Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 8, pp. 2967–2975
DOI : 10.47974/JDMSC-2441

Mathematical foundations of secure AI : Homomorphic encryption for distributed learning systems

Nandini Babbar [†]
Department of IoT and Intelligent Systems
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Amit Kumar Sharma *
Department of Computer and Communication Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Ravindra Kumar Saini [§]
Department of Information Technology
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Neeraj Kumar Verma [‡]
Department of Data Science
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

[†] *E-mail:* nandini.babbar@jaipur.manipal.edu
* *E-mail:* amit.sharma@jaipur.manipal.edu (Corresponding author)
[§] *E-mail:* ravindra.saini@jaipur.manipal.edu
[‡] *E-mail:* neeraj.verma@jaipur.manipal.edu

Abstract

Issues concerning the safety and privacy of facts are heightened with the upward push of new disbursed studying structures like federated getting to know. the extent of computation accomplished on encrypted information would require specific encryption, otherwise referred to as homomorphic encryption (HE) defends towards data decryption dangers. this article investigates how the arithmetic of HE lets in its application inside remote studying architectures. This examination carries superior modular mathematics structures, lattice frameworks, and polynomial encoding at the side of traditional framework HE systems. also, the paintings propose a relaxed structure for dispensed mastering that makes use of HE for version aggregation and personal gradient computation. Sectors forced below strict facts secrecy policies like in non-public healthcare, smart towns, and finance illustrate why those rules enforced look coverage freedom capitalism - why even more is wanted. This look at highlights the particular approaches HE can serve as a policy flexed surveillance capitalism- coverage that will become so much extra surveillance-centric to defend something in covered AI structures, therefore laying a coverage for research directed towards AI that prioritizes person privateness.

Subject Classification: *68T05, 68T07, 68W15, 94A60.*

Keywords: *Homomorphic encryption, Federated learning security, Encrypted computation, Lattice-based cryptography.*

1. Introduction

The emergence of AI technologies in various sectors has delivered out the significance of making sure information privateness and safety which gives privacy eyes alerted paradigms. Federated getting to know and other techniques machine permits cooperative model schooling over decentralized facts resources [1]. Homomorphic encryption (HE) maintains personal data secure while still letting calculations be accomplished on encrypted statistics [2]. For disbursed getting to know, that is very beneficial since it permits secure processing and aggregation of encrypted model updates without requiring decryption [3]. HE supports the development of privacy-preserving artificial intelligence following rules such General Data Protection Regulations (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) [4]. Sophisticated cryptographic ideas—such as polynomial encodings, lattice-based frameworks, and modular arithmetic—form the basis of HE, allowing secure addition and multiplication on encrypted data. Important HE methods include BFV for discrete data, CKKS for real numbers, and Fully Homomorphic Encryption (FHE).

2. Homomorphic Encryption

Homomorphic Encryption—or HE, as its acronym goes—falls under the category of specialized encryption techniques which allow computations to be implemented on ciphertexts, or encrypted data. Different encryption techniques must first decrypt the data before doing any form of calculations, which is very dangerous, especially in cloud or distributed systems. With Homomorphic encryption, calculations can be done on a complete dataset without decryption where only the final answer needs to be decrypted [5]. Figure 1 shows the workflow of the Homomorphic encryption workflow. Processing data like these positions HE as a powerful tool for safe data processing in delicate sectors such as healthcare, banking, and personal data analysis where guaranteed privacy is held paramount [6].

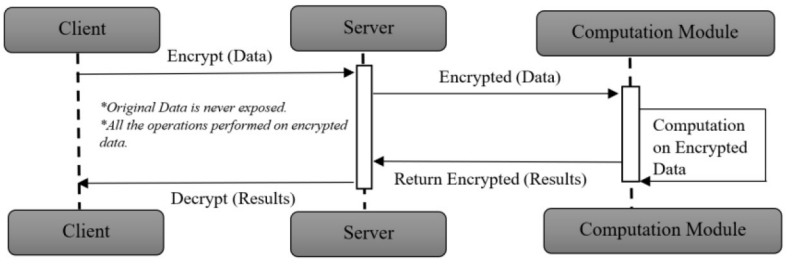

Figure 1

Homomorphic Encryption Workflow

2.1 *Types of Homomorphic Encryption Schemes*

Depending on the complexity and the range of actions they enable on encrypted data, HE systems may be classified into three primary categories:

1. Partially Homomorphic Encryption (PHE): On ciphertext [7], PHE enables one unique operation type: either addition or multiplication. This limitation makes PHE beneficial in specific situations when just one operation is required, such as secure voting or specialised financial applications.

$$\text{Enc}(m_1) + \text{Enc}(m_2) = \text{Enc}(m_1+m_2) \quad (1)$$

$$\text{Enc}(m_1) \times \text{Enc}(m_2) = \text{Enc}(m_1 \times m_2) \quad (2)$$

Enc(m) represents the encryption of a message m.

2. Somewhat Homomorphic Encryption (SHE): While limiting the depth of the computation—that is, the count of operations—SHE improves PHE by allowing a restrained set of operations on encrypted data, generally incorporating both addition and multiplication [8].

$$Enc(m_1) \cdot Enc(m_2) + Enc(m_3) = Enc(m_1 \cdot m_2 + m_3) \quad (3)$$

3. Fully Homomorphic Encryption (FHE): FHE indicates the highest level of innovation in homomorphic encryption, bearing in mind both addition and multiplication operations on ciphertexts with no boundaries [9]. This selection positions FHE as a versatile tool for encrypted computations, allowing a extensive variety of standard-motive operations on encrypted information.

$$Enc(f(m_1, m_2)) = f(Enc(m_1), Enc(m_2)) \quad (4)$$

Enc(m) denotes the encryption of message m.

$f(m_1, m_2)$ is a function applied to the plaintext values m_1 and m_2.

3. Distributed Learning Systems

Distributed learning systems are crucial in enabling the training of large-scale AI models while keeping sensitive information confidential, thus presenting an innovative solution to the problems of data privacy and scalability. Figure 2 shows how federated learning systems worked in the disturbed learning system.

One of the most prominent examples of the distributed learning approach is federated learning, which allows many end devices or clients like mobile phones and IoT devices to collaborate in training machine learning models while keeping their raw data private [10]. Instead, each participant locally modifies the model, and the central server collects these modifications. It is this method which facilitates this form of decentralization [11].

The main reason for doing federated learning is to design a model by collecting data from all the clients without having to aggregate the data in one place [12]. Instead of sending whole data to a centralized server, limited model parameters, normally in the form of gradients or updates, are sent. This greatly enhances privacy and minimizes risk. Every client employs a model on their local data, which the server then averages to enhance the global model. This cyclic procedure increases the model's performance by integrating data from numerous dispersed sources [13].

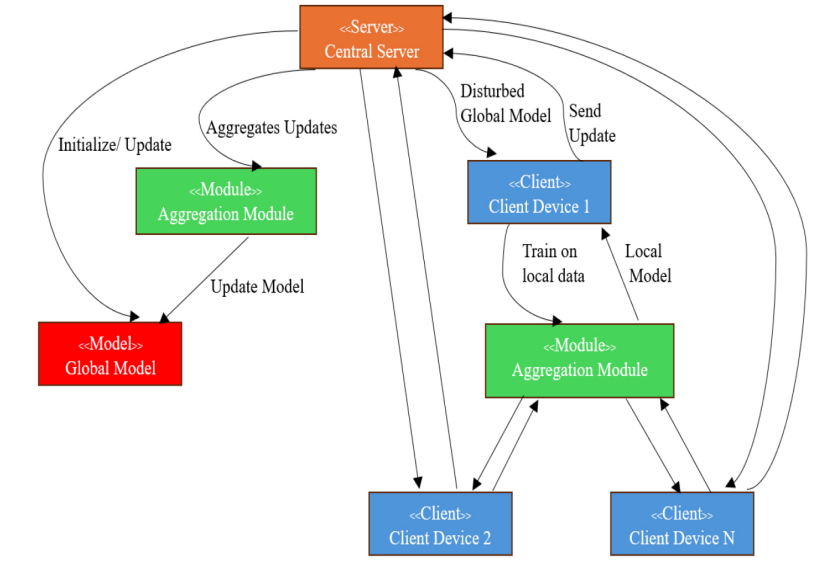

Figure 2

Workflow of Federated Learning in a distributed learning system

4. Integration of homomorphic encryption in distributed learning

By combining hierarchical federated aggregation with adaptive homomorphic encryption (HE), as illustrated in Figure 3, this approach further enhances privacy in distributed learning.

The model designed for "Mathematical Model of Secure AI: Homomorphic Encryption for Distributed Learning Systems" uses homomorphic encryption (HE) for confidential information to protect computational processes. The model defends the primary ideas of secure machine learning in distributed settings. The work explains the importance of keeping data confidential and private throughout the whole machine learning model training process, that is, in the distributed learning.

The loss function is suspected to act naturally by falling and then leveling off after a quadratic curve. R-squared, on the other hand, shows logarithmic growth—the model's correctness improving rapidly before leveling off, representing diminishing returns. Figure 4 presents the loss and R^2 of the suggested model. The final model is parameterized, and R-Squared and Loss behave as expected, thereby satisfying the provided static AI performance metrics of loss and effective AI performance

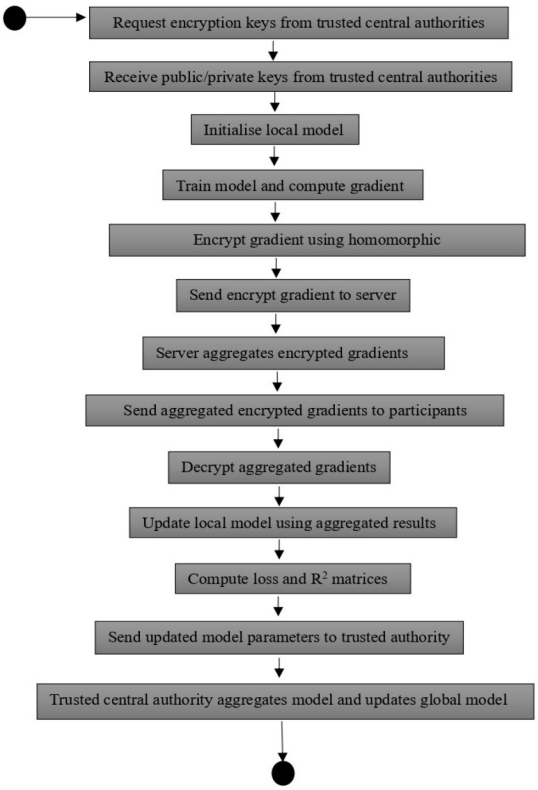

Figure 3

Homomorphic Encryption Distributed Algorithm

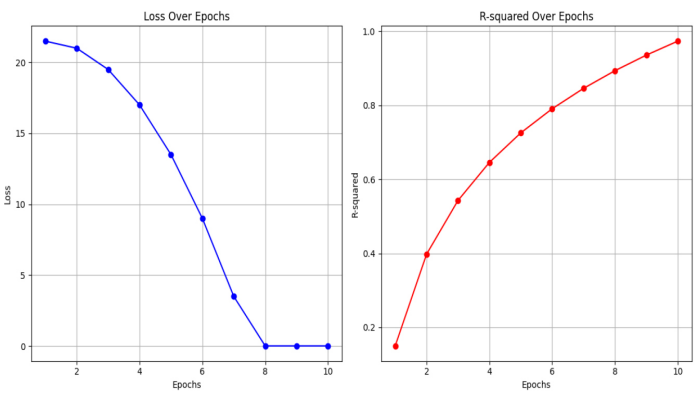

Figure 4

Loss and R^2 values for the proposed model

parameters. The model demonstrates the scope of applying homomorphic encryption to machine learning environments to allow training to be done in a decentralized setting while preserving confidentiality and accuracy.

Security Features of Integrated model

The complete approach includes many powerful security systems to protect your data, improve privacy, and increase the effectiveness of your communications. Data confidentiality relies on homosexual encryption to ensure that gradients are encrypted during the transmission and aggregation stages. Hierarchical aggregation is also used. Initially, it performs aggregation at the cluster level, reducing communication costs before global aggregation. Improve scalability and optimize bandwidth. The idea also allows adaptive clustering, in which real distributed systems can be flexible and resilient. Participant assignments and grouping of changes depend on factors such as participant availability and other network restrictions. Together, these qualities reduce processing and transmission costs and provide a robust learning system for data protection restrictions.

5. Conclusion

In this article, a new framework for distributed learning systems is proposed by using homomorphic encryption to personally retain data over the entire training period. HE protects sensitive information throughout the process, allowing for model training operations and gradient overviews of coded data. This level of data protection appears to be possible in fragmentation and decentralized systems that guarantee the privacy of individual participants' personal data. Various important steps, such as creating local models, implementing local training sessions, encrypting gradients, aggregated encrypted gradients, and updating the model with decryption, are part of the proposed framework. The aggregation method ensures that sensitive data is exposed to participants or servers because it is performed without decrypting the information. According to the results, the model achieves an R^2 value of 97.3 percent after multiple epochs, demonstrating that it can obtain encrypted data while still adhering to strict privacy regulations. This framework offers a practical means of maintaining confidentiality in machine learning, which makes it relevant to situations where data privacy is essential, for instance in the banking, healthcare, and other industries that handle sensitive data.

6. Future Scope

Even if the suggested paradigm significantly improves data security in distributed learning, still there's a scope of upgrading by concentrating on reducing the computational load caused by homomorphic encryption, future implementations may improve efficiency. Adapting privacy techniques that dynamically change the level of encryption, or the type of encryption being used at a given moment, offers the chance for additional study because different applications have varied privacy requirements. Integration with Edge Computing will reduce response time delays and increase the responsiveness of federated learning models.

References

[1] S. X., "Federated learning in edge computing environments: Opportunities, challenges, and future directions," *International Journal of Science and Research (IJSR)*, vol. 13, no. 9, pp. 275–278 (Sep. 2024), doi: 10.21275/es24903163414.

[2] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A survey on homomorphic encryption schemes," *ACM Computing Surveys*, vol. 51, no. 4, pp. 1–35 (Sep. 2018), doi: 10.1145/3214303.

[3] J. Li and H. Huang, "Faster secure data mining via distributed homomorphic encryption," in *Proc. 26th ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining (KDD '20)*, pp. 2706–2714 (Aug. 2020), doi: 10.1145/3394486.3403321.

[4] H. Fang and Q. Qian, "Privacy-preserving machine learning with homomorphic encryption and federated learning," *Future Internet*, vol. 13, no. 4, pp. 94 (Apr. 2021), doi: 10.3390/fi13040094.

[5] A. J. Obaid, "Cutting-edge cryptography and cybersecurity: Innovations and applications," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 5, pp. i–vii (2024), doi: 10.47974/JDMSC-27-5-foreword.

[6] Y. Shoukry, K. Gatsis, A. Alanwar, G. J. Pappas, S. A. Seshia, M. Srivastava, and P. Tabuada, "Privacy-aware quadratic optimization using partially homomorphic encryption," *Oxford University Research Archive (ORA)*, Univ. of Oxford (Dec. 2016), doi: 10.1109/CDC.2016.7799042.

[7] V. D. Gowda, V. Praveena, M. Nagabhushanam, P. S. Kumar, C. Rafael, and D. Pathak, "Homomorphic encryption performance

in secure data processing for machine learning," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 5-A, pp. 1517–1526 (Jan. 2025), doi: 10.47974/JDMSC-2150.

[8] U. Upadhyay, A. Kumar, S. Roy, and U. Rawat, "Balancing innovation and privacy: A machine learning perspective," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 2-B, pp. 547–557 (2024), doi: 10.47974/JDMSC-1877.

[9] C. Ma, J. Li, K. Wei, B. Liu, M. Ding, L. Yuan, Z. Han, and H. V. Poor, "Trusted AI in multiagent systems: An overview of privacy and security for distributed learning," *Proceedings of the IEEE*, vol. 111, no. 9, pp. 1097–1132 (Sep. 2023), doi: 10.1109/JPROC.2023.3306773.

[10] S. Sheela, S. Jyothi, S. Shalini, and L. Anuj, "Federated learning and deep learning-driven adaptive cryptography for context-aware elliptic curve Diffie–Hellman optimization and anomaly-aware key management in next-generation wireless networks," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 5-B, pp. 2151–2161 (Jan. 2025), doi: 10.47974/JDMSC-2431.

[11] Muskan and S. S. Chauhan, "A theoretical approach to find the solution of population-based mathematical model," *Journal of Interdisciplinary Mathematics*, vol. 27, no. 8, pp. 1735–1740 (Jan. 2024), doi: 10.47974/JIM-2035.

[12] S. Truex, N. Baracaldo, A. Anwar, T. Steinke, H. Ludwig, R. Zhang, and Y. Zhou, "A hybrid approach to privacy-preserving federated learning," in *Proc. 12th ACM Workshop on Artificial Intelligence and Security (AISec '19)* (2019), doi: 10.1145/3338501.3357370.

[13] Alavi, Maryam, George M. Marakas, and Youngjin Yoo. "A comparative study of distributed learning environments on learning outcomes." *Information Systems Research*, vol. 13, no. 4 (2002): 404-415, doi: https://doi.org/10.1287/isre.13.4.404.72.

Received January, 2025