Homomorphic Encryption and Authentication for Healthcare Applications

Swapnil Sharma 4NM21EC161

Uditaparna Sarmah 4NM21EC173

Vineet M Dodamani 4NM21EC183

Vikas Rai K 4NM22EC421

Under the Guidance of

Dr. K. S. SHIVAPRAKASHA
Professor

Department of Electronics & Communication Engineering

NITTE EDUCATION TRUST | NMAM INSTITUTE OF TECHNOLOGY

Contents

- Introduction
- Literature Survey
- Block Diagram
- Requirement Analysis
- Work Progress
- Gantt Chart
- References

Introduction

What is Homomorphic Encryption?

- Encryption method that allows computations to be performed on encrypted data without decryption.
- The result of the computation is also encrypted, preserving data privacy throughout the process.
- Three main types: Fully Homomorphic Encryption (FHE), Partially Homomorphic Encryption (PHE) and Somewhat Homomorphic Encryption (SHE).

Why Homomorphic Encryption and Authentication?

- Data Privacy: Enables computations on encrypted data.
- Security: Limits access to authorized users.
- Efficiency: Allows secure, efficient data processing.

Introduction

Why Use Homomorphic Encryption in Healthcare?

- Secure Data Sharing
- Remote Data Analysis
- Cloud-Based Healthcare

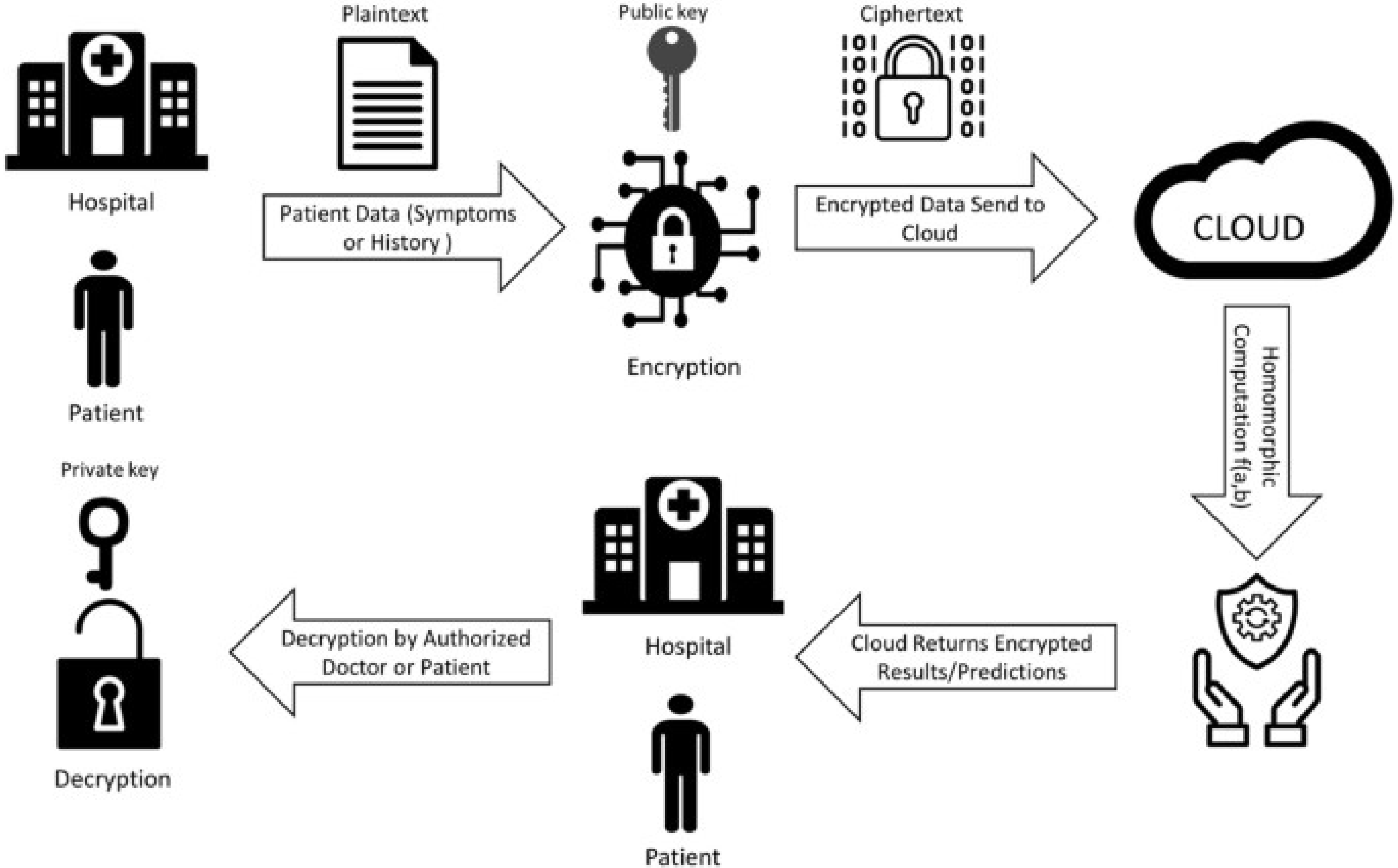

Fig. 1 Homomorphic Encryption

Literature Survey

Click Here

RSA Algorithm

Key Generation:

- Select p and q, both are prime, $p \neq q$
- Calculate $n = p \times q$
- Calculate $\phi(n) = (p-1) \times (q-1)$
- Select integer e such that $\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
- Calculate d: $d \equiv e^{-1}$
- Public key: $PU = \{e, n\}$
- Private key: $PR = \{d, n\}$

Encryption:

- Plain Text : $M < n$
- Cipher Text : $C = M^e \bmod n$

Decryption:

- Plain Text : $M = C^d \bmod n$

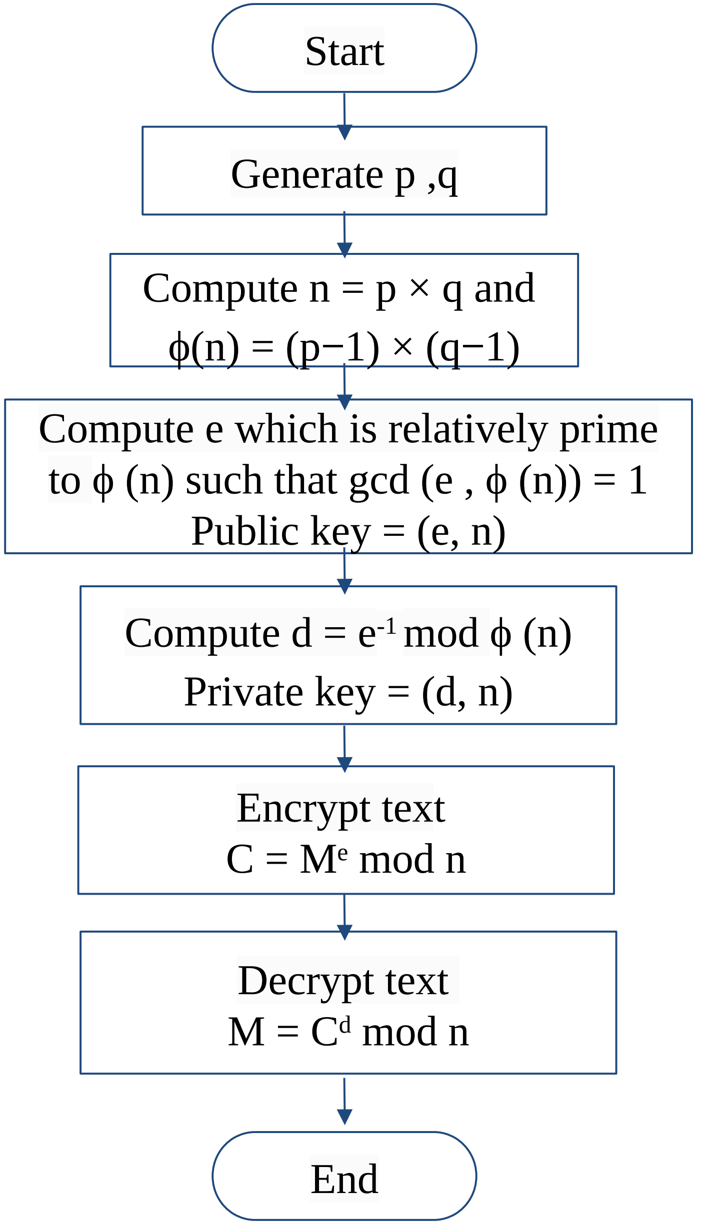

Fig. 2 Flowchart of RSA Cryptosystem

Paillier Cryptosystem

Key Generation:

- Select two large prime numbers p and q where gcd (pq, (p-1)(q-1)) = 1
- Calculate $n = p \times q$
- Calculate $\lambda = \text{lcm}\ (p-1, q-1)$
- Select 'g' as a random integer where $g \in Z^*_{n^2}$
- Define $L(x) = \frac{x-1}{n}$
- Ensure 'n' divides the order of 'g' by checking the existence of the following modular multiplicative inverse.
  $u = (L\{g^{\lambda} \bmod n^2\})^{-1} \bmod n$
- Public Key = (n, g)
- Private Key = (λ, u)

Paillier Cryptosystem

Encryption:

- Select r as a random integer where $r \in Z^*_n$
- Cipher text $c = g^m \times r^n \bmod n^2$

Decryption:

- Plaintext $m = L(c^{\lambda} \bmod n^2) \times u \bmod n$

Paillier Cryptosystem

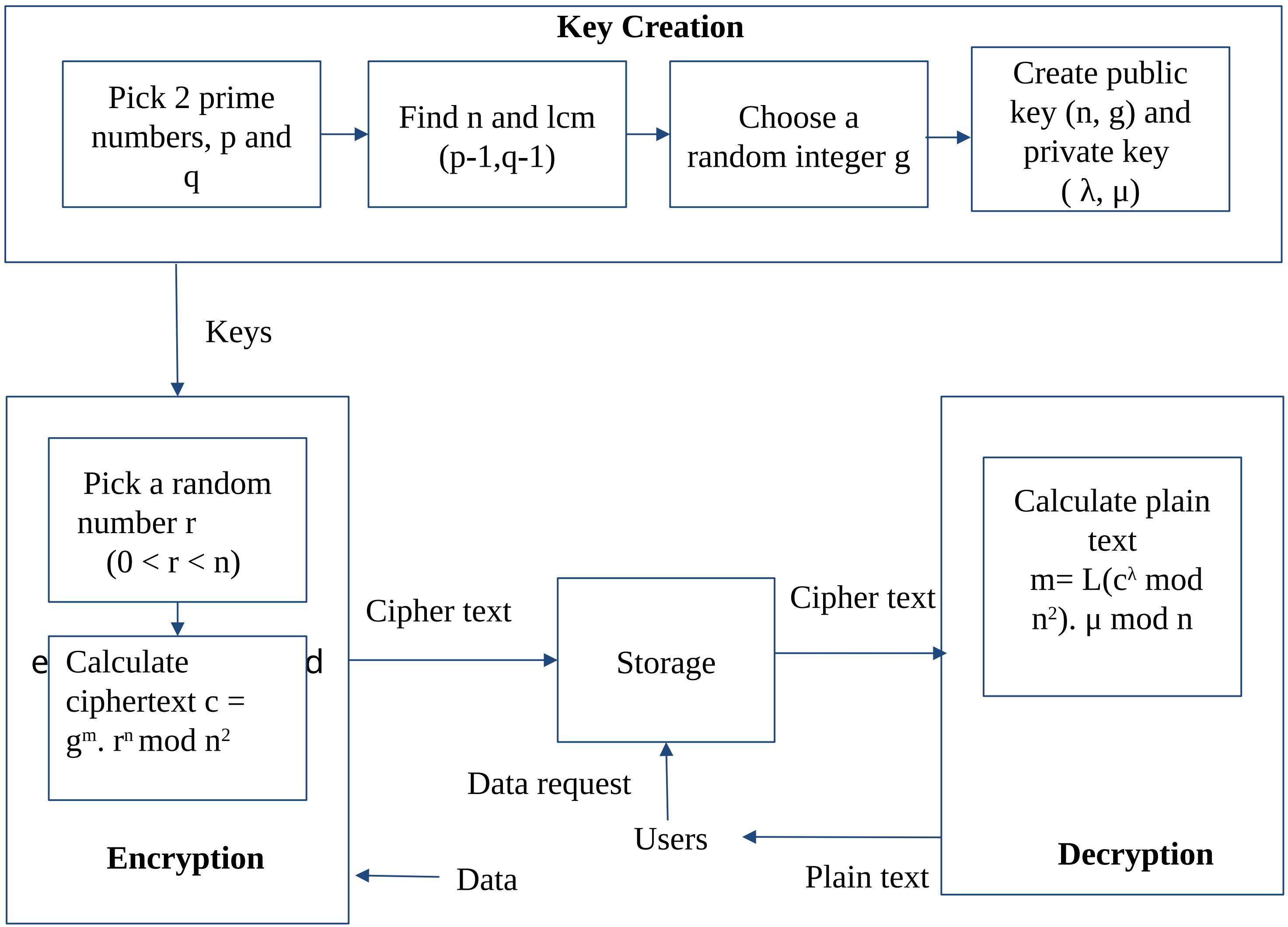

Fig. 3 Paillier Cryptosystem

Homomorphic Property of RSA and Paillier Cryptosystem

RSA Cryptosystem:

- RSA supports a **multiplicative homomorphic property**.

- Encryption:

  $c_1 = m_1^e \bmod n$ & $c_2 = m_2^e \bmod n$

- Homomorphic Multiplication:

  $\mathbf{c_1 \times c_2 = (m_1 x\, m_2)^e \bmod n}$

- Decryption:

  $\mathbf{m' = (c_1 \times c_2)^d \bmod n = (m_1 x\, m_2) \bmod n}$

Paillier Cryptosystem:

- The Paillier cryptosystem is a **probabilistic asymmetric algorithm**. It is known for its **additive homomorphic properties**.

- Encryption:

  $c_1 = g^{m1} r^n_1 \bmod n^2$ & $c_2 = g^{m2} r_2^n \bmod n^2$

- Homomorphic Addition:

  $\mathbf{c_1 c_2 = (g^{m1}.r^n_1).(g^{m2}.r^n_2) \bmod n^2 = g^{m1+m2}. (r1.r2)^n \bmod n^2}$

- Decryption:

  $\mathbf{D(c_1 c_2 \bmod n^2) = m_1 + m_2 \bmod n}$

Block Diagram

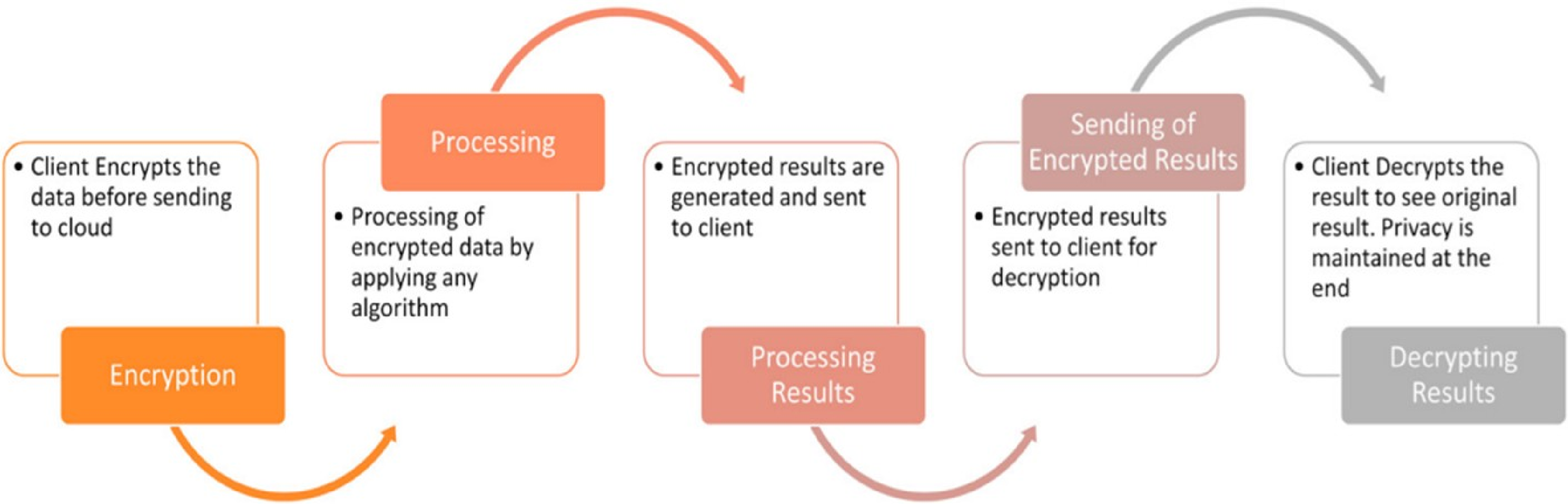

Fig. 4 Process of Homomorphic Encryption for Providing Security in Cloud

Requirement Analysis

Table I: Software Requirement

Sl. No	Requirement	Justification
01	Python Programming	The latest version of python language i.e. Python 3.11 series is used in this system. This language is employed in developing the backend logic facilitating the collection and processing of encrypted feedback. It is also utilized for its versatility and ease of integration with homomorphic encryption libraries.
02	Spyder	Spyder IDE is an open-source Python IDE designed for data science and scientific computing. It features a powerful editor, an integrated IPython console for interactive coding, and a variable explorer to easily manage and inspect data. Spyder's environment is particularly suited for developing and testing complex algorithms, such as those used in homomorphic encryption, due to its robust debugging and visualization tools.

Requirement Analysis

Table I: Software Requirement

Sl. No	Requirement	Justification
03	Anaconda	One of the top cloud computing platforms is Amazon Web Services (AWS), which provides a wide range of services on a pay-per-use basis. Without having to invest in physical infrastructure, consumers may access databases, machine learning, storage, processing capacity, and more with AWS. Because of its scalable, dependable, and secure services, businesses, governments, and startups all favour it.
04	Tkinter	Tkinter is the standard GUI toolkit that comes bundled with python.

Work Split

Table II: Work split

Sl. No	Phase	Description
01	Literature Survey	• A survey on basics of HE methods • Types of HE • Paillier Cryptosystem and RSA Cryptosystem
02	System Architecture and Design	• Defining the overall structure, components, and interactions within the student feedback system. • Outlining the data flow, user interfaces, and backend data processing.
03	Homomorphic Encryption Implementation	• Implementing Pascal Pailliers and RSA algorithm for preserving privacy of student feedback system. using PySEAL library to generate encryption and decryption keys • Using Spyder platform
04	Documentation	• Code documentation for developers. • Documenting user guides for end-users. • System documentation outlining the architecture and deployment processes.

Result and Analysis

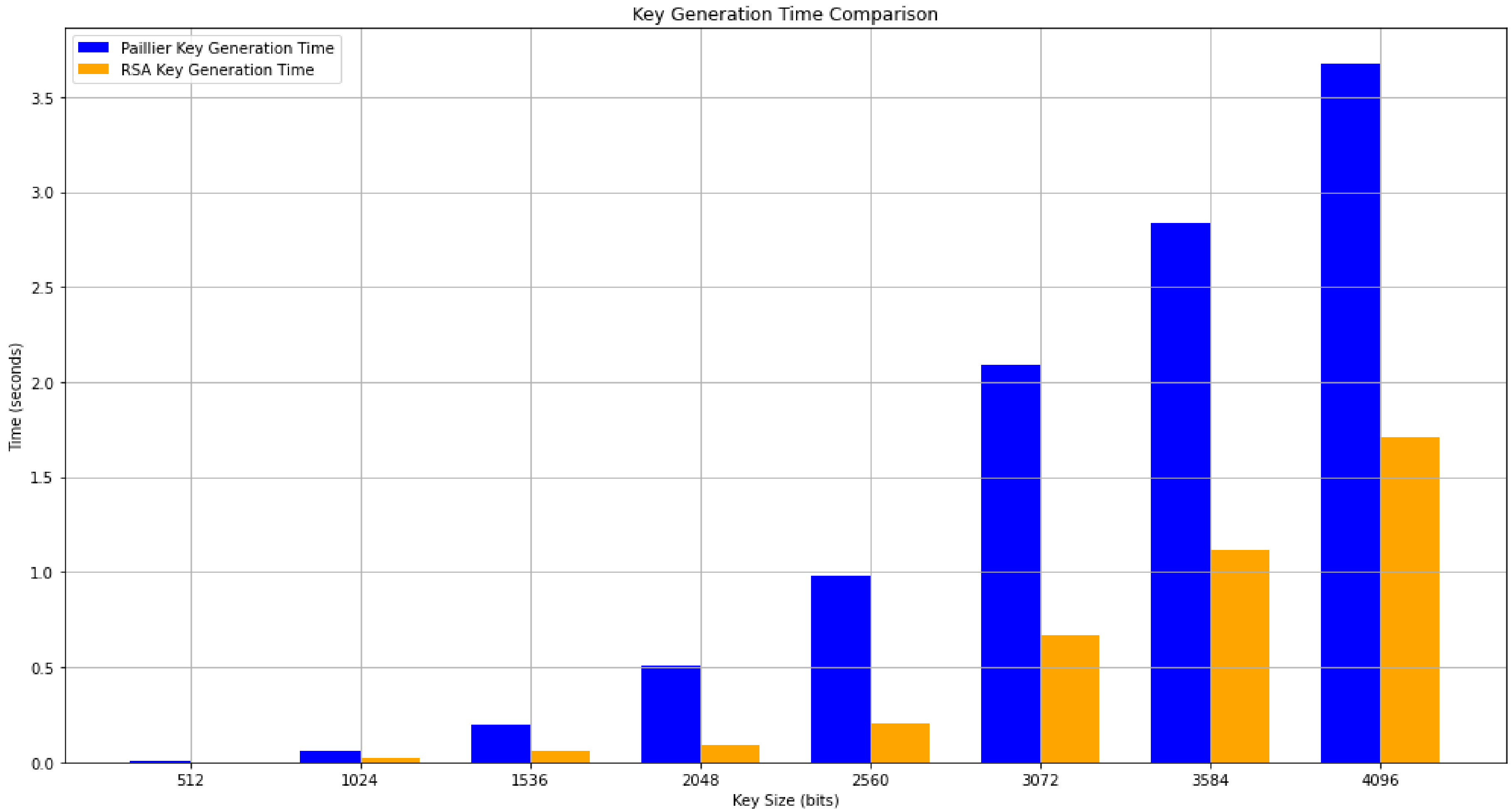

Fig. 5 Key Generation Time Analysis for RSA and Paillier Algorithm

Result and Analysis

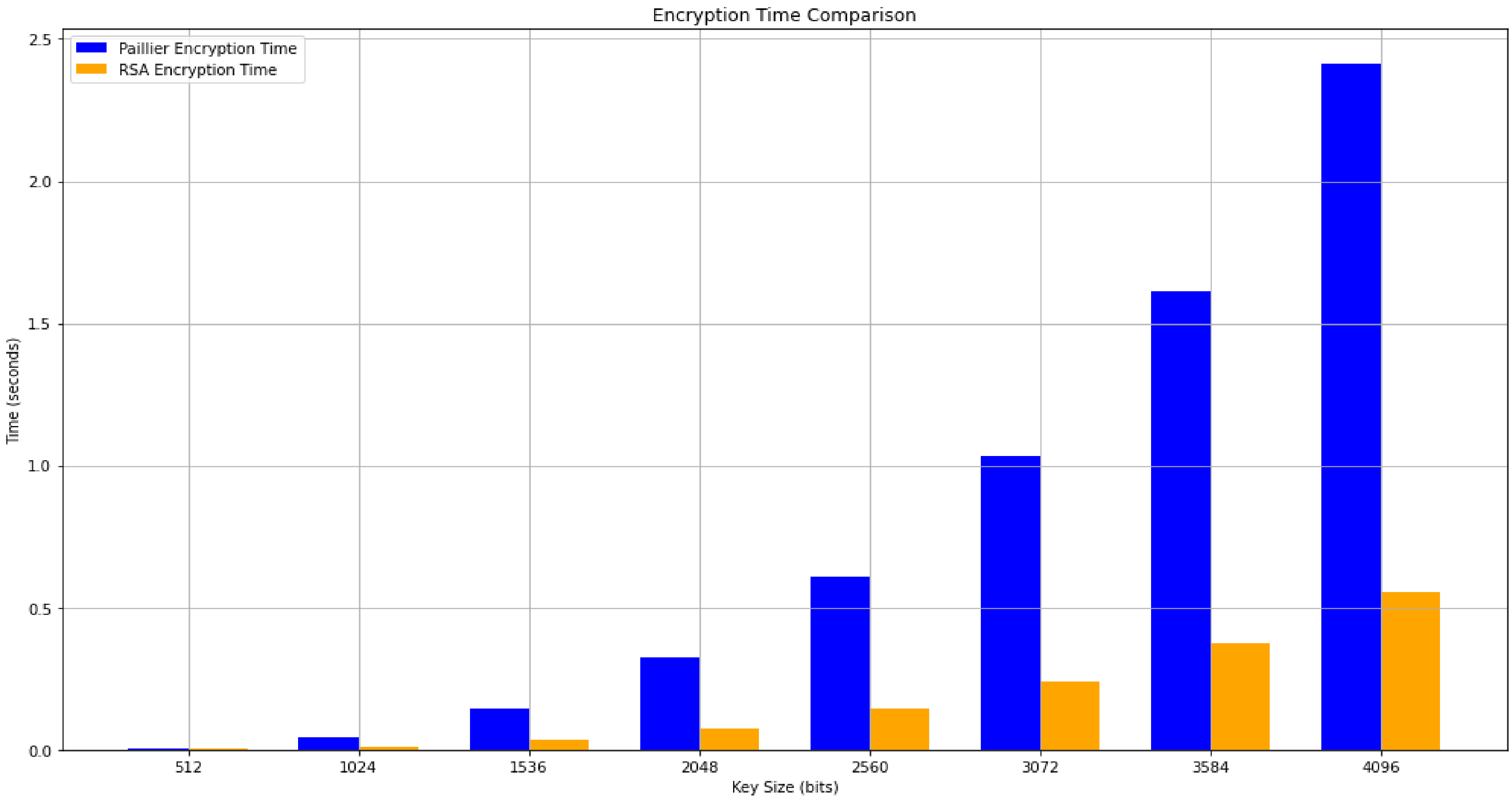

Fig. 6 Encryption Time Analysis for RSA and Paillier Algorithm

Result and Analysis

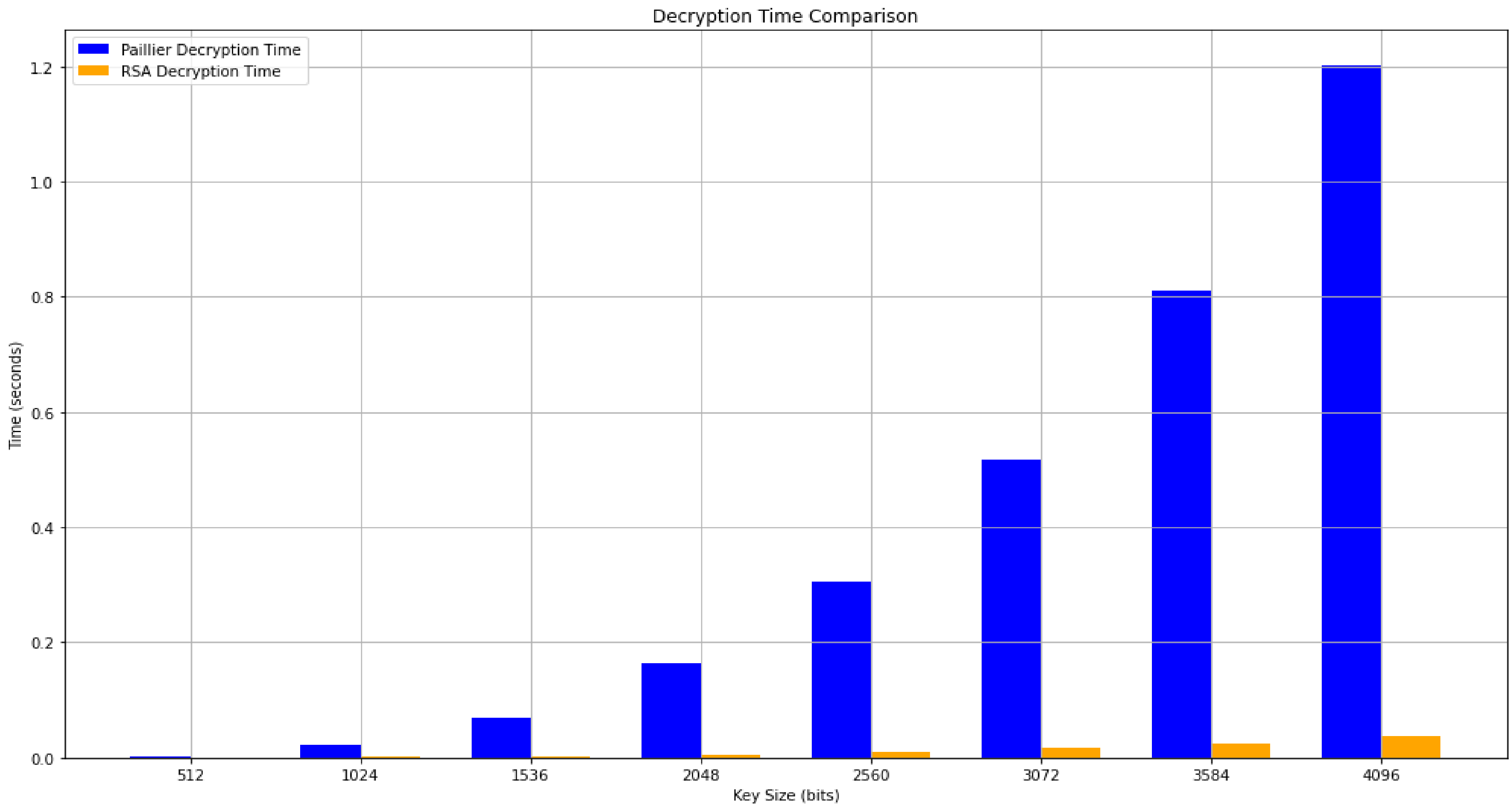

Fig. 7 Decryption Time Analysis for RSA and Paillier Algorithm

Result and Analysis

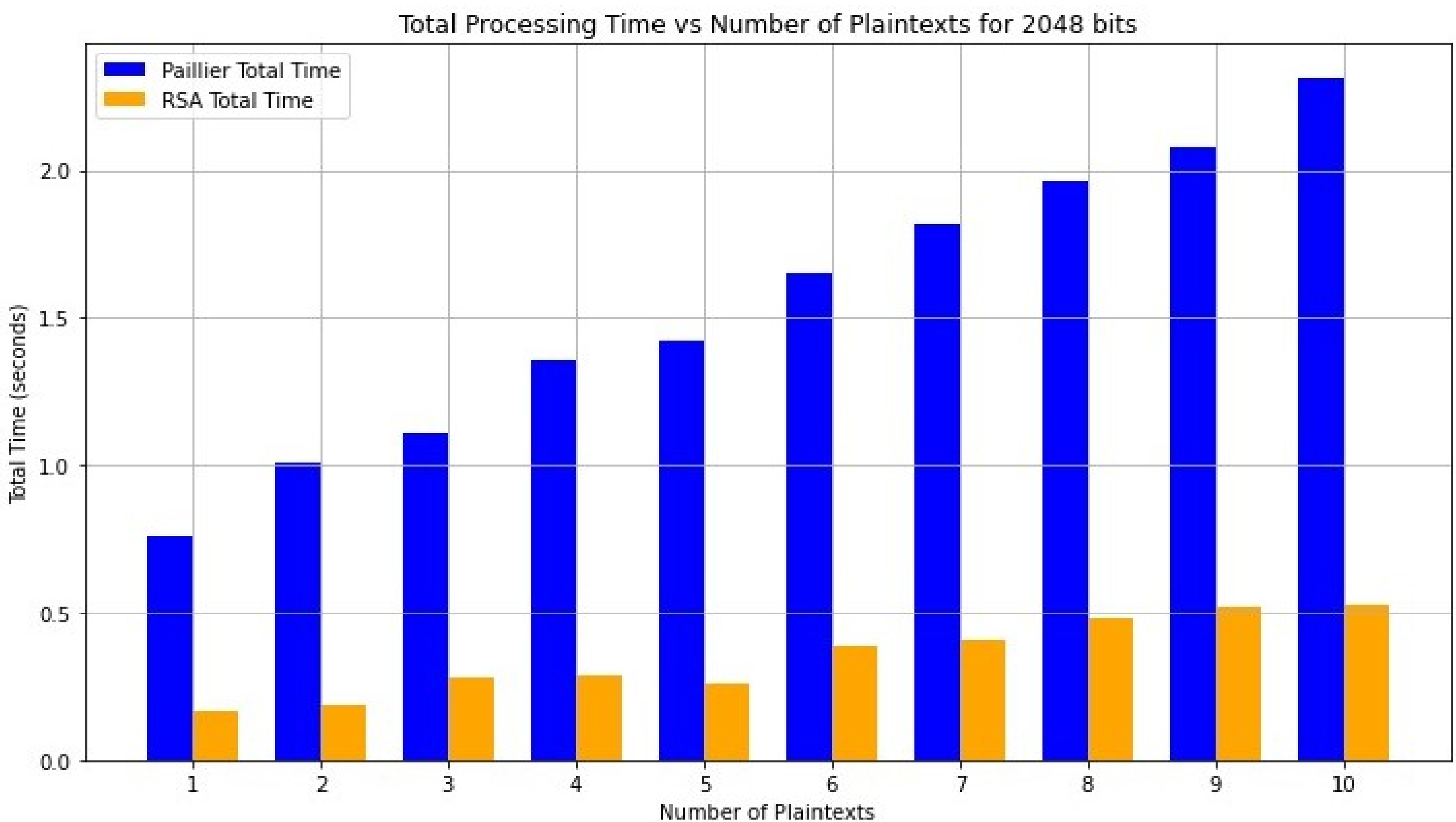

Fig. 8 Time Analysis for RSA and Paillier Algorithm with Multiple Messages

Gantt Chart

[Click Here]

Paper Publication

Upcoming Milestones:

A paper based on the project is being communicated to International Conference on Recent Advances in Science and Engineering Technology, an IEEE Conference from IEEE Bangalore Section.

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, Information Preserving. "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).
7. Zhang, Chuan, Lei Huang 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.

References

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. 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.
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.

References

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.

Thank You