International Journal of Computer Science
and Engineering (IJCSE)
ISSN (P): 2278–9960; ISSN (E): 2278–9979
Vol. 14, Issue 1, Jan–Jun 2025; 437–454
© IASET

International Academy of Science,
Engineering and Technology
IASET Connecting Researchers; Nurturing Innovations

HOMOMORPHIC FEDERATION: PRIVACY-PRESERVING COLLABORATIVE LEARNING ACROSS DECENTRALIZED CLOUD NODES

Soham Sunil Kulkarni[1]***, Shivani Inamdar***[2] ***& Prof.(Dr.) Avneesh Kumar***[3]

[1]*University of California, Irvine, CA 92697, United States*

[2]*University of California, Irvine, USA*

[3]*SCAT, Galgotia's University, Greater Noida, India*

ABSTRACT

In the current era of expansive data generation, leveraging this data while ensuring privacy has become paramount, especially in collaborative environments like cloud computing. The concept of federated learning offers a promising solution by enabling multiple decentralized participants to build a common, robust machine learning model without sharing the data itself. However, traditional federated learning still faces significant challenges in terms of privacy and security, particularly against inference attacks and during the aggregation process in the cloud. This paper introduces "Homomorphic Federation," a novel approach that integrates homomorphic encryption (HE) into the federated learning framework to enhance privacy and security in collaborative learning across decentralized cloud nodes.

Homomorphic Federation exploits the potential of homomorphic encryption to perform computations on encrypted data, ensuring that individual data contributions remain confidential throughout the learning process. This method addresses the core vulnerabilities in federated learning by encrypting the model updates sent to the aggregator, which performs the model averaging without ever accessing the unencrypted data. The encrypted aggregated model is then distributed back to the participants for further iterations, preserving the confidentiality and integrity of each participant's data.

Our methodology involves a layered encryption approach tailored to federated learning architectures, with specific emphasis on scalability and efficiency to handle the computational overhead introduced by HE. We also propose an optimized encryption scheme that reduces the size of encrypted payloads, thereby enhancing the practical feasibility of deploying Homomorphic Federation in real-world scenarios.

Through extensive experiments conducted across various decentralized cloud nodes, our results demonstrate that Homomorphic Federation not only achieves comparable accuracy to traditional federated learning models but also significantly enhances data privacy and model security. We analyze the performance impact of integrating homomorphic encryption into federated learning, focusing on computational overhead, communication costs, and model convergence times.

The adoption of Homomorphic Federation can revolutionize privacy-preserving collaborative learning, particularly in sectors like healthcare and finance where data sensitivity is paramount. By enabling secure, private, and efficient collaborative machine learning, Homomorphic Federation holds the potential to foster more widespread adoption of AI across industries while complying with stringent data privacy regulations like GDPR and HIPAA.

This paper contributes to the growing field of secure and private AI by bridging the gap between theoretical encryption techniques and practical, scalable applications in machine learning. It paves the way for future research into more efficient homomorphic encryption techniques and their integration into more complex machine learning and data analytics frameworks.

KEYWORDS: *Homomorphic Encryption, Federated Learning, Privacy-Preserving, Collaborative Learning, Decentralized Cloud, Data Security, Scalable AI, GDPR Compliance.*

Article History

Received: 17 Jan 2025 | Revised: 24 Jan 2025 | Accepted: 31 Jan 2025