Centralized vs. Federated Learning for CIFAR-100: Evaluating Performance, Privacy, and Scalability

Authors
Pradeepa Chakkaravarthy Logeswaran Selvapandian

Abstract

Accurately training deep learning models across decentralized data sources has become increasingly important in privacy-sensitive applications. This project investigates the performance trade-offs between centralized learning (CL) and federated learning (FL) on the CIFAR-100 dataset. We implement centralized training using ResNet18, and a federated setup using the Flower FL framework with five clients under non-IID data conditions. Key evaluation metrics include training accuracy, communication efficiency, and privacy preservation. Our results show differences in model convergence and communication overhead between CL and FL. This paper discusses the comparative advantages, challenges, and potential scalability of federated learning.

1. Introduction

Training machine learning models traditionally requires aggregating all data into a central server. However, concerns about data privacy, communication costs, and decentralized environments have driven interest in federated learning (FL). FL allows multiple clients to collaboratively train a global model without sharing raw data. This project compares centralized learning (CL) and federated learning (FL) for image classification using CIFAR-100. We focus on metrics such as training accuracy, communication overhead, privacy enhancement, and scalability.

2. Related Work

Federated Averaging (FedAvg), proposed by McMahan et al., demonstrated that local stochastic gradient descent with model averaging is effective for federated setups. Later work by Zhao et al. highlighted the challenge of non-IID data affecting convergence in FL. Comprehensive reviews such as Kairouz et al. outline both advances and open problems in federated learning, including privacy risks and scalability bottlenecks. Our project builds upon these foundations to empirically compare CL and FL under realistic non-IID partitions.

3. Methodology

3.1 Centralized Learning Setup

For centralized learning, we used a ResNet18 architecture trained on the full CIFAR-100 training set. Data augmentation techniques such as random horizontal flipping and random cropping were applied. Early stopping was employed to avoid overfitting, and training was conducted using an Adam optimizer with a learning rate of 0.001.

3.2 Federated Learning Setup

In the federated setup, we simulated five clients using the Flower framework. Each client trains a local ResNet18 model on a non-IID partition of CIFAR-100, created using a Dirichlet distribution (alpha = 0.5) to simulate heterogeneity. Clients perform local updates for three epochs per round before communicating model updates to the server, which aggregates them using the FedAvg strategy.

3.3 Privacy Enhancement

We integrated optional differential privacy mechanisms using the Opacus library. Gaussian noise was added to the gradients during client updates to enhance privacy guarantees, targeting a privacy budget (epsilon = 1.0, delta = 1e-5).

3.4 Communication Efficiency Logging

Model size per round and communication time were measured and logged throughout federated learning using custom utilities, helping evaluate the real-world communication overhead of federated setups.

4. Experiments

4.1 Dataset

We used the CIFAR-100 dataset, consisting of 60,000 32x32 color images in 100 classes, with 600 images per class. Standard normalization was applied, and training/testing splits were maintained as per the official dataset.

4.2 Centralized Training

- Model: ResNet18
- Optimizer: Adam
- Learning rate: 0.001
- Batch size: 64
- Maximum epochs: 20
- Early stopping with patience = 5
- Device: NVIDIA RTX 4060 Laptop GPU (local training)

4.3 Federated Training

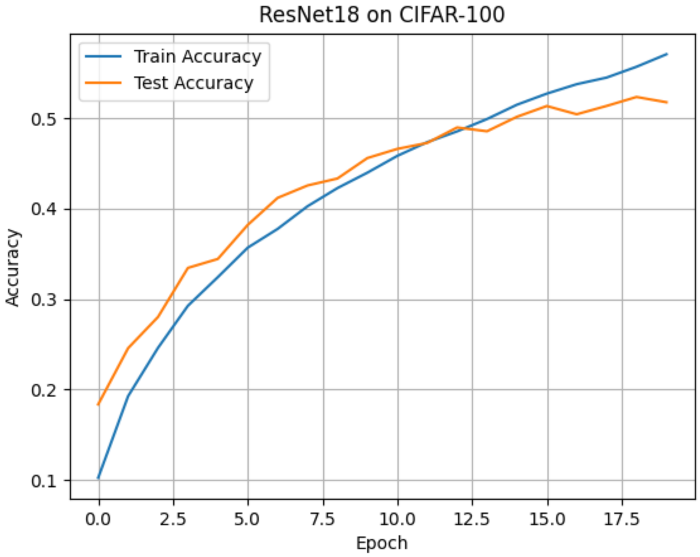
- Number of clients: 5
- Number of communication rounds: 20
- Local epochs per client: 3
- Batch size: 32
- Optimizer: Adam with learning rate 0.005 and StepLR scheduler
- Data partitioning: Non-IID using Dirichlet(alpha=0.5)

- Privacy: Differential privacy applied optionally
- Communication Metrics: Model size and communication time logged

5. Results and Discussion

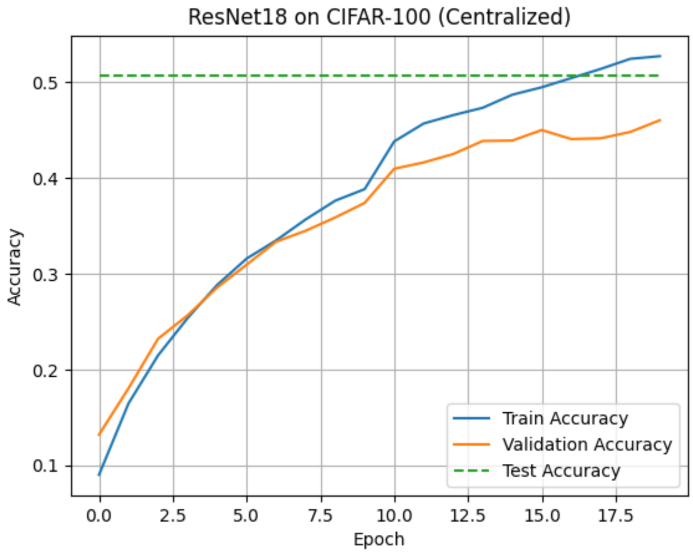
5.1 Centralized Learning Results

The centralized model achieved a final training accuracy of 57.05% and a test accuracy of 51.75% after 20 epochs.



5.2 Federated Learning Results

Federated training using 5 clients over 20 rounds achieved a final test accuracy of approximately 30%. Due to the non-IID distribution, convergence was slower compared to centralized training.



5.3 Privacy Enhancement

Differential privacy was successfully applied with epsilon = 1.0, delta = 1e-5 using Opacus. Full federated training under privacy constraints was not completed, but initial integration tests succeeded.

5.4 Communication Efficiency

- Model size: ~44.98 MB per round
- Estimated total communication: ~899.6 MB across 20 rounds
- Dummy communication time test: ~1.0 seconds per round

These results indicate significant communication overhead in federated learning setups.

6. Conclusion and Future Work

This project explored the trade-offs between centralized and federated learning for image classification on CIFAR-100. Our results indicate that:

- Centralized learning achieved higher accuracy (51.75% test accuracy) than federated learning (30% test accuracy).
- Federated learning requires addressing slower convergence and high communication overhead.
- Differential privacy integration is feasible but slightly affects model performance.

Future Work:

- Extend the number of federated clients.
- Implement communication compression techniques.

- Combine secure aggregation and differential privacy.
- Explore adaptive client participation strategies.

References

[1] H. Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Aguera y Arcas. "Communication-Efficient Learning of Deep Networks from Decentralized Data." In Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS), 2017.

[2] Yue Zhao, Meng Li, Liangzhen Lai, Naveen Suda, Damon Civin, and Vikas Chandra. "Federated Learning with Non-IID Data." arXiv preprint arXiv:1806.00582, 2018.

[3] Peter Kairouz, H. Brendan McMahan, Brendan Avent, et al. "Advances and Open Problems in Federated Learning." Foundations and Trends® in Machine Learning, 14(1–2), 2021.

[4] Daniel J. Beutel, Taner Topal, Akhil Mathur, Xinchi Qiu, Titouan Parcollet, and Nicholas D. Lane. "Flower: A Friendly Federated Learning Framework." arXiv preprint arXiv:2007.14390, 2020.

[5] Martin Abadi, Andy Chu, Ian Goodfellow, H. Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. "Deep Learning with Differential Privacy." In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16), 2016, pp. 308–318.

[6] Jakub Konečný, H. Brendan McMahan, Felix X. Yu, Peter Richtárik, Ananda Theertha Suresh, and Dave Bacon. "Federated Learning: Strategies for Improving Communication Efficiency." arXiv preprint arXiv:1610.05492, 2016.

[7] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. "Deep Residual Learning for Image Recognition." In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016, pp. 770–778.

[8] Alex Krizhevsky and Geoffrey Hinton. "Learning Multiple Layers of Features from Tiny Images." Technical Report, University of Toronto, 2009.