



















ORIGINAL

## Privacy and security framework for medical data in a cloud infrastructure utilizing lightweight blockchain technology

### Marco de privacidad y seguridad para datos médicos en una infraestructura en la nube que utiliza tecnología blockchain liviana

Kosim Rakhmanov<sup>1</sup>  , Dilfuza Makhmudova<sup>2</sup>  , Shaanvar Shamansurov<sup>3</sup>  , Mexrangiz Narzullayeva<sup>4</sup>   
, Zebo Almatova<sup>5</sup>  , Ugilkhon Akilova<sup>6</sup>  , Nadira Mirametova<sup>7</sup>  , Aynash Omarova<sup>8</sup>  

<sup>1</sup>Samarkand State Medical University, Uzbekistan.

<sup>2</sup>Chirchik State Pedagogical University, Chirchik, Uzbekistan.

<sup>3</sup>Center for development of professional Qualification of medical workers, Tashkent, Uzbekistan.

<sup>4</sup>Samarkand State Medical University, Samarkand, Uzbekistan.

<sup>5</sup>Jizzakh State Pedagogical University, Uzbekistan.

<sup>6</sup>“Tashkent Institute of Irrigation and Agricultural Mechanization Engineers” National Research University, Tashkent, Uzbekistan.

<sup>7</sup>Ajiniyaz Nukus State Pedagogical Institute.

<sup>8</sup>Tashkent Institute Of Chemical Technology.


**Cite as:** Rakhmanov K, Makhmudova D, Shamansurov S, Narzullayeva M, Almatova Z, Akilova U, et al. Privacy and security framework for medical data in a cloud infrastructure utilizing lightweight blockchain technology. Health Leadership and Quality of Life. 2024;3:193. <https://doi.org/10.56294/hl2024.193>

Submitted: 02-03-2024

Revised: 24-06-2024

Accepted: 03-11-2024

Published: 04-11-2024

Editor: PhD. Prof. Neela Satheesh 

Corresponding author: Kosim Rakhmanov 

#### ABSTRACT

Cloud-based information has consistently attracted cyber attackers. Medical Data (MD) on the cloud has emerged as a new focal point of interest. Assaults on MD may have devastating repercussions for healthcare companies. The decentralized management of cloud data helps mitigate the impact of assaults. A public ledger supported by a decentralized network of peers has been shown to provide reliable, auditable computing using Blockchain Technology (BT). Implementing authorization mechanisms and cryptographic primitives is inadequate for mitigating contemporary cyber risks and resolving privacy and security issues related to cloud-based environments. This study presents a Privacy and Security Framework in Cloud Infrastructure employing Lightweight Blockchain Technology (PSF-CI-LBT) for MD. A patient-focused MD management program using BT for storage has been introduced to enhance privacy. Cryptographic algorithms are employed to encrypt patients' MD and to guarantee concealment. The encryption, decryption time, and economic feasibility (cost) of the proposed technique's smart contract (SC) framework are assessed, along with the methodologies used for analyzing MD to encrypt and mask a patient's MD.

**Keywords:** Privacy; Security; Medical Data; Cloud; Blockchain; Lightweight; Cryptography.

#### RESUMEN

La información basada en la nube ha atraído constantemente a los atacantes cibernéticos. Los datos médicos (MD) en la nube han surgido como un nuevo punto focal de interés. Los ataques a los MD pueden tener repercusiones devastadoras para las empresas de atención médica. La gestión descentralizada de los datos en la nube ayuda a mitigar el impacto de los ataques. Se ha demostrado que un libro de contabilidad público respaldado por una red descentralizada de pares proporciona computación confiable y auditable utilizando tecnología Blockchain (BT). La implementación de mecanismos de autorización y primitivos criptográficos es inadecuada para mitigar los riesgos cibernéticos contemporáneos y resolver problemas de privacidad y

seguridad relacionados con los entornos basados en la nube. Este estudio presenta un marco de privacidad y seguridad en la infraestructura de la nube que emplea tecnología Blockchain ligera (PSF-CI-LBT) para MD. Se ha introducido un programa de gestión de MD centrado en el paciente que utiliza BT para el almacenamiento para mejorar la privacidad. Se emplean algoritmos criptográficos para cifrar los MD de los pacientes y garantizar la ocultación. Se evalúan el cifrado, el tiempo de descifrado y la viabilidad económica (costo) del marco de contrato inteligente (SC) de la técnica propuesta, junto con las metodologías utilizadas para analizar MD para cifrar y enmascarar los MD de un paciente.

**Palabras clave:** Privacidad; Seguridad; Datos Médicos; Nube; Blockchain; Ligero; Criptografía.

## INTRODUCTION

Significant efforts are underway to integrate MD and information technology, resulting in substantial transformations within the healthcare sector. These alterations impact patients' treatment procedures, necessitating meticulous data management.<sup>(1)</sup> Healthcare treatment relies entirely on data, raising issues around information security and privacy. Authorization or restricted access to a person's private MD pertains to the concept of privacy, signifying that only verified entities may access confidential information. Securing personal MD against eavesdroppers or invaders pertains to security, which denotes the system's capability to safeguard users' private information from external threats.<sup>(2)</sup> Authorized entities involved in the MD security process will get authorization to save and access MD from the cloud. The relationship between the system and the patient needs a secure connection. Various authentication protocols<sup>(3,4)</sup> have been developed to safeguard privacy and security. Inadequate security may lead to catastrophic outcomes such as data loss and theft. Numerous hackers seek unsecured channels to access critical MD inside the cloud network. In several instances, MD loss has adverse effects on patients and healthcare institutions.<sup>(5)</sup> Recent assaults on MD inside cloud systems have resulted in significant data loss in many nations, including the USA and the UK. Patients' private MD was stored on the cloud without encryption, enabling attackers to expropriate crucial information. Assume a situation in which patients save their data in an Electronic Medical Record (EMR) system for archiving and subsequent access.<sup>(6)</sup>

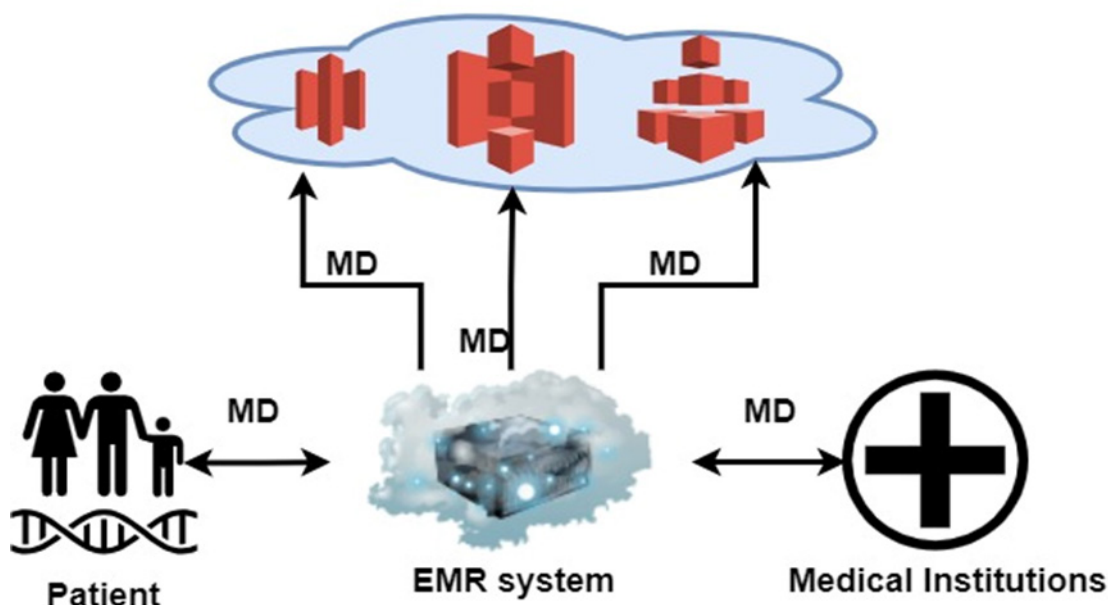


Figure 1. Generalized structure of EMR systems

Figure 1 illustrates a generalized structure of EMR systems. In the illustration, patients and healthcare institutions engage as data transmitters and recipients. The EMR system oversees the whole process that regulates the information flow inside the system. The primary component is the cloud, where data is stored. Patients provide their personal information to physicians and medical facilities via these EMR systems. Assume patients store their data in a cloud system that utilizes BT as an MD storage platform. The system will record the data on the BT upon the patient's sharing of her information with the system. The MD's responsibility is platform-centric, for instance,<sup>(7,8,9,10)</sup> whereby the system offers data storage services even when data is disseminated to physicians or medical organizations. Therefore, the system is accountable for data loss.

The abovementioned issues are resolved by storing encrypted MD in the cloud system. Consequently, if the system loses authority over the BT, patients will be responsible for their data since they manage the encryption keys alone. The patients regulate the sharing of information inside the system. The solution has mitigated risks associated with data preservation via the use of cryptographic functions and BT.<sup>(11,12)</sup> The system will securely store encrypted personal MD, safeguarding overall privacy; even in a cyberattack, the compromised data will remain incomprehensible to the attacker. Attackers will need the keys to obtain the plaintext of the encoded private MD. No identifiers exist for these records; only keys for encryption will be utilized to determine the encrypted and anonymous MD.<sup>(13)</sup>

### Privacy and Security Framework for Medical Data in a Cloud Infrastructure Utilizing Lightweight Blockchain Technology

The architecture and design perspectives of the proposed framework are shown in this section. The suggested PSF-CI-LBT model for MD is demonstrated in figure 2.

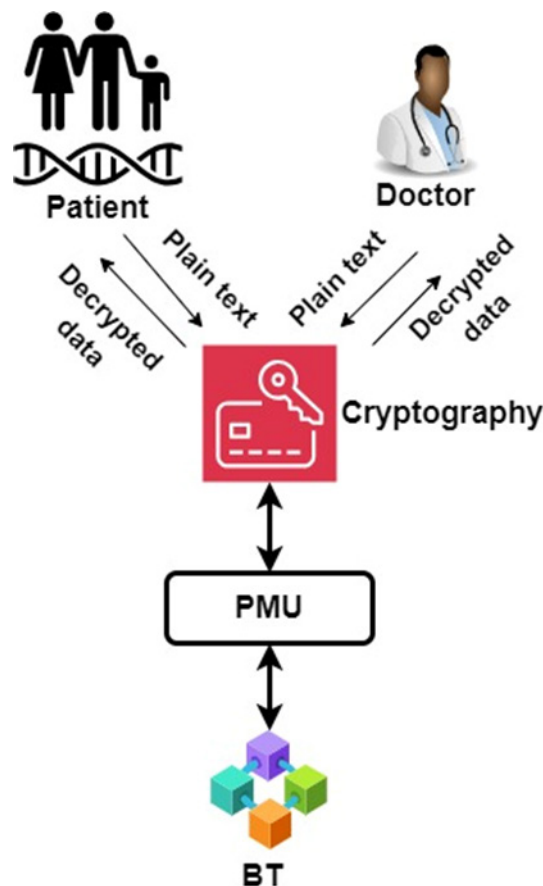


Figure 2. Architecture of the proposed PSF-CI-LBT for MD

The patient is the data transmitter and is accountable for transmitting their private MD to the system. A patient significantly contributes to safeguarding their own MD.<sup>(14)</sup> The data transmitted to the network must be precise; otherwise, any inaccuracies might adversely affect the patient since the whole therapy relies on this critical information. Nonetheless, our technology will acquire the consumers' encrypted data.<sup>(15)</sup> Data encryption will occur at the commencement of the suggested technique's execution procedure. Data recipients will solicit data after confirming their identities to the system. The User Registration Unit (URU) will function as the authentication tool.

The suggested method accommodates encrypted data from clients. Data encryption will occur at the commencement of the process's operation. Data receivers will solicit data after confirming their identities to the system.<sup>(16)</sup> The URU will function as the authentication method. Upon verification, both parties can engage with Private Manageable Units (PMUs) to transfer their private MD inside the cloud. They only require a login into the network and access over a secure route. The PMU will transmit users' private MD to the network.<sup>(17)</sup> The PMU is the intermediate unit between the components of the two tiers inside our system. The PMU necessitates an encrypted communication route for interaction with the PMU. The BT will retain the users' info. The LBT transactions will provide an identification that enables users to retrieve the data afterward.<sup>(18)</sup>

Our method is categorized into two tiers to enhance comprehension. The user will use the Graphical User

Interface (GUI) to engage with our system. The components of stage 1 are the URU and the PMU. In stage 2, the paper will engage with lower-level parts of the system via the PMU. An illustration of this is the component of stage 2: blockchain. BT is being used in the MD library.<sup>(19)</sup> These approaches use permission-based LBT, necessitating authentication. The procedures of LBT are as follows:

Stage 1: to enter the platform, the MD sender must submit their user ID and password.

Stage 2: upon acquiring admission to the system, the data transmitter will transmit MD to the PMU for storage.

Stages 3 and 4: the third and fourth steps of our system will transpire at level 2, wherein the PMU transmits the U\_ID (Block ID, indicating the location of user data storage) to the LBT, which subsequently returns the U\_ID, enabling users to enter the BT in the future and identify the precise block where the MD is stored.

Stage 5: the U\_ID produced by the BT will be delivered to the MD sender in this subsequent step.

Stage 6: from this point onward, the subsequent steps pertain to the MD receiver. This step necessitates signing in, in addition to step one, following which the data recipient may request MD.

Stage 7: in this stage, the MD receiver will solicit the data from the PMU, accompanied by the U\_ID. PMU will get the U\_ID for further usage.

Stage 8: in this step, the PMU will solicit the BT along with the U\_ID.

Stage 9: in this step, the LBT will respond by returning it to the PMU. Steps 8 and 9 replicate steps 3 and 4 with different MD.

Stage 10: the PMU transmits confidential information to the data receiver at this stage.

### Protocol among MD Transmitter and System

Figure 3 illustrates the low-level perspective of the transmitting protocol. A patient will assume the function of a data transmitter in this protocol. Encrypted information will be provided to the system. The production of ciphertexts relies only on a mechanism referred to as the encryption function [20]. The generic version of this function is  $Enc(x,y)$ . Subsequently, the operation of this function has been given below in equation (1)

$$Enc(key,Data) = U\_ID \quad (1)$$

U\_ID is the user identifier. By supplying the key and MD to this function, the information transmitter will generate a U\_ID and transmit it to the system. The public key encrypting method, such as Elliptic Curve Cryptography (ECC), will encrypt confidential information.<sup>(21)</sup> Let  $x$  be the data transmitter of the system.  $x$  will first seek access to the system by submitting the U\_ID  $_x$  (block number of user  $x$ ) and PD  $_x$  (Password of  $x$ ). The system will send a validation to  $x$  upon receipt of the correct U\_ID and password. If  $x$  successfully signs into the system and receives verification, they will transmit U\_ID  $_x$  to PMU over an encrypted channel. An encrypted channel will ensure the safety of data transfer. At this level, PMU will engage with the BT using the SC of the framework.

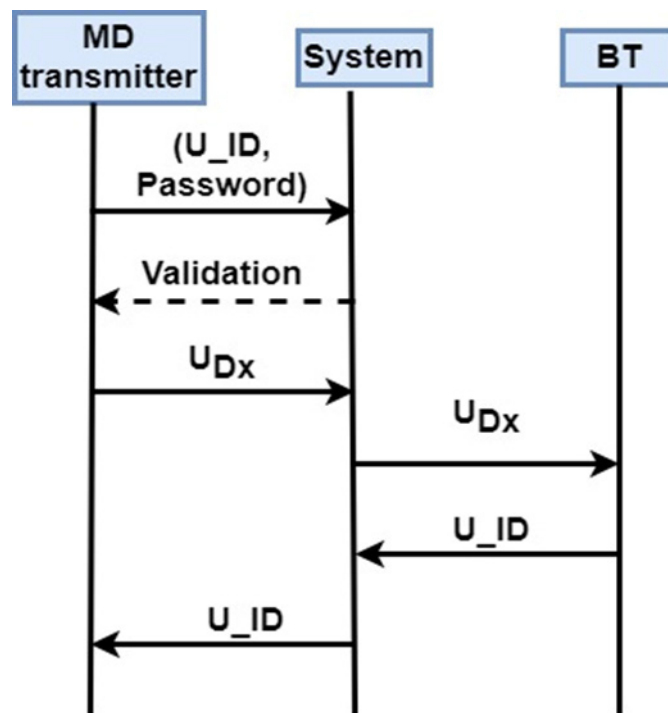


Figure 3. Low-level perspective of the transmitting protocol

The framework's SC is structured to ensure that the BT returns the block number designated as U\_ID  $_x$ .

Each block has a distinct identifier that serves as the identification for a certain patient. PMU will receive the  $U\_ID\_x$  for every MD transaction in the framework, which is designated as  $U\_ID\_x$  for  $x$ . PAU will transmit the  $U\_Dx$  (encrypted data of user  $x$ ) to the BT, after which the SC will generate and provide the unique identifier  $U\_ID\_x$ , for  $x$ . Subsequently, PMU will transmit the  $U\_ID\_x$  to  $x$  and conclude the protocol's execution.  $x$  must retain this  $U\_ID\_x$ ; otherwise,  $x$  will be unable to obtain their confidential information. Obtaining the  $U\_ID\_x$  serves as validation for  $x$ , indicating that the MD has been stored in the system, allowing  $x$  to sign out and terminate the encrypted communication with the overall system.

#### Protocol among MD Receiver and System

The proposed LBT system's reception process will need two authentication levels. Upon registering or logging into the system, parties must supply the  $U\_ID$  to get their MD over the protected channel. If they do not provide the  $U\_ID$  at this step, they cannot obtain their MD. The  $U\_ID$  is essential for obtaining the actual MD. Figure 4 illustrates a detailed perspective of the receiving process.<sup>(22)</sup> Assume user  $x$  seeks to recover the data they sent to the system during the transmission phase. Similar to the transmitting stage, this stage is regulated by a validation or registering unit, requiring  $x$  to sign in before gaining access to the system.<sup>(23)</sup> This login necessitates the user's ID and password provided during the registration process. The system will offer verification only if  $x$  gives the required  $U\_ID$  and password. Upon confirmation,  $x$  can engage with the system over an encrypted link. In this connection with the system,  $x$  must supply  $U\_ID\_x$ . Upon acquiring the  $U\_ID\_x$  system, it will engage with the BT. This contact will occur at the second stage of the LBT system.<sup>(24)</sup> Only PMU can engage with the BT; the system's SC will serve as the gateway.

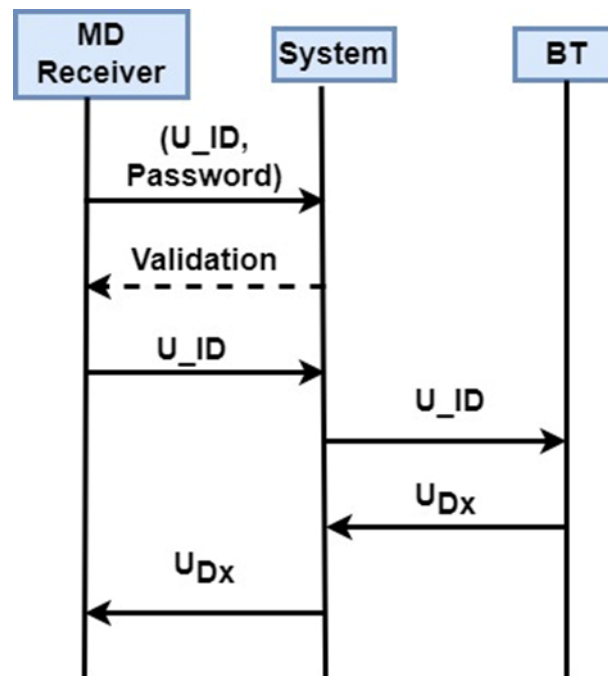


Figure 4. Low-level perspective of the receiving protocol

The SC will transmit the  $U\_ID\_x$  to the BT to get the MD of  $x$ . The 256-bit hash of the associated block number will be verified in the SC; the procedure to get the MD will proceed upon matching the hash to a given block. The circumstances will be managed using the SC.<sup>(25)</sup> Assume the hash of any given block is 0x3b1c1498fc1c149fb4c8196f927a4e49b34ca9991b75.

$x$  will only be allowed to access their MD if the hash of  $U\_ID\_x$ 's associated block is identical. The BT will transmit the  $U\_Dx$  to PMU, which will, after that, be routed to  $x$ . Upon the conclusion of this MD collection period, it will cease.  $x$  will get the  $U\_Dx$ , which must be decrypted to obtain the real raw MD.<sup>(26)</sup> To decode the MD, the user has to utilize the  $Dec(x,y)$

$$\text{function.Dec}(\text{key}, U\_Dx) = \text{plaintext} \quad (2)$$

$x$  will employ equation 2, using the key and  $U\_Dx$  to extract the raw MD.

## RESULTS AND DISCUSSION

The suggested methodology was evaluated by programming the application on the Java platform. The visual depiction of the performance metrics is created using MATLAB 2021a software on a Windows 10 operating system with 8GB RAM, using line and bar charts. For the performance evaluation of the proposed methodology, many performance metrics are studied, including encryption time, decryption time, and computational cost of the key.



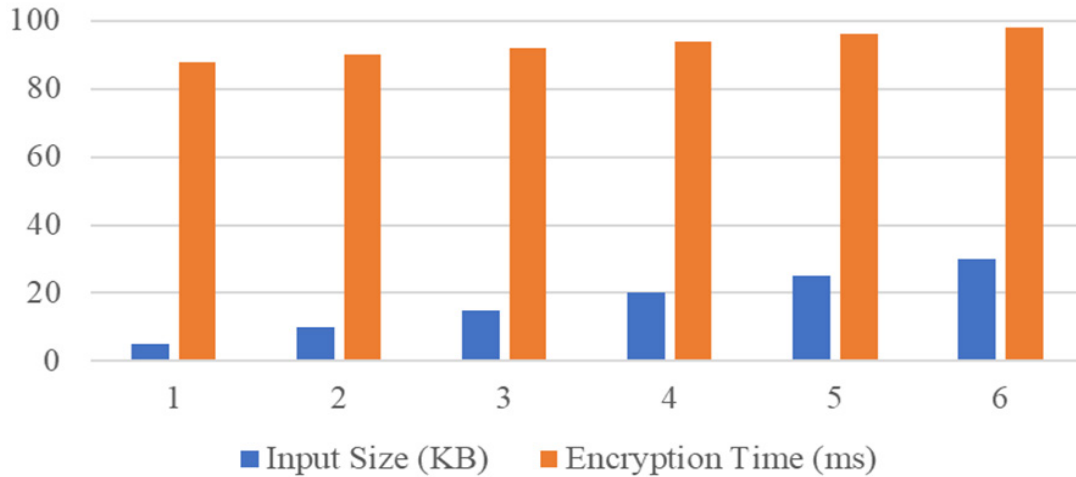


Figure 5. Encryption duration (ms) versus the input size (KB) of the MD

Figure 5 illustrates the encryption duration (ms) versus the input size (KB) of the MD. The suggested methods include measuring the encryption duration during the cipher text creation on the transmitter's end. This approach examines different input sizes to assess the degree of change in encryption time relative to input size. As the input file escalates from 5-30 KB, the encryption duration consistently increases from 89 ms to 97 ms. This signifies a linear association between input size and encryption duration, implying that more significant input quantities need more computing power for encryption. The incremental rise in duration signifies a foreseeable scaling of processing time according to data size expansion, a typical characteristic of encryption methods.

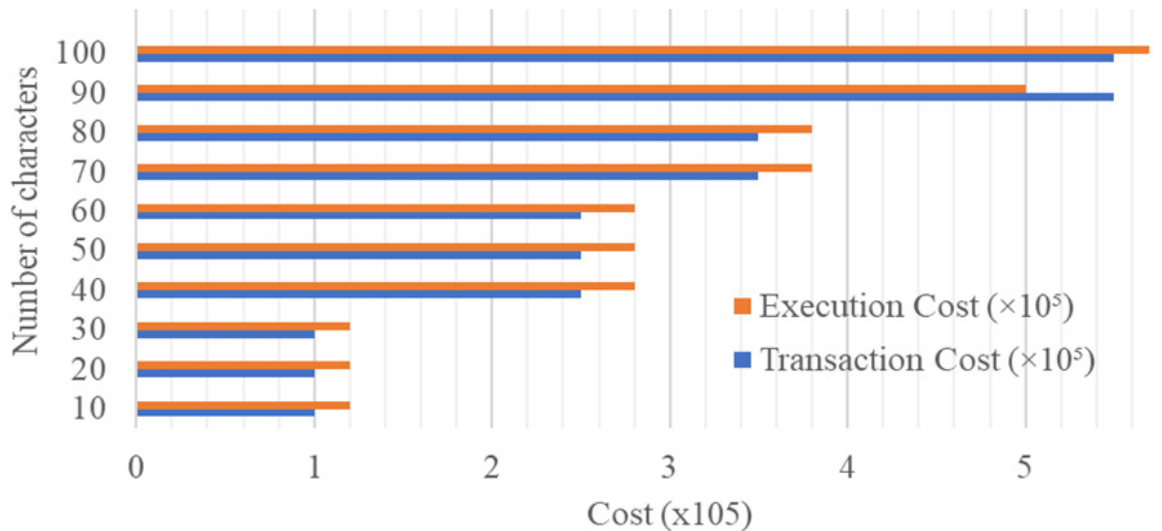


Figure 6. Economic feasibility (cost) analysis against the number of characters for PSF-CI-LBT

Figure 6 illustrates the economic feasibility (cost) analysis against the number of characters for PSF-CI-LBT of SC. The number of characters is used to compute the computational cost. To accurately understand the performance conclusion, the suggested technique executes the SC with varying input string lengths. Figure 6 indicates that the computational cost escalates with the string length. However, the intervals for operational expenses rise linearly, with transaction costs slightly exceeding execution costs.

For string lengths of up to 30 characters, both transaction cost and execution cost remain invariant at  $1 \times 10^5$  and  $1.2 \times 10^5$ , respectively. Beyond this barrier, a substantial escalation in expenses occurs. Within the 40 to 60 characters region, the transaction cost escalates to  $2.5 \times 10^5$ , but the execution cost climbs to  $2.8 \times 10^5$ , maintaining stability throughout this interval. Exceeding 70 characters, both expenses undergo an additional increase. For string lengths ranging from 70 to 80 characters, the transaction cost escalates to  $3.5 \times 10^5$ , whereas the execution cost jumps to  $3.8 \times 10^5$ . Ultimately, at 90 and 100 characters, the transaction cost attains  $5.5 \times 10^5$ , whereas the execution cost escalates to  $5 \times 10^5$  and  $5.7 \times 10^5$ , respectively. This signifies that both transaction and execution costs escalate in distinct increments as string length rises, mirroring the rising computing complexity associated with managing larger strings.

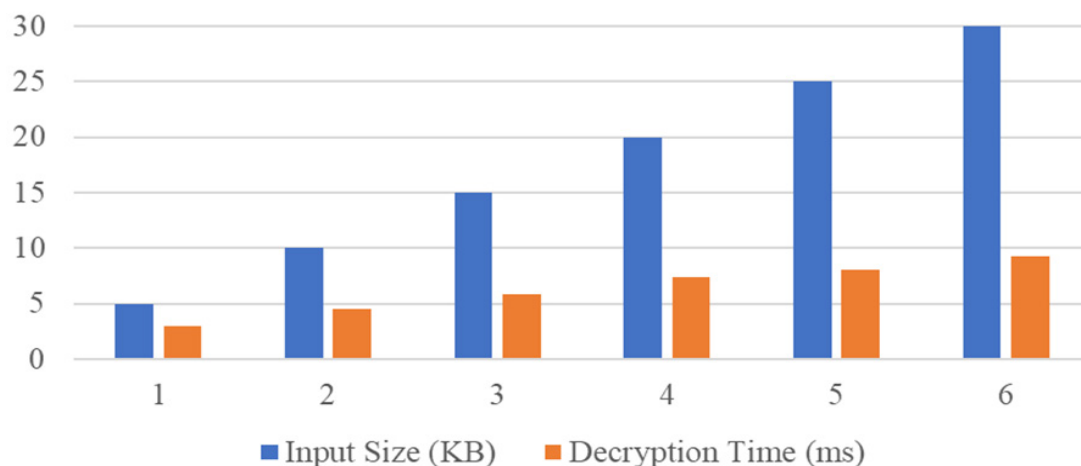


Figure 7. Decryption duration (ms) with the input size (KB) of the MD

Figure 7 illustrates the decryption duration (ms) with the input size (KB) of the MD. The suggested methods include computing the decryption duration while generating the plaintext on the receiving end. The paper examines the relationship between varying input sizes and the corresponding variations in decryption time growth rates. As the input size escalates, the decryption duration extends, signifying that higher data volumes need more time for decryption.

For minimal input quantities, such as 5 KB, the decryption duration is relatively brief at 3 ms. When the input size doubles to 10 KB, the decryption duration escalates to 4.5 ms. The rising trend continues consistently, with further increments in input size, reaching 9.3 ms at 30 KB. The data indicates that decryption time increases non-linearly with input size, exhibiting a more pronounced escalation between bigger input sizes, especially between 15 KB and 30 KB. This signifies the increasing computational burden as data volume increases, illustrating the intricacy of decryption methods for more significant inputs.

## CONCLUSIONS

The deployment of authorization methods and cryptographic primitives is insufficient for addressing modern cyber threats and resolving privacy and security concerns associated with cloud settings. This research introduces a Privacy and Security Framework in Cloud Infrastructure using Lightweight Blockchain Technology (PSF-CI-LBT) for Medical Data. Patient-centric MD management software using BT for storage has been implemented to improve privacy. Cryptographic techniques are used to encrypt patients' medical data and ensure confidentiality. The encryption, decryption duration, and economic viability (cost) of the proposed smart contract (SC) architecture are evaluated alongside the approaches used for MD analysis to encrypt and obscure patient MD. As the input file size goes from 5 KB to 30 KB, the encryption time steadily rises from 89 ms to 97 ms. This indicates a linear relationship between input size and encryption time, suggesting that larger input volumes need more computational capacity for encryption. At 90 and 100 characters, the transaction cost reaches  $5.5 \times 10^5$ , whereas the execution cost increases to  $5 \times 10^5$  and  $5.7 \times 10^5$ , respectively. This indicates that both transaction and execution costs increase in separate steps as string length increases, reflecting the heightened computational complexity involved in handling more significant strings. The data demonstrates that decryption time escalates non-linearly with input size, particularly intensifying between larger input sizes, notably between 15 KB and 30 KB. This indicates the growing processing demand as data amount escalates, highlighting the complexity of decryption techniques for more significant inputs.

## REFERENCES

1. Adeghe, E. P., Okolo, C. A., & Ojeyinka, O. T. (2024). Evaluating the impact of blockchain technology in healthcare data management: A review of security, privacy, and patient outcomes. *Open Access Research Journal of Science and Technology*, 10(2), 013-020.
2. Molli, V. L. P. (2023). Blockchain Technology for Secure and Transparent Health Data Management: Opportunities and Challenges. *Journal of Healthcare AI and ML*, 10(10), 1-15.
3. Amintoosi, H., Nikooghadam, M., Shojafar, M., Kumari, S., & Alazab, M. (2022). Slight: A lightweight authentication scheme for smart healthcare services. *Computers and Electrical Engineering*, 99, 107803.
4. Maarouf, A., Sakr, R., & Elmougy, S. (2024). An Offline Direct Authentication Scheme for the Internet of Medical Things based on Elliptic Curve Cryptography. *IEEE Access*.

5. Chenthara, S., Ahmed, K., Wang, H., Whittaker, F., & Chen, Z. (2020). Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. *Plos one*, 15(12), e0243043.
6. Liu, B. J., & Huang, H. K. (2020). Picture archiving and communication systems and electronic medical records for the healthcare enterprise. In *Biomedical information technology* (pp. 105-164). Academic Press.
7. Marutha, N. (2021). Medical records preservation strategies in improving healthcare service providers' access to patients' medical histories in the Limpopo hospitals, South Africa. *Information Development*, 37(1), 174-188.
8. Stafford, T. F., & Treiblmaier, H. (2020). Characteristics of a blockchain ecosystem for secure and sharable electronic medical records. *IEEE Transactions on Engineering Management*, 67(4), 1340-1362.
9. Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, 50, 102407.
10. Al Mamun, A., Azam, S., & Gritti, C. (2022). Blockchain-based electronic health records management: a comprehensive review and future research direction. *IEEE Access*, 10, 5768-5789.
11. Younis, M., Lalouani, W., Lasla, N., Emokpae, L., & Abdallah, M. (2021). Blockchain-enabled and data-driven smart healthcare solution for secure and privacy-preserving data access. *IEEE Systems Journal*, 16(3), 3746-3757.
12. Singh, S., Hosen, A. S., & Yoon, B. (2021). Blockchain security attacks, challenges, and solutions for the future distributed iot network. *Ieee Access*, 9, 13938-13959.
13. Toraman, P. Ş., Ergün, N., & Çalıcı, B. (2020). Some abiotic stress on growth and lipid peroxidation on wheat seedlings. *Natural and Engineering Sciences*, 5(3), 144-154. <https://doi.org/10.28978/nesciences.832975>
14. Shuen, T. K., Talib, C. A., Osman, S., Ying, S. T., Ahmad, I. S., Anggoro, S., Erna, M., & Fah, L. Y. (2024). Integrated Framework for the Implementation of Visual Programming Language in Science Experiment for Secondary School. *Indian Journal of Information Sources and Services*, 14(3), 45-51. <https://doi.org/10.51983/ijiss-2024.14.3.07>
15. Bayhan, Y. K. (2021). The Fish Fauna of the Atatürk Dam Lake (Adıyaman/Turkey). *Natural and Engineering Sciences*, 6(3), 237-255. <http://doi.org/10.28978/nesciences.1036854>
16. Abdul Latheef, N. (2022). Career Guidance Sources in Libraries: A Study of Arts & Science Colleges Affiliated to Thiruvalluvar University, Tamil Nadu. *Indian Journal of Information Sources and Services*, 12(1), 21-27. <https://doi.org/10.51983/ijiss-2022.12.1.3061>
17. Ozyilmaz, A. T. (2021). Synthesis of Poly (Aniline-Co-O-Anisidine) Film in Electrolyte Mixture and Its Anticorrosion Behavior. *Natural and Engineering Sciences*, 6(3), 197-207. <http://doi.org/10.28978/nesciences.1036850>
18. Ramakrishnan, J., Ravi Sankar, G., & Thavamani, K. (2022). A Scientometric Study on Neuroanatomy Literature. *Indian Journal of Information Sources and Services*, 12(1), 34-46. <https://doi.org/10.51983/ijiss-2022.12.1.3102>
19. Yağlıoğlu, D., & Turan, C. (2021). Occurrence of Dusky Grouper *Epinephelus marginatus* (Lowe, 1834) from the Black Sea: Is it the Mediterranization Process of the Black Sea?. *Natural and Engineering Sciences*, 6(3), 133-137. <http://doi.org/10.28978/nesciences.1036841>
20. Salauddin, N. (2022). Accessibility of Information Resources and Services in the Library for the Users with Disabilities: A Study. *Indian Journal of Information Sources and Services*, 12(1), 47-51. <https://doi.org/10.51983/ijiss-2022.12.1.3158>
21. Karimov, B. K., et al. (2020). Relationship between the concentrations of nitrogen compounds and the water discharge in the Chirchik River, Uzbekistan. *IOP Conference Series: Earth and Environmental Science*, 614, 012154. <https://doi.org/10.1088/1755-1315/614/1/012154>



22. Karimov, A., et al. (2019). Rethinking settlements in arid environments: Case study from Uzbekistan. E3S Web of Conferences, 97, 05052. <https://doi.org/10.1051/e3sconf/20199705052>
23. Odilov, A., et al. (2024). Utilizing deep learning and the Internet of Things to monitor the health of aquatic ecosystems to conserve biodiversity. Natural and Engineering Sciences, 9(1), 72-83. <https://doi.org/10.28978/nesciences.1491795>
24. Ebenezar, U. S., Vennila, G., Balakrishnan, T. S., & Krishnan, P. (2024, June). Optimizing Healthcare Delivery through CloudBased Clinical Decision Support Systems. In 2024 OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0 (pp. 1-6). IEEE.
25. Krishnan, P., Jain, K., Aldweesh, A. et al. OpenStackDP: a scalable network security framework for SDN-based OpenStack cloud infrastructure. J Cloud Comp 12, 26 (2023). <https://doi.org/10.1186/s13677-023-00406-w>
26. Krishnan P., Achuthan K. (2019) CloudSDN: Enabling SDN Framework for Security and Threat Analytics in Cloud Networks. UBICNET 2019. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 276. Springer, Cham. [https://doi.org/10.1007/978-3-030-20615-4\\_12](https://doi.org/10.1007/978-3-030-20615-4_12)

## FINANCING

The authors did not receive financing for the development of this research.

## CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

## AUTHORSHIP CONTRIBUTION

*Conceptualization:* Kosim Rakhmanov, Dilfuza Makhmudova, Shaanvar Shamansurov, Mexrangiz Narzullayeva, Zebo Almamatova, Ugilkhon Akilova, Nadira Mirametova, Aynash Omarova.

*Data curation:* Kosim Rakhmanov, Dilfuza Makhmudova, Shaanvar Shamansurov, Mexrangiz Narzullayeva, Zebo Almamatova, Ugilkhon Akilova, Nadira Mirametova, Aynash Omarova.

*Formal analysis:* Kosim Rakhmanov, Dilfuza Makhmudova, Shaanvar Shamansurov, Mexrangiz Narzullayeva, Zebo Almamatova, Ugilkhon Akilova, Nadira Mirametova, Aynash Omarova.

*Research:* Kosim Rakhmanov, Dilfuza Makhmudova, Shaanvar Shamansurov, Mexrangiz Narzullayeva, Zebo Almamatova, Ugilkhon Akilova, Nadira Mirametova, Aynash Omarova.

*Methodology:* Kosim Rakhmanov, Dilfuza Makhmudova, Shaanvar Shamansurov, Mexrangiz Narzullayeva, Zebo Almamatova, Ugilkhon Akilova, Nadira Mirametova, Aynash Omarova.

*Project management:* Kosim Rakhmanov, Dilfuza Makhmudova, Shaanvar Shamansurov, Mexrangiz Narzullayeva, Zebo Almamatova, Ugilkhon Akilova, Nadira Mirametova, Aynash Omarova.

*Resources:* Kosim Rakhmanov, Dilfuza Makhmudova, Shaanvar Shamansurov, Mexrangiz Narzullayeva, Zebo Almamatova, Ugilkhon Akilova, Nadira Mirametova, Aynash Omarova.

*Software:* Kosim Rakhmanov, Dilfuza Makhmudova, Shaanvar Shamansurov, Mexrangiz Narzullayeva, Zebo Almamatova, Ugilkhon Akilova, Nadira Mirametova, Aynash Omarova.

*Supervision:* Kosim Rakhmanov, Dilfuza Makhmudova, Shaanvar Shamansurov, Mexrangiz Narzullayeva, Zebo Almamatova, Ugilkhon Akilova, Nadira Mirametova, Aynash Omarova.

*Validation:* Kosim Rakhmanov, Dilfuza Makhmudova, Shaanvar Shamansurov, Mexrangiz Narzullayeva, Zebo Almamatova, Ugilkhon Akilova, Nadira Mirametova, Aynash Omarova.

*Display:* Kosim Rakhmanov, Dilfuza Makhmudova, Shaanvar Shamansurov, Mexrangiz Narzullayeva, Zebo Almamatova, Ugilkhon Akilova, Nadira Mirametova, Aynash Omarova.

*Drafting - original draft:* Kosim Rakhmanov, Dilfuza Makhmudova, Shaanvar Shamansurov, Mexrangiz Narzullayeva, Zebo Almamatova, Ugilkhon Akilova, Nadira Mirametova, Aynash Omarova.