Research Article

Secure Cloud Medical Data Using Optimized Homomorphic Encryption

[1]S. Gnana Sophia, [2]Dr.K.K. Thanammal, [3]Dr.S.S. Sujatha

[1]MS University,
Research Scholar, Department of Computer Science and, S.T. Hindu College,
Abishakapatti, Tirunelveli-627012, Tamilnadu, India.
gnanasophiajournals@gmail.com
[2]MS University,
Associate Professor, Department of Computer Science and Applications, S.T. Hindu College,
Abishakapatti, Tirunelveli-627012, Tamilnadu, India.
[3]MS University,
Associate Professor, Department of Computer Science and Applications, S.T. Hindu College,
Abishakapatti, Tirunelveli-627012, Tamilnadu, India.

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 16 April 2021

Abstract: Protection of medical images on the virtual transmission platform is a simple and demanding activity, using multiple techniques to protect the digital file, such as cryptography, steganography and watermarking. This are the digital image protection approaches to meet security goals, i.e. confidentiality, trustworthiness, and usability. In this paper, the medical images are deposited in the cloud utilizing optimized homomorphic encryption. To increase the security level Rider Optimization Algorithm (ROA) is utilized to select the optimal key. Homomorphic encryption is a method of authentication which helps one to perform observes of the encrypted information through decrypting it. When the data is decrypted, the calculation consequence is stable, the same as if the procedures were conducted on the unprotected data. After completing the encrypted data, the encrypted images can be stored in the cloud and the decryption the same process is utilized to reconstruct the original images. For the experimental analysis, the performance of the proposed method is analyzed by the various parameters such as execution time, encryption time, and decryption time. The execution time of the proposed method is 2% decrease the HE existing method and 4% reduce the ECC algorithm.

Keywords*:* Homomorphic encryption, Rider Optimization Algorithm, Encrypted data and execution time.

1. Introduction

Patient privacy and protection continue to evolve with developments in computer analytics and information technologies as a leading concern for healthcare organizations [1]. This innovation is highly promising; they also pose crucial concerns of privacy, protection, and ethics, which can become major obstacles to the fulfillment of anticipated prospects and long-term progress if left unaddressed [2, 3]. Sometimes, in addition to Electronic Health Record (EHR) data, data researchers in most healthcare institutions are more involved in gathering and analyzing new forms and methods of under-leveraged data, such as mobile health, sensor networks, emails, and social media [4]. There has been no policy progress affecting various essential privacy concerns that have emerged from a largely different paper-based medical record structure to a different, digitalized, and interconnected environment [5, 6]. Along, these changes lead to a state where new privacy and safety threats are encountered by patients' medical record results. Cloud computing is a very modern concept and is going to have a huge effect on our lives. Through this application, computer services and equipment can be reached anytime and wherever [7]. The healthcare sector is rapidly changing, and it is predicted that the future healthcare paradigm will be information-centric. To navigate transition and uncertainty, the industry will profit from cloud technologies [8]. This promising technology will help promote cooperation between multiple healthcare providers, teamwork, and coordination.

The cloud will help provide better efficiency for the dollar for the healthcare sector. It can deliver connectivity and technologies that are fast, modular, scalable, and cost-effective [9]. Computer protection is a growing computer science field that specializes on the security of computer technology and knowledge regarding unauthorized access, hardware hacking, data misuse, and general threats such as backdoors, denial-of-service (DoS) attacks, and phishing [10, 11]. Protecting critical data and device resources is the purpose of implementing information security initiatives preserving an operating system requires protecting the network infrastructure of a computer system, while data protection is more concerned with defending data collected or exchanged within computer systems and cloud applications [12, 13]. Diversely, privacy is measured one of the key safety goals; it implements convinced laws with

standards that control the degree to which data on persons can be viewed, obtained [14, 15]. Instead of data protection, data ownership is more linked to data privacy. When using information technology, privacy may be asserted as a moral right for people and organizations, although data protection is not in itself a moral right [16].

In recent years many encryption algorithms have been utilized to encrypt the data and store the data in cloud. Here, we are utilized to optimized homomorphic algorithm has been utilized to encrypt and store the data in cloud. The optimal keys are generated by using rider optimization algorithm. It is used to select the keys are optimally by the encrypted process [17]. The rest of the paper, section 2 explains the various existing method and the technique, section 3 represents the proposed methodology, section 4 provides the result section and section 5 explains the conclusion part.

2. Literature review

A lot of researchers are analyzed to secure the medical data in cloud is given below, Blanquer, I., et al, [18] analyzed stable cloud medical data in 2020. It holds memory and disk vital data authenticated, that can only be obtained within trustworthy equipment extension-protected distributed systems. Inside these conditions, data were anonymized and transmitted anonymously to external sites hosting accelerator computers, retaining the same storage space and decreasing potential problems even in encrypted backends.

Marwan, M., et al, [19] developed a stable cloud health care approach using deep learning in 2018. Usually, to more easily distinguish image pixels, they utilize SVM and FCM. In addition, to increasing the possibility of possible leakage of medical knowledge, they integrate a further stage, the CloudSec module, into the traditional two-layered structure. The findings of the experiment show that using SVM was an important concept for continuous classification of images and data security.

In 2019, Pirbhulal, S., et al, [20] studied the security of medical data for wearable medical data. ECG signals from 40 stable participants, including the laboratory atmosphere and the i-e-physio net freely accessible database, were used. The observational findings demonstrate that less time duration with power usage (0.0068ms and 0.196 micro Joule/Byte) than Alarm net (0.0128ms and 0.351 micro Joule/Byte) and BSN-care (0.0175ms and 0.53 micro Joule/Byte) were required in the system. In addition, the experiments also demonstrate that the biometric data transmission framework not only provides accidental with identical keys, but also offers a trade-off between protection and utilization of resources.

Bhargavi, U., et al, [21] indicated the protection of health big data photos utilizing decoy approaches in 2019. The implementation of the decoy methodology to providing EHRs with protection was suggested in this article. The danger of malicious threats and foreign interference rests with the EHRs. This work addresses internal attacks and manages them. It also contains studies on honey-pots and methods of malware detection. The risk of an attack was further detected and the operator is alerted. The specifics of intrusions have also been logged.

In 2017, a protection framework for medical information in a health cloud was created by Al Hamid, H. A., et al, [22]. In this article, a fog processing system has been used to protect confidential healthcare data in the cloud. To this end, on the basis of bilinear pairing authentication, a tri-party one-round encrypted key agreement protocol has been developed that can produce a session key among the respondents and connect efficiently between them. Finally, by the introduction of a decoy methodology, confidential biomedical data was processed and protected safely.

HAN, S., et al, [23] also established cloud encryption and privacy protection for big data in 2019. To secure the contact channel and distributed data from malicious access this paper recommends an SSGK. A group key was required to protect the distributed data and a hidden distribution mechanism was used to transmit the group key in SSGK, unlike previous works. Comprehensive scalability and reliability evaluations reveal that their protocol significantly eliminates the protection and confidentiality risks of cloud storage data sharing and saves nearly 12 percent of storage space.

3. Proposed methodology

This section describes the medical images are stored in the cloud using optimized homomorphic encryption. Here, the medical images are encrypted using homomorphic encryption. For the encryption process the keys are optimally selected using rider optimization algorithm. After the encrypted image, the image can be stored in the cloud. After that the decryption, the same process is used. The overall diagram of the proposed method is given below,

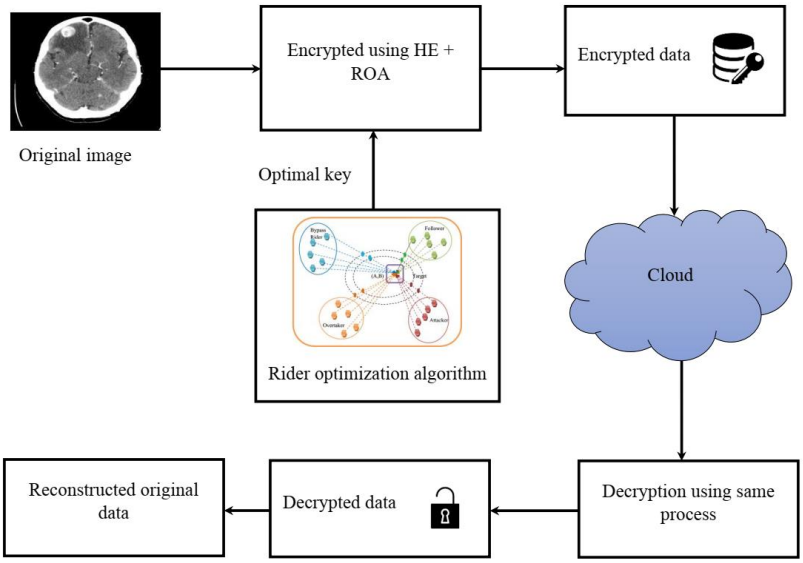


Figure 1: Overall diagram of the proposed method

3.1 Homomorphic encryption

Homomorphic encryption plays an extra role to authenticate the data or image, and is referred to as a public key cryptosystem. This mechanism has four operations that optionally decrypt the assessment algorithm details, which are a key generation, encryption, evaluation, and decryption; it produces an equivalent result if we have performed the process on the first messages. In applications segregated from multiple variables used to choose the encryption plot, the plan's decision is subject to the kind of operations being performed.

3.1.1 Key generation

A system for authentication and encryption keys and the corresponding image using a symmetric key; protection is provided for both privacy and reliability. A private key and a public key linked to it; an asymmetric key (public-key) algorithm uses a key match. The main recognition algorithm currently proceeds to choose the additional variables to document the public key (H_{PK}) and private Key (H_{SK}).

$$K = cd \text{ and } \omega = lcm(r-1, s-1) \quad (1)$$

Initialize arbitrary encryption and decryption keys for this operation, using ROA technique to customize this key and have the rest of the device's image protection styles with the ideal private and public key.

3.2 Rider optimization algorithm

A party of runners, as well as the bypass rider, follower, over taker, and assailant, are the inspiration for ROA. All riders in the ROA should follow the predefined approach, which can be summarized as follows:

With the leading direction, the bypass rider can meet the objective: The group rider's initialization can be sated as follows:

$$Y_t = \{Y_t(i,j)\}, \qquad 1 \le i \le R; 1 \le j \le Q \quad (2)$$

Where R represents the riders' total. The dimension of the optimization question is denoted by Q. t reflects instant time. At time t, Y_t reflects the location of i^{th} rider. It notes that the rider for the bypass rider in the following case and the position can be calculated as described:

$$Y_{t+1}^{B}(i,j) = \delta[Y_t(\eta,j) * \beta(j) + Y_t(\xi,j) * \lfloor 1 - \beta(j) \rfloor] \quad (3)$$

If δ represents the random numbers in $\lfloor 0,1 \rfloor$, η represents the irregular quantity in η, ξ represents a quantity that can be picked since 1 to R. Furthermore, β is the irregular number of $\lfloor 0,1 \rfloor$ per dimension, but with size $1 \times Q$.

By tracking the bypass rider, the follower reaches at the target: For bypass rider, the location of follower is important, the key explanation for this is that the follower's walk path depending on the bypass rider. The location of the follower can then be modified utilizing formula (4),

$$Y_{t+1}^{F}(i,k) = Y^{L}(L,K) + \left\lfloor cos\left(T_{i,k}^{t}\right) * Y^{L}(L,K) * d_i^t \right\rfloor \quad (4)$$

Where k denotes the chooser of the coordinates and Y^L represents the pass rider index. In the k^{th} coordinate, $T_{i,k}^{t}$ represents the steering angle of the i^{th} rider and d d_i^t represents the i^{th} rider's path to be travelled.

Not only does the over taker pursue his own location, but the data is obtained rendering to the bypass rider as well: The location of the over taker depends on three variables, including the selector of the coordinates, the comparative

success rate and the predictor of position. The primary reason being that the bypass rider and his own documents must be collected by the over taker. Consequently, the location of the over taker can be changed by formulas (5),

$$Y_{t+1}^{O}(i,k) = Y_t(i,k) + \lfloor D_t^I(i) * Y^L(L,K) \rfloor \quad (5)$$

Where $Y_t(i,k)$ denotes the location of the i[th] rider in the k[th] coordinate, and $D_t^I(i)$ represents the route pointer of i[th] rider. The direction indicator can be determined as follows:

$$D_t^I(i) = \left[\frac{2}{1-log(S_t^R(i))}\right] - 1 \quad (6)$$

Where $S_t^R(i)$ denotes the i[th] rider's success rate.

The attacker utilizes the optimum speed for the destination position to be achieved: The attacker's aim is to gain the leader's location, and the travel technique is close to the followers. Importantly, in this technique all the location of the attackers is changed, rather than the chosen person. The attacker's location can be set as follows,

$$Y_{t+1}^{A}(i,j) = Y^L(L,j) + \left[cos\left(T_{i,j}^t\right) * Y^L(L,j) * d_i^t\right] \quad (7)$$

Where $Y^L(L,j)$ denotes the leader's location. $T_{i,j}^t$ represents the steering angle of the i[th] rider in the j[th] coordinate.

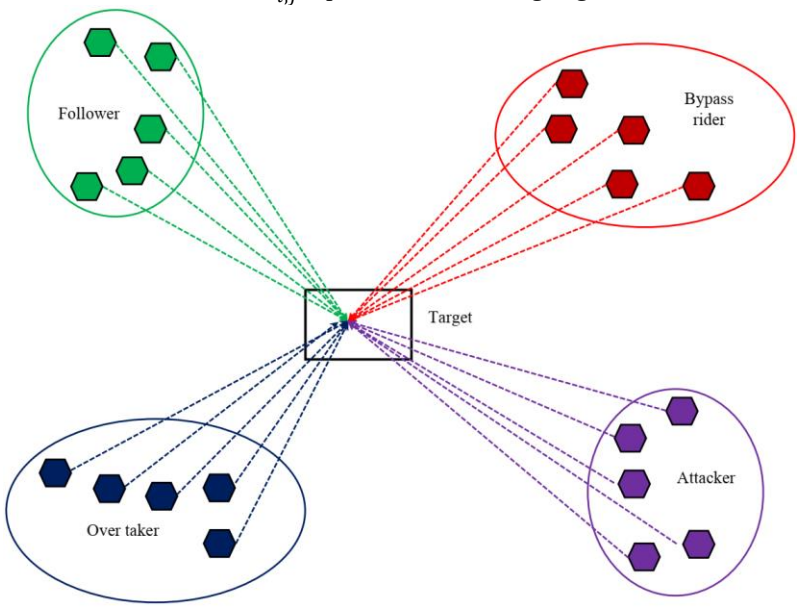


Figure 2: Structure of ROA

The authentication method for the hidden image of the first image is currently functional. The ideal public key would encode each pixel of a picture in the encryption analysis process. Calculating the figure telling cipher data operation may be described as message bit m. Use the H_{SK} client secret key to encode the original I_P image and create $H_{k-opt}(I_p)$ and K_{pt} will give this I_c cipher image to the server along with the public key. $H_{pk} = (k,i)$ and $K_{sk} = (c,d)$ $Enc(I, H_{sk})$ for indicate random variable r and z_k^*, compute cipher data $c = I.r^k mod k^2$.

For completing the encryption process, the encrypted images are stored in the cloud. After the retrieval process the same process is used to decrypt the data. and finally, the reconstructed image can be obtained. The decryption process of homomorphic encryption is given below,

3.3 Decryption

Check the image cipher consisting of the encoded pixel addressed by (c,d) and the key vector S in the decoding method. Through the use of two veils, in specific the hidden mask $< as >$ and also the goggles, the decoding procedure is used in a gradual improvement. To decipher the ciphertext and other secret parameters for the message bit (pixel estimate) m. The client using its K will decode the produced $dec(f(H_{sk-opt}))$ and it receives the first result.

$$Dec\ Image = \frac{L(C^a mod k_{opt}{}^2)}{L(i^a mod k_{opt}{}^2)} mod\ k \quad (8)$$

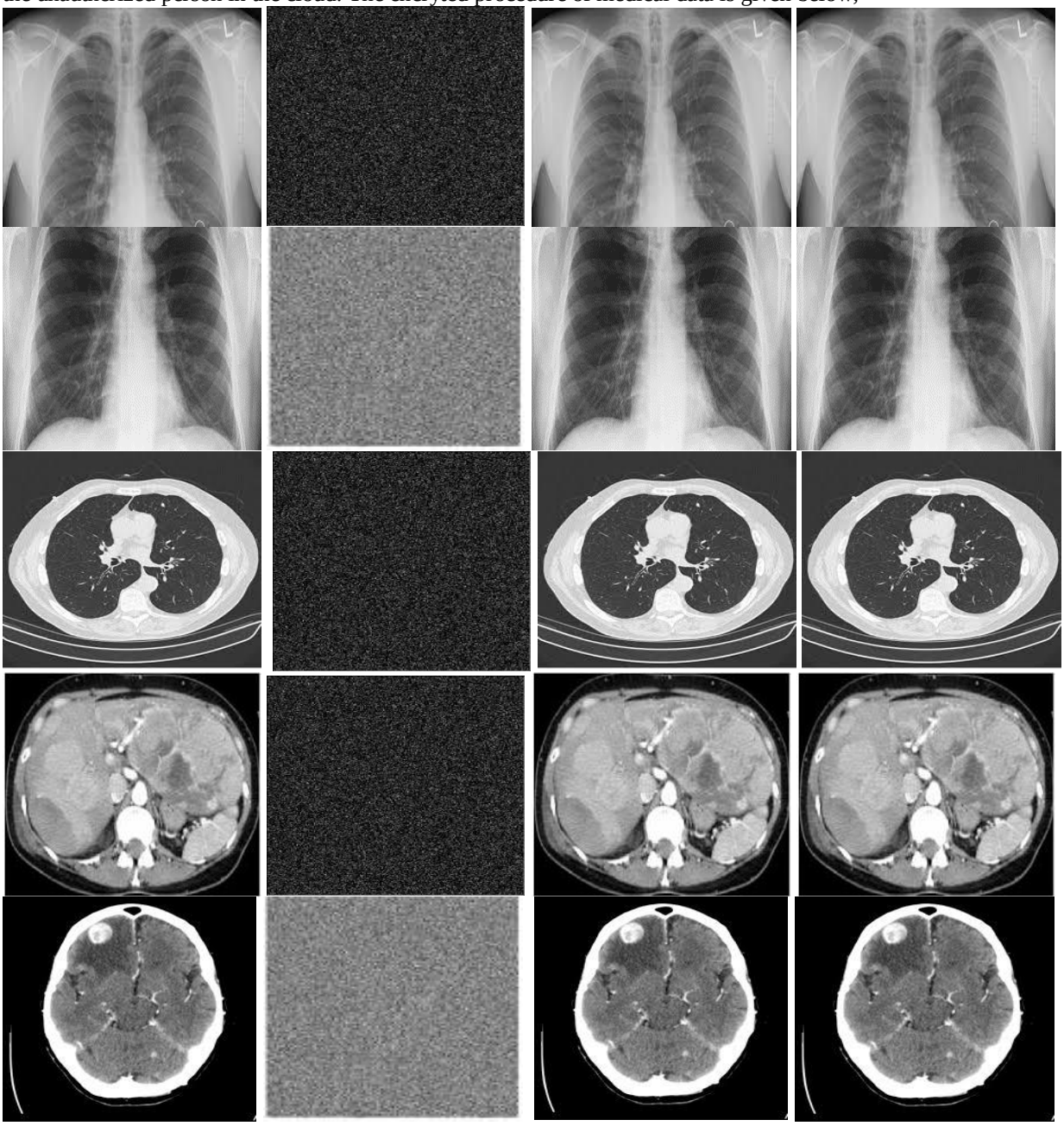
4. Result and discussion

Image safety shows that optimized Homomorphic encryption (HE) was implemented with an i5 processor and 4 GB RAM using MATLAB 2016a with optimized pointer HE. Three regular organs (liver, brain, lungs) of assessing the potential are considered in the simulator. Homomorphic encryption can process ciphertext data directly, essentially guaranteeing cloud consumer data protection. HE is used to encrypting medical data to secure storage purposes. The

expected information hiding graph is evaluated by safety control techniques, such as execution time, encryption time and decryption. This section addressed the ramifications of the suggested and current strategies to encrypted images.

4.1 Experimental analysis

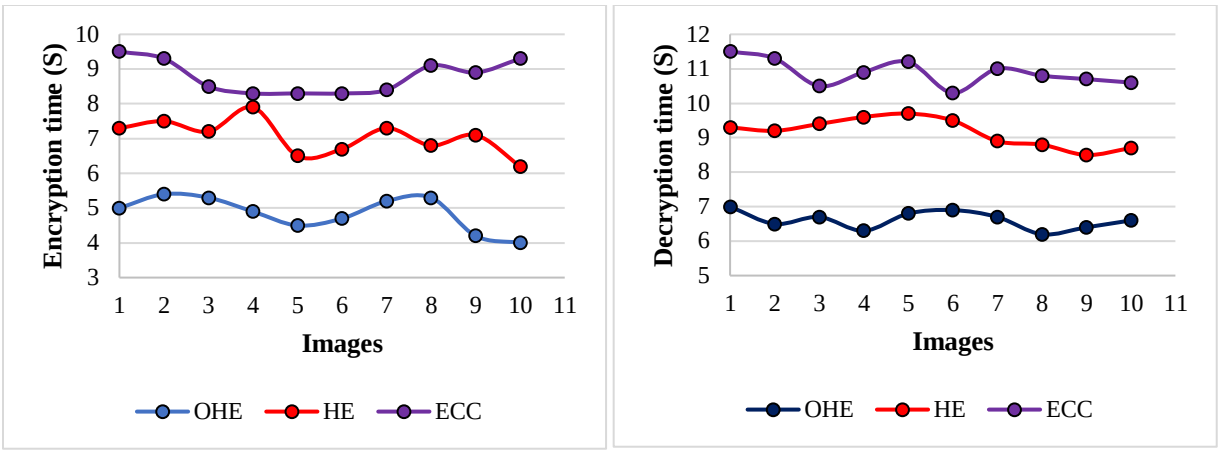
The medical images can be stored in the cloud for encrypt the data and it is useful to access the user, it does not access the unautherized person in the cloud. The encryted procedure of medical data is given below,



(a) (b) (c) (d)

Figure 3: Experimental analysis of the proposed method (a) Input, (b) Encrypted image, (c) Decrypted image and (d) Reconstructed output image

Figure (3) represents the experimental analysis of the proposed method. here the input medical images are encrypted by using optimized homomorphic encryption. In this encrypted image are used to secure the input data. In the encrypted data can be store in the cloud and the unauthorized person doesn't access the cloud. For the decryption, the same process is used and the reconstructed output is given. The homomorphic encryption that also can encode the original image to either the encrypted image is shown in this image.



(a) (b)

Figure 4: Comparative analysis of the proposed method (a) Encryption time and (b) Decryption time

The figure (4), represents the comparative analysis of encryption time, and decryption time of the proposed method against the existing method such as homomorphic encryption and elliptical curve cryptography. The encryption time of the suggested method is seen in figure (a). The method of encryption or converting information when it is moved to cloud storage is cloud authentication. Organizations of cloud storage encrypt data and transfer the user's encryption keys. When required, these keys are utilized to securely decrypt data. The approach suggested for the encryption time is to decrease the HE by 2 percent and the ECC algorithm by 4%.

In figure (b) represents the decryption time of the proposed method against the existing method. Decryption transforms the concealed data back into readable data. Decryption is considered the translation of authenticated information into its original form. It is basically an operation of reversed encryption. This decodes, the encoded data such that only an authenticated user may decrypt the information and a hidden key is used throughout the decryption. The system suggested is easier for the decryption process than the current method.

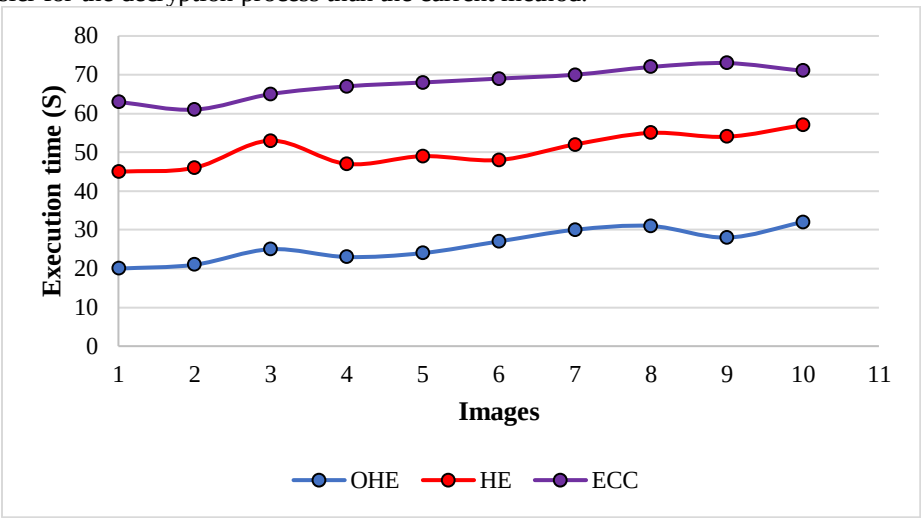


Figure 5: Comparative analysis of execution time

The comparative study of the suggested system against the current method by the time of implementation is seen in figure (5). Here, when considering the current method, the implementation time of the new method is minimized. The implementation time of the suggested approach is 3% decreased by the HE algorithm and 7% by the ECC algorithm.

5. Conclusion

In this article, we showed a functioning architecture of a web service using homomorphic encryption for conducting confidential intelligent detection activities on protected health info. Although processing just authenticated info, the web host allows forecasts, knowing little about the sensitive patient data sent. For the encryption, optimized homomorphic encryption algorithm is utilized to encrypt the data and it can be stored in cloud. For the experimental analysis, the encryption time is 20% reduced by the HE and 35% decreased the ECC algorithms.

Reference

1. Marwan, M., Kartit, A. and Ouahmane, H., 2018. A framework to secure medical image storage in cloud computing environment. Journal of Electronic Commerce in Organizations (JECO), 16(1), pp.1-16.
2. Lakshmi, V.S. and Deepthi, P.P., 2019. An efficient scheme for secure domain medical image fusion over cloud. Multimedia Tools and Applications, 78(15), pp.20609-20636.
3. Marwan, M., Kartit, A. and Ouahmane, H., 2016, May. A secure framework for medical image storage based on multi-cloud. In 2016 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech) (pp. 88-94). IEEE.
4. Marwan, M., Kartit, A. and Ouahmane, H., 2016. Secure cloud-based medical image storage using secret share scheme. In 2016 5th International Conference on Multimedia Computing and Systems (ICMCS) (pp. 366-371). IEEE.
5. Marwan, M., AlShahwan, F., Sifou, F., Kartit, A. and Ouahmane, H., 2019. Improving the Security of Cloud-based Medical Image Storage. Engineering Letters, 27(1).
6. Malayil, M.V. and Vedhanayagam, M., 2021. A novel image scaling based reversible watermarking scheme for secure medical image transmission. ISA transactions, 108, pp.269-281.
7. Lakshmi, C., Thenmozhi, K., Rayappan, J.B.B., Rajagopalan, S., Amirtharajan, R. and Chidambaram, N., 2020. Neural-assisted image-dependent encryption scheme for medical image cloud storage. Neural Computing and Applications, pp.1-14.
8. Vincent, J., Pan, W. and Coatrieux, G., 2016, March. Privacy protection and security in ehealth cloud platform for medical image sharing. In 2016 2nd International Conference on Advanced Technologies for Signal and Image Processing (ATSIP) (pp. 93-96). IEEE.
9. Lounis, A., Hadjidj, A., Bouabdallah, A. and Challal, Y., 2016. Healing on the cloud: Secure cloud architecture for medical wireless sensor networks. Future Generation Computer Systems, 55, pp.266-277.
10. Raja, S.P., 2019. Joint medical image compression–encryption in the cloud using multiscale transform-based image compression encoding techniques. Sādhanā, 44(2), p.28.
11. Das, I., Halder, A. and Roy, S., 2016. Secure Medical Image Sharing and Storing (Image Encryption and Hiding) in Cloud Environment.
12. Selvi, J.H.A. and Rajendran, T., A Review on Secured mode of Medical Image Storage in Cloud.
13. Rajendran, S. and Doraipandian, M., 2021. Chaos Based Secure Medical Image Transmission Model for IoT-Powered Healthcare Systems. In IOP Conference Series: Materials Science and Engineering (Vol. 1022, No. 1, p. 012106). IOP Publishing.
14. Huang, X. and Du, X., 2013, June. Efficiently secure data privacy on hybrid cloud. In 2013 IEEE International Conference on Communications (ICC) (pp. 1936-1940). IEEE.
15. Marwan, M., Kartit, A. and Ouahmane, H., 2017, May. A Novel Approach for Security in Cloud-Based Medical Image Storage Using Segmentation. In International Symposium on Ubiquitous Networking (pp. 247-258). Springer, Cham.
16. Li, C.T., Lee, C.C., Wang, C.C., Yang, T.H. and Chen, S.J., 2015, November. Design flaws in a secure medical data exchange protocol based on cloud environments. In International Conference on Algorithms and Architectures for Parallel Processing (pp. 435-444). Springer, Cham.
17. Usha, G., Vinoth, N.S., Veena, Nancy, M. and Evangeline, D., 2020, November. A secure cloud based image processing technique. In AIP Conference Proceedings (Vol. 2277, No. 1, p. 130004). AIP Publishing LLC.
18. Blanquer, I., Brasileiro, F., Brito, A., Calatrava, A., Carvalho, A., Fetzer, C., … Silva, F. (2020). Federated and secure cloud services for building medical image classifiers on an intercontinental infrastructure. Future Generation Computer Systems.
19. Marwan, M., Kartit, A., & Ouahmane, H. (2018). Security Enhancement in Healthcare Cloud using Machine Learning. Procedia Computer Science, 127, 388–397.
20. Pirbhulal, S., Samuel, O. W., Wu, W., Sangaiah, A. K., & Li, G. (2019). A joint resource-aware and medical data security framework for wearable healthcare systems. Future Generation Computer Systems.
21. Bhargavi, U., Gundibail, S., Manjunath, K., & Renuka, A. (2019). Security of Medical Big Data Images using Decoy Technique. 2019 International Conference on Automation, Computational and Technology Management (ICACTM).
22. Al Hamid, H. A., Rahman, S. M. M., Hossain, M. S., Almogren, A., & Alamri, A. (2017). A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility with Pairing-Based Cryptography. IEEE Access, 5, 22313–22328.
23. HAN, S., HAN, K., & ZHANG., S. (2019). A Data Sharing Protocol to Minimize Security and Privacy Risks of Cloud Storage in Big Data Era. IEEE Access, 1–1.