Hindawi
Mobile Information Systems
Volume 2022, Article ID 3850246, 8 pages
https://doi.org/10.1155/2022/3850246

*Research Article*

# Privacy-Enhanced Data Fusion for Federated Learning Empowered Internet of Things

**Qingxin Lin,[1] Kuai Xu,[2] Yikun Huang ,[2] Feng Yu,[3,4] and Xiaoding Wang [3,4]**

[1]*Fuzhou University Zhicheng College, Fuzhou 350001, Fujian, China*
[2]*Concord University College Fujian Normal University, Fuzhou 350117, Fujian, China*
[3]*College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350117, Fujian, China*
[4]*Engineering Research Center of Cyber Security and Education Informatization, Fujian Province University, Fuzhou 350117, Fujian, China*

Correspondence should be addressed to Yikun Huang; fjnuhyk@163.com and Xiaoding Wang; wangdin1982@fjnu.edu.cn

Received 19 July 2022; Revised 1 September 2022; Accepted 15 September 2022; Published 3 October 2022

Academic Editor: Miao Ye

IoT sensors have already penetrated into extremely broad fields such as industrial production, smart home, environmental protection, medical diagnosis, and bioengineering. Although efficient data fusion helps improve the quality of intelligent services provided by the Internet of things, because the perceived data carry the sensitive information of the perceived object, the data fusion process is prone to the risk of privacy leakage. To this end, in this paper, we proposed a privacy-enhanced federated learning data fusion strategy. This strategy adds Gaussian noise at different stages of federated learning to achieve privacy protection in the data fusion process. Experimental results show that this strategy provides better privacy protection while achieving high-precision IoT data fusion.

## 1. Introduction

The Internet of things, also known as a sensor network, connects any item to the Internet through information sensing equipment such as radio frequency identification, infrared sensors, global positioning systems, and laser scanners for information exchange and communication, to achieve intelligent identification, positioning, tracking, monitoring, and management. The large-scale deployment and application of various sensors is an indispensable basic condition for the Internet of things. For example, different applications need to deploy different sensors, covering smart industry, smart security, smart home, smart transportation, smart medical care, etc. It can be seen that IoT sensor technology plays an important role in economic development and promotes social progress.

At present, most of the intelligent services provided by the Internet of things need to outsource user data to service providers for analysis and processing, which may easily lead to the leakage of sensitive information [1]. With the improvement of user privacy protection awareness and the promulgation of relevant laws and regulations, data analysis services based on traditional machine learning can no longer meet users' privacy protection needs. Although existing cryptographic technology can solve some privacy leakage problems, both symmetric encryption systems and asymmetric encryption systems have the risk of key leakage, and high-cost encryption chips cannot be popularized to terminal devices. In order to solve the problem of user data privacy leakage in related service scenarios, Google proposed federated learning technology [2, 3].

Federated learning is a distributed machine learning technology with privacy-preserving properties that can generate secure, accurate, and robust data models without analyzing the real data of users. In the intelligent service scenario based on federated learning, the service provider convenes different participants to provide data models by publishing federated learning tasks and aggregates all data models through the aggregation server to generate a reliable global model to provide related services. The reliability of the global model is crucial, and a reliable global model can provide secure and stable services for IoT applications. It is worth noting that the use of cryptography technology can achieve data privacy protection. However, the use of cryptography often requires a trusted third party to generate a key for data encryption, which is difficult to achieve in the Internet of things. Compared with cryptography, federated learning does not require a trusted third party and is easy to deploy. Even if the federated learning server is not trusted, the privacy protection of data can be achieved by adding noise to the model, so federated learning has more advantages in data sharing.

The problem solved in this paper is formally described as follows, that is, how to realize data sharing under the premise of privacy protection. Based on the above analysis, a data fusion architecture is first proposed based on federated learning, as shown in Figure 1. The architecture consists of three layers: perception layer, data fusion layer, and intelligent service layer. Among them, the perception layer obtains perception data and sends the data to the data fusion layer through various sensors such as wearable sensors, vehicle-mounted sensors, surveillance cameras, and industrial sensors. In the data fusion layer, each federated learning (FL) data fusion center is responsible for the intelligent fusion processing of perception data and provides the fusion data to the intelligent service layer. This layer provides technical support for various intelligent services of the Internet of things such as intelligent transportation, smart grid, intelligent manufacturing, and intelligent logistics. All in all, the perception layer provides the necessary data to the intelligent service layer through the data fusion layer, and the intelligent service layer sends feedback information to it, hoping to improve the quality of the intelligent service.

According to this architecture, we consider using federated learning techniques to achieve privacy-enhanced data fusion. Furthermore, we combine differential privacy techniques with different stages of federated learning to further improve privacy protection during data fusion. The main contributions of this paper are as follows:

(1) To achieve privacy-preserving data fusion, we propose a privacy-enhanced federated learning data fusion strategy. This strategy not only adds differential privacy noise in the local model training process but also adds differential privacy noise in the federated training process, at the cost of a certain model accuracy, and the differential privacy protection of the local model and that of the global model are achieved simultaneously.

(2) Experimental results show that this strategy provides better privacy protection while achieving high-precision IoT data fusion.

The rest of this paper is organized as follows: Related work is described in the Related Work section. The system model is given in the System Model section. The specific implementation of the proposed strategy is elaborated in the Implementation Details of the Proposed Strategy section. Performance evaluations are given in the Performance Evaluation section. The Conclusions section concludes this paper.

## 2. Related Work

Federated learning for data fusion is an effective means for IoT to provide intelligent services, and the reliability of the federated learning global model determines the quality of services. More and more scholars at home and abroad have carried out research on how to ensure the reliability of the federated learning global model under different needs and have produced many excellent research results.

For federated learning task publishers, the reliability of the global model is the focus of attention. Researchers further ensure global model reliability by detecting anomalous models in the models to be aggregated. Cao et al. [4] mapped the local models into a graph through the Euclidean distance between local models and selected the local model for aggregation by solving the maximum clique problem in the graph, realizing the detection of anomalous models in federated learning. Zhao et al. [5] generated a dataset for auditing the local model through the trained generative adversarial network, and the prediction and evaluation results of the local model in the dataset were used as the criterion for judging whether it was an abnormal model, so as to realize the detection of abnormal models. Zhao et al. [6] proposed a proxy-based anomaly model detection mechanism, selecting participants with relatively stable performance in federated learning to perform anomaly model detection. Tolpegin et al. [7] extracted abnormal model features by performing dimensionality reduction and principal component analysis on the local model and realized abnormal model detection in the process. Liu et al. [8] proposed a federated learning scheme PEFL to mitigate poisoning attacks under privacy enhancement. In [9], an asynchronous update paradigm for real-time identification of client network parameters was proposed. This paradigm adopted a linear fusion method based on sequential filtering, considered communication delay, and asynchronously fused the parameters of the federation center. Then, a client real-time identification method based on linear filtering was established to obtain new label samples at unequal intervals, and the client was expected to have better performance.

For federated learning participants, the biggest demand is that federated learning can protect the private data of their training from being leaked. Since privacy and model reliability cannot be taken into account at the same time, existing research work mainly seeks a balance between the two, that is, reducing the loss of global model reliability while meeting the needs of participants for privacy protection. In [10], a privacy-preserving federated learning scheme, LDP-Fed, was proposed, which allows federated learning participants to protect the privacy of the model through personalized local differential privacy technology to prevent the leakage of deep information in the local model. Hu et al. [11] introduced differential privacy technology in federated learning and used the uncertainty brought by heterogeneity

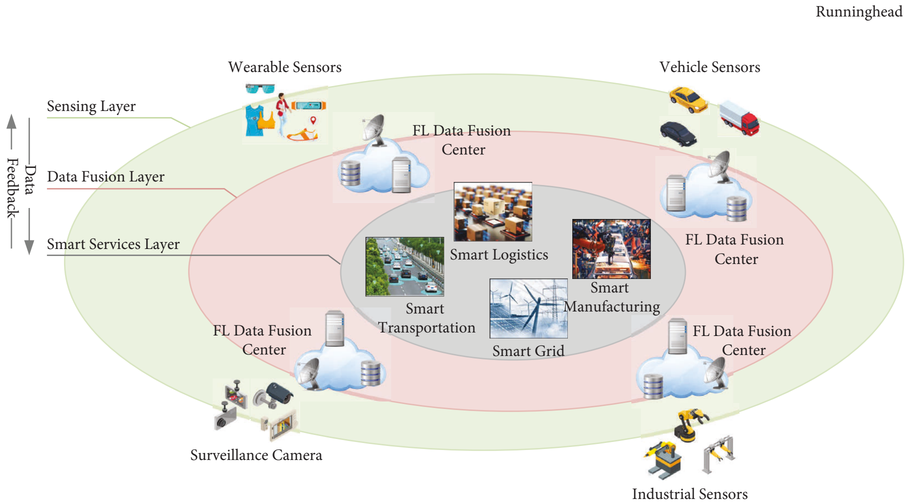


Figure 1: Federated learning-based data fusion architecture.

of IoT devices to perform differential privacy on the model to reduce the risk of privacy leakage. In [12], differential privacy technology and self-normalization technology were introduced in federated learning and the differential privacy noise layer and SELU security training layer were added during model training to realize the privacy protection of uploaded models. In [13], a blockchain-based federated learning training strategy was proposed, which uses differential privacy and homomorphic encryption technology to ensure the privacy of participants in the process of local model transmission and aggregation. Zhang and Luo [14] generated training data for local training by training a GAN model and proposed a new loss function, which enabled the generated training data to have indistinguishable visual features from the original data and protect the privacy of the training data of the participants. Liu et al. [15] used the sparse features of the feature map in the network model to represent the data that participants used for local training and realized the privacy protection of the real data. Xu et al. [16] proposed an efficient and privacy-preserving vertical-federated learning framework FedV, which implemented a two-stage noninteractive secure-federated aggregation method by introducing functional encryption and realized the privacy protection of real data of participants. In [17], Lin et al. proposed a secure joint learning mechanism based on variational autoencoders to resist inference attacks, in which participants reconstructed the original data through variational autoencoders, and trained local models on this basis to protect data privacy. In [18], a heterogeneous model fusion-federated learning mechanism was proposed, in which each node trained learning models of different scales according to its own computing power. After the parameter server received the training gradient of each node, it used the repetition matrix to correct the received gradient, then updated the corresponding region of the global model according to the mapping matrix, and finally assigned the compressed model to the corresponding node.

The above literature provides a large number of excellent algorithms for data fusion in the Internet of things. However, how to combine the privacy protection of local data with the privacy protection of the federated learning process to further strengthen the privacy protection of federated learning is still a problem worthy of research.

## 3. System Model

To achieve privacy-preserving data fusion in IoT, we need to consider the following three entities:

(i) Sensor (data provider): the sensor aggregates sensed data to the data fusion center through wireless or wired transmission.

(ii) Federated learning (FL)-based data fusion center: the data fusion center uses local sensor data for model training so that the local model can carry the information of local data. In addition, differential privacy noise needs to be added in the local model training process to achieve differential privacy protection of the local model.

(iii) Federated learning server: this server aggregates the local models of each data aggregation center to form a global model and adds differential privacy noise in the process to further improve the differential privacy protection capability of the global model.

### 3.1. Security Model

*3.1. Security Model.* The privacy breach scenarios we consider are as follows. First, IoT smart service providers may be interested and commercialize private information about objects whose sensors are collecting data, thereby exposing their privacy, and federated learning can help reduce that risk. However, the aggregation server of federated learning may also be curious about the privacy of the perceived object, so there is also the risk of privacy leakage during the federated learning process. Differential privacy protection in local model training helps mitigate this risk. In addition, malicious attackers try to obtain the private information of perceptual objects from the global model through inference attacks. Adding differential privacy protection to the global model can effectively resist such attacks.

```
Input: Initial model parameter $\theta$ received from the FL fusion server, learning rate $\eta$, local sensor dataset $D$, gradient clipping $C$, privacy budget $\epsilon$, sensitivity $s$, and Gaussian noise to be added satisfying $(\epsilon, \sigma) - DP$
Output: Final model parameter $\widetilde{\theta}$
for $t \in T$ do
    Calculate the gradient $g_i$ for each batch $D_i \in D$
    Clip the gradient by $g_i = g_i/\max(1, |g_i|/C)$ and calculate average gradient $g = 1/|D| \sum g_i$
    Perform gradient descent by $\theta \leftarrow \theta - \eta g$
    Add Gaussian noise by $\widetilde{\theta} = \theta + N(\sigma^2)$, where $\sigma^2 = 2s^2 \log(1.25/\sigma)/\epsilon^2$
end for
```

Algorithm 1: Local data fusion with differential privacy protection.

```
Input: Local model parameter $\theta^k$, privacy budget $\epsilon$, sensitivity $s$, and Gaussian noise to be added satisfying $(\epsilon, \sigma) - DP$
Output: Global model parameter $\theta$ to be released
for each FL-based data fusion center do
    Calculate the weighted average model by $\widetilde{\theta} = \sum_{k=1}^{K} n_k/n\theta^k$
    Add Gaussian noise by $\theta = \widetilde{\theta} + N(\sigma^2)$, where $\sigma^2 = 2s^2 \log(1.25/\sigma)/\epsilon^2$
end for
```

Algorithm 2: Global data fusion with differential privacy protection.

## 4. Implementation Details of the Proposed Strategy

The data fusion strategy proposed in this paper is mainly composed of two modules, namely, the local data fusion module with differential privacy protection and the global data fusion module with differential privacy protection. The difference between these two modules is to add differential privacy noise to different stages of the federated learning process, thereby resisting privacy leak attacks on different objects.

*4.1. Local Data Fusion with Differential Privacy Protection.* Local data fusion is achieved by training a deep neural network model on local sensor data. In a deep neural network, by deploying multiple neurons at multiple levels and adjusting the connection weights between neurons by means of layer-by-layer training, the original feature data can undergo multiple nonlinear transformations. The fitting of any limited given input and output data finally obtains stable features for subsequent problem analysis. In the deep neural network algorithm, in order to evaluate the difference between the predicted value of the proposed neural network and the actual value, it is represented by a loss function $L$, and the mean square error loss function is used in this paper, i.e., $L(\theta, x) = 1/n \sum_{i=1}^{n} (y_i - x_i)^2$, where $\theta$ is the weight coefficient of the neural network to be trained, $x$ represents the target value, $y$ represents the predicted value output, and the subscript $i$ represents the sample label. The purpose of deep neural network algorithm training is to minimize the loss function $L$. For complex neural networks, minimizing the loss function $L$ is usually performed by stochastic gradient descent. That is, we randomly select training samples in batches during each iteration and calculate the partial derivative of the loss function $L$, denoted by $g = 1/|D| \sum_{x \in D} \nabla_{\theta} L(\theta, x)$, where $D$ denotes the batches of samples, and then update the weight coefficient $\theta$ along the negative gradient direction towards the local minimum.

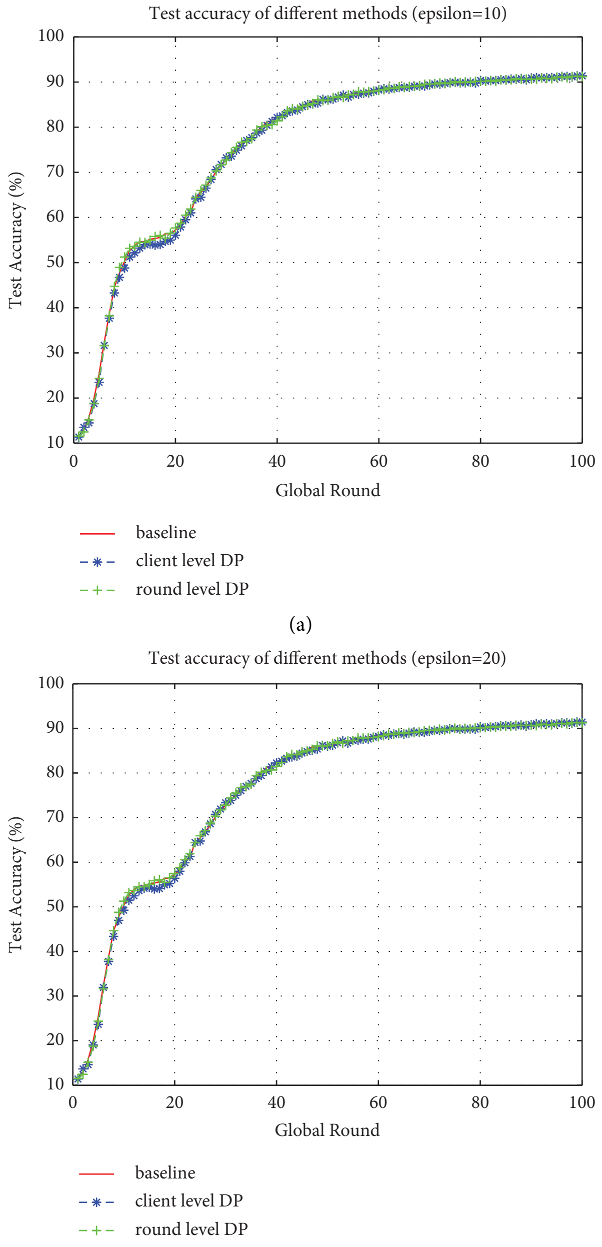
We adopt the differential privacy stochastic gradient algorithm whose objective function minimizes the loss function $L$ by continuously training and adjusting the weight coefficients $\theta$. The basic idea is as follows: in each iteration process, we first calculate the gradient of randomly generated batch samples $\nabla L(\theta, x_i)$, and gradient clipping is performed based on the $L_2$ norm of the computed gradient values. Considering the privacy protection of the sample data, the clipped gradient is updated with the mean value of the sum of the gradient and random noise based on the additional Gaussian noise method [19]. That is, by adding Gaussian noise with $\sigma^2 = 2s^2 \log(1.25/\sigma)/\epsilon^2$, the $(\epsilon, \sigma)$ differential privacy is achieved. Then, the weight coefficient $\theta$ of the next iteration is obtained. The implementation details of the local data fusion with differential privacy protection are summarized in Algorithm 1.

*4.2. Global Data Fusion with Differential Privacy Protection.* After the local model data fusion model is trained, the model will be sent to the federated learning server for aggregation. During training of the local model, we add Gaussian noise to resist privacy leakage attacks that may be launched by curious federated learning servers and IoT smart service providers. However, for inference attacks that malicious attackers may launch on the model, we add Gaussian noise again during the model release process to further enhance the model's privacy protection capabilities. The execution process of global data fusion with privacy protection is summarized in Algorithm 2.

*4.3. Security Analysis.* The strategy proposed in this paper can resist privacy leakage attacks. First, in the training of the local model by the data fusion center, we add differential

Table 1: Parameter setup.

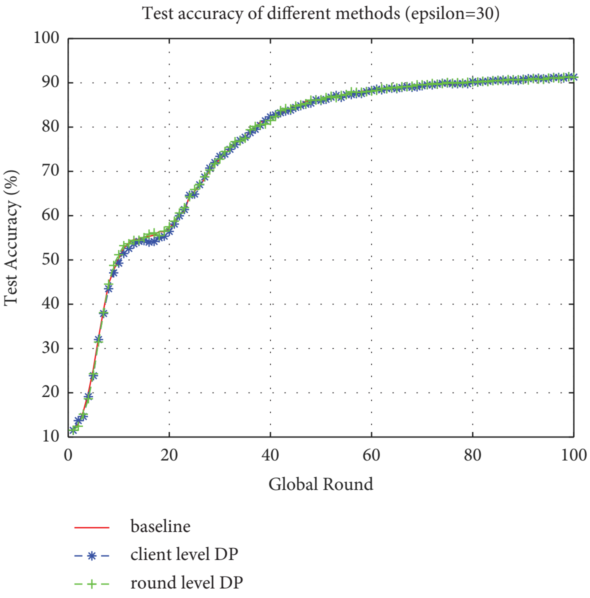
| Hyperparameter | Value |
|---|---|
| Dp_$\delta$ | $1e-5$ |
| Dp_$\epsilon$ | 10, 20, 30 |
| Epochs | 100 |
| Num_users | 100 |
| Frac | 0.1 |
| Local_ep | 1 |
| Local_bs | 100 |
| Learning rate | 0.01 |
| Lr_decay | 0.995 |



(a)

(b)

Figure 2: Continued.



(c)

Figure 2: Accuracy on the MNIST dataset with different differential privacy protections: (a) $\epsilon = 10$, (b) $\epsilon = 20$, and (c) $\epsilon = 30$.

privacy noise to the gradient of the model update so that the local model can get differential privacy protection after the local model training is completed. Second, after the local model is aggregated to the federated learning server, the server adds differential privacy noise to the aggregated model again and then distributes the noise model to each data fusion center so that the global model can get stronger differential privacy protection. We repeat the above process until federated learning converges. Due to the post-processing properties of differential privacy, the entire federated learning process has differential privacy protection. In addition, since the model is protected by differential privacy, it increases the possibility of attackers recovering user data through reasoning attacks and also increases the difficulty of attackers launching known plaintext attacks and ciphertext only attacks.

## 5. Performance Evaluation

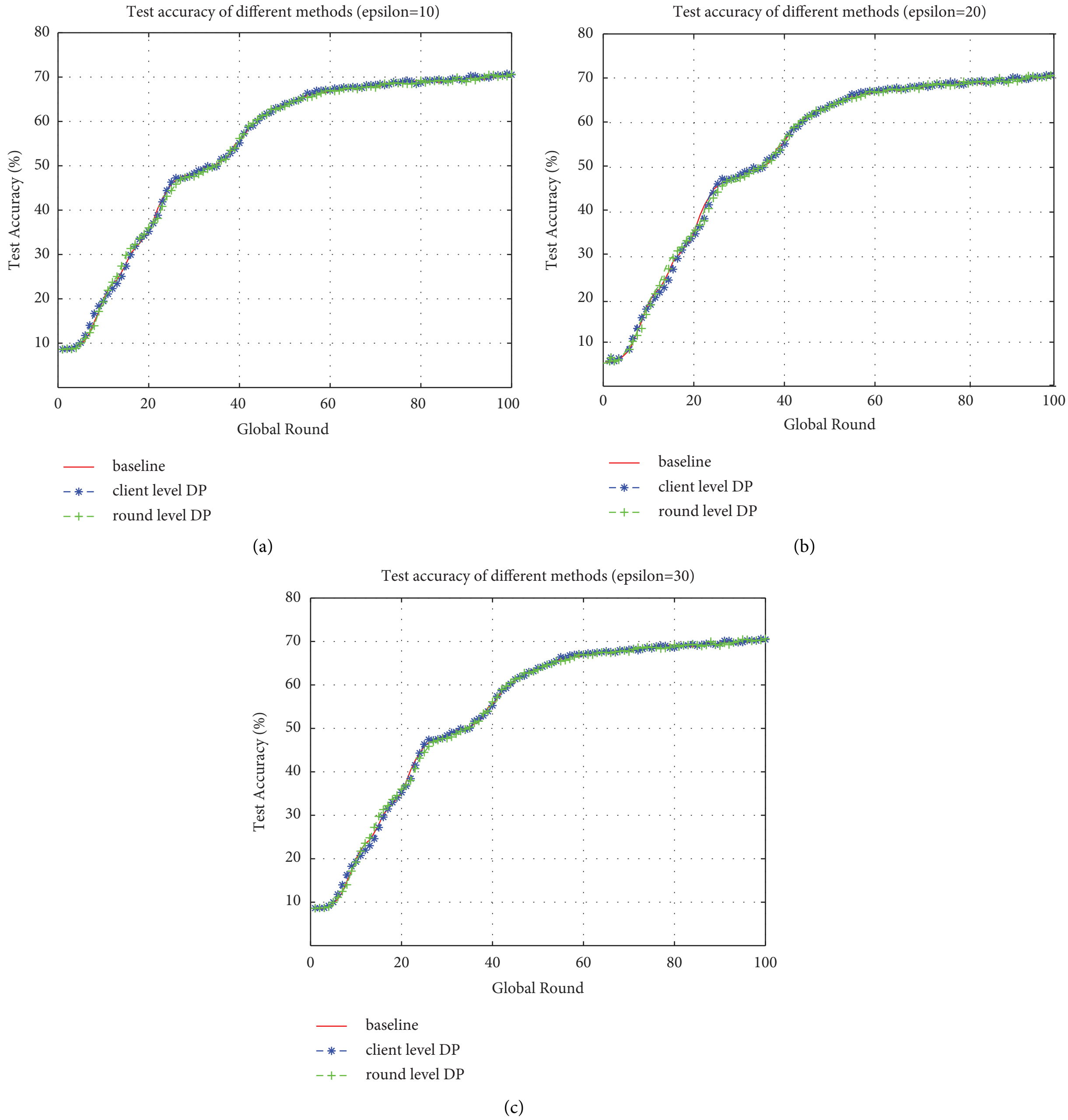
*5.1. Experimental Environment.* The experiment is conducted to evaluate the performance of the proposed strategy on the computer equipped with i7 6.4GHZ processor, 32G memory, and win7 64-bit system. Federated learning is constructed through the Python-based deep learning framework (Tensorflow 2.2.0).

In the experiment, both the local model and the global model use CNN, which has 2 convolutional layers ($1 * 10$, kernelsize = 5; $10 * 20$, kernelsize = 5), dropout layers, and two fully connected layers ($320 * 50$; $50 * 10$). The datasets used in this experiment are the MNIST dataset and the Fashion- MNIST dataset. The MNIST dataset is a widely used handwritten digit recognition dataset, commonly used for performance evaluation of image classification algorithms in the field of computer vision. There are 10 digit classes in this dataset, from digit 0 to digit 9. The MNIST dataset contains 70,000 grayscale images with a resolution of $28 * 28$, of which 60,000 images are used for training the model and another 10,000 images are used for validation. The Fashion-MNIST dataset is an extended version of MNIST. The Fashion-MNIST dataset contains 70,000 grayscale images, including a training set of 60,000 images and a test set of 10,000 images. Each is a $28 * 28$ grayscale image, including different types of t-shirts, dresses, and boots. In the experiments, we fix other hyperparameters and adjust $\epsilon \in (10, 20, 30)$ for multiple experiments. The rest of parameters are given in Table 1.

In this experiment, we compare noise-added local model training, denoted by client level DP, noise-added global model training, denoted by round level DP, and the baseline strategy (FedAvg) [20] in terms of model accuracy.

## 6. Experimental Results

Figures 2 and 3 show the accuracy of our proposed strategy for local model training and global model training under different privacy budgets, i.e., $\epsilon \in (10, 20, 30)$. It can be observed from Figure 2 that the accuracies of three strategies all rise rapidly before 20 rounds, then slowly rise after that, and converge to the optimal accuracy when approaching 100 rounds, which is about 90%. In addition, local model training and global model training do not have lower accuracy than FedAvg under the same number of epochs due to the addition of Gaussian noise. Furthermore, under different privacy budgets, the accuracy of the local model and the global model is not much different. It can be observed from Figure 2 that the accuracy of three strategies increases rapidly before 30 rounds, then slowly increases, and converges to the optimal accuracy, which is about 70%,



(a)

(b)

(c)

Figure 3: Accuracy on the Fashion-MNIST dataset with different differential privacy protections: (a) $\epsilon = 10$, (b) $\epsilon = 20$, and (c) $\epsilon = 30$.

when approaching 100 rounds. In addition, the accuracy of local model training and global model training under the same number of epochs is close to FedAvg, and under different privacy budgets, the accuracy of the local model and the global model is not much different.

## 7. Conclusions

The deep fusion of data collected by various sensors in the Internet of things is an urgent problem to be solved. In addition, in the process of data fusion, the privacy of objects collected by sensors may be leaked due to data fusion, which means the necessity of data fusion and privacy protection. To this end, we propose a privacy-enhanced federated learning data fusion strategy. This strategy not only adds differential privacy noise in the local model training process but also adds differential privacy noise in the federated training process, so as to realize the differential privacy protection of the local model and the differential privacy protection of the global model at the same time. Experimental results and theoretical analysis show that this strategy provides better privacy protection while achieving high-precision IoT data fusion. Considering that the addition of noise will affect the accuracy of the model, our future research directions include how to reduce the impact of noise on the global model accuracy under different local models.

## Data Availability

The Fashion-MNIST data used to support the findings of this study have been deposited in the repository, that is, https://github.com/zalandoresearch/fashion-mnist.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grant nos. U1905211 and 61702103 and the Natural Science Foundation of Fujian Province under Grant nos. 2020J01167 and 2020J01169 and 2022J01644.

## References

[1] M. Al-Rubaie and J. M. Chang, "Privacy-preserving machine learning: threats and solutions," *IEEE Security & Privacy*, vol. 17, no. 2, pp. 49–58, 2019.

[2] J. Konečnỳ, H. B. McMahan, D. Ramage, and P. Richtárik, "Federated optimization: distributed machine learning for on-device intelligence," 2016, https://arxiv.org/abs/1610.02527.

[3] J. Konečnỳ, H. B. McMahan, X. Yu Felix, P. Richtárik, T. S. Ananda, and D. Bacon, "Federated learning: strategies for improving communication efficiency," 2016, https://arxiv.org/abs/1610.05492.

[4] Di Cao, S. Chang, Z. Lin, G. Liu, and D. Sun, "Understanding distributed poisoning attack in federated learning," in *Proceedings of the 2019 IEEE 25th International Conference on Parallel and Distributed Systems (ICPADS)*, Tianjin, China, December 2019.

[5] Y. Zhao, J. Chen, J. Zhang, Di Wu, M. Blumenstein, and S. Yu, "Detecting and mitigating poisoning attacks in federated learning using generative adversarial networks," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 7, Article ID e5906, 2022.

[6] L. Zhao, S. Hu, Q. Wang et al., "Shielding collaborative learning: mitigating poisoning attacks through client-side detection," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 5, p. 1, 2020.

[7] T. Tolpegin, S. Truex, M. E. Gursoy, and L. Liu, "Data poisoning attacks against federated learning systems," *Computer Security - ESORICS 2020*, vol. 32, pp. 480–501, 2020.

[8] X. Liu, H. Li, G. Xu, Z. Chen, X. Huang, and R. Lu, "Privacy-enhanced federated learning against poisoning adversaries," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 4574–4588, 2021.

[9] X. Ma, C. Wen, and T. Wen, "An asynchronous and real-time update paradigm of federated learning for fault diagnosis," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 12, pp. 8531–8540, 2021.

[10] S. Truex, L. Liu, Ka-Ho 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*, Heraklion, Greece, April 2020.

[11] R. Hu, Y. Guo, H. Li, Q. Pei, and Y. Gong, "Personalized federated learning with differential privacy," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 9530–9539, 2020.

[12] O. Ibitoye, M. O. Shafiq, and A. Matrawy, "Differentially private self-normalizing neural networks for adversarial robustness in federated learning," *Computers & Security*, vol. 116, Article ID 102631, 2022.

[13] S. Kumar, S. Dutta, S. Chatturvedi, and M. P. S. Bhatia, "Strategies for enhancing training and privacy in blockchain enabled federated learning," in *Proceedings of the 2020 IEEE Sixth International Conference on Multimedia Big Data (BigMM)*, pp. 333–340, IEEE, New Delhi, India, September 2020.

[14] X. Zhang and X. Luo, "Exploiting Defenses against gan-based Feature Inference Attacks in Federated Learning," 2020, https://arxiv.org/abs/2004.12571.

[15] B. Liu, Y. Guo, and X. Chen, "Pfa: privacy-preserving federated adaptation for effective model personalization," *Proceedings of the Web Conference*, vol. 2021, Article ID 3449847, pp. 923–934, 2021.

[16] R. Xu, N. Baracaldo, Yi Zhou, A. Ali, J. Joshi, and H. Ludwig, "Fedv: privacy-preserving federated learning over vertically partitioned data," in *Proceedings of the 14th ACM Workshop on Artificial Intelligence and Security*, Los Angeles , CA , USA, September 2021.

[17] H. Lin, W. Liu, and X. Wang, "A secure federated learning mechanism for data privacy protection," in *Proceedings of the 2021 20th International Conference on Ubiquitous Computing and Communications (IUCC/CIT/DSCI/SmartCNS)*, London, United Kingdom, December 2021.

[18] X. Lu, Y. Liao, C. Liu, P. Lio, and P. Hui, "Heterogeneous model fusion federated learning mechanism based on model mapping," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 6058–6068, 2022.

[19] C. Dwork, A. Roth, and C. Xiao, "The algorithmic foundations of differential privacy," *Foundations and Trends® in Theoretical Computer Science*, vol. 9, no. 3-4, pp. 211–407, 2013.

[20] B. McMahan, E. Moore, D. Ramage, S. Hampson, and y A. Blaise Aguera, "Communication-efficient learning of deep networks from decentralized data," *Artificial intelligence and statistics*, vol. 20, pp. 1273–1282, 2017.