Journal of Computer Networks, Architecture and High Performance Computing
Volume 7, Number 1, Januari 2025
https://doi.org/10.47709/cnahpc.v7i1.5385

Submitted : Jan 23, 2025
Accepted : Jan 23, 2025
Published : Jan 25, 2025

A Novel Privacy-Preserving Algorithm for Secure Data Sharing in Federated Learning Frameworks

Fahmy Ferdian Dalimarta[1)*], Nina Faoziyah[2)], Doni Setiawan[3)]
[1,2,3)] Universitas Muhammadiyah Tegal, Indonesia
[1)]fahmy@umtegal.ac.id, [2)]ninafaoziyah@gmail.com, [3)]donisetiawan@umtegal.ac.id,

ABSTRACT

Federated Learning (FL) has emerged as a promising paradigm for the collaborative training of machine learning models across decentralized devices while preserving data privacy. However, ensuring data security and privacy during model updates remains a critical challenge, particularly in scenarios that involve sensitive data. This study proposes a novel Privacy-Preserving Algorithm (PPA-FL) designed to enhance data security and mitigate privacy leakage risks in FL frameworks. The algorithm integrates advanced encryption techniques, such as homomorphic encryption, with differential privacy to secure model updates without compromising the utility. Furthermore, it incorporates a dynamic noise-adjustment mechanism to adaptively balance privacy and model accuracy. Extensive experiments on benchmark datasets demonstrate that PPA-FL achieves a competitive trade-off between privacy protection and model performance compared to existing methods. The proposed approach is computationally efficient and scalable, making it suitable for real-world applications in healthcare, finance, and the IoT environment. This research contributes to advancing secure data-sharing practices in federated learning, fostering the broader adoption of privacy-preserving machine learning solutions.

Keywords: Data Security; Differential Privacy; Federated Learning; Homomorphic Encryption; Privacy-Preserving Algorithm

INTRODUCTION

In the era of digital transformation, the exponential growth of data has necessitated innovative approaches to machine learning and data analysis. Federated Learning (FL) has emerged as a paradigm-shifting framework that enables the decentralized training of machine learning models without the necessity of centralizing sensitive data. By leveraging the computational capabilities of distributed devices, FL facilitates collaborative learning while preserving the privacy of the local data. This characteristic has rendered FL particularly valuable in domains such as healthcare, finance, and the Internet of Things (IoT), where data privacy is of paramount importance. Notwithstanding its potential, FL encounters substantial challenges in preserving the security and privacy of data during model training and update exchanges. Conventional approaches to FL, while efficacious in safeguarding raw data, frequently render model updates susceptible to adversarial attacks including reconstruction and inference attacks. These vulnerabilities may result in privacy breaches, undermining the trustworthiness of FL systems, and impeding their widespread adoption.

To address these challenges, researchers have investigated various privacy-preserving mechanisms including encryption techniques and differential privacy. However, these methods frequently require trade-offs among privacy, computational efficiency, and model performance. Achieving an optimal balance remains an unresolved issue, particularly in resource-constrained environments such as Internet of Things (IoT) systems and edge computing networks.

This study proposes a novel Privacy-Preserving Algorithm for Federated Learning (PPA-FL) to enhance data security and mitigate privacy leakage risks in FL frameworks. The proposed algorithm integrates

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 7, Number 1, Januari 2025
https://doi.org/10.47709/cnahpc.v7i1.5385

Submitted : Jan 23, 2025
Accepted : Jan 23, 2025
Published : Jan 25, 2025

advanced homomorphic encryption with differential privacy, enabling secure and efficient model updates without compromising the performance. Furthermore, it introduces a dynamic noise adjustment mechanism that adaptively balances privacy protection and model accuracy, thereby addressing the limitations of static noise-injection techniques. The main contributions of this study are as follows.

1. A Novel Privacy-Preserving Algorithm combines homomorphic encryption and differential privacy to secure model updates effectively.
2. The dynamic noise adjustment mechanism adaptively modulates the level of noise added to the model updates, achieving an optimal balance between privacy and accuracy.
3. We evaluate the proposed algorithm on benchmark datasets and compare it with state-of-the-art methods to demonstrate its efficacy, scalability, and computational efficiency.

The remainder of this paper is organized as follows: Section 2 provides a comprehensive review of related literature on privacy-preserving FL techniques. Section 3 describes the design and methodology of the proposed PPA-FL method. Section 4 presents the experimental results and subsequent analysis. Section 5 discusses the practical implications and potential applications of the research and concludes the study with insights into future research directions.

LITERATURE REVIEW

Federated Learning (FL) is a rapidly evolving field, and substantial research efforts have been dedicated to addressing privacy and security concerns. Existing privacy-preserving techniques can be broadly categorized as encryption-based, differential-privacy, and hybrid models that integrate multiple approaches.

Encryption-Based Methods

Encryption techniques, particularly homomorphic encryption, have garnered significant attention in the domain of data security because of their unique capacity to perform computations on encrypted data without requiring decryption. This capability is especially advantageous in environments where data confidentiality is of paramount importance, such as cloud computing and healthcare. Several studies have pioneered a fully homomorphic encryption scheme that facilitates arithmetic operations on ciphertexts, thereby enabling secure data processing while maintaining confidentiality (Agarwal & Shrivastava, 2021; Jung et al., 2021). This innovation has been further investigated in various applications including healthcare data security, where the protection of sensitive patient information is critical (Ali et al., 2023).

Despite the advantages of homomorphic encryption, it is imperative to acknowledge the computational overhead associated with these techniques. The complexity of operations on encrypted data frequently results in substantial performance costs, which can render them impractical in resource-constrained environments (Chatterjee & Sengupta, 2018). For instance, although homomorphic encryption enables secure computations, the processing time and resource requirements can be prohibitive, particularly in scenarios involving large datasets or real-time processing requirements (Ngabo & El Beqqali, 2019). This challenge has prompted researchers to investigate optimization strategies and alternative encryption methods that balance security and efficiency (Cidem Dogan & Altindis, 2020; Jung et al., 2021).

Moreover, the integration of homomorphic encryption into various systems, such as wireless sensor networks and cloud infrastructure, has demonstrated its potential to enhance data security while addressing the challenges of computational overhead (Idris & issahku, 2024; Salim et al., 2021). However, the tradeoff between security and performance remains a critical consideration for practitioners and researchers alike, necessitating the ongoing exploration of hybrid approaches that can leverage the strengths of multiple encryption techniques (K L & Nair, 2019; Salim et al., 2021).

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 7, Number 1, Januari 2025
https://doi.org/10.47709/cnahpc.v7i1.5385

Submitted : Jan 23, 2025
Accepted : Jan 23, 2025
Published : Jan 25, 2025

Differential Privacy

Differential privacy has emerged as a fundamental approach for safeguarding individual contributions within aggregated data, particularly in machine learning contexts. A significant advancement in this area is the development of a differentially private stochastic gradient descent (DP-SGD) algorithm that incorporates noise into gradient updates to obscure individual data points. This method facilitates the training of models while maintaining privacy guarantees, thereby enabling the utilization of sensitive data without compromising individual privacy (Parker et al., 2022a; Ziegler et al., 2022a). The integration of differential privacy into machine learning frameworks has been widely acknowledged for its potential to protect user data during model training, rendering it a critical area of research in privacy-preserving data analysis (JUNG et al., 2021a; Park et al., 2019).

However, the application of static noise injection methods in DP-SGD can result in a reduction in the model accuracy, particularly in scenarios where data are limited. The trade-off between privacy and utility is a well-documented challenge in the implementation of differential privacy (H. Liu et al., 2018a; Ma et al., 2024). For instance, although the addition of noise can effectively protect individual data points, excessive noise can obscure the underlying patterns in the data, resulting in models that exhibit poor performance on unseen data (H. Wang et al., 2021a; Y. Wang et al., 2019). Researchers have observed that this issue is particularly pronounced in applications involving small datasets, where the signal-to-noise ratio is crucial for the model performance (Park et al., 2021; Shi & Zhu, 2024). Consequently, there is increasing interest in adaptive noise mechanisms that can dynamically adjust the magnitude of noise based on data characteristics and the desired level of privacy (Fan & Cui, 2021; Thantharate et al., 2024).

Moreover, recent studies have explored alternative strategies to enhance the effectiveness of differential privacy, while mitigating its impact on model accuracy. Techniques such as concentrated differential privacy and personalized differential privacy have been proposed to provide stronger privacy guarantees without significantly compromising the utility (Park et al., 2019; Z. Zhang et al., 2021). These methods aim to optimize the balance between privacy and accuracy, allowing for more precise control over the privacy budget and noise-injection processes (B. Liu et al., 2024; H. Liu et al., 2021). As the field advances, the development of hybrid models that integrate differential privacy with other privacy-preserving techniques such as federated learning is also being investigated to further enhance data security while maintaining model performance (Li et al., 2023a; Y. Zhang et al., 2023).

Hybrid Models

Hybrid approaches that integrate encryption and differential privacy have emerged as promising solutions for enhancing data protection in various applications, particularly in federated learning (FL) contexts. These approaches aim to leverage the strengths of both homomorphic encryption and differential privacy to provide robust privacy guarantees, while facilitating effective data analysis. For instance, researchers have proposed frameworks that combine homomorphic encryption with local differential privacy, thereby enabling secure computations on sensitive data without exposing individual contributions (Li et al., 2023b; Ziegler et al., 2022b). This integration is particularly advantageous in scenarios where data are distributed across multiple devices because it allows collaborative learning while maintaining stringent privacy standards.

Nevertheless, the implementation of hybrid approaches remains a challenge. A primary concern is the balance between the privacy guarantees provided by these methods, the computational efficiency, and the model performance. The computational overhead associated with homomorphic encryption can be substantial, often resulting in increased latency and resource consumption (Yang et al., 2024). Furthermore, while differential privacy effectively mitigates data reconstruction attacks, the noise injection required to achieve privacy can compromise the accuracy of the models, particularly in data-scarce environments (JUNG et al., 2021b; H. Wang et al., 2021b). This trade-off between privacy and utility constitutes a critical

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 7, Number 1, Januari 2025
https://doi.org/10.47709/cnahpc.v7i1.5385

Submitted : Jan 23, 2025
Accepted : Jan 23, 2025
Published : Jan 25, 2025

consideration that researchers must address when designing hybrid privacy-preserving frameworks.

Recent studies have explored various strategies to optimize the performance of hybrid models. For instance, adaptive noise mechanisms and dynamic privacy budgets have been proposed to enhance the utility of differentially private models while maintaining robust privacy guarantees (H. Liu et al., 2018b; Parker et al., 2022b). Moreover, advancements in federated learning algorithms that incorporate both homomorphic encryption and differential privacy have demonstrated potential in improving model accuracy without compromising privacy (Johnson et al., 2018). These developments underscore the efficacy of hybrid approaches in not only safeguarding sensitive data but also preserving the effectiveness of machine learning models in practical applications.

Notwithstanding these advancements, extant methodologies have limitations in terms of scalability, adaptability, and practical implementation. Our proposed algorithm addresses these deficiencies by introducing a dynamic noise adjustment mechanism and optimizing computational efficiency, thereby rendering it suitable for real-world FL scenarios.

METHOD

The design and methodology of the proposed Privacy-Preserving Algorithm for Federated Learning (PPA-FL) emphasize the integration of robust security measures while maintaining computational efficiency and model performance. Figure 1 illustrates the key components of PPA-FL.

The proposed system comprises three main entities. First, clients distribute devices that train local models using private datasets and participate in a Federated Learning (FL) process. The aggregator is a central server responsible for aggregating encrypted model updates and orchestrating the FL process. Finally, the Adversary Model is a threat model that assumes potential eavesdropping on communication channels, and attempts to reconstruct sensitive information from model updates.

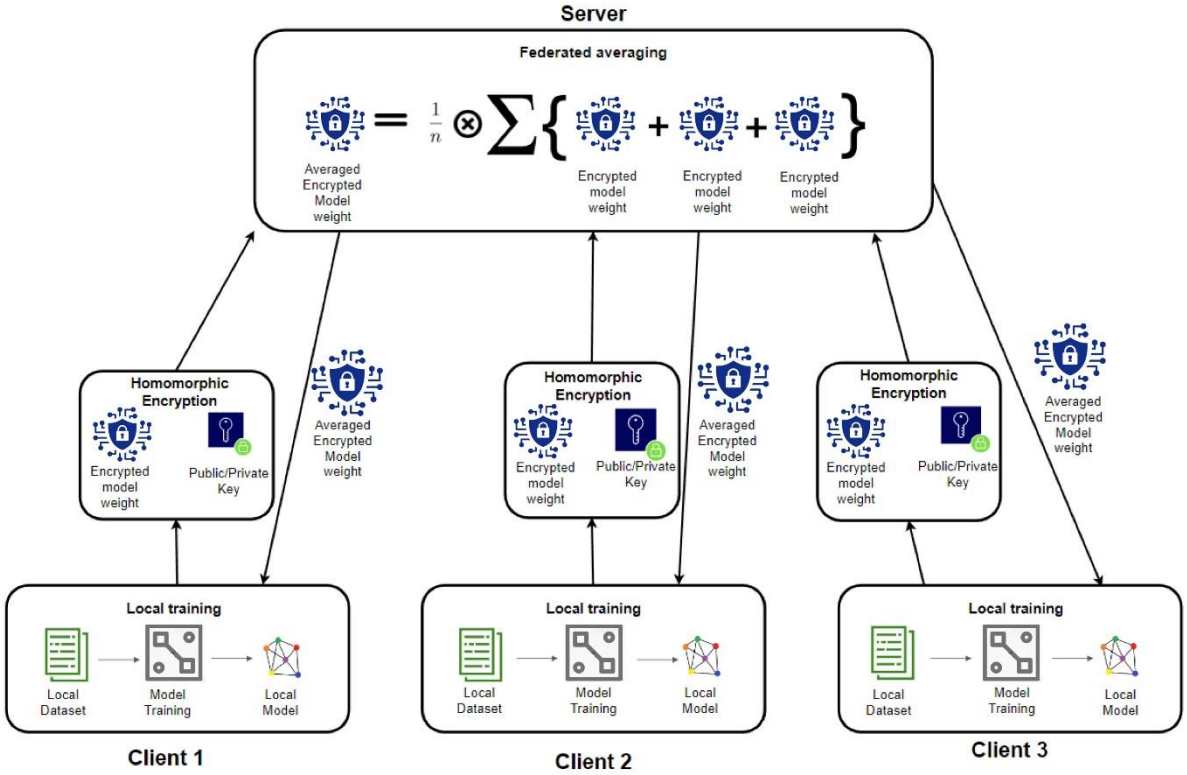

Fig. 1 Key Components of PPA-FL

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 7, Number 1, Januari 2025
https://doi.org/10.47709/cnahpc.v7i1.5385

Submitted : Jan 23, 2025
Accepted : Jan 23, 2025
Published : Jan 25, 2025

In Federated Learning, each client i has its own local data D_i, and the goal is to minimize the global loss function $F(\theta)$ while preserving privacy. The objective can be written as

$$F(\theta) = \frac{1}{N}\sum_{i=1}^{N}\mathbb{E}_{D_i}[\mathcal{L}_i(\theta)] \quad (1)$$

where $\mathcal{L}_i(\theta)$ is the local loss function for client i, N is the number of clients, and θ is the model parameter.

Homomorphic encryption enables the secure computation of encrypted data. In PPA-FL, each client encrypts its local model updates by using a lightweight homomorphic encryption scheme before transmitting them to the aggregator. The aggregator performs arithmetic operations directly on the encrypted updates without decryption, thereby ensuring data confidentiality throughout the aggregation process. To mitigate privacy leakage, differential privacy is applied to the model updates prior to encryption. The Differential Privacy mechanism can be applied to model updates, as follows:

$$\theta'_i = \theta_i + \mathcal{N}(0, \sigma^2) \quad (2)$$

where θ'_i is the noisy update sent by client i, and $\mathcal{N}(0, \sigma^2)$ is a Gaussian noise term with a standard deviation σ, which is tuned to control the privacy level. Then to ensure privacy during model updates, clients can share only their gradients or parameters with the server after applying some privacy-preserving techniques. A typical update can be written as:

$$\theta_i^{t+1} = \theta_i^t - \eta\nabla\mathcal{L}_i(\theta_i^t) \quad (3)$$

here, η is the learning rate, and the gradient $\nabla\mathcal{L}_i(\theta_i^t)$ can be encrypted or perturbed with noise.

The PPA-FL incorporates a noise-injection mechanism that perturbs updates with controlled noise. The noise level was dynamically adjusted based on the sensitivity of the dataset and the desired privacy budget, achieving an optimal balance between privacy protection and model accuracy.

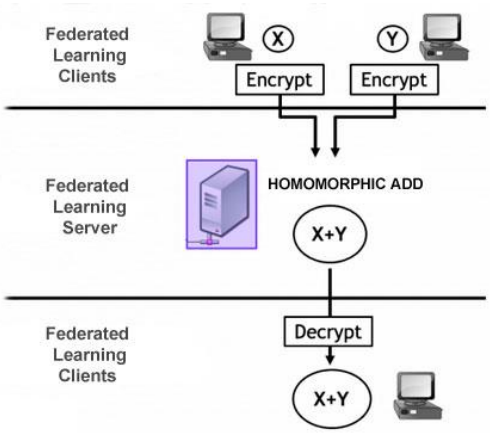

Fig. 2 Homomorphic Encryption Method

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 7, Number 1, Januari 2025
https://doi.org/10.47709/cnahpc.v7i1.5385

Submitted : Jan 23, 2025
Accepted : Jan 23, 2025
Published : Jan 25, 2025

In contrast to conventional static noise injection methods, PPA-FL utilizes a dynamic noise-adjustment mechanism. This mechanism evaluates the balance between privacy and accuracy in real time and adaptively modifies the noise level to maintain high model utility while adhering to privacy constraints. This approach ensured the efficacy of the algorithm across diverse datasets and scenarios. To enhance the robustness, a secure aggregation protocol is implemented to ensure that individual contributions remain concealed from the aggregator. This protocol employs cryptographic techniques to prevent inference attacks even in the event of an aggregator compromise.

The algorithm is designed to minimize the computational overhead of client devices by utilizing lightweight cryptographic operations and efficient noise-generation techniques. This design ensures scalability and practicality, particularly in resource-constrained environments such as IoT networks. By integrating these components, PPA-FL achieves a high level of privacy protection and computational efficiency, thereby addressing the key challenges in the existing FL frameworks. The code below applies Differential Privacy (DP) to the gradients of the model before sending them to the server. This ensures that individual data points are not easily identifiable by introducing noise to the model updates.

```
def gaussian_noise(gradients, epsilon, delta):
    # Generate noise based on the gradients
    # Epsilon (privacy budget) and delta (failure probability) control the privacy level
  noise = np.random.normal(0, scale=calculate_noise_scale(gradients, epsilon, delta),
        size=gradients.shape)
  return noise

def calculate_noise_scale(gradients, epsilon, delta):
    # This calculates the scale of the noise based on gradients, epsilon, and delta
    sensitivity = np.max(np.abs(gradients)) # Example: sensitivity of the gradients
    noise_scale = sensitivity / epsilon
    return noise_scale
```

The noise was generated from a Gaussian distribution with a mean of 0. The scale (standard deviation) of noise was calculated using the calculated_noise_scale function. The size of the noise matches the size of the gradient vector. Another function for encrypting and securing the aggregation is as follows:

```
def encrypt_update(gradients):
    # Example encryption method using RSA
    private_key, public_key = rsa.generate_private_key(public_exponent=65537, key_size=2048)

    # Encrypt the gradients using the public key
    encrypted_gradients = public_key.encrypt(gradients, padding.PKCS1v15())
    return encrypted_gradients

def decrypt_update(encrypted_gradients, private_key):
    # Decrypt the gradients using the private key
    decrypted_gradients = private_key.decrypt(encrypted_gradients, padding.PKCS1v15())
    return decrypted_gradients
```

This code demonstrates how to encrypt gradients or model updates before sending them from the client to the server. Encryption is used to protect the privacy of model updates during transmission.

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 7, Number 1, Januari 2025
https://doi.org/10.47709/cnahpc.v7i1.5385

Submitted : Jan 23, 2025
Accepted : Jan 23, 2025
Published : Jan 25, 2025

RESULT

The experiments were conducted using two datasets commonly utilized in FL research: the MNIST dataset for handwritten digit classification (Deng, 2012), and the CIFAR-10 dataset for image recognition (Krizhevsky, 2009).

Table 1. Experimental Setup

Parameter	Data 1	Data 2
Dataset	MNIST	CIFAR-10
Model	CNN	ResNet-18
Evaluation	Model Accuracy Privacy Budget (ϵ) in Differential Privacy Computation Time (s)	

The accuracy results in Table 2 demonstrate the advantages of the PPA-FL approach. For the MNIST dataset, PPA-FL achieved an accuracy of 96.8%, surpassing that of FL with DP, which yielded an accuracy of 95.5%. Similarly, for the CIFAR-10 dataset, PPA-FL enhanced the accuracy from 84.1% to 85.9%. These improvements substantiate the efficacy of the dynamic noise adjustment mechanism in mitigating the impact of noise on the model performance while maintaining robust privacy guarantees.

Table 2. Model Accuracy Comparison

Dataset	Standard FL (%)	FL with DP (%)	Proposed PPA-FL (%)
MNIST	98.2	95.5	96.8
CIFAR-10	87.6	84.1	85.9

The privacy budget (ϵ) is a critical metric in differential privacy that quantifies the trade-off between privacy and utility. PPA-FL exhibits significantly lower ϵ values compared to FL with DP, indicating enhanced privacy guarantees. Specifically, on MNIST, PPA-FL achieved a privacy budget of 0.5, representing a 50% reduction compared to the baseline. For CIFAR-10, a reduction from 1.5 to 0.8 was observed, further demonstrating the efficacy of dynamic noise adjustment. Table 3 presents the results.

Table 3. Privacy Budget (ϵ) Analysis

Dataset	FL with DP (ϵ)	Proposed PPA-FL (ϵ)
MNIST	1.0	0.5
CIFAR-10	1.5	0.8

The computational efficiency of PPA-FL demonstrates a notable improvement over traditional FL implementations that incorporate differential privacy (DP). As illustrated in Table 4, for the MNIST dataset, the proposed PPA-FL algorithm reduced the computation time from 149 s (FL with DP) to 131 s, indicating a significant optimization. Similarly, for the CIFAR-10 dataset, PPA-FL decreased the computation time from 312 to 268 s. These findings indicate that lightweight encryption and dynamic noise-adjustment mechanisms play a crucial role in maintaining efficiency without compromising security or accuracy.

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 7, Number 1, Januari 2025
https://doi.org/10.47709/cnahpc.v7i1.5385

Submitted : Jan 23, 2025
Accepted : Jan 23, 2025
Published : Jan 25, 2025

Table 4. Computational Time

Dataset	Standard FL (s)	FL with DP (s)	Proposed PPA-FL (s)
MNIST	120	149	131
CIFAR-10	244	312	268

The accuracy gains achieved by the PPA-FL, as listed in Table 2, substantiate the efficacy of the dynamic noise adjustment mechanism. By implementing noise levels tailored to the dataset characteristics, the algorithm mitigates the degradation in model performance, which is typically associated with privacy-preserving measures. The lower privacy budget values presented in Table 3 demonstrate that PPA-FL provides enhanced privacy protection compared with existing approaches. This is particularly significant in sensitive applications, where data confidentiality must be prioritized without compromising functionality.

Table 4 lists the computational efficiency of the proposed algorithm. The lightweight cryptographic operations and optimized aggregation protocols ensure scalability, rendering PPA-FL suitable for IoT devices and edge computing scenarios. These results collectively corroborate the core premise of PPA-FL, that is, achieving a balanced trade-off between privacy, accuracy, and computational efficiency. By addressing these conflicting objectives, the PPA-FL provides a robust solution for the deployment of federated learning in real-world applications.

DISCUSSIONS

The results obtained from the experiments demonstrate the effectiveness and practicality of the proposed Privacy-Preserving Algorithm for Federated Learning (PPA-FL) in addressing the dual challenges of privacy preservation and model performance in federated learning (FL) systems. This section examines the insights derived from the results, compares the proposed approach with the existing methods, evaluates its limitations, and discusses its potential for real-world deployment.

One of the primary objectives of PPA-FL is to achieve an optimal balance between privacy and model performance. The results indicate that the dynamic noise adjustment mechanism employed by PPA-FL significantly mitigates the performance degradation typically associated with static noise injection methods for differential privacy. For instance, the model accuracy on the MNIST dataset improved from 95.5% with traditional FL methods incorporating differential privacy to 96.8% with PPA-FL, representing a substantial reduction in utility loss caused by noise. Similarly, for the CIFAR-10 dataset, PPA-FL maintained higher accuracy while providing stronger privacy guarantees (lower privacy budget ϵ). These findings demonstrate the ability of PPA-FL to dynamically adapt to noise levels based on the sensitivity of the data, ensuring a robust privacy-utility balance.

The privacy budget (ϵ) values achieved by PPA-FL were substantially lower than those of traditional FL methods, reflecting enhanced privacy guarantees. For example, a 50% reduction in ϵ was observed for the MNIST dataset, with a similar trend for CIFAR-10. These reductions underscore the efficacy of combining homomorphic encryption with differential privacy to secure model updates against adversarial attacks. Moreover, the secure aggregation protocol further strengthens these guarantees by preventing reconstruction or inference attacks even in the presence of a compromised aggregator.

Computational overhead has been a persistent challenge in the adoption of privacy-preserving FL techniques, particularly those that rely on cryptographic methods. PPA-FL mitigates this issue by employing lightweight homomorphic encryption schemes and efficient noise-generation techniques. As shown in Table 3, the computational time for PPA-FL was notably lower than that for FL with traditional differential privacy despite the incorporation of additional encryption. This efficiency is particularly valuable in resource-

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 7, Number 1, Januari 2025
https://doi.org/10.47709/cnahpc.v7i1.5385

Submitted : Jan 23, 2025
Accepted : Jan 23, 2025
Published : Jan 25, 2025

constrained environments, such as IoT networks and edge devices, where computational power and energy consumption are critical constraints.

When compared to existing privacy-preserving techniques, such as fully homomorphic encryption and static differential privacy, PPA-FL demonstrates several advantages. Traditional homomorphic encryption methods often impose significant computational overhead, rendering them impractical for large-scale FL systems. Conversely, static differential privacy approaches encounter difficulties in maintaining accuracy in scenarios involving highly sensitive or heterogeneous data. By integrating homomorphic encryption and differential privacy with a dynamic noise adjustment mechanism, PPA-FL effectively addresses these limitations, offering a scalable and adaptable solution for privacy-preserving FL.

Notwithstanding its advantages, PPA-FL is not without limitations. The performance of the algorithm may be influenced by the complexity of the dataset and the model architecture. Although the experimental results indicate consistent improvements across benchmark datasets, further testing on real-world, large-scale datasets is necessary to fully validate its scalability and adaptability. Additionally, the selection of encryption schemes and privacy budget parameters requires careful calibration to balance the computational overhead and privacy guarantees, which may present challenges in highly dynamic environments.

The implications of these findings extend beyond their theoretical significance, highlighting the potential of PPA-FL for practical implementation in diverse domains. By ensuring robust privacy guarantees and high model utility, PPA-FL addresses key barriers to the adoption of FL in privacy-sensitive industries, such as healthcare, finance, and IoT. Furthermore, its alignment with regulatory standards, such as GDPR and HIPAA, renders it an attractive option for organizations seeking to enhance their data governance strategies while leveraging collaborative machine learning.

CONCLUSION

This paper presents a Privacy-Preserving Algorithm for Federated Learning (PPA-FL), addressing critical challenges in maintaining data privacy and security while optimizing model performance in federated learning (FL) frameworks. By integrating homomorphic encryption with differential privacy and introducing a dynamic noise-adjustment mechanism, the proposed algorithm offers a robust solution to the inherent trade-offs between privacy, accuracy, and computational efficiency in FL systems.

The key contributions of this work lie in its novel approach to safeguarding privacy during model training and updating exchanges, particularly against adversarial attacks, such as data reconstruction and inference. Through dynamic noise adjustment, PPA-FL adapts noise levels based on dataset sensitivity and privacy budget requirements, ensuring high model utility without compromising on stringent privacy guarantees. Furthermore, the lightweight cryptographic operations employed in PPA-FL significantly enhance computational efficiency, rendering it suitable for deployment in resource-constrained environments, such as IoT networks and edge computing systems.

Experimental evaluation on benchmark datasets, including MNIST and CIFAR-10, demonstrated the efficacy of PPA-FL. The algorithm achieved improved model accuracy compared to traditional FL approaches with static differential privacy mechanisms, while delivering stronger privacy guarantees, as evidenced by lower privacy budget values. Additionally, the computational time savings observed across the experiments highlight the practicality of the algorithm for real-world applications.

The implications of PPA-FL are far reaching. In healthcare, this facilitates collaborative learning for disease diagnosis and genomic data analysis. In finance, it enables fraud detection and credit scoring, while ensuring customer data confidentiality. IoT systems support scalable learning in smart and autonomous systems. Moreover, the algorithm finds applications in the retail, education, and government sectors, underscoring its versatility in the privacy-sensitive domains.

By addressing the limitations of existing privacy-preserving FL techniques, PPA-FL paves the way for the wider adoption of federated learning in real-world scenarios. Its design not only aligns with regulatory

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 7, Number 1, Januari 2025
https://doi.org/10.47709/cnahpc.v7i1.5385

Submitted : Jan 23, 2025
Accepted : Jan 23, 2025
Published : Jan 25, 2025

standards such as GDPR and HIPAA but also fosters trust among stakeholders, encouraging broader participation in collaborative machine learning initiatives.

Future research can build upon this work by exploring more advanced encryption schemes to further enhance security, optimize noise adjustment mechanisms for more complex datasets, and extend the applicability of the algorithm to emerging fields such as federated reinforcement learning and multimodal data processing. In conclusion, PPA-FL represents a significant advancement in the development of secure, efficient, and adaptable federated learning systems, contributing to the broader goal of advancing privacy-preserving technologies in the era of data-driven innovation.

REFERENCES

Agarwal, P., & Shrivastava, P. (2021). Enhancing Data Security in Cloud Computing through Homomorphic Encryption. *Computology: Journal of Applied Computer Science and Intelligent Technologies*, *1*(1), 32–39. https://doi.org/10.17492/computology.v1i1.2104

Ali, A., Al-rimy, B. A. S., Alsubaei, F. S., Almazroi, A. A., & Almazroi, A. A. (2023). HealthLock: Blockchain-Based Privacy Preservation Using Homomorphic Encryption in Internet of Things Healthcare Applications. *Sensors*, *23*(15), 6762. https://doi.org/10.3390/s23156762

Chatterjee, A., & Sengupta, I. (2018). Translating Algorithms to Handle Fully Homomorphic Encrypted Data on the Cloud. *IEEE Transactions on Cloud Computing*, *6*(1), 287–300. https://doi.org/10.1109/TCC.2015.2481416

Cidem Dogan, D., & Altindis, H. (2020). Storage and Communication Security in Cloud Computing Using a Homomorphic Encryption Scheme Based Weil Pairing. *Elektronika Ir Elektrotechnika*, *26*(1), 78–83. https://doi.org/10.5755/j01.eie.26.1.25312

Deng, L. (2012). The mnist database of handwritten digit images for machine learning research. *IEEE Signal Processing Magazine*, *29*(6), 141–142.

Fan, T., & Cui, Z. (2021). Adaptive differential privacy preserving based on multi-objective optimization in deep neural networks. *Concurrency and Computation: Practice and Experience*, *33*(20). https://doi.org/10.1002/cpe.6367

Idris, I. A., & issahku, F. Y. (2024). Advancing Wireless Sensor Network Security through the Implementation of Homomorphic Encryption for Secure and Private Image Processing. *International Journal for Research in Applied Science and Engineering Technology*, *12*(1), 1464–1474. https://doi.org/10.22214/ijraset.2024.58180

Johnson, N., Near, J. P., & Song, D. (2018). Towards practical differential privacy for SQL queries. *Proceedings of the VLDB Endowment*, *11*(5), 526–539. https://doi.org/10.1145/3187009.3177733

JUNG, K., LEE, H., & CHUNG, Y. D. (2021a). Differentially Private Neural Networks with Bounded Activation Function. *IEICE Transactions on Information and Systems*, *E104.D*(6), 905–908. https://doi.org/10.1587/transinf.2021EDL8007

JUNG, K., LEE, H., & CHUNG, Y. D. (2021b). Differentially Private Neural Networks with Bounded Activation Function. *IEICE Transactions on Information and Systems*, *E104.D*(6), 905–908. https://doi.org/10.1587/transinf.2021EDL8007

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 7, Number 1, Januari 2025
https://doi.org/10.47709/cnahpc.v7i1.5385

Submitted : Jan 23, 2025
Accepted : Jan 23, 2025
Published : Jan 25, 2025

Jung, W., Lee, E., Kim, S., Kim, J., Kim, N., Lee, K., Min, C., Cheon, J. H., & Ahn, J. H. (2021). Accelerating Fully Homomorphic Encryption Through Architecture-Centric Analysis and Optimization. *IEEE Access*, *9*, 98772–98789. https://doi.org/10.1109/ACCESS.2021.3096189

K L, A., & Nair, T. R. G. (2019). Data storage lock algorithm with cryptographic techniques. *International Journal of Electrical and Computer Engineering (IJECE)*, *9*(5), 3843. https://doi.org/10.11591/ijece.v9i5.pp3843-3849

Krizhevsky, A. (2009). *Learning Multiple Layers of Features from Tiny Images*. 32–33. https://www.cs.toronto.edu/~kriz/learning-features-2009-TR.pdf

Li, Y., Du, W., Han, L., Zhang, Z., & Liu, T. (2023a). A Communication-Efficient, Privacy-Preserving Federated Learning Algorithm Based on Two-Stage Gradient Pruning and Differentiated Differential Privacy. *Sensors*, *23*(23), 9305. https://doi.org/10.3390/s23239305

Li, Y., Du, W., Han, L., Zhang, Z., & Liu, T. (2023b). A Communication-Efficient, Privacy-Preserving Federated Learning Algorithm Based on Two-Stage Gradient Pruning and Differentiated Differential Privacy. *Sensors*, *23*(23), 9305. https://doi.org/10.3390/s23239305

Liu, B., Eric B. Blancaflor, Fang, T., & Cao, L. (2024). Privacy Protection Based on Federated Learning. *Journal of Artificial Intelligence and Technology*. https://doi.org/10.37965/jait.2024.0503

Liu, H., Peng, C., Tian, Y., Long, S., & Wu, Z. (2021). Balancing Privacy-Utility of Differential Privacy Mechanism: A Collaborative Perspective. *Security and Communication Networks*, *2021*, 1–14. https://doi.org/10.1155/2021/5592191

Liu, H., Wu, Z., Zhou, Y., Peng, C., Tian, F., & Lu, L. (2018a). Privacy-Preserving Monotonicity of Differential Privacy Mechanisms. *Applied Sciences*, *8*(11), 2081. https://doi.org/10.3390/app8112081

Liu, H., Wu, Z., Zhou, Y., Peng, C., Tian, F., & Lu, L. (2018b). Privacy-Preserving Monotonicity of Differential Privacy Mechanisms. *Applied Sciences*, *8*(11), 2081. https://doi.org/10.3390/app8112081

Ma, J., Hu, J., & Peng, Z. (2024). Privacy Preservation of Nabla Discrete Fractional-Order Dynamic Systems. *Fractal and Fractional*, *8*(1), 46. https://doi.org/10.3390/fractalfract8010046

Ngabo, C. I., & El Beqqali, O. (2019). Implementation of Homomorphic Encryption for Wireless Sensor Networks Integrated with Cloud Infrastructure. *Journal of Computer Science*, *15*(2), 235–248. https://doi.org/10.3844/jcssp.2019.235.248

Park, C., Hong, D., & Seo, C. (2019). An Attack-Based Evaluation Method for Differentially Private Learning Against Model Inversion Attack. *IEEE Access*, *7*, 124988–124999. https://doi.org/10.1109/ACCESS.2019.2938759

Park, C., Kim, Y., Park, J.-G., Hong, D., & Seo, C. (2021). Evaluating Differentially Private Generative Adversarial Networks Over Membership Inference Attack. *IEEE Access*, *9*, 167412–167425. https://doi.org/10.1109/ACCESS.2021.3137278

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 7, Number 1, Januari 2025
https://doi.org/10.47709/cnahpc.v7i1.5385

Submitted : Jan 23, 2025
Accepted : Jan 23, 2025
Published : Jan 25, 2025

Parker, K., Hale, M., & Barooah, P. (2022a). Spectral Differential Privacy: Application to Smart Meter Data. *IEEE Internet of Things Journal*, *9*(7), 4987–4996. https://doi.org/10.1109/JIOT.2021.3107770

Parker, K., Hale, M., & Barooah, P. (2022b). Spectral Differential Privacy: Application to Smart Meter Data. *IEEE Internet of Things Journal*, *9*(7), 4987–4996. https://doi.org/10.1109/JIOT.2021.3107770

Salim, M. M., Kim, I., Doniyor, U., Lee, C., & Park, J. H. (2021). Homomorphic Encryption Based Privacy-Preservation for IoMT. *Applied Sciences*, *11*(18), 8757. https://doi.org/10.3390/app11188757

Shi, L., & Zhu, H. (2024). A study of user data privacy protection algorithms in the context of metaverse based on emotional AI IoT. *Applied Mathematics and Nonlinear Sciences*, *9*(1). https://doi.org/10.2478/amns.2023.2.00636

Thantharate, P., Bhojwani, S., & Thantharate, A. (2024). DPShield: Optimizing Differential Privacy for High-Utility Data Analysis in Sensitive Domains. *Electronics*, *13*(12), 2333. https://doi.org/10.3390/electronics13122333

Wang, H., Zhang, J., Lu, C., & Wu, C. (2021a). Privacy Preserving in Non-Intrusive Load Monitoring: A Differential Privacy Perspective. *IEEE Transactions on Smart Grid*, *12*(3), 2529–2543. https://doi.org/10.1109/TSG.2020.3038757

Wang, H., Zhang, J., Lu, C., & Wu, C. (2021b). Privacy Preserving in Non-Intrusive Load Monitoring: A Differential Privacy Perspective. *IEEE Transactions on Smart Grid*, *12*(3), 2529–2543. https://doi.org/10.1109/TSG.2020.3038757

Wang, Y., Kifer, D., & Lee, J. (2019). Differentially Private Confidence Intervals for Empirical Risk Minimization. *Journal of Privacy and Confidentiality*, *9*(1). https://doi.org/10.29012/jpc.660

Yang, C., Qi, J., & Zhou, A. (2024). Wasserstein Differential Privacy. *Proceedings of the AAAI Conference on Artificial Intelligence*, *38*(15), 16299–16307. https://doi.org/10.1609/aaai.v38i15.29565

Zhang, Y., Lu, Y., & Liu, F. (2023). A Systematic Survey for Differential Privacy Techniques in Federated Learning. *Journal of Information Security*, *14*(02), 111–135. https://doi.org/10.4236/jis.2023.142008

Zhang, Z., Wu, T., Sun, X., & Yu, J. (2021). MPDP *k* -medoids: Multiple partition differential privacy preserving *k* -medoids clustering for data publishing in the Internet of Medical Things. *International Journal of Distributed Sensor Networks*, *17*(10), 155014772110425. https://doi.org/10.1177/15501477211042543

Ziegler, J., Pfitzner, B., Schulz, H., Saalbach, A., & Arnrich, B. (2022a). Defending against Reconstruction Attacks through Differentially Private Federated Learning for Classification of Heterogeneous Chest X-ray Data. *Sensors*, *22*(14), 5195. https://doi.org/10.3390/s22145195

Ziegler, J., Pfitzner, B., Schulz, H., Saalbach, A., & Arnrich, B. (2022b). Defending against Reconstruction Attacks through Differentially Private Federated Learning for Classification of Heterogeneous Chest X-ray Data. *Sensors*, *22*(14), 5195. https://doi.org/10.3390/s22145195

* Corresponding author