CHFDS: Clustered-based Hierarchical Federated Learning Framework with Differential Privacy and Secure Aggregation

Chih-Hung Han*, Wei-Chih Yin*, Chia-Yu Lin†, and Ted T. Kuo‡
* *Department of Computer Science and Engineering, Yuan Ze University, Taoyuan, Taiwan*
† *Department of Computer Science and Information Engineering, National Central University, Taoyuan, Taiwan*
‡ *College of Artificial Intelligence, National Yang Ming Chiao Tung University, Tainan, Taiwan*
Corresponding Author: Chia-Yu Lin (sallylin0121@ncu.edu.tw)

2023 International Conference on Consumer Electronics - Taiwan (ICCE-Taiwan) | 979-8-3503-2417-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICCE-Taiwan58799.2023.10226768

***Abstract*—Federated learning is proposed to solve data privacy and security issues for traditional machine learning, which requires the training dataset to be stored locally on a machine or data center for training. However, federated learning may have problems like Non-Independent and Identically Distributed (Non-IID) data and private security. Non-IID can lead to lower training accuracy than expected, and there may be a risk of privacy leakage in the data uploaded by clients. Therefore, this paper proposes CHFDS: Clustered-based Hierarchical Federated Learning Framework with Differential Privacy and Secure Aggregation. Before training begins, we cluster all clients so that the data distribution between clients in each group is similar. This means only a random subset of clients from each cluster is selected in each training round instead of all clients participating in the training. We can use this method to adjust the data balance of participating training. Finally, we add differential privacy and secure aggregation to the clustering and training process to improve the privacy and security of the proposed clustered federated learning framework.**

I. Introduction

Federated learning (FL) is a distributed learning framework where clients train a global model using their private data under the supervision of a server. Clients submit only model weights to protect their privacy. However, communication heterogeneity arises when multiple clients participate or are distributed over a wide geographic range, increasing communication costs.

Hierarchical federated learning (HFL) [1] was developed to reduce network transmission burden and solve the communication cost problem faced by FL. HFL introduced intermediate aggregators called "regional aggregators" between the FL server and clients to share the loads. FL clients upload their local models to a regional aggregator, which aggregates and sends the model update to the FL server. The FL server performs another aggregation to form the next round global model and redistributes it to all clients via their regional aggregator. Regional aggregators can be deployed at 5G edge computing facilities while the FL server is at the mobile operator's cloud.

However, even though HFL can effectively reduce network communication costs, federated learning still has the following problems that need to be addressed:

1) The training data among clients may exhibit Non-Independent and Identically Distributed (Non-IID) features, leading to statistical heterogeneity. It may cause the global model trained to be biased towards specific directions, resulting in lower accuracy than expected.
2) Recently, some studies have pointed out [2], [3] that there may be privacy concerns with the model weights uploaded by clients after training. Attackers may infer the original data used for training by reverse-engineering the model weights.

Since the concept of FL was proposed, some studies have used clustering methods to improve the accuracy of model training. [4] proposed a "weight-similarity-based client clustering" (WSCC) clustering method, which uses affinity propagation and cosine distance to cluster clients dynamically. The author of [5] mentioned the "federated learning by inference similarity" (FLIS) algorithm. After the client returns the trained model to the server, the server obtains inference results on its own small dataset and clusters clients based on the similarity of the inference results. In [6], the "federated learning with hierarchical clustering" (FL+HC) method was designed, which added the concept of hierarchical clustering under FL. Clients are clustered based on the similarity between their local model updates and the global model, and each cluster was trained as a specialized model.

However, current research on FL clustering usually clusters model weights without any protection measures, and there is still a risk of privacy leakage even if the model weights returned by the clients are used for clustering. Therefore, this paper proposes CHFDS. Before training begins, all clients submit their data distributions with added differential privacy (DP) to the server via the zone site for clustering so that the data distributions among clients in each cluster are similar. Then, in each round of training, a subset of clients from each cluster is selected for training, and secure aggregation (SA) is added to the model aggregation stage [7]. We expect to achieve the two effects of "reduced impact of Non-IID on the model convergence" and "protection of client information" through the above methods.

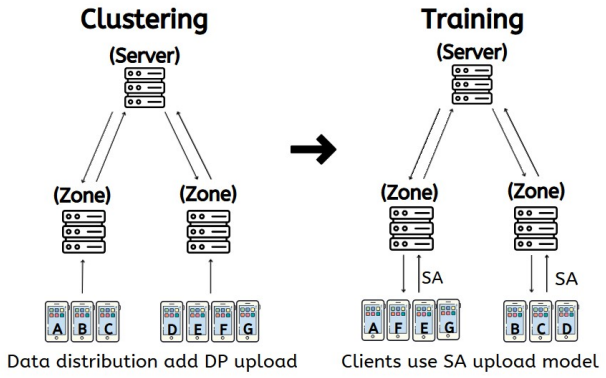

Fig. 1. The architecture of CHFDS.

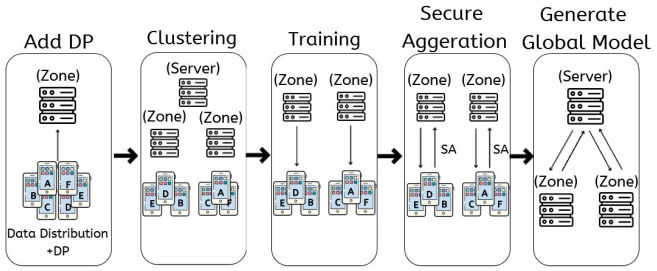

Fig. 2. The flow chart of CHFDS.

II. CHFDS: Clustered-based Hierarchical Federated Learning Framework with Differential Privacy and Secure Aggregation

The architecture of CHFDS is shown in Figure 1, which contains the servers, the zone sites, and the clients from top to bottom. The main flow chart is shown in Figure 2. Initially, the server sends a training task to the zone sites, requesting data distribution from all clients. The clients use differential privacy to add Gaussian noise to the data distribution to protect privacy and then return the data to the zone sites. The data with added noise is then used for clustering, and the AP clustering or K-means method can be used. After clustering, clients with similar data distributions are classified under the same zone site to form clusters. At this point, federated learning starts, and SA is added simultaneously. Here we refer to the security aggregation protocol, and Salvia [8] deploying SA into our architecture. The following is the training process after clustering:

1) Each zone site samples its own client devices for training. Because of the data distribution similarity, only a portion of the client devices needs to be involved in each round of training.
2) The global model weights are distributed to the client devices participating in the training.
3) The client devices train the model using their data and add two masks to the model based on the concept of SA before returning it to the zone site.
4) The zone site aggregates the encrypted models returned by the client devices into the regional model.

Finally, all the regional models are aggregated upwards to the server to form a new round of global models.

III. Discussion

In this study, the framework is based on HFL, and clustering is used to mitigate the impact of Non-IID. In addition, DP and SA are used to protect the client's data privacy during the data uploading phase. The expected effects are:

- Protection of client information: During the clustering phase, the data distribution of the client has been added with noise, so it is impossible to know the exact data distribution status. In the model uploading phase, the client will perform SA with other participating clients in the group. Finally, the zone site can only see the aggregated model weights of all clients.
- Reduced impact of Non-IID on the model convergence: Because only a portion of clients is selected from each cluster in each training round, the data balance can be adjusted based on this.

IV. Conclusion

In this paper, we proposed a CHFDS framework to address the impact of Non-IID data on federated learning and the issue of data privacy. We used client clustering to elect representative clients for a region to participate in FL without losing model performance. Moreover, we integrated differential privacy and secure aggregation to protect client privacy. In the future, our research will focus on the grouping benefits of different Non-IID data distributions. Furthermore, we will explore how to select customers from each group during each training round to mitigate the effect of Non-IID data.

Acknowledgements

This work is sponsored by the National Science and Technology Council (NSTC) under the project NSTC 111-2622-8-A49-023 and NSTC 110-2222-E-008-008-MY3.

References

[1] Lumin Liu et al., "Client-edge-cloud hierarchical federated learning," in *IEEE International Conference on Communications (ICC)*.
[2] Ligeng Zhu, Zhijian Liu, and Song Han, "Deep leakage from gradients," *Advances in neural information processing systems*, vol. 32, 2019.
[3] Bo Zhao et al., "idlg: Improved deep leakage from gradients," *arXiv preprint arXiv:2001.02610*, 2020.
[4] Pu Tian et al., "Wscc: A weight-similarity-based client clustering approach for non-iid federated learning," *IEEE Internet of Things Journal*, vol. 9, no. 20, pp. 20243–20256, 2022.
[5] Mahdi Morafah et al., "Flis: Clustered federated learning via inference similarity for non-iid data distribution," *arXiv preprint arXiv:2208.09754*, 2022.
[6] Christopher Briggs et al., "Federated learning with hierarchical clustering of local updates to improve training on non-iid data," in *IEEE International Joint Conference on Neural Networks (IJCNN)*.
[7] Keith Bonawitz et al., "Practical secure aggregation for privacy-preserving machine learning," in *ACM SIGSAC Conference on Computer and Communications Security*.
[8] Kwing Hei Li et al., "Secure aggregation for federated learning in flower," in *ACM International Workshop on Distributed Machine Learning*.