International Journal of System Design and Computing
Volume 02, Issue 01, January – June (2024)

RESEARCH ARTICLE

DOUBLE SECURE CLOUD MEDICAL DATA USING EUCLIDEAN DISTANCE-BASED OKAMOTO UCHIYAMA HOMOMORPHIC ENCRYPTION

M. Anisha[1, *] and V. Adlin Beenu [2]

[1] Department of Computer Science and Engineering from Satyam College of Engineering and Technology, Aralvaimozhi, Anna University, India.
[2] Department of Computer Science and Engineering, Arunachala college of Engineering for Women, Manavilai, Anna University Chennai, India.

[*]*Corresponding e-mail: aninisha519@gmail.com*

Abstract – Electronic Medical Records (EMRs) are computerized copies of paper records used in healthcare settings. Data from these systems allows doctors to quickly access and manage patients' medical records at healthcare institutions. Medical data security safeguards patients' rights and the duties of healthcare workers. Sharing such medical records with another medical organization is challenging for them. Cloud computing (CC) is the most effective way for storing this sort of data and addressing these issues. In this research a novel DOuble SEcure MEDical Cloud data (DOSE MED) technique has been proposed that enhances privacy and security of medical data. The proposed DOSE MED method consists of three stages namely, registration phase, encryption phase and storage/decision phase. The proposed method utilizes Okamoto Uchiyama's homomorphic encryption technique to add prediction capability on the cloud which paves the way for disease prediction by medical practitioners. Euclidean distance-based classifier has been used for predicting data without decrypting it. The security findings demonstrate that the proposed DOSE MED provides selective security for the chosen keyword assaults. Performance analysis and real-world simulation trials demonstrate that this system is both efficient and practicable.

Keywords *– Okamoto Uchiyama homomorphic encryption, Electronic Medical Records, Cloud computing.*

1. INTRODUCTION

"Cloud computing" refers to the supply of numerous internet services such as networking, processing power, and storage [1]. This approach improves scalability, flexibility, and cost-efficiency by enabling users to access and store data and programs on remote servers rather than local hardware [2]. The main cloud service providers are Google Cloud Platform, Microsoft Azure, and Amazon Web Services (AWS). CC supports diverse applications from web hosting to big data analytics and machine learning [3,4].

Cloud computing in Electronic Medical Records (EMRs) enhances the storage, accessibility, and security of patient data [5]. It allows healthcare providers to access and update patient records in real-time from any location, improving collaboration and patient care. Cloud-based EMRs also offer scalable storage solutions and robust etc. [6]. Additionally, they enable compliance with regulations through advanced security measures and encryption. This technology supports telemedicine, facilitating remote consultations and continuous patient monitoring [7].

Security of medical data is crucial to protect sensitive patient data from breaches and unauthorized access [8]. This includes robust encryption, safe access restrictions, and frequent audits to assure data integrity and confidentiality. Compliance with standards such as HIPAA (Health Insurance Portability and Accountability Act) is critical, which requires special precautions for EHRs [9,10]. Additionally, educating healthcare staff on best security practices and using advanced threat detection systems can mitigate risks and enhance overall data security. The major contribution of the work has been followed by

- The proposed DOSE MED method consists of three stages namely, registration phase, Encryption phase, and storage/decision phase.
- In the registration phase, the patient and medical centre must have to register their identity with the network administrator to receive the medical EHR.
- In the Encryption phase, the medical centre generates an encrypted medical data by using DNA combined with Okamoto Uchiyama and stores in cloud storage.
- In the Storage/decision phase the encrypted medical health records from Medical Centre, will be

computed without being decrypted and takes decision about prediction based on Euclidean distance classifier.

The remaining portion of the work has been followed by, section 2 represents the literature review of the proposed, section 3 represents the proposed methodology, section 4 represents the introduction of the proposed, and section 5 represents the conclusion and future work of the proposed methodology.

2. LITERATURE SURVEY

The objective of the literature survey is to provide a concise overview as well as full information regarding current systems. The purpose of the literature survey is to thoroughly define the technical specifics associated with the primary project in a brief and straightforward way.

In 2023 Boomija, M.D. and Raja, S.K., [11] developed the Secure Partially Homomorphic Encryption (SPHE) algorithm to encrypt the data that is outsourced and to operate on the ciphertext by multiplying and dividing it. This technique is especially useful for computing on data that is outsourced and protecting patient electronic health records.

In 2023 Rahmani, P., et al., [12] developed a revolutionary technique for relational databases that combines data concealing and secret sharing to safeguard the confidentiality and secrecy of secret characteristics. One or more cover characteristics in a relation are embedded into one or more hidden attributes in the same relation. A set of shares columns is designed to seem to be connected with just the cover attributes.

In 2022 Pan, H., et al., [13] suggested an IoT medical data sharing program with cloud-chain collaboration and policy fusion. A dispute resolution and fusion technique that permits co-authorization of medical data by the patient and the physician is introduced in relation to asymmetric access control rights. Experiments proved that the suggested technique is feasible, and the security analysis indicated that it meets the requirements of secrecy and verifiability of the recovered information.

In 2022 Kartit, A., [14] proposed a new strategy for maintaining data secrecy, based on Hadoop MapReduce operations and a multi-agent system. Furthermore, to build intelligent distributed computing for effective management of Virtual Machine (VM) workloads, a method based on the Bat Algorithm (BA) was adopted.

In 2023 Alabdulatif, A., et al., [15] proposed a new cloud-based hybrid access control system for securing medical big data in healthcare enterprises. The study's findings indicate that the access control approach can resist the majority of assaults and serve as the cornerstone for further secure and safe medical big data solutions.

In 2022 Ramachandra, M.N., et al., [16] developed the use of the Triple Data Encryption Standard (TDES) approach to secure massive data in cloud environments. By making the Data Encryption Standard (DES) keys larger, the suggested TDES approach offers a comparatively easier solution to safeguard data privacy and prevent assaults. The outcomes of the trial demonstrated how well the suggested TDES approach secures and protects massive healthcare data on the cloud.

In 2022 Alluhaidan, A.S., [17] presented a unique method for guaranteeing storage and access safety using integrated transformed Paillier and KLEIN algorithms (ITPKLEIN-EHO), which leverages elephant herd optimizations (EHOs) to offer lightweight features. This proposed method's experiments on several EEG data sets for implementation are conducted using MATLAB.

3. PROPOSED METHODOLOGY

In this research a novel DOuble SEcure MEDical Cloud data (DOSE MED) technique has been proposed that enhances privacy and security of medical data.

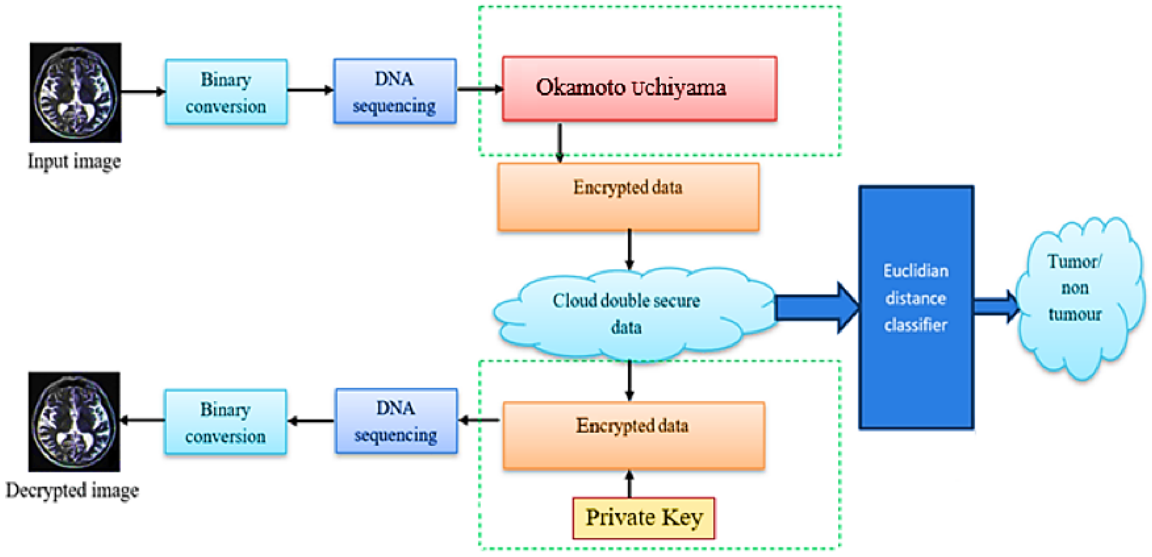

Figure 1. proposed methodology

The proposed DOSE MED method consists of three stages namely, registration phase, encryption phase and storage/decision phase. The proposed method utilizes Okamoto Uchiyama's homomorphic encryption technique to add prediction capability on the cloud which paves the way for disease prediction by medical practitioners. Euclidean distance-based classifier has been used for predicting data without decrypting it. The security findings demonstrate that the proposed DOSE MED provides selective security for the chosen keyword assaults.

The identity theft, will result in major financial troubles as well as a great deal of inconvenience in the life that can last for years. But it far worse in certain respects. If an identity thief tampers with the medical data, the file may contain inaccurate information about user's medical history and diagnosis. An OU algorithm is then used to encrypt the DNA sequences. After encryption, the encrypted image can be safely stored in the cloud. Using Euclidean distance classifier, the images can be compared for prediction.

The architecture of the proposed DOSE MED method is depicted in Figure 1. The suggested plan established a secure conduit for the provably safe storage of electronic medical records. To be more precise, the physician makes a diagnosis and creates a medical record after the patient registers on the hospital system. The medical facility must keep the records on file so that the patient may access his information at any time and the researcher can always find out specifics. Medical records must be encrypted before being saved as they include information pertaining to the patient's private. Here, the data are encrypted using DNA OU-HE server and then uploads it to the database for storage.

3.1. Binary Conversion

Binary conversion is the process of converting a number from the decimal (base-10) system to the binary (base-2) system. In binary, each digit represents a power of 2, starting from 2^0 on the right. For example, the decimal number 10 is converted to binary by determining the highest power of 2 less than or equal to 10, which is 8 (2^3). The next highest power of 2 is 2 (2^1), and then 0 (2^0). Therefore, 10 in decimal is represented as 1010 in binary. This method involves repeated division by 2 and recording the remainders.

3.2. DNA Sequencing Conversion

Deoxyribose Nucleic Acid is the abbreviation for DNA. DNA is a polymer made up of deoxyribonucleotides, which are monomers. Each nucleotide is made up of three fundamental components: deoxyribose sugar, phosphate group, and a nitrogenous base. Purines (Adenine and Guanine) and pyrimidines are the two forms of nitrogenous bases (Cytosine and Thymine). They are denoted by the letters A, G, C, and T. G connects to C, while A binds to T. The binary values for the DNA bases are displayed in Table 1. The order of bases may be ascertained by DNA sequencing, and in simple sequence format, they can be illustrated by a single letter.

Table 1. Binary values for DNA Bases

DNA	BINARY VALUES
A	00
G	01
C	10
T	11

DNA encryption is the technique of using a statistical approach to hide genetic information to increase genetic privacy in DNA sequencing operations. The goal is to figure out the approaches that are reliable and the role of legislation in assuring that the genetic privacy is protected indefinitely.

3.3. Okamoto Uchiyama [OU]

The OU cryptosystem was created in 1998 by Tatsuaki Okamoto and Shigenori Uchiyama. It is a public key cryptosystem. It makes use of (Z/nZ) *, the multiplicative group of integers modulo n. N applies the p2q evaluation, where p and q are big prime numbers.

3.3.1. OU Homomorphic Encryption [OU-HE]

HE is the procedure of encoding data into ciphertext that can be parsed and employed like the original ciphertext. OU Homomorphic encryption enables complex mathematical operations on encrypted data without needing decryption. OU claims that the OU cryptosystem satisfies the requirements for homomorphic encryption (HE) in this work. With HE, encrypted data may be computed without needing to be initially decrypted. Data owners that need to transmit data to the cloud for processing but do not trust the service provider with the unencrypted data frequently utilize HE. The data owner transmits the data to the server after encrypting it using a HE technique. Without first decrypting the data, the server then uses the encrypted data to carry out the required calculations and sends the encrypted results back to the data owner. Since the private key is unique to the data owner, only they are able to decipher the outcome. Figure 2 illustrates the example of the OU Homomorphic encryption.

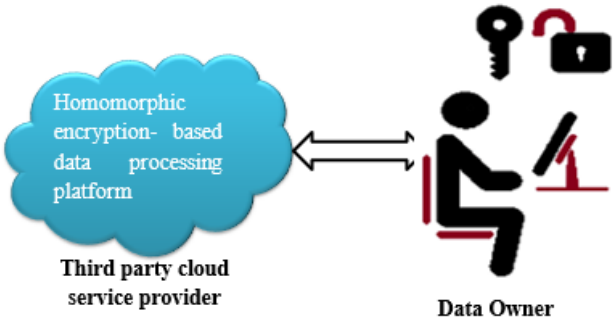

Figure 2. Homomorphic Encryption

3.3.2. OU Homomorphic Decryption

Decryption technology transforms encrypted code or data into a form that can be easily understood and read by humans or machines. This is basically called decrypting encrypted data. This happens on the receiving side. Messages can be decrypted using private or private keys. The diagram below clearly shows the decryption technique and the

ciphertext. H. The ciphertext is converted back to the original message.

3.4. Euclidean distance classifier

Euclidean distance is the most widely used point-to-distance measurement. Based on this distance metric, the classifier is straightforward and easy to use. The Euclidean distance rule uses the mean class values as class centers to compute pixel-center distances. This technique is superior for classifying a monogenous area at the main level. Its quick classification time is what makes it advantageous. Euclidean distance can be used as a basic similarity measure to compare pixel values between an image under consideration and a reference image (e.g., a healthy image). If the Euclidean distance is significantly different from a threshold, it might indicate the presence of a disease or anomaly. Since Euclidean distance yields superior results than other techniques of distance estimation, it is employed. Since the method does not make judgments based on the original data, it is nonparametric. The following formula can be utilized to evaluate the Euclidean distance (Figure 3).

$$D = \sqrt{(A_1 - YB_1)^2 + (A_2 - B_2)^2 + \cdots + (A_n - B_n)^2} \quad (1)$$

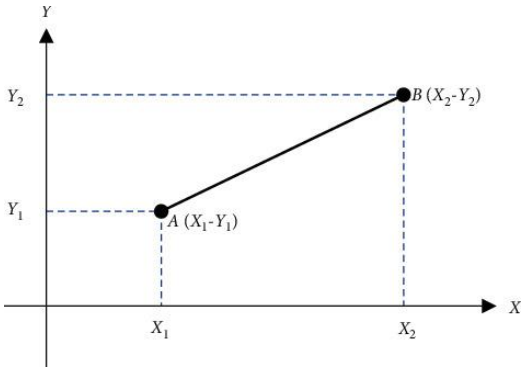

Figure 3. Calculation of Euclidean distance

Based on the difference in the pixel values the disease will be predicted by using the reference image that is encrypted and stored in the cloud.

4. RESULT AND DISCUSSION

The framework's assessment metrics specify the stakeholders, functions, and addressed problems to help meet privacy standards. This study's novel setup was developed using MATLAB 2019b, a deep learning toolkit.

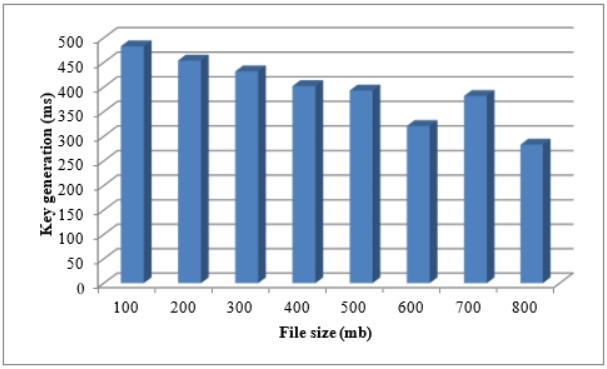

Figure 4. Performance analysis of key generation in DOSE MED

The graphical representation of the suggested technique for key generation is given in Figure 4. The recommended technique's key generation is compared to its file size. The file size of the suggested approach varies from 100 to 800 MB depending on the key generation. The recommended solution has a file size of 100 MB and generates keys in 487 milliseconds. The suggested technology generates keys in 323 milliseconds and has a file size of 600 megabytes. The key generation of the suggested methodology varies according on the file size of the proposed method.

Figure 5 depicts the suggested method's encryption time depending on encryption time. The proposed model encryption time is evaluated using data that can be encrypted with the encryption algorithm. The encryption time can be estimated using the proposed method's file size. The method's encryption time varies depending on the file size of the suggested method.

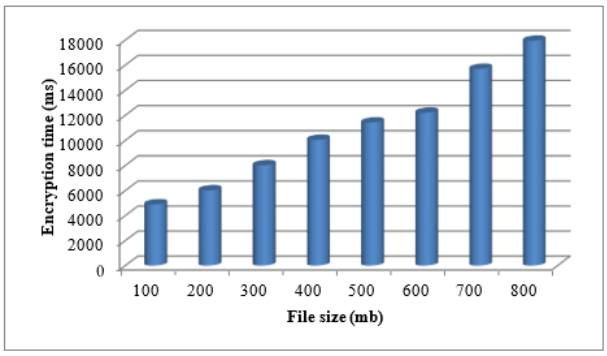

Figure 5. Performance analysis of encryption time in DOSE MED

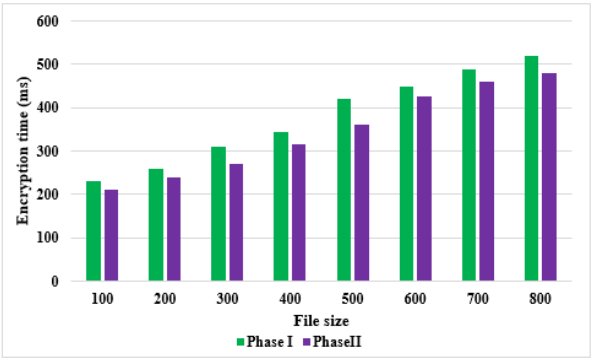

Figure 6. Encryption time comparison

A comparison of the proposed technique and the existing techniques is shown in Figure 6. The encryption time of the suggested DOSE MED technique is better than the existing method BACK method. This encryption time of the technique is based on the file size of the method which varies from 100 to 800 Mb. By comparing the proposed and the existing method, the proposed method is very much better than the existing method.

A comparison of the proposed technique and the existing techniques is shown in Figure 7. The encryption time of the suggested DOSE MED technique is better than the existing method BACK method. This encryption time of the technique is based on the file size of the method which varies from 100 to 800 Mb.

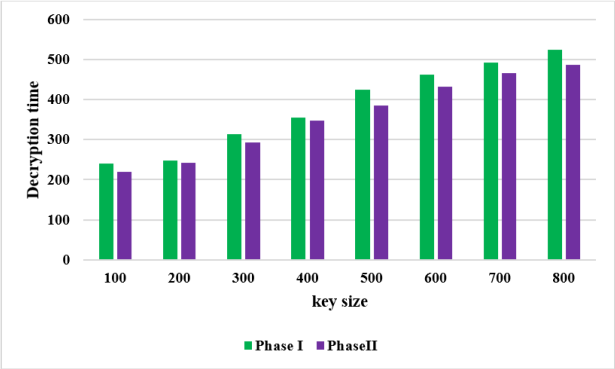

Figure 7. Decryption time comparison

5. CONCLUSION

In this paper a novel Double Secure medical Cloud data (DOSE MED) using DNA Okamoto Uchiyama homomorphic encryption technique has been proposed in this work. Through the use of OU-HE technology, the method offers effective access control for electronic medical records, preventing unauthorized individuals from viewing the patient's confidential information. In addition, the Euclidean distance classifier aids in data prediction, data originality and traceability, and the resolution of central authority security deficiencies. All of these factors were taken into consideration while utilizing the cloud storage platform to guarantee the safe storage of medical data. However, this scheme still has some shortcomings, such as the access privilege and require specialized storage infrastructure and may lead to increased storage costs, then the Error Rates of the data stored. The proposed secure data transmission scheme will be extended to work in an uncontrolled environment in future by focusing on enhancing the efficiency and security of DNA-based OU-HE methods. This includes developing more robust encryption algorithms that can handle larger medical images and reduce computation overhead.

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] G.R. Babu, P.V. Chintalapati, P.K. Sree, A. Pudi, and C.V. Ramana, "A Context Sensitive with Effective Task Migration in Mobile Cloud Computing Services", *In 2023 3rd International Conference on Computing and Information Technology (ICCIT)*, pp. 201-205, 2023. IEEE. [CrossRef] [Google Scholar] [Publisher Link]

[2] Y.C. Wang, J. Xue, C. Wei, and C.C.J. Kuo, "An overview on generative ai at scale with edge-cloud computing", *IEEE Open Journal of the Communications Society*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] R.R. Irshad, S. Hussain, I. Hussain, J.A. Nasir, A. Zeb, K.M. Alalayah, A.A. Alattab, A. Yousif, and I.M. Alwayle, "IoT-Enabled Secure and Scalable Cloud Architecture for Multi-User Systems: A Hybrid Post-Quantum Cryptographic and Blockchain based Approach Towards a Trustworthy Cloud Computing", *IEEE Access.* 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] S.S. Vellela, B.V. Reddy, K.K. Chaitanya, and M.V. Rao, "An integrated approach to improve e-healthcare system using dynamic cloud computing platform", *In 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, pp. 776-782, 2023. IEEE. [CrossRef] [Google Scholar] [Publisher Link]

[5] H.B. Mahajan, A.S. Rashid, A.A. Junnarkar, N. Uke, S.D. Deshpande, P.R. Futane, A. Alkhayyat, and B. Alhayani, "RETRACTED ARTICLE: Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems", *Applied Nanoscience*, vol. 13, no. 3, pp. 2329-2342, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] V. Chamola, A. Goyal, P. Sharma, V. Hassija, H.T.T. Binh, and V. Saxena, "Artificial intelligence-assisted blockchain-based framework for smart and secure EMR management", *Neural Computing and Applications*, vol. 35, no. 31, pp.22959-22969, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] G. Peng, A. Zhang, and X. Lin, "Patient-centric fine-grained access control for electronic medical record sharing with security via dual-blockchain", *IEEE Transactions on Network Science and Engineering*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] S. Bera, S. Prasad, and Y.S. Rao, "Verifiable and Boolean keyword searchable attribute-based signcryption for electronic medical record storage and retrieval in cloud computing environment", *The Journal of Supercomputing*, vol. 79, no. 18, pp.20324-20382, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] S. Fugkeaw, L. Wirz, and L. Hak, "Secure and Lightweight Blockchain-enabled Access Control for Fog-Assisted IoT Cloud based Electronic Medical Records Sharing", *IEEE Access*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] R. Akangbe, and T. Charles-Chinkata, "Dealing with Data Breaches on Patient's EMR Sensitive Data: A Comprehensive Approach," *Frontiers in Digital Health*, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] M.D. Boomija, and S.K. Raja, "Securing medical data by role-based user policy with partially homomorphic encryption in AWS cloud", *Soft Computing*, vol. 27, no. 1, 559-568, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] P. Rahmani, M. Taheri, and S.M. Fakhrahmad, "A novel secure data outsourcing scheme based on data hiding and secret sharing for relational databases", *IET Communications*, vol. 17, no. 7, pp. 775-789, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] H. Pan, Y. Zhang, X. Si, Z. Yao, and L. Zhao, "MDS 2-C 3 PF: A Medical Data Sharing Scheme with Cloud-Chain Cooperation and Policy Fusion in IoT", *Symmetry*, vol. 14, no. 12, pp. 2479, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] A. Kartit, "New Approach Based on Homomorphic Encryption to Secure Medical Images in Cloud Computing," *Trends in Sciences*, vol. 19, no. 9, pp. 3970-3970, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[15] A. Alabdulatif, N.N. Thilakarathne, and K. Kalinaki, "A Novel Cloud Enabled Access Control Model for Preserving the Security and Privacy of Medical Big Data", *Electronics*, vol. 12, no. 12, pp.2646, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[16] M.N. Ramachandra, M. Srinivasa Rao, W.C. Lai, B.D. Parameshachari, J. Ananda Babu, and K.L. Hemalatha, "An efficient and secure big data storage in cloud environment by using triple data encryption standard", *Big Data and Cognitive Computing*, vol. 6, no. 4, pp.101, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[17] A.S. Alluhaidan, "Secure Medical Data Model Using Integrated Transformed Paillier and KLEIN Algorithm Encryption Technique with Elephant Herd Optimization for Healthcare Applications", *Journal of Healthcare Engineering*, 2022. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

M. Anisha 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 for Women, Manavilai, Anna University, currently she is pursuing her ME degree in Computer Science and Engineering from Satyam College of Engineering and Technology, Aralvaimozhi, Anna University, India. Her interested research area is cloud computing, and Internet of Things, Image Processing.

V. Adlin Beenu She received her BE degree in computer science and engineering from Arunachala college of engineering for women, Manavilai, Anna University. She received her ME degree in computer science and engineering from Arunachala college of engineering for women, Manavilai, Anna University Chennai. Her interested research area is IOT, Data science, and image processing.

Arrived: 06.05.2024
Accepted: 02.06.2024