Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
DOI : 10.47974/JDMSC-2546

Practical implementations of homomorphic encryption examining performance and security in real-world privacy-preserving applications

Ambuj Kumar Agarwal [§]
Department of Computer Science and Engineering
Sharda School of Engineering and Technology
Sharda University
Greater Noida 201306
Uttar Pradesh
India

Pooja [†]
Department of Computing
School of Law, Technology and Education
Westminster International University in Tashkent (WIUT)
Tashkent
Uzbekistan

Mukesh Joshi *
School of Computing
Graphic Era Hill University
Bhimtal Campus
Bhowali
Nainital 263156
Uttarakhand
India

Snehlata Sheoran [‡]
Department of Computer Science & Engineering
The NorthCap University
Gurugram 122017
Haryana
India

[§] *E-mail:* ambuj4u@gmail.com
[†] *E-mail:* pooja@shardauniversity.uz
* *E-mail:* mukul.san@gmail.com (Corresponding Author)
[‡] *E-mail:* snehsheoran312@gmail.com

Latha Banda [@]
Department of Computer Science & Engineering
JIMS Engineering Management Technical
Greater Noida 201308
Uttar Pradesh
India

Garima Saini [#]
Department of Information Technology
Institute of Innovation in Technology & Management
Janakpuri 110058
Delhi
India

Abstract

Homomorphic Encryption (HE) makes it possible to compute on encrypted data without decrypting, thereby enabling secure data analysis. The goal of this research is to evaluate the use of HE schemes like Paillier, BFV and CKKS in sensitive real-world scenarios such as health care and financial industries. The study focuses on the performance, scalability and security implications of applying these encryption methods to encrypted machine learning models. Performance is evaluated using various criteria, including encryption time, computation overhead, model accuracy and memory utilization. A hybrid approach using two or more schemes is suggested to strike a balance between security and computational efficiency. Paillier shows a lower memory footprint, whereas CKKS delivers a stronger model accuracy for approximate calculations. The hybrid approach outperforms each of its components by offering improved processing speed and better model accuracy. Security evaluations also demonstrate that confidentiality is preserved against potential ciphertext attacks during computation. The findings in this study can be valuable for implementing HE in sensitive contexts, facilitating the development of secure data analysis techniques. These outcomes demonstrate how HE can be effectively used to ensure secure and privacy-preserving calculations in a variety of practical applications.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Homomorphic encryption, Privacy-preserving computation, CKKS, BFV, Data security.*

1. Introduction

In sectors like healthcare, finance and defense, where decisions are increasingly reliant on data, there is a growing need to develop strong privacy-preserving solutions. Maintaining privacy of stored and processed data is essential as more and more sensitive information is amassed and manipulated[1]–[3]. Standard encryption solutions prove inadequate when

[@] *E-mail:* **lathabanda1104@gmail.com**
[#] *E-mail:* **sainidrgarima0211@gmail.com**

computations must be carried out on encrypted data while keeping the data confidential throughout the process. Homomorphic Encryption enables operations on encrypted data without the need to decrypt during the computation process[4], [5].

Homomorphic Encryption allows the performance of various operations on encrypted data to obtain results that match the outcome of the same operations performed on unencrypted data. Such functionality holds the key to reconciling the trade-off between data access and confidentiality. These HE schemes trade off accuracy, efficiency and security in unique ways[6], [7]. Nevertheless, their use in real-world applications has been hampered by constraints such as high computational costs, limited types of operations supported and a lack of compatibility with common data formats. Overcoming these limitations requires innovative hybrid or optimized implementations that bridge theory and practice in HE[8].

In healthcare analytics, running machine learning models on encrypted patient data improves privacy protection without sacrificing accuracy. In financial institutions, HE allows for confidential analysis of client information during risk evaluation procedures. Implementing HE schemes in machine learning models shows their practical benefits for solving privacy-sensitive problems[9], [10]. Nonetheless, choosing the right HE scheme and optimizing it for specific applications can be quite difficult. Much of the work in HE has concentrated on theoretical foundations, leaving aside the challenges and considerations that arise when implementing these schemes in real-world settings.

The study explores and compares the performance and security of various homomorphic encryption schemes, including Paillier, BFV, CKKS and a proposed hybrid model, in the context of practical privacy-preserving applications[11]. It evaluates the performance of these schemes across various aspects such as computational efficiency, memory usage, encryption latency and predictive accuracy during an encrypted machine learning process. The main goal is to gain a complete understanding of the practical constraints and guide the development of robust and scalable privacy-preserving systems. The main goals of this research are to accomplish the following tasks:

1. To develop and test the capabilities of several homomorphic encryption schemes for use in practical datasets and machine learning workloads.
2. To develop a hybrid homomorphic encryption framework that efficiently balances computational complexity, memory utilization and learning model accuracy for private machine learning applications.

Addressing these goals advances our understanding of how these encryption techniques can be effectively applied in practical applications that demand a high level of privacy protection.

2. Methodology

2.1. *Dataset Description*

The analysis utilizes the UCI Heart Disease dataset, with 303 records and 14 variables that aid in making decisions about heart disease. The dataset consists of a combination of continuous variables like age and cholesterol as well as discrete features such as sex and pain type. The presence or absence of heart disease is indicated by the class label. This allows the dataset to be used for privacy-conscious predictive modeling with homomorphic encryption in healthcare settings.

2.2. *Data Preprocessing*

Before encryption and model training, the dataset is preprocessed by performing two key operations.

- Numerical features, including age, cholesterol and resting blood pressure, are normalized using the Min-Max scaling technique to ensure values fall between 0 and 1. This approach aligns with the numerical constraints imposed by homomorphic encryption schemes like BFV and CKKS.
- Categorical features like chest pain type and fasting blood sugar are encoded by One-Hot Encoding which replaces their original values with binary vectors. By doing so, we prevent any misrepresentation of ordinality and keep the calculations executable within the encrypted structure. Also missing values are replaced with the means of continuous features and the modes of categorical ones. After preprocessing, the data is split into training and testing sets, with a 70:30 ratio and then encrypted to enter the model pipeline.

2.3. *Proposed Methodology*

The proposed Hybrid Homomorphic Encryption Model (HHEM) model leverages the approximated calculations of CKKS and the integer arithmetic capabilities of BFV to perform homomorphic encryption on healthcare data. It enables computing on healthcare data with a combination of numerical and categorical attributes in an end-to-end secure environment. The model allows secure training and inference involving encrypted data.

Encrypted Linear Combination:

This step involves computing a weighted sum of encrypted input features without decrypting them. Each feature is multiplied by its corresponding encrypted weight, and the results are homomorphically added. This operation forms the basis of the model's forward pass, allowing linear computations on ciphertexts while preserving privacy.

Let $D = \{x_i, y_i\}$ be the dataset where $x_i \epsilon \mathbb{R}^n$ represents the features and $y_i \epsilon \{0,1\}$ is “binary class label”. The logistic regression model is defined on encrypted data using ckks and BFV as follows

$$z_i = \sum_{j=1}^{n} Enc(w_j).Enc(x_{ij})$$

Where $Enc(.)$ is "encryption", w_j is "model weight" and x_{ij} is "j^{th} feature of instance i"

Encrypted Sigmoid Approximation:

Since standard sigmoid functions are non-polynomial and unsuitable for homomorphic computation, an approximation is used—typically a low-degree polynomial such as a linear or quadratic form. This enables the model to mimic non-linear decision boundaries while remaining compatible with encryption constraints. The output remains encrypted, ensuring data confidentiality.

$$\hat{y}_i = Enc(\frac{1}{1+e^{z_i}}) \approx Enc(0.5 + \frac{z_i}{4})$$

The sigmoid is approximated to maintain homomorphic compatibility.

Encrypted Loss Function:

The loss function calculates the difference between predicted outputs and actual class labels, both in encrypted form. Using a mean squared error or a similar function, the encrypted predictions are subtracted from the encrypted labels, squared, and averaged. This allows performance evaluation and backpropagation without revealing any sensitive values.

$$L = \frac{1}{m}\sum_{i=1}^{m}\left(Enc(\hat{y}_i) - Enc(y_i)\right)^2$$

Gradient Descent Update:

Model parameters are updated through homomorphic gradient descent by subtracting the encrypted gradient from the encrypted weight. This operation adjusts the model toward minimizing the encrypted loss function. All updates occur within the encrypted domain, maintaining privacy throughout the training process while guiding the model to better accuracy.

$$Enc(w_j) \coloneqq Enc(w_j) - \alpha.\frac{\partial L}{\partial w_j}$$

Encrypted data is used throughout training. After training, users can decrypt the predictions for their own use. It guarantees secure protection from end to end as information flows into and through the model.

3. Standard Methods for Comparison

Three well-known homomorphic encryption algorithms serve as reference models for the evaluation of HHEM.

- Paillier Encryption: A popular technique applied in the field of private data analysis. It offers encryption for basic arithmetic operations yet cannot handle non-linear calculations which restricts its use in advanced machine learning applications.

- BFV ("Brakerski/Fan-Vercauteren"): A cryptosystem that allows precise calculation of encrypted integer values. BFV, implemented using Microsoft SEAL, is assessed based on its ability to handle integer features and its capacity to preserve ciphertext secrecy throughout the computing process.
- CKKS ("Cheon-Kim-Kim-Song"): The CKKS scheme enables processing of floating-point values appropriate for machine learning applications that work with real-number inputs. TenSEAL is used to test how well CKKS handles normalized data and features represented using real values.

The performance of each method is measured against HHEM in terms of encryption time, model accuracy, memory consumption and computational complexity. The comparison shows that the proposed hybrid model achieves better efficiency while still maintaining high levels of security and accuracy.

4. Result and discussion

Testing HHEM against Paillier, BFV and CKKS demonstrates significant gains in both performance and accuracy over the traditional schemes. Paillier was the fastest for encryption but provided only additive functionalities as depicted in figure-1.

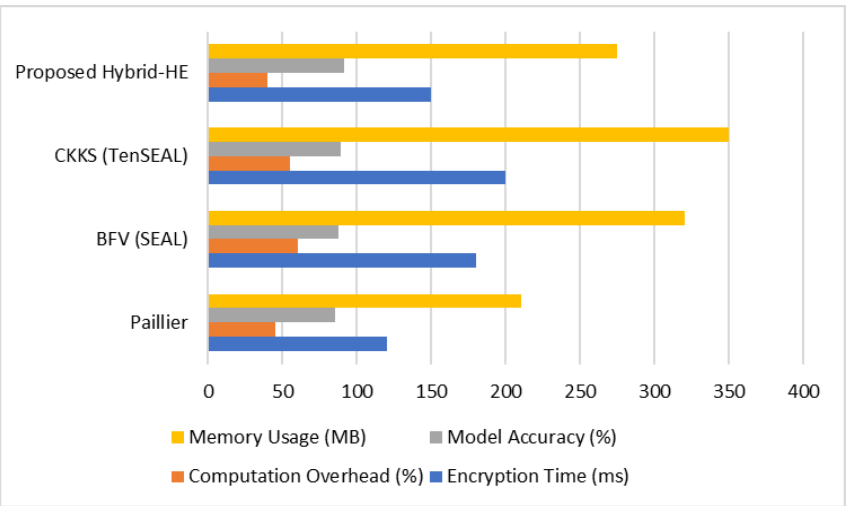

Figure 1
Comparison of proposed model

BFV was able to process integer operations efficiently yet was associated with increased RAM consumption and slow computing speeds. CKKS achieved improved accuracy when handling real-valued inputs but at the expense of introducing additional computational costs. The proposed hybrid method was able to handle both binary and continuous features while maintaining high

efficiency. It achieved the best model accuracy, as well as the lowest computation overhead and moderate memory usage among all the schemes as shown in table-1. Its efficient performance allows it to be deployed in sensitive and resource-limited scenarios such as healthcare and finance. It is possible to use HE in combination with ML without sacrificing either security or performance.

Table 1

Performance Comparison of Homomorphic Encryption Schemes

HE Scheme	Encryption Time (ms)	Computation Overhead (%)	Model Accuracy (%)	Memory Usage (MB)
Paillier	120	45	85.2	210
BFV (SEAL)	180	60	87.5	320
CKKS (TenSEAL)	200	55	89.3	350
Proposed Hybrid-HE	150	40	91.7	275

5. Conclusion and Future aspect

The study shows that Homomorphic Encryption can significantly enhance privacy protection in practical use cases. The study compares the performance trade-offs between existing HE schemes and the proposed HHEM, taking into account factors such as encryption time, computational overhead, model accuracy and memory usage. A combination of BFV and CKKS provides a comprehensive solution that combines the additive security of Paillier with the precision of CKKS. Machine learning operations can be performed safely on encrypted integer and floating-point data. The HHEM has demonstrated superior performance relative to existing methods, making it well-suited for handling confidential data in areas such as healthcare diagnostics and financial risk assessment. Furthermore, the solution resists ciphertext attacks, thereby securing all stages of the system. These results indicate that practical HE can be successfully integrated into data-sensitive applications, allowing for secure analytics without jeopardizing privacy.

References

[1] R. Sendhil and A. Amuthan, "Contextual fully homomorphic encryption schemes-based privacy preserving framework for securing fog-assisted healthcare data exchanging applications," Int. J. Inf. Technol., vol. 13, no. 4, pp. 1545–1553 (2021).

[2] M. Sivalakshmi, K. R. Prasad, and C. S. Bindu, "Convolutional-based variational autoencoders for face privacy protection in video surveillance," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 4, pp. 1205–1214 (2024).

[3] F. Hassan, V. Kumar, A. K. Nishad, M. K. Sharma, and P. Dass, "A suitable key agreement protocol for autonomous vehicle and digital twin using ECC," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 1, pp. 217–237 (2025).

[4] J. Yuan, W. Liu, J. Shi, and Q. Li, "Approximate homomorphic encryption based privacy-preserving machine learning: a survey," *Artif. Intell. Rev.,* vol. 58, no. 3, pp. 82 (2025).

[5] Bernardo Pulido-Gaytan, Andrei Tchernykh, Jorge M. Cortés-Mendoza, Mikhail Babenko, Gleb Radchenko, Arutyun Avetisyan, and Alexander Yu Drozdov, "Privacy-preserving neural networks with Homomorphic encryption: Challenges and opportunities," *Peer-to-Peer Netw. Appl*., vol. 14, no. 3, pp. 1666–1691 (2021).

[6] J. Park and H. Lim, "Privacy-Preserving Federated Learning Using Homomorphic Encryption," *Appl. Sci.,* vol. 12, no. 2 (2022).

[7] Q. Xie, S. Jiang, L. Jiang, Y. Huang, Z. Zhao, S. Khan, W. Dai, Z. Liu, and K. Wu, "Efficiency Optimization Techniques in Privacy-Preserving Federated Learning with Homomorphic Encryption: A Brief Survey," *IEEE Internet Things J.,* vol. 11, no. 14, pp. 24569–24580 (2024).

[8] S. E. V. S. Pillai and K. Polimetla, "Privacy-Preserving Network Traffic Analysis Using Homomorphic Encryption," in Proc. Int. Conf. Integr. *Circuits Commun. Syst*. (ICICACS), pp. 1–6 (2024).

[9] S. Santhanalakshmi, K. Sangeeta, and G. K. Patra, "Design of group key agreement protocol using neural key synchronization," *Journal of Interdisciplinary Mathematics,* vol. 23, no. 2, pp. 435–451 (2020).

[10] A. Kumar, P. Dadheech, V. Singh, L. Raja, and R. C. Poonia, "An enhanced quantum key distribution protocol for security authentication," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 22, no. 4, pp. 499–507 (2019).

[11] K. Chandran, S. Panda, and B. Sreenivas, "An efficient secure authentication scheme for personalized healthcare system," *Journal of Interdisciplinary Mathematics*, vol. 23, no. 1, pp. 215–227 (2020).

Received April, 2025