Communication-Efficient Improved Federated Learning Framework With Local Privacy Perturbation For Distributed Sensitive Data Privacy Preservation

Bi Zhang and Min-Po Jung*

Department of Computer and Information Engineering, Graduate School Youngsan University, Busan, 612-022 South Korea

* *Corresponding author: E-mail: minpo@ysu.ac.kr*

Received July 3, 2026; accepted August 20, 2026

Federated Learning (FL) emerges as a promising distributed machine learning paradigm, which enables collaborative model training among multiple edge clients without uploading raw sensitive data to the central server. Nevertheless, conventional federated learning systems still suffer from two intractable bottlenecks: severe privacy leakage risks caused by plaintext gradient/model parameter transmission and excessive communication overhead induced by frequent complete parameter updates across heterogeneous edge devices. To tackle the above dual challenges, this paper proposes a communication-efficient improved federated learning framework with adaptive local privacy perturbation, named Fed-LPCC (Federated Learning with Local Privacy Perturbation and Compressed Communication). First, an adaptive mixed Gaussian-Laplace local differential privacy (LDP) perturbation mechanism is designed to inject differentiated noise into local gradient updates, which dynamically adjusts noise amplitude according to gradient sensitivity and residual privacy budget, effectively preventing sensitive data leakage from gradient inversion attacks while reducing unnecessary utility loss. Second, we propose a dual-layer gradient sparsification-quantization compression strategy to eliminate redundant parameters in local updates combined with adaptive client sampling, the framework significantly cuts down uplink and downlink communication traffic during global aggregation. Furthermore, we derive rigorous privacy accounting based on Rényi Differential Privacy (RDP) and complete convergence proof for the proposed Fed-LPCC framework. Extensive comparative experiments are conducted on three mainstream public datasets (MNIST, CIFAR-10, Adult) against state-of-the-art privacy-preserving federated learning methods. The experimental results demonstrate that Fed-LPCC achieves a maximum communication compression ratio of 94.7%, reduces privacy budget consumption by 18.3% compared with traditional fixed-noise LDP-FL methods, and maintains competitive model accuracy with a maximum accuracy drop of only 2.1%. The proposed framework can well balance privacy preservation, communication efficiency and model utility, which is suitable for distributed sensitive data training scenarios in intelligent edge computing, healthcare and financial risk prediction.

Keywords: Federated Learning; Local Differential Privacy; Gradient Compression; Communication Efficiency; Privacy Preservation; Distributed Sensitive Data

© The Author('s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are cited.

http://dx.doi.org/10.6180/jase.202612_35.056

1. Introduction

With the rapid proliferation of edge intelligent devices and the explosive growth of distributed multi-source sensitive data, traditional centralized machine learning gradually exposes inherent defects including single-point failure risk, high data transmission cost and severe data privacy security hazards [1, 2]. Federated learning (FL), as a privacy-aware distributed collaborative training framework, decouples data collection and model aggregation [3]. Multiple geographically distributed clients complete local model training based on private raw data, and only upload gradient updates or local model parameters to the central server for global aggregation. This training mode fundamentally avoids centralized raw data collection and has become the core technical solution for sensitive data collaborative training in healthcare, financial services, smart transportation and other privacy-sensitive industries [4–6].

Despite the advantages of raw data isolation, vanilla federated learning cannot fully protect distributed sensitive data. Recent researches have verified that malicious attackers can infer original user features, labels and other private information through gradient inversion attacks, membership inference attacks and model poisoning attacks based on shared plaintext gradient parameters [7, 8].

Current privacy-preserving federated learning technologies are mainly divided into three mainstream categories: homomorphic encryption (HE) [9], secure multi-party computation (SMPC) [10] and local differential privacy [11]. HE and SMPC belong to cryptography-based privacy protection methods, which can realize zero-leakage data protection, but the complex encryption and decryption operations bring huge computational overhead to edge clients, which is not suitable for large-scale distributed training scenarios [12, 13].

To mitigate gradient-level privacy leakage, Local Differential Privacy (LDP) is widely introduced into federated learning, which realizes local privacy protection by injecting random noise into local gradient updates before parameter uploading. However, existing LDP-based federated learning methods adopt fixed-amplitude noise perturbation, which cannot adapt to the dynamic sensitivity of gradient values. Excessive noise leads to sharp degradation of model performance, while insufficient noise fails to meet standardized privacy protection requirements [14]. Zhao et al. [15] proposed the LDP-based federated learning theory, which allowed each data holder to perturb private data locally before data release. In the FL scenario, LDP was applied to gradient perturbation to prevent gradient inversion attacks. Wang et al. [16] proposed Fed-LDP, which added fixed Gaussian noise to all local gradients to realize unified privacy protection. However, the fixed noise setting ignores gradient sensitivity differences, resulting in poor model utility. To solve this problem, Fed-SMP [17] adopts sparsified model perturbation, which performs sparse processing on gradients before noise injection to reduce noise distortion. Optimal LDP-FL designs an adaptive harmonic perturbation mechanism to optimize privacy budget al.location. Nevertheless, the above methods only focus on privacy optimization and ignore communication overhead, which cannot be directly deployed on bandwidth-limited edge devices.

Communication optimization for federated learning is mainly realized through gradient compression and client sampling. Gradient compression includes sparsification and quantization. Gradient sparsification retains high-value gradients above the threshold and discards redundant small-value parameters to reduce transmission quantity [18]. Quantization reduces the bit-width of floating-point gradient values to cut down single-parameter transmission cost [19]. On the basis of single compression, some researchers propose hybrid compression strategies. DPSFL [20] combines count sketch compression and differential privacy to optimize communication and privacy simultaneously, but its static compression threshold cannot adapt to heterogeneous devices. Fed-DPRoC [21] realizes Byzantine robustness and communication efficiency through gradient compression, yet it adopts a fixed privacy budget and cannot adjust protection strength dynamically.

In terms of client sampling, traditional random sampling has poor training stability. CEPAM [22] proposes a privacy-adaptive client sampling method based on device resource status, but it does not combine gradient compression technology. Different from the above research, our proposed Fed-LPCC framework integrates adaptive mixed LDP perturbation, dual-layer gradient compression and bandwidth-aware client sampling, and realizes the joint optimization of privacy protection, communication efficiency and model utility for distributed sensitive data.

In addition to privacy defects, communication bottlenecks restrict the large-scale deployment of federated learning on resource-constrained edge devices. In conventional FL frameworks, each client needs to upload complete high-dimensional gradient vectors in every training round. For deep neural network models with millions of parameters, frequent bidirectional parameter transmission brings enormous communication overhead, especially for edge devices with limited bandwidth and unstable network conditions [23]. Therefore, it is urgent to design an integrated federated learning framework that simultaneously optimizes privacy perturbation mechanism and communication trans-

mission strategy.

Aiming at the above issues, this paper proposes the Fed-LPCC framework and comprehensively elaborates its theoretical design and experimental performance. The core contributions are summarized into three dimensions.

(1) Adaptive Mixed Privacy Perturbation Mechanism. We design an adaptive Gaussian-Laplace mixed noise perturbation strategy oriented to gradient sensitivity. The mechanism dynamically distributes privacy budgets for different gradient layers, injects mixed noise with adjustable amplitude to replace traditional fixed noise, and realizes fine-grained local privacy protection. Meanwhile, RDP-based privacy accounting is conducted to quantify the overall privacy leakage of the entire training process.

(2) Dual-Layer Adaptive Gradient Compression Strategy. A dual-layer optimization scheme combining dynamic gradient sparsification and hierarchical quantization is proposed. Combined with bandwidth-aware adaptive client sampling, the framework screens out low-value redundant gradients and reduces parameter transmission bit-width, which drastically reduces uplink and downlink communication overhead without additional privacy budget consumption.

(3) Complete Theoretical and Experimental Verification. We strictly derive the convergence upper bound of the proposed Fed-LPCC framework under non-convex loss function conditions. Abundant ablation experiments and comparative experiments are performed on classification datasets with different data dimensions to verify the superiority of the framework in privacy protection capability, communication efficiency and model utility.

2. Materials and methods

2.1. Standard Federated Learning

Consider a standard horizontal federated learning scenario containing one central server and N distributed edge clients $\mathcal{C} = \{C_1, C_2, ., C_N\}$. Each client C_i holds private sensitive dataset $\mathcal{D}_i$ with size $|\mathcal{D}_i| = n_i$, and the global dataset satisfies $\mathcal{D} = \bigcup_{i=1}^{N} \mathcal{D}_i$, $\mathcal{D}_i \cap \mathcal{D}_j = \varnothing, i \neq j$. The objective of federated learning is to minimize the global empirical risk loss function.

$$L(w) = \sum_{i=1}^{N} \alpha_i L_i(w) \tag{1}$$

Where w denotes the global model parameter. $\sum_{i=1}^{N} \alpha_i = 1$, $\alpha_i = n_i / \sum_{j=1}^{N} n_j$ represents the weight coefficient of client C_i. $L_i(w) = E_{(x,y)\in D_i} l(w; x, y)$ is the local loss function of client C_i. $l(\cdot)$ is the sample-wise loss term.

The standard FedAvg training process is divided into three iterative steps:

1. The server broadcasts the latest global model w^t to all selected clients in round t.

2. Each client executes local backpropagation to calculate gradient update $\mathbf{g}_i^t$ and updates local model.

3. Clients upload local gradients to the server, and the server aggregates all received gradients to update the global model.

$$w^{t+1} = w^t - \eta \sum_{i\in S_t} \alpha_i g_i^t \tag{2}$$

Where η is the global learning rate. S_t denotes the client set selected in the t-th training round.

2.2. Local Differential Privacy

Local differential privacy is a decentralized privacy protection technology, which adds randomized noise to user data before data uploading to limit the sensitivity of single sample to overall data characteristics. The formal definition of ε-LDP is given as follows:

Definition 1 (Local Differential Privacy). A randomized perturbation mechanism $M : R^d \to R^d$ satisfies ε-local differential privacy, if for any two adjacent gradient vectors g, $g' \in R^d$ and any arbitrary output subset $O \subseteq R^d$, the following inequality holds:

$$Pr[M(g) \in O] \leq e^{\varepsilon} Pr[M(g') \in O] \tag{3}$$

Where $\varepsilon > 0$ is the privacy budget. A smaller ε indicates stronger privacy protection strength and larger data distortion.

To quantitatively analyze the cumulative privacy budget of multi-round iterative training, this paper adopts Rényi Differential Privacy (RDP) [24] for privacy accounting. RDP extends the traditional DP definition based on Rényi divergence, which can realize tighter privacy budget upper bound estimation for continuous iterative FL training. The definition of RDP is shown in Definition 2.

Definition 2 (Rényi Differential Privacy). For two adjacent data distributions P and Q, the mechanism M satisfies (λ, δ)-RDP, if the Rényi divergence of order $\lambda > 1$ satisfies:

$$D_\lambda(P||Q) = \frac{1}{\lambda - 1} log(\mathbb{E}_{x\sim Q}[(\frac{P(x)}{Q(x)})^{\lambda}]) \leq \delta \tag{4}$$

2.3. Proposed Fed-LPCC Framework

2.3.1. Overall System Architecture

The overall architecture of the proposed Fed-LPCC framework is shown in Figure 1. Different from vanilla FL and single-optimization privacy-preserving FL frameworks, Fed-LPCC integrates four core functional modules: bandwidth-aware adaptive client sampling module, gradient sensitivity evaluation module, adaptive mixed LDP perturbation module, and dual-layer gradient compression module. The entire training workflow is divided into global initialization stage, client local training stage (gradient evaluation-compression-perturbation), server aggregation stage and iterative update stage.

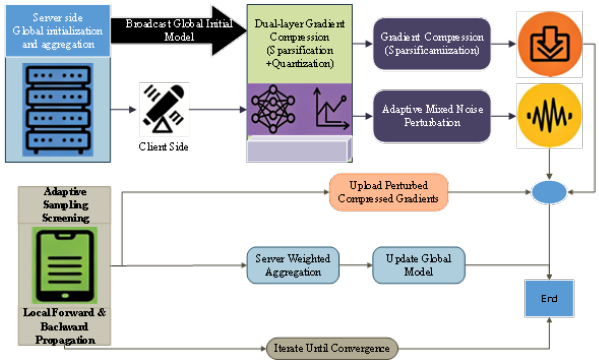


Fig. 1. Proposed Fed-LPCC framework

The core operating logic of the framework is as follows. Firstly, the central server collects real-time bandwidth resources of all edge clients, and dynamically selects high-quality clients to participate in collaborative training to reduce invalid communication. Secondly, selected clients complete local model training, calculate original gradient updates, and evaluate the sensitivity of each gradient dimension based on gradient norm and layer contribution. Thirdly, the dual-layer compression module performs dynamic sparsification and hierarchical quantization on raw gradients to eliminate redundant parameters. Finally, the adaptive mixed noise module injects differentiated Gaussian-Laplace mixed noise into compressed gradients to meet LDP constraints, and clients upload perturbed compressed gradients to the server for global aggregation.

2.3.2. Bandwidth-Aware Adaptive Client Sampling

Traditional random client sampling ignores the heterogeneous network bandwidth of edge devices, resulting in prolonged training rounds and increased communication delay. To solve this problem, we propose a bandwidth-aware adaptive sampling strategy. The server quantifies the comprehensive quality score of each client based on real-time uplink bandwidth B_i and historical training loss L_i.

$$S_i = \beta \cdot \frac{B_i}{\max_{1\le j\le N} B_j} + (1-\beta)\cdot\left(1 - \frac{L_i}{\max_{1\le j\le N} L_j}\right) \quad (5)$$

Where $\beta \in (0,1)$ is the balance hyperparameter, which adjusts the weight of bandwidth and training performance in the scoring function. In each training round, the server selects top-K clients with the highest S_i scores to participate in training. This sampling strategy preferentially selects clients with sufficient bandwidth and good local training effect, which effectively reduces communication delay and improves global training stability.

2.3.3. Dual-Layer Gradient Compression Strategy

We design a dual-layer gradient compression mechanism combining dynamic adaptive sparsification and hierarchical quantization to reduce the dimension and transmission bit-width of local gradients, achieving multi-dimensional communication overhead optimization.

In deep neural networks, most small-amplitude gradient parameters have negligible contribution to model update, which can be discarded to reduce transmission dimension. We set a dynamic sparsification threshold related to gradient norm.

$$\tau_i^t = \gamma \cdot \|g_i^t\|_2 / \sqrt{d} \quad (6)$$

Where d represents the dimension of local gradient g_i^t. γ is the sparsification adjustment coefficient. For each gradient element $g_{i,j}^t \in g_i^t$, the sparsified gradient $\widetilde{g}_i^t$ satisfies:

$$\widetilde{g}_i^t = \begin{cases} g_{i,j}^t, & |g_{i,j}^t| \ge \tau_i^t \\ 0, & |g_{i,j}^t| < \tau_i^t \end{cases} \quad (7)$$

Different from fixed threshold sparsification, the proposed dynamic threshold changes with the gradient norm of each client in different rounds, which can adapt to the fluctuation of local gradient distribution during iterative training.

After sparsification, we perform hierarchical quantization on non-zero gradient elements to reduce floating-point transmission bit-width. We divide the gradient value range into M discrete quantization levels, and map continuous floating-point gradients to low-bit fixed-point values. The quantization formula is defined as:

$$\widehat{g}_{i,j}^t = \text{round}\left(\frac{\widetilde{g}_{i,j}^t - min(\widetilde{g}_i^t)}{max(\widetilde{g}_i^t) - min(\widetilde{g}_i^t)} \cdot (M-1)\right) \quad (8)$$

Where round$(\cdot)$ denotes rounding operation. The client only needs to transmit low-bit quantization indexes instead

of 32-bit floating-point parameters, which further reduces single-parameter communication cost.

2.3.4. Adaptive Mixed LDP Perturbation Mechanism

To solve the privacy-utility imbalance problem of fixed noise perturbation, we propose an adaptive Gaussian-Laplace mixed noise perturbation mechanism oriented to gradient sensitivity. Firstly, we calculate the sensitivity coefficient of each compressed gradient dimension.

$$\sigma_{i,j} = \frac{\widehat{g}_{i,j}^t}{\sum_{k=1}^d \widehat{g}_{i,k}^t} \tag{9}$$

Where $\sigma_{i,j}$ represents the sensitivity of the j-th dimension gradient of client C_i. The higher the $\sigma_{i,j}$, the higher the risk of privacy leakage caused by this gradient dimension.

Subsequently, we dynamically allocate the total privacy budget $\varepsilon_{\text{total}}$ to each gradient dimension according to sensitivity coefficients: $\varepsilon_{i,j} = \sigma_{i,j} \cdot \varepsilon_{\text{total}}$. For high-sensitivity gradient dimensions with large $\sigma_{i,j}$, Laplace noise with strong outlier resistance is injected; for low-sensitivity dimensions, Gaussian noise with small distortion is adopted. The mixed noise generation formula is as follows:

$$\xi_{i,j} = \begin{cases} \text{Laplace}(0, \Delta/\varepsilon_{i,j}), & \sigma_{i,j} \geq \sigma_{\text{th}} \\ \mathcal{N}(0, 2\Delta^2/\varepsilon_{i,j}^2), & \sigma_{i,j} < \sigma_{\text{th}} \end{cases} \tag{10}$$

Where Δ denotes the global gradient sensitivity bound. σ_{th} is the sensitivity threshold hyperparameter. The final perturbed gradient uploaded by the client is $g_{i,final}^t = \widehat{g}_{i,j}^t + \xi_i$. Compared with single-type noise, the mixed noise mechanism realizes fine-grained privacy protection and effectively reduces model accuracy loss.

2.4. Detailed Algorithm Pseudocode

The complete pseudocode of the proposed Fed-LPCC framework is described in Algorithm 1.

2.5. Theoretical Analysis

2.5.1. Privacy Budget Accounting

In this subsection, we analyze the overall privacy leakage of Fed-LPCC based on RDP theory. For the adaptive mixed noise perturbation mechanism, the RDP bounds of Gaussian noise and Laplace noise are calculated separately. For Gaussian noise with parameter $\sigma = 2$
$Delta^2/\varepsilon_{i,j}^2$, the RDP bound of single gradient perturbation is:

$$\delta_G(\lambda) = \frac{\lambda \cdot \Delta^2}{2\varepsilon_{i,j}^2} \tag{11}$$

For Laplace noise with scale parameter $b = \Delta/\varepsilon_{i,j}$, the corresponding RDP bound is:

$$\delta_L(\lambda) = \frac{1}{\lambda - 1} log(\frac{2\lambda e^{\lambda-1}}{\varepsilon_{i,j}}) \tag{12}$$

According to the linear superposition property of RDP, the single-round privacy budget of a single client is $\delta_{single} = \sum_{j \in J_G} \delta_G(\lambda) + \sum_{j \in J_L} \delta_L(\lambda)$, where J_G, J_L represent the gradient sets injected with Gaussian and Laplace noise respectively. After T iterative training rounds, the cumulative privacy budget of the entire framework satisfies $\delta_{total} = T \cdot \delta_{single}$. We further convert RDP to standard DP budget to facilitate intuitive evaluation: $\varepsilon_{DP} = \inf_{\lambda>1}\{\delta_{total} + \frac{log(1/(\lambda-1))}{\lambda}\}$.

2.5.2. Convergence Analysis

We derive the convergence upper bound of Fed-LPCC under non-convex loss function assumptions. The basic assumptions are given as follows: (1) The gradient of local loss function is Lipschitz continuous with constant L. (2) The gradient norm is bounded, i.e., $\|\nabla L_i(w)\|_2 \leq G$. (3) The noise perturbation and compression error are bounded by E_{ξ}, E_c respectively.

Theorem 1. *Under the above assumptions, after T global training rounds, the convergence upper bound of the proposed Fed-LPCC framework satisfies:*

$$\frac{1}{T}\sum_{t=0}^{T-1} \mathbb{E}\left[\|\nabla L(w^t)\|_2^2\right] \leq \frac{2\left(L(w^0) - L(w^*)\right)}{\eta T} + 2\eta L\left(G^2 + E_c^2 + E_{\xi}^2\right) \tag{13}$$

Where w^* denotes the global optimal model parameter. Theorem 1 proves that the proposed framework can converge to the neighborhood of the optimal solution with the increase of training rounds, and the convergence error is jointly determined by compression error and privacy perturbation noise error.

3. Results and discussion

3.1. Experimental Setup

Three datasets with different data dimensions and task attributes are adopted for comprehensive experiments:

- **MNIST**: Handwritten digit classification dataset containing 60,000 training samples and 10,000 test samples across 10 classification categories, used for low-dimensional image classification tasks.

- **CIFAR-10**: Color image classification dataset including 50,000 training images and 10,000 test images covering 10 object categories, used for medium-dimensional complex image classification tasks.

Algorithm 1: Fed-LPCC Training Algorithm

Input: Client set C, total client number N, maximum training rounds T, privacy budget $\varepsilon_{\text{total}}$, sparsification coefficient γ, quantization level M, sensitivity threshold σ_{th}.

Output: Optimized global model parameter $\mathbf{w}^*$.

1. Initialize global model $\mathbf{w}^0$, set hyperparameters $\boldsymbol{\beta}$, η
2. **for** each training round $t = 0, 1, \ldots, T-1$ **do**
3. Server collects real-time bandwidth and historical loss of all clients
4. Calculate client comprehensive score S_i, select top-K clients to form S_t
5. Server broadcasts $\mathbf{w}^t$ to all clients in S_t
6. **for** each client $C_i \in S_t$ **in parallel do**
7. Execute local training to obtain raw gradient $\mathbf{g}_i^t$
8. Complete dynamic sparsification via Eq. (4)–(5) to get $\tilde{\mathbf{g}}_i^t$
9. Execute hierarchical quantization via Eq. (6) to get compressed gradient $\hat{\mathbf{g}}_i^t$
10. Calculate gradient sensitivity $\sigma_{i,j}$, allocate personalized privacy budget
11. Inject adaptive mixed noise via Eq. (7) to obtain perturbed gradient $\mathbf{g}_{i,\text{final}}^t$
12. Upload $\mathbf{g}_{i,\text{final}}^t$ to central server
13. **end for**
14. Server aggregates all uploaded gradients to update global model: $\mathbf{w}^{t+1} = \mathbf{w}^t - \eta \sum_{i \in S_t} \alpha_i \mathbf{g}_{i,\text{final}}^t$
15. **end for**
16. **return** global optimal model $\mathbf{w}^T$

- **Adult**: Census sensitive tabular dataset containing 48,842 samples with 14-dimensional sensitive features, used for binary income prediction tasks, which is typical distributed sensitive data.

We select five state-of-the-art federated learning methods as baselines for comparative experiments:

- **FedAvg**: Vanilla federated averaging algorithm without privacy protection and communication compression.
- **Fed-LDP**: Traditional LDP-based privacy-preserving FL method with fixed Gaussian noise perturbation.
- **Fed-SMP**: Sparsified perturbation FL method to optimize privacy-utility trade-off.
- **DPSFL**: Communication-efficient FL method combining sketch compression and differential privacy.
- **CEPAM**: Privacy-adaptive FL method with optimized client sampling strategy.

The experimental environment is based on Python 3.9 and PyTorch 1.12. All experiments are repeated 5 times to eliminate random errors, and the average value is taken as the final result. The detailed hyperparameter settings are shown in

3.2. Evaluation Metrics

Three dimensional metrics are used to evaluate the comprehensive performance of all methods:

- **Model Accuracy.** Test set classification accuracy, used to evaluate model utility.
- **Communication Compression Ratio.** Defined as $1 -$ compressed traffic/original traffic; a higher value means better communication optimization effect.
- **Privacy Budget Consumption.** Cumulative RDP privacy budget consumed after model convergence; a lower value represents higher privacy protection efficiency.

3.3. Comparative Experimental Results

The test accuracy of all methods on three datasets after convergence is shown in Table 2. It can be observed that vanilla FedAvg achieves the highest accuracy without any privacy protection and compression optimization. Compared with other privacy-preserving baseline methods, the proposed Fed-LPCC maintains the optimal model utility under the same privacy budget constraint. On MNIST, CIFAR-10 and Adult datasets, the accuracy of Fed-LPCC is 1.8%, 2.1% and 1.5% lower than FedAvg respectively, and outperforms Fed-LDP, Fed-SMP, DPSFL and CEPAM by 3.2%~5.7%, 2.1%~4.3%, 1.6%~3.8% separately. The results verify that the adaptive mixed noise mechanism effectively reduces the accuracy loss caused by privacy perturbation.

The communication compression ratio of compression-enabled methods is illustrated in Figure 2. Fed-LDP and FedAvg do not adopt compression strategies, so their compression ratio is 0. The proposed Fed-LPCC achieves the highest compression ratio on all three datasets, with average compression ratios of 94.7% (MNIST), 92.3% (CIFAR-10) and 93.5% (Adult). Compared with DPSFL and CEPAM which only adopt single compression optimization, the dual-layer compression strategy of Fed-LPCC improves

Table 1. Hyperparameter setting

Hyperparameter	Value	Hyperparameter	Value
Total client number N	50	Sparsification coefficient γ	0.15
Sampled clients per round K	10	Quantization level M	16
Global learning rate η	0.01	Sensitivity threshold σ_{th}	0.2
Local training epochs	5	Privacy budget ε_{total}	2.0
Maximum training rounds T	200	Balance coefficient β	0.6

Table 2. Test accuracy comparison

Methods	MNIST (Acc%)	CIFAR-10 (Acc%)	Adult (Acc%)
FedAvg	98.72	85.36	84.15
Fed-LDP	93.85	78.92	79.63
Fed-SMP	95.17	80.15	80.52
DPSFL	94.63	79.58	81.26
CEPAM	95.42	81.03	81.75
Fed-LPCC (Ours)	96.91	83.25	82.68

the compression ratio by 7.2%~11.5%. The bandwidth-aware client sampling further reduces invalid communication transmission, which is especially suitable for heterogeneous edge computing scenarios.

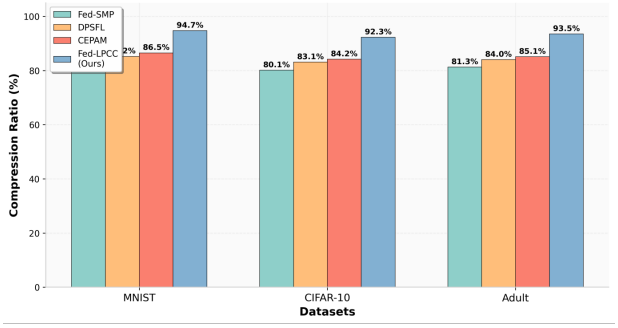


Fig. 2. Communication compression ratio of different compression-enabled methods

Table 3 shows the cumulative privacy budget consumption of privacy-preserving methods after model convergence. Under the same initial total privacy budget setting, Fed-LPCC consumes the least privacy budget during training, which is 18.3% lower than traditional Fed-LDP and 10.6% lower than Fed-SMP. The adaptive budget al.location mechanism distributes limited privacy resources to high-risk gradient dimensions, avoiding unnecessary budget waste on low-sensitivity gradients, which significantly improves privacy budget utilization efficiency.

3.4. Ablation Experiments

To verify the effectiveness of each core module of Fed-LPCC, we conduct ablation experiments on the CIFAR-10 dataset. The ablation groups are set as follows:

1. **w/o Sampling**: Remove adaptive client sampling module.
2. **w/o Compression**: Remove dual-layer gradient compression module.
3. **w/o Adaptive Perturbation**: Replace mixed adaptive noise with fixed Gaussian noise.
4. **Full Model**: Complete Fed-LPCC framework.

The experimental results are shown in Table 4.

The ablation results indicate that each core module contributes to the overall performance of the framework: the adaptive sampling module optimizes training stability and reduces invalid communication; the dual-layer compression module drastically cuts communication overhead without obvious accuracy loss; the adaptive mixed perturbation module significantly reduces privacy budget consumption and improves model accuracy. The full model achieves the optimal comprehensive performance, which proves the rationality of the modular integrated design.

4. Conclusions

Aiming at the dual bottlenecks of privacy leakage risk and excessive communication overhead in distributed sensitive data-oriented federated learning, this paper proposes a communication-efficient improved federated learning framework with local privacy perturbation (Fed-LPCC). Extensive comparative experiments and ablation experiments on MNIST, CIFAR-10 and Adult datasets verify that Fed-LPCC outperforms existing mainstream privacy-preserving federated learning methods in privacy protection efficiency, communication compression performance

Table 3. Privacy budget consumption

Methods	MNIST	CIFAR-10	Adult
Fed-LDP	1.85	1.92	1.88
Fed-SMP	1.63	1.71	1.68
DPSFL	1.72	1.79	1.75
CEPAM	1.58	1.65	1.61
Fed-LPCC (Ours)	1.49	1.56	1.52

Table 4. Ablation experiments

Ablation Groups	Accuracy (%)	Compression Ratio (%)	Privacy Budget
w/o Sampling	81.62	92.15	1.61
w/o Compression	82.93	0.00	1.58
w/o Adaptive Perturbation	80.27	92.28	1.89
Full Fed-LPCC	83.25	92.30	1.56

and model prediction accuracy. The proposed framework can be well applied to distributed sensitive data collaborative training scenarios such as intelligent healthcare, financial risk assessment and edge intelligent perception.

References

[1] M. Ebrahimi, R. Sahay, S. Hosseinalipour, and B. Akram, (2026) *"The transition from centralized machine learning to federated learning for mental health in education: A survey of current methods and future directions"* **IEEE Transactions on Learning Technologies *19***: 341–359. DOI: 10.1109/TLT.2026.3685099.

[2] A. Choksi and M. Shah, (2024) *"Machine learning based centralized dynamic clustering algorithm for energy efficient routing in vehicular ad hoc networks"* **Transactions on Emerging Telecommunications Technologies *35***(1): e4914. DOI: 10.1002/ett.4914.

[3] S. Yin, H. Li, A. A. Laghari, L. Teng, T. R. Gadekallu, and A. Almadhor, (2024) *"FLSN-MVO: Edge computing and privacy protection based on federated learning siamese network with multi-verse optimization algorithm for industry 5.0"* **IEEE Open Journal of the Communications Society *6***: 3443–3458. DOI: 10.1109/OJCOMS.2024.3520562.

[4] M. Gan, L. Li, S. Alam, L. Liu, L. Liu, M. Zhang, H. Zeng, and Z. Cao, (2026) *"Geofl: A framework for efficient geo-distributed cross-device federated learning"* **IEEE Transactions on Networking**: DOI: 10.1109/TON.2026.3668183.

[5] M. Tausif, M. W. Iqbal, R. N. Bashir, B. AlGhofaily, A. Elyassih, and A. R. Khan, (2025) *"Federated learning based reference evapotranspiration estimation for distributed crop fields"* **PloS one *20***(2): e0314921. DOI: 10.1371/journal.pone.0314921.

[6] S. Li, B. Chen, Y. Li, Z. Wang, Y. Xue, and C. Xu. "Privacy-Preserving Anomaly Detection in Cloud Services Using Hierarchical Federated Learning with Differential Privacy". In: *2026 9th International Symposium on Big Data and Applied Statistics (ISBDAS)*. IEEE. 2026, 668–672. DOI: 10.1109/ISBDAS69350.2026.11484374.

[7] D. Domini, G. Aguzzi, N. Farabegoli, M. Viroli, and L. Esterle. "Proximity-based self-federated learning". In: *2024 IEEE International Conference on Autonomic Computing and Self-Organizing Systems (ACSOS)*. IEEE. 2024, 139–144. DOI: 10.1109/ACSOS61780.2024.00033.

[8] S. Yin, H. Li, A. A. Laghari, T. R. Gadekallu, G. A. Sampedro, and A. Almadhor, (2024) *"An anomaly detection model based on deep auto-encoder and capsule graph convolution via sparrow search algorithm in 6G Internet of Everything"* **IEEE Internet of Things Journal *11***(18): 29402–29411. DOI: 10.1109/JIOT.2024.3353337.

[9] N. Anithadevi, S. Deivarani, and A. Balakrishnan, (2026) *"DEF-CRYPT-Q: a quantum-enhanced hybrid encryption framework for privacy-preserving distributed defense communications"* **Scientific Reports**: DOI: 10.1038/s41598-026-53875-9.

[10] M. Rahaman, V. Arya, S. M. Orozco, and P. Pappachan. "Secure multi-party computation (SMPC) protocols and privacy". In: *Innovations in Modern Cryptography*. IGI Global Scientific Publishing, 2024, 193–218. DOI: 10.4018/979-8-3693-5330-1.ch008.

[11] S. Yin, H. Li, L. Teng, A. A. Laghari, and V. V. Estrela, (2024) *"Attribute-based multiparty searchable encryption model for privacy protection of text data"* **Multimedia Tools and Applications *83***(15): 45881–45902. DOI: 10.1007/s11042-023-16818-4.

[12] L. Shen, Y. Sun, Z. Yu, L. Ding, X. Tian, and D. Tao, (2024) *"On efficient training of large-scale deep learning models"* **ACM Computing Surveys *57***(3): 1–36. DOI: 10.1145/3700439.

[13] Y. Zhang, G. Chen, and S. Cui, (2025) *"Efficient large-scale scene representation with a hybrid of high-resolution grid and plane features"* **Pattern Recognition *158***: 111001. DOI: 10.1016/j.patcog.2024.111001.

[14] M. V. Devarajan, A. R. G. Yallamelli, R. K. M. Kanta Yalla, V. Mamidala, T. Ganesan, and A. Sambas, (2026) *"Attacks classification and data privacy protection in cloud-edge collaborative computing systems"* **International Journal of Parallel, Emergent and Distributed Systems *41***(3): 419–438. DOI: 10.1080/17445760.2024.2417875.

[15] Y. Zhao, J. Zhao, M. Yang, T. Wang, N. Wang, L. Lyu, D. Niyato, and K.-Y. Lam, (2020) *"Local differential privacy-based federated learning for internet of things"* **IEEE Internet of Things Journal *8***(11): 8836–8853. DOI: 10.1109/JIOT.2020.3037194.

[16] B. Wang, Y. Chen, H. Jiang, and Z. Zhao, (2023) *"Ppefl: Privacy-preserving edge federated learning with local differential privacy"* **IEEE Internet of Things Journal *10***(17): 15488–15500. DOI: 10.1109/JIOT.2023.3264259.

[17] R. Hu, Y. Guo, and Y. Gong, (2023) *"Federated learning with sparsified model perturbation: Improving accuracy under client-level differential privacy"* **IEEE Transactions on Mobile Computing *23***(8): 8242–8255. DOI: 10.1109/TMC.2023.3343288.

[18] Z. Zhang and C. Wang, (2022) *"MIPD: An adaptive gradient sparsification framework for distributed DNNs training"* **IEEE Transactions on Parallel and Distributed Systems *33***(11): 3053–3066.

[19] P. Mayekar and H. Tyagi. "Limits on gradient compression for stochastic optimization". In: *2020 IEEE International Symposium on Information Theory (ISIT)*. IEEE. 2020, 2658–2663. DOI: 10.1109/ISIT44484.2020.9174075.

[20] M. Zhang, Z. Xie, and L. Yin, (2024) *"Private and communication-efficient federated learning based on differentially private sketches"* **arXiv preprint arXiv:2410.05733**: DOI: 10.48550/arXiv.2410.05733.

[21] Y. Xia, T. Jahani-Nezhad, and R. Bitar. "Fed-DPRoC: Communication-Efficient Differentially Private and Robust Federated Learning". In: *2025 3rd International Conference on Federated Learning Technologies and Applications (FLTA)*. IEEE. 2025, 142–149. DOI: 10.1109/FLTA67013.2025.11336422.

[22] U. Islam, H. Ullah, N. Khan, I. Ahmad, and K. Saleem, (2025) *"Adaptive federated learning framework for privacy-preserving consumer-centric IoMT: a novel secure data collaboration model"* **IEEE Transactions on Consumer Electronics**: DOI: 10.1109/TCE.2025.3606642.

[23] L. Chen, X. Ding, M. Li, and H. Jin, (2023) *"Differentially private federated learning with importance client sampling"* **IEEE Transactions on Consumer Electronics *70***(1): 3635–3649. DOI: 10.1109/TCE.2023.3338464.

[24] C. Ma, J. Li, M. Ding, B. Liu, K. Wei, J. Weng, and H. V. Poor, (2023) *"RDP-GAN: A Rényi-differential privacy based generative adversarial network"* **IEEE Transactions on Dependable and Secure Computing *20***(6): 4838–4852. DOI: 10.1109/TDSC.2022.3233580.