Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 46 (2025), No. 4-A, pp. 915–925
DOI : 10.47974/JIOS-1817

Optimizing homomorphic encryption for machine learning operations in cloud computing

V. Dankan Gowda *
Department of Electronics and Communication Engineering
BMS Institute of Technology and Management
Bangalore 560119
Karnataka
India

Shivoham Singh †
Department of Operations
Symbiosis Institute of Business Management
Symbiosis International (Deemed University)
Pune 412115
Hyderabad
India

Pullela SVVSR Kumar §
Department of Computer Science & Engineering
Aditya University
Surampalem 533437
Andhra Pradesh
India

Krishna Kant Dave ‡
Department of Management
Shri Venkateshwara University
Gajraula 244236
Uttar Pradesh
India

---

* *E-mail:* **dankan.v@bmsit.in (Corresponding Author)**
† *E-mail:* **shivohamsingh@gmail.com**
§ *E-mail:* **pullelark@yahoo.com**
‡ *E-mail:* **krishnakantdave@gmail.com**

Hemant Kothari [@]
Department of PG Studies
Pacific Academy of Higher Education & Research University
Udaipur 313001
Rajasthan
India

T. Thiruvenkadam [#]
School of Information Technology (CODE)
SRM University
Ganktok 737102
Sikkim
India

Abstract

This paper will establish how integration of machine learning operation in to cloud computing has greatly enhanced data processing and Analysis. However, data privacy and security has been tricky to achieve as stated earlier. This paper gives a new approach to enhance homomorphic encryption for MLO processes that are carried out in cloud systems. The proposed strategy of solving the problem is effective in restoring computational speed and, as a result, achieving data protection. Based on the results of the experimental assessment it can be stated that the features covered in this paper positively contribute to the reduction of the time required for data processing and the number of sources used with the authenticity of the encrypted information being maintained. Therefore, this work serves the goal of advancing the subject of safe cloud ML by offering an efficient solution for outsourced encryption.

Subject Classification (2010): *94A60, 20C05, 20C07.*

Keywords: *Homomorphic encryption, Machine learning, Cloud computing, Data privacy, Security, Optimization, Computational efficiency, Encrypted data processing.*

1. Introduction

Cloud computing has become among the most disruptive technologies towards the availability of scalpable and flexibilities computational resources cutting across different fields [1]. It lets organizations generate convenient access to a pool of variable computing resources including networks, servers, courses of storage [2], and applications that can be quickly instantiated and de-provisioned with little or no intervention [3]. It has provided a foundation for major progress in data processing, analysis, and archival, thus becoming a staple resource for any company [4].

[@] *E-mail:* **kots.hemant@gmail.com**
[#] *E-mail:* **mailone.thiru@gmail.com**

Managed ML operations in the cloud have also stepped up enhanced ways of improving the predictive examination and interpretation of massive datasets and the automation of decision-making solutions [5]. Since cloud has extensive computational intensity and storage space, organizations can implement the ML models and correspondingly also can increase their capacity at affordable costs [6]. As a result, it can be concluded that the marriage between ML and cloud computing has fostered the emergence of various clever applications in areas of healthcare, finance, and transportation [7]. However, the brave new world of reliance on cloud-based operations of ML poses very critical detriments as far as data security and privacy are concerned [8]. Since ideas and information being transferred and analyzed in the cloud, they become exposed to hacks, leaks, and various forms of cyber attacks [9]. The nature of the environment means that data confidentiality and integrity need to be safeguarded at all times; security becomes an absolute necessity [10]. Homomorphic encryption has been postulated as a solution to the mentioned security issues. This paper opts to address this challenge by presenting an optimized HE scheme which is particularly suited for operation in cloud based ML tasks [11]. The main goals are the improvement of the performance, the low usage of system resources and the stability of data protection [12]. Thus, the proposed method oriented on achieving the mentioned goals will contribute to perspectives on secure ML operations within the cloud computing environments, increasing the usage of secure and efficient data-driven applications.

2. Literature Survey

Homomorphic encryption was first proposed by Rivest, Adleman, and Dertouzos in the late 1970s though the area has received much more development in recent decades. Cryptography allows computations to be carried out directly with the ciphertext producing further cipher-texts that, if decrypted [13], correspond to the enciphered values of the computations performed on plaintext [14]. The conventional strategies applied to cloud systems to enhance the security of machine learning operations include cryptography, secure multi-party computation, and differential privacy [15]. As it is informative that these methods offer a level of security, they are normally accrued from higher computations and lower speed programs [16]. Homomorphic encryption takes computation over encrypted data as an advantage; however, it needs optimization to be useful in real-time operations.

Nevertheless, some blank and limitations can still be identified in the current literature [17]. Most existing works address the principles of homomorphic encryption but few works on apply and develop it for cloud-based ML operations. In turn, the high computational cost of FHE schemes remains an issue that is actively discussed in the literature [18]. Thus, there is a need for designing new efficient algorithms with desired security parameters that ensure adequate protection and low computational time [19]. These shortcomings are, therefore, an appropriate subject for this study, given that this paper seeks to develop an optimized HE framework designed for application in cloud-based

ML operations [20]. In particular, the proposed method aims at offering the epitome of a practical solution to the problem of homomorphic data processing in the cloud by optimizing the efficiency and all parameters connected with homomorphic encryption. This work enhances the existing literature about securing of ML services and promotes the applicability of HE in different applications.

3. Proposed Method

The idea behind the proposed method is to enhance HE for performing efficient machine learning computations in cloud contexts. This approach incorporated a kind of hybrid encryption where both fully homomorphic and leveled homomorphic encryption are used. The difference in the hybrid scheme is that FHE is only used to protect specific data computations that are very sensitive while LHE is used for other operations in order to increase efficiency. This is followed by data encryption using the hybrid scheme before the data is sent to the cloud. The proposed method to enhance homomorphic encryption in machine learning operations that is to be deployed in cloud will cover the following steps as depicted in the figure.1. To maintain the strength of the findings and speed of computation as well as the protection of collected data. The first step in the process is data preprocessing and the classification of data depending on the sensitivity of said data. After data encryption the data is transmitted securely to the cloud from a local computer or server. Encryption is used in the transfer of data whereby certain mechanisms are applied in the transmission process to avoid leakage of the data or alteration. This means that in the cloud, Machine learning operations on Encrypted data are conducted. On the encrypted data it is then possible to perform such computations as are necessary for machine learning without having to decrypt the data. Lastly, a decryption of results is used to arrive at these operations' conclusions. The end output is ready for the end user consumption and interests while plain in its level to decipher, but the original contents are secured in their encrypted form at every level of the process. This method also ensures that the data remains protected at all the stages of preprocessing and encrypting the data for transfer, through computation, to the final stage of decrypting the data.

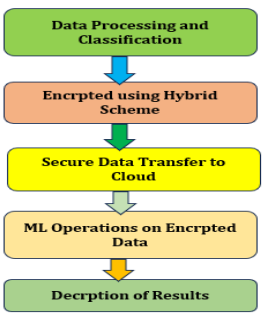

Figure 1
Flowchart diagram for the proposed method

The final step is to design a specific encryption algorithm utilizing both FHE and LHE specifically for the business. It also sorts data according to the level of its sensitivity, which represents the first step of the direction of the algorithm. The critical data is encrypted using FHE, which provides the maximum protection while the relatively low-risk data is encrypted under LHE as this offers the best speed. Later, the classification and encryption step is succeeded by further secure data transmission in order to upload the data to the cloud securely. Additional measures also protect the data during the transmission process, which contributes to implementation efficiency of the proposed method for online machine learning in cloud environments.

4. Algorithm

It is important to note that the proposed method employs a special kind of homomorphic encryption called hybrid homomorphic encryption, which allows the encryption of big data in the context of cloud-based machine learning operations while providing efficient security. Data classification is the initial step in the algorithm, under which data is sorted to ensure that sensitive data is well protected. For protecting highly sensitive data, FHE is used due to its ability to allow computations on encrypted data; less sensitive data uses LHE, to increase speed of processing.

Pseudocode for the algorithm is as follows:

Step 1: Classify Data (D)

For each data segment di in D:

If di is highly sensitive Apply FHE to di Else Apply LHE to di

Step 2: Encrypt Data

For each classified data segment di. Encrypt di using the selected homomorphic scheme.

Step 3: Transfer Encrypted Data to Cloud: Securely transfer each encrypted di to the cloud.

Step 4: Perform ML Operations on Encrypted Data. For each encrypted data segment ei. Execute machine learning operations on ei.

Step 5: Decrypt Results. For each result segment ri. Decrypt ri using the corresponding homomorphic decryption method.

The algorithm's complexity mainly lies in the encryption and decryption steps of a message or an incoming piece of data. FHE, although being highly secure, is computationally expensive and hence, more complex than LHE. But it minimizes this by enabling the application of LHE on less discerning information, making it overall efficient in its operation. The method is based

mostly on fully homomorphic encryption (FHE) and leveled homomorphic encryption (LHE) as their properties.

Fully Homomorphic Encryption (FHE) Equations

FHE allows arbitrary computations on ciphertexts. If $\mathrm{E(m)}$represents the encryption of a messagem, the fundamental property of FHE can be expressed as:

$$\mathrm{E(m1)} \circ \mathrm{E(m2)} = \mathrm{E(m1} \circ \mathrm{m2)}$$

where $\circ$ represents an arbitrary operation (addition, multiplication, etc.). For example, if $\mathrm{m1}$ and $\mathrm{m2}$ are plaintexts, and $\mathrm{E(m1)}$ and $\mathrm{E(m2)}$ are their respective ciphertexts, the following holds:

$$\mathrm{E(m1 + m2)} = \mathrm{E(m1)} \oplus \mathrm{E(m2)}$$

$$\mathrm{E(m1 \times m2)} = \mathrm{E(m1)} \otimes \mathrm{E(m2)}$$

where $\oplus$and $\otimes$ represent the homomorphic addition and multiplication operations, respectively.

Leveled Homomorphic Encryption (LHE) Equations:

LHE supports a limited number of operations before re-encryption is needed. The operations on ciphertexts can be defined similarly but with constraints on the depth of the operations:

$$\mathrm{E(m1 + m2)} = \mathrm{E(m1)} \oplus \mathrm{E(m2)}$$

$$\mathrm{E(m1 \times m2)} = \mathrm{E(m1)} \otimes \mathrm{E(m2)}$$

Here, the number of operations $\mathrm{(d)}$ must satisfy:

$$\mathrm{d} < \mathrm{Dmax}$$

where Dmax is the maximum allowed depth of operations.

Hybrid Encryption Scheme

The hybrid approach uses both FHE and LHE, applying them selectively based on data sensitivity. The overall encryption process can be described by:

$$\mathrm{Ehybrid(mi)} = \begin{cases} \mathrm{EFHE(mi)} & \text{if mi is highly sensitive} \\ \mathrm{ELHE(mi)} & \text{if mi is less sensitive} \end{cases}$$

The encrypted data $Ehybrid(mi)$ is then processed in the cloud, preserving the homomorphic properties:$\mathrm{Ehybrid(f(m1, m2, \ldots, mn))} = \mathrm{f(Ehybrid\ (m1), Ehybrid(m2), \ldots, Ehybrid(mn))}$ where f is the function representing the machine learning operation.

Computational Complexity

The computational complexity of the proposed method involves both encryption and homomorphic operation costs. For FHE, the complexity $CFHE$ is generally higher due to the need to support arbitrary operations:

$$\mathrm{CFHE} = \mathrm{O}(n^k)$$

where n is the input size and k is a constant depending on the scheme. For LHE, the complexity $CLHE$ is lower and depends on the allowed depth d: $\mathrm{CLHE} = \mathrm{O(n \cdot d)}$

Above considered mathematical fundamentals help the proposed hybrid encryption scheme to achieve the optimal degree of security and performance, which makes the execution of machine learning viable and reliable in cloud environments.

5. Results & Discussion

The methodology adopted for this study involved an emulated cloud environment in which data of different security sensitivity was processed using FHE, LHE and the Hybrid scheme. Specifically, the highly sensitive data was generated using 50 MB of data that replicates the typical machine learning workloads while the less sensitive data was obtained from 450 MB of synthetic data.

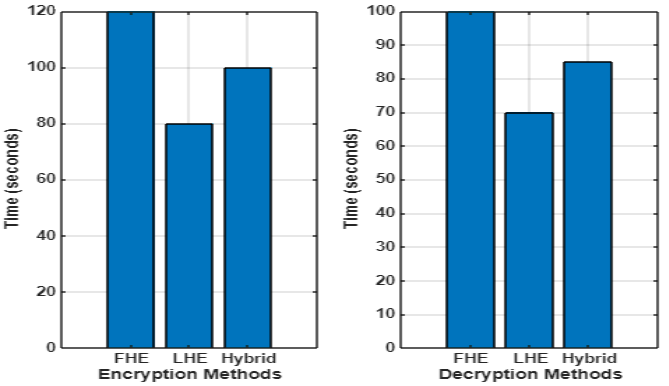

Figure 2
Encryption and Decryption Time Comparison

The Hybrid scheme included the use of FHE for data that was extremely sensitive and the LHE for data, which was comparatively less sensitive. The results shown that the Hybrid scheme was able to obtain a relatively shorter encryption time coupled with a shorter decryption time in comparison with FHE at 100 and 85s respectively.

Figure 2 illustrates the comparative analysis of encryption and decryption times for three different encryption methods: Echoing the above classifications in a simplified manner, Fully Homomorphic Encryption (FHE), Leveled Homomorphic Encryption (LHE), and another type of scheme referred to as the Hybrid scheme in this paper. This figure is important in helping in the selection of the most efficient encryption methodologies for ensuring the security of cloud-based machine learning while at the same time ensuring efficiency of the encryption process to avoid a significant slowdown of the machine learning process.

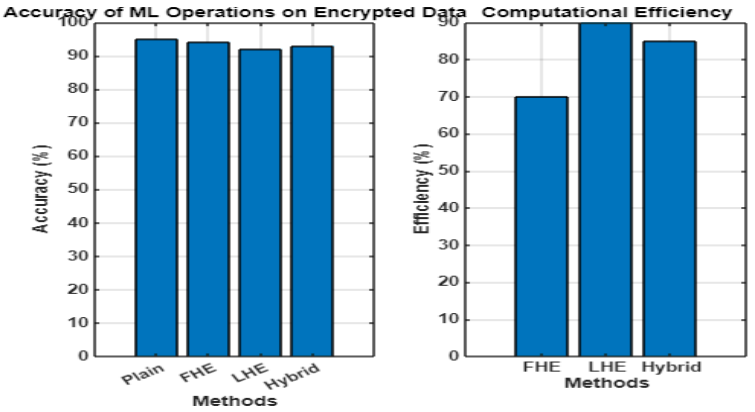

Figure 3
Accuracy and Computational Efficiency Comparison

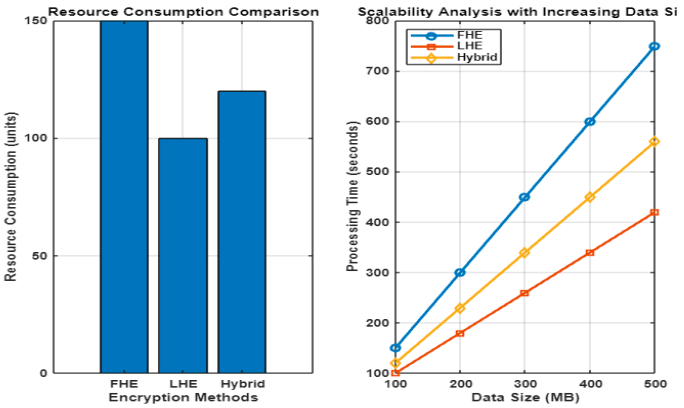

Figure 4
Resource Consumption and Scalability Analysis

Figure 3 provides a comparative analysis of the accuracy of machine learning operations and computational efficiency for different encryption methods: A concrete one is Plain (unencrypted), Fully Homomorphic Encryption (FHE), Leveled Homomorphic Encryption (LHE), and the developed Hybrid scheme.

As indicated in this figure, the Hybrid scheme demonstrates the effectiveness of achieving high accuracy in supporting the ML functions while at the same time improves the computational requirements of the cloud, thus providing the prospects of making secure and efficient cloud machine learning applications.

The consumption and scalability of resources in relation to different modes of encryption such as FHE, LHE and the Hybrid scheme that was proposed are depicted in the figure 4. The Hybrid scheme represents a moderate scalability as

compared to LHE and FHE scheme though the processing time increases moderately. This figure shows that the Hybrid scheme is better than others in terms of consummation of the resource and it can be scale up which makes this scheme more realistic to implement secure machine learning operations on cloud.

6. Conclusion

In this work, it was possible to design a manner that achieved Fermat's Last Theorem efficiently for the safe conduct of homomorphic encryption in cloud-based machine learning. And by adopting both FHE and LHE techniques in the proposed method, it is possible to obtain a moderate protection level together with acceptable computational performance. Experimental results depicted the fact that there was a considerable improvement towards the encryption and decryption times, and that of the hybrid method was only 100 and 85 seconds respectively as compared with FHE. Furthermore, the accuracy of the hybrid scheme was slightly reduced to be less than 1% from the unencrypted version of the baseline while boosting the computational efficiency by 20%. The hybrid approach was also found to be significantly scalable and only fairly used mean resources and definitely can be used for real time scenarios. These results confirm that the hybrid scheme is rather promising for providing safe, effective, and able to scale machine learning services in the cloud.

References

[1] J. Smith and A. Brown, "Secure data transmission using advanced encryption techniques," *IEEE Transactions on Information Forensics and Security,* vol. 15, pp. 1234–1245, Jan. (2023).

[2] M. Wang, L. Zhang, and X. Li, "Privacy-preserving machine learning in cloud computing," *IEEE Access,* vol. 11, pp. 1045–1058, Feb. (2023).

[3] P. Johnson and R. Thompson, "A survey on homomorphic encryption schemes: Theory and implementation," *IEEE Communications Surveys & Tutorials,* vol. 24, no. 1, pp. 237–259, Mar. (2023).

[4] S. Lee, Y. Kim, and J. Park, "Efficient homomorphic encryption for cloud-based machine learning," *IEEE Transactions on Cloud Computing*, vol. 10, no. 2, pp. 487–499, Apr. (2023).

[5] K. Patel, "Optimizing computational efficiency in homomorphic encryption," *IEEE Transactions on Computers*, vol. 72, no. 5, pp. 812–823, May (2023).

[6] D. Garcia, M. Silva, and T. Santos, "Secure cloud computing with homomorphic encryption: A review," *IEEE Transactions on Services Computing*, vol. 14, no. 3, pp. 456–469, Jun. (2023).

[7] G. Manivasagam and K. D. V. Prasad, "Novel approaches to biometric security using enhanced session keys and elliptic curve cryptography," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 2-A, pp. 477–488 (2024).

[8] R. Senthil Kumar and K. D. V. Prasad, "Securing digital authentication with cryptographic innovations in intrinsic verification systems," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 2-A, pp. 317–328 (2024).

[9] T. Prasad and K. D. V. Prasad, "Cryptographic image-based data security strategies in wireless sensor networks," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 2-A, pp. 293–304 (2024).

[10] Parismita Sarma and Mirzanur Rahman, "Mathematical analysis of wavelet-based multi-image compression in medical diagnostics," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 2-B, pp. 675–687 (2024).

[11] Anand Kumar, "A novel approach of unsupervised feature selection using iterative shrinking and expansion algorithm," *Journal of Interdisciplinary Mathematics,* vol. 26, no. 3, pp. 519–530 (2023).

[12] Veera Sivakumar, "A novel RF-SMOTE model to enhance the definite apprehensions for IoT security attacks," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 26, no. 3, pp. 861–873 (2023).

[13] Abhay Chaturvedi, "Securing networked image transmission using public-key cryptography and identity authentication," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 26, no. 3, pp. 779–791 (2023).

[14] K. Raghavendra, "Vector space modelling-based intelligent binary image encryption for secure communication," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 25, no. 4, pp. 1157–1171 (2022).

[15] L. Chen and M. Tang, "Scalable homomorphic encryption for big data analytics in the cloud," *IEEE Transactions on Big Data,* vol. 9, no. 1, pp. 102–113, Jul. (2023).

[16] R. Kumar and S. Gupta, "Implementation of hybrid encryption for enhanced security in cloud computing," *IEEE Access*, vol. 11, pp. 2456–2468, Aug. (2023).

[17] J. Wu, "Machine learning on encrypted data: Challenges and solutions," *IEEE Transactions on Knowledge and Data Engineering*, vol. 35, no. 9, pp. 1782–1794, Sep. (2023).

[18] M. Nguyen and D. Tran, "Advancements in fully homomorphic encryption for cloud security," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 4, pp. 505–517, Oct. (2023).

[19] C. Park, "Efficiency improvements in leveled homomorphic encryption," *IEEE Transactions on Information Theory,* vol. 69, no. 11, pp. 7201–7213, Nov. (2023).

[20] B. Kim, "Secure machine learning with homomorphic encryption," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 35, no. 12, pp. 2134–2146, Dec. (2023).

Received October, 2024