International Journal of Computer and Engineering Optimization (IJCEO)
Volume 1, Issue 1, September – October (2023)

RESEARCH ARTICLE

BLOCK CHAIN ASSISTED CLOUD BASED MEDICAL DATA STORAGE VIA QUANTUM DIFFIE-HELLMAN KEY EXCHANGE

G. Sreetha[1, *] and T. V. Chitra[2]

[1]Department of Computer Science and Engineering, Arunachala College of Engineering for Women, Manavilai, Tamilnadu, India.

[2]Department of Computer Science and Engineering, Arunachala College of Engineering for women, Manavilai, Tamilnadu, India.

[*]*Corresponding e-mail: sreethasree2000@gmail.com*

Abstract – Electronic Health Records (EHR) security ensures the confidentiality of patients' information and guarantees healthcare providers' accountability. Sharing such medical records with third party through an unsecure channel may be abused or disclosed to other unauthorized parties. Therefore, there is a rising need for a novel technology, which allows for outsourcing the data through an unsecure channel while preserving the privacy of EHR. In this paper, a novel Block chain Assisted Cloud based Key exchange (BACK) technique has been introduced, that uses blockchain technology for secure data transmission. The proposed method uses the novel secure Quantum Diffie Hellman key exchange (QDHKE) system for sharing the key in an unsecure environment. The BACK methodology helps in sharing the medical data through unsecure channel while maintaining the confidentiality and privacy of health information. The proposed method has been evaluated using CloudSim simulator. The efficiency of the technique has been assessed in terms of particulars like the time it takes to encrypt, decode, and execute and computational cost. According to the experimental results, the proposed BACK method achieves less encryption time of 12.5%, 7.4%, and 4.65% than existing techniques such as Healthchain, Blockchain integrated with IPFS, and Blockchain-based FL respectively.

Keywords *– Medical data security, blockchain, Key exchange, Quantum Diffie-Hellman.*

1. INTRODUCTION

The vast volume of medical data must be shared in order to increase medical knowledge and is a crucial tool for documenting patient information for therapy [1]. However, under the previous approach, each healthcare system had its own set of medical servers where it kept all of the data linked to health. Traditional Electronic Health Records (EHR) systems sometimes have a single point of failure since they are centralized [2-6]. The emergence of block chain technology has led to the creation of a creative solution to this issue, because it has the properties like anonymity, decentralization, and immutability [7-12]. All EHRs must be maintained on a blockchain, which is difficult because of the expenditure and size [13]. The most practical option for obtaining this kind of data and resolving these problems is cloud computing [14-17].

Cloud computing provides various services where, data outsourcing is one of those important services. This service enables users to outsource their data to one or more database service providers and grant authorized clients getting into the data. The security of outsourced data is one of the primary issues in outsourcing [18-20]. If EHR security has been compromised, patient personal information may be exposed, resulting in major issues.

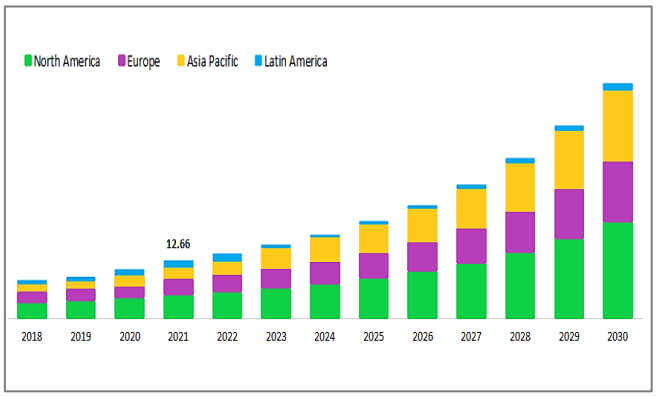

Figure 1. Statistics of medical data cyberattacks

According to the Centre for Strategic and foreign Studies, the US Cybersecurity and Infrastructure Security Agency (CISA) recognized Conti ransomware in over 400 assaults against US and foreign organizations in September 2021, as indicated in Figure 1. Therefore, to address the privacy concerns, a novel Block chain Assisted Cloud based Key exchange (BACK) technique has been introduced in this paper, which allows for data outsourcing through unsecure channel and also enhances privacy and security of medical data. The main objectives of the suggested BACK technique are given as below.

- Initially, the sensor data will be gathered from the victim in the form of EHR and provided to the medical center (MC) for diagnosis.
- For outsourcing the data to other MC's, the MC and patients will register themselves in the cloud as an authorized user by providing their identities with the help of network administrator (NA).
- For uploading the data, the MC will encrypt the data using homomorphic encryption and stored it in the cloud and a transaction data log will be created in the blockchain.
- For accessing the data, the user connects with the network administrator and the medical centre over public channels, and his or her identification is verified. After verification, the key will be exchanged using QDHKE, which preserves the security of the data in an unsecure environment.
- The effectiveness of the suggested method has been assessed based on certain metrics, including the execution, decryption, and encryption times.

This corresponds to the manner in which the remainder of the paper was written. Section 2 provides an overview of the literature review for secure medical data sharing. Section 3 describes the BACK methodology in detail. Section 4 describes the particulars of the experiment's execution and outcomes. The planned work's conclusion and future directions are covered in Section 5.

2. LITERATURE REVIEW

Medical EHR data sharing has been considered as the crucial thing during data outsourcing, because the privacy of medical data is necessary. Therefore, many researchers have concentrated on secure data sharing and provided many solutions for data security. This section discusses several works that use cloud and blockchain technology to share EHR.

In 2019, Niu, J., et al [21] suggested a blockchain-based attribute cryptosystem-based medical data exchange system. The analysis outcomes demonstrated that the suggested technique provides better computing performance than other similar techniques and meets the confidentiality and falsifiability requirements of the random Oracle model. This is a negative because the steps for mutual authentication and session key negotiation are not covered.

In 2020, Chenthara, et al [22] proposed a completely new clinical chain model that guarantees the integrity, scalability, and security of electronic health records. founded on the blockchain. According to the experimental results, the proposed methodology provides higher data security and data integrity amidst permitting all parties involved in the medical chain system to share and access medical records The main flaw is that once implemented, many customers who register for verification will share their information with other parties in an unreliable manner.

In 2021, Zaabar, B., et al [23] offered a novel architecture that gets around the issue of centralized storage by using a distributed database. Results of performance evaluation and comparative analysis of Hyperledger Caliper have demonstrated the superiority of various throughput and latency metrics, blockchain-based healthcare systems must be robust with regards to privacy and security requirements. This system's drawback is that it is unable to ensure perfect forward secrecy.

In 2022, Jayabalan, J. and Jeyanthi, N., [24] introduced a blockchain-oriented model connected to IPFS for electronic medical databases in health care. According to the experimental results, the suggested off-chain healthcare information storage approach using IPFS shields the blockchain architecture from scalability problems. The disadvantages were that they could not ensure data integrity or provide fine-grained access control to medical information.

In 2022, Singh, M.B. and Pratap, A., [25] proposed a secure privacy-preserving architecture in smart healthcare using a blockchain-based IoT cloud platform and federated learning (FL). Using this technique, customers can obtain fully built machine learning models without storing private data on cloud servers. The drawback is that the proposed work is not suitable for real-world environments.

In 2023, Adeniyi, A.E. et al. [26] created a altered AES algorithm to protect patient health information by changing the final cycle of AES. In terms of encryption time, modified AES exceeds the AES algorithm, with regards to decryption time; AES performs better than modified AES. However, this cannot minimize the amount of computation any further.

In 2023, Gupta, I. et al. [27] created a safe, efficient, and privacy-preserving communication model (SeCoM) for the preservation of medical data Experiments demonstrate that it enhances privacy protection, detection efficiency, and data utilization by up to 9.49%, 83%, and 43.25%, respectively. The temporal complexity of this procedure is its downside.

The above reviewed methods were helpful in sharing the data securely. However, these methods possess some drawbacks that were discussed above. In order to overcome these drawbacks, a novel Block chain Assisted Cloud based Key exchange (BACK) technique has been introduced in this paper, which is discussed in section 3.

3. BLOCK CHAIN ASSISTED CLOUD BASED KEY EXCHANGE MECHANISM

In this section a novel Block chain Assisted Cloud based Key exchange (BACK) technique has been introduced which allows for data outsourcing through an unsecure channel and also enhances privacy and security of medical data. Registration phase, authentication phase, and storage phase are the three phases of the proposed BACK technique. Initially, the sensor data will be obtained from the patient's electronic health record and provided to the medical center (MC) for diagnosis. For outsourcing the data to other MC's, the MC and patients will register themselves in the cloud as an authorized user by providing their identities with the help of network administrator (NA). For uploading the data, the MC will encrypt the data using homomorphic encryption and stored it in the cloud and a transaction data log will be created in the blockchain. For

accessing the data, the user connects with the network administrator and the medical centre over public channels, and his or her identification is verified. After verification, the key will be exchanged using QDHKE, which preserves the security of the data in an unsecure environment. The architecture of the proposed BACK technique is given in figure 2.

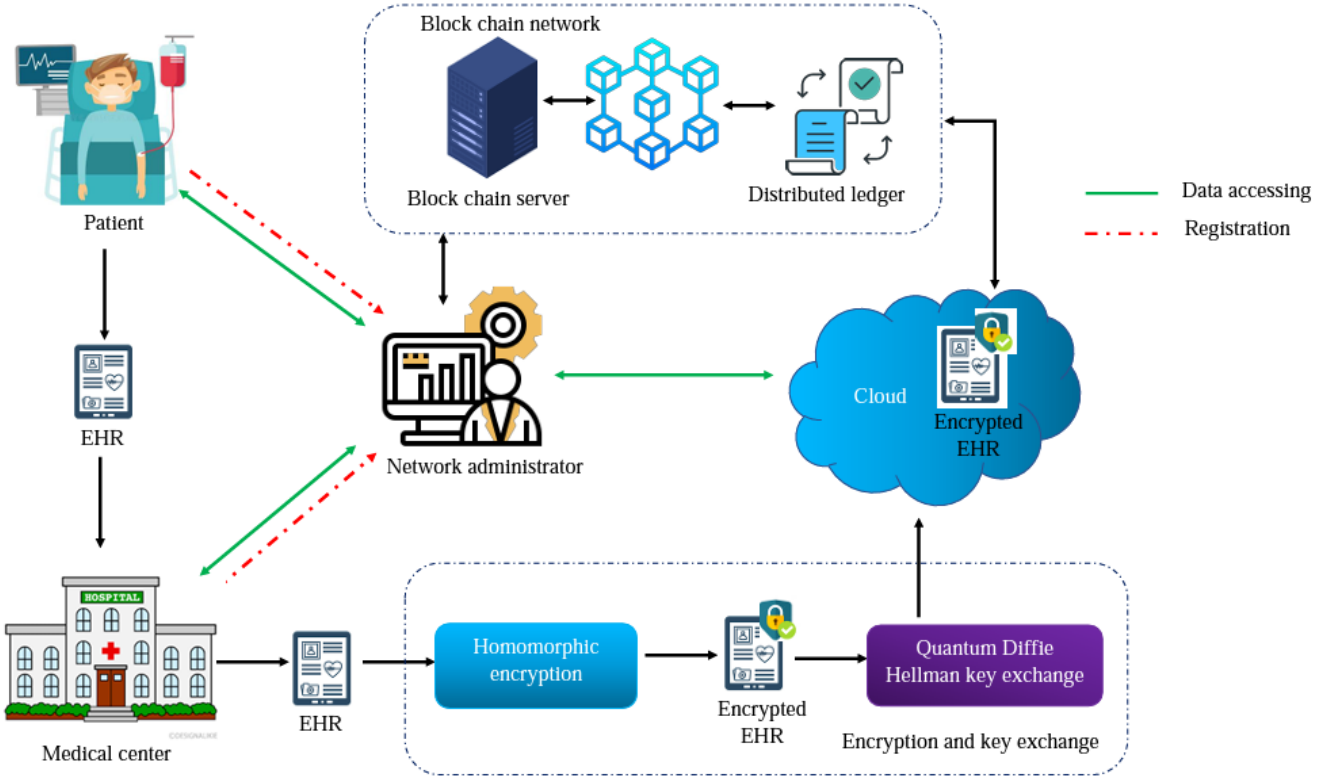

Figure 2. BACK architecture

3.1. Registration Phase

Initially, the patient will come to MC and the medical devices such as ECG, EEG will be connected to the person and the data will be collected by the doctor in the form of EHR. After acquisition, for uploading and accessing the data from the cloud needs registration. Therefore, the patient and MC should register themselves as the authorised users in the cloud with the help of network administrator.

3.1.1 Patient Registration

The patient (p_a) must register his or her identify with the network administrator in order to receive the medical diagnostic. The NA will assist the patient in registering his or her public and private keys, which will be done via a secure connection. The registration for patient has been shown in figure 3.

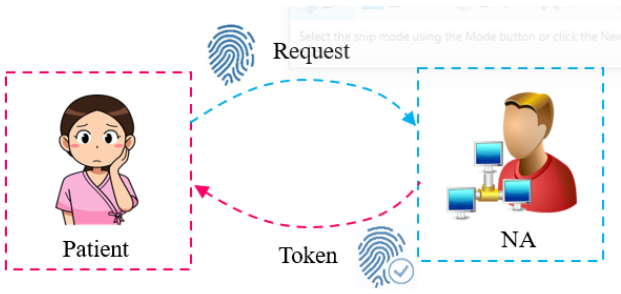

Figure 3. Patient registration

Step 1: p_a request NA for registration and send their biometrics for storage

Step 2: NA computes their biometrics and send a token p_t to p_a for future reference.

3.1.2. Medical centre registration phase

To communicate data from various healthcare centres, medical centres must first register with the network administrator, and the process is shown in figure 4.

Step 1: MC selects ID and transmits the unique identify to NA through protected medium.

Step 2:NA computes ID and stores ID in database. The NA sends token M_t to MC viva secure channel.

Step 3: MC save M_t in his database for future communication system.

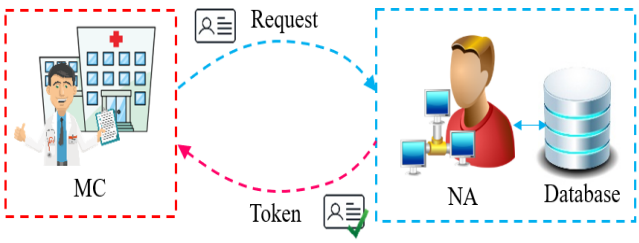

Figure 4. MC registration

3.2 Storage Phase

After registration, the medical centre generates encrypted EHR using homomorphic encryption for preserving privacy of the data and stores EHR in Cloud Storage.

3.2.1. Homomorphic encryption

The algorithms that make up the public-key, homomorphic encryption method that we employ are as follows:

- KeyGen (parms) produces a public evaluation key (evk) and a public/private key pair (pk, sk). When the parms system parameter is supplied, both of them are used in homomorphic multiplication.
- Encryption algorithm Enc(pk,m). Plaintext m should be encrypted with public key pk.
- Dec(sk,c) is a decryption algorithm that uses private key sk to decode ciphertext c.
- Given the input encryptions c1 and c2 of m1 and m2, the homomorphic addition operation Add (c1, c2) generates a cipher text that encrypts the total of m1 and m2.
- • Mult (c1, c2) is a homomorphic multiplication function that, assuming the encryptions c1 and c2 of m1 and m2, generates cipher text which encrypts the m1 + m2 result.

3.2.2. Quantum Diffie-Hellman key exchange

For exchanging the key for decrypting the EHR, a revolutionary physics-based quantum DH protocol (abbreviated as qDH) has been used which will be thoroughly explained. A quantum state in the qDH protocol will be the equivalent of the final key in the traditional DH protocol. In the lines that follow, the qDH protocol's requirements are detailed.

Suppose there are two communication parties, X and Y, that can exchange qubits. Each of the parties X and Y has a set of secret values that are designated by the letters SX and SY, respectively. These fixed secrets will be used to create shared, secret states for X and Y during the key exchange mechanism.

The initial secrets contained in SX and SY are retained stored by X and Y, respectively, while these created secret states are considered to be ephemeral ones.

Both sides must have agreed on a predetermined SP of shared, publically available information prior to the qDH communication. Since qDH takes into account quantum states and their two operations, SP contains state information of an initial, common state. |0i will be used to indicate it.

Thus, SP = |0i,..., where "..." denotes the presence of additional, shared, and publicly available information, which is optional. Given that the initial state |0i is shared or known to the public, X and Y must be able to prepare such a precise state.

Any operation for X and Y must therefore have a mutually known state as its starting point. In addition, the sets SX, SY, and SP result in the respective individual unitary operators U(SX), U(SY), and U(SP). Later, concrete illustrations of SX, SY, SP and their respective unitary operations will be shown. It is first demonstrated how the general qDH scheme is composed of:

- Party X creates a qubit state |0i according to the information supplied and made accessible to the public by SP. Then, depending on the secrets of set SX, X transmits a qubit |Xi=U(SX)|0i to Y, where U(SX) is a unitary operator.Depending on the secrets of set SY.
- Party Y receives |Ai and alters it using its own unitary operator U(SY). This leads to the equation |YAi=U(SY)|Xi.Y now follows the same procedures that X did in the first two steps.
- A qubit state |0i is created by Y according to the shared, accessible information SP. A qubit |Yi= U(SY)|0i is sent from Y to X.
- Party X receives $|\psi Yi$ and modifies that state by with U(SX), and unitary U(SP). This results in $|\psi XYi := U(SP)U(SX)|\psi Yi.$ Both communication parties are now in possession of the following states: $|\psi XYi$ (for X at the end of step 4) and $|\psi YXi$ (for Y at the end of step 2).

We now require, that $U(SP)U(SX)U(SY) = U(SY)U(SX)$. (1) Given that constraint for U(SX), U(SY), and U(SP), one has $|\psi XYi = |\psi YXi$, (2) and as a result, despite never having sent these final states and without being aware of each other's set of secrets, both X and Y are in possession of identical quantum states. Figure 5 illustrates such idea.

Actions taken on the side of X are represented, X. similar to the Y as the heading. The quantum states sent and their direction of transmission are shown in the "quantum channel" column. The following gives a straightforward illustration of SX, SY, SP, and their corresponding unitary operators.

3.3 Authentication Phase

When a new user wants to access to the EHR, he will be authenticated. Patient and MC communicate with NA and, he will start the authentication process in the public channel. After authorization, the key will be exchanged. The process for authorization has been given as follows.

Step 1: p_t and MC login with their token, ID and biometric.

Step 2: NA verifies the token T and biometric by comparing it with their data and aborts if not the authenticated one.

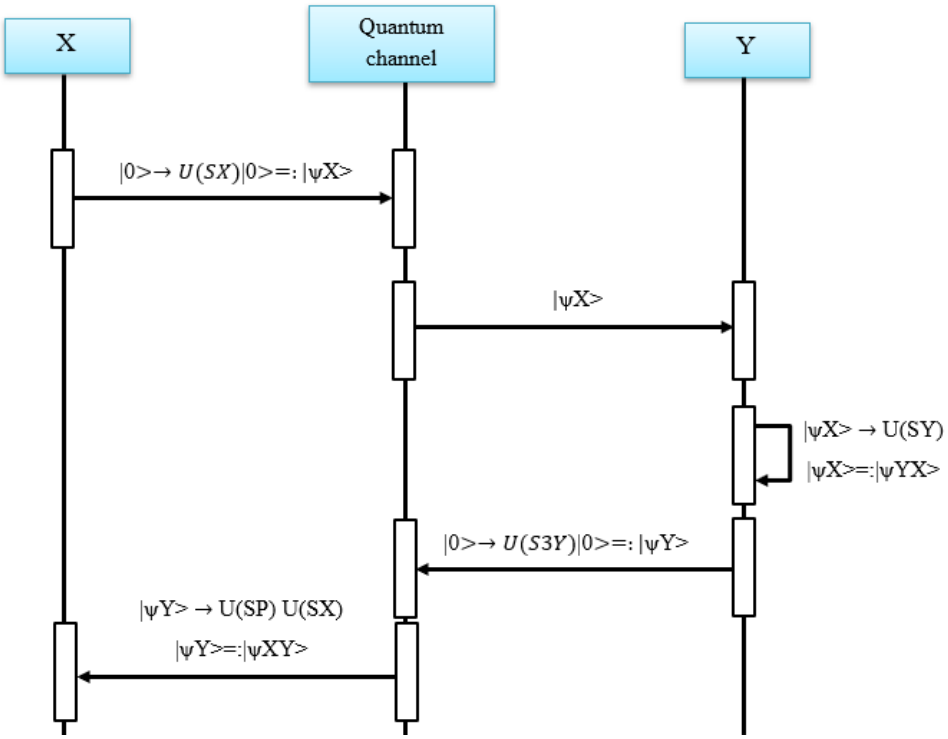

Figure 5. Working of Quantum Diffie Hellman key exchange

3.4 *Uploading data-log in blockchain*

The cloud server computes access rate of the user, transaction histories, and creates a data log, and uploads it to the blockchain. The data is finally stored in the cloud server's database. Each blocks contain the details of previous value, hash function and the data, which is represented in figure 6. Blockchain makes the proposed BACK system secure, because it is immutable and it is transparent. So, there will be no cheating among the users and the data will be more secure.

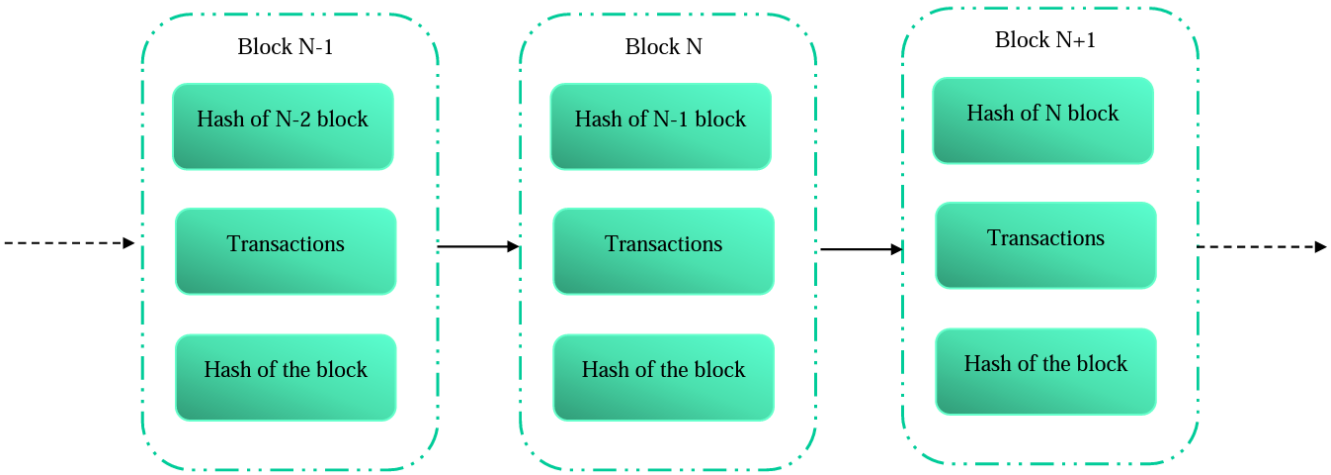

Figure 6. Blockchain mechanism of data storing

4. RESULTS AND DISCUSSION

The data upload procedure, access control mechanism, and encryption technology discussed in the previous part are all included in the method suggested in this article. This paper conducts Histogram analysis, and comparison analysis in terms of encryption time, decryption time, execution cost and security strength with previous work. Aiming to evaluate and validate the proposed novel BACK technique, the proposed scheme has been implemented on cloudsim platform and performance has been assessed.

4.1. BraTS 2020 dataset

The Segmentation of Brain Tumors The dataset, known as BraTS 2020, consists of multimodal 3D brain MR pictures and ground truth brain tumour segmentation annotated by medical professionals, with four T1, T1-c, T2, and FLAIR MRI modalities. 335 photos make up the BraTS 2020 dataset, 230 of which are used for training and 105 for testing. Edoema, enhancing tumour, necrosis, and non-enhancing tumour are all described as tumour subregions. Based on the description, three nested subregions were

created: total tumour (WT), tumour core (TC), and enhancing tumour (ET). The implications of the suggested and present techniques for encrypted images will be discussed in this section.

Figure 7 (a) shows the medical center homepage where they can access the data and update the data. Figure 7(b) represents the patient registration page, where the patient details need to be entered for their registration. Figure 7(c) represents the medical record updation page where we can update the medical records and also enter new medical data records. Figure 7(d) represents the patient detail access page in where we can view patient details and medical records.

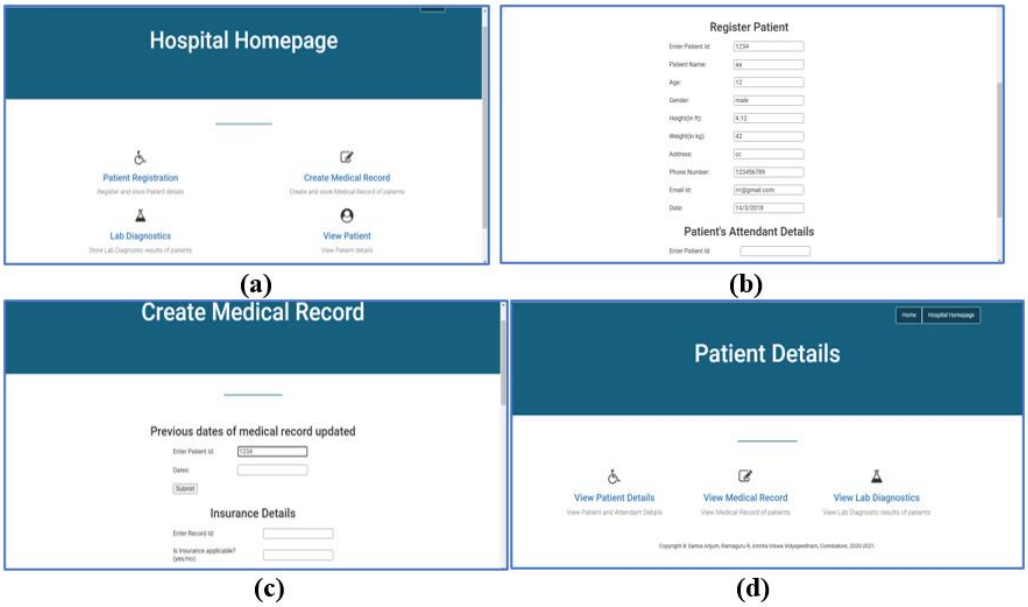

Figure 7. Real-time implementation (a) medical center Homepage (b) Patient registration page (c) Medical record updation (d) Patient detail access page

4.2. Performance Analysis

The medical images are saved in the cloud in encrypted form to provide security. Accessing the medical images by the authorized user is very simple on the other hand unauthorized users cannot access the medical image. The procedure for encryption of medical images is shown in Figure. 8.

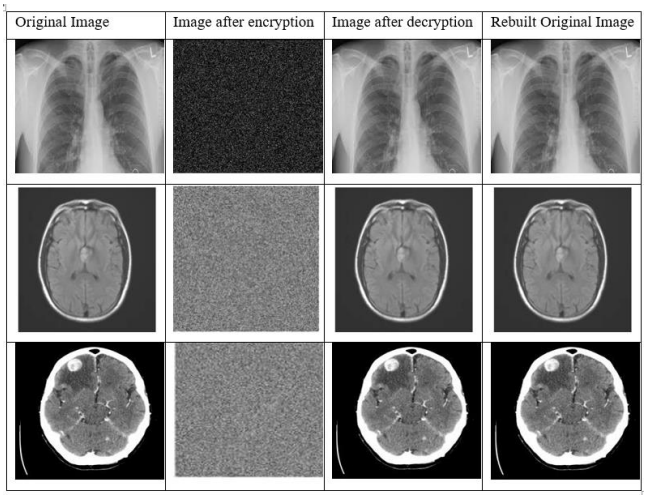

Figure 8. Performance analysis for BACK technique

The above figure describes the performance analysis of the BACK technique. Encryption is done to securely store the input medical data. Medical images that are kept in the cloud are encrypted and only accessible by the user. The images are not accessible to unauthorized users. The original image that has been rebuilt is also decrypted with the same technique. The images are transformed into an encrypted form using homomorphic encryption.

4.3. Histogram analysis

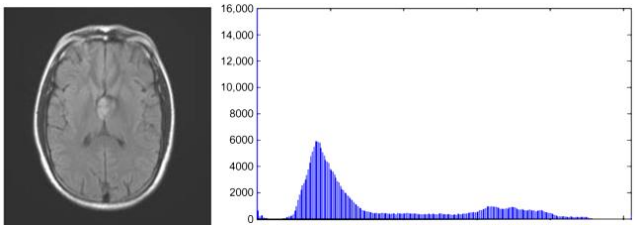

Figure 9. Histogram of original image

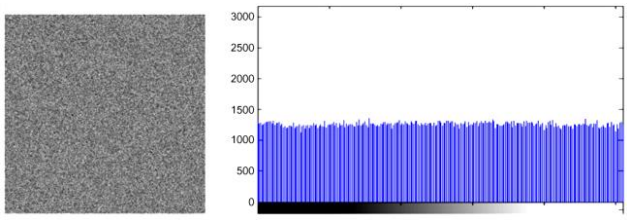

Figure 10. Histogram of encrypted image

The scatter plots of medical images throughout the encryption process are shown in Figures 9 and 10, which largely suggest that the scatter plots of the actual and encrypted picture may be distinguished from one another.

After encryption, the histogram's coherence demonstrates that the suggested model provides protection against attackers.

4.4 Comparison analysis

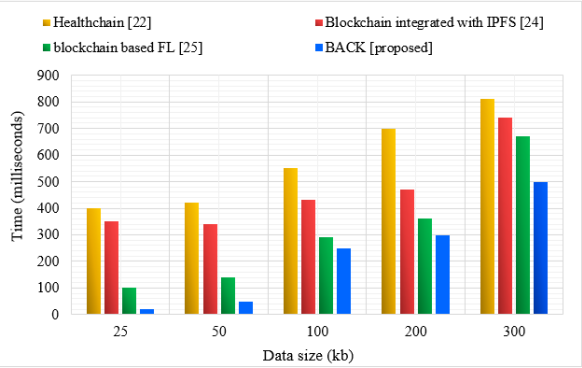

Figure 11. Encryption time comparison

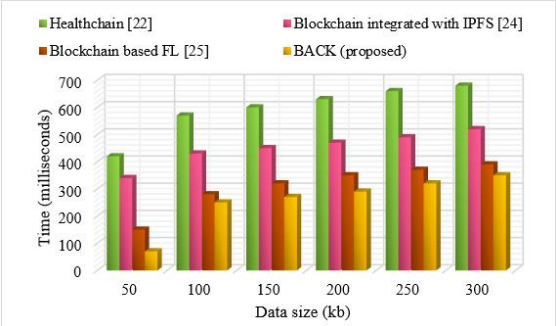

Figure 12. Decryption time comparison

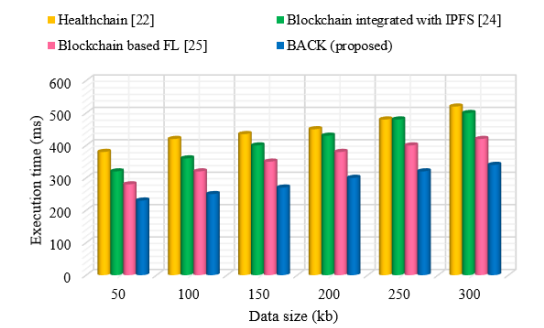

Figure 13. Comparative analysis of execution time

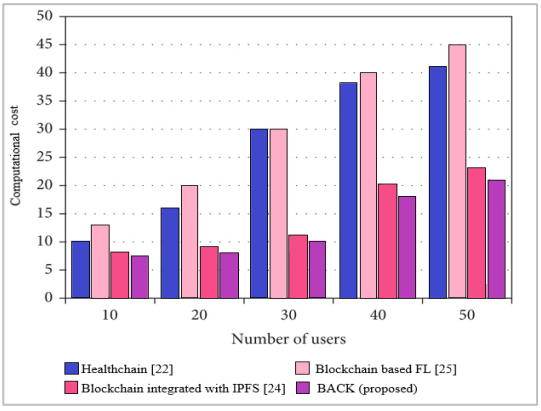

Figure 14. Comparative analysis of computational time

Figure 11 shows the encryption times of the existing Healthchain [22], Blockchain integrated with IPFS [24], Blockchain based FL [25] and proposed BACK algorithms. An increase in key size (bits) can enhance encryption time, according to this study. According to the experimental results, the proposed BACK method achieves less encryption time of 12.5%, 7.4%, and 4.65% than existing techniques such as Healthchain, Blockchain integrated with IPFS, and Blockchain based FL.

The proposed system and the existing approach are compared in Figure. 12 at the time of implementation. The proposed BACK method implementation time is quicker than the existing techniques. From the figure 13, it is clear that the proposed method achieves less execution time than existing techniques such as Healthchain [22], Blockchain integrated with IPFS [24], Blockchain based FL [25].

Figure 14 represents the computational time contrasting the suggested approach with the methods already in use. From the figure, it is clear that the proposed method achieves less computational cost than other existing techniques.

5. CONCLUSION

In this paper, an efficient BACK technique has been proposed for protecting the health records of patients while outsourcing the data through cloud storage. The proposed system ensured data and device security by implementing information security measures. The proposed method has been evaluated using CloudSim simulator. An evaluation of the effectiveness of the suggested strategy is based on several metrics, including execution time, encryption time, computational cost and decryption time. The suggested BACK technique is compared to state-of-the-art techniques such as Healthchain, Blockchain integrated with IPFS, Blockchain based FL. According to the experimental results, the proposed BACK method achieves less encryption time of 12.5%, 7.4%, and 4.65% than existing techniques such as Healthchain, Blockchain integrated with IPFS, and Blockchain based FL. E-healthcare data exchanged across multiple networks will be the subject of more data security and privacy assessments in the future.

CONFLICTS OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

FUNDING STATEMENT

No funding was received to assist with the preparation of this manuscript.

ACKNOWLEDGEMENTS

The authors would like to thank the reviewers for all of their careful, constructive and insightful comments in relation to this work.

REFERENCES

[1] Y. Alemami, A.M. Al-Ghonmein, K.G. "Al-Moghrabi, and M.A. Mohamed, Cloud data security and various cryptographic algorithms", *International Journal of Electrical and Computer Engineering*, vol.13, no. 2, pp.1867, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] S. Gadde, J. Amutharaj, and S. Usha. "A security model to protect the isolation of medical data in the cloud using hybrid cryptography", *Journal of Information Security and Applications*, vol. 73, pp.103412, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] M.K. Abdul-Hussein, and H.T. ALRikabi. "Secured Transfer and Storage Image Data for Cloud Communications", *International Journal of Online & Biomedical Engineering*, vol. 19, no. 6, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] N. Santos, B. Ghita, and G. Masala. "Medical Systems Data Security and Biometric Authentication in Public Cloud Servers", *IEEE Transactions on Emerging Topics in Computing*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] G. Sucharitha, V.E.D.U.L.A. Sitharamulu, S.N. Mohanty, A. Matta, and D. Jose, "Enhancing Secure Communication in the Cloud through Blockchain Assisted-CP-DABE", *IEEE Access*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] G. Borghini, S. Caputo, L. Mucchi, A. Rashid, S. Jayousi, M. Hämäläinen, T. Paso, and M. Hernandez. "Security of Wireless Body Area Networks for Healthcare Applications: Comparison between ETSI and IEEE Approaches", *In 2023 IEEE 17th International Symposium on Medical Information and Communication Technology (ISMICT)*, pp. 1-6. IEEE, 2023, May. [CrossRef] [Google Scholar] [Publisher Link]

[7] B. Chen, T. Xiang, D. He, H. Li, and K.K.R. Choo. "BPVSE: Publicly Verifiable Searchable Encryption for Cloud-Assisted Electronic Health Records", *IEEE Transactions on Information Forensics and Security*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] X. Li, H. Zhao, and W. Deng. "BFOD: Blockchain-based privacy protection and security sharing scheme of flight operation data", *IEEE Internet of Things Journal*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] J. Liu, Y. Fan, R. Sun, L. Liu, C. Wu, and S. Mumtaz. "Blockchain-Aided Privacy-Preserving Medical Data Sharing Scheme for E-Healthcare System", *IEEE Internet of Things Journal*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] X. Liu, S. Zhang, H. Huang, W. Wang, and R. Malekian, "A Verifiable and Efficient Secure Sharing Scheme in Multiowner Multiuser Settings", *IEEE Systems Journal*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] B.D. Deebak, and S.O. Hwang. "A Cloud-Assisted Medical Cyber-Physical System Using a Privacy-Preserving Key Agreement Framework and a Chebyshev Chaotic Map", *IEEE Systems Journal*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] M.F. Alomari, M.A. Mahmoud, Y.B. Yusoff, N. Gharaei, R.A. Abdalla, and S.S. Gunasekaran, "Data Encryption-enabled Cloud Cost Optimization and Energy Efficiency-based Border Security Model". *IEEE Access*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] H. Gao, H. Huang, L. Xue, F. Xiao, and Q. Li, "Blockchain-enabled Fine-Grained Searchable Encryption with Cloud-edge Computing for Electronic Health Records Sharing", *IEEE Internet of Things Journal*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] Z. Hua, X. Liu, Y. Zheng, S. Yi, and Y. Zhang, "Reversible data hiding over encrypted images via preprocessing-free matrix secret sharing", *IEEE Transactions on Circuits and Systems for Video Technology*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] A. Ali, M.F. Pasha, A. Guerrieri, A. Guzzo, X. Sun, A. Saeed, A. Hussain, and G. Fortino. "A Novel Homomorphic Encryption and Consortium Blockchain-based Hybrid Deep Learning Model for Industrial Internet of Medical Things", *IEEE Transactions on Network Science and Engineering*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[16] J. Sun, G. Xu, T. Zhang, X. Yang, M. Alazab, and R.H. Deng, "Privacy-Aware and Security-Enhanced Efficient Matchmaking Encryption", *IEEE Transactions on Information Forensics and Security*. 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] P. Tian, C. Guo, K.K.R. Choo, X. Tang, and L. Yao, "A Privacy Preserving Hybrid Range Search Scheme over Encrypted Electronic Medical Data in IoT Systems", *IEEE Internet of Things Journal*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[18] Y. Wang, and D. Papadopoulos. "Multi-User Collusion-Resistant Searchable Encryption for Cloud Storage", *IEEE Transactions on Cloud Computing*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[19] R.R. Irshad, S.S. Sohail, S. Hussain, D.Ø. Madsen, M.A. Ahmed, A.A. Alattab, O.A.S. Alsaiari, K.A.A. Norain, and A.A.A. Ahmed "A Multi-Objective Bee Foraging Learning-based Particle Swarm Optimization Algorithm for Enhancing the Security of healthcare data in cloud system", *IEEE Access*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[20] N. Yang, C. Tang, Q. Zhou, and D. He. "Dynamic Consensus Committee-based for Secure Data Sharing with Authorized Multi-Receiver Searchable Encryption", *IEEE Transactions on Information Forensics and Security*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[21] J. Niu, X. Li, J. Gao, and Y. Han. "Blockchain-based anti-key-leakage key aggregation searchable encryption for IoT", *IEEE Internet of Things Journal*, vol.7, no.2, pp.1502-1518, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[22] S. Chenthara, K. Ahmed, H. Wang, F. Whittaker, and Z. Chen, "Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology", *Plos one*, vol.15, no. 12, pp. e0243043, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[23] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, "HealthBlock: A secure blockchain-based healthcare data management system", *Computer Networks*, vol. 200, p.108500, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[24] J. Jayabalan, and N. Jeyanthi. "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy", *Journal of Parallel and Distributed Computing*, vol.164, pp.152-167, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[25] Singh, M.B. and Pratap, A., "BPFISH: Blockchain and Privacy-preserving FL Inspired Smart Healthcare", arXiv preprint arXiv:2207.11654, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[26] A.E. Adeniyi, K.M. Abiodun, J.B. Awotunde, M. Olagunju, O.S. Ojo and N.P. Edet, "Implementation of a block cipher algorithm for medical information security on

cloud environment: using modified advanced encryption standard approach", *Multimedia Tools and Applications*, pp. 1-15. [CrossRef] [Google Scholar] [Publisher Link]

[27] I. Gupta, D. Saxena, A.K. Singh and C.N. Lee, "SeCoM: An Outsourced Cloud-Based Secure Communication Model for Advanced Privacy Preserving Data Computing and Protection", *IEEE Systems Journal*, pp. 1-12, 2023. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

G. Sreetha, she was born in Kanyakumari District, Tamilnadu, India in 2000. She received her BE degree in computer science and engineering from Arunachala college of engineering, Manavilai, Anna University, India in 2021. Currently she is pursuing her ME degree in computer science and engineering from Arunachala college of Engineering, Manavilai, Anna University, India. Her interested research area is cloud computing, and cryptography.

T. V. Chithra received her B.E. degree in CSE from M.S University, Tirunelveli in 2004, and obtained M.E. degree in CSE from Anna University, Chennai in 2009. She obtained Ph.D. degree from Anna University, Chennai for her research work on Wireless Sensor Network in 2021. She has published 4 papers in international journals, fourteen papers in conferences and four books. Currently she is working as Associate Professor in the Department of CSE Arunachala College of Engineering for Women, India. Her research areas of interest include WSN, BigData, Cloud Computing, Internet of Things.

Arrived: 02.08.2023
Accepted: 29.09.2023