

SUPPLEMENTARY MATERIAL FOR: ENHANCING THE PRIVACY OF FEDERATED LEARNING THROUGH DATA SYNTHESIS

Anonymous authors

Paper under double-blind review

1 ADDITIONAL EXPERIMENTS AND RESULTS

1.1 ACCURACY COMPARISON FOR TWO CLIENT SETUP

In the table 1 and 1 we present the results for the accuracy comparison of PPFed, FedAvg and DOSFL+ for the case of 2 clients. We split the data among the two clients in an iid fashion. We can observe that PPFed almost performs comparable to DOSFL+ and even marginally better for MLP+FashionMNIST case. The large gap with convnet is due to the DCGM algorithm.

Model+Dataset	FedAvg (Accuracy %)	DOSFL+ (Accuracy %)	PPFed (Accuracy %)
ConvNet + CIFAR10	76.14	49.06	48.82
LeNet+MNIST	98.36	92.84	91.8
MLP+FashionMNIST	85.15	80.18	80.67

Table 1: Top 1 % Accuracy comparison for 2 clients across datasets and models

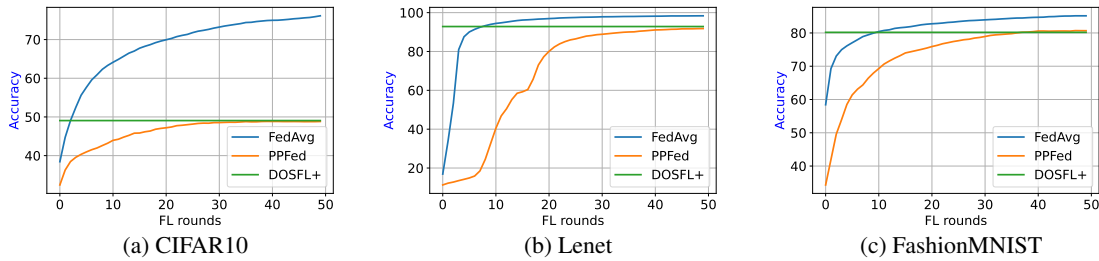


Figure 1: Comparison of methods across different datasets with 2 clients

1.2 ACCURACY VS TIME TRADE-OFF FOR PPFED

In the Figures 2,3 we analyze the Accuracy vs Time trade-off for PPFed method when there are 5 and 2 clients respectively.

Hollow markers indicate the accuracy of a freshly initialised model trained for 300 epochs, on CD generated using the value of K (hyperparameter in dcm algorithm) indicated by the shape of the marker; and the time taken for generation of CD, at the end of Stage 1 of PPFed. Furthermore, each solid marker represents the accuracy of an model trained for 20 local epochs on CD generated using K value indicated by the marker during an FL Round, and the training + aggregation time taken for that FL Round in Stage 2 of PPFed. The black line joining solid markers in these plots indicates the Pareto frontier which is the set of Pareto-efficient configurations with respect to accuracy and training time.

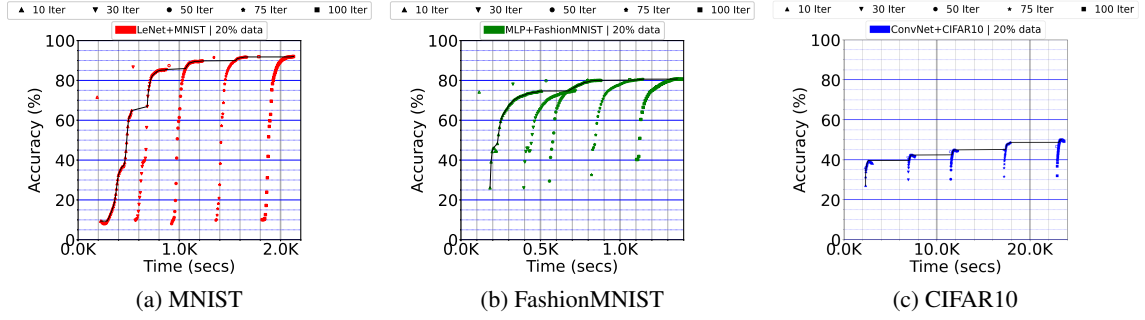


Figure 2: PPFed | i.i.d. | 5 clients | Accuracy vs Time Trade-Off

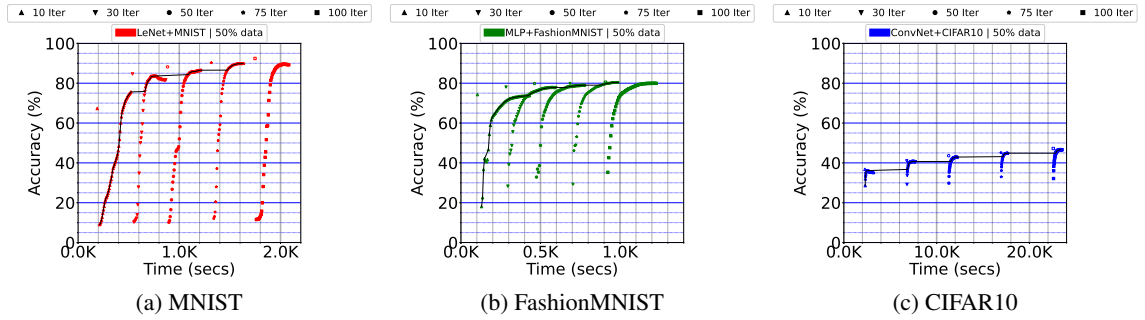


Figure 3: PPFed | i.i.d. | 2 clients | Accuracy vs Time Trade-Off

1.3 ACCURACY VS TIME COMPARISON OF PPFED, FEDAVG AND CENTRALIZED TRAINING

In the figures 4,5, we capture the Accuracy vs time plots of PPFed, FedAvg and centralized training for lenet model and MNIST dataset. In this analysis we ignore the time required for condensed data generation. We only compare the Federated learning on condensed data for PPFed vs FedAvg. It can be clearly seen that the time required for convergence of PPFed is relatively lower compared to FedAvg.

Similarly the figures 6,7 capture the Accuracy vs time plots of PPFed, FedAvg and centralized training for MLP model and FashionMNIST dataset.

The figures 9,8 capture the Accuracy vs time plots of PPFed, FedAvg and centralized training for ConvNet model and CIFAR-10 dataset.

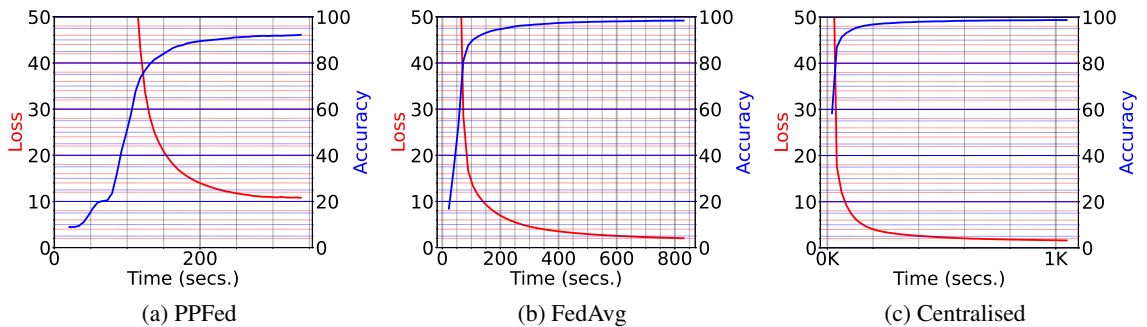


Figure 4: LeNet+MNIST | i.i.d. | 2 clients | Accuracy vs Time

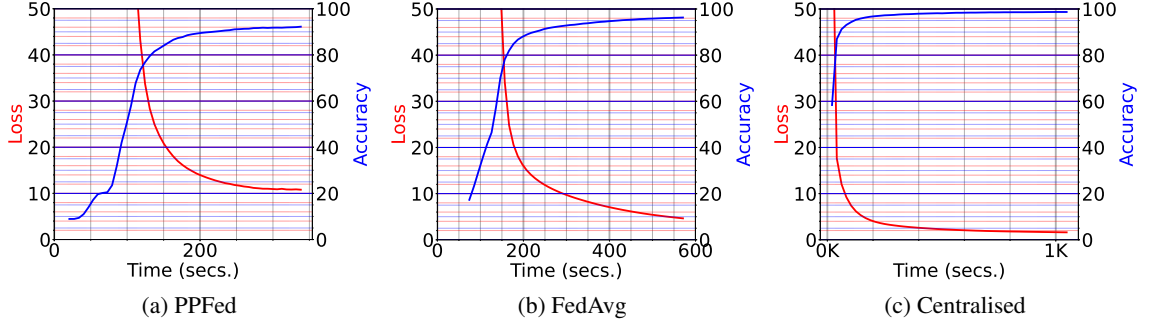


Figure 5: LeNet+MNIST | i.i.d. | 5 clients | Accuracy vs Time

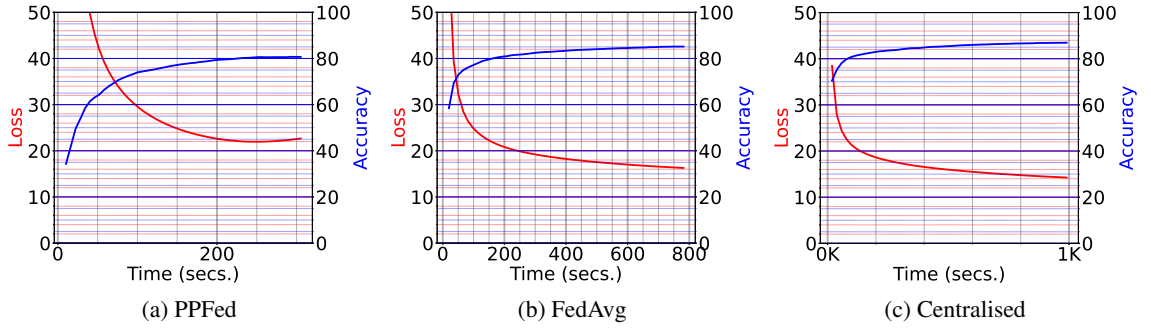


Figure 6: MLP+Fashion MNIST | i.i.d. | 2 clients | Accuracy vs Time

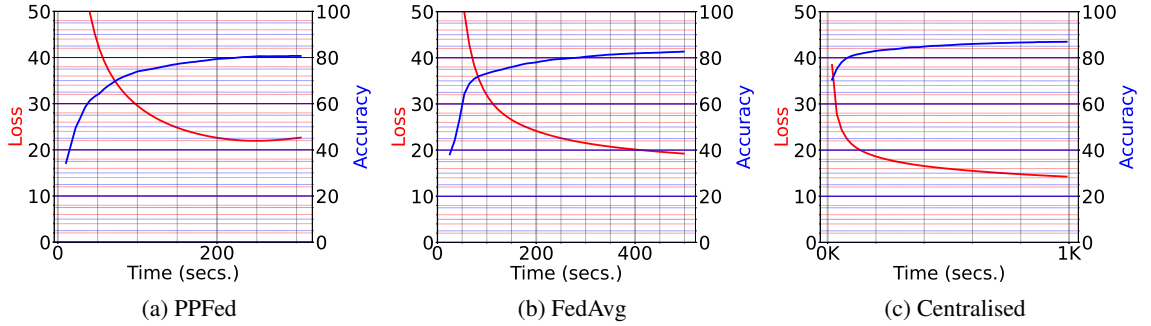


Figure 7: MLP+Fashion MNIST | i.i.d. | 5 clients | Accuracy vs Time

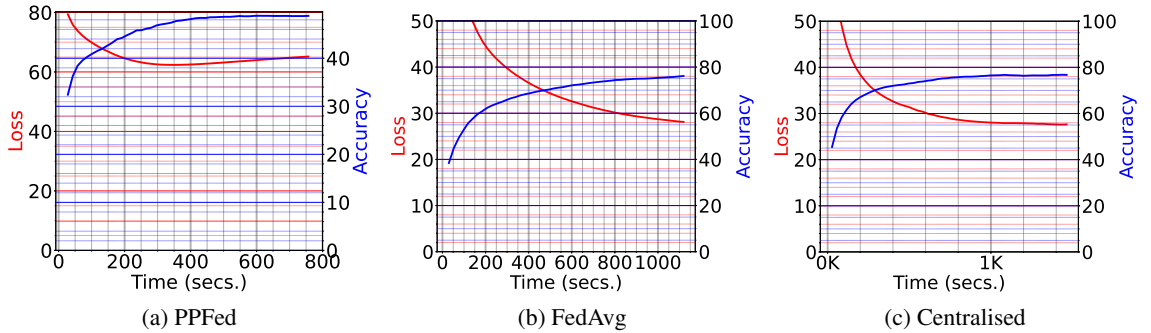


Figure 8: ConvNet+CIFAR10 | i.i.d. | 2 clients | Accuracy vs Time

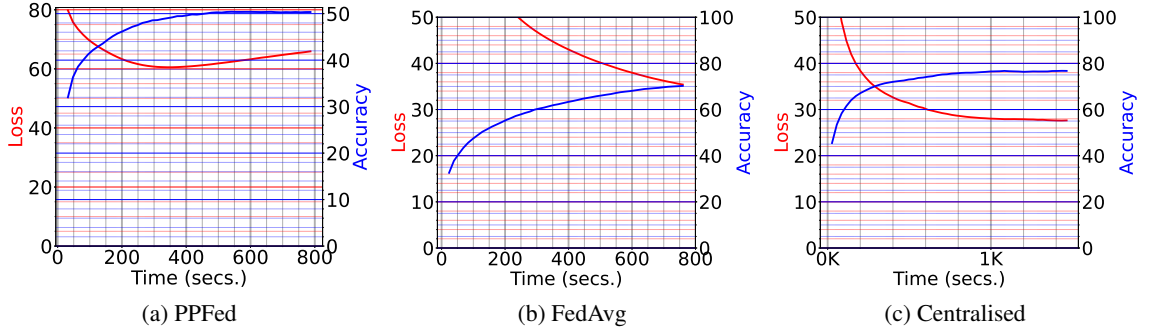


Figure 9: ConvNet+CIFAR10 | i.i.d. | 5 clients | Accuracy vs Time

1.4 DATA TRANSFER STATISTICS

In the figure 10, we compare the amount of cumulative data transfer in the network for PPFed and FedAvg as the FL rounds progresses. We see that data sent from the server to clients is roughly double the size as the models stored at the server are of double the size compared to the client models in the Flower framework. We also see that both the methods utilize similar bandwidths.

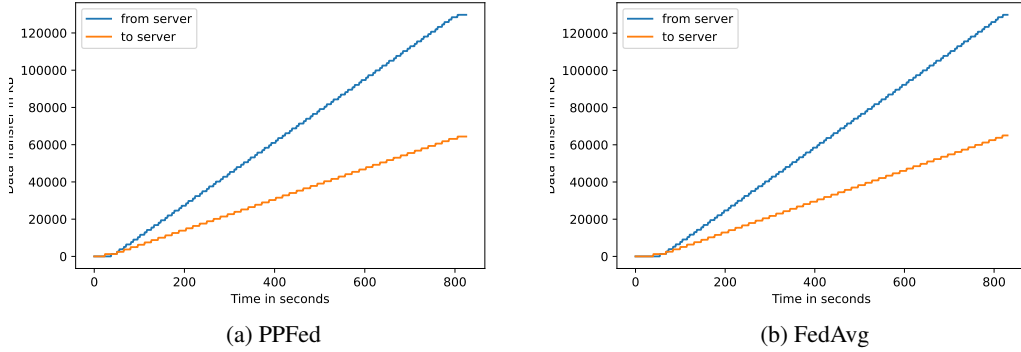


Figure 10: ConvNet-CIFAR10 data transfer per client