Paper Review: Amplitude-Varying Perturbation for Balancing Privacy and Utility in Federated Learning

H3Art
International School
Jinan University
Guangzhou, China

***Abstract*—This review examines the paper "Amplitude-Varying Perturbation for Balancing Privacy and Utility in Federated Learning," which addresses the significant challenge of balancing privacy and utility in federated learning (FL). FL has become a vital paradigm for training machine learning models across decentralized data sources while preserving data privacy. However, the privacy risks associated with shared model updates require robust privacy-preserving mechanisms. The reviewed paper proposes an innovative amplitude-varying perturbation mechanism that dynamically adjusts the noise level over time, as opposed to traditional differential privacy (DP) methods that use a constant noise amplitude. This approach aims to enhance both convergence and accuracy while ensuring strong privacy guarantees. The review delves into the key contributions of the paper, including the introduction of this novel DP perturbation mechanism, the derivation of analytical bounds, and the extensive experimental validation across various models (MLP, SVM, CNN) and datasets (MNIST, ADULT, CIFAR10, FMNIST). The findings highlight the potential of the proposed method to significantly improve the performance of privacy-preserving FL by offering a flexible and effective solution to the trade-offs between privacy and utility.**

***Index Terms*—Federated learning, differential privacy, time-varying noise variance, convergence analysis.**

I. Introduction

Federated learning (FL) has emerged as a promising paradigm for training machine learning models across distributed data sources without the need to centralize the data. This decentralized approach is particularly valuable in scenarios where data privacy is of paramount importance, such as healthcare and finance. Despite its advantages, FL poses significant privacy challenges, as model updates shared between clients and the central server can potentially leak sensitive information [1], [2]. To mitigate these risks, differential privacy (DP) has been widely adopted, adding random noise to model updates to ensure that individual data points cannot be easily inferred [3], [4]. However, this noise can degrade the model's utility, creating a challenging trade-off between privacy and accuracy.

As illustrated in Fig. 1, even in scenarios with an honest server, attackers can attempt to eavesdrop or capture private information during the local model upload and global model sharing processes. Notably, Shokri *et al.* [5] demonstrated that private information about local datasets can be derived from trained local models. Moreover, model inversion attacks are able to extract private information by using black-box attacks to predict models [6], [7].

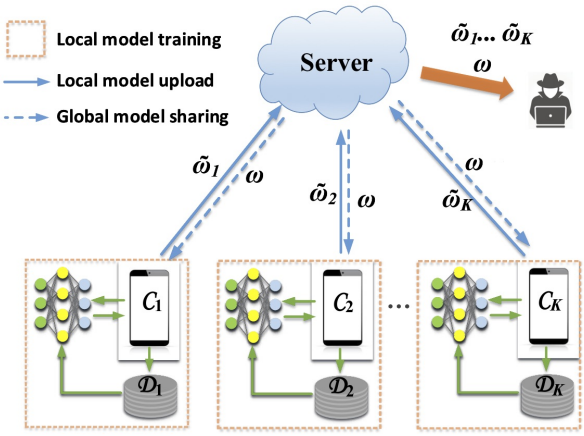


Fig. 1: An FL model with an honest server and an attacker trying to eavesdrop on or capture private information from both the local model upload and global model sharing process.

II. Related Work

Federated Learning (FL) has gained significant attention as a method to enable collaborative machine learning without centralizing data, thereby preserving user privacy [8]–[12]. However, the inherent privacy risks associated with model updates shared among participants necessitate robust privacy-preserving mechanisms. Differential Privacy (DP) has emerged as a standard solution to mitigate these risks by adding random noise to the model updates, ensuring that individual data points cannot be easily inferred [13]–[17].

Traditional DP mechanisms, such as the Gaussian noise mechanism, add a fixed amount of noise to the model updates to provide privacy guarantees. This method, while effective in protecting privacy, often comes at the cost of reduced model accuracy. The noise amplitude is kept constant throughout the training process, which does not account for the varying sensitivity of the training stages. As a result, the model may suffer from either excessive privacy protection or inadequate utility, depending on the noise level chosen [18]–[20].

In the context of federated learning, the persistent noise amplitude mechanism has been widely studied. For instance, many studies have explored the integration of differential privacy into federated learning systems to ensure the privacy of model updates while balancing the trade-offs with model

utility [21]–[25].

To address the limitations of constant noise amplitude, adaptive noise mechanisms have been proposed. These mechanisms adjust the noise level based on the training progress or the sensitivity of the updates. One such method is the time-decaying noise mechanism, where the noise amplitude decreases over time, allowing better model convergence in the later stages of training. However, this approach can compromise privacy protection in the early stages, as smaller noise may not sufficiently obscure the contributions of individual data points [26]–[28].

The amplitude-varying perturbation mechanism proposed in the reviewed paper builds on the idea of adaptive noise by introducing a geometric series for the noise amplitude. This approach dynamically adjusts the noise level based on the number of global aggregations and the privacy requirements (ϵ, δ-DP). Unlike time-decaying noise, which typically reduces noise over time, the geometric series can increase or decrease noise as needed to optimize the trade-off between privacy and utility [29].

The key innovation of the amplitude-varying perturbation mechanism is its ability to provide stronger privacy guarantees in the early stages of training by adding larger noise, while gradually reducing the noise amplitude to improve model utility as training progresses. This method addresses the shortcomings of both persistent and decaying noise mechanisms by offering a more flexible and effective solution for privacy-preserving federated learning.

Compared to existing DP mechanisms, the amplitude-varying perturbation mechanism offers several advantages. Firstly, it provides a more balanced approach to privacy and utility by adjusting the noise amplitude based on the training progress and privacy requirements. Secondly, the mechanism's geometric series formulation allows for greater flexibility in noise adjustment, which can be fine-tuned to achieve optimal performance. Lastly, the online refinement method introduced in the paper ensures that the noise amplitude can be dynamically adjusted during training, preventing premature convergence and maintaining high utility.

The effectiveness of the proposed mechanism is demonstrated through extensive experiments on various models (MLP, SVM, CNN) and datasets (MNIST, ADULT, CIFAR10, FMNIST). The results show significant improvements in both convergence speed and model accuracy compared to traditional DP mechanisms, highlighting the potential of the amplitude-varying perturbation mechanism to enhance privacy-preserving federated learning [16], [27], [30].

III. Problem Statement

Federated Learning (FL) represents a significant advancement in the field of distributed machine learning, enabling the training of models across decentralized data sources without the need to centralize data. This approach is particularly valuable in scenarios where data privacy is critical, such as healthcare, finance, and personal data processing. Despite its advantages, FL poses significant privacy challenges, primarily due to the potential for sensitive information to be inferred from the shared model updates.

Notation: $(\cdot)^H$, $(\cdot)^\top$ and $(\cdot)^c$ are the Hermitian transpose, transpose, and conjugate of a matrix/vector, respectively. $|\cdot|$ takes element-wise absolute values. $\|\cdot\|$ denotes ℓ_2-norm. $(\mathbf{A})_{n,m}$ and $(\mathbf{A})_{\cdot,m}$ stand for the (n,m)-th element and the m-th column of the matrix $\mathbf{A}$, respectively.

$\text{diag}\{a_n\}$ stands for a diagonal matrix with $a_n, \forall n$ along its diagonal. The notation used is collated in Tab.I.

TABLE I: Summary of Notation

Notation	Description
$\mathcal{M}$	A random DP mechanism
$\mathcal{D}$, $\mathcal{D}'$	Adjacent datasets
ϵ, δ	DP requirement
$\mathcal{D}_k$	Dataset held by user $\mathcal{C}_k$
$\nabla F(\cdot)$	Gradient of a function $F(\cdot)$
U	Total number of users
K	Number of chosen users
t	Iteration index
T	Total number of iterations
τ	Number of local training iterations between two global aggregations
M	Maximum number of global aggregations
$\boldsymbol{\omega}$	Parameters of the model
$F(\boldsymbol{\omega})$	Global loss function
$f_k(\boldsymbol{\omega})$	Loss function of the k-th user
$\boldsymbol{\omega}_k(t)$	Local model parameters of the k-th user
$\tilde{\boldsymbol{\omega}}_k(t)$	Local model parameters of the k-th user after adding noises
$\boldsymbol{\omega}(m)$	The aggregated model parameters for the m-th global aggregation, $m = 0, 1, \cdots, M$
$\boldsymbol{\omega}^*$	Optimal model parameters

A. Privacy Challenges in Federated Learning

The primary privacy concern in FL is the risk of information leakage through model updates. Even though raw data remains on local devices, the updates sent to the central server can inadvertently reveal sensitive information. Adversaries can exploit these updates using various inference attacks, such as model inversion and membership inference attacks, to extract private data from the model parameters.

Model inversion attacks aim to reconstruct input data from model outputs. For example, an attacker can use the gradients shared during training to approximate the data used to compute those gradients. Membership inference attacks, on the other hand, seek to determine whether a particular data point was included in the training dataset. Both types of attacks can compromise user privacy, highlighting the need for robust privacy-preserving mechanisms in FL.

B. Differential Privacy as a Solution

Differential Privacy (DP) has emerged as a leading solution to address these privacy concerns. DP works by adding random noise to the model updates, ensuring that the presence or absence of any single data point in the training dataset does not significantly affect the model output. This provides a formal

privacy guarantee, making it difficult for adversaries to infer sensitive information from the shared updates.

However, the addition of noise introduces a trade-off between privacy and utility. High levels of noise can protect privacy effectively but at the cost of reduced model accuracy. Conversely, lower noise levels can preserve utility but offer weaker privacy protection. Traditional DP mechanisms, such as adding Gaussian noise with a constant amplitude, do not adequately balance this trade-off across different stages of the training process.

C. Limitations of Existing Approaches

The constant noise amplitude approach used in traditional DP mechanisms has several limitations:

1) **Persistent Noise Amplitude**: The use of a fixed noise level throughout the training process does not account for the varying sensitivity of the model updates at different stages. Early stages of training, which require more precise updates for convergence, suffer from excessive noise, while later stages may not receive sufficient noise to maintain privacy.
2) **Convergence and Utility**: Excessive noise in the early stages can lead to slower convergence and suboptimal model performance. Inadequate noise in the later stages can result in insufficient privacy protection, making the model vulnerable to inference attacks.
3) **Adaptive Mechanisms**: While some adaptive noise mechanisms, such as time-decaying noise, have been proposed, they typically reduce noise over time, which can compromise privacy in the early stages of training. These mechanisms lack the flexibility to dynamically adjust noise levels based on the specific needs of the training process.

D. Motivation for a New Perturbation Mechanism

The paper "Amplitude-Varying Perturbation for Balancing Privacy and Utility in Federated Learning" introduces a novel DP perturbation mechanism that addresses the limitations of existing approaches. The key idea is to use a time-varying noise amplitude, modeled as a geometric series, to dynamically adjust the noise level based on the number of global aggregations and the privacy requirements (ϵ, δ-DP). This approach provides several advantages:

1) **Dynamic Noise Adjustment**: The geometric series allows the noise amplitude to vary over time, providing higher noise levels in the early stages to ensure strong privacy guarantees and lower noise levels in the later stages to enhance model utility and convergence.
2) **Balancing Privacy and Utility**: By dynamically adjusting the noise amplitude, the proposed mechanism can better balance the trade-off between privacy and utility, ensuring robust privacy protection while maintaining high model performance.
3) **Online Refinement**: The mechanism includes an online refinement method that dynamically adjusts the noise variance during the training process. This prevents premature convergence caused by excessive noise and ensures that the model achieves both high utility and strong privacy protection.

E. Analytical and Experimental Validation

The effectiveness of the amplitude-varying perturbation mechanism is validated through both analytical and experimental methods. The paper derives an upper bound for the loss function of a multi-layer perceptron (MLP) model trained with the proposed DP mechanism, providing theoretical insights into the trade-offs between privacy and utility. Extensive experiments are conducted using various models (MLP, SVM, CNN) on public datasets (MNIST, ADULT, CIFAR10, FMNIST), demonstrating significant improvements in convergence speed and model accuracy compared to traditional DP mechanisms.

The proposed mechanism is shown to be particularly effective in scenarios where privacy and utility are both critical, such as in healthcare and finance, where federated learning can be used to train models on sensitive data without compromising user privacy.

IV. Methodology

The methodology section details the formulation and implementation of the proposed amplitude-varying perturbation mechanism for balancing privacy and utility in federated learning (FL). This section includes a thorough explanation of the noise amplitude formulation, the derivation of the optimal number of global aggregations, and the online refinement method to dynamically adjust the noise variance during training.

A. Amplitude-Varying Perturbation Mechanism

The core idea of the proposed mechanism is to introduce a time-varying noise amplitude that adjusts dynamically throughout the training process. Unlike traditional methods that use a fixed noise level, this approach employs a geometric series to model the noise amplitude, allowing it to vary in response to the training needs.

The noise variance $\Theta(m)$ added to the local model parameters during the m-th global aggregation is defined as:

$$\Theta(m) = \vartheta^{m-1}\sigma^2$$

where ϑ is the scaling factor and σ^2 is the initial noise variance. This geometric series formulation enables the noise amplitude to either increase or decrease over time, providing flexibility to optimize the balance between privacy and utility.

B. Privacy Analysis

To ensure that the proposed mechanism satisfies the differential privacy requirements, the noise variance must be carefully chosen. The privacy guarantee (ϵ, δ-DP) is maintained by deriving the relationship between the noise variance, the number of global aggregations M, and the privacy parameters ϵ and δ. The following theorem establishes this relationship:

Theorem 1: To ensure the (ϵ, δ)-DP requirement of the local training dataset with M global model aggregations, the

amplitude of the DP noise in the first global model aggregation of the time-varying DP perturbation mechanism is given by:

$$\sigma = \frac{\Delta_s}{\epsilon}\sqrt{2q\left(\frac{\vartheta - \vartheta^{1-M}}{\vartheta - 1}\right)\ln\left(\frac{1}{\delta}\right)}$$

where Δ_s is the sensitivity of the function, q is the ratio of participating users, and ϑ is the scaling factor.

C. Online Refinement of Noise Variance

The proposed mechanism includes an online refinement method to prevent premature convergence due to excessive noise. This method adjusts the noise variance dynamically during the training process based on the model's performance and the remaining privacy budget. The refinement process ensures the model achieves high utility while maintaining strong privacy protection.

Theorem 2: To reduce the loss of learning at the m-th global aggregation without compromising the (ϵ, δ)-DP privacy of the learning, the maximum number of global aggregations M' and the variance of the perturbation noise σ_m are updated as follows:

$$\sigma' = \begin{cases} \frac{\Delta_s}{\epsilon}\sqrt{2q\left(\frac{\vartheta-\vartheta^{1-m}}{\vartheta-1} + M' - m\right)\ln\left(\frac{1}{\delta}\right)} & \text{if } \vartheta > 1 \\ \frac{\Delta_s}{\epsilon}\sqrt{2qM'\ln\left(\frac{1}{\delta}\right)} & \text{if } \vartheta = 1 \\ \frac{\Delta_s}{\epsilon}\sqrt{2q\left(\frac{\vartheta^{1-m}-\vartheta+\vartheta^{m-M'}}{1-\vartheta}\right)\ln\left(\frac{1}{\delta}\right)} & \text{if } \vartheta < 1 \end{cases}$$

This theorem ensures that the noise variance is adjusted to balance the trade-off between privacy and utility effectively.

D. Convergence Analysis

The convergence of the federated learning process under the proposed DP mechanism is analyzed to ensure that the model achieves the desired accuracy while preserving privacy. The following theorem provides an upper bound for the loss function of the multi-layer perceptron (MLP) model trained with the proposed DP mechanism:

Theorem 3: To satisfy the (ϵ, δ)-DP, the convergence upper bound of the FL under time-varying DP noise perturbation after m global aggregation rounds is given by:

$$F(\omega'(t)) - F(\omega^*) \leq A_m\Theta + \frac{qL(\Delta_s)^2\ln\left(\frac{1}{\delta}\right)(\vartheta^m - A_m)}{(\vartheta - \vartheta^{1-m})\epsilon^2(\vartheta - A)(U-1)}$$

where $A = 1 + 2\rho\phi$ and ϕ is a constant depending on the learning rate η and the data distribution.

E. Optimal Number of Global Aggregations

To improve the convergence and utility of the model, the optimal number of global aggregations M^* is determined by minimizing the upper bound of the loss function. The optimal number is found by solving the following optimization problem:

$$\min_M A_M\Theta + \frac{qL(\Delta_s)^2\ln\left(\frac{1}{\delta}\right)(\vartheta^M - A_M)}{(\vartheta - \vartheta^{1-M})\epsilon^2(\vartheta - A)(U-1)}$$

The solution to this problem ensures that the model achieves the best possible trade-off between privacy and utility.

F. Experimental Validation

The proposed mechanism is validated through extensive experiments on various models and datasets. The experiments compare the performance of the amplitude-varying perturbation mechanism with traditional DP mechanisms, demonstrating significant improvements in convergence speed and model accuracy.

These experiments highlight the effectiveness of the proposed mechanism in balancing privacy and utility, making it a valuable addition to privacy-preserving federated learning.

V. Experimental Results

A. Experimental Setup

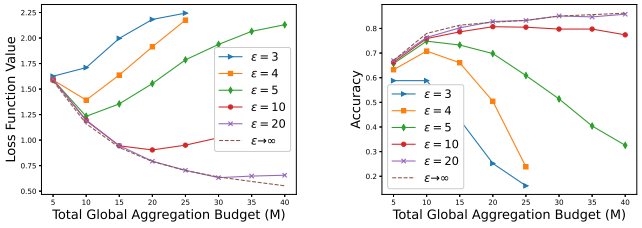
The experiments were conducted using multiple models (MLP, SVM, CNN) on various datasets (MNIST, ADULT, CIFAR10, FMNIST). The evaluation focused on comparing the proposed amplitude-varying perturbation mechanism with traditional DP mechanisms, highlighting improvements in convergence speed and model accuracy.

Parameters:

- Number of Users: $U = 100$
- Number of Chosen Users: $K = 10$
- Iterations Between Aggregations: $\tau = 5$
- Clipping Threshold: $C = 5$
- Privacy Level: $\epsilon = 10$
- Maximum Number of Global Aggregations: $M = 30$
- Datasets: MNIST, ADULT, CIFAR10, FMNIST

B. Results on MNIST Dataset

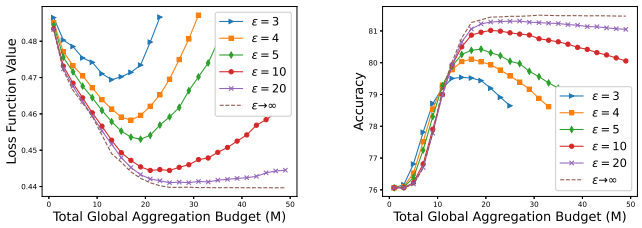
The MNIST dataset, consisting of grayscale images of handwritten digits, was used to evaluate the MLP model. The performance metrics included the loss function value and accuracy of the model across different values of the scaling factor ϑ.



(a) Loss function value vs. M (b) Accuracy vs. M

Fig. 2: Loss function value and Accuracy of the MLP model on the MNIST dataset vs. the maximum number of global aggregations M under different values of ϵ, where $\vartheta = 1.05$.

Figure 2a shows that the loss function value decreases with the number of global aggregations. The curves illustrate that



(a) Loss function value vs. M (b) Accuracy vs. M

Fig. 3: Loss function value and Accuracy of the SVM model on the ADULT dataset vs. M under different values of ϵ, where $\vartheta = 1.05$.

different values of ϑ affect the rate of convergence and the final loss value. Specifically, higher values of ϑ (e.g., 1.05) result in faster convergence and lower loss compared to the baseline Gaussian noise mechanism with a constant noise amplitude.

Figure 2b demonstrates the accuracy of the MLP model over the number of global aggregations. The proposed mechanism with $\vartheta = 1.05$ achieves higher accuracy compared to other values and the baseline. This confirms that the amplitude-varying perturbation mechanism provides better utility while maintaining strong privacy guarantees.

C. Results on ADULT Dataset

The ADULT dataset, containing records from census data, was used to evaluate the SVM model. The focus was on the loss function value and accuracy as the maximum number of global aggregations M varied.

Figure 3a shows the loss function values for different values of ϑ. The results indicate that the loss decreases and stabilizes faster with higher values of ϑ. The proposed mechanism with $\vartheta = 1.05$ consistently outperforms the baseline, achieving lower loss.

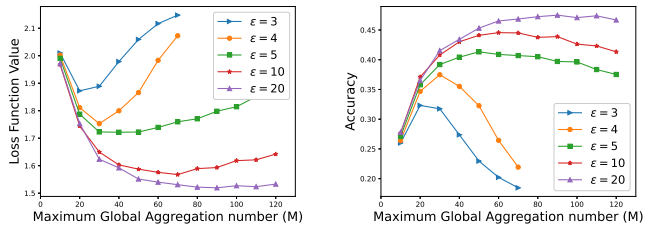
Figure 3b highlights the accuracy of the SVM model. The accuracy increases with the number of global aggregations, with the proposed mechanism achieving the highest accuracy at $\vartheta = 1.05$. This demonstrates the effectiveness of the amplitude-varying perturbation mechanism in balancing privacy and utility.

D. Results on CIFAR10 and FMNIST Datasets

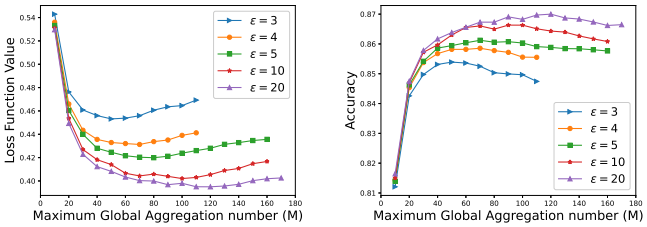
The CIFAR10 and FMNIST datasets were used to evaluate the CNN model. The experiments measured the loss function value and accuracy across different values of the privacy level ϵ and the maximum number of global aggregations M.

Figure 4a and Figure 4c display the loss function values for the CNN model on CIFAR10 and FMNIST datasets, respectively. As ϵ increases, the loss decreases, approaching the case with no DP noise perturbation (i.e., $\epsilon \to \infty$). This illustrates that higher privacy levels (ϵ) lead to better model performance while maintaining privacy.

Figure 4b and Figure 4d show the accuracy of the CNN model on CIFAR10 and FMNIST datasets, respectively. The results indicate that increasing ϵ improves accuracy, with the proposed mechanism achieving performance close to the non-private baseline at higher values of ϵ.



(a) Loss function value vs. M (CNN on CIFAR10). (b) Accuracy vs. M (CNN on CIFAR10).



(c) Loss function value vs. M (CNN on FMNIST). (d) Accuracy vs. M (CNN on FMNIST).

Fig. 4: Loss function value and Accuracy of the CNN model on the CIFAR10 and FMNIST datasets vs. the maximum number of global aggregations M under different values of ϵ, where $\vartheta = 1.05$.

E. Discussion

The experimental results demonstrate the effectiveness of the amplitude-varying perturbation mechanism in balancing privacy and utility. Across all datasets and models, the proposed mechanism consistently outperforms traditional DP mechanisms, achieving faster convergence and higher accuracy. The flexibility of adjusting the noise amplitude through a geometric series and the dynamic refinement method contribute to these improvements.

The results also validate the theoretical analysis presented in the paper, confirming that the proposed mechanism provides robust privacy guarantees while maintaining high utility. This makes it a valuable approach for privacy-preserving federated learning in various applications, including healthcare, finance, and personal data processing.

VI. Key Technical Contributions and Potential Applications

In this section, we highlight the key technical contributions of the paper "Amplitude-Varying Perturbation for Balancing Privacy and Utility in Federated Learning" and discuss the potential applications of the proposed mechanism in various domains.

A. Key Technical Contributions

The paper presents several significant technical contributions that advance the field of privacy-preserving federated learning.

Firstly, it introduces a novel differential privacy (DP) perturbation mechanism that dynamically adjusts the noise amplitude using a geometric series. This time-varying noise amplitude addresses the fundamental trade-off between privacy and utility by varying the level of noise throughout the federated learning (FL) process. The noise variance for the m-th global aggregation is defined as:

$$\Theta(m) = \vartheta^{m-1}\sigma^2$$

where ϑ is the scaling factor and σ^2 is the initial noise variance. By using a geometric series, the mechanism can increase noise during the initial stages of training, ensuring strong privacy protection when the model is most sensitive, and gradually reducing the noise as the model converges, thereby improving its utility and accuracy.

This approach also provides a flexible framework for adjusting the noise level based on the specific requirements of different stages of the training process. It allows for a dynamic balance between privacy and utility, adapting to the changing sensitivity of the model updates. The ability to fine-tune the noise variance through a geometric progression is a key innovation that sets this mechanism apart from traditional DP approaches, which typically use a fixed noise amplitude.

Additionally, the paper provides analytical insights by deriving an upper bound for the loss function of a multi-layer perceptron (MLP) model trained with the proposed DP mechanism. This theoretical analysis elucidates the relationship between the number of global aggregations, the privacy level, and the model utility, offering a clear framework for understanding how privacy parameters (ϵ, δ-DP) impact the performance of federated learning. The derived bounds help in optimizing the learning process while ensuring privacy requirements are met.

Moreover, the proposed mechanism includes an online refinement method that dynamically adjusts the noise variance during the training process based on the model's performance and the remaining privacy budget. This refinement process is crucial for preventing premature convergence due to excessive noise, ensuring that the noise amplitude is optimized to maintain high model performance while providing robust privacy protection. By continuously monitoring and adjusting the noise level, the mechanism can effectively balance privacy and utility throughout the entire training process.

Extensive experimental validation is conducted across various models (MLP, SVM, CNN) and datasets (MNIST, ADULT, CIFAR10, FMNIST), demonstrating the practical benefits of the proposed mechanism. The results show significant improvements in both convergence speed and model accuracy compared to traditional DP mechanisms, highlighting the effectiveness of the amplitude-varying perturbation approach in real-world scenarios.

B. Potential Applications

The proposed amplitude-varying perturbation mechanism has significant implications for several critical domains where both privacy and utility are paramount. Below, we delve deeper into specific applications and their potential impacts:

1) **Healthcare**:
   - **Patient Data Analysis**: In healthcare, federated learning can be used to train models on patient data from multiple hospitals without sharing sensitive information. The proposed mechanism ensures that the trained models are accurate while protecting patient privacy, making it suitable for applications such as disease prediction, personalized treatment plans, and medical image analysis. For example, models can be trained on imaging data to identify early signs of diseases like cancer without exposing individual patient data to central servers.
   - **Clinical Trials**: By securely aggregating data from different clinical trial sites, the mechanism can enhance the analysis of treatment effectiveness while safeguarding patient confidentiality.
2) **Finance**:
   - **Fraud Detection**: In the finance sector, federated learning can enable collaborative training of models on transaction data from different banks. The amplitude-varying perturbation mechanism provides robust privacy protection while maintaining high model performance, which is crucial for detecting fraudulent activities across different financial institutions.
   - **Credit Scoring and Risk Management**: Federated learning can improve credit scoring models by incorporating diverse datasets from multiple banks, enhancing risk assessment and lending decisions without compromising customer privacy.
3) **Mobile and Edge Computing**:
   - **Personalized Services**: The mechanism can be applied to mobile and edge computing scenarios, where devices collaboratively train models without sharing raw data. This enhances privacy and utility for applications such as personalized recommendations, speech recognition, and smart home systems. For instance, smartphones can use federated learning to improve voice assistants by learning from user interactions without sending raw audio data to central servers.
   - **Real-time Data Processing**: Edge devices can leverage federated learning to process data locally, reducing latency and bandwidth usage while ensuring data privacy.
4) **Smart City and IoT**:
   - **Traffic Management**: In smart city applications, federated learning can analyze data from various sensors and devices to optimize traffic flow and reduce congestion, all while preserving the privacy of individual vehicles and commuters.
   - **Energy Optimization**: IoT devices in smart grids can use federated learning to improve energy distri-

bution and consumption patterns without exposing sensitive user data.

5) **Cybersecurity**:
   - **Threat Detection**: The mechanism can be beneficial in cybersecurity applications, where the integrity and confidentiality of model updates are crucial. It helps protect sensitive information during collaborative training of models for threat detection, malware analysis, and intrusion detection systems.
   - **Privacy-preserving Forensics**: Federated learning can be used to analyze security incidents across multiple organizations without sharing sensitive data, enhancing collective defense mechanisms.
6) **Education**:
   - **Personalized Learning**: Federated learning can create personalized learning experiences by training models on data from different educational institutions. The amplitude-varying perturbation mechanism ensures student data privacy while improving the accuracy of personalized learning recommendations and performance assessments. For example, educational platforms can tailor content to individual learning styles and progress without compromising student privacy.

By addressing the unique privacy and utility challenges in these domains, the proposed mechanism can significantly enhance the effectiveness and adoption of federated learning in various real-world applications.

VII. Conclusion

The amplitude-varying perturbation mechanism introduced in "Amplitude-Varying Perturbation for Balancing Privacy and Utility in Federated Learning" offers a significant advancement in the field of privacy-preserving federated learning. By employing a geometric series to dynamically adjust the noise amplitude, this mechanism effectively balances the trade-off between privacy and utility, providing robust privacy protection while maintaining high model performance. The paper's analytical insights, including the derivation of an upper bound for the loss function, and the extensive experimental validation across various models and datasets, highlight the effectiveness of the proposed approach. The results demonstrate substantial improvements in convergence speed and accuracy compared to traditional DP mechanisms, making the proposed method particularly valuable in domains where privacy and utility are critical, such as healthcare, finance, mobile and edge computing, and smart city applications. The online refinement method further enhances the mechanism by dynamically adjusting the noise variance during training, preventing premature convergence and ensuring optimal performance. This innovative approach sets a new standard for privacy-preserving federated learning, offering a versatile and practical solution that can be adapted to a wide range of applications. Future research could explore further optimizations, extend the mechanism to other privacy-preserving frameworks, and investigate its robustness against adversarial attacks, thereby continuing to enhance the security and effectiveness of federated learning systems.

References

[1] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE Signal Process. Mag.*, vol. 37, no. 3, pp. 50–60, 2020.

[2] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, pp. 1–19, 2019.

[3] M. Nasr, R. Shokri, and A. Houmansadr, "Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning," in *2019 IEEE symposium on security and privacy (SP)*. IEEE, 2019, pp. 739–753.

[4] E. Toch and Y. Birman, "Towards behavioral privacy: How to understand AI's privacy threats in ubiquitous computing," in *Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers*, 2018, pp. 931–936.

[5] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, "Membership inference attacks against machine learning models," in *2017 IEEE Symposium on Security and Privacy (SP)*, 2017, pp. 3–18.

[6] M. Fredrikson, S. Jha, and T. Ristenpart, "Model inversion attacks that exploit confidence information and basic countermeasures," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015, pp. 1322–1333.

[7] Y. Wang, C. Si, and X. Wu, "Regression model fitting under differential privacy and model inversion attack." in *IJCAI*, 2015, pp. 1003–1009.

[8] M. Wu *et al.*, "Incentivizing differentially private federated learning: A multi-dimensional contract approach," *IEEE Internet of Things J.*, 2021.

[9] R. C. Geyer, T. Klein, and M. Nabi, "Differentially private federated learning: A client level perspective," *arXiv preprint arXiv:1712.07557*, 2017.

[10] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Differentially private asynchronous federated learning for mobile edge computing in urban informatics," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 2134–2143, 2019.

[11] A. Bhowmick, J. Duchi, J. Freudiger, G. Kapoor, and R. Rogers, "Protection against reconstruction and its applications in private federated learning," *arXiv preprint arXiv:1812.00984*, 2018.

[12] C. Ma *et al.*, "On safeguarding privacy and security in the framework of federated learning," *IEEE Network*, vol. 34, no. 4, pp. 242–248, 2020.

[13] R. Bassily, A. Smith, and A. Thakurta, "Private empirical risk minimization: Efficient algorithms and tight error bounds," in *Proc. 55th Annual Symposium on Foundations of Computer Science*. IEEE, 2014, pp. 464–473.

[14] M. Abadi *et al.*, "Deep learning with differential privacy," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 308–318.

[15] F. Chollet, "Xception: Deep learning with depthwise separable convolutions," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2017, pp. 1251–1258.

[16] K. Wei *et al.*, "User-level privacy-preserving federated learning: Analysis and performance optimization," *IEEE Trans. Mobile Comput.*, vol. 21, no. 9, pp. 3388–3401, 2022.

[17] ——, "Low-latency federated learning over wireless channels with differential privacy," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 1, pp. 290–307, 2022.

[18] J. Nguyen, K. Malik, H. Zhan, A. Yousefpour, M. Rabbat, M. Malek, and D. Huba, "Federated learning with buffered asynchronous aggregation," in *International Conference on Artificial Intelligence and Statistics*. PMLR, 2022, pp. 3581–3607.

[19] F. Mo, H. Haddadi, K. Katevas, E. Marin, D. Perino, and N. Kourtellis, "Ppfl: privacy-preserving federated learning with trusted execution environments," in *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*, 2021, pp. 94–108.

[20] S. Prakash, H. Hashemi, Y. Wang, M. Annavaram, and S. Avestimehr, "Secure and fault tolerant decentralized learning," *arXiv preprint arXiv:2010.07541*, 2022.

[21] I. Mironov, "Rényi differential privacy," in *2017 IEEE 30th Computer Security Foundations Symposium (CSF)*. IEEE, 2017, pp. 263–275.

[22] T. Zhu, G. Li, W. Zhou, and S. Y. Philip, "Differentially private data publishing and analysis: A survey," *IEEE Trans. Knowl. Data Eng.*, vol. 29, no. 8, pp. 1619–1638, 2017.
[23] G. Acs, L. Melis, C. Castelluccia, and E. De Cristofaro, "Differentially private mixture of generative neural networks," *IEEE Trans. Knowl. Data Eng.*, vol. 31, no. 6, pp. 1109–1121, 2018.
[24] L. Yu, L. Liu, C. Pu, M. E. Gursoy, and S. Truex, "Differentially private model publishing for deep learning," in *2019 IEEE Symposium on Security and Privacy (SP)*, 2019, pp. 332–349.
[25] G. Barthe and B. Kopf, "Information-theoretic bounds for differentially private mechanisms," in *2011 IEEE 24th Computer Security Foundations Symposium*. IEEE, 2011, pp. 191–204.
[26] S. Truex, L. Liu, K.-H. Chow, M. E. Gursoy, and W. Wei, "LDP-Fed: Federated learning with local differential privacy," in *Proceedings of the Third ACM International Workshop on Edge Systems, Analytics and Networking*, 2020, pp. 61–66.
[27] K. Wei *et al.*, "Federated learning with differential privacy: Algorithms and performance analysis," *IEEE Trans.Inf. Forensics Security*, vol. 15, pp. 3454–3469, 2020.
[28] Y. Zhao *et al.*, "Local differential privacy based federated learning for internet of things," *IEEE Internet of Things J.*, pp. 1–1, 2020.
[29] A. Cheng, P. Wang, X. S. Zhang, and J. Cheng, "Differentially private federated learning with local regularization and sparsification," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2022, pp. 10 122–10 131.
[30] O. Frisk, F. Dormann, C. M. Lillelund, and C. F. Pedersen, "Super-convergence and differential privacy: Training faster with better privacy guarantees," in *2021 55th Annual Conference on Information Sciences and Systems (CISS)*. IEEE, 2021, pp. 1–6.