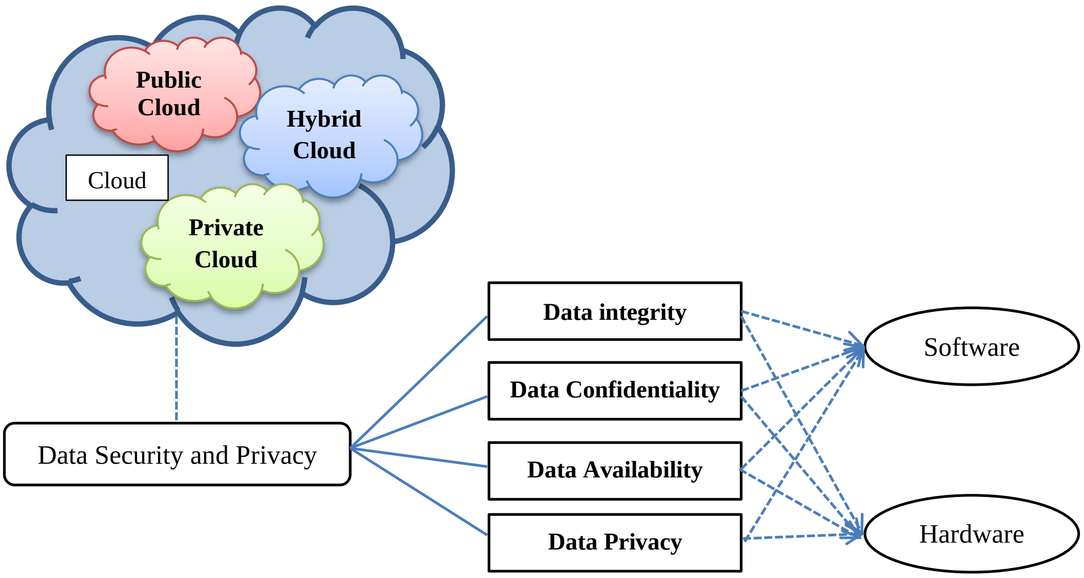

Fig. 1. Management of Privacy and Data Security in Cloud Computing

At the core of the proposed framework lies the use of encryption techniques to safeguard sensitive medical data both at rest and during transmission. Encryption serves as a fundamental mechanism for protecting data by encoding it into an unreadable format, thereby ensuring that only authorized individuals with the appropriate decryption keys can access and decipher the information [7]. By employing encryption methods such as symmetric and asymmetric encryption algorithms, the framework aims to provide robust protection for medical data stored in cloud environments, mitigating the risk of unauthorized access and data breaches.

In addition to encryption, the framework incorporates access controls to enforce fine-grained permissions and restrict data access to authorized personnel based on predefined roles and privileges. Access control mechanisms ensure that only authorized individuals, such as healthcare professionals and authorized personnel, have the necessary permissions to access specific medical records. By delineating access rights and implementing robust authentication mechanisms, such as multi-factor authentication and biometric verification, the framework bolsters the security posture of the system and fosters compliance with regulatory standards such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR).

Furthermore, the framework includes mechanisms for secure authentication and identity verification to prevent unauthorized access and mitigate the risk of data breaches. Secure authentication mechanisms, such as digital certificates and token-based authentication, are employed to verify the identity of users and devices accessing medical data stored in cloud environments, enhancing the overall security posture of the system.

Compliance with regulatory requirements is also a critical aspect of the proposed framework. By adhering to stringent data protection regulations such as HIPAA and GDPR, the framework ensures that medical data is handled and stored in accordance with legal and ethical considerations, thereby safeguarding patient privacy and maintaining regulatory compliance.

In conclusion, this paper presents a comprehensive framework for privacy-preserving cybersecurity in cloud-based medical data transactions. By integrating encryption techniques, access controls, secure authentication mechanisms, and regulatory compliance measures, the framework offers a holistic solution for securely managing medical data in cloud storage environments. By enhancing trust and confidence in digital healthcare systems, this framework paves the way for the seamless integration of cloud technologies into the healthcare ecosystem, ultimately benefiting patients, healthcare providers, and other stakeholders alike.

2. Literature Review

In [8], data protection is accomplished by preserving data privacy utilizing the implementation of the Tracy-Singh product and the proposed CAViaR-based BSA, which results in the greatest privacy-preserving coefficients. Combining CAViaR and BSA yields in the intended CAViaR-based BSA. Utility and privacy functions are combined to establish a novel objective function. With minimum responsiveness of 251.339 s, maximal detection of sincere consumers of 32.451%, maximal security of 96.5%, and minimal information loss of 3.5%, the proposed CAViaR-based BSA operates superior to other approaches.

[9] Presented a blockchain-based medical data information system that permits the secure collection, storage, and sharing of EMR and SHR data, thus dealing with the flaws of the existing medical information system. It was recommended to employ an Internet of Things (IoT) based medical data collection system that collects the data generated through medical devices, which might improve the durability and effectiveness of SHR data collection. The test's result suggests the system's whole efficiency is influenced by how effectively the blockchain system runs.

[10] In terms of System Execution Time (SET) and Average Delay, the Secure and Robust Healthcare-based Blockchain conduct (SRHB) is put up against the recommended PRMS (Patient Medical Records Management System). Information minimizing, effective medical data sharing, and user privacy maintenance are only some of the quality matrices that gauge how effective a suggested PRMS design performs. PRMS is a security architecture that allows patients legal title over their health knowledge while blocking illegal access to patient health records preserved in third-party databases.

[4] Recommended SPChain, a blockchain-based medical data swap, and privacy-preserving eHealth system, as an alternative to the foregoing difficulties. Additionally, the basic structure of blockchains enables data retrieval in blockchain-based eHealth systems inefficiently. At last, we brought up how the system's implementation on an analog network leveraging real-world miner distribution data can meet the proposal's security requirements. We examined the storage charges and the processing costs of data extraction with certain of the present-day solutions. The final results confirmed our system's durability and performance.

[5] Illustrated how to employ blockchain, DDSS, and hybrid computing to provide architecture-level solutions to the issues increased. The proposed architecture simultaneously provides a platform for different stakeholders in the healthcare field to make digital agreements; in addition, smart agreements automate medical emergency alerting and primary medical services. The system-level traceability is achieved through blockchain-based tamper-proof public ledgers. Other proposed cryptography techniques, like SRAC, guarantee the security and privacy of medical data.

[6] Proposed a layered architecture for a cloud-based, secure edge healthcare system that enables real-time disease prediction, diagnosis, and rehabilitation. For securing data at the outermost computing layer, the recommendation implements additive homomorphic encryption that sustains privacy and leverages sophisticated filtering and offloading mechanisms to minimize the response time and network bandwidth between the edge and cloud layers.

[7] Suggested an arrangement that might allow the safe exchanging of electronic health records (EHRs) throughout multiple parties while leveraging probably suspicious third-party services, involving cloud computing, was the issue of this thesis. The fragile state of health data requires that the response to this difficulty must be able to provide acceptable security and privacy. We developed a framework for the transmission of electronic health data to develop this solution. A dominant ABE methodology termed Multi-Authority Ciphertext Policy Attribute Based Encryption with Outsourcing (MACP-ABEwO) provides the core of our framework.

3. Methodology

The methodology for implementing the proposed framework for privacy-preserving cybersecurity in healthcare cloud storage environments encompasses a systematic approach to address the complex challenges of securing medical data while ensuring compliance with regulatory standards such as HIPAA and GDPR.

The first step involves conducting a comprehensive literature review to gain insights into existing frameworks, challenges, and best practices related to cloud storage security in healthcare. This review serves as the foundation for understanding the specific requirements and considerations relevant to safeguarding medical data in cloud environments.

Based on the findings from the literature review, the next phase focuses on identifying the precise requirements for the framework. This involves determining the essential components necessary to ensure the privacy and security of medical data, including encryption methods, access control mechanisms, authentication protocols, and regulatory compliance measures.

With the requirements clearly defined, the framework design phase begins. Here, the emphasis is on developing a cohesive and integrated solution that addresses all identified needs. The design incorporates robust encryption techniques to protect data both at rest and during transmission, ensuring confidentiality and integrity. Access control mechanisms are implemented to enforce fine-grained permissions, restricting data access to authorized personnel based on their roles and privileges.

Authentication and identity verification mechanisms are integral parts of the framework design, aimed at preventing unauthorized access and mitigating the risk of data breaches. Secure authentication methods, such as multi-factor authentication, are employed to verify user identities effectively. Identity verification mechanisms further enhance security by confirming the authenticity of users before granting access to sensitive data.

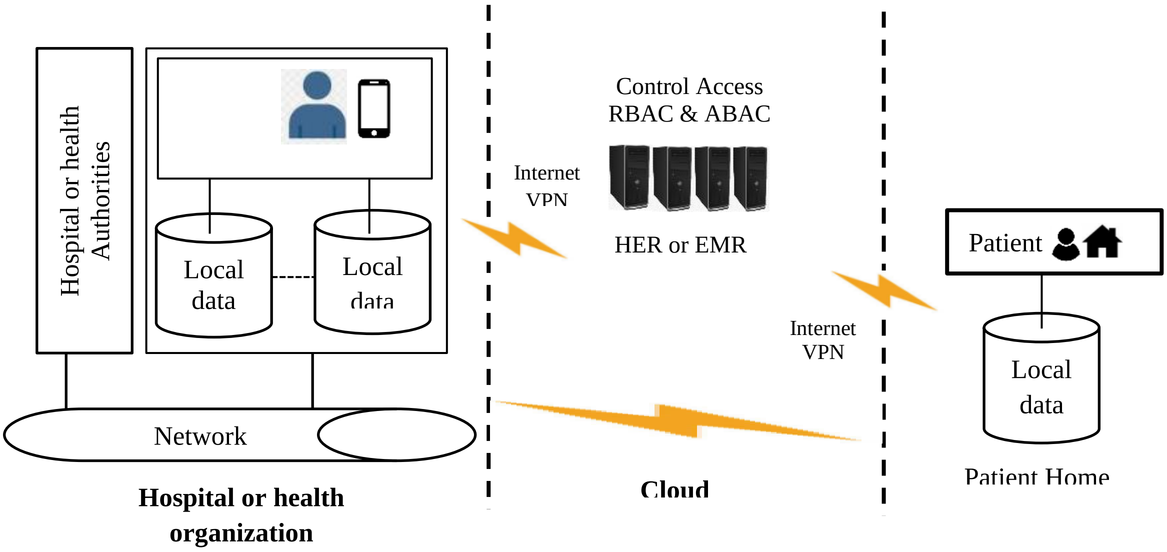

Fig. 2. Proposed System Architecture

To ensure compliance with regulatory requirements, the framework is designed to adhere to standards such as HIPAA and GDPR. This involves incorporating features and safeguards that align with the specific provisions outlined in these regulations, thereby ensuring that patient privacy is adequately protected.

This method is essential for securely processing sensitive patient data in cloud environments as shown in Figure 2. It ensures compliance with privacy regulations and standards, facilitates efficient data management, and fosters trust among patients and healthcare providers by safeguarding information integrity and confidentiality. The initial phase of the framework involves the planning of the Privacy Preserving Data Security Management System (PP-DSMS), comprising several pivotal steps.

Firstly, gaining approval to commence the DSMS is imperative to ensure organizational endorsement and comprehension of its objectives. Subsequently, assessing the organization's structure and behavior, along with conducting a thorough risk evaluation, is undertaken. This evaluation entails identifying potential security risks, vulnerabilities, and threats to healthcare data stored and managed in the cloud. This information enables informed decision-making regarding the implementation of effective security measures and risk mitigation strategies. Following the risk assessment, the development of a Risk Management and Treatment Plan becomes imperative. This plan delineates selected security controls, risk mitigation strategies, and protocols for monitoring, reviewing, and continuously enhancing the DSMS. Finally, the DSMS is established, incorporating all identified processes, controls, and guidelines to furnish a comprehensive and secure framework for healthcare data management in the cloud.

Once the framework design is finalized, the integration and testing phase commences. All components of the framework are integrated into a cohesive solution, and rigorous testing is conducted to validate its effectiveness and reliability. This testing encompasses

various scenarios and use cases to ensure that the framework performs as intended under different conditions.

Documentation and deployment guidelines are prepared to facilitate the implementation of the framework in healthcare organizations. Training materials are developed to educate personnel on using the framework effectively and adhering to security protocols.

Validation and feedback from stakeholders, including healthcare professionals and IT experts, are sought to assess the framework's efficacy and usability. Continuous improvement efforts are undertaken based on this feedback, as well as emerging threats and regulatory changes, to ensure that the framework remains effective in safeguarding medical data in cloud storage environments.

In summary, the methodology for implementing the proposed framework for privacy-preserving cybersecurity in healthcare cloud storage environments follows a systematic approach encompassing literature review, requirement identification, framework design, integration and testing, documentation and deployment, validation and feedback, and continuous improvement. Through these steps, the framework aims to provide a comprehensive solution for securely managing medical data in cloud storage, thereby enhancing trust and confidence in digital healthcare systems.

4. Result and Discussion

Ensuring security in cloud computing, especially concerning medical data, is paramount. Protecting patients' privacy and data safety are crucial, given the increasing use of cloud technology in healthcare. This paper explores security management in cloud computing for healthcare data, focusing on challenges, approaches, and potential solutions. With sensitive patient information stored and processed in the cloud, addressing security concerns becomes imperative. The discussion emphasizes the importance of robust security measures to uphold patient privacy rights and mitigate risks associated with data breaches in the healthcare industry's evolving landscape.

The rapid expansion of cloud computing has revolutionized the healthcare industry, offering scalability, cost-effectiveness, and access to extensive computing resources. However, migrating healthcare data to the cloud introduces inherent security risks, including unauthorized access, data breaches, and privacy violations. Therefore, implementing robust security management practices is crucial to safeguard patient information and uphold trust in healthcare systems. Given the sensitive nature of patient data, prioritizing effective security measures is essential to maintain confidentiality and integrity within healthcare environments.

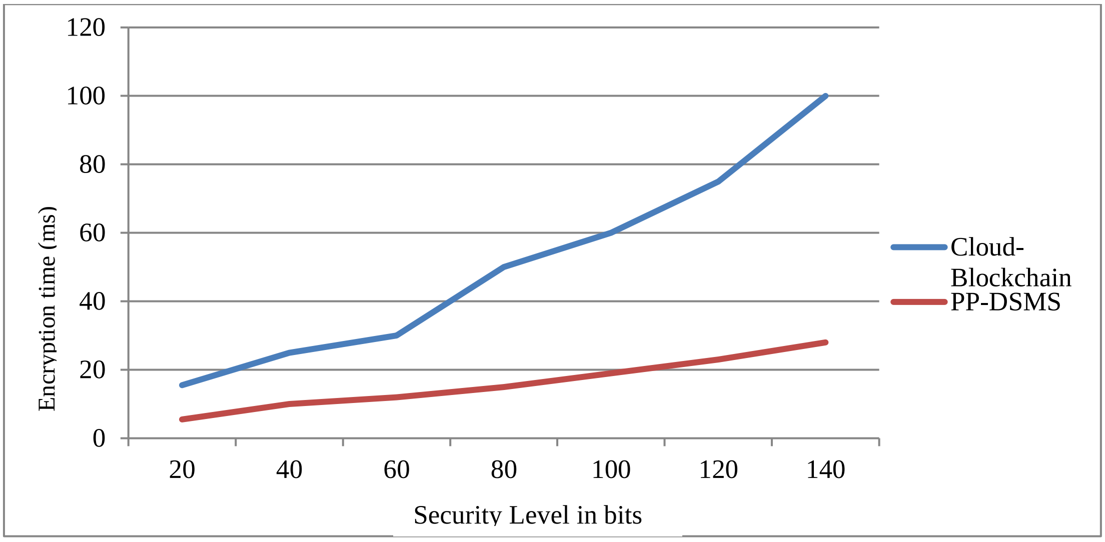

Fig. 3. Duration of Encryption

Figure 3 represents the encryption duration result graph. The x-axis would represent the file size and the security level, ranging from small to large files, and the y-axis would represent the encryption time required for each file size. The proposed PP-DSMS is compared with tradition cloud-blockchain system and the outcome shows that the proposed model takes less time to encrypt data than the cloud-blockchain system. It shows the efficiency of the proposed cybersecurity system.

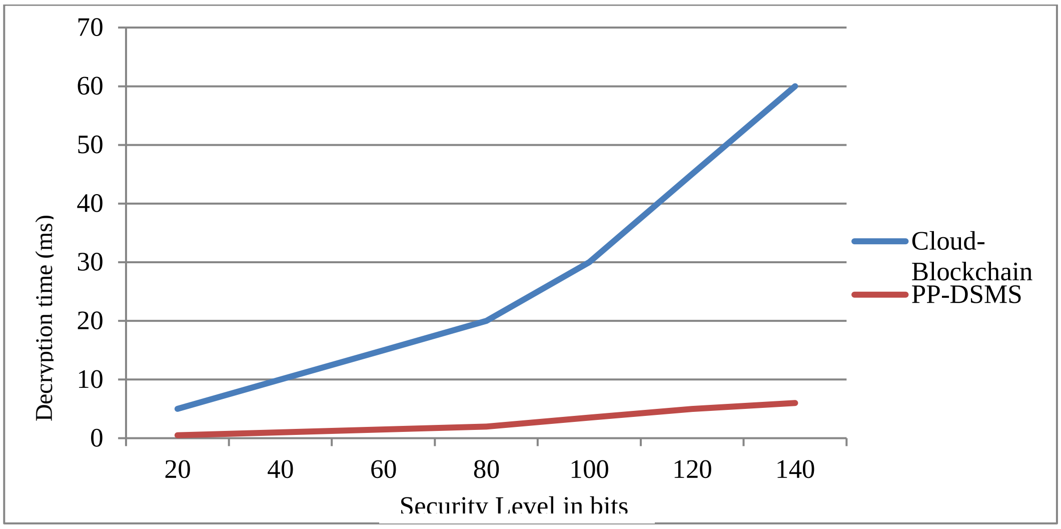

Fig. 4. Duration of Decryption

When encryption time is low, it means that the process of encrypting data takes less time to complete. This is beneficial for systems and applications that require quick and efficient encryption, especially in scenarios where data needs to be encrypted and decrypted frequently, such as medical or data storage applications. However, it's also important to balance encryption time with the level of security provided by the encryption algorithm. While faster encryption times are desirable for efficiency, PP-DSMS ensure THE high level of security to protect sensitive information from unauthorized access.

Table 1. Comparative Analysis

Parameters	**Cloud-Blockchain**	**PP-DSMS**
Time for data storage	2ms	900ns
Time for accessing data	4ms	2ms
Uptime	98%	100%
Downtime	1.5%	0% (Negligible)
Storage space	Cloud limited	Number of nodes limited
Data integrity	96%	98%
Scalability	No	Yes
Data encryption cost	High	Low
Maximum file size	2GB	Unlimited

However, similar to encryption time, it's important to balance decryption time with the level of security provided by the decryption algorithm. While faster decryption times are desirable for efficiency, it's crucial to ensure that the decryption method used still provides a high level of security to protect sensitive information from unauthorized access. Figure 4 depicts that the proposed method provides high efficiency by take less decryption time and also maintain highest security level. Comparative analysis of the models is represented in Table 1.

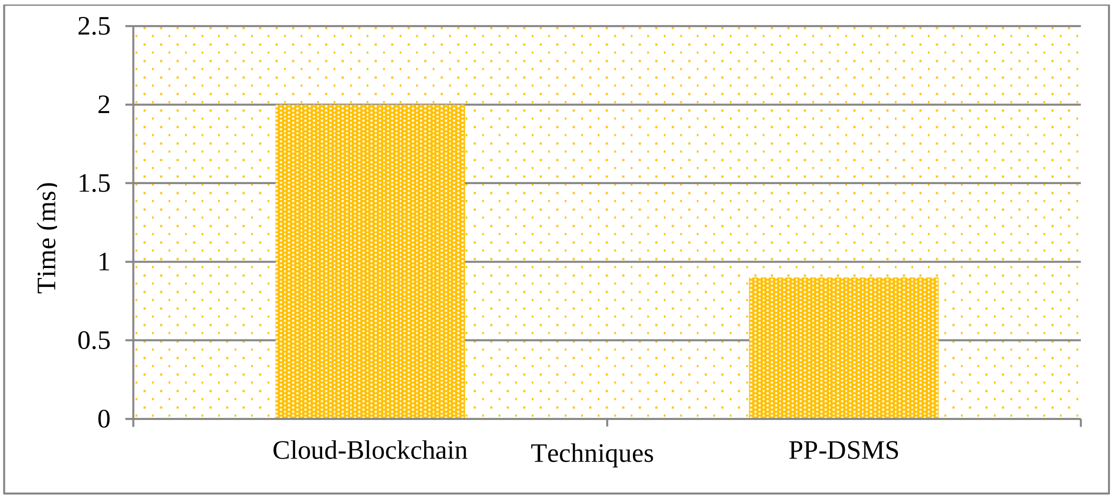

Fig. 5. Storage Time Evaluation

From the table 1, the time for data storage and data accessing is understandable for the proposed system framework. The analysis presented in Figure 5 indicates that the proposed PP-DSMS system surpasses the performance of the cloud-based blockchain system. The graph trend demonstrates a shorter storage time, specifically 0.9 milliseconds in the DSMS of the proposed system, in contrast to the 2 milliseconds in the cloud-based system. This improvement is attributed to the utilization of a smart contract with fewer steps in the proposed authorization scheme.

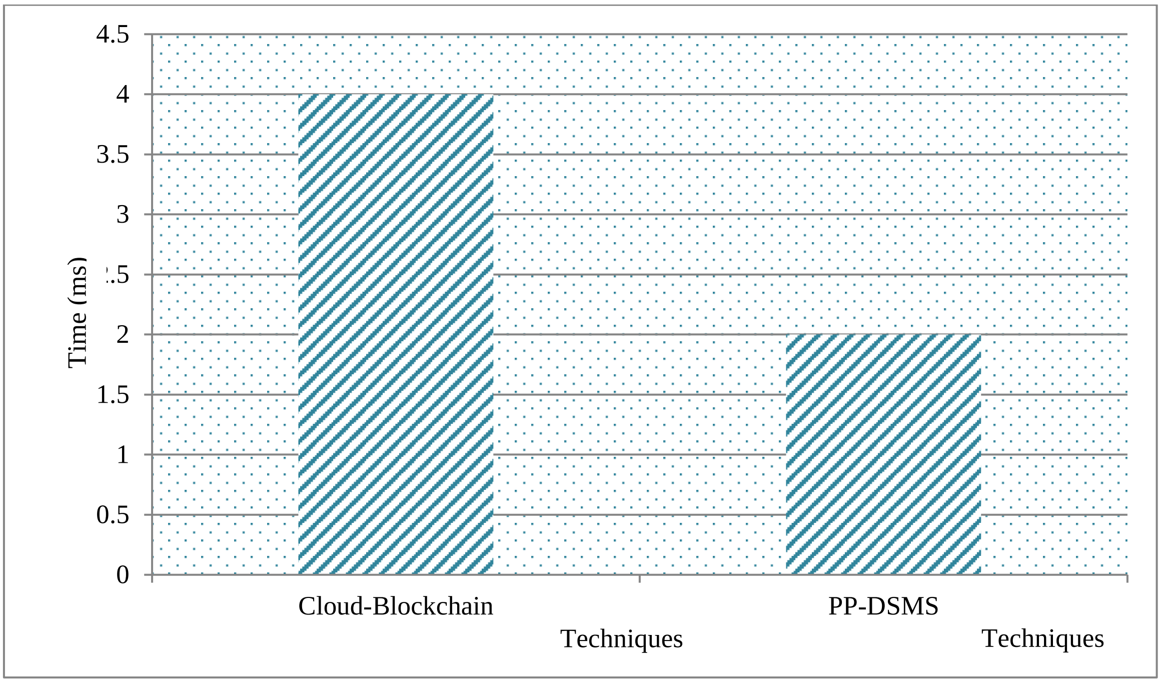

Fig. 6. Access Time Evaluation

Figure 6 depicts the performance evaluation regarding the time needed for accessing storage and retrieving files. The graph illustrates that accessing a 50 MB file is generally quicker in the proposed system compared to the cloud-based setup. This is attributed to the utilization of the DSMS network as data storage nodes, where files are stored in a decentralized manner, not reliant on a central server. Consequently, the system identifies the nearest unit for storage, reducing latency and enhancing storage and retrieval efficiency.

5. Conclusion

The paper introduces a comprehensive framework called privacy preserving data security management system (PP-DSMS) to meet the urgent demand for privacy-preserving cybersecurity in healthcare, propelled by the widespread integration of cloud storage solutions. Through meticulous integration of encryption techniques, the framework ensures robust data confidentiality and integrity, both at rest and during transmission, allowing access solely to authorized entities. Implementation of fine-grained access controls further strengthens security by limiting data access to authorized personnel based on predefined roles and privileges. Moreover, the framework incorporates sophisticated authentication and identity verification mechanisms to thwart unauthorized access attempts and mitigate the likelihood of data breaches. By amalgamating privacy preservation principles with robust cybersecurity measures, the framework offers a comprehensive solution for securely managing medical data within cloud storage environments, addressing the complex challenges posed by modern healthcare data management. Ultimately, this approach fosters trust and confidence in digital healthcare systems by assuring stakeholders of the steadfast protection of sensitive medical information. Through its multifaceted approach encompassing encryption, access controls, authentication, and regulatory compliance, the framework establishes a resilient foundation for the secure and efficient handling of medical data in the cloud, thereby promoting the advancement of digital healthcare while mitigating associated risks.

References

[1] Mishra, A., Jabar, T. S., Alzoubi, Y. I., & Mishra, K. N. (2023). Enhancing privacy-preserving mechanisms in Cloud storage: A novel conceptual framework. *Concurrency and Computation: Practice and Experience*, e7831.

[2] Amanat A, Rizwan M, Maple C, Zikria YB, Almadhor AS and Kim SW (2022) Blockchain and cloud computing-based secure electronic healthcare records storage and sharing. *Front. Public Health* 10:938707. doi: 10.3389/fpubh.2022.938707

[3] Huang, L., & Lee, HH. (2020). A Medical Data Privacy Protection Scheme based on Blockchain and Cloud Computing. *Wireless Communications and Mobile Computing, 2020,* 1-11.

[4] Hemanth Kumar, N.P., & Prabhudeva, S. (2022). An Authorization Framework for Preserving Privacy of Big Medical Data via Blockchain in Cloud Server. International Journal of Advanced Computer Science and Applications, 13(3), 140-150.

[5] Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. Data Security and Privacy in Cloud Computing. International Journal of Distributed Sensor Networks, 2014, 1-9.

[6] Alabdulatif, A., Thilakarathne, N. N., & Kalinaki, K. (2023). A Novel Cloud Enabled Access Control Model for Preserving the Security and Privacy of Medical Big Data. *Electronics*, *12*(12), 2646.

[7] Qin, C., Wu, L., Meng, W., Xu, Z., Li, S., & Wang, H. (2023). A privacy-preserving blockchain-based tracing model for virus-infected people in cloud. *Expert Systems with Applications*, *211*, 118545.

[8] Gajmal, Y. M., & Udayakumar, R. (2022). Privacy and utility-assisted data protection strategy for secure data sharing and retrieval in cloud system. *Information Security Journal: A Global Perspective*, *31*(4), 451-465.

[9] Chen, Z., Xu, W., Wang, B., & Yu, H. (2021). A blockchain-based preserving and sharing system for medical data privacy. *Future Generation Computer Systems*, *124*, 338-350.

[10] Zala, K., Thakkar, H. K., Jadeja, R., Singh, P., Kotecha, K., & 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*, 85777-85791.

[11] Zou, R., Lv, X., & Zhao, J. (2021). SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system. *Information Processing & Management*, *58*(4), 102604.

[12] Egala, B. S., Pradhan, A. K., Badarla, V., & Mohanty, S. P. (2021). Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control. *IEEE Internet of Things Journal*, *8*(14), 11717-11731.

[13] Jayaram, R., & Prabakaran, S. (2021). Onboard disease prediction and rehabilitation monitoring on secure edge-cloud integrated privacy preserving healthcare system. *Egyptian Informatics Journal*, *22*(4), 401-410.

[14] Ilokah, M. (2020). *Design of a secure privacy preserving cloud based framework for sharing electronic health data*. University of Ontario Institute of Technology (Canada).