Federated Learning for Large Language Models

*Archit Ojha*

*School of CSE andTechnology Bennett University Greater Noida, India*

*Aryan Singh*

*School of CSE and Technology*

*Bennett University Greater Noida, India*

*Vaibhav Ahlawat*

*School of CSE and Technology Bennett University Greater Noida, India*

*Soumay Choudhry*

*School of CSE and Technology Bennett University Greater Noida, India*

1. Introduction

As data collection in the ML field increases, storing and managing data is not the only problem we face today. Privacy and security of data are also taken into consideration. Privacy of one’s personal information has always been a priority, and over the years, many works have been done to improve security and data privacy. The nature of most of the data is privacy-sensitive, to overcome this data breach problem, the Federated learning approach comes into play. Federated learning is an approach of Machine Learning in which data sets are trained on multiple edge devices locally without any sharing of data.

Federated learning implementation has significantly impacted data privacy and security and made the training of data sets easier. As previously ,centralized methods were used in which data was trained and a model was created on the one server which may expose the personal information and data. But with Federated learning models are trained on edge devices and with no sharing of data to another server no personal data is exposed.

It allows total control of the model on the edge user i.e. which information to share, remove or hide all actions are taken on the user's consent which make it a very reliable form of learning for training the large models. Privacy-perspective wise private data doesn't leave the device and only meaningful data is used in the training which makes it very privacy friendly.However, Federated learning is vulnerable to poisoning attacks which aim at causing convergence to the wrong model. Federated learning can be classified into horizontal,vertical and transfer learning based on their distribution.horizontal-same features but different samples,vertical -same user but different features,transfer-not having enough data to train. Federated learning distributed deep learning by eliminating central approach techniques and training data set on their devices.With the increase in IoT devices and edge devices the collection of data has become efficient and for large data Federated learning is best for model training over the traditional methods.

All the measures and privacy safeguards ensure that the Federated learning does not violate the GDPR or another data based law.

This technique of training models on decentralized data involves a central server and a group of clients. Clients are compute nodes that perform local training using their local data. The central server first sends a standard global model to a group of clients. Clients then train the global model with local data and provide local models back to the server. The server aggregates the local models into a new global model and then starts a new training round. This process may be repeated several times until the global model converges or a certain threshold is reached.

Federated optimization has several key properties that differentiate it from a typical distributed optimization problem:

• **Non-IID**: The training data on a given client is typically based on the usage of the mobile device by a particular user, and hence any particular user’s local dataset will not be representative of the population distribution.

• **Unbalanced Similarly**: some users will make much heavier use of the service or app than others, leading to varying amounts of local training data.

• **Massively distributed**: We expect the number of clients participating in an optimization to be much larger than the average number of examples per client.

• **Limited communication**: Mobile devices are frequently offline or on slow or expensive connections.

Table 1: Literature Review

| S.no | Paper Name | Dataset | Implementation | Results |
| --- | --- | --- | --- | --- |
| 1. | Communication-Efficient Learning Deep Networks From Decentralized Data | Large-scale next-word prediction  ( 10 million public social media posts ) | FederatedAveraging Algorithm (FedAvg): Combines local SGD updates with global model averaging. | Achieved 10.5% accuracy in 35 rounds with FedAvg (23× fewer than FedSGD). |
| 2. | Federated Learning of Large Language Models with Parameter-Efficient Prompt Tuning and Adaptive Optimization. | QNLI, SST-2, CoLA, MRPC, RTE, and BoolQ. | FedPepTAO: A parameter-efficient prompt tuning approach combined with adaptive optimization. | Outperformed baselines by up to **60.8% in accuracy** and reduced training time by up to **97.59%**. |
| 3. | Fed-ensemble: Ensemble Models in Federated Learning for Improved Generalization and Uncertainty Quantification | MNIST, FEMNIST, CIFAR-10, CIFAR-100, Shakespeare, OpenImage, 3D Printer Dataset | Trains an ensemble of K models using random permutations | Outperformed baseline fl methods like FedAvg, FedProx, and FedBe across datasets. |
| 4. | ARobust Privacy-Preserving Federated Learning Model Against Model Poisoning Attacks | MNIST, KDDCup, Amazon Reviews | They introduce an internal auditor that evaluates encrypted gradient similarity and distribution to differentiate between benign and malicious gradients | Demonstrates significant robustness against both targeted and untargeted attacks in IID and non-IID settings. |
| 5. | OpenFedLLM: Training Large Language Models on Decentralized Private Data via Federated Learning | Alpaca, Alpaca-GPT4, FinGPT, MedAlpaca, Code-Alpaca, MathInstruct, UltraFeedback, HH-RLHF | Introduced a research-friendly framework/codebase, named OpenFedLLM | Outperformed state-of-the-art models like GPT-4 in domain specific  datasets |
| 6. | Federated Learning for Breast Density Classification: A Real-World Implementation | 2D mammography and tomosynthesis images | Implemented using the FederatedAveraging algorithm to aggregate model updates from decentralized client data. | 6.3% Improvement in accuracy on local test datasets.A45.8% improvement in generalizability on external test dataset |
| 7. | TITANIC: Towards Production Federated Learning with Large Language Models | Wikitext-2-raw-v1 dataset  ( 36,700 text samples ) | A mechanism to partition LLMs and facilitate seamless forward and backward passes across client devices. | achieved similar convergence trends to centralized training. |

| 8. | Federated Large Language Models for Swarm Intelligence: A Survey | GLUE, MRPC, SST2, and OntoNotes, IMDB, Yelp, and AGNEWS | Ppaper explores multiple federated learning techniques for LLMs in swarm intelligence contexts | Does not present new experimental results |
| --- | --- | --- | --- | --- |
| 9. | Federated Large Language Models: Current Progress and Future Directions | GLUE, MRPC, SST2, Medical VQA, Weather Forecasting Data | The paper explores efficient federated fine-tuning methods privacy-preserving techniques, and communication-optimized frameworks | Achieve performance comparable to centralized models when well-optimized. |
| 10. | Heterogeneous Federated Learning: State-of-the-art and Research Challenges | IoT data, healthcare data, and more | The paper categorizes HFL methods into data-level, model-level, and server-level strategies to address heterogeneity in data, models, and system coordination. | Does not present new experimental results |
| 11. | Model Merging in LLMs, MLLMs, and Beyond: Methods, Theories, Applications, and Opportunities | Reviews existing works in the fields of large language models (LLMs) | Model merging strategies span preparation techniques and advanced integration methods to optimize the fusion of diverse model capabilities. | highlights the practical applications and challenges of model merging across fields |