ENSURING DATA SECURITY FOR PATIENT HEALTH RECORDS WITH CLOUD-BASED BLOCKCHAIN MONITORING AND ACCURATE DISEASE CLASSIFICATION USING CNN

Mr. Sunil Kumar R M[1], Dr. A. Jayachandran[2]

Article History: **Received:** 11.02.2023 **Revised:** 18.04.2023 **Accepted:** 10.06.2023

Abstract

Blockchain technology enables secure and transparent data sharing, ensuring that only authorized parties can access the data. Moreover, Attribute-based Access Control (ABAC) provides more granular control over data access by granting it based on specific attributes, such as a patient's age or medical condition. In this paper, a proposed Blockchain-based Healthcare system with a cloud-based system is used for patient health monitoring. A secure and reliable healthcare-based blockchain with attribute-based encryption is suggested as a better solution to data access problems. The encryption is performed using homomorphic encryption techniques, and the hybrid Equilibrium with Poor and Rich Optimization (HEPRO) can perform the key generation operation. To convert an input (a message) into a fixed-size 256-bit value known as a hashed key, a cryptographic hash function called SHA-256 (Secure Hash Algorithm 256-bit) is used. After decrypting the patient details, the Weighted Convolutional Neural Network (CNN) is employed to classify the disease and provide treatment for the patient. Furthermore, wearable devices are utilized in the proposed system to collect patient data, offering real-time updates on the patient's health condition, which can be crucial in emergency situations.

Keywords: Blockchain, Attribute-Based Access Control, Cloud-Based Systems, Encryption, Hybrid Equilibrium With Poor And Rich Optimization And Key Generation.

[1,2]School of Computer Science, Presidency University, Bangalore, India

DOI: 10.31838/ecb/2023.12.6.42

1. INTRODUCTION

Securely transferring medical data is a challenge in healthcare. Traditional methods like Electronic Health Records (EHRs) are vulnerable to cyber-attacks [1], [2], [3]. There is a need for secure and efficient medical data sharing to enhance patient care, clinical decision-making, and safety. Concerns arise regarding the security and privacy of patient data with the increasing development of EHRs [4], [5]. Blockchain is a secure and transparent technology that can effectively protect sensitive healthcare data from cyber-attacks. Its decentralized design prevents single points of failure, making it an ideal solution for securing Electronic Health Records (EHRs) [6], [7]. Smart contracts provide security, transparency, and automation in various fields, including healthcare. In healthcare, they increase the confidentiality and safety of EHRs by defining data access and modification conditions [8], [9], [10].

The paper explores the use of blockchain and smart contracts for securing EHRs, addressing the challenges of EHR management and highlighting their benefits. It provides real-world examples and discusses future developments and implications for the healthcare industry. The contributions include the hybridization of the Equilibrium Optimization Algorithm (EOA) with Poor and Rich Optimization (HEPRO) for encryption and key generation, splitting the EOA population for optimization, utilizing the secure SHA256 hash function, and improving disease classification in CNN using the weighted loss function with RMSE and HERPO algorithm.

2. LITERATURE SURVEY

The recent existing papers in blockchain for EHR data sharing and patient monitoring are discussed in this section.

In 2020, Shamshad, et al., [11] have suggested a revolutionary blockchain-based EHR sharing system that protected privacy and security for better diagnosis and effective therapies in TMIS.

In 2019, Liu, et al., [12] have introduced a medical protection system data and sharing based on blockchain. To enhance the hospital's electronic health system, the paper suggested a method for exchanging and protecting medical data that was based on a private blockchain owned by the facility.

In 2018, Zhang, and Lin, [13] have enhance the diagnosis in e-Health systems, the paper offered a blockchain-based safe and privacy-preserving PHI sharing (BSPP) approach. The two main forms of blockchains were first invented, together with their respective data formats and consensus procedures.

In 2019, Shen, et al., [14] have introduced sensors and mobile applications which were able to track the physical state of patients due to the widespread deployment of IoT devices.

In 2020, S Cheng, et al., [15] have discussed medical data vendors' authentication method that poses a security risk and consumers could have been resolved using bilinear mapping and intractable problems. The hospital and blockchain node could authenticate each other in two directions, and the trustworthiness of the trusted third party could be avoided.

Problem Formulation

Medical data exchange among various healthcare institutions and stakeholders is crucial for enhancing patient care and advancing medical research. Nevertheless, openness, security, and privacy protection are frequently absent from conventional data exchange procedures. Medical data centralization also introduces a single point of failure and leaves the data open to cyber-attacks. Medical data must also be safeguarded against illegal access and disclosure since it contains sensitive information about patients, including their medical history, diagnoses, and treatments. Thus, a safe and privacy-preserving mechanism is required for authorized parties to share medical data.

This study suggests a blockchain-based system for exchanging medical data that includes ABAC and privacy protection. To guarantee data integrity, accessibility, and transparency, the suggested approach makes use of the tamper-proof and decentralized features of blockchain technology. It is a good idea to have a backup plan in place in case the backup plan fails. The suggested methodology also incorporates privacy-preserving methods including data anonymization, encryption, and differential privacy to safeguard private patient data against illegal access and disclosure. The privacy-preserving methods make sure that, while safeguarding patient privacy, only authorized persons with the required qualities may access the pertinent medical data. In general, the proposed blockchain-based healthcare information exchange method solves the shortcomings of conventional data-sharing methods and offers a safe, open, and privacy-preserving alternative for the exchange of health information among authorized individuals.

Problem Solution

The suggested algorithm follows multiple phases to achieve desired outcomes. Patient records are collected and encoded for privacy protection before being saved in the cloud server. The system ensures data redundancy for data recovery in case of server unavailability. Encryption and decryption techniques, including homomorphic encryption and

HERPO key generation, are used to enhance cloud security. The proposed system aims to secure sensitive healthcare data and prevent unauthorized access using encryption and blockchain technology.

To implement this approach we use following steps :

- **Generate cryptographic keys:** Use HEPRO to create a pair of keys - a public key for encryption and a private key for decryption.
- **Encrypt data:** Apply homomorphic encryption techniques using the public key to protect the data during transmission or storage in the cloud.
- **Use blockchain:** Store the encrypted data on a secure and transparent blockchain ledger.
- **Decrypt data:** Authorized users can decrypt the data using their private key, ensuring secure access.

Equilibrium optimizer

Another meta-heuristic method, the equilibrium Optimizer (EO), which is motivated by physical principles, for resolving optimization issues. The following three steps serve as illustrations of the EO algorithm's analysis and determination is discussed below.

Step 1: Initialization

At this stage, EO makes use of a collection of particles, And each particle represents a vector of concentration that encapsulates the reaction to the ideal solution. The following Eq. (1) is used to produce the initial concentrations vector at random inside the search space:

$$\vec{C}_i = c_{min} + (c_{max} - c_{min}) \times r,\ i = 0,1,2,\ldots,n \quad (1)$$

Where r is a random number between [0,1], $\vec{V}_i$ represents the concentration vector of the particle c_{min} and c_{max} provide the issue's minimum and maximum limits for each dimension, with n denoting how many objects are in the group.

Step 2: Candidates and the equilibrium pool ($\vec{C}_{eq,pool}$)

Each meta-heuristic algorithm has a distinct objective based on its unique characteristics. When EO (Evolutionary Optimization) reaches the equilibrium state, it potentially finds an optimal solution for the optimization problem. The number of iterations required to reach equilibrium is unknown to EO during the optimization phase. EO utilizes two options: the average of the top four particles and the top four particles found in the population at equilibrium. These five equilibrium possibilities enhance EO's ability to explore and exploit, with the first four candidates assisting in increasing diversification and improvement on average.These five possibilities are kept in the Equilibrium pool vector which is shown in Eq. (2),

$$\vec{C}_{eq,pool} = [\vec{C}_{eq(1)}, \vec{C}_{eq(2)}, C_{eq(3)}, \vec{C}_{eq(4)}, \vec{C}_{eq(avg)}] \quad (2)$$

Step 3: Concentration Updating

The following phrase aids in EO's ability to maintain a tenable balance between intensity and diversity. In a real control volume, turnover rate ($\vec{F}$) in Eq. (3) might change over time, hence is meant to be a random value between 0 and 1.

$$\vec{F} = e^{-\vec{\lambda}(t-t_0)} \quad (3)$$

Where, using the following equations, t is lowered with the increase of the iteration (t),

$$t = \left(1 - \frac{t}{t_{max}}\right)^{\left(k_2 * \left(\frac{t}{t_{max}}\right)\right)} \quad (4)$$

Where the current iteration is t, and the maximum iteration is t_{max} and k_2 is a fixed value used to regulate the ability to intensify (exploit). To enhance the variety and intensity of EO, another element, k_1, is employed in Eq. (5). It is constructed as follows:

$$\overrightarrow{t_0} = \frac{1}{\vec{\lambda}}\ln(-k_1 sign(\vec{r} - 0.5)[1 - e^{-\vec{\lambda}t}]) + t \quad (5)$$

Where k_1 is a constant that is used to regulate exploration potential; as k_1 increases, diversification and intensification capabilities improve, k_2 is a constant variable that is used to manage the ability to exploit in relation to k_1. When k_2 is higher, the capacity for intensification is better and the capacity for diversification is worse. Another word for the intensification operator's improvement is generation rate ($\vec{R}$), which is written in Eq. (6) as,

$$\vec{R} = \vec{R}_0 * e^{-\vec{\lambda}(t-t_0)} \quad (6)$$

It is written as follows, where $\vec{\lambda}$ is a random vector with range [0, 1] and $\vec{R}_0$ is the starting value.

$$\vec{R}_0 = \overrightarrow{RCP} * (\vec{C}_{eq} - \vec{\lambda} * \vec{c} \quad (7)$$

$$\overrightarrow{RCP} = \begin{cases} 0.5r_1, r_2 > RP \\ 0, \ Otherwise \end{cases} \quad (8)$$

Where Equilibrium pool and candidates is represented as $\vec{C}_{eq}$, the two integers $r_1\ and\ r_2$ are chosen at random from 0 to 1. According to a probability RP, the generation rate control parameter $\overrightarrow{RCP}$ in this equation decides regardless of the generating rate is applied to the updating process. Finally, here is the EO updating is given in Eq. (9),

$$\vec{C} = \vec{c}_{eq} + \left(\vec{c} - \vec{c}_{eq}\right) \times \vec{F} + \frac{\vec{R}}{\vec{\lambda} \times V} * (1 - \vec{F}) \quad (9)$$

Where V has the value of 1. Hybrid equilibrium optimization with is a technique that combines the advantages of both poor and rich optimization approaches into the equilibrium optimization. Basically the PRO have two classes like poor and rich. The poor methods are characterized by their ability to quickly converge to a solution but with low precision, while rich optimization methods are characterized by their ability to converge to a highly accurate solution but with high computational cost.

SHA-256 is a widely used cryptographic hash function that converts input into a fixed-size hash value. It is considered secure and resistant to collision attacks. SHA-256 is commonly used for cryptographic purposes such as digital signatures, message authentication codes (MACs), and key derivation functions, ensuring data integrity in critical applications.

After updating the current population rate the total population is splited into two parts using the poor and rich optimization. The two parameters called $\vec{C}_1$ and $\vec{C}_2$ which is similar to the movement of poor and rich solution, given in Eq. (10) and Eq. (11).

$$\vec{C}_1^{t+1} = \vec{C}_1^t + \alpha * [\vec{C}_1^t - \vec{C}_{2.max}^t] \quad (10)$$

$$\vec{C}_2^{t+1} = \vec{C}_2^t + \alpha * \left[\frac{\vec{C}_1^t + \vec{C}_{1.mean}^t + \vec{C}_{1.min}^t}{3} - \vec{C}_2^t\right] \quad (11)$$

Where $\vec{C}_1^t$ and $\vec{C}_1^{t+1}$ are the current solution of the $\vec{C}_1$ and $\vec{C}_2^t$ and $\vec{C}_2^{t+1}$ are the current solution of the $\vec{C}_2$, α is a constant, $\vec{C}_{2.max}^t$ is the best solution of the population $\vec{C}_2$ and similarly the worst solution of the $\vec{C}_2^t$ is $\vec{C}_{1.min}^t$.

Decryption Process

As the data is now completely encrypted, the instant the doctor logs in to view patient information, he begins to get the data in encrypted form. The doctor must authenticate himself in order to decode this data. The physician does this by uploading a photo, which is subsequently verified by comparing it to the physician database on the local server. If they match, the data is decrypted; If not, the request for authentication is turned down or rejected. The encryption algorithm is simply reversed during the decryption procedure. During the decryption procedure, the first data block is retrieved from the generated key itself, and the SHA256 hash compute is then applied to the following block.

Disease classification using CNN

After decrypting the data, the patient details are given to the CNN for disease classification. Based on the classifications of the disease, the doctor knows the priority of the disease which is treated at first. Convolution, pooling, and a fully connected layer are the three fundamental layers of a CNN structure. These various layers have a function in various tasks.

Convolution Layer

A pixel's output value in the convolution process is determined as the weighted sum of its own value and the values of its neighbours. The convolution kernel, also known as the filter, is the weights matrix. The input data becomes convoluted when kernel filters are applied. Eq. (12) below gives the fundamental equation for convolution:

$$y_k = \sum_{n=0}^{N-1} X_n f_{k-n} \quad (12)$$

Where, y, x, f, and N refer to the output vector, the input signal, the filter, and the number of variables respectively. The windowing operation of the data 's windowed h filter allows for the recognition of the features. Typically, Convolution is followed by activation in an ESA system. The ReLU is frequently employed for activation in deep learning networks. Equation provides the mathematical expression for the ReLU activation function in Eq. (13).

$$f(x) = \begin{cases} 0 \; if \; x < 0 \\ x \; if \; x \geq 0 \end{cases} \quad (13)$$

Pooling Layer

The goal of the pooling layer is to decrease both the feature map and the quantity of variables utilized in the network. A type of non-linear down sampling is the idea of the ESA pooling. The input data is divided into a number of non-overlapping rectangles for the pooling process, and each sub-maximum region's or average value is calculated (rectangle). This approach makes it possible to guarantee translation stability while reducing the size of the property as needed. There are two common pooling techniques: average pooling and maximum pooling. Because of its positive findings, this study utilized maximum pooling.

Fully Connected Layer

These layer's features are transformed into one-dimensional feature vectors by the data pattern's features. Like traditional artificial neural networks, fully connected layers operate in the same way. The fully connected layer has a lot of parameters, which is its biggest drawback. The calculation load increases as a result of their excessive parameter count. As shown in Figure 1, the procedures used to

analyze the EEG signal data in the recommended network topology in our study.

Weighted Loss Function (WLF) with HERPO
In a typical CNN, the loss function is used to measure the difference between the predicted outputs and the actual outputs. The most commonly used loss function for regression problems is the Mean Squared Error (MSE). However, it is possible to use a modified loss function in a CNN that uses the root mean squared error (RMSE) instead of MSE. The RMSE is the square root of the MSE, and it is used to penalize larger errors more heavily than smaller errors. To use the RMSE as a loss function in a CNN, you would need to modify the existing code that calculates the loss. Instead of calculating the MSE, you would calculate the RMSE using the following formula in Eq. (14) to Eq. (19),

$$RMSE = \sqrt{\frac{\sum_{i=1}^{J}(X_i - \widehat{X_i})^2}{J}} \qquad (14)$$

Where the parameters like $\lambda = 0.9$, $\sigma = 0.1$ are introduced for effectively predict the difference between actual and predicted value, which are given in Eq. (15), (16) and Eq. (17),

$$\alpha_a = \lambda * (X_i - \widehat{X_i}) \qquad (15)$$

$$\beta_a = \sigma * \left(\frac{X_{imax} + X_{imin}}{2} - \frac{\widehat{X_{imax}} + \widehat{X_{imin}}}{2}\right) \qquad (16)$$

$$\gamma_a = \lambda * \left(\frac{X_{imax} + X_{imin}}{2} - \frac{\widehat{X_{imax}} + \widehat{X_{imin}}}{2}\right) \qquad (17)$$

The weighted loss function WLF is given in Eq. (18),

$$WLF = \sqrt{\frac{\sum_{i=1}^{J}\left(\alpha_{\widehat{X_{imax}}} - \gamma_a X_{imax} - \beta_a X_{imin} - \beta_a \alpha_{a,Idle_{min}} - \gamma_a\right)^2}{J}} \qquad (18)$$

The proposed modified WLF is utilized for fine tuning the parameter of the CNN to improve the performance of disease classification. Therefore, the parameters of the CNN such as Mini BATCH SIZE, Momentum, and Learning Rate are taken as the hyperparameters for fine tuning performance.

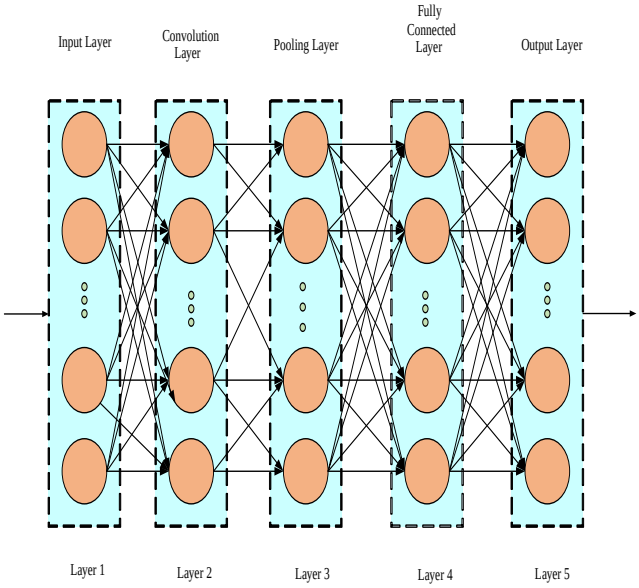

Figure 1: Structure of CNN layers

The final layer, max pooling, reduces this size of the input data. These data are vectorized in the following layer, then transferred to the fully connected layer. Using the classification data, the mental health of the patient is monitored by the doctor.

3. RESULT AND DISCUSSION

In this section the dataset used for patient disease classification is discussed. After decrypting the patient data, the CNN classifier is used for classifying the disease. Both the suggested model's and the classifier model's performance is discussed and contrasted with the methods already in use. Using the Python platform, the implementation is carried out.

EEG Psychiatric Disorders Dataset
The proposed method uses the EEG Psychiatric Disorders Dataset, which includes EEG recordings from individuals with mental conditions. This dataset contains approximately 1000 characteristics for detecting psychiatric diseases and covers various illnesses such as depression, personality disorders, anxiety disorders, schizophrenia, eating disorders, and addictive behaviors. The dataset is divided into two sets: Data 1 for training (70% of the data) and

Data 2 for testing (30% of the data). Performance metrics, including Encryption Time (ET), Decryption Time (DT), Key Generation Time (KGT), and Restoration Efficiency (RE), are evaluated to assess efficiency. Table 1 displays the metric values for Data 1.

Table 1: Comparison of metrics for data 1

Metrics	**CHOA**	**EO**	**PRO**	**Proposed**
ET(s)	0.130654	0.120921	0.11891	0.11551
DT(s)	0.116658	0.112097	0.110581	0.107419
KGT (s)	0.247313	0.233018	0.229491	0.222929
RE	0.75187	0.793594	0.796818	0.802673

The table compares different metrics for four encryption algorithms: Chimp optimization algorithm (CHOA), EO, PRO, and the Proposed algorithm. The metrics include ET, DT, Key Generation Time, and Restoration Efficiency.

ET: This metric measures the time taken by each algorithm to encrypt a message. From the table, we can see that the proposed algorithm has the lowest ET of 0.11551 seconds, followed by CHOA (0.130654 seconds), EO (0.120921 seconds), and PRO (0.11891 seconds).

DT: This metric measures the time taken by each algorithm to decrypt an encrypted message. Here, we can see that the proposed algorithm has the lowest DT of 0.107419 seconds, followed by PRO (0.110581 seconds), EO (0.112097 seconds), and CHOA (0.116658 seconds).

Key Generation Time: This metric measures the time taken by each algorithm to generate a key for encryption. Here, we can see that the proposed algorithm has the lowest KGT of 0.222929 seconds, followed by PRO (0.229491 seconds), EO (0.233018 seconds), and CHOA (0.247313 seconds).

Restoration Efficiency: This metric measures the efficiency of the algorithm in restoring the original message from the encrypted message. The proposed algorithm has the highest RE of 0.802673, followed by PRO (0.796818), EO (0.793594), and CHOA (0.75187).

In terms of ET, DT, KGT, and RE, the suggested approach outperforms the competition. Yet it's critical to remember that other elements, including implementation difficulty and security, are as significant in deciding whether an encryption technique is appropriate for a certain use case.

For the second the training data is 80% and the testing data is 20% (Data 2). The metrics comparison for the data 2 is shown in table 2.

Table 2: Comparison of metrics for data 1

Metrics	**CHOA**	**EO**	**PRO**	**Proposed**
ET(s)	0.121305	0.120298	0.113157	0.110396
DT(s)	0.118394	0.103926	0.105232	0.102664
Key Generation Time(s)	0.239698	0.224224	0.218389	0.21306
Restoration Efficiency	0.819981	0.75487	0.857799	0.875386

The table provides a comparison of four metrics for different encryption schemes: CHOA, EO, PRO, and Proposed for the Data 2. These metrics are ET, DT, key generation time, and restoration efficiency.

ET
It refers to the time taken to encrypt a message using the encryption scheme. The table reveals that the Proposed system has the lowest ET of 0.110396 seconds, followed closely by the PRO scheme with a time of 0.113157 seconds. CHOA and EO schemes take slightly longer, with ETs of 0.121305 and 0.120298 seconds, respectively. The ET for the data 1 and data 2 is shown in Figure 2.

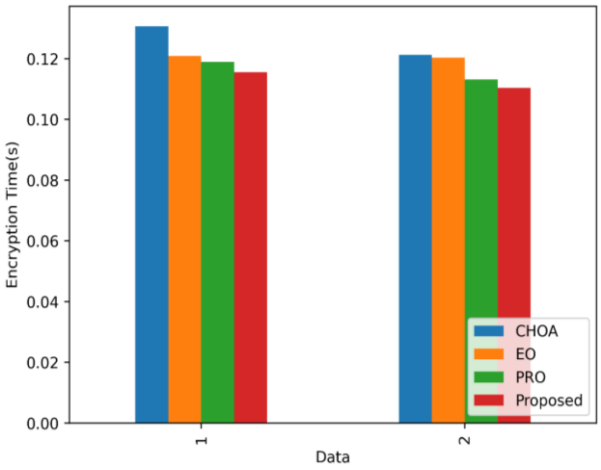

Figure 2: ET of the proposed and existing techniques

DT It refers to the time taken to decrypt an encrypted message using the encryption scheme. The table 1 & 2 proves that the Proposed scheme has the lowest DT of 0.102664 seconds, followed by the PRO scheme with a time of 0.105232 seconds. CHOA and EO schemes take slightly longer, with DTs of 0.118394 and 0.103926 seconds, respectively. Figure 3 displays the DT for Data 1 and Data 2.

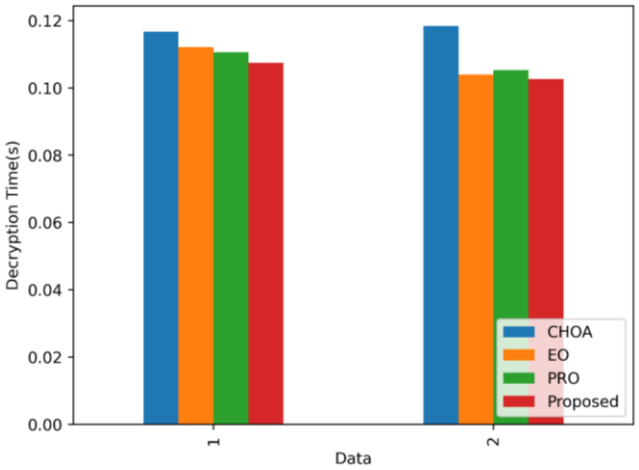

Figure 3: DT of the proposed and existing techniques

KGT

It refers to the time taken to generate the encryption keys used by the encryption scheme. The table 1 & 2 illustrates that the Proposed scheme has the lowest KGT of 0.21306 seconds, followed by the PRO scheme with a time of 0.218389 seconds. CHOA and EO schemes take slightly longer, with key generation times of 0.239698 and 0.224224 seconds, respectively. In Figure 4, the KGT for data 1 and data 2 is displayed.

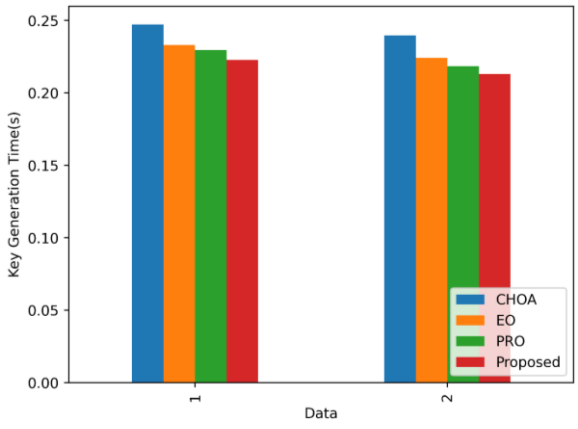

Figure 4: KGT of the proposed and existing techniques

RE

It refers to the efficiency of the encryption scheme in restoring the original message after decryption. The table shows that the Proposed scheme has the highest RE of 0.875386, followed by the PRO scheme with a RE of 0.857799. CHOA and EO schemes have lower restoration efficiencies of 0.819981 and 0.75487, respectively. Figure 5 displays the RE for encrypting Data 1 and Data 2.

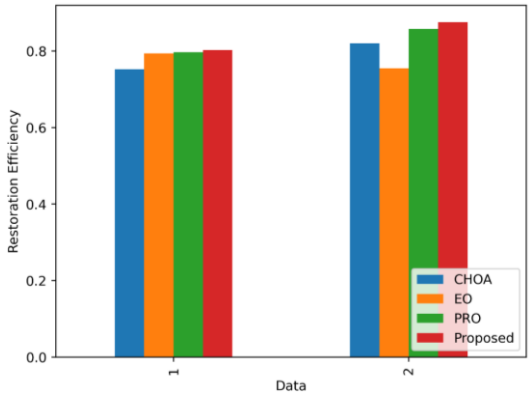

Figure 5: RE of the proposed and existing techniques

The CNN's performance is evaluated and compared to other methods such as RNN, ANN, SVM, and Bi-LSTM. Data 1, comprising 70% for training and 30% for testing, is used to assess and compare these techniques. Table 2 presents the comparison between the proposed CNN and the existing methods for Data 1.

Table 2: Comparison of classifier performance for Data 1

Metrics	**RNN**	**ANN**	**SVM**	**Bi-LSTM**	**CNN**
Accuracy	0.884762	0.858682	0.82698	0.844309	0.920205
Precision	0.877489	0.901105	0.792149	0.808748	0.91263
Sensitivity	0.892212	0.813413	0.869237	0.887452	0.927943
Specificity	0.87741	0.903351	0.785281	0.801737	0.912569
F-Measure	0.857204	0.829885	0.802118	0.818925	0.891533
MCC	0.923788	0.850387	0.832518	0.849963	0.967521
NPV	0.892182	0.824206	0.8687	0.886903	0.927932
FPR	0.02702	0.020723	0.024812	0.025332	0.020175
FNR	0.005786	0.004291	0.006647	0.006786	0.003536

The table presents evaluation metrics for different machine learning models in a specific task. The metrics include Accuracy, Precision, Sensitivity, Specificity, F-Measure, MCC, NPV, FPR, and FNR. Accuracy measures overall correctness of predictions, with the CNN model achieving the highest accuracy (0.920205) and SVM having the lowest accuracy (0.82698). Precision indicates a model's ability to detect positive occurrences, with the ANN model achieving the best precision (0.901105) and SVM having the lowest precision (0.792149). Sensitivity measures how well the model detects positive examples, with the CNN model having a sensitivity of 0.927943 and the ANN model having a sensitivity of 0.813413, as shown in the table.

4. CONCLUSION

In conclusion, the proposed Blockchain-based Healthcare system with a cloud-based system provides a secure and reliable solution to the existing problems in healthcare data access. The system incorporates ABAC for granular control over data access and homomorphic encryption techniques for secure data sharing. The utilization of wearable devices for real-time patient data collection was an essential aspect of the proposed system, providing quick updates in emergency situations. Additionally, the CNN can classify the disease and provide treatment after decrypting the patient's details.

The KGT for the proposed model was 0.21306s which was higher than the existing techniques like PRO, EO, and CHOA. Similarly, the RE was also high as 87.53%. Overall, the proposed system can potentially revolutionize the healthcare industry, ensuring secure and transparent data sharing while providing efficient and effective patient care.

5. REFERENCES

1. Nagasubramanian, G., Sakthivel, R.K., Patan, R., Gandomi, A.H., Sankayya, M. and Balusamy, B., 2020. Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. *Neural Computing and Applications*, *32*, pp.639-647.
2. Alsayegh, M., Moulahi, T., Alabdulatif, A. and Lorenz, P., 2022. Towards secure searchable electronic health records using consortium blockchain. *Network*, *2*(2), pp.239-256.
3. Sabu, S., Ramalingam, H.M., Vishaka, M., Swapna, H.R. and Hegde, S., 2021. Implementation of a Secure and privacy-aware E-Health record and IoT data Sharing using Blockchain. *Global Transitions Proceedings*, *2*(2), pp.429-433.
4. Vimalachandran, P., Liu, H., Lin, Y., Ji, K., Wang, H. and Zhang, Y., 2020. Improving accessibility of the Australian My Health Records while preserving privacy and security of the system. *Health Information Science and Systems*, *8*, pp.1-9.
5. Hashim, F., Shuaib, K. and Sallabi, F., 2021. Medshard: Electronic health record sharing using blockchain sharding. *Sustainability*, *13*(11), p.5889.
6. Yaqoob, I., Salah, K., Jayaraman, R. and Al-Hammadi, Y., 2021. Blockchain for healthcare data management: opportunities, challenges, and future recommendations. *Neural Computing and Applications*, pp.1-16.
7. Amir Latif, R.M., Hussain, K., Jhanjhi, N.Z., Nayyar, A. and Rizwan, O., 2020. A remix IDE: smart contract-based framework for the healthcare sector by using Blockchain technology. *Multimedia tools and applications*, pp.1-24.
8. Nguyen, D.C., Pathirana, P.N., Ding, M. and Seneviratne, A., 2019. Blockchain for secure ehrs sharing of mobile cloud based e-health systems. *IEEE access*, *7*, pp.66792-66806.
9. Fatokun, T., Nag, A. and Sharma, S., 2021. Towards a blockchain assisted patient owned system for electronic health records. *Electronics*, *10*(5), p.580.
10. Lee, J.S., Chew, C.J., Liu, J.Y., Chen, Y.C. and Tsai, K.Y., 2022. Medical blockchain: Data sharing and privacy preserving of EHR based on smart contract. *Journal of Information Security and Applications*, *65*, p.103117.
11. Shamshad, S., Mahmood, K., Kumari, S. and Chen, C.M., 2020. A secure blockchain-based e-health records storage and sharing scheme. *Journal of Information Security and Applications*, *55*, p.102590.
12. Liu, X., Wang, Z., Jin, C., Li, F. and Li, G., 2019. A blockchain-based medical data sharing and protection scheme. *IEEE Access*, *7*, pp.118943-118953.
13. Zhang, A. and Lin, X., 2018. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *Journal of medical systems*, *42*(8), p.140.
14. Shen, B., Guo, J. and Yang, Y., 2019. MedChain: Efficient healthcare data sharing via blockchain. *Applied sciences*, *9*(6), p.1207.
15. Cheng, X., Chen, F., Xie, D., Sun, H. and Huang, C., 2020. Design of a secure medical data sharing scheme based on blockchain. *Journal of medical systems*, *44*(2), p.52.
16. Balachandar S., Chinnaiyan R. (2019) Centralized Reliability and Security Management of Data in Internet of Things (IoT) with Rule Builder. In: Smys S., Bestak R., Chen JZ., Kotuliak I. (eds) International Conference on Computer Networks and Communication Technologies. Lecture Notes on Data Engineering and Communications Technologies, vol 15. Springer, Singapore
17. G. Sabarmathi and R. Chinnaiyan, Reliable Machine Learning Approach to Predict Patient Satisfaction for Optimal Decision Making and Quality Health Care,*2019 International Conference on Communication and Electronics Systems (ICCES)*, Coimbatore, India, 2019, pp. 1489-1493
18. Hari Pranav A; M. Latha; Ashwin. M. S; R. Chinnaiyan, "BlockchainAs a Service (BaaS) Framework for Government Funded Projects e-Tendering Process Administration and Quality Assurance using Smart Contracts," *2021 International Conference on Computer Communication and Informatics (ICCCI)*, 2021, pp. 1-4, doi: 10.1109/ICCCI50826.2021.9402348.
19. Hari Pranav A;M. Senthilmurugan;Pradyumna Rahul K;R. Chinnaiyan , "IoT and Machine Learning based Peer to Peer Platform for Crop Growth and Disease Monitoring System using Blockchain," *2021 International Conference on Computer Communication and Informatics (ICCCI)*, 2021, pp. 1-5, doi: 10.1109/ICCCI50826.2021.9402435.