Blockchain-based Scalable and Secure EHR Data Sharing using Proxy Re-Encryption

Naresh Sammeta
School of Computer Science and Engineering,
VIT-AP University, Amaravati, India
samnaresh@gmail.com

Latha Parthiban
Department of Computer Science,
Pondicherry University Community College, India
lathaparthiban@yahoo.com

Abstract: *Electronic Health Record (EHR) includes highly sensitive data like medical images, prescriptions, medical test result, medical history of patients, etc., these sensitive data cannot be transmitted in its original form in the network due to security issues. Hence, encryption is done prior to transmission. To increase the speed of data transfer and to overcome the storage issues, data is usually transferred through the cloud. Hence, to ensure the security and scalability of the data, a third-party encryption called re-encryption is performed at the proxy cloud. This re-encryption ensures that the data can be reliably transmitted through the network. In this research, a novel scheme called block-chain based EHR data sharing using chaotic re-encryption (BC-EDS-CR) is proposed. In the proposed scheme, re-encryption is performed using chaos theory. The proposed re-encryption scheme ensures that the cloud administrator cannot access the medical data. Metrics such as Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Structural Similarity Index (SSIM), entropy and correlation coefficient are used in evaluating this scheme. It was found that the proposed scheme outperforms the existing methods by achieving a PSNR of 57.66, SSIM of 0.985 and MSE of 0.058.*

Keywords: *EHR, blockchain, chaos theory, re-encryption, cloud.*

Received March 25, 2021; accepted March 17, 2022
https://doi.org/10.34028/iajit/20/5/2

1. Introduction

Recently, e-health has emerged as a popular technology in the field of medical informatics. E-health comprises of a wide variety of services like tele-medicine, medical prescription, medical diagnosis, Electronic Health Record (EHR), etc., [18]. With the evolution of internet, vision and electronic device systems, there has been tremendous transformation from the traditional paper storage technology to the electronic storage technology. EHR management systems have been designed to ensure privacy, security and accuracy of medical records. These systems aid in enhancing the relationship between the patients and the medical experts throughout the world. In addition, these systems are designed to ensure secure storage of medical data [21]. Cloud-based storage is popularly being used for storing the EHR information. However, these systems encounter various issues like lack of authentication, integrity, etc. The medical data stored in the cloud can be easily altered, manipulated, or even removed. In such cases, the life of the patients is put to a high level of risk [2]. Since medical data contain sensitive information, maintaining the integrity of this system is mandatory. Any damage to its centralized system can damage the entire network. To increase the reliability of this structure, block-chain systems are popularly employed. All the members of the block-chain register to the network [6]. The main advantage of the block-chain technology is that it can be connected to the Internet of Things. Thus, access to smart medicine is possible. The relationship between different entities can be enhanced using this interconnection. All the entities have the right to access the network data securely [25]. The main aim of designing block chain is to enable different entities that do not have trust with each other to exchange information. This is done using encryption techniques. The block chain is designed such that there is a dedicated entity responsible for providing the encryption keys [3]. Cloud-based health care systems are employed for preserving the medical data. In these systems access control is achieved using attribute-based technique. Here, the patients or the data owners own the right to control the access of their information [16]. A block-chain system based on fabric framework has also been proposed. Here, authorization of block-chain members was done using digital systems. Access management was done based on the authentication. Data was stored using cloud storage [13]. Multi-typed block chain systems are also used. These systems aim at providing increased diagnosis results. Public key encryption was employed by these systems. The privacy preservation was achieved using keyword search technique [8]. Systems for preserving the data stored in the cloud against illegal modifications have been proposed. In these systems the key for accessing data is outsourced by authenticated users only [4].

The rest of the paper is organized as follows: Section 2 covers the related work. Section 3 describing the proposed methods for the entire research work with architectural designs and mathematical formulations. Following this, section 4 demonstrates the results obtained for the simulation analysis, and discusses the inferences. Finally, section 6 describes the conclusion and future scope of the proposed mechanism.

2. Related Work

The purpose of this chapter is to provide a comprehensive overview of current state-of-the-art blockchain enabled healthcare systems, specifically ones that employ blockchain for secure transmission of medical records.

2.1. Literature Review

Afzal *et al*. [1] has proposed a scheme for secure transmission of health data using resource constrained platform. In this work, the third-party encryption was performed using the cloud. In the pre-processing step watermarking was done to hide the sensitive information. The data hiding was performed using a host image. The system was designed such that the encryption time was minimized. Encryption was done using two schemes. The first scheme was chaotic encryption and the second scheme was the bit plane encryption. Lee *et al*. [11] presented a framework using proxy re-encryption for securing the health care data. In this work, a new framework was proposed for encryption of health care data based on private key generation. According to this scheme, a dedicated private key generator was used for the generation of keys. These keys were distributed to both the sender and the receiver. The proxy in the centre was unaware of the private keys of the sender and the receiver. These two works suggest the use of proxy cloud in performing re-encryption. Huixian *et al*. [9] proposed an MPKC-based threshold proxy signcryption scheme that resists quantum attacks. The scheme is proven confidential and unforgeable based on the Multivariate Quadratic and Isomorphism Polynomial problems.

Wang *et al*. [24] designed a scheme for the EHR data sharing using a cloud-based framework. In this paper, block chain technology was utilized to offer anonymity to the system. In addition, this system was designed such that it offered verifiability. The EHR data was provided by the data provider. This data can be requested by the data requester. This is done using key word search scheme. The proxy encryption was performed in a conditional way so that the security of the data and the access control was ensured. Techapanupreeda *et al*. [22] proposed protecting patient privacy through electronic transactions in healthcare systems. Scyther and Automated Validation of Internet Security Protocols (AVISPA) were used to demonstrate the accountability transaction protocol's security to overcome all security issues. Kim *et al*. [10] proposed a scheme for securing the medical data using cloud-assisted protocol. Here, block chain was used for ensuring the integrity of the system. Encryption was done using Elliptic Curve Cryptography (ECC). The cloud server was designed to encrypt the medical data using the ECC scheme. The access control of the system was ensured using log transactions. In addition, this system was designed to provide automatic validation of data using log transactions integrated with cloud computing. This two research strengthens the blockchain technology in EHR management and encryption.

Sumathi and Ezra [20] has introduced a scheme for the cloud re-encryption using both symmetric and asymmetric algorithms. The main aim of this scheme was to collect the information once and analyze it many times based on the evolution of new technologies. In this way, the medical data can be analyzed effectively. Since, both the symmetric and asymmetric systems were combined the security level attained by this system was too high. Also, this system provided uni-directional encryption of data. Pournaghi *et al*. [15] has proposed a framework in which attribute-based encryption was utilized. In this work, the privacy of the medical data was ensured using fine-grain access control technique. In addition, the private block chains were used by this framework to increase the instant access capability of the system. Also, this system was simulated using OPNET to verify the performance of the framework. It was observed that the computational complexity of this system was less. Also, the storage capacity was observed to be high. The works from [14, 20] validates their security enhancement schemes in cloud platforms in different ways. The former never addressed the computational efficiency, whereas the latter significantly addressed the computation complexity and opens up the way to generate our research solution improving these current proposals.

Elhadad [7] has presented a scheme for the encryption of health data using DNA computing technique. Here, three keys were generated and used. The first key was generated for the owner of the data. The second key was generated for the proxy and the third key was generated for the user of the data. The user can use the data only after decrypting the information that was encrypted by the proxy. In this way, data privacy and data security were ensured in this system. Plaintext files were used for verifying the quality of this proposed DNA based framework. To provide confidentiality, integrity, authenticity, anonymity, non-repudiation, and untraceability, blockchain based electronic voting [19] is convenient and practical for voters and by using a blind multi-document locking mechanism which can be used to facilitate the simultaneous voting on multiple issues, thus reducing the number of signing instances that are required. Chen *et al*. [5] has presented a searchable scheme for ensuring the privacy of health care data. In this scheme, very high level of confidence was achieved using block chain technique. Complex logic expressions were used for storing the index of the health care data. In this way, the security of the data was ensured. In addition, this index was stored in the block chain. Whenever a user needs to access the data, the user must use the expression to find the index and can then access the medical data. These two models fail to ensure optimal storage utilization.

Nguyen *et al*. [14] has designed a framework for medical data privacy protection using mobile cloud. In this paper, high level of security was guaranteed using mobile cloud. The block chain was combined with the decentralized file system to ensure the access control. EHR data sharing was done using smart contracts. Here, Amazon cloud computing system was used for providing the data encryption. This system achieved light weight and reliable access control. Also, very less network latency was achieved in this scheme. Wang and Song [23] proposed a scheme for attaining confidentiality of the data using attribute-based cryptosystem. The encryption of data was done using a combination of two technologies. The first was the identity-based encryption and the second was the attribute-based cryptosystem. Digital signatures were also added to increase the integrity of the framework.

2.2. Discussion on Related Work

Since the volume and complexity of the current and future EHR in real-time scenarios increases dramatically, this paper's research solution is inevitable in the medical domain. Therefore, this research paper aims to present the following:

- A framework design for the proposed blockchain-based EHR data sharing using chaotic re-encryption (BC-EDS-CR) to ensure the scalability and security in digital healthcare.
- Statistical design for the encryption and decryption of the EHR data in the proxy cloud.
- Design of protocol structure for the proposed BC-EDS-CR showing the relation among the research center, data owner, data provider, proxy cloud, and the health center.
- Experimental results and following results validating the proposed BC-EDS-CR model.

3. Proposed Methodology

The main objective of this framework is to design a novel architecture for the EHR data sharing using block-chain based system. The system must be designed such that scalable and secure data sharing is achieved.

3.1. Traditional EHR Data Sharing Approach

The traditional EHR data sharing approach comprises of users, search agent and hospitals. In Figure 1 illustrates that there are t number of users. When the user wants to find a suitable hospital, he first transfers the EHR to the search agent. The user encrypts the data using the private key of the search agent *Ks* to form *E*(*m*, *Ks*). This data is then used by the search agent to find a suitable health center. The search agent encrypts data using the health center's private key *Kh* to form *E* (*E*(*m*, *Ks*), *Kh*). This double encrypted data is transferred to the suitable hospital by the health center. The big downside of this method is that if *t* numbers of users exist, then *t* numbers of encryptions must be made. This raises the overhead computing of the standard solution.

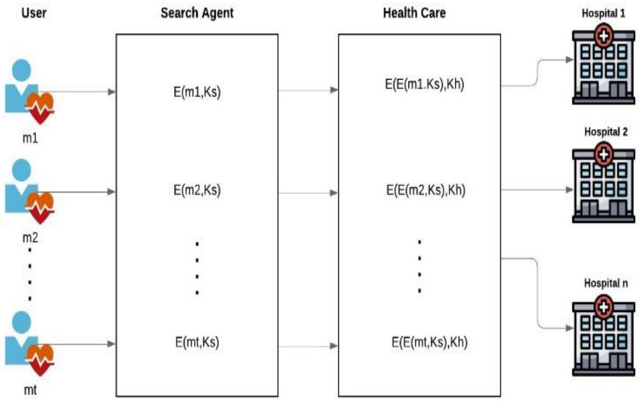


Figure 1. Traditional EHR data sharing approach.

3.2. Proposed EHR Data Sharing Using Chaotic Re-Encryption

The single point of failure that may occur in traditional EHR systems also affects current alternatives that rely on a centralized database. Past solutions have failed to address issues with performance and scalability, leaving users vulnerable to privacy linkage attacks. In this work, we suggest a decentralized file system and permissioned Blockchain technology-based healthcare data exchange system. The Proposed EHR data sharing scheme using chaotic re-encryption is shown in Figure 2.

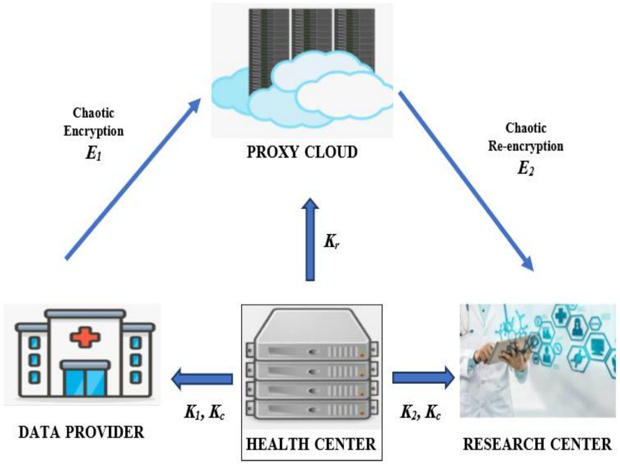


Figure 2. Proposed EHR data sharing using chaotic re-encryption.

Figure 2 illustrates that the health centre is the main key generator device in the proposed scheme. Initially, the research centre requests for a EHR data from the data owner. The data owner sends an acknowledgement to the data provider and the research centre. The health centre generates the keys K_1, K_2, K_c, and K_r. It transfers the keys K_1 and K_c to the data provider and keys K_2 and K_c to the research center. Furthermore, it sends the key K_r to the proxy cloud. The data provider does chaotic encryption of the EHR data to compute E_1 and sends to proxy cloud. Using the key K_r, the proxy cloud does chaotic re-encryption and sends the re-encrypted information E_2 to the research center. The research center then decrypts and retrieves back the EHR data.

3.2.1. Architecture of Blockchain based EHR Data Sharing Using Chaotic Re-Encryption (BC-EDS-CR)

In this work, chaotic theory is used for the encryption of EHR data. In order to generate chaotic sequences, logistic maps [12] can be used as follows:

$$Z_{n+1} = 3.995 Z_n (1 - Z_n) \quad (1)$$

Where Z_0 is the initial value ranges between 0 and 1 and Z_n is the sequence value at the instance n. A sequence of chaotic values is derived from the above equation as $\{Z_1, Z_2, Z_3, ...\}$. This sequence of values is then converted an unsigned integer format ranging from 0 to 255. This is obtained by multiplying the sequence with 255. In this work, two different initial values are used as keys for the generation of two different chaotic sequences used for encryption.

$$K_1 = Z_0^1, K_2 = Z_0^2 \text{ and } K_r = \frac{Z_0^2}{Z_0^1} \quad (2)$$

Here, Z_0^1 is the first initial value for the first encryption key generation, Z_0^2 is the second initial value for second encryption key generation and K_r is the ratio key used for the re-encryption of data. Figure 3 shows the architecture of block-chain based EHR data sharing using chaotic re-encryption (BC-EDS-CR). Figure 3 shows that all the entities in the EHR data sharing unit are connected using a block-chain. To establish this data sharing, all the four entities namely, research center, data owner, data provider, proxy cloud and the health center must register with the block-chain.

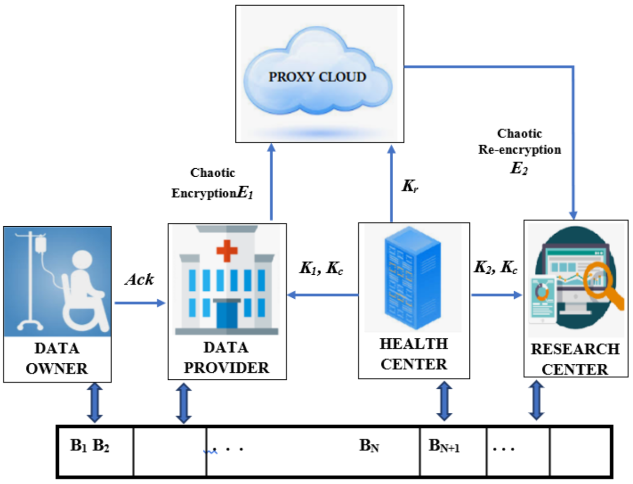


Figure 3. Proposed architecture of block-chain based EHR data sharing using chaotic re-encryption (BC-EDS-CR).

The process of proposed chaotic re-encryption is performed as follows. The data provider initially encrypts the EHR with key K_1 and sends the encrypted data E_1. The data provider also sends common key encryption E_C the encrypted version of the key K_1 using a common key K_c to the proxy cloud.

$$E_1 = E[EHR]_{K_1} \quad (3)$$

$$E_C = E[K_1]_{K_c} \quad (4)$$

Where $E[EHR]_{K_1}$ is the encrypted version of the EHR using the key K_1.The proxy cloud then re-encrypts E_1 using the ratio key to compute E_2 and sends to research center. It also sends the common key encryption E_C that it received from the data provider to the research center.

$$E_1 = E[E_1]_{K_r} \quad (5)$$

Where $E[E_1]_{K_r}$ is the encrypted version of the E_1 using the key K_r. The research center then decrypts and retrieves EHR using the following steps. In the first step, it decrypts the E_C using common key K_c to find K_1.

$$K_1 = D[E[K_1]_{K_c}]_{K_c} \quad (6)$$

The research center uses the key K_2 obtained from the health center and the computed key K_1 to find ratio key. It computes the ratio key K_r using the keys K_1 and K_2 as

$$K_r = \frac{K_2}{K_1} \quad (7)$$

The first encrypted data E_1 is then computed by decrypting E_2 using the ratio key K_r. Finally, the EHR data is computed by decrypting E_1 using the key K_1.

$$E_1 = D[E_2]_{K_r} \quad (8)$$

$$EHR = D[E_1]_{K_1} \quad (9)$$

The finally computed EHR is used by the research center for its analysis purpose. In this way, the proxy cloud is unaware of the data being transmitted. Thus, the scalability and the security of the data is ensured in this framework.

3.2.2. Protocol of Proposed BC-EDS-CR Scheme

The protocol of the proposed BC-EDS-CR scheme is given in Figure 4. This protocol involves research center, data owner, data provider, proxy cloud and the health center.

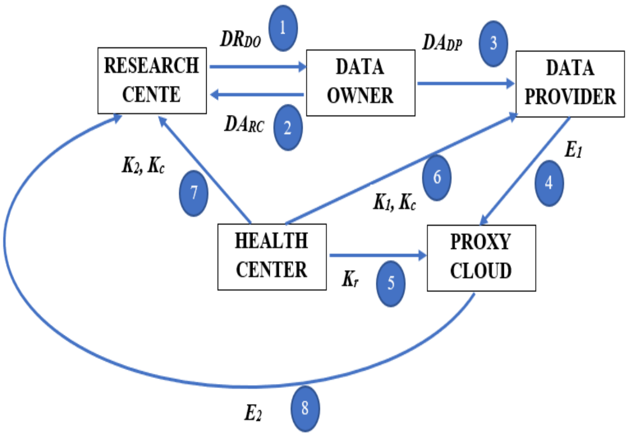


Figure 4. Protocol diagram of proposed BC-EDS-CR scheme.

Figure 4 illustrates that the first step is the transfer of data request DR_{DO} from the research center to the data owner. Afterwards the data owner sends the approval DA_{RC} to the research center. The data owner also gives the data provider an acknowledgment DA_{DP}. The data provider sends encrypted EHR data E_1 to the proxy cloud. The health center generates the encryption keys and sends the ratio key K_r to the proxy cloud. It also transfers the keys K_1 and K_C to the data provider. It also sends the keys K_2 and K_C to the research center. The proxy cloud sends the re-encrypted data to the research center.

3.2.3. Advantages of the Proposed BC-EDS-CR Scheme

The main advantage of the proposed scheme is the reduction in the number of encryptions. This reduction has resulted in effective time utilization for the entire process in the proposed blockchain technology. This characteristic improves the performance of the application scenario. The real-time scenarios with remote monitoring using an IoT-cloud healthcare system seek robust and secure EHR management having minimum processing and computational overhead. This reduction in the number of encryption tasks in this proposal eliminates the computational overhead and ensures the feasibility of this model to improve the user experience. Another benefit is that the proxy cloud has no access to the data. Since the data contains sensitive information, security in the proxy cloud is the main objective. This is achieved using the proposed chaotic re-encryption technique.

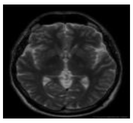
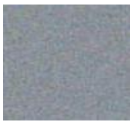
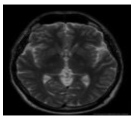
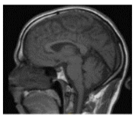
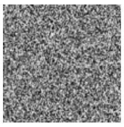
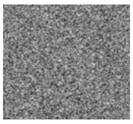
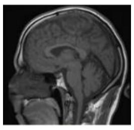
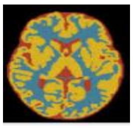
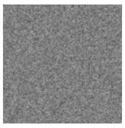
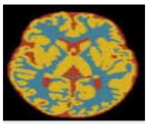
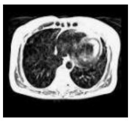
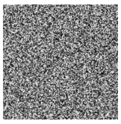
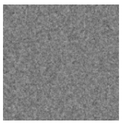
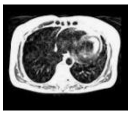
4. Results

Blockchain is a shared ledger computation mechanism. It provides easy access, compatibility, privacy, integrity, and decentralisation [2, 23, 24]. Decentralisation allows data stored in the Blockchain to be replicated across several computers, avoiding a single point of failure of the central server. The availability enables for data access when needed; but a few machines may fail. Data integrity is linked to data maintenance, which protects it from unauthorised changes. Blockchain technology is used in the proposed system to access and share patient medical records.

4.1. Performance Analysis

Encryption of data was performed using chaotic re-encryption algorithm. We evaluate the proposed re-encryption algorithm's performance using four different medical images. For visual analysis, the results obtained after encryption, re-encryption and decryption of medical images using the proposed chaotic re-encryption algorithm is shown in Table 1, it is obvious that the results of decryption are comparable to the original images. Furthermore, we observe that the encrypted and re-encrypted data are completely random, implying that the medical information is very safe. We employed measures such Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Matrix (SSIM), Entropy, and Correlation Coefficient (CC) to assess our system for further quantitative evaluation [17]. The suggested BC-EDS-CR technique was tested against various encryption algorithms such as Rivest-Shamir-Adleman (RSA), Advanced Encryption Standard (AES), and Elliptic Curve Cryptography (ECC).

Table 1. Encryption and decryption results using medical images for the proposed scheme.

Img #	Medical Images	Encrypted image	Re-encrypted image	Decrypted image
1				
2				
3				
4				

- **Mean Square Error (MSE)**: the average difference between the original image *O* and the decrypted image *D* is given by MSE. It is provided by

$$MSE = (1/N^2)\sum_{i=1}^{N}\sum_{j=1}^{N}[O(i,j) - D(i,j)]^2 \tag{10}$$

- **Peak Signal to Noise Ratio (PSNR)**: PSNR is the signal-to-error value ratio. It is computed as follows:

$$PSNR = 10\,log\frac{255^2}{(1/N^2)\sum_{i=1}^{N}\sum_{j=1}^{N}[O(i,j) - D(i,j)]^2} \tag{11}$$

- **Structural Similarity Index (SSIM)**: the similarity between the original and decrypted images is determined using SSIM. It has been evaluated as follows:

$$SSIM = \frac{(2\mu_o\mu_d+C_1)(2\sigma_{od}+C_1)}{({\mu_o}^2+{\mu_d}^2+C_1)({\sigma_o}^2+{\sigma_d}^2+C_2)} \tag{12}$$

- **Entropy**: entropy gives the amount of information content. It is computed using

$$Entropy = \sum_{i=0}^{2N-1} P_i \, log(1/P_i) \tag{13}$$

- **Correlation Coefficient (CC)**: the percentage of correlation between the original and decrypted images is indicated by CC. It is computed as follows:

$$r_{od} = \frac{cov(o,d)}{\sqrt{D(o)D(d)}} \tag{14}$$

Where $cov(o,d) = \frac{1}{N^2}\sum_{i=1}^{N^2}[o_i - E(o)][d_i - E(d)]$

Here, $D(o) = \frac{1}{N^2}\sum_{i=1}^{N^2}[o_i - E(o)]^2$ and (15)

$$D(d) = \frac{1}{N^2}\sum_{i=1}^{N^2}[d_i - E(d)]^2 \tag{16}$$

Where

$$E(o) = \frac{1}{N^2}\sum_{i=1}^{N^2} {o_i}^2 \, and \, E(d) = \frac{1}{N^2}\sum_{i=1}^{N^2} {d_i}^2 \tag{17}$$

Figure 5 shows the PSNR comparison for all four images.

Table 2. PSNR Comparison of RSA, AES, ECC, and BC-EDS-CR.

Image Number	PSNR			
	RSA	AES	ECC	BC-EDS-CR
1	31.19	43.12	31.19	53.12
2	39.91	44.63	44.91	54.63
3	48.83	51.23	44.83	51.23
4	44.95	58.98	54.95	58.98

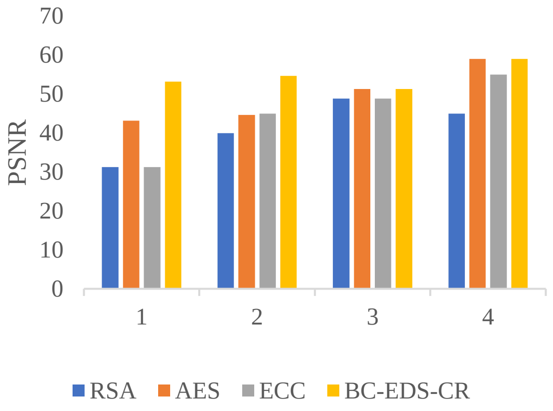


Figure 5. Comparison of PSNR.

According to Table 2 and Figure 5, the suggested BC-EDS-CR method outperforms RSA, AES, and ECC. The RSA algorithm's average PSNR for the four photos is 41.22. In contrast, the AES algorithm has a value of 49.49. The PSNR achieved by the ECC algorithm is 54.49. The planned BC-EDS-CR system, on the other hand, has the greatest PSNR of 57.66. As a result, we conclude that the suggested method provides the optimum PSNR performance.

Table 3. MSE Comparison of RSA, AES, ECC, and BC-EDS-CR.

Image Number	MSE			
	RSA	AES	ECC	BC-EDS-CR
1	0.23	0.132	0.162	0.032
2	0.286	0.145	0.106	0.065
3	0.241	0.109	0.141	0.059
4	0.217	0.137	0.117	0.077

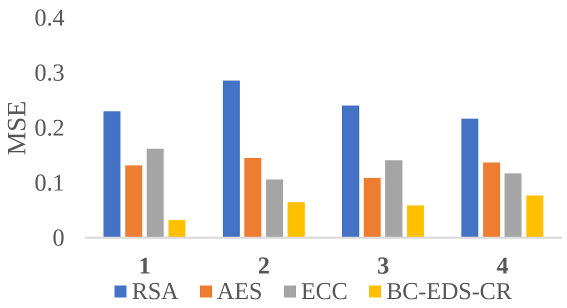


Figure 6. Comparison of MSE

In terms of MSE, Table 3 and Figure 6 show that the proposed BC-EDS-CR scheme outperforms RSA, AES, and ECC. The RSA method has an average MSE of 0.2435 for the four pictures. In contrast, the AES algorithm has a value of 0.13. The MSE for the ECC algorithm is 0.131. The suggested BC-EDS-CR system, on the other hand, gets the lowest MSE of 0.058. As a result, we conclude that the suggested system performs the best in terms of MSE.

Table 4. SSIM Comparison of RSA, AES, ECC, and BC-EDS-CR.

Image Number	SSIM			
	RSA	AES	ECC	BC-EDS-CR
1	0.527	0.765	0.797	0.965
2	0.682	0.796	0.882	0.996
3	0.662	0.797	0.862	0.997
4	0.682	0.785	0.882	0.985

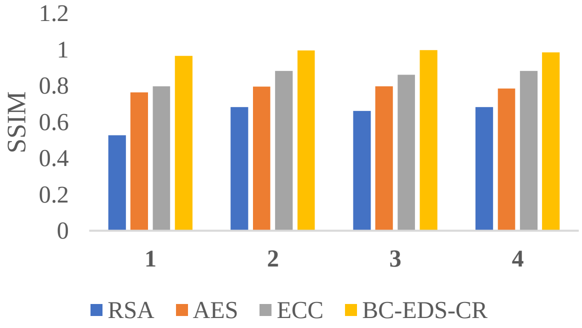


Figure 7. Comparison of SSIM.

Table 4 and Figure 7 show that the proposed BC-EDS-CR scheme outperforms RSA, AES, and ECC in terms of SSIM. The RSA algorithm's average SSIM value for the four photos is 0.638. In comparison, the AES algorithm has a value of 0.785. The ECC method has an SSIM of 0.855. Rather, the suggested BC-EDS-CR method yields a maximum SSIM of 0.985. As a result, we conclude that the suggested strategy performs the best in terms of SSIM.

Table 5. Entropy Comparison of RSA, AES, ECC and BC-EDS-CR.

Image Number	**ENTROPY**			
	RSA	**AES**	**ECC**	**BC-EDS-CR**
1	0.527	0.765	0.797	0.965
2	0.682	0.796	0.882	0.996
3	0.662	0.797	0.862	0.997
4	0.682	0.785	0.882	0.985

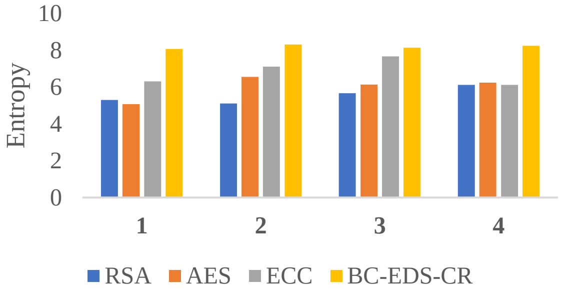


Figure 8. Comparison of entropy.

Table 5 and Figure 8 show that the proposed BC-EDS-CR scheme performs the best in terms of entropy when compared to RSA, AES, and ECC. For the RSA algorithm, the average entropy value for the four photos is 5.55. The AES algorithm has a value of 6.01. The ECC algorithm has an entropy of 6.8. The suggested BC-EDS-CR method, on the other hand, obtains a maximum entropy of 8.20. As a result, we conclude that the suggested method has the best entropy performance.

Table 6. Correlation coefficient comparison of RSA, AES, ECC and BC-EDS-CR.

Image Number	**Correlation Coefficient**			
	RSA	**AES**	**ECC**	**BC-EDS-CR**
1	0.72	0.78	0.82	0.98
2	0.71	0.79	0.81	0.99
3	0.73	0.77	0.83	0.97
4	0.65	0.79	0.84	0.99

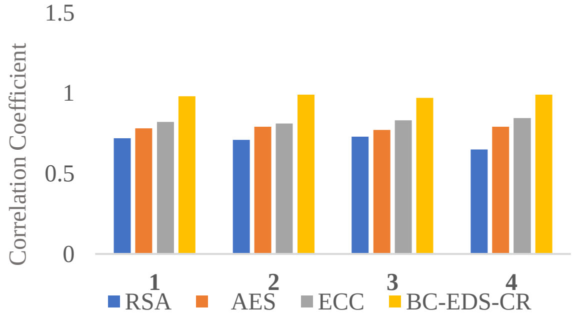


Figure 9. Comparison of correlation coefficient.

Table 6 and Figure 9 indicate that the proposed BC-EDS-CR method outperforms RSA, AES, and ECC. The RSA algorithm's average correlation coefficient for the four photos is 0.702. In comparison, the AES algorithm has a value of 0.782. The ECC method obtains a correlation value of 0.826. Rather, the suggested BC-EDS-CR method obtains a maximum correlation value of 0.998. As a result, we conclude that the suggested method outperforms all others in terms of correlation coefficient.

4.2. Computational Complexity Analysis

The proposed system was simulated using MATLAB R2015b on a Windows Intel i5 core CPU with 4GB RAM. The suggested framework's encryption and decryption times are compared to those of other cryptographic techniques.

Table 7. Comparison of encryption time of cryptographic algorithms (in ms).

Number of users *t*	**RSA**	**AES**	**ECC**	**BC-EDS-CR**
10	145.3	137.6	99.5	42.9
20	189.6	189.2	127.3	69.4
30	201.2	190.6	163.9	83.5
40	235.6	210.4	183.2	93.1
50	271.4	234.9	193.9	84.8

Table 7 compares encryption time for different user counts. We observed that as the number of users rises, so does the encryption time. RSA, AES, ECC, and BC-EDS-CR encryption times for ten users are 145.3ms, 137.6ms, 99.5ms, and 42.9ms, respectively. Likewise, the encryption times of RSA, AES, ECC, and BC-EDS-CR for 30 users are 201.2ms, 190.6ms, 163.9ms, and 83.5ms, respectively. As a result, it is evident that the suggested BC-EDS-CR technique takes the shortest time to encrypt. This indicates that the overall speed of the blockchain network shall be fast. This would improve the framework's efficiency.

Table 8. Comparison of decryption time of cryptographic algorithms (in ms).

Number of users t	**RSA**	**AES**	**ECC**	**BC-EDS-CR**
10	122.9	135.4	89.3	38.3
20	139.5	143.6	113.1	49.6
30	181.2	164.2	143.4	61.1
40	235.7	198.5	171.7	74.3
50	241.4	202.4	181.3	81.5

Table 8 compares encryption times for different numbers of users. We discover that as the number of users grows, so does the decryption time. The decryption times of RSA, AES, ECC, and BC-EDS-CR for ten users are 122.9ms, 135.4ms, 89.3ms, and 38.3ms, respectively. Similarly, the decryption times of RSA, AES, ECC, and BC-EDS-CR for 50 users are 241.4ms, 202.4ms, 181.3ms, and 81.5ms, respectively. As a result, the suggested BC-EDS-CR technique has the lowest decryption time. As a result, it is clear that the suggested technique has low computational complexity.

5. Conclusions

In this paper, we developed and pitched a novel strategy for assuring scalable and secure EHR data transfer. In this scheme, re-encryption of data was performed using a third-party entity called proxy cloud. We proposed a new scheme called block-chain based EHR data sharing using chaotic re-encryption (BC-EDS-CR). Initially, the data was encrypted by the data provider and transmitted to the cloud. The cloud then re-encrypts the data and sends to the research center. The research center decrypts the data and analyses it. In this way the security of the data in the transmission network was ensured. Encryption was done using a chaotic sequence generated using logistic chaotic maps. The quality of encryption was analyzed using both visual and quantitative analysis. It was shown that the proposed scheme outperformed various other encryption schemes like RSA, AES and ECC. BC-EDS-CR scheme attained very high correlation coefficient of 0.9982. It was also deduced that the encryption and decryption time of the proposed encryption algorithm was very low compared to other encryption schemes. In particular, the proposed BC-EDS-CR scheme utilized a minimum average time of about 74.74ms and 60.96ms for encryption and decryption respectively.

References

[1] Afzal I., Parah S., Hurrah N., and Song O., “Secure Patient Data Transmission on Resource Constrained Platform,” *Multimedia Tools and Applications*, pp. 1-26, 2020. DOI:10.1007/s11042-020-09139-3

[2] Azaria A., Ekblaw A., Vieira T., and Lippman A., “MedRec: Using Blockchain for Medical Data Access and Permission Management,” *in Proceedings of the 2nd International Conference on Open and Big Data*, Vienna, pp. 25-30, 2016. DOI 10.1109/OBD.2016.11

[3] Banerjee M., Lee J., and Choo K., “A Blockchain Future for Internet of Things Security: A Position Paper,” *Digital Communications and Networks*, vol. 4, no. 3, pp. 149-160, 2018. DOI:10.1016/j.dcan.2017.10.006

[4] Cao S., Zhang G., Liu P., Zhang X., and Neri F., “Cloud-Assisted Secure eHealth Systems for Tamper-Proofing EHR Via Blockchain,” *Information Sciences*, vol. 485, pp. 427-440, 2019. DOI:10.1016/j.ins.2019.02.038

[5] Chen L., Lee W., Chang C., Choo K., and Zhang N., “Blockchain Based Searchable Encryption for Electronic Health Record Sharing,” *Future Generation Computer Systems*, vol. 95, pp. 420-429, 2019. DOI:10.1016/j.future.2019.01.018

[6] Dagher G., Mohler J., Milojkovic M., and Marella P., “Ancile: Privacy-Preserving Framework for Access Control and Interoperability of Electronic Health Records Using Blockchain Technology,” *Sustainable Cities and Society*, vol. 39, pp. 283-297, 2018. https://doi.org/10.1016/j.scs.2018.02.014

[7] Elhadad A., “Data Sharing Using Proxy Re-Encryption Based on DNA Computing,” *Soft Computing*, vol. 24, pp. 1-8, 2020. DOI:10.1007/s00500-019-04041-z

[8] Elisa N., Yang L., Li H., Chao F., and Naik N., “Consortium Blockchain for Security and Privacy-Preserving in E-Government Systems,” *in Proceedings of the 19th International Conference on Electronic Business*, Newcastle upon Tyne, pp. 99-107, 2019. https://doi.org/10.48550/arXiv.2006.14234

[9] Huixian L., Jin G., Lingyun W., and Liaojun P., “MPKC-based Threshold Proxy Signcryption Scheme,” *The International Arab Journal of Information Technology*, vol. 17, vo. 2, pp. 196-206, 2020. https://doi.org/10.34028/iajit/17/2/7

[10] Kim M., Yu S., Lee J., Park Y., and Park Y., “Design of Secure Protocol for Cloud-Assisted Electronic Health Record System Using Blockchain,” *Sensors*, vol. 20, no. 10, pp. 2913, 2020. doi: 10.3390/s20102913.

[11] Lee C., Li C., Chen C., and Chiu S., “A Searchable Hierarchical Conditional Proxy Re-encryption Scheme for Cloud Storage Services,” *Information Technology and Control*, vol. 45, no. 3, pp. 289-299, 2016. https://doi.org/10.5755/j01.itc.45.3.13224

[12] May R., “Simple Mathematical Models with Very Complicated Dynamics,” *Nature*, vol. 26, pp. 457, 1976. DOI:10.1038/261459a0

[13] Mikula T. and Jacobsen R., “Identity and Access Management with Blockchain in Electronic Healthcare Records,” *in Proceedings of the 21st Euromicro Conference on Digital System Design*, Prague, pp. 699-706, 2018. 10.1109/DSD.2018.00008

[14] Nguyen D., Pathirana P., Ding M., and Seneviratne A., “Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems,” *IEEE Access*, vol. 7, pp. 66792-66806, 2019. DOI: 10.1109/ACCESS.2019.2917555

[15] Pournaghi S., Bayat M., and Farjami Y., “MedSBA: A Novel and Secure Scheme to Share Medical Data Based on Blockchain Technology and Attribute-Based Encryption,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, pp. 4613-4641 2020. DOI:10.1007/s12652-020-01710-y

[16] Riad K., Hamza R., and Yan H., “Sensitive and Energetic IoT Access Control for Managing Cloud Electronic Health Records,” *IEEE Access*, vol. 7, pp. 86384-86393, 2019. DOI: 10.1109/ACCESS.2019.2926354

[17] Sara U., Akter M., and Uddin M., “Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study,” *Journal of Computer and Communications*, vol. 7, no. 3, pp. 8-18, 2019. DOI: 10.4236/jcc.2019.73002

[18] Sillence, E., Little L., and Briggs P., “E-Health,” *in Proceedings of the 22nd British HCI Group*

Annual Conference on People and Computers: Culture, Creativity, Interaction-Volume 2, BCS Learning and Development Ltd. pp. 179-180, 2008.

[19] Su P. and Su T., "Secure Blockchain-Based Electronic Voting Mechanism," *The International Arab Journal of Information Technology*, vol. 20 no. 2, pp. 253-261, 2023. https://doi.org/10.34028/iajit/20/2/12

[20] Sumathi R. and Ezra K., "SCEHSS: Secured Cloud Based Electronic Health Record Storage System with Re-Encryption at Cloud Service Provider," *International Journal of Computer and Communication Engineering*, pp. 162-166, 2013. DOI: 10.7763/IJCCE.2013.V2.161

[21] Tang F., Ma S., Xiang Y., and Lin C., "An Efficient Authentication Scheme for Blockchain-Based Electronic Health Records," *IEEE Access*, vol. 7, pp. 41678-41689, 2019. DOI: 10.1109/ACCESS.2019.2904300

[22] Techapanupreeda C., Rattagan E., and Kurutach W., "A Transaction Security Accountability Protocol for Electronic Health Systems," *The International Arab Journal of Information Technology*, vol. 19, no. 3, pp. 289-297, 2022. https://doi.org/10.34028/iajit/19/3/1

[23] Wang H. and Song Y., "Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain," *Journal of Medical Systems*, vol. 42, 2018. doi: 10.1007/s10916-018-0994-6.

[24] Wang Y., Zhang A., Zhang P., and Wang H., "Cloud-Assisted EHR Sharing with Security and Privacy Preservation Via Consortium Blockchain," *IEEE Access*, vol. 7, pp. 136704-136719, 2019. DOI: 10.1109/ACCESS.2019.2943153

[25] Yue X., Wang H., Jin D., Li M., and Jiang W., "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control," *Journal of Medical Systems*, vol. 40, no. 10, pp. 218, 2016.

Naresh Sammeta holds a B.E, M.E and Ph.D. in Computer Science & Engineering, India. He has 16+ years of teaching experience and is currently an Assistant Professor in the School of Computer Science and Engineering, VIT-AP University, Amaravati, India. He has published 20 papers in peer-reviewed journals and conferences and granted one Patent. His research interests include Blockchain Technology, Cloud Computing and Information Security. He is a Life member of many professional societies like ISTE, CSTA, ACM, IAENG, and IACSIT.

Latha Parthiban holds an B.E, M.S, M.E and Ph.D degree in CSE and completed a PDF and has filed for a patent. Her teaching experience spans over 27 years in various Engineering colleges currently an Associate Professor in the Dept. of CS, Pondicherry University Community College, India and her research interest includes Soft Computing, Expert systems, Image Processing and cloud computing. She has published 122 peer reviewed Scopus indexed/SCI journals and presented papers in 60 international and national conferences. She is a Life member of many professional societies like IEEE, CSI, IACSIT, IAE, ISTE.