International Journal of Interpreting Enigma Engineers (IJIEE)

https://ejournal.svgacademy.org/index.php/ijiee/

OPEN ACCESS

# OPTIMIZED CLOUD SECURITY ECC-ENHANCED HOMOMORPHIC PAILLIER RE-ENCRYPTION


Veeresh Dachepalli

Original Article

Software Developer, Elemica Inc. CrossPoint at Valley Forge, 550 Swedesford Rd #310, Wayne, PA 19087

*Corresponding Author's Email: Veereshd513@gmail.com*

## Abstract

In the dynamic domain of cloud computing, ensuring data security is of utmost importance. Conventional encryption techniques, while providing a high level of security, introduce substantial computational burdens, rendering them impractical for environments with limited resources. In response to this predicament, our study introduces a novel lightweight encryption framework that amalgamates Elliptic Curve Cryptography (ECC) with Homomorphic Paillier Re-Encryption, thereby reinforcing the security of data within cloud infrastructures.

Our methodology exploits the inherent advantages of ECC, notably its ability to maintain stringent security measures with relatively smaller key dimensions, thereby optimizing efficiency without sacrificing the level of security. The integration of ECC with Homomorphic Paillier Encryption facilitates the execution of secure computations on ciphered data, maintaining user privacy while permitting the cloud to perform meaningful data operations. The re-encryption feature of our scheme ensures the secure mobility and modification of data sans decryption, thus augmenting security measures and operational flexibility.

The proposed encryption paradigm has been validated through rigorous theoretical scrutiny and empirical implementation, revealing marked enhancements in both computational efficiency and security measures when juxtaposed with established encryption techniques. The empirical evidence suggests that the streamlined nature of our encryption scheme renders it exceptionally compatible with real-world cloud applications, particularly in scenarios where the optimization of resources is imperative.

This work contributes to the field of cloud data security by providing a scalable, efficient, and secure encryption solution, paving the way for more secure and practical cloud computing applications.

***Keywords: Elliptic Curve Cryptography; Homomorphic Encryption; Paillier Re-Encryption; Cloud data storage, Cloud computing; Cloud Data Security; Lightweight Encryption; Secure Data Computation; Resource-Efficient Cryptography; Python for Cloud; Cyber threats;***

## Introduction

Cloud computing is swiftly gaining traction as a preferred method for data storage and retrieval. However, data security remains a significant concern within this domain [1]. It's a favored choice among businesses, enterprises, and individuals due to its cost-effectiveness, scalability, robust security, and flexibility. Cloud computing enables organizations to tap into extensive computing resources from any global location [2]. Moreover, it facilitates the storage of substantial data volumes, including emails, documents, applications, and complete databases, which can be disseminated across networks in real-time [3]. This capability grants organizations the flexibility to access data and applications from any

place, anytime, proving particularly advantageous for multi-location businesses [4]. Additionally, cloud computing aids in slashing IT infrastructure expenses as the need to invest in and upkeep costly hardware or software is eliminated. It also assures a more secure and dependable setting through the adoption of cutting-edge security protocols and technology [5]. Notably, cloud computing provides scalability, enabling businesses to swiftly and effortlessly augment their IT infrastructure in response to growth requirements [6].

Despite these advantages, cloud computing faces challenges that necessitate attention. Security is a primary issue; data in the cloud is susceptible to cyber threats and breaches, necessitating vigilant protection by users [7]. There's also the risk of data leakage, with the potential for unauthorized access to sensitive information. Another hurdle is scalability; users must be capable of adjusting their cloud storage and computing resources to align with their business's evolving demands [8].

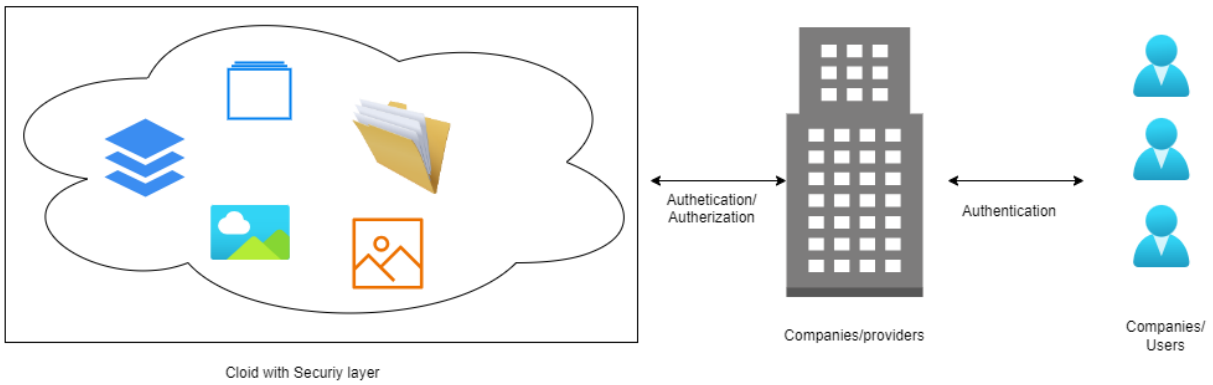
Various methods have been devised to tackle security concerns in cloud computing, encompassing two principal strategies: physical and logical security [9]. Physical security measures include the creation of firewalls to deter unauthorized access, the establishment of secure networks, the implementation of multi-level authentication mechanisms, vigilant monitoring and logging of data access attempts, robust encryption of data, stringent access controls, and the assurance of secure physical locations for servers and data storage [10]. Logical security, on the other hand, pertains to the software and applications utilized in cloud computing. It involves safeguarding data via encryption, bolstering application security, managing identities and access, and employing data loss prevention tactics such as tracking file movements and enforcing security policies to avert data loss [11]. Furthermore, larger corporations are advised to invest in cloud-based security solutions offered by specialized firms, ensuring access to the most advanced and secure support systems. With appropriate security measures in place, cloud computing can be a reliable and secure method for data storage and retrieval.

Cryptography is the art of securing digital communications, information, and data through mathematical and computer science principles [12, 13]. It serves as a vital tool to thwart unauthorized access to sensitive information. Cryptography encompasses algorithms, protocols, and encryption techniques to shield data whether in transit, at rest, or stored in the cloud. It also includes the use of digital signatures and message authentication codes to verify the security and authenticity of message contents [14]. As a cornerstone of cybersecurity, cryptography ensures the confidentiality, integrity, and authenticity of digital information and communications across various applications, including secure web browsing, email encryption, secure online banking, and protected cloud storage [15]. In the ongoing battle against cybercrime, cryptography plays a pivotal role by securing information from unauthorized access. As cyber threats evolve, the importance of cryptography in maintaining the security of networks, systems, and data escalates [16]. Cryptography also provides data authentication and integrity, confirming the sender's identity and the data's unaltered state during transmission. It can protect data from unauthorized access [17], and its encryption algorithms can be refined over time to maintain data security amidst evolving access technologies [18]. Additionally, cryptography can authenticate digital certificates, manage access control, and safeguard messages from alteration. By understanding and implementing these security mechanisms, we can ensure secure communication, storage, and processing of data, thereby shielding it from malicious entities [19]. The cryptographic technique offers robust security coupled with high performance, making it an exemplary choice for users seeking to secure their data [20].

To safeguard data within cloud environments, it is essential to adhere to a set of best practices that mitigate the risk of cyber threats and breaches. These practices include understanding the shared responsibility between cloud providers and customers for security measures; selecting reliable cloud service providers that comply with recognized security standards; employing strong authentication methods like multifactor authentication; encrypting sensitive data both at rest and in transit; securing the network perimeter; managing access through identity and access management systems; maintaining visibility of the cloud security posture; establishing and enforcing cloud security policies; protecting containerized applications; conducting regular vulnerability assessments; adopting a zero-trust security model; performing penetration testing; ensuring compliance with regulatory requirements; having an incident response plan ready; securing all applications; keeping the data security posture in mind; consolidating cybersecurity solutions; and leveraging cloud detection and response strategies. By implementing these practices, organizations can significantly enhance the security of their data in the cloud.

**Figure 1: Explaining the current cloud providers process**

Image designed in : https://app.diagrams.net/




## Related works

Suganya et al. introduced a novel security encryption algorithm for cloud data storage, termed Stochastic Gradient Descent Long Short-Term Memory (SGD-LSTM), which is augmented by the Blowfish encryption technique [21]. The SGD-LSTM classifier is designed to predict and prevent unauthorized access to cloud data. This method operates in three phases: intrusion detection, authentication, and registration, utilizing the Enron Email Dataset for validation. The Blowfish algorithm is employed to ensure that only authenticated individuals can access information within the cloud. However, the key schedule and encryption process are time-intensive, necessitating a longer duration for completion.

Kousalya et al. have enhanced RSA-based Role-Based Access Control (RBAC) using Extendable Access Connectivity Markup Language (XACML) to bolster rights management and data encryption [22]. This approach leverages cryptographic principles and simplifies admission management. The Rivest-Shamir-Adleman (RSA) method provides information protection and anonymity, with RBAC focusing on user identity verification. Nonetheless, this method is characterized by a slow data transfer rate and is not suitable for encrypting public data.

Dawson et al. have implemented the Security of Cloud Data Using the Soldier Ant Algorithm (SAA), which integrates the Diffie-Hellman algorithm with delta encoding techniques [23]. The method begins by generating ASCII values for the alphabets in the plaintext to be transmitted. The Diffie-Hellman algorithm secures the communication channel between the cloud client and service provider, while Newton Backward Interpolation is used to decrypt the cipher text. However, this method is limited to symmetric key exchange and lacks a robust authentication process.

Fatima et al. have developed a Particle Swarm Optimization (PSO) strategy with improved homomorphic encryption to enhance cloud security [24]. The encryption key is refined using the swarm optimization process. This innovative combination of homomorphic encryption and PSO offers a viable solution for key management and sharing, although it results in larger cipher texts and requires additional processing time.

Swathy et al. have introduced Hybrid Cryptography for Cloud Computing Data Security, utilizing both Elliptic Curve Cryptography and the Blowfish algorithm [25]. The Blowfish algorithm encrypts patient data on the primary storage device, while the key is secured using a public key elliptic curve. The processes of key generation, encryption, and decryption are managed by both Blowfish and ECC algorithms. Despite the robust security provided, the encrypted image size is larger, and the implementation is complex, posing challenges for secure deployment within a limited timeframe.

**Table1: It describes the authors' information, the techniques and parameters used by them, and limitations.**

| Sl.No. | AUTHOR'S NAME | TECHNIQUE USED | PARAMETRS USED | LIMITATIONS |
|---|---|---|---|---|
| 1 | Suganya et.al [21]. | SGD-LSTM | Decryption time, Encryption, accuracy, f-score, f-score, precision, recall, f-score, accuracy, and RMSE. | Long time period, Slow process. |
| 2 | Kousalya et.al [22]. | RBAC | Key size, Encryption time, Decryption time, Execution time and Throughput. | Slow data transfer rate, Can't use for public data encryption. |
| 3 | Dawson et.al [23]. | SAA | Encryption time, Decryption time and Execution time. | Lack of authentication procedure, Long time period. |
| 4 | Fatima et.al [24]. | Homomorphic encryption, PSO | Execution time and Utilization of Resource. | Cipher texts are much larger than the plain texts, More time period. |
| 5 | Swathy et.al [25]. | ECC and Blowfish algorithm | Encryption time and Decryption time. | Encrypted data size is bigger, More complicate to implement. |

**Motivation and problem statement**

In today's digital landscape, cloud data security has become increasingly critical as a multitude of companies and individuals shift towards remote computing solutions. Effective cloud data protection necessitates diligent monitoring to identify and rectify system vulnerabilities promptly. A key hurdle is ensuring secure data access; thus, implementing robust authentication protocols is vital to restrict data access to authorized users only. Additionally, safeguarding data against external threats is imperative, requiring organizations to formulate and uphold a comprehensive IT security policy to guarantee the safety of cloud-stored data.

As cloud data security continues to advance, it is crucial for organizations to stay alert to protect their data proactively. Engaging external cloud vendors elevates security risks, but the adoption of lightweight cryptography can significantly bolster cloud data security. This encryption technique renders data indecipherable to unauthorized parties, adding a crucial layer of defense, particularly for data at rest. It also facilitates secure online access and sharing of information. Moreover, lightweight cryptography enables businesses to authenticate and manage user roles effectively in the cloud, ensuring appropriate permissions and privileges, thereby enhancing both security and reliability.

Given the surge in cloud computing usage, encrypting data is now a fundamental aspect of securing it across cloud platforms. Lightweight cryptography emerges as a practical and dependable method for data protection. Hence, the advocacy for lightweight cryptography is driven by its potential to fortify cloud data security substantially.

## Objectives

The major objectives of the proposed work are,

- To introduce a new multi-objective optimization algorithm for generating suitable keys for the encryption process.
- To propose a Lightweight Elliptic Curve assisted Homomorphic Paillier Re-Encryption (LEC_HPRE) approach for performing dual encryption process to afford security to the private input data.
- To enhance the confidentiality of each input data, cloud storage is performed and the private data is accessed by enabling decryption process using private keys.
- To validate the performance of proposed study by evaluating varied metrics and the achieved results are compared with other existing methods for proving the efficacy of proposed study.

## Proposed Methodology

Cloud computing represents the forefront of data storage and application execution, offering users a virtually limitless processing capacity. Its benefits include seamless accessibility, scalability, and the sharing of resources. Despite cloud storage's evolution into a sophisticated service model, its adoption by entities such as businesses and individuals is hindered by concerns regarding the privacy of sensitive data. Previous studies have introduced various security mechanisms, yet they fall short due to inherent limitations. Consequently, this study proposes a robust solution designed to fortify cloud security through optimized key generation coupled with a Lightweight Homomorphic Cryptographic Algorithm.

The methodology of the proposed research encompasses several stages: data acquisition, optimal key generation, lightweight encryption, cloud storage, and decryption. The process begins with the generation of random input data for cloud outsourcing. To enhance the efficacy of the encryption, keys are optimally selected using a novel Multi-Objective Osprey Algorithm (MO_OA). This algorithm fine-tunes parameters such as the degree of modification, hiding ratio, and information security ratio to derive the most effective keys. These keys are then employed in the proposed Lightweight Elliptic Curve assisted Homomorphic Paillier Re-Encryption (LEC_HPRE) method. Initially, Elliptic Curve Cryptography (ECC) is applied to encrypt the data, followed by a re-encryption using the Paillier cryptographic algorithm. This dual-layer encryption significantly increases the security of the private input data before it is stored in the cloud. Access to the private data is subsequently granted through a decryption process utilizing the private key generated by the proposed method.

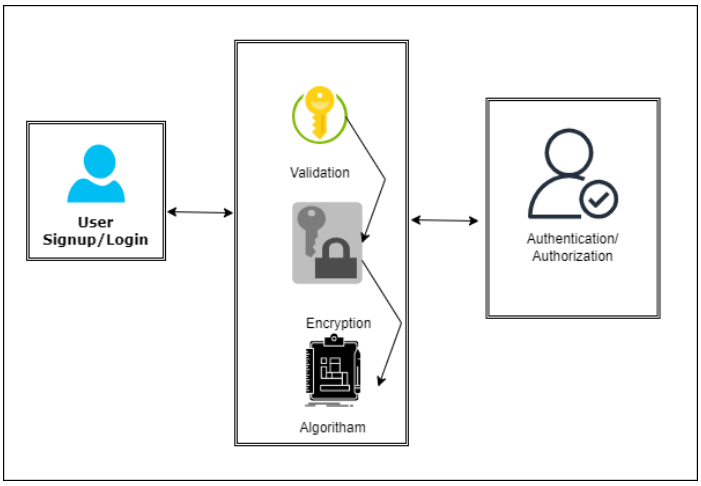



**Figure 2: Proposed validation layer**

### Expected outcomes

The performance of the proposed system is rigorously assessed through a comprehensive evaluation of metrics such as encryption time, decryption time, computational overhead, and network throughput. The system's efficiency is further substantiated by benchmarking its results against those of established methodologies.

### Implementation tool:

Python - Python has been chosen as the programming language for the proposed project due to its numerous strengths that cater to the development of complex security systems. Its user-friendly syntax ensures a smooth development process, while its extensive libraries, such as `PyCrypto` and `PyCryptodome`, provide a wealth of pre-built functions for cryptographic operations. The language's platform independence allows for deployment across various systems, and its scalability means it can handle growing data demands efficiently. Additionally, Python's strong community support

offers a rich resource for developers to draw upon during the project lifecycle. These attributes make Python an optimal choice for implementing the advanced security features required for protecting data in cloud computing environments.

## References


1. George, A. Shaji, and S. Sagayarajan. "Securing Cloud Application Infrastructure: Understanding the Penetration Testing Challenges of IaaS, PaaS, and SaaS Environments." *Partners Universal International Research Journal* 2, no. 1 (2023): 24-34.
2. Tank, Birju, and Vaibhav Gandhi. "A Comparative Study on Cloud Computing, Edge Computing and Fog Computing." (2023).
3. Atiq, Haseeb Ullah, Zulfiqar Ahmad, Sardar Khaliq Uz Zaman, Muhammad Amir Khan, Asad Ali Shaikh, and Amal Al-Rasheed. "Reliable resource allocation and management for IoT transportation using fog computing." Electronics 12, no. 6 (2023): 1452.
4. Lee, Tian-Fu, Kun-Wei Lin, Yi-Pei Hsieh, and Kuo-Chang Lee. "Lightweight Cloud Computing-Based RFID Authentication Protocols Using PUF for e-Healthcare Systems." IEEE Sensors Journal 23, no. 6 (2023): 6338-6349.
5. Telo, Joan. "Smart City Security Threats and Countermeasures in the Context of Emerging Technologies." International Journal of Intelligent Automation and Computing 6, no. 1 (2023): 31-45.
6. Razi, Mohammed, and Ali Batan. "Opportunities and Challenges of Cloud Computing in Developing Countries." Artificial Intelligence in Society 3, no. 1 (2023): 1-8.
7. Akbar, Hussain, Muhammad Zubair, and Muhammad Shairoze Malik. "The Security Issues and challenges in Cloud Computing." International Journal for Electronic Crime Investigation 7, no. 1 (2023): 13-32.
8. Guo, Jian, and Hua Guo. "Real-Time Risk Detection Method and Protection Strategy for Intelligent Ship Network Security Based on Cloud Computing." Symmetry 15, no. 5 (2023): 988.
9. Venkatesan, Srinath, Julio César Moyano Alulema, Ángel Geovanny Guamán Lozano, and Jhonny Marcelo Orozco Ramos. "Modeling Software Architecture Design on Data Storage Security in Cloud Computing Environments." Journal of Survey in Fisheries Sciences 10, no. 3S (2023): 5387-5395.
10. Semantha, Farida Habib, Sami Azam, Bharanidharan Shanmugam, and Kheng Cher Yeo. "PbDinEHR: A Novel Privacy by Design Developed Framework Using Distributed Data Storage and Sharing for Secure and Scalable Electronic Health Records Management." Journal of Sensor and Actuator Networks 12, no. 2 (2023): 36.
11. Gousteris, Solonas, Yoannis C. Stamatiou, Constantinos Halkiopoulos, Hera Antonopoulou, and Nikos Kostopoulos. "Secure distributed cloud storage based on the blockchain technology and smart contracts." Emerging Science Journal 7, no. 2 (2023): 469-479.
12. Liang, Wei, Yongkai Fan, Kuan-Ching Li, Dafang Zhang, and Jean-Luc Gaudiot. "Secure data storage and recovery in industrial blockchain network environments." IEEE Transactions on Industrial Informatics 16, no. 10 (2020): 6543-6552.
13. Ramachandra, Mohan Naik, Madala Srinivasa Rao, Wen Cheng Lai, Bidare Divakarachari Parameshachari, Jayachandra Ananda Babu, and Kivudujogappa Lingappa Hemalatha. "An efficient and secure big data storage in cloud environment by using triple data encryption standard." Big Data and Cognitive Computing 6, no. 4 (2022): 101.
14. Ren, Yongjun, Yan Leng, Yaping Cheng, and Jin Wang. "Secure data storage based on blockchain and coding in edge computing." Math. Biosci. Eng 16, no. 4 (2019): 1874-1892.
15. Prajapati, Priteshkumar, and Parth Shah. "A review on secure data deduplication: Cloud storage security issue." Journal of King Saud University-Computer and Information Sciences 34, no. 7 (2022): 3996-4007.
16. Sajid, Faiqa, Muhammad Abul Hassan, Ayaz Ali Khan, Muhammad Rizwan, Natalia Kryvinska, Karovič Vincent, and Inam Ullah Khan. "Secure and efficient data storage operations by using intelligent classification technique and RSA algorithm in IoT-based cloud computing." Scientific Programming 2022 (2022): 1-10.
17. Rajeh, Wahid. "Hadoop distributed file system security challenges and examination of unauthorized access issue." Journal of Information Security 13, no. 2 (2022): 23-42.

18. Achar, Sandesh. "Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in our Modern Threat Landscape." International Journal of Computer and Systems Engineering 16, no. 9 (2022): 379-384.
19. Shabaz, Mohammad. "A secure two-factor Authentication framework in cloud computing." Security and Communication Networks 2022 (2022).
20. Hammad, Muhammad, Akhtar Badshah, Ghulam Abbas, Hisham Alasmary, Muhammad Waqas, and Wasim Ahmed Khan. "A provable secure and efficient authentication framework for smart manufacturing industry." IEEE Access (2023).
21. Suganya, M., and T. Sasipraba. "Stochastic Gradient Descent long short-term memory based secure encryption algorithm for cloud data storage and retrieval in cloud computing environment." Journal of Cloud Computing 12, no. 1 (2023): 1-17.
22. Kousalya, A., and Nam-kyun Baik. "Enhance cloud security and effectiveness using improved RSA-based RBAC with XACML technique." International Journal of Intelligent Networks 4 (2023): 62-67.
23. Dawson, John Kwao, Ben Beklisi Kwame Ayawli, Sylvester Agyemang, Philemon Baah, and Samuel Akyeramfo-Sam. "Ensuring Cloud Data Security Using the Soldier Ant Algorithm." Journal of Advances in Information Technology 14, no. 1 (2023).
24. Faiz, Mohammad, Nausheen Fatima, Ramandeep Sandhu, Mandeep Kaur, and Vipul Narayan. "Improved Homomorphic Encryption for Security in Cloud using Particle Swarm Optimization." Journal of Pharmaceutical Negative Results (2022): 4761-4771.
25. Chinnasamy, P., S. Padmavathi, R. Swathy, and S. Rakesh. "Efficient data security using hybrid cryptography on cloud computing." In Inventive Communication and Computational Technologies: Proceedings of ICICCT 2020, pp. 537-547. Springer Singapore, 2021.