2024 International Conference on Recent Advances in Science & Engineering Technology (ICRASET)

Secured Homomorphic Encryption and Authentication for Healthcare

Swapnil Sharma
NITTE (Deemed to be University)
Department of ECE
N.M.A.M. Institute of Technology,
Nitte - 574110, India
swapnilsharma806@gmail.com

Uditaparna Sarmah
NITTE (Deemed to be University)
Department of ECE
N.M.A.M. Institute of Technology,
Nitte - 574110, India
uditaparnasarmah@gmail.com

Vineet M. Dodamani
NITTE (Deemed to be University)
Department of ECE
N.M.A.M. Institute of Technology,
Nitte - 574110, India
vineetmd01@gmail.com

Vikas Rai K.
NITTE (Deemed to be University)
Department of ECE
N.M.A.M. Institute of Technology,
Nitte - 574110, India
vikki9013@gmail.com

Ramachandra H. N.
NITTE (Deemed to be University)
Department of ECE
N.M.A.M. Institute of Technology,
Nitte - 574110, India
rcrao.udupi@gmail.com

K. S. Shivaprakasha
NITTE (Deemed to be University)
Department of ECE
N.M.A.M. Institute of Technology,
Nitte - 574110, India
shivaprakasha.ks@nitte.edu.in

***Abstract*— Secure communication and data processing is one of the vital requirements for applications like healthcare, feedback systems, voting etc. In the traditional cryptographic algorithms, the data is to be decrypted before processing. When the processing is carried at a third party, the privacy is compromised. Thus, such applications require a system where the data processing is done without actually knowing the data. Homomorphic Encryption (HE) is one such solution to this problem where, the encrypted data is processed at the third-party level without performing decryption. It provides secured data communication between sender(s) and receiver by preserving privacy. It not only assures privacy but also avoids multiple decryption operations to perform data processing. Nevertheless, one of the challenges in this system is to guarantee the authenticity of the data requester. This can be accomplished using authentication protocols over HE. This paper proposes an Authentication Protocol over a Partial Homomorphic Encryption (PHE) system for healthcare data. The patient data is processed at cloud in encryption domain and the results are sent to the data requester on proving one's authenticity. This ensures both privacy of the information and authenticity of the data requester.**

***Keywords*— Homomorphic Encryption, Paillier system, Partial Homomorphic Encryption Introduction**

I. INTRODUCTION

Homomorphic Encryption (HE) means the kind of encryption that supports calculations to be performed on the encrypted data without decryption. The conventional methods of data security such as encryption for storage and transmission expose the data to threat actors when the data need to be decrypted for processing. This pose a big problem especially in areas of specialty such as the health sector where issues to do with privacy and confidentiality are of major importance. The weakness that still persists with conventional encryption systems is that they cannot handle data securely during computation. To counter this problem, HE allows for computation on encrypted data. This capability is very useful for applications that deal with private data like healthcare system where data confidentiality is also very important. HE does not require the data to be decrypted for computation purposes hence ensuring that the data is secure even during computation. With this technology, it is possible to safely and effectively manage personal data with no violation of the data's security.

In this work, a design of secure system for healthcare applications employing HE technique is considered. Amongst the types of HE algorithms Partial Homomorphic Encryption (PHE) is becoming increasingly popular. PHE supports either addition or multiplication operation performed in encrypted domain. The proposed work uses one of the basic PHE algorithms, the Paillier encryption. Paillier supports additive homomorphism. Nevertheless, other operations can also be realized using masking process. A comparison of the Paillier system with the traditional RSA is also presented in the paper. Though RSA requires lesser computing time, homomorphic operations offered by Paillier make it more suitable for healthcare applications. Also, all other arithmetic operations can be realized through Paillier system using masking operation. Thus, for implementation Paillier algorithm is considered in this paper.

The rest of the paper is organized as follows: Section II provides an overview of related studies in area of HE. Section III presents the mathematical modelling of RSA and Paillier encryption techniques. Section IV provides the findings and discussion of this work where the RSA and Paillier are compared in detail. Lastly, Section V summarizes the results and the potential lines of research in the field.

II. RELATED WORK

Though HE scheme is becoming increasingly popular in the recent past, RSA can be regarded as the one of the earlier algorithms supporting, HE operations. RSA algorithm, introduced in 1978, enables secure communication using a public key for encryption and a private key for decryption. Its security is based on the difficulty of factoring large numbers, and it supports digital signatures. RSA remains crucial in modern cryptography [1].

Advanced Encryption Standard (AES) is highlighted for its speed and efficiency in securing large data, making it ideal for modern needs. DES, though historically significant, is vulnerable to attacks due to its small key length. RSA offers strong security but is slower than AES and DES. The study presented in [2] emphasizes choosing

979-8-3503-8860-2/24/$31.00 ©2024 IEEE

encryption methods based on specific security requirements. A new multi-signature scheme that offers faster, more efficient security with reduced costs and easy integration into existing systems was proposed in [3]. Public key cryptography, pioneered in the 1970s, transformed secure communication, enabling secure key exchanges and becoming vital for modern digital security [3]. Table I presents the comparison of various variants of RSA presented in the past literature.

TABLE I RSA ALGORITHM

Paper	HE Operations Supported	Application	Hard Problem Base
[2]	Multiplicative	Public Key Infrastructure	2^{bkc}
[3]	Multiplicative	Blockchain and Cryptocurrencies	DL-based, Multi-signature
[1]	Multiplicative	Secure Key Exchange	$C = M^e mod\, n$ $M = C^d mod\, n$

Paper [4] highlights the basic concepts of public key cryptography. The paper also gives an insight into HE in healthcare, emphasizing its ability to process encrypted data securely while protecting privacy.

HE allows operations on encrypted data, essential for secure cloud computing. It includes partial, somewhat, and fully homomorphic types, each with its own challenges. Recent advancements focus on improving efficiency and noise reduction [5]. Optimization of HE operations with GPU-accelerated Fast Fourier Transform was discussed in [6]. It improves Fully Homomorphic Encryption (FHE) performance for secure cloud computing, addressing computational overhead and integration complexity.

The article [7] introduces Privacy Preserving Disease Prediction (PPDP), a secure e-healthcare system that uses encrypted data and Single-Layer Perceptron learning, improving privacy, accuracy, and efficiency. The proposed framework uses contextual FHE to secure healthcare data in fog-assisted clouds, ensuring confidentiality and resisting attacks. This work builds on concepts from [5, 8].

A secure cloud computing algorithm is introduced, combining HE and multi-party computation to protect data confidentiality and integrity in untrusted cloud environments, enabling secure computations on encrypted data without decryption [9]. An optimized decryption algorithm for the Paillier cryptosystem is proposed, improving decryption speed and efficiency without compromising security, making it suitable for low-processing-power environments like mobile devices and embedded systems [10].

The study proposed in [11] examines HE and distributed ledger technology for securing Swiss health data, addressing legal and ethical challenges while ensuring compliance with data protection laws. The work proposed in [12] highlights securing Electronic Health Records (EHRs) in the cloud using the Paillier cryptosystem to encrypt patient images, ensuring data privacy and secure access for authorized healthcare professionals. A system using PHE is proposed to ensure data confidentiality in cloud computing. It allows operations on encrypted data without decryption, enhancing privacy and security, especially in sensitive fields like healthcare [13].

Paper [14] proposes a model where the cloud computing system uses homomorphic re-encryption for secure operations on encrypted data. It supports basic operations while preserving confidentiality. Security performances are validated through simulations. ReActHE is a deep neural network for privacy-preserving biomedical predictions using HE. It overcomes limitations in handling nonlinear functions, ensuring accurate and secure computations with better performance [15].

Linear Resilient Decisional Diffie-Hellman is a privacy-preserving scheme for online disease diagnosis using HE. It secures medical data and ensures efficient, private computations. Users maintain control over their sensitive health information [16]. Paper [17] reviews encryption techniques for protecting patient privacy in healthcare, focusing on IoT and wearable devices, and evaluates symmetric and asymmetric methods for secure data transmission and storage.

A privacy-preserving collaborative learning protocol for healthcare using cloud computing is proposed in [18]. It splits the deep learning model, outsourcing heavy computation to the cloud while keeping patient data secure.

Paper [19] introduces a secure genome analysis method using HE, comparing different HE schemes for different tasks. It builds on concepts from RSA and HE, as discussed in [10]. Compared to [19], which covers genome analysis, paper [20] focuses on improving quality scores and uses RSA concepts from [1, 3] for model selection. It also features advanced re-encryption techniques for enhanced data security.

Table II presents the summary of popular applications of HE and the HE operations supported in each of these methods.

Table III presents a gist of the application of HE in the healthcare domain.

TABLE II
POPULAR APPLICATIONS OF HOMOMORPHIC ENCRYPTION

Citation	HE Operations Supported	Type of HE	Applications
[16]	Additive, Multiplicative	PHE, FHE	Medical Data Processing, Secure Cloud Computing
[21]	Additive, Multiplicative	FHE	Tesla C2050 GTX 690
[10]	Additive, Multiplicative	FHE, PHE	Confidentiality of user data
[12]	Multiplicative	FHE	HER
[13]	Multiplicative	PHE, FHE	Storage of healthcare data
[17]	Additive, Multiplicative	PHE, FHE	Information Security, Mobile Healthcare
[15]	Additive, Multiplicative	FHE	Precise and privacy-preserving algorithm with a non-approximating HE scheme

TABLE III
HOMOMORPHIC ENCRYPTION IN HEALTHCARE

Citation	Area of Research	Methods Used
[22]	Heart disease prediction	Principal Component Algorithm
[7]	Multiple diseases	Single-Layer Perceptron (SLP) Learning Algorithm Data Encryption Using Random Matrices Threat Model and Security Analysis
[23]	Diabetes and Heart disease	Genomes dataset, GTEx, and ALSPAC
[24]	Heart disease and diabetes	Contextual Fully Homomorphic Encryption Techniques-based Privacy Preserving Framework (CFHET- PPF)
[25]	Heart disease	Cryptanalysis and homomorphic encryption
[19]	Cancer, Cardiovascular diseases	Convolutional Neural Network
[16]	Convolutional Neural Network	Electronic Health Records
[11]	Melanoma	Data discovery method

III. Methodology

A. Paillier Cryptosystem

Paillier cryptosystem was introduced in the year 1999. It supports additive homomorphism.

The mathematical modelling for this system is as follows:

Key Generation:
Select p and q, p and q both are prime, $p \neq q$

Calculate $N = p \times q$ (1)
Calculate $\lambda = LCM((p-1),(q-1))$ (2)

Select $g \epsilon Z_N$ such that

$$gcd\ \left[\left(\frac{g^{\lambda}\, mod\, N^2 - 1}{N}\right), N\right] = 1 \tag{3}$$

Select r such that $gcd\ (r, N) = 1$

Public Key : $PU = \{N, g\}$
Private Key : $PR = \{\lambda\}$

Encryption:
Plain text, $M < N$

$$\text{Cipher text, } C = g^M r^N\ mod\ N^2 \tag{4}$$

Decryption:
Cipher Text, C

$$\text{Plain Text, } M = \frac{L(C^{\lambda}\ mod\ N^2)}{L(g^{\lambda}\ mod\ N^2)}\ mod\ N \tag{5}$$

$$\text{Where, } L(u) = \frac{u-1}{N} \tag{6}$$

B. Masking

Masking and demasking are helpful for comparison operations in HE while maintaining data confidentiality. Masking is a process where encrypted data is masked with a random mask so that the values should not be predictable while performing the computation. Whereas, demasking unveils the mask once operations are effected thus allowing for the final output to be seen without compromising on the aspect of security. In the context of HE, this approach is very important especially when performing comparisons since that is where leakage of information on the encrypted values can occur. As the work includes masking and demasking, comparison operations can also be performed using the Paillier encryption that is vital operation needed on health records.

C. Compare Operation

The concept of masking and demasking are considered in the proposed system with intentions of comparing two encrypted integers. In particular, the data of COVID-19 is considered for analysis. A threshold for the blood oxygen level is set with an objective to determine the number of people with statistics deviating from a specified threshold value. This is especially helpful in reviewing patient data analytics like the oxygen level, or temperature in an attempt to notice those who are either extremely high or low.

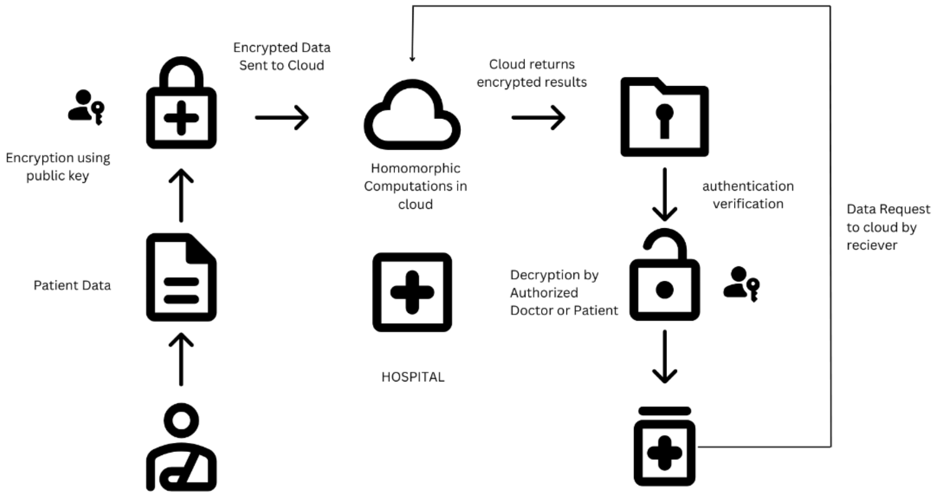
Encrypted Data Sent to Cloud
Cloud returns encrypted results
Encryption using public key
Homomorphic Computations in cloud
authentication verification
Data Request to cloud by reciever
Patient Data
Decryption by Authorized Doctor or Patient
HOSPITAL

Fig. 1. System model

D. Authentication

The system incorporates the use of passwords through the SHA-256 to authenticate users and ensure that they are genuine. The password set by the user is neither stored or transfer in plaintext form, rather a hashed form of the password is stored. After the user has entered his/her password, it is hashed again using the SHA-256 function and compared to the password stored in the database. If the two hashes are equal the user is considered to be authenticated.

In mathematical terms, this protocol is based on the properties of the SHA-256 hash function that generates a fixed string of 256 bits in length regardless of the input string size. To prevent brute force attacks the protocol makes use of the preimage resistance property of the SHA-256 hash function so that nobody can easily guess the original password from the hash. Moreover, SHA-256 is characterized by a high avalanche effect, which implies that a small change of data input leads to a significant alteration of data output, which increases protection.

E. System Model

The overall system model of the proposed work is presented in Figure 1.

Encryption of Patient Data and Transmission to the Cloud: In this phase, patient data is gathered and encrypted with the help of a public key for the safety of the data. The encrypted data is then transmitted to the cloud and to ensure that sensitive information is not exposed during the transmission.

Homomorphic operations in the cloud environment: After the data is encrypted, the encrypted data is sent to the cloud where homomorphic computations are made on the data. Such computations enable operations on the data without having to decrypt it. The cloud then analyses the data and passes back the result encrypted to ensure privacy is observed.

Data Requester, Authentication, and Decryption: The last phase is where the data requester which could be a doctor, hospital management or the patient request for the processed data from the cloud. Once the requester has been authenticated, he or she is given the encrypted results which has to be decrypted to access the information. This makes it possible for only the right people to access the information since it is classified.

IV. Results and Analysis

This section details the implementation of the proposed system.

Simulation environment is detailed as follows:

Tool: Python 3.12.1 (Spyder)

System Specification: Intel i5 Processor, 64 bit Windows 11 OS, 16GB RAM.

A. *Comparison of RSA Algorithm and Paillier Encryption in terms of time*

The performance comparison of RSA with Paillier system was carried out in terms of computational time required for key generation, encryption, decryption and processing operations. Figure 2 presents the plot of Encryption time required in RSA and Paillier systems as a function of Key size.

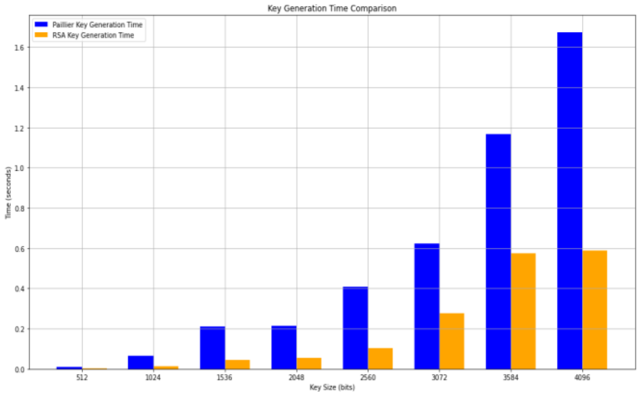

Fig. 2. Key generation time for RSA and Paillier system

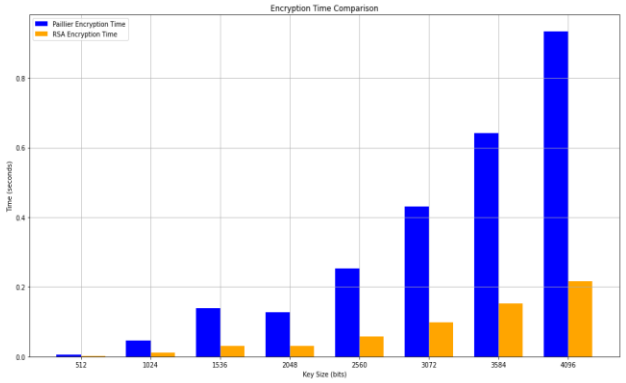

Fig. 3. Encryption time for RSA and Paillier system

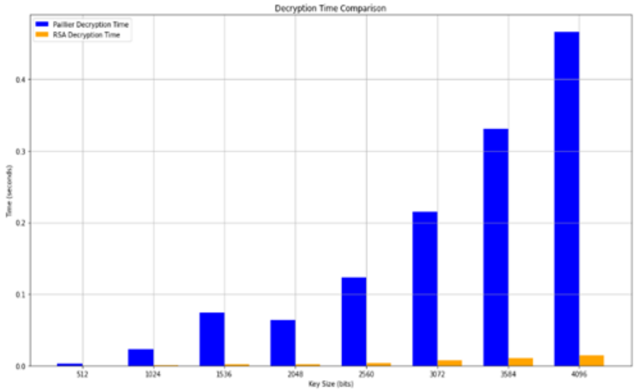

Fig. 4 Decryption time for RSA and Paillier system

Figure 3 presents the encryption time of RSA and Paillier algorithms for different key lengths. Despite the fact that RSA encryption is faster because of the simplified modular exponentiation, Paillier encryption is more preferable because it supports homomorphic properties that are mandatory for privacy-preserving applications.

The decryption time of the same algorithms is depicted in the Figure 4. RSA is faster as decryption operation is less in RSA than in Paillier. However, as Paillier uses more complicated modular arithmetic and key management for decryption, it is slower. However, Paillier supports additive homomorphism which is desirable for most of the operations needed for the proposed healthcare applications.

B. *Comparison of RSA Algorithm and Paillier Encryption in terms of time required to process N plaintexts*

In Figure 5, the total processing time of the two cryptosystems, namely Paillier and RSA, which uses 2048-

bit key size is considered as a function of number of plaintexts. From the graph it is evident that Paillier takes much more time than RSA to compute and the time taken by Paillier increases exponentially with the increase in the number of plaintexts from 1 to 10 taking over 2 seconds for 10 plaintexts. RSA on the other hand has a much lower and relatively constant processing time, which only slightly increases with the increase in the number of plaintexts. Figure 5 gives a direct comparison between RSA and Paillier based on the amount of time taken to process the data as a function of number of plaintexts.

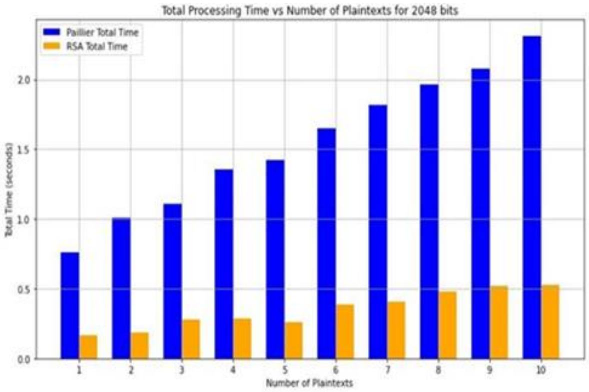

Fig. 5 Total processing time for N plaintexts

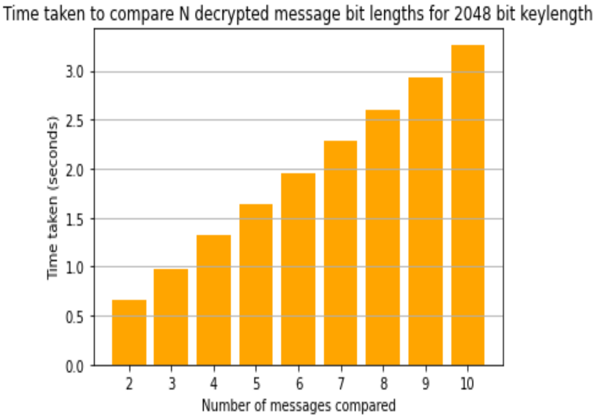

Fig. 6 Processing time for compare operation of N plaintext in Paillier system

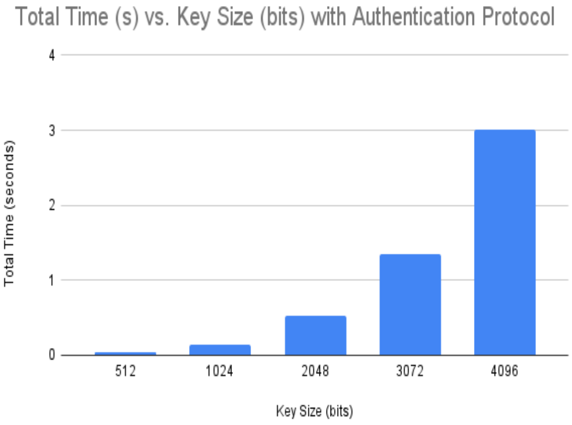

Fig. 7 Processing time for Paillier encryption with authentication protocol

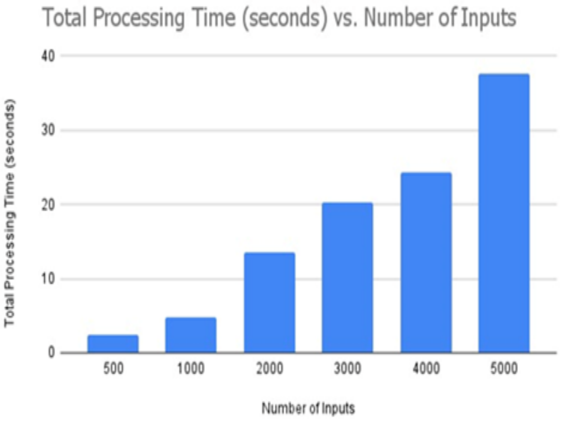

Fig. 8 Processing time requirement for Paillier system

C. Time Analysis of Comparison Operation in Paillier Cryptosystem

Time needed to perform comparison operation using Paillier cryptosystem is presented in Figure 6. A key size of 2048-bit is used for the analysis. As it was mentioned before, Paillier does not support comparison operation in encrypted domain. However, such operations are performed with the help of masking and demasking processes. With the increase in the number of plaintexts, the time taken for comparison increases exponentially as shown in Figure 6. This reveals the computational cost incurred by these techniques. However, this approach works well in allowing for secure comparisons, thus demonstrating how Paillier's encryption can be used to perform tasks it was not initially designed for, all the while still preserving privacy.

D. Time Analysis after Integrating Authentication

Figure 7 details the relationship between the size of the key and the time taken to process the Paillier cryptosystem with authentication support. With the increase in the key size, the total time taken for the authentication and encryption also increases at a very high rate. This shows that the time taken to perform the authentication protocol is highly dependent on the computational complexity of the authentication protocol.

E. Analysing COVID-19 Pandemic Data

Using the proposed system an attempt was made to perform computations in COVID 19 data in an opensource dataset presented in [26]. Blood oxygen saturation levels were considered for analysis. Data of a single person (with volume of the data varied for analysis) was considered and computed the number of deviations in the blood oxygen level from the threshold. The analysis of the results revealed the fact that the number of input values influenced the processing time, which confirmed the effectiveness of the proposed approach. Hence the Paillier system provides a solution for securely analyzing sensitive healthcare data especially where privacy is of paramount importance.

V. CONCLUSION

This paper proposes a HE-based privacy-preserving healthcare data solution. A secure HE can be considered as a major step towards ensuring the security and privacy of the data in healthcare settings. The proposed system empowers computations using HE such that it can process data directly without having to decrypt them, thus reducing exposure of sensitive data to unauthorized personnel. This makes it possible for the patients' data to be kept secure right from the time the information is submitted to the various healthcare professionals and thus, minimizes data leakage. The design of the system ensures that, apart from having the basic functionality, the authentication and privacy of customers are well protected.

In addition, this paper discusses the possibility of applying state-of-the-art cryptographic methods in real-world solutions in the healthcare industry. With data privacy continuously becoming an issue because of the increasing use of technology in data processing, these solutions provide a viable method of ensuring that sensitive information is safeguarded while at the same time allowing for meaningful information and analysis to be conducted. As a part of the future work, many other operations can be implemented using the proposed system on healthcare data.

References

[1] Milanov, Evgeny. "The RSA algorithm." RSA laboratories (2009): 1-11.

[2] Mahajan, Prerna, and Abhishek Sachdeva. "A study of encryption algorithms AES, DES and RSA for security." Global journal of computer science and technology 13, no. 15 (2013): 15-22.

[3] Ma, Changshe, Jian Weng, Yingjiu Li, and Robert Deng. "Efficient discrete logarithm based multi-signature scheme in the plain public key model." Designs, Codes and Cryptography 54 (2010): 121-133.

[4] Hellman, Martin E. "An overview of public key cryptography." IEEE Communications Magazine 40, no. 5 (2002): 42-49.

[5] Munjal, Kundan, and Rekha Bhatia. "A systematic review of homomorphic encryption and its contributions in healthcare industry." Complex & Intelligent Systems 9, no. 4 (2023): 3759-3786.

[6] Transforms, InformationYPreserving. "Complex Adaptive Systems, Publication 3 Cihan H. Dagli, Editor in Chief Conference Organized by Missouri University of Science and Technology 2013Y Baltimore, MD." Procedia Computer Science 20 (2013): 000-000.

[7] Zhang, Chuan, Liehuang Zhu, Chang Xu, and Rongxing Lu. "PPDP: An efficient and privacy-preserving disease prediction scheme in cloud-based e-Healthcare system." Future Generation Computer Systems 79 (2018): 16-25.

[8] Sendhil, R., and A. Amuthan. "Contextual fully homomorphic encryption schemes-based privacy preserving framework for securing fog-assisted healthcare data exchanging applications." International Journal of Information Technology 13, no. 4 (2021): 1545-1553.

[9] Das, Debasis. "Secure cloud computing algorithm using homomorphic encryption and multi-party computation." In 2018 International Conference on Information Networking (ICOIN), pp. 391-396. IEEE, 2018.

[10] Ogunseyi, Taiwo Blessing, and Tang Bo. "Fast decryption algorithm for paillier homomorphic cryptosystem." In 2020 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS), pp. 803-806. IEEE, 2020.

[11] Scheibner, James, Marcello Ienca, and Effy Vayena. "Health data privacy through homomorphic encryption and distributed ledger computing: an ethical-legal qualitative expert assessment study." BMC Medical Ethics 23, no. 1 (2022): 121.

[12] Aiswarya, R., R. Divya, D. Sangeetha, and V. Vaidehi. "Harnessing healthcare data security in cloud." In 2013 International Conference on Recent Trends in Information Technology (ICRTIT), pp. 482-488. IEEE, 2013.

[13] Bensitel, Yasmina, and Rahal Romadi. "Secure data storage in the cloud with homomorphic encryption." In 2016 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech), pp. 1-6. IEEE, 2016.

[14] Ding, Wenxiu, Zheng Yan, and Robert H. Deng. "Encrypted data processing with homomorphic re-encryption." Information Sciences 409 (2017): 35-55.

[15] Song, Chen, and Xinghua Shi. "ReActHE: A homomorphic encryption friendly deep neural network for privacy-preserving biomedical prediction." Smart Health 32 (2024): 100469.

[16] Zhou, Yousheng, Liyuan Song, Yuanni Liu, Pandi Vijayakumar, Brij B. Gupta, Wadee Alhalabi, and Hind Alsharif. "A privacy-preserving logistic regression based diagnosis scheme for digital healthcare." Future Generation Computer Systems 144 (2023): 63-73.

[17] Nayak, Nachiketha, Prajwal G. Anchan, H. N. Ramachandra, and K. S. Shivaprakasha. "Secure Communication for Healthcare Using Homomorphic Encryption: A Comparative Study." In 2023 2nd International Conference on Futuristic Technologies (INCOFT), pp. 1-4. IEEE, 2023.

[18] Hao, Meng, Hongwei Li, Guowen Xu, Zhe Liu, and Zongqi Chen. "Privacy-aware and resource-saving collaborative learning for healthcare in cloud computing." In ICC 2020-2020 IEEE International Conference on Communications (ICC), pp. 1-6. IEEE, 2020.

[19] Kim, Miran, and Kristin Lauter. "Private genome analysis through homomorphic encryption." In BMC medical informatics and decision making, vol. 15, pp. 1-12. BioMed Central, 2015.

[20] Alloghani, Mohamed, Mohammed M. Alani, Dhiya Al-Jumeily, Thar Baker, Jamila Mustafina, Abir Hussain, and Ahmed J. Aljaaf. "A systematic review on the status and progress of homomorphic encryption technologies." Journal of Information Security and Applications 48 (2019): 10236.

[21] Wei Wang, Yin Hu, Lianmu Chen, Xinming Huang, Senior Member, IEEE, and Berk Sunar, Member, IEEE. "Exploring the Feasibility of Fully Homomorphic Encryption". IEEE Transactions on Computers 64, no. 3 (2013): 698-706.

[22] Boomija, M. D., and S. V. Kasmir Raja. "Secure predictive analysis on heart diseases using partially homomorphic machine learning model." In Proceedings of International Joint Conference on Advances in Computational Intelligence: IJCACI 2021, pp. 565-581. Singapore: Springer Nature Singapore, 2022.

[23] Sarkar, Esha, Eduardo Chielle, Gamze Gürsoy, Oleg Mazonka, Mark Gerstein, and Michail Maniatakos. "Fast and scalable private genotype imputation using machine learning and partially homomorphic encryption." IEEE access 9 (2021): 93097-93110.

[24] Sendhil, R., and A. Amuthan. "Contextual fully homomorphic encryption schemes-based privacy preserving framework for securing fog-assisted healthcare data exchanging applications." International Journal of Information Technology 13, no. 4 (2021): 1545-1553.

[25] Xu, Wenju, Qingqing Zhao, Yu Zhan, Baocang Wang, and Yupu Hu. "Privacy preserving association rule mining based on electronic medical system." Wireless Networks (2022): 1-15.

[26] Alavi, A., Bogu, G.K., Wang, M. et al. Real-time alerting system for COVID-19 and other stress events using wearable data. Nat Med 28, 175–184 (2022) (https://www.nature.com/articles/s41591-021-01593-2#Sec22