International Journal of Current Bio-Medical Engineering (IJCBE)
Volume 1, Issue 1, September – October (2023)

RESEARCH ARTICLE

SECURE STORAGE OF LUNG BRAIN MULTI-MODAL MEDICAL IMAGES USING DNA HOMOMORPHIC ENCRYPTION

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

[1,2,3]Department of Computer Science and Application, St. Hindu College, Nagercoil, 629002, India.

*Corresponding e-mail: gnanasophiajournals@gmail.com

Abstract – Protecting the medical data on the online platform for transmitting data is a simple and demanding task. In the modern world, various methods are used to safeguard the digital image such as cryptography, watermarking, and steganography. These methods are used for protecting digital images in order to achieve security objectives such as confidentiality, reliability, and usefulness. In the proposed method, the medical images are encrypted and stored in cloud using DNA Homomorphic Encryption (DNA-HE) algorithm. The key is generated using Rider Optimization Technique to ensure security. It acts as double encryption technique. Homomorphic encryption is an authentication approach that allows one to perform observations on encrypted data by decrypting it. In DNA Homomorphic Encryption algorithm, the input data will be a DNA sequence. The same procedure is used to decrypt the encrypted data. Performance of the proposed technique is evaluated using a number of factors, including execution, encryption, and decryption times.

Keywords: *DNA Homomorphic algorithm, Rider Optimization algorithm, Encrypting medical images, Decryption.*

1. INTRODUCTION

With advancements in computer analytics and information technology, patient privacy and protection continue to expand as a top priority for healthcare organizations. [1]. One of the most valuable and sensitive forms of data in information systems are medical photographs. In the current trends in cloud computing for patient care, this is a demanding and necessary requirement [3]. The transmission of medical pictures via the internet necessitates the adoption of a strong encryption method that can withstand cryptographic intrusions [2]. Data analysts at most healthcare institutions are sometimes increasingly active in obtaining and examining latest kinds and techniques of under-influenced data, like sensor networks, mobile health, social media, and emails in addition to EHR data [4].

The study of secure communication methods, or cryptography, limits who may read a message's contents to the sender and the intended receiver. When transmitting information virtually, cryptography is used to encrypt and decrypt email and other plain-text messages. Cryptographic procedures are employed to maintain data confidentiality and integrity. Depending on the security criteria and risks involved, several cryptographic systems can be used during data transmission and storage.

As a result of developments in communication, patients' medical record results are now subjected to increased privacy and security risks. Cloud computing is a relatively new concept that will have a significant impact on our lives [1]. Cloud computing is a method of computing that allows cloud users to share resources. Given the large number of individuals and organizations who utilize cloud services, it is critical to guarantee security as well as quick data transfer and sharing. As a result, cloud computing confronts two major difficulties: storage and security [16]. The goal of executing information security efforts is to protect important data and device resources. The protection of data is mainly concerned with safeguarding collected data or shared within cloud applications and computer systems, whereas maintaining an operating system requires securing a computer system's network architecture [1].

The first challenge is developing trust in remote deployment. A cloud is a distributed computing model in which a user's actions are carried out on a remote server in a data center. A client must guarantee that the base framework performs the cloud request on the client's own machine while ensuring consistency and secrecy in a cloud environment. To encode the data and save the encoded data in the cloud, a variety of encryption algorithms were applied. Here we are using DNA Homomorphic Encryption technique to encrypt medical images. Rider optimization algorithm is used for key generation.

Consider developing effective strategies for rigorous knowledge validation and procedure in order to meet the following goals in terms of ensuring cloud data security and trustworthiness under the previously described demanding design: (1) Storage accuracy: to guarantee that users' data is deposited and preserved in the cloud in a timely and accurate manner. (2) Rapid information error localization: locate the faulty server as rapidly as possible until an information eruption is noticed. (3) Dynamic metadata provision: to maintain a consistent level of cloud data consistency confirmation, even if clients change, add to, or remove documents. Our technique enables an external auditor to review users' outsourced information on the cloud without knowing the specifics of the data stored. The approach used here, unlike current approaches, enables for flexible and efficient public auditing of Cloud Computing.

The remaining portions of this paper are organized as follows. The article gives a quick overview of the relevant work in Section II. The proposed technique is presented in Section III. Section IV's detailed presentation of the experiment's findings shows how effective the proposed strategy is. The last section of the essay is Section V.

2. RELATED WORK

The Homomorphic encryption (HE) technique has been used in several research papers for efficient cloud computing with medical data protection have been discussed below.

In 2020, Elmahdi, E., et al [5] suggested an enhanced AOMDV approach to make data flow in MANETs reliable and safe when hostile nodes are present by distributing the components of the full information into separate channels and utilizing a HE mechanism for cryptographic process. According to the simulation results, the system has a greater throughput and packet distribution ratio which are both desired characteristics for emergency applications on MANETs.

Ullah et al [6] introduced a novel kernel homomorphic encryption technique in 2019. After the number of noises was exceeded, the entire negotiating system failed. The rate of advancement for processing, errors, and noises in the electronic world and cloud computing was accelerating daily. To decrease the growth of sounds and computation, they incorporate a revolutionary kernel HE method. The Ker-HE strategy was utilized to reduce the quantity of sounds by employing kernel and kernel homomorphism. These operations were used to reduce the length of the ciphertext during decryption and to clean up any errors or noise.

In 2017, Zhang et al [7] have presented a general technique based on the HE Scheme for developing a reliable cloud storage system. They were the first to look at the connection between HE schemes and secure cloud storage, and they provide G-SCS, a generic approach to build a Secure Cloud Storage protocol that can be used with any HE Scheme (HES). The proposed G-SCS approach found stable over a concept that meets cloud storage security requirements.

Cheon, J.H., et al [8] presented FHE over integers based on CRT in 2015. This paper discusses the third approach, which is based on the Chinese Remainder Theorem and can be constructed homomorphically. It was discovered that one particular plaintext/ciphertext combination may defeat this approach. They will address this issue by employing a more effective strategy to introduce an error into a message before encryption. They show that the strategy is completely homomorphic and resistant to chosen-plaintext threats under the approximate GCD presumption and the sparse subset sum assumption, providing a stable update to their original concept.

In 2019, Li, R., et al [9] suggested, FHE-based smart grid anomaly detection system for privacy protection. They presented a LUT method for analyzing any single-integer input variable in this study. At the time, integer encoding was more effective than bitwise encoding. The length of the evaluation was independent of the objective since they employed the LUT approach. This protocol also supported other structures that relied on FHE for a single input challenging function evaluation.

In 2020, Li, et al [10], presented new security concepts. extended IND-CPA protection to incorporate the passive protection requirements for (homomorphic) approximation encryption algorithms. The requirement for suitable authentication notions for approximation encryption illustrates the necessity of concurrently examining correctness and security, two essential characteristics of cryptographic systems.

Velliangiri S., et al [11] proposed an analysis of dimensionality reduction techniques for effective computing in 2019. They look at feature extraction techniques like EMD and PCA, as well as feature filtering techniques like correlation, LDA, and forward selection, to see how efficient and accurate they are. Their ideas were widely employed in DNNs for improving recognition accuracy and diagnosing medical images.

In 2019, Williamson, R. C., et al [12], proposed Dimensionality reduction as a link between extensive neural recordings and extensive network systems. They assist in the development of network models, which will be used to predict future studies. Single-neuron and paired spike train statistics were previously used to connect neuronal data with network models. To depict the multi-dimensional structure of neuronal population functioning, their study has started to integrate neuronal recordings with network models. Working memory, decision-making, muscle coordination, and a number of other topics have all been studied using this method.

In 2016, Wu, Z., et al [13] proposed that Cloud computing will be used to develop a new parallel and distributed paradigm for huge hyperspectral image analysis. They use dimensionality reduction as an example of how cloud computing systems may be used to execute distributed parallel hyperspectral data processing and accelerate hyperspectral data computations.

In 2017, Kim, et al [14] introduced a new HE-based stable KNN query processing method. They also developed an encrypted index method that performs data filtering without revealing data access patterns in order to achieve high query system speed. According to a study, the method surpasses the present system in terms of query processing costs while preserving user privacy.

In 2016, Wang, Xiaofen [15] proposed a one-round meeting position calculation protocol in which the location service provider interacts with a semi-trusted cloud server that serves as a computing hub and does most of the computations. The computer hub, the meet decision server, and the users all worked together to keep the user location safe from outside and inside threats. In order to examine the protocol's effectiveness, they employ smart phones to assess its mathematical efficiency. The outcomes of the simulation and a comparison of their protocol to one with comparable features show that it is a more efficient and realistic approach.

Different algorithms have been discussed in various papers. In this paper, we present a DNA Homomorphic Encryption for secure storing of medical data to store the medical data in a secure manner.

3. PORPOSED MODELLING

This section describes DNA Homomorphic Encryption technique, where the medical images are saved in the cloud. Here, the medical images are converted to binary form. A DNA strand is created from the binary data. The keys are created using the Rider Optimization Algorithm (ROA) and the DNA sequences are encrypted using homomorphic encryption. After encryption, the encrypted image can be securely stored in cloud. The same process is used for decryption. The block diagram for the DNA Homomorphic encryption method is represented in Fig:1.

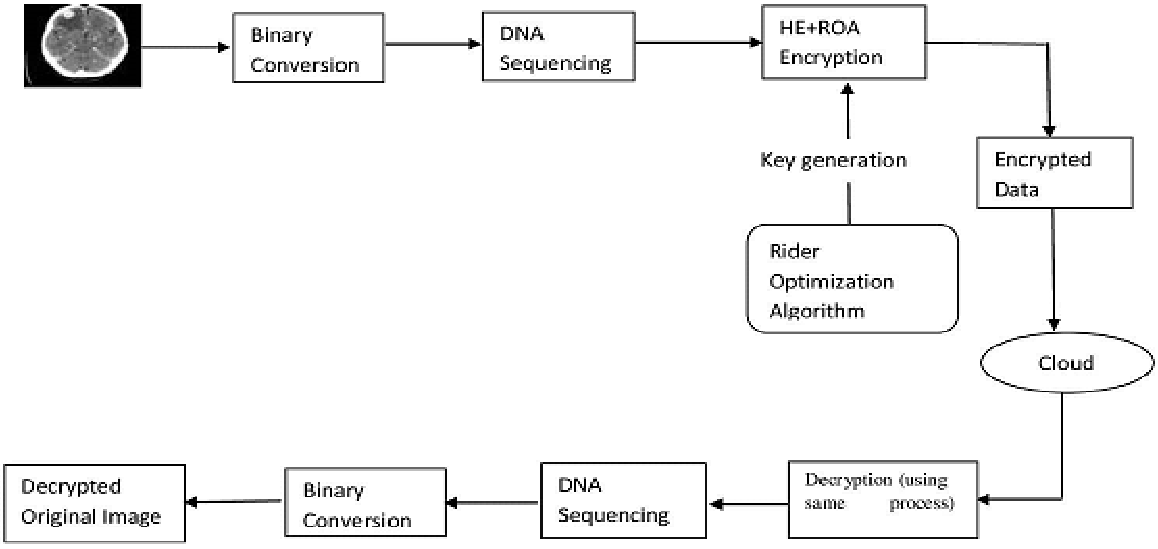


Figure 1. Overall image of the DNA-HE algorithm

3.1 DNA sequencing

Before the image is mapped to a DNA sequence, it must be converted into binary form. Binary digits, often termed as bits, store either 0 or1, attempting to make them the smallest storage units. Adenine(A), guanine(G), cytosine(C), and thymine(T) are the four nitrogenous bases of DNA. Use of the four nucleotides in sequence is the most significant aspect of the DNA-based data masking process. A DNA sequence can be made up of any combination of these nucleotides. When DNA is sequenced, the order of bases can be determined, and they may be represented by single letter in plain sequence format.

Table 1. Binary values for DNA Bases

DNA	BINARY VALUES
A	00
G	01
C	10
T	11

In the above table, the binary values for the DNA bases have been given.

3.2 DNA Homomorphic Encryption

Homomorphic encryption is a form of enciphering technique which permits users to compute on encrypted information without having to decrypt it first. The term "homomorphic" comes from the Greek word "homomorphosis," which means "identical structure”. The same mathematical operations on encrypted or decrypted data get the same results because the structure of the data in a homomorphic encryption scheme retains its structure. Homomorphic encryption, unlike other safe computing systems, uses arithmetic functions that focus on addition and multiplication rather than Boolean functions, and only requires a few rounds of interactions. The four operations of this mechanism are key generation, encryption, evaluation, and decryption, which can optionally decrypt the assessment algorithm details. In DNA-HE method the input will be given in the form of DNA sequences.

3.2.1 Key generation

Key generation is the process of creating cryptographic keys. A key is used to encrypt and decode data. A tool or programme that generates keys is known as a keygen. A symmetric key is used to secure both privacy and reliability in a system for encryption keys and authentication and the corresponding image. The primary recognition algorithm has been considering which extra variables can be used to document the public and private keys.

$$Key = ab \ \ and \ \omega = lcm(u-1, v-1) \qquad (1)$$

Apply the ROA technique to configure arbitrary encryption and decryption keys for this procedure, then use the optimal private and public key for the remainder of the device's image protection schemes.

3.3 Rider Optimization Algorithm

Riders compete to reach a predetermined destination, which motivates the Rider Optimization Algorithm (ROA). The steps are as follows:

The method is initially started using four groups of riders represented by the letter X, with position initializations done in any order. The group's initiation is determined by

$$M_k = \{M_k(x,y)\} \qquad 1 \leq x \leq S; 1 \leq y \leq T \qquad (2)$$

Here S represents count of riders and $M_K(x,y)$ represent the position of x^{th} rider in y^{th} size at k^{th} time immediately. The number of riders is calculated by adding the number of cyclists in each group and is represented as,

$$S \ = \ R + F + O + K + B \qquad (3)$$

Here R represents bypass rider, F represents follower, O represents overtaker, K represents attacker and B represents rag bull rider. $R + F + O + K + B \ = \ {}^{S}/_{5}$ (4)

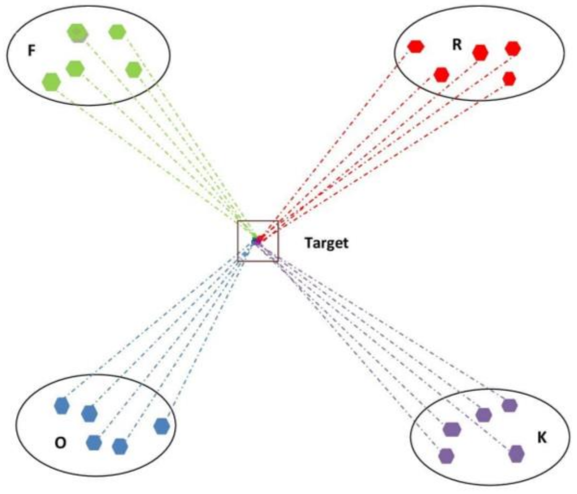


Figure 2. Structure of Rider optimization Algorithm

Following the initialization of rider group settings, each rider's success rate is analyzed. The success rate is computed by multiplying the distance between the rider and the destination by the success rate,

$$Success \ Rate \ = \frac{1}{\|M_x - k_i\|} \qquad (5)$$

Each rider's position in each group is updated in order to establish who is in the lead and who will win. As a result, the rider uses the features of each rider stated in the specification to update the position. The update position of each rider is expressed below

$$M_{k+1}^{v} \, (x,j) \ = M^H(H,j) + \left\lfloor cos\left(\varphi_{x,j}^{k} * M^H(H,j) * \partial_x^k\right)\right\rfloor (6)$$

Here j represents coordinate selector, M^H represents leading rider position, H represents leader’s index, $\varphi_{x,j}^{k}$ represents the angle of steering considering x^{th} rider in j^{th} coordinate and ∂_x^k represents the distance.

$$M_{k+1}^{j}(x,j) = M_k(x,j) + [I_k^*(x) * M^H(H,j)] \qquad (7)$$

Here $I_k^*(x)$ denotes direction indicator. The attacker aims to become the leader by following the leader's update procedure, which is defined as follows:

$$M_{k+1}^{\alpha}(x,\rho) \ = M^H(H,\rho) \ + \ [cos \, \varphi_{x,e}^{k} \ * \ M^H(H,\rho)] \ + \partial_x^k \qquad (8)$$

The standard bypass rider is described as, and the update rule for bypass riders is shown here

$$M_{k+1}^{c} \ = \ \lambda \, [M_k(Z,T) \ * \ \delta(\rho) \ + \ M_k(\in,\rho \,) \ * [1 - \delta(\rho)] \qquad (9)$$

Here $\lambda \ r$represents random number, Z represents random number between 1 to T, ∈ represents random number which ranges between 1 to T and δ represents random number varies between 0 to 1.

Success Rate Calculation

When the updating method is completed, the rate of success for each rider is determined.

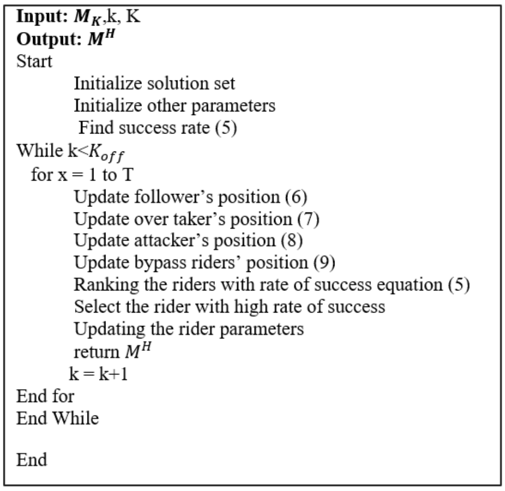
Rider Parameter Updating process

To find an appropriate solution, the update parameter for the rider is essential**.**

Off Time of Rider

For developing an appropriate solution, the parameter of rider's update is crucial.

Algorithm for Rider optimization Algorithm



```
Input: $M_K$,k, K
Output: $M^H$
Start
        Initialize solution set
        Initialize other parameters
         Find success rate (5)
While k<$K_{off}$
  for x = 1 to T
        Update follower’s position (6)
        Update over taker’s position (7)
        Update attacker’s position (8)
        Update bypass riders’ position (9)
        Ranking the riders with rate of success equation (5)
        Select the rider with high rate of success
        Updating the rider parameters
        return $M^H$
       k = k+1
End for
End While

End
```

The images that are encrypted can be saved in the cloud to complete the encryption process. The data is decrypted using the same procedure that was used to retrieve it. Atlast, the rebuilt image can be received. The decryption process for DNA-HE method is given below.

3.4 Decryption

Data that has been rendered unreadable by encryption can be restored to its original, unencrypted condition through the process of decryption. In the process of decryption, the system gathers and converts the jumbled data into text and graphics that can be understood by both the reader and the system. Both human and automated methods are available for decryption. A combination of keys or passwords can also be used.

$$Decrypted\ image\ = \frac{X(A^{\alpha} mod\ Key_{opt}^{2})}{X(X^{\alpha} mod\ key\ _{opt}^{2})}\ mod\ key \quad (10)$$

4. RESULTS AND DISCUSSIONS

This section discussed about the execution of DNA-HE (DNA Homomorphic Encryption Technique). DNA-HE can directly process ciphertext data, effectively ensuring cloud customer data security. DNA-HE is used to encrypt medical data for safe storage. This section explored the consequences of the suggested and current approaches for encrypted photographs.

4.1 Performance analysis

The medical images are saved in cloud in encrypted form in order to provide security. Accessing the medical images for the user is very simple on the other hand unauthorized users cannot be able to access the medical image. The procedure for encryption of medical images is shown in fig:3.

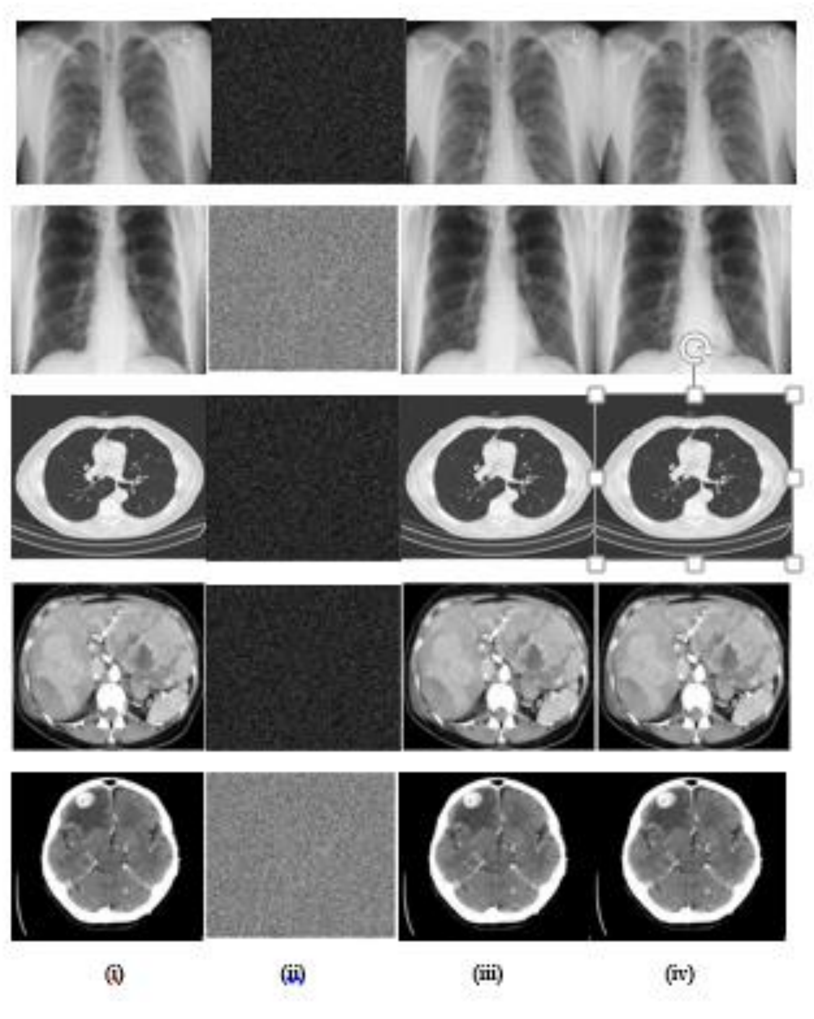


Figure 3. Performance analysis for DNA-HE (i) Original image (ii)Image after encryption (iii)Image after decryption (iv) Rebuilt Original image

The above figure describes the performance analysis of the DNA-HE technique. Encryption is done to securely store the input medical data. The medical images are encrypted and stored in cloud and it can be accessed only by the user. Unauthorized user cannot able to access the images. For decryption, the same method is repeated again and the reconstructed original image will be given. The DNA homomorphic encryption can convert the images to encrypted image is shown above. First the medical images will be converted into binary format and then into DNA sequence, it will be given as input.

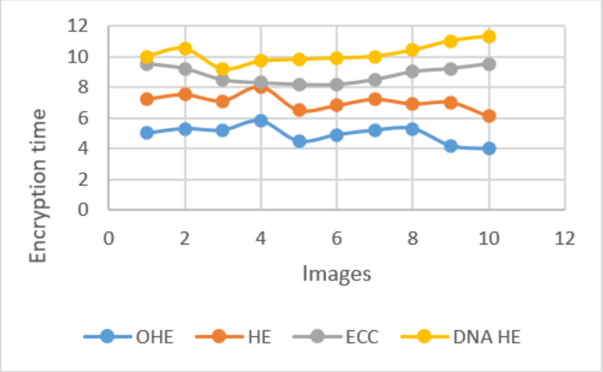


Figure 4. comparative analysis for encryption time

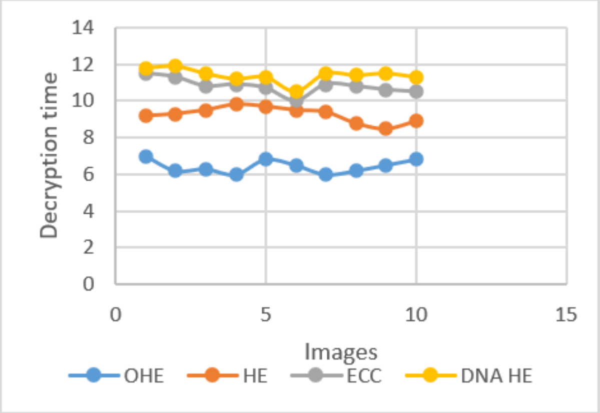


Figure 5. comparative analysis for decryption time

The figure (4) and (5) depicts a comparison of the proposed method's encryption and decryption times to known methods such as elliptical curve cryptography, homomorphic encryption and optimized homomorphic encryption. Figure 4 shows the encryption time of the recommended approach. Cloud authentication is a means of encrypting or transforming data as it is transported to cloud storage. Cloud Service provider companies encode data and transmit the encryption keys to the user. For decrypting the data, these keys are required. For the encryption time, it is advised that the HE algorithm be reduced by 2% and the ECC algorithm by 4%.

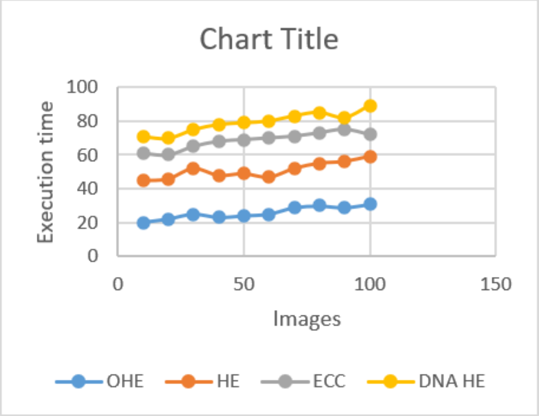


Figure 6. comparative analysis of execution time

Figure 6 shows a comparison of the proposed system to the current method at the time of implementation. When compared to the existing method, the new method's implementation time is reduced. The DNA-HE algorithm reduces the implementation time of the recommended technique by 3%, while the ECC algorithm reduces it by 7%.

5. CONCLUSION

In this research, we propose a realistic web service architecture that uses DNA-HE to perform private detection utilizing knowledge operations on protected health information. The site host permits predictions despite just processing authorized data and understanding nothing about the highly confidential data provided. An efficient DNA homomorphic encryption technique is used to encrypt and store the data on the cloud. According to the trial's findings, the OHE algorithm reduced encryption time by 10%, the HE methods by 20%, and the ECC algorithms by 35%.

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

Not applicable

ACKNOWLEDGEMENTS

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.

REFERENCES

[1] S.G. Sophia, "Secure Cloud Medical Data Using Optimized Homomorphic Encryption", *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. *12*, no. 7, pp. 2702-2708, 2021. [Cross Ref] [Google Scholar] [Publisher Link]

[2] V. Pavithra, and C. Jeyamala, "A survey on the techniques of medical image encryption", In *2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, IEEE, pp. 1-8, 2018. [Cross Ref] [Google Scholar] [Publisher Link]

[3] S. Muthusundari, M.A. Berlin, R. Sasikumar, B. Alekhya, K. Mohanasundaram, and P. Prashant, "Transmitting data in a secure way using double protection encryption scheme", *Materials Today: Proceedings*. 2020. [Cross Ref] [Google Scholar] [Publisher Link]

[4] M. Marwan, A. Kartit, and H. Ouahmane, "Secure cloud-based medical image storage using secret share scheme," In *2016 5th International Conference on Multimedia Computing and Systems (ICMCS)* IEEE, pp. 366-371, 2016. [Cross Ref] [Google Scholar] [Publisher Link]

[5] E. Elmahdi, S.M. Yoo, and K. Sharshembiev, "Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks", *Journal of Information Security and Applications*, vol. *51*, p.102425, 2020. [Cross Ref] [Google Scholar] [Publisher Link]

[6] S. Ullah, X.Y. Li, M.T. Hussain, and Z. Lan, "Kernel homomorphic encryption protocol", *Journal of Information Security and Applications*, vol. *48*, p.102366, 2019. [Cross Ref] [Google Scholar] [Publisher Link]

[7] J. Zhang, Y. Yang, Y. Chen, J. Chen, and Q. Zhang, "A general framework to design secure cloud storage protocol using homomorphic encryption scheme", *Computer*

Networks, vol. *129*, pp.37-50, 2017. [Cross Ref] [Google Scholar] [Publisher Link]

[8] J.H. Cheon, J. Kim, M.S. Lee, and A. Yun, "CRT-based fully homomorphic encryption over the integers", *Information Sciences*, vol. *310*, pp.149-162, 2015. [Cross Ref] [Google Scholar] [Publisher Link]

[9] R. Li, Y. Ishimaki, and H. Yamana, "Fully homomorphic encryption with table lookup for privacy-preserving smart grid", In *2019 IEEE International Conference on Smart Computing (SMARTCOMP)* IEEE. pp. 19-24, 2019. [Cross Ref] [Google Scholar] [Publisher Link]

[10] J. Li, J. Wu, G. Jiang, and T. Srikanthan, "Blockchain-based public auditing for big data in cloud storage", *Information Processing & Management*, vol. *57*, no. 6, p.102382, 2020. [Cross Ref] [Google Scholar] [Publisher Link]

[11] S. Velliangiri, and S. Alagumuthukrishnan, "A review of dimensionality reduction techniques for efficient computation", *Procedia Computer Science*, vol. *165*, pp.104-111, 2019. [Cross Ref] [Google Scholar] [Publisher Link]

[12] R.C. Williamson, B. Doiron, M.A. Smith, and M.Y. Byron, "Bridging large-scale neuronal recordings and large-scale network models using dimensionality reduction", *Current opinion in neurobiology*, vol. *55*, pp.40-47, 2019. [Cross Ref] [Google Scholar] [Publisher Link]

[13] Z. Wu, Y. Li, A. Plaza, J. Li, F. Xiao, and Z. Wei, "Parallel and distributed dimensionality reduction of hyperspectral data on cloud computing architectures", *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. *9*, no. 6, pp.2270-2278, 2016. [Cross Ref] [Google Scholar] [Publisher Link]

[14] H.I. Kim, H.J. Kim, and J.W. Chang, "A secure kNN query processing algorithm using homomorphic encryption on outsourced database", *Data & knowledge engineering*, vol. *123*, p.101602, 2019. [Cross Ref] [Google Scholar] [Publisher Link]

[15] X. Wang, "One-round secure fair meeting location determination based on homomorphic encryption", *Information Sciences*, vol. *372*, pp.758-772, 2016. [Cross Ref] [Google Scholar] [Publisher Link]

[16] S.P. Raja, "Joint medical image compression–encryption in the cloud using multiscale transform-based image compression encoding techniques", *Sādhanā*, vol. *44*, no.2. p.28, 2019. [Cross Ref] [Google Scholar] [Publisher Link]

AUTHORS

S. Gnana Sophia is an Assistant professor of the Computer Applications Department at Scott Christian College, Nagercoil, Tamilnadu, India. She has received her Bachelor's degree in Computer Science from Women's Christian College, Nagercoil and a Master's degree in Computer Science from Srimati Indira Gandhi College Trichy, Tamilnadu. She has several years of work experience in the field of teaching and have arranged/organized many conferences, seminars, workshops and various other events. She has published many refereed journal articles/conference papers. Her research interest includes Cloud-based Encryption Technologies.

K. K. Thanammal received the M.Sc (Computer Science) Degree from Bharathidasan University, Tiruchirappalli in 1992, M.Phil (Computer Science) Degree from Manonmaniam Sundaranar University, Tirunelveli in 1999, M.Tech (Computer Science) Degree from Vinayaka Mission University, Salem in 2007 and Ph.D. (Computer Science) Degree from Manonmaniam Sundaranar University, Tirunelveli in 2015. She is working as Associate Professor in the Computer Science Department at S.T.Hindu College, Nagercoil since 1993. She has 27 years of teaching experience. She has published seven papers in journals and presented in seven National and International Conferences. Her current research interest focuses on Image Processing, Neural Networks, Medical imaging, and Cloud based Encryption Technologies.

S. S. Sujatha completed her MCA degree in Alagappa University, Karaikudi in 1993, M.Phil (Computer Science) Degree from Manonmaniam Sundaranar University, Tirunelveli in 2003, She completed her doctorate degree at Mother Teresa University, in 2014. She is working as Associate Professor in the Computer Science Department at S.T.Hindu College, Nagercoil since 1994. She has published eighteen papers in journals and presented in three International Conferences. Her current research interest focuses on Image Processing, Data Mining, Cloud Computing and Cloud based Encryption Technologies

Arrived: 04.07.2023
Accepted: 17.09.2023