 ISSN: 2349-6002

Privacy-Preserving Computation Using Homomorphic Encryption in Cloud Computing

Janhvi Mishra
Department of Computer Science, Rajasthan College of Engineering for Women, Jaipur, India

Abstract- Cloud computing has evolved into a key technology supporting modern data-driven systems by offering scalable, flexible, and accessible computational resources. However, delegating sensitive data storage and processing to cloud providers introduces significant privacy concerns, particularly regarding unauthorized access and data exposure. Conventional encryption protects stored and transmitted data, but it requires decryption prior to processing, thereby exposing the plaintext during computation. Homomorphic Encryption (HE) overcomes this limitation by enabling operations to be performed directly on encrypted information without revealing the underlying content.
This paper provides an accessible and structured overview of privacy-preserving computation using HE in cloud environments. It covers the theoretical basis of HE, reviews present HE schemes, and examines their practical viability. A prototype implemented using Microsoft SEAL highlights the advantages, constraints, and performance impact of HE. The paper concludes with optimization approaches and discusses future prospects for real-world adoption.

Keywords: Cloud Computing, Cryptography, Data Security, Homomorphic Encryption, Privacy Preservation

I. INTRODUCTION

Cloud computing has significantly transformed the storage, management, and processing of large-scale data by delivering cost-effective, scalable, and flexible infrastructure. Despite its widespread adoption, maintaining confidentiality of data stored on third-party servers remains one of the primary challenges. Multiple real-world data breach incidents demonstrate the limitations of traditional protection techniques.
Although existing cryptographic solutions secure data during transmission and storage, they require decryption for processing tasks such as analytics, machine learning model training, or database queries. This results in potential exposure of sensitive content to cloud platforms. Homomorphic Encryption (HE), originally conceptualized by Rivest, Adleman, and Dertouzos in 1978, presents a groundbreaking solution by supporting computation over encrypted data. This preserves privacy while enabling meaningful processing. With increasing dependency on digital platforms, secure computation techniques like HE have become essential for future-ready cloud architectures.

II. BACKGROUND AND MOTIVATION

A. Overview of Cloud Computing

According to the National Institute of Standards and Technology (NIST), cloud computing offers on-demand access to shared computing resources such as servers, storage, platforms, and software services. These services are typically categorized into IaaS, PaaS, and SaaS delivery models. While centralizing data in cloud environments provides operational efficiency, it also raises substantial security concerns. As organizations digitize critical data and services, implementing advanced security models becomes increasingly important.

B. Privacy Challenges in the Cloud

Cloud computing environments introduce multiple privacy-related challenges including limited transparency into cloud operations, risk of insider attacks, and vulnerabilities in multi-tenant infrastructures. Additionally, compliance frameworks such as GDPR and HIPAA impose strict requirements for securing personal and sensitive data. This has increased the need for techniques that preserve privacy even while the data is being processed. Therefore, cryptography-based secure computation emerges as a promising solution.

C. Importance of Homomorphic Encryption

Homomorphic Encryption supports encrypted computations such as addition, multiplication, and in some cases, complex algorithms. For example, a healthcare organization could analyze encrypted medical records without exposing patient data. Due to such capabilities, HE is gaining attention across sectors including finance, national security, and cloud-based AI training. As demand grows for privacy-preserving technology, HE is emerging as a crucial component in securing data processing workflows.

III. LITERATURE REVIEW

A. Early Developments

The concept of privacy homomorphisms emerged in 1978, and early cryptographic systems such as RSA and ElGamal supported only partial homomorphic properties (either addition or multiplication). Although not fully practical at the time, these early approaches laid the groundwork for further research.

B. Emergence of Fully Homomorphic Encryption (FHE)

Craig Gentry introduced the first fully homomorphic encryption model in 2009, marking a major milestone in cryptographic research. Despite its theoretical significance, the scheme relied on complex lattice-based operations and bootstrapping, resulting in high computational cost.

C. Modern HE Frameworks

Progress in the last decade has led to several HE libraries including HElib, Microsoft SEAL, and PALISADE. Even though execution speed has improved, computations on encrypted data are still significantly slower compared to plaintext processing.

D. Related Research

Modern research combines HE with secure hardware modules, multiparty computation, and federated learning. Studies involving encrypted AI inference and privacy-preserving big-data analytics show promising progress.

IV. RESEARCH PROBLEM AND OBJECTIVES

A. Problem Statement

Although HE provides a high level of privacy, it also introduces challenges such as computational overhead, large ciphertext sizes, and tuning complexity. These constraints make real-world implementation difficult. Therefore, this research focuses on exploring methods to make HE-based computation practical for cloud systems.

B. Objectives

- Assess available HE frameworks in terms of performance and security.
- Develop a functional model demonstrating encrypted cloud computations.
- Analyze trade-offs involving scalability, usability, and efficiency.
- Suggest improvements for enhancing HE adoption in cloud-based architectures.

V. METHODOLOGY

A. Research Design

This study follows a mixed research methodology involving theoretical study and practical experimentation. A working prototype was implemented to evaluate HE in a real cloud environment.

B. Tools and Frameworks

The experiment utilized Microsoft SEAL (version 4.1), Python programming, C++, and Microsoft Azure compute environment.

C. Experimental Procedure

A dataset was encrypted and transferred to a cloud environment. The cloud executed operations such as summation and averaging directly on the encrypted values. The results were sent back to the client and decrypted for verification.

D. Evaluation Metrics

Evaluation was based on computational performance, storage usage, accuracy, and scalability.

VI. RESULTS AND ANALYSIS

The prototype confirmed that HE-based processing provides correct results but incurs noticeable performance overhead. Optimization strategies such as batching and fine-tuning encryption parameters can help reduce these delays.

Metric	Plaintext	Encrypted (HE)	Overhead
Computation Time	0.12 s	3.87 s	32×
Data Size	2 MB	18 MB	9×
Accuracy	100%	100%	—

VII. DISCUSSION

HE offers strong security benefits, but large computation times currently limit its capability in latency-sensitive systems. Combining HE with solutions such as secure enclaves or GPU acceleration may significantly improve performance. As HE becomes more efficient and user-friendly, adoption is expected to increase across industries requiring strict data confidentiality.

VIII. CONCLUSION

Homomorphic Encryption represents a promising advancement toward secure and privacy-preserving cloud computation. Although its current performance limitations restrict widespread deployment, ongoing research and technological improvements are rapidly closing the gap. With continued optimization, HE may soon become an essential part of scalable and secure data processing systems.

REFERENCES

[1] lbrecht, M., et al. (2021). Homomorphic Encryption Standard. Homomorphic Encryption. org.
[2] Chen, J., Liu, X., & Zhang, Y. (2022). Hybrid privacy-preserving computation using HE and TEE. IEEE Transactions on Cloud Computing.
[3] Gentry, C. (2009). Fully Homomorphic Encryption using Ideal Lattices. Proceedings of STOC.
[4] Halevi, S., & Shoup, V. (2020). HElib – Implementation of Homomorphic Encryption. IBM Research.
[5] Microsoft Research. (2024). Simple Encrypted Arithmetic Library (SEAL).
[6] National Institute of Standards and Technology. (2011). The NIST Definition of Cloud Computing.