A Privacy-Preserving Federated Learning Method with Homomorphic Encryption for Chronic Kidney Disease Stage Prediction

M. Gayathri Hegde
Department of CSE, University Visvesvaraya College of Engineering, Bangalore University, Bangalore, Karnataka, India
gaya3kamath@gmail.com(corresponding author)

B. Ruthvika
Department of ISE, JSS Academy of Technical Education, Bangalore, Karnataka, India
ruthvikab2004@gmail.com

Ruthu B. Jain
Department of ISE, JSS Academy of Technical Education, Bangalore, Karnataka, India
ruthujain04@gmail.com

P. Deepa Shenoy
Department of CSE, University Visvesvaraya College of Engineering, Bangalore University, Bangalore, Karnataka, India
shenoypd1@gmail.com

K. R. Venugopal
Department of CSE, University Visvesvaraya College of Engineering, Bangalore University, Bangalore, Karnataka, India
venugopalkr@uvce.ac.in

Arvind Canchi
TrustwellHospitals, Bangalore, Karnataka, India | SagarHospitals, Bangalore, Karnataka, India
canchi8@gmail.com

Received: 5 May 2025 | Revised: 27 May 2025 and 9 June 2025 | Accepted: 15 June 2025

 DOI: https://doi.org/10.48084/etasr.11928

ABSTRACT

Federated Learning (FL) enables collaborative model training across decentralized healthcare institutions without requiring the sharing of Electronic Healthcare Records (EHRs), thereby ensuring data locality and reducing privacy risks. In this study, a baseline FL framework was implemented with one central server and four hospital clients, utilizing a real-time Chronic Kidney Disease (CKD) dataset.However, privacy assessments conducted using three simulated adversarial attacks, model inversion, Membership Inference Attacks (MIA), and gradient leakage, revealed significant vulnerabilities in the plain FL setup.To address these vulnerabilities, this work proposes a secure Federated Learning-Homomorphic Encryption (FL-HE) framework that integrates FL with encryption techniques using the TenSEAL library. The proposed FL-HE framework introduces a layer-wise encryption strategy, securing model parameters, bias, and feature normalization, ensuring end-to-end confidentiality. While the integration of HE introduces computational overhead, the FL-HE framework achieves a high prediction accuracy of 98.6%, nearly identical to the 98.7% achieved by the unencrypted FL model. These results underscore the strong privacy-preserving capabilities of the FL-HE framework without compromising the performance of the model, making it suitable for applications like in healthcare, where the privacy of data is of utmost importance.

Keywords-federated learning; homomorphic encryption; electronic health records; privacy-preservation; secure model aggregation

I. INTRODUCTION

The digitization of healthcare data has accelerated significantly following the COVID-19 pandemic, transitioning from paper-based patient records to Electronic Healthcare Records (EHRs) [1]. EHRs have become a primary resource for developing Machine Learning (ML) models aimed at disease diagnosis, predictive analytics, and personalized treatment in modern healthcare systems.However, training such models often requires aggregating data from multiple hospitals onto a centralized server, which introduces several challenges:i)regulatory barriers, including compliance with Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR); ii) privacy risks, as centralized storage increases the potential for data breaches; and iii) data heterogeneity, which may lead to biased models and poor generalization due to limited diversity across centralized datasets.

The sensitivity and legal constraints surrounding EHRs hinder centralized data sharing, prompting the development of privacy-preserving ML methods such as Federated Learning (FL). In FL, participating hospitals collaboratively train ML models without exposing raw EHR data; only encrypted model updates (e.g., gradients or weights) are exchanged.However, even though the raw data remains on the local hospital server, recent research has raised the risk of privacy leakages through reverse engineering approaches such as gradient inversion attacks, in which the EHR data can be constructed from the shared updates, resulting in a serious threat to patient confidentiality.

To address this, researchers have explored secure extensions to FL, such asDifferential Privacy (DP)[2], Paillerencryption technique[3], Secure Multiparty Computation (SMPC)[4], and Homomorphic Encryption (HE)[5] techniques. Each technique presents unique trade-offs regarding scalability, security, and practicality in real-world applications like finance [6], air quality forecasting [7], and computer vision [8]. Other techniques, such as Spectrasave Encryption (SE) with dynamic k-anonymity [9], Spectrasave Encryption-Dynamic ℓ-Diversity Anonymity (SE-DℓDA) for secure multiparty computation [10], and entropy-based multi-scheme Fully Homomorphic Encryption (FHE) with Rivest Shamir Adleman (RSA) [11], further underscore the number of alternative approaches for safeguarding data in cloud-enabled or distributed healthcare settings.Among these techniques, FL with HE strikes a practical balance between security, computational feasibility, and model utility. Thus, this study proposes a Federated Learning with Homomorphic Encryption (FL-HE) framework tailored for Chronic Kidney Disease (CKD) stage classification.In this framework, clients encrypt their model updates using a HE scheme before transmitting them to a central server.The server, in turn, performs secure aggregation on these encrypted updates and transmits the aggregated model (after decryption) back to the clients. This process repeats over multiple communication rounds, ensuring end-to-end protection of model parameters throughout training.This work's key contributions are:

- Design of an FL-HE framework for secure and accurate classification of CKD stages (1–5), preserving patient confidentiality through encrypted parameter sharing.
- Introduction of a secure global normalization protocol to compute feature-wise mean and variance without disclosing raw client statistics.
- Development of a resource-efficient encrypted aggregation mechanism optimized for clinical parameters, reducing per-round encryption overhead.
- Clinical validation using real-world patient data from The Bangalore Hospital, Karnataka, India, achieving 98% global accuracy while maintaining full HIPAA compliance.

These contributions bridge the gap between cryptographic privacy and practical Artificial Intelligence (AI) deployment in healthcare.

II. RELATED WORK

Table I explores the rapidly growing realm of integrating FL with privacy-preserving techniques in healthcare settings. These studies aim to balance data utility with rigorous privacy guarantees.

Although FL inherently reduces privacy risks by retaining data locally, it remains susceptible to inference attackssuch as gradient leakage, model inversion, and Membership Inference Attacks (MIA), through shared model updates. DP and SMPC, while offering strong privacy guarantees, often compromise on scalability, efficiency, or accuracy. Furthermore, most HE-based approaches overlook vulnerabilities in preprocessing stages, such as feature normalization, and lack real-world deployment evidence.

III. METHODOLOGY

Recent research in federated environments has introduced performance-optimized architectures such as embedding-based learning for intelligent data partitioning [27] and query expansion techniques to improve federated search accuracy [28]. Drawing inspiration from these approaches, our architecture supports both local client-level computation and central secure aggregation, tailored for clinical model training and deployment.

A. Dataset Description

The dataset used in this study was collected from the Bangalore Hospital, located in Bangalore, Karnataka, India. After preprocessing steps described in [29], the dataset consisted of399 patient records,17 clinical features, and 1 target variable: CKD stage classification (ranging from Stage 1 to Stage 5).To address the limited sample size and enhance the robustness of the federated learning framework, data augmentation was performed using Gretel.ai, a synthetic data generation platform.

TABLE I. FL AND PRIVACY TECHNIQUES IN HEALTHCARE

Ref.	Privacy Techniques	Key Highlights	Limitations
[12]	Local DP	Clipping and clustering to withstand Byzantine attacks	Noise may affect model accuracy;limited real-world testing
[13]	SMPC+ Blockchain	Verifies model integrity using blockchain	High computational overhead
[14]	DP	Evaluates impact of privacy budget on model accuracy	The privacy budget is inversely proportional to the accuracy
[15]	DP + SMPC	Integrates DP with secure aggregation with ResNet	Scalability issues with huge model sizes increased training time
[16]	HE	Secure aggregation with HE	High computational complexity due to multiplicative depth; slower convergence
[17]	DP	Personalized model voting for heterogeneous FL	Requires precise abstention threshold setting
[18]	Adaptive DP	Uses adaptive ε to balance accuracy and privacy	Limited to binary classification; lacks large-scale validation
[19]	HE	Improved privacy with edge-assisted computation	Network latency synchronization issues
[20]	Distributed HE	Handles data quality issues	Accuracy depends on data quality detection
[21]	SMPC	Secure multi-client fusion with additive sharing client model	Synchronization overhead; lacks fault tolerance
[22]	Personalized DP	Individualizedεsettings for user-level control	Risk of data imbalance; requires tweaking of personalization parameters
[23]	HE + Secret sharing	Robust dual privacy technique	Computationally intensive; increases latency in aggregation
[24]	HE	Enhanced security by re-encryption	Complex Key management; deterioration of performance in large models
[25]	DP +SMPC	Hybrid privacy-preserving AI approach	No implementation or experimental validation provided
[26]	Custom encryption framework	Cryptography with multi-class privacy	High encryption/decryption costs

TABLE II. DATA DISTRIBUTION TO THE SERVER AND CLIENTS

Description	Dataset Size
Client1(Hospital 1)	399
Client 2 (Hospital 2)	500
Client 3 (Hospital 3)	755
Client 4 (Hospital 4)	1,004
Federated Sever	5,000

This process resulted in a synthetic dataset of 5,000 instances that maintained statistical parity with the original dataset.From this augmented dataset, random subsets were allocated to four simulated clients, each representing a distinct hospital, thereby creating a realistic federated learning environment. The full set of 5,000 synthetic instances was retained at the central server for global model evaluation. The distribution of data among the clients is summarized in Table II.

B. Problem Formulation

Table III denotes the notations used in the problem formulation.

TABLE III. NOTATIONS FOR THE PROBLEM FORMULATION

Notations	Description
N	Number of clients participating in FL
D_i	Local dataset at client i
$L_i(w)$	Local loss function at client i
$L(w;(x,y))$	Loss for a sample (x,y) using model w
w^*	Final optimal global model
w^t	Global model at round t
w_i^{t+1}	Local model update at client i at round t
η	Learning rate
SK	Secret key used for decryption
PK	Public key used for encryption
$\frac{Enc()}{Dec()}$	Encryption/Decryption function
c_i^t	Encrypted model update from client i at round t
c_{agg}^t	Aggregated encrypted model from clients at round t
w_{agg}^t	Decrypted aggregated model update at round t
$\oplus$	HE operator
q	Modulus used in encryption schemes to control the numeric range
λ	Security parameter for key generation
m	Plain text model parameter before encryption
e	Noise term added during encryption
x_i	Feature value at client I
μ/σ^2	Mean / Variance of feature values
$\frac{Enc(\mu)}{Enc(\sigma^2)}$	Encrypted Mean / Encrypted Variance of feature value

Consider N clients with local datasets D_i ,where $i = 1,2,\dots N$. The aim is to collaboratively train a global model w^*while preserving privacy usingHE. Instead of sharing raw data, each client transmits encrypted model updates to a central server, which aggregates them without decryption.The objective function for the global model is defined as:

$$w^* = arg\min_w \sum_{i=1}^{N} \frac{|D_i|}{|D|} L_i(w) \quad (1)$$

where $L_i = \frac{1}{|D_i|}\sum_{(x,y)\in D_i} L\big(w;(x,y)\big)$ is the local loss.Thisfederated optimization process proceeds over$T$communication rounds.

C. HE Scheme for Sharing Model Parameters

This study adopts the Cheon–Kim–Kim–Song (CKKS) encryption scheme [30], which supports approximate arithmetic operations on real numbers, crucial for secure computation in privacy-preserving ML.

1) Key Generation

The encryption process begins with the generation of a Secret Key (SK) and a Public Key (PK):

$$SK \leftarrow KeyGen\big(1^\lambda\big)$$

$$PK = SK\ /s \quad (2)$$

whereλ is the security parameter(commonly 128 or 256 bits). The KeyGen function generates theSK, while the PK is derived by excluding the sensitive secret component$s$. This separation allows the PK to be safely distributed for encryption.

2) Encryption Scheme

Model parameters are encrypted using the CKKS scheme as follows:

$$Enc(w_i) = PK(m + e)\ mod\ q \quad (3)$$

Each client encrypts its locally trained model parameters$w_i$by encoding the values as plaintext vectors$m$and introducing a small noise term$e$(automatically handled by the TenSEAL library), followed by modular reduction. This process preserves the structure necessary for homomorphic operations while ensuring numerical stability.In the proposed framework, model updates are encrypted on a layer-wise basis. Each layer's weights are flattened into vectors, then encoded and encrypted using the CKKS HE scheme. This design allows efficient vectorized homomorphic operations during aggregation. Bias terms are also encrypted to ensure the confidentiality of all trainable parameters during both communication and aggregation. CKKS's support for approximate arithmetic enables secure addition and multiplication over real-valued encrypted data.

3) Decryption Scheme

The decryption of ciphertext$c$is performed by computing its inner product with the SK:

$$Dec(c) = \langle c, SK \rangle\ mod\ q \quad (4)$$

This operation returns an approximate plaintext value, maintaining acceptable numerical accuracy due to CKKS's design.

D. Secure Federated Averaging with HE

The FL-HE framework uses FedAvgalgorithm, allowing encrypted model updates to be securely aggregated by the central server.

1) Local Model Training

Each client $i$updates its model during eachFL round$t$using gradient descent:

$$w_i^{t+1} = w^t - \eta \nabla L_i(w_i) \quad (5)$$

where w^t represents the global model at round t, η is the learning rate and L_i is the local loss function.

2) Model Parameter Encryption

Each client encrypts its locally updated model before transmission:

$$c_i^t = Enc_{pk}(w_i^{t+1}) \quad (6)$$

This ensures that the server receives only encrypted weights, preserving privacy.

3) Secure Aggregation

The server aggregates the encrypted updates c_i^t from all$N$clients using homomorphic addition$\oplus$:

$$c_{agg}^t = \bigoplus_{i=1}^{N} c_i^t \quad (7)$$

4) Decryption and Global Model Update

The server decrypts the aggregated ciphertext and computes the average to obtain the global model:

$$w_{agg}^t = \frac{1}{N} Dec_{SK}(c_{agg}^t) \quad (8)$$

$$w^{(t+1)} = w_{agg}^t \quad (9)$$

This updated model$w^{(t+1)}$is then broadcast to clients for the next training round.

E. Secure Feature Normalization

To maintain consistent training dynamics across clients, feature normalization is conducted securely in encrypted form, preventing information leakage from global statistics.

- Encrypted mean$Enc(\mu)$ is computed as:

$$\mu = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (10)$$

$$Enc(\mu) = \frac{1}{N}\sum_{i=1}^{N} Enc(x_i) \quad (11)$$

- Encrypted variance $Enc(\sigma^2)$ is derived by computing the sum of squared deviations:

$$\sigma^2 = \frac{1}{N}\sum_{i=1}^{N}(x_i - \mu)^2 \quad (12)$$

$$Enc(\sigma^2) = \frac{1}{N}\sum_{i=1}^{N}(Enc(x_i) - Enc(\mu))^2 \quad (13)$$

These operations ensure that individual client-level data remains private while allowing normalized model inputs at the global level.

F. Model Architecture

The proposed FL-HE framework integrates a feed-forward neural network composed of three hidden layers with 128, 64, and 32 neurons, respectively. Each hidden layer employs the ReLU activation function to introduce non-linearity, while a 30% dropout rate is applied to mitigate overfitting. The network is designed to process 17 input features, which include clinical biomarkers and demographic variables. The output layer comprises five neurons, corresponding to the five stages of CKD, and uses a softmax activation function with cross-entropy loss to handle multi-class classification.For data privacy compliance, clients encrypt the updates to models as described in (3) and then send these encrypted updates to the server. Secure federated averaging occurs on the server, maintaining the confidentiality of sensitive parameters throughout the training process.Each client conducts local training using the Adam optimizer with a learning rate of 0.001, along with early stopping (patience = 3) to avoid overfitting and reduce unnecessary computation. The global model is evaluated using a centralized test dataset of 5,000 instances, enabling consistent and fair performance comparison. This architecture balances predictive accuracy

with stringent privacy guarantees, making it suitable for healthcare applications.

G. Experimental Setup

The FL-HE framework was evaluated on a system equipped with a 12th Gen Intel®Core™ i7-1255U CPU running at 1.70 GHz, with 16 GB of RAM and 128 MB Intel®Iris®Xe integrated graphics, operating on Windows 11. The FL environment was implemented using PyTorch 2.6.0 and Python 3.12.7. To enable secure computations on encrypted model weights, the TenSEAL library was used to integrate the CKKS HE scheme into the FL pipeline.

H. FL-HE Parameters

The proposed FL-HE framework used key encryption parameters, aligned with widely accepted cryptographic standards, which are summarized in Table IV.

TABLE IV. CKKS SECURITY PARAMETERS

Parameter	Value	Security Level
Polynomial Degree	16,834	128-bit
Coefficient Modulus	[60, 40, 40, 60]	NIST- L3
Precision Scale	2^{40}	12-bit mantissa

A 128-bit security level is widely regarded as a cryptographic baseline, offering strong protection against brute-force attacks. The selected polynomial degree of 16,834 ensures a sufficiently large ciphertext modulus, enabling support for the required multiplicative depth needed for deep learning model training while adhering to HE standards [31]. The precision scale of 2^{40}represents a practical trade-off between numerical precision and computational efficiency. It allows for approximately 12 decimal digits of precision, which is sufficient for encrypted real-number computations in neural networks without incurring significant performance overhead.

IV. RESULTS AND DISCUSSION

A. Plain FL

Initially, this work implemented the plain FL setup with the same dataset specification and four clients. Then we simulated privacy attacks like model inversion attacks, MIA and gradient leakage attacks for three training rounds on four clients. The key observations of these attacks were:

- Model inversion attack: Dummy inputs were successfully generated for all four clients,indicating the model's susceptibility to reconstruction of input-like representations from shared model updates, posing a risk to data privacy.
- MIA: The precision of MIA ranged from 43% to 62% across different clients and training rounds, demonstrating moderate risk of inferring whether a specific data sample was used during training.
- Gradient leakage attack: The gradients corresponding to input features were non-zero and semantically interpretable, highlighting the potential for adversaries to reconstruct sensitive input data through gradient inversion techniques.

These findings confirm the vulnerability of plain FL to inference and reconstruction attacks, reinforcing the need for enhanced privacy-preserving mechanisms.

B. Comparative Analysis of Plain FL and FL-HE Framework

1) Performance Metrics

Figure 1 illustrates the relationship between communication rounds and model accuracy for both the plain FL and FL-HE frameworks. Both approaches exhibit rapid convergence, with plain FL achieving 98.7% accuracy and FL-HE achieving 98.6% by the 10^{th} round. This negligible performance gap confirms that integrating HE with FL does not significantly degrade model accuracy.

Figure 2 compares the per-client model accuracy across 10 communication rounds under both frameworks. Each of the four clients follows a similar convergence pattern, demonstrating that FL-HE maintains consistent performance across distributed environments while enhancing privacy guarantees.

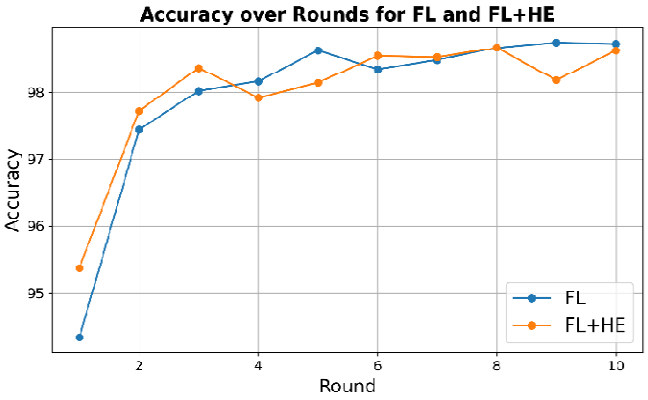

Fig. 1. Performance of the global model after every round.

2) Time Efficiency Analysis

Figure 3 depicts the computational time for FL and FL-HE measured across three primary operations: encryption, aggregation, and decryption. In the plain FL setup, no time is spent on encryption or decryption, and the aggregation process takes approximately 5.1 s. Additionally, there is a transmission delay of around 0.83 s due to the transfer of uncompressed model parameters, bringing the total completion time to 5.93 s.In contrast, the FL-HE framework incurs additional overhead due to the integration of homomorphic encryption. Specifically, encryption requires approximately 1.5 s, while decryption takes about 0.15 s. The aggregation time marginally increases to 5.3 s, attributed to the added complexity of processing encrypted model parameters. However, the transmission delay is slightly reduced to 0.5 s, as encrypted model updates are pre-packed into fixed-size ciphertext structures, enabling more efficient data transfer.Overall, while the FL-HE framework introduces modest overhead primarily in the encryption and decryption stages, the total completion time is 7.45 s,only slightly higher than the 5.93 s of plain FL.

3) Communication and Memory Overhead

Table V highlights a substantial increase in communication and memory overhead within the FL-HE framework, particularly during aggregation and model update transmission. This increase is primarily attributed to ciphertext expansion and the computational requirements associated with performing encrypted arithmetic operations.While these overheads are non-negligible, they represent a necessary trade-off for achieving strong privacy guarantees. To mitigate these costs in real-world deployments, optimization strategies, including ciphertext batching, hyperparameter tuning, and model pruning, can be employed. These techniques aim to reduce the communication footprint and memory consumption, thereby improving the scalability and efficiency of privacy-preserving FL systems without compromising on data confidentiality.

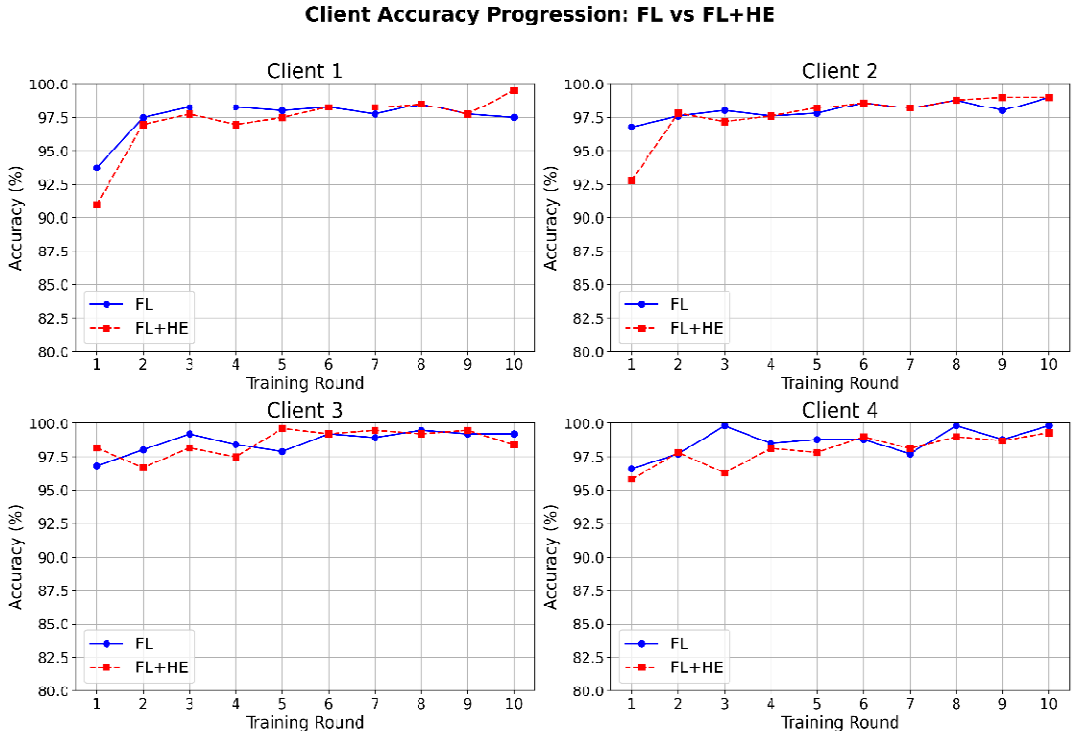

Fig. 2. Progression of accuracy on the four clients in FL & FL-HE.

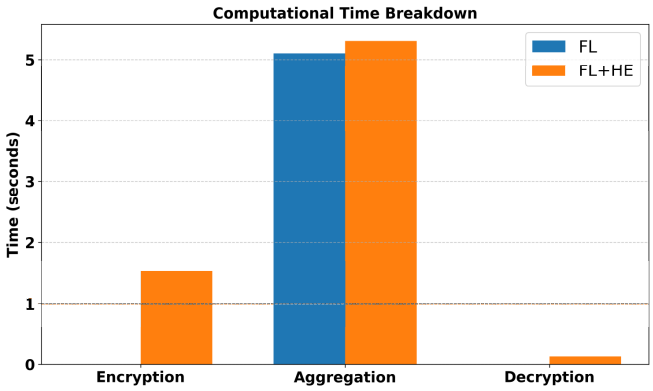

Fig. 3. time of FL & FL-HE.

TABLE V. COMPARISON OF COMMUNICATION & MEMORY OVERHEAD

Metric	Plain FL (MB)	FL-HE (MB)
Average Model Update Size	0.197	4.053
Aggregation Memory Overhead	0.049	12.544
Average Round Trip Size	0.395	7.825

4) Privacy and Security Analysis

To assess the FL-HE framework's privacy assurances, we simulated the same three privacy attacks as those on the plain FL framework. Under the FL-HE framework, the integration of CKKS-based HE for model parameters and secure feature normalization during transmission and aggregation rendered these attacks computationally infeasible. By ensuring that model weights and gradients remain encrypted throughout the communication and aggregation process, the framework effectively eliminates direct data exposure, thereby significantly enhancing privacy protection.

Despite its strong privacy-preserving capabilities, several limitations of the proposed framework warrant consideration:

- Computational overhead: HE introduces non-trivial latency and increased memory consumption due to ciphertext expansion and complex arithmetic operations.
- Scalability constraints: The current implementation has been validated on a small-scale setup involving four clients; its performance and stability in large-scale federated environments remain to be evaluated.

- CKKS precision trade-offs: The use of approximate arithmetic in CKKS may result in minor numerical inaccuracies, particularly in deeper or highly sensitive neural architectures.
- Attack resilience in real-world scenarios: While simulated attack scenarios demonstrated the framework's robustness, real-world adversarial environments may introduce more sophisticated threats that require further investigation and mitigation.

V. CONCLUSION

Electronic Healthcare Records (EHRs) encapsulate highly sensitive and comprehensive healthcare data, necessitating robust privacy and security mechanisms during storage and analysis. To address these concerns, this work proposes a novel Federated Learning with Homomorphic Encryption (FL-HE) framework designed to preserve data privacy while enabling collaborative model training across multiple hospitals. The framework consists of a federated server and four clients (representing hospitals) using a real-time Chronic Kidney Disease (CKD) dataset.

To evaluate the privacy vulnerabilities of a standard FL setup, we first simulated three well-known privacy attacks, model inversion, Membership Inference Attacks (MIA), and gradient leakage, on a plain FL configuration. These attacks revealed substantial privacy risks, validating the need for enhanced protection mechanisms. In response, our proposed framework integrates the Cheon–Kim–Kim–Song (CKKS)HE scheme within the FL pipeline to ensure the encrypted transmission, aggregation of model updates, and secure feature normalization.

Experimental results demonstrate that despite the added cryptographic overhead, the FL-HE model achieves a classification accuracy of 98.6%, only 0.1% lower than that of the plain FL setup. This confirms that strong privacy guarantees can be achieved without sacrificing model utility. The key contributions of this work include:

- Designing an end-to-end privacy-preserving FL-HE system suitable for real-world healthcare settings.
- Implementing layer-wise encrypted model training and secure feature normalization to protect against known privacy attacks.
- Empirically demonstrating that FL with homomorphic encryption maintains competitive accuracy while enhancing resilience to data leakage threats.

Future work will focus on reducing encryption-related computational overhead through techniques such as model compression and quantization, improving the efficiency of secure training. We also plan to scale the framework to support a larger number of clients using parallelized or hierarchical aggregation strategies. Furthermore, the integration of hybrid privacy-preserving techniques, including Differential Privacy (DP), Secure Multiparty Computation (SMPC), and adaptive privacy budgets, will be explored to reinforce security and ensure compliance with evolving regulatory standards in diverse healthcare environments.

ACKNOWLEDGMENT

We extend our sincere gratitude to the Bangalore Hospital, Bangalore, Karnataka, India, for generously providing the dataset essential to this research. We are especially thankful to the staff of the Laboratory and IT departments for their invaluable assistance and cooperation throughout the study. All necessary permissions were obtained prior to data access, and the research was conducted in strict accordance with applicable ethical guidelines to ensure the confidentiality, integrity, and security of patient information.

REFERENCES

[1] B. A. Satterfield, O. Dikilitas, and I. J. Kullo, "Leveraging the Electronic Health Record to Address the COVID-19 Pandemic,"*Mayo Clinic Proceedings*, vol. 96, no. 6, pp. 1592–1608, Jun. 2021, https://doi.org/10.1016/j.mayocp.2021.04.008.

[2] J. Fu, Z. Chen, and X. Han, "Adap DP-FL: Differentially Private Federated Learning with Adaptive Noise," in *2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Wuhan, China, Dec. 2022, pp. 656–663, https://doi.org/10.1109/trustcom56396.2022.00094.

[3] C. Song, Z. Wang, W. Peng, and N. Yang, "Secure and Efficient Federated Learning Schemes for Healthcare Systems,"*Electronics*, vol. 13, no. 13, Jul. 2024, Art. no. 2620, https://doi.org/10.3390/electronics13132620.

[4] L. Chen, D. Xiao, Z. Yu, and M. Zhang, "Secure and efficient federated learning via novel multi-party computation and compressed sensing,"*Information Sciences*, vol. 667, May 2024, Art. no. 120481, https://doi.org/10.1016/j.ins.2024.120481.

[5] J. Park and H. Lim, "Privacy-Preserving Federated Learning Using Homomorphic Encryption,"*Applied Sciences*, vol. 12, no. 2, Jan. 2022, Art. no. 734, https://doi.org/10.3390/app12020734.

[6] G. Long, Y. Tan, J. Jiang, and C. Zhang, "Federated Learning for Open Banking," in *Lecture Notes in Computer Science*, Cham: Springer International Publishing, 2020, pp. 240–254.

[7] A. Alwabli, "Federated Learning for Privacy-Preserving Air Quality Forecasting using IoT Sensors,"*Engineering, Technology & Applied Science Research*, vol. 14, no. 4, pp. 16069–16076, Aug. 2024, https://doi.org/10.48084/etasr.7820.

[8] D. Shenaj, G. Rizzoli, and P. Zanuttigh, "Federated Learning in Computer Vision,"*IEEE Access*, vol. 11, pp. 94863–94884, 2023, https://doi.org/10.1109/access.2023.3310400.

[9] D. Dhinakaran, N. Jagadish Kumar, N. P. Ponnuviji, and B. Praveen Kumar, "Safeguarding confidentiality and privacy in cloud-enabled healthcare systems with spectrasafe encryption and dynamic k-anonymity algorithm,"*Expert Systems with Applications*, vol. 279, Jun. 2025, Art. no. 127584, https://doi.org/10.1016/j.eswa.2025.127584.

[10] D. Dhinakaran, G. Prabaharan, K. Valarmathi, S. M. Udhaya Sankar, and R. Sugumar, "Safeguarding Privacy by utilizing SC-DℓDA Algorithm in Cloud-Enabled Multi Party Computation,"*KSII Transactions on Internet and Information Systems*, vol. 19, no. 2, Feb. 2025, https://doi.org/10.3837/tiis.2025.02.014.

[11] D. Dhinakaran, L. Srinivasan, D. Selvaraj, and T. P. Anish, "A Novel Privacy Preservation of Healthcare Data with Information Entropy-Based Multi-Scheme Fully Homomorphic Encryption and Rivest Shamir Adleman Techniques,"*Biomedical Engineering: Applications, Basis and Communications*, Feb. 2025, https://doi.org/10.4015/s1016237224500601.

[12] L. Zhang, G. Fang, and Z. Tan, "FedCCW: a privacy-preserving Byzantine-robust federated learning with local differential privacy for healthcare,"*Cluster Computing*, vol. 28, no. 3, Jun. 2025, https://doi.org/10.1007/s10586-024-04894-6.

[13] A. P. Kalapaaking, I. Khalil, and X. Yi, "Blockchain-based Federated Learning with SMPC Model Verification Against Poisoning Attack for Healthcare Systems,"arXiv, 2023, https://doi.org/10.48550/ARXIV.2304.13360.

[14] K. B. Nampalle, P. Singh, U. V. Narayan, and B. Raman, "Vision Through the Veil: Differential Privacy in Federated Learning for Medical Image Classification,"arXiv, Jun. 2023, https://doi.org/10.48550/arXiv.2306.17794.

[15] M. H. Fares and A. M. S. E. Saad, "Towards Privacy-Preserving Medical Imaging: Federated Learning with Differential Privacy and Secure Aggregation Using a Modified ResNet Architecture." arXiv, 2024, https://doi.org/10.48550/ARXIV.2412.00687.

[16] B. Wang, H. Li, Y. Guo, and J. Wang, "PPFLHE: A privacy-preserving federated learning scheme with homomorphic encryption for healthcare data,"*Applied Soft Computing*, vol. 146, Art. no. 110677, Oct. 2023, https://doi.org/10.1016/j.asoc.2023.110677.

[17] Y. Xu, J. Zhang, and Y. Gu, "Privacy-Preserving Heterogeneous Federated Learning for Sensitive Healthcare Data." arXiv, 2024, https://doi.org/10.48550/ARXIV.2406.10563.

[18] R. Ahmed, P. K. R. Maddikunta, T. R. Gadekallu, N. K. Alshammari, and F. A. Hendaoui, "Efficient differential privacy enabled federated learning model for detecting COVID-19 disease using chest X-ray images,"*Frontiers in Medicine*, vol. 11, Jun. 2024, https://doi.org/10.3389/fmed.2024.1409314.

[19] B. Zhu and L. Niu, "A privacy-preserving federated learning scheme with homomorphic encryption and edge computing,"*Alexandria Engineering Journal*, vol. 118, pp. 11–20, Apr. 2025, https://doi.org/10.1016/j.aej.2024.12.070.

[20] H. Wang, Q. Wang, Y. Ding, S. Tang, and Y. Wang, "Privacy-preserving federated learning based on partial low-quality data,"*Journal of Cloud Computing*, vol. 13, no. 1, Mar. 2024, https://doi.org/10.1186/s13677-024-00618-8.

[21] T. Muazu, Y. Mao, A. U. Muhammad, M. Ibrahim, U. M. M. Kumshe, and O. Samuel, "A federated learning system with data fusion for healthcare using multi-party computation and additive secret sharing,"*Computer Communications*, vol. 216, pp. 168–182, Feb. 2024, https://doi.org/10.1016/j.comcom.2024.01.006.

[22] S. Li, Y. Liu, F. Feng, Y. Liu, X. Li, and Z. Liu, "HierFedPDP:Hierarchical federated learning with personalized differential privacy,"*Journal of Information Security and Applications*, vol. 86, Nov. 2024, Art. no. 103890, https://doi.org/10.1016/j.jisa.2024.103890.

[23] Z. Shi, Z. Yang, A. Hassan, F. Li, and X. Ding, "A privacy preserving federated learning scheme using homomorphic encryption and secret sharing,"*Telecommunication Systems*, vol. 82, no. 3, pp. 419–433, Mar. 2023, https://doi.org/10.1007/s11235-022-00982-3.

[24] H. Ku, W. Susilo, Y. Zhang, W. Liu, and M. Zhang, "Privacy-Preserving federated learning in medical diagnosis with homomorphic re-Encryption,"*Computer Standards & Interfaces*, vol. 80, Mar. 2022, Art. no. 103583, https://doi.org/10.1016/j.csi.2021.103583.

[25] R. G. Goriparthi, "Federated Learning Models for Privacy-Preserving AI in Distributed Healthcare Systems,"*International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, vol. 14, no. 1, pp. 650–673, 2023.

[26] S. M. Gouse and V. B. Burra, "An Efficient Multi-Class Privacy-Preserving-Based Encryption Framework for Large Distributed Databases,"*International Journal of Reliability, Quality and Safety Engineering*, vol. 30, no. 04, Aug. 2023, https://doi.org/10.1142/s0218539323410036.

[27] A. Garba, S. Khalid, I. Ullah, S. Khusro, and D. Mumin, "Embedding based learning for collection selection in federated search,"*Data Technologies and Applications*, vol. 54, no. 5, pp. 703–717, Oct. 2020, https://doi.org/10.1108/dta-01-2019-0005.

[28] A. Garba, S. Khalid, and I. Ullah, "Understanding the impact of query expansion on federated search,"*Multimedia Tools and Applications*, vol. 83, no. 4, pp. 10393–10407, Jan. 2024, https://doi.org/10.1007/s11042-023-15831-x.

[29] M. Gayathri Hegde, P. S. Marellavar, G. Sunil Kumar, P. D. Shenoy, K. R. Venugopal, and C. Arvind, "A WebApp Framework for the prediction of e-GFR value and CKD stage using Regression-based Machine Learning Algorithms," in *2024 IEEE 5th India Council International Subsections Conference (INDISCON)*, Chandigarh, India, Aug. 2024, pp. 1–6, https://doi.org/10.1109/indiscon62179.2024.10744278.

[30] J. H. Cheon, A. Kim, M. Kim, and Y. Song, "Homomorphic Encryption for Arithmetic of Approximate Numbers," in *Lecture Notes in Computer Science*, Cham: Springer International Publishing, 2017, pp. 409–437.

[31] M. Albrecht *et al.*, "Homomorphic Encryption Security Standard,"*HomomorphicEncryption.org*, Toronto, Canada, Technical Report, Nov. 2018.