WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Comparative Analysis of Fortifying Cloud Data Security Using Homomorphic Encryption

Unnimaya M U[1], Dr. Shibily Joseph[2]

[1]Department of Computer Science and Engineering Government Engineering College, Wayanad Kerala, India unnimayamu2001@gmail.com
[2]Department of Computer Science and Engineering Government Engineering College, Wayanad Kerala, India shibily.j@gecwyd.ac.in

ABSTRACT—

This research project focuses squarely on the pivotal objective of enhancing the security of cloud-stored data through the implementation of homomorphic encryption. In contemporary cloud computing paradigms, ensuring the confidentiality and integrity of sensitive information is paramount, given the increasing reliance on cloud-based storage and processing. Homomorphic encryption emerges as a promising solution, allowing computations to be performed directly on encrypted data without the need for decryption, thus mitigating the risk of unauthorized access or data breaches. The primary thrust of this study is to design, develop, and assess a homomorphic encryption algorithm specifically tailored to address the unique challenges posed by cloud data security. Through meticulous experimentation and rigorous analysis, the research aims to demonstrate the practical efficacy of homomorphic encryption in safeguarding cloud-based data from unauthorized access and malicious tampering. While the application of a simple arithmetic operation, such as addition, serves as a proof of concept, the ultimate objective is far- reaching: to fortify the integrity and confidentiality of cloud-stored data across various domains and industries. By delving into the intricacies of homomorphic encryption and its integration within cloud computing environments, this research endeavors to provide tangible solutions and insights that can inform best practices in data security. The findings and recommendations derived from this study hold significant promise for enhancing the resilience of cloud based systems against potential threats and vulnerabilities. In essence, this research represents a critical step forward in ensuring the trustworthiness and reliability of cloud computing infrastructures in an increasingly interconnected and data-driven world.

Index Terms- Cloud Computing, Homomorphic Encryption, Security, Data Protection.

I. Introduction

In the era of digital transformation, cloud computing has become a cornerstone of modern technological advancements, enabling seamless storage, processing, and management of vast volumes of data. While its adoption spans across various industries, the growing reliance on cloud infrastructures brings heightened concerns about data security and privacy. Ensuring the confidentiality and integrity of sensitive information stored in the cloud has become a critical challenge, as threats such as unauthorized access, data breaches, and malicious tampering continue to proliferate. Homomorphic encryption (HE) has emerged as a ground breaking cryptographic technique that holds immense potential for addressing these security concerns. Unlike traditional encryption methods, HE allows computations to be performed directly on encrypted data without requiring decryption. This distinctive capability ensures that data remains secure throughout its lifecycle, even when processed by untrusted cloud environments. By preserving data confidentiality during computation, homomorphic encryption significantly reduces vulnerabilities and bolsters the trustworthiness of cloud systems. This research aims to explore the application of homomorphic encryption as a robust solution to the challenges posed by cloud data security. Specifically, it seeks to design and implement a tailored HE algorithm to enhance the protection of cloud stored information. Through detailed experimentation and analysis, the study endeavors to assess the feasibility and efficacy of homomorphic encryption in safeguarding sensitive data against potential threats.

The findings of this research aspire to contribute to the development of secure and reliable cloud infrastructures, addressing critical security gaps in an increasingly interconnected and data-driven world. By focusing on the interplay between advanced cryptographic techniques and practical cloud security applications, this work aims to pave the way for innovative solutions that can redefine data protection standards across industries.

II. LITERATURE REVIEW

[1] In this paper, they proposed a new cryptographic scheme, a simulation environment was set up on a standard computing system configured with an Intel i7 processor, 16 GB RAM, and a 512 GB SSD, operating on Ubuntu 20.04 LTS. The implementation utilized C and Python 3.8, incorporating libraries such as NumPy for numerical operations, PyCryptodome for cryptographic functionality, and Matplotlib for visual analysis. This setup was selected to support secure computations while ensuring stable and efficient performance during comprehensive testing and evaluation. The key generation process involved creating a 128-bit symmetric encryption key K using a cryptographic random number generator. This key was employed to encrypt a

10MB text file F, which contained random data to simulate sensitive information. To enhance security, AES in CBC (Cipher Block Chaining) mode was implemented. This ensured that identical plaintext blocks produced unique ciphertext blocks, thereby mitigating risks associated with pattern detection. Additionally, an input matrix was encrypted and transformed into an encrypted output, resulting in the ciphertext C. For the secret sharing phase, a 256-bit prime number p was selected to ensure p exceeded the maximum differential k, which is the difference between the file size and the minimum shares required for reconstruction. A polynomial f(x) was constructed by setting non-zero coefficients a1,a2,....,ak-1 chosen randomly from the finite field zp. Using a threshold value k=5, a total of n=10 shares were generated, allowing any combination of 5 shares to reconstruct the original secret key K. During the encryption process, the symmetric key K was applied to the file F to produce the ciphertext C. The polynomial f(x) represented the key K, and 10 random values of x from Zp were evaluated to compute the corresponding shares(xi,f(xi)). These shares were distributed across simulated cloud servers to emulate a distributed storage environment. To validate the scheme's practicality, arithmetic operations like addition and multiplication were performed directly on the encrypted shares stored in the cloud without exposing the original data. This demonstrated the capability for secure computations within a cloud environment. For key reconstruction, any 5 shares (xi, si) were retrieved from the cloud servers. Using Lagrange interpolation, the original key K was reconstructed accurately. The recovered key was then used to decrypt the ciphertext C, successfully retrieving the original file F. The integrity of the decryption process was verified by comparing the retrieved file with the original. The performance of the scheme was evaluated by measuring critical metrics such as the time taken for key generation, encryption, decryption, share creation, and reconstruction. The computational overhead introduced by homomorphic operations was also analyzed. Additionally, a security assessment was conducted to test the scheme against potential attacks, demonstrating its robustness and efficiency through execution time metrics and success rates.

[2] This paper underscores the potential of the ModifiedEHC algorithm in achieving faster processing times, making it a viable solution for secure cloud-based applications with high integrity-checking requirements. One suggested approach involves a system architecture comprising three core components: a data owner, an Authority Server (AS), and a cloud server for data storage. In this setup, the data owner is tasked with applying hashing and concatenation techniques to the data, followed by dividing it into smaller blocks and encrypting these blocks before uploading them to cloud servers. For validation, the Authority Server retrieves data from the cloud, encrypts it using robust algorithms, and compares it to the client's original data. A match confirms the integrity of the data, whereas discrepancies may indicate tampering, poor data management, or potential attacks. The performance of this methodology was evaluated through simulations conducted on a system with an Intel Core i5 processor and 8 GB RAM using the CloudSim platform. Key metrics assessed included the time taken for encryption, decryption, and key generation under varying input sizes. Comparative analysis demonstrated that the ModifiedEHC algorithm significantly outperformed the standard EHC algorithm in all aspects. Specifically, ModifiedEHC exhibited reduced key generation, encryption, and decryption times, highlighting its efficiency. However, the study noted that execution time increased with higher polynomial degrees, primarily due to the linear complexity of polynomial operations involved in encryption and decryption.

[3] This paper introduces a homomorphic encryption-based security scheme tailored for cloud computing environments. This approach ensures secure data transmission between users and the cloud while maintaining data safety during storage. The scheme is designed to facilitate convenient data search and processing by users and third-party agencies without compromising security. However, the study acknowledges that fully homomorphic encryption, while promising, presents computational challenges that require further research to enhance its practicality.

This paper highlights the pressing need for effective encryption mechanisms and shared security responsibilities in cloud computing, emphasizing the potential of homomorphic encryption to mitigate key security risks and protect sensitive data.

In this paper the methodology employs fully homomorphic encryption to enable secure data processing directly on encrypted data without the need to decrypt it. Users or trusted third parties can perform computations on the encrypted data and decrypt the results to access meaningful outcomes. For instance, in the context of a medical information system, electronic medical records are stored in ciphertext on cloud servers. When health departments need to analyze safety concerns, such as disease prevalence in specific regions or age groups, they can provide the encrypted medical records to specialized data processing services. These services process the encrypted data and return accurate results, which users can decrypt to obtain actionable insights.

The study explores the performance of a Hybrid Homomorphic Encryption system, focusing on the integration of the GM and RSA cryptosystems. Three text files of varying sizes were selected as input to evaluate and compare the encryption and decryption performance of the Enhanced Hybrid Encryption Scheme (EHES) and the proposed hybrid encryption algorithm.

The experiment was conducted on a machine equipped with an Intel® Core™ i7-5600U CPU @ 2.60 GHz and 4 GB of RAM. Performance metrics, including encryption and decryption times, were recorded for both algorithms. The results indicate that the EHES algorithm supports a single multiplicative operation, while the proposed hybrid algorithm supports both additive and multiplicative operations, significantly enhancing its utility.

Moreover, the proposed algorithm demonstrated superior performance, achieving encryption and decryption speeds three times faster than the EHES algorithm. This improvement highlights its potential for practical applications requiring efficient cryptographic operations.

The findings underscore the advantages of combining GM and RSA schemes within a hybrid framework, offering a robust and versatile solution for secure data processing with enhanced operational flexibility and efficiency.

[4] The study proposes a homomorphic encryption scheme as a solution to address concerns related to user security and trust. This cryptographic approach ensures the protection of client data stored on the cloud while allowing secure computational processes by various applications. The research underscores the unique capabilities of homomorphic encryption, enabling secure data processing without the need to decrypt sensitive information.

Homomorphic encryption proves especially relevant in the banking sector, safeguarding customer information against unauthorized access by service providers or internal employees. Cloud Service Providers (CSPs) can process client queries and provide data responses while maintaining the privacy and confidentiality of customer information.

However, the study acknowledges a significant challenge that is the computational cost of performing operations on ciphertexts using fully homomorphic encryption remains high. To address this limitation, the paper emphasizes the importance of ongoing research to optimize encryption algorithms and enhance computational efficiency for ciphertext operations.

This paper effectively highlights the transformative potential of homomorphic encryption in digital banking, ensuring robust security and trust while identifying areas for further development to improve practicality and efficiency.

[5] This study introduces a two-layer encryption approach designed to enhance data security in cloud computing environments. The proposed methodology combines symmetric and asymmetric cryptographic techniques, leveraging their respective strengths to create a robust encryption framework. The first layer employs a symmetric key algorithm based on substitution and permutation methods inspired by the Feistel structure. This is further enhanced by Shannon's principles of diffusion and confusion, implemented through logical opera- tions such as XOR, XNOR, shifting, and swapping. This layer establishes a strong foundation for initial data encryption. The second layer incorporates asymmetric cryptography,

utilizing the RSA algorithm's multiplicative homomorphic feature to facilitate secure operations on encrypted data. By enabling computations directly on ciphertext, this approach ensures that the encoded results align with the outcomes of equivalent operations on plaintext, thereby preserving the integrity of encrypted data.

Additionally, the second layer modifies RSA by integrating homomorphic encryption, further enhancing its applicability for cloud-based security. This modification allows complex mathematical operations to be executed on encrypted data without decryption, safeguarding sensitive information even within untrusted systems or applications.

The dual-layer encryption system demonstrates significant potential for secure data handling, especially in scenarios requiring advanced computations on encrypted data, such as in cloud computing. By combining symmetric and homomorphic encryption techniques, the proposed approach effectively strengthens data security while addressing key challenges in contemporary cryptographic practices.

[6] This study introduces a robust cryptographic algorithm designed to address critical security challenges while maintaining efficiency for resource-constrained devices such as IoT systems. The proposed method focuses on enhancing resilience against various attacks by generating ciphertext using a random and unpredictable key. The incorporation of confusion, diffusion, and avalanche effects ensures that the resulting ciphertext is highly secure and resistant to cryptanalysis, rendering it nearly unbreakable.

A notable feature of the algorithm is its efficient response time, which makes it suitable for lightweight devices where computational overhead is a significant concern. This efficiency is critical in scenarios involving IoT devices, where rapid processing and minimal resource consumption are essential for optimal performance.

The study concludes that the proposed algorithm effectively balances robust security with performance, making it an ideal candidate for IoT and other low-power applications. Future work is aimed at enhancing the key generation phase to support variable key lengths, ensuring compatibility with a broader range of devices, including those requiring higher computational power. This advancement could further extend the algorithm's applicability to diverse domains, strengthening its position as a versatile and secure cryptographic solution.

[7] The paper introduces a novel effective lightweight homomorphic cryptographic algorithm which contains two layers of encryption. The first layer uses the new effective lightweight cryptographic algorithm. Second layer multiplicative homomorphic schemes considered for enhancing data security in cloud computing. The experimental results of the proposed algorithm presented a strong security level.

This study introduces a novel and effective Lightweight Homomorphic Cryptographic Technique aimed at strengthening cloud security. The proposed solution incorporates a dual-layer encryption strategy that combines both symmetric and asymmetric cryptographic principles for enhanced data protection.

The first encryption layer employs an innovative lightweight cryptographic algorithm designed for high efficiency and minimal resource consumption. The second layer leverages a multiplicative homomorphic encryption scheme, enabling secure computations on encrypted data without compromising its confidentiality. Together these layers provide security while maintaining the flexibility and performance required for modern cloud environments.

The effectiveness of the technique is evaluated across multiple metrics, including computational time, memory usage, and key sensitivity. Additionally, statistical analysis and entropy change analysis were conducted to assess the robustness of the encryption process. An image histogram was employed to visually represent the encryption's impact, highlighting the system's ability to maintain data integrity and withstand cryptographic attacks.

This dual-layer approach successfully balances security and efficiency, making it a promising solution for securing sensitive data in cloud computing systems. The research underscores the potential of lightweight cryptographic methods to meet the growing demands of secure and scalable cloud services

[8] This research focuses on improving data privacy and optimizing computational efficiency in multi-cloud environments by proposing a secure system model with an increased number of clouds. The study acknowledges the challenges of implementing homomorphic encryption in real world multi-cloud

applications and identifies solutions like multi-key homomorphic encryption and multiparty extensions, such as the ”Threshold setup,” supported by the OpenFHE library for BGV, BFV, and CKKS schemes.

The proposed model is specifically designed for managing multi-cloud electronic medical records. The architecture leverages homomorphic encryption algorithms to protect individual privacy in both networked and multi-cloud scenarios. The novelty of this approach lies in its reliance on OpenFHE, a widely recognized open-source library, making it accessible and easily configurable even for non-experts.

Feasibility tests were conducted by performing simple homomorphic operations within the proposed framework, demonstrating its practicality and effectiveness. The multicloud setup enables secure data handling while enhancing privacy and operational efficiency, especially in sensitive domains like healthcare.

This study underscores the importance of robust cryptographic techniques and highlights the utility of open source libraries in advancing the adoption of homomorphic encryption in complex multi-cloud environments.

[9] This paper introduces a secure model for banking data storage and processing in cloud servers by leveraging Partially Homomorphic Encryption (PHE) and a re-encryption proxy server. The proposed model addresses the critical need for secure mathematical operations on encrypted banking data, ensuring privacy and integrity in cloud environments.

The architecture consists of four main components: a cloud storage server (SS), the bank’s application (data provider), a proxy server (PS) for re-encryption, and the customer’s application. The security mechanism relies on the Paillier cryptosystem, which supports homomorphic operations. The SS and PS generate their respective public-private key pairs.

A shared public key (SHpk) is created by combining their public keys and distributed to the bank’s and customer’s applications. The bank’s application splits and encrypts the data using the SHpk via the Paillier cryptosystem before storing it on the cloud server. Customer applications submit requests (e.g., balance inquiry or withdrawal) along with their public key (Cpk). The cloud server authenticates the request. The SS performs mathematical operations on the encrypted data (e.g., calculating the remaining balance) and applies a re-encryption process through the PS to enhance security before delivering the results to the customer. This method ensures the confidentiality of sensitive customer data while allowing secure remote operations. The re-encryption proxy further fortifies security by enabling an additional layer of cryptographic transformation.

The proposed model effectively combines homomorphic encryption and proxy re-encryption to mitigate security challenges in cloud-based banking systems. Its scalability and ability to perform computations on encrypted data make it suitable for modern financial applications, enhancing trust in cloud-based banking services.

[10] The authors propose a novel methodology to enhance key allocation and key management practices. Their approach aims to optimize these processes to strengthen data security during transmission. This study highlights an important area of research, suggesting that addressing these key management issues can lead to more secure cloud environments and increase the trust of businesses and individuals in cloud computing systems.

The paper lays the groundwork for future research possibilities by introducing a new dimension of study focused on the optimization of cryptographic practices in the cloud. By improving key management and addressing weaknesses in existing encryption techniques, the proposed methodology could significantly contribute to the enhancement of cloud data security.

This paper addresses the crucial security concerns surrounding cloud computing by focusing on encryption techniques commonly used by Cloud Service Providers (CSPs). The study reviews existing encryption methodologies and identifies areas for improvement, particularly in the context of securing data as it moves across the cloud infrastructure. A key challenge in cloud security is the management and allocation of cryptographic keys, which can significantly impact the overall security and efficiency of data transmission.

III. Proposed Model

The proposed model uses Pailier homomorphic encryption technique to enhance the cloud data security by adding an additional level of security. Here there is considering a situation when a client wants to store a file on a cloud server by utilizing private sharing information. First the data is encrypted with Pailier homomorphic encryption algorithm and Shamir’s secrete sharing technique also applied and a trusted encryption also taken place and a trusted agency to provide additional level of security. When data owner requests for data retrieval it will reconstruct the data.

IV. CONCLUSION

The literature shows the importance of secure computation on encrypted data in cloud environments. Our contribution focuses on refining homomorphic encryption techniques, addressing the limitations of large key sizes and computational inefficiencies in existing methods. Our approach contributes to the field by reducing encryption computation time and increasing processing speed, overcoming existing challenges with encryption overhead while maintaining high levels of security and confidentiality for cloud-stored data. This project is feasible and addresses critical cloud security challenges, offering significant benefits to organizations relying on cloud services. With proper optimization and resource allocation, it can become a robust solution for enhancing data security in cloud environments.

References

[1] Sijjad Ali, Shuaib Ahmed Wadho, Aun Yichiet, Ming Lee Gan, and Chen Kang Lee. Advancing cloud security: Unveiling the protective potential of homomorphic secret sharing in secure cloud computing. *Egyptian Informatics Journal*, 27:100519, 2024.

[2] Naili Dwivedi, Mamta Swarnkar, Anita Soni, and Manmohan Singh. Cloud security enhancement using modified enhanced homomorphic cryptosystem. In *2023 IEEE Renewable Energy and Sustainable E- Mobility Conference (RESEM)*, pages 1–6. IEEE, 2023.

[3] Zainab Hikmat Mahmood and Mahmood Khalel Ibrahem. New fully ho- momorphic encryption scheme based on multistage partial homomorphic encryption applied in cloud computing. In *2018 1st Annual international conference on information and sciences (AiCIS)*, pages 182–186. IEEE, 2018.

[4] Sonam Mittal, Priya Jindal, and KR Ramkumar. Data privacy and system security for banking on clouds using homomorphic encryption. In *2021 2nd International Conference for Emerging Technology (INCET)*, pages 1–6. IEEE, 2021.

[5] Feng Zhao, Chao Li, and Chun Feng Liu. A cloud computing security solution based on fully homomorphic encryption. In *16th international conference on advanced communication technology*, pages 485–488. IEEE, 2014.

[6] Ch Rupa, Greeshmanth, and Mohd Asif Shah. Novel secure data protection scheme using martino homomorphic encryption. *Journal of Cloud Computing*, 12(1):47, 2023.

[7] Fursan Thabit, Ozgu Can, Sharaf Alhomdy, Ghaleb H Al-Gaphari, and Sudhir Jagtap. A novel effective lightweight homomorphic cryptographic algorithm for data security in cloud computing. *International Journal of intelligent networks*, 3:16–30, 2022.

[8] Yulliwas Ameur, Samia Bouzefrane, et al. Handling security issues by using homomorphic encryption in multi-cloud environment. *Procedia Computer Science*, 220:390–397, 2023.

[9] Muna Mohammed Saeed Altaee and Mafaz Alanezi. Enhancing cloud computing security by paillier homomorphic encryption. *International Journal of Electrical and Computer Engineering (IJECE)*, 11(2):1771– 1779, 2021.

[10] Mohd Atif Kaleem, Parvez Mahmood Khan, and Usman Ali Khan. Strengthening of homomorphic encryption scheme for cloud environ- ment using particle optimization algorithm. In *2021 Fourth international conference on computational intelligence and communication technologies (CCICT)*, pages 397–405. IEEE, 2021.