Federated Learning in Wireless Security

Ekansh Singh
ee1200490@iitd.ac.in

Tanish Singh Tak
ee1200560@iitd.ac.in

Dr. Harshan Jagadeesh
jharshan@iitd.ac.in

***Abstract*—The contemporary landscape of data science confronts a paradigm shift marked by the imperatives of stringent data privacy regulations. Navigating this landscape requires innovative solutions to facilitate secure data sharing in scenarios where third parties are reluctant due to privacy constraints. In response to this challenge, our research endeavors to devise a pioneering approach by using Federated Learning and cryptographic methods.**

This report includes the problem statement that shows our investigation—a complex challenge arising from the delicate equilibrium between ensuring data privacy and facilitating collaborative model training. Leveraging the MNIST dataset as a foundation, our project employs Federated Learning to address scenarios where data centralization is impractical due to privacy concerns.

This report encapsulates our ongoing work, presenting an in-depth analysis of the methodologies employed, the challenges encountered, and the outcomes achieved thus far. Our findings not only contribute to the discourse on privacy-preserving machine learning but also lay the groundwork for a broader exploration of federated learning in diverse application domains. As we outline our next course of action, the synthesis of cryptographic methods and federated learning emerges as a promising avenue for unlocking the potential of secure and privacy-respecting collaborative data analytics.

***Index Terms*—Federated Learning, privacy, neural networks, correlation, ensemble learning**

I. Introduction

This report explores the innovative application of federated learning, a privacy-preserving machine learning paradigm. Federated learning is a machine learning approach that allows multiple parties to collaboratively train a shared machine learning model while keeping their data decentralized and private.

In Federated Learning, merging multiple models to boost accuracy is a clear objective. Ensemble learning plays a crucial role in this context, harnessing collective data from diverse models to enhance overall performance and reliability. Ensemble learning includes various techniques like (Weighted) Average Method, Bagging, Boosting, Stacking, tailored to specific aspects of model collaboration. We used the (Weighted) Average Method in our initial work to gain some insights on how merging of models can increase the accuracy. The concept of Federated Learning revolves around the idea of training models across multiple devices or nodes (such as smartphones, edge devices, or servers) where the data resides, rather than transferring the data to a central server for processing. This approach is particularly useful in scenarios where data privacy is crucial, like in healthcare, finance, or situations where data cannot be easily moved due to regulatory or privacy constraints. There isn't much literature about how it can be implemented on MNIST dataset and we have tried to use FL on the MNIST dataset to achieve increase in accuracy without explicity revealing the infomation about the models. Instead of centralizing the dataset on a single server, the model is trained collaboratively by aggregating local updates made on each client device while preserving the privacy of individual data samples. The flow basically consistes of 4 steps:

- **Initialization:** Initial model sent to all the devices
- **Local Training:** Every client trains the model on its local data improving the specifics of their dataset
- **Model Aggregation:** The updated models are aggregated/combined to create an improved model and sent to the global server
- **Iteration:** Step 2 and 3 are repeated untill it converges or overfits while maintaining data and model privacy

This can also be used to quantify how diverse is the third-party dataset compared to ours so as to achieve more diversity without any compromise to privacy of data.

II. Dataset

In our project, we utilized the MNIST dataset for image classification purposes. The MNIST data comprises an extensive array of 28x28 grayscale images depicting handwritten digits ranging from 0 to 9. Recognized as a benchmark dataset, MNIST holds prominence as an evaluative metric for the development and assessment of machine learning models, specifically within the domain of digit recognition. It contains 60K datapoints in the training dataset and 10K datapoints in the testing dataset. The incorporation of the MNIST dataset in our research served as a foundational element for both training and evaluating the efficiency of our models.

III. Our Work

A. Approach-I

We constructed a neural network utilizing the MNIST dataset for the purpose of image classification. In order to investigate the impact of weights and bias sharing between two distinct models, our approach involved the training of one model on data comprising images falling within the range of zero to four, while concurrently training the second neural network on a distinct dataset comprising images falling within the range of five to nine. Subsequently, we conducted testing on both of our models employing two distinct datasets: one comprising images within the range of zero to four, and the other comprising images within the range of five to nine. Following this initial evaluation, we merged our two models using the (Weighted) Average Method. Subsequently, we subjected this updated model to testing using the earlier test datasets, observing the impact on accuracy of the model. The observations made are given in the following Table 1.

TABLE I: Accuracy Comparison

Model Type	Test Dataset Type	Accuracy (in %)
Model_04	Dataset_04	98.988
Model_59	Dataset_59	98.478
Model_04	Dataset_04	0.0
Model_59	Dataset_59	0.0
Model_merged	Dataset_04	51.683
Model_merged	Dataset_59	62.292

[1]

We initially noticed high accuracy rates in the first two cases due to the similarity between training and testing datasets. In contrast, accuracy dropped to zero in the subsequent two cases, where the testing dataset differed from the training dataset, highlighting the absence of relevant training data. However, in the final two cases, when testing the model with merged weights and bias, we observed a substantial accuracy improvement, rising from 0% to approximately 50-60% for both datasets.

B. Approach-II

In the first approach, we subjected our models, trained on datasets containing digits from zero to four and five to nine, to cross-testing scenarios. But we can not easily explain the increase in accuracy with respect to the diversity in data since the numbers on which data was trained and tested were completely different, hence giving zero accuracy initially. In the subsequent approach, we departed from dividing datasets based on numerical ranges and instead created two distinct datasets, each comprising digits from zero to nine. Subsequently, two models were trained on these datasets, and their accuracies were evaluated on a shared test dataset. Following this assessment, we employed the (Weighted) Average method to merge the models, subsequently evaluating the accuracy of the merged model on the test dataset and noting the resultant accuracy.

TABLE II: Accuracy Comparison

Model Type	Accuracy (in %)
Model_1	93.72
Model_2	93.30
Model_merged	36.23

Initially, we observed accuracy rates of approximately 93% in the first two cases. Nevertheless, in the final case, wherein the model was tested with merged weights and biases, a decline in accuracy to 36.23% was noted. The reason for the following decrease in accuracy could be the single-time averaging of weights and biases. To address this, we intend to implement the federated averaging algorithm in our subsequent approach, aiming to enhance the model's overall performance.

C. Approach III

In this approach, to facilitate collaborative learning without centralizing data, the MNIST dataset was divided into two balanced subsets. Each subset contained 200 samples from each of the 10 classes, resulting in two datasets, each consisting of 2000 samples. This balanced representation across classes ensured a fair distribution of digit samples for training.

The implementation followed an iterative Federated Learning process mentioned in the paper in the references. Initially, an initial model was distributed to all devices hosting the respective subsets. Each device performed local model training on its subset, leveraging the local data without sharing it externally. The updated models were aggregated to create an improved global model, and this process iterated multiple times to refine the global model collaboratively.

Across iterative rounds, both models exhibited a noticeable increase in accuracy. The accuracy improvements were tracked and recorded for each iteration. Graphical representations indicated consistent enhancement in model performance over successive rounds of collaborative training.

The observed accuracy increase can be attributed to the collaborative nature of Federated Learning. Leveraging diverse but balanced subsets allowed models to generalize better by learning from a wider spectrum of data while preserving individual data privacy. Challenges encountered, such as heterogeneity in local datasets, were addressed through aggregation techniques and careful model updating strategies.

Comparing the final accuracy of models after multiple iterations with their initial performance showcased a significant improvement. This experiment underscores the effectiveness of iterative Federated Learning on decentralized datasets derived from the MNIST dataset. It highlights the potential of this approach in enhancing model accuracy while respecting data privacy constraints.

TABLE III: Accuracy vs Iteration for Model 1

Iteration	Accuracy (in %)
1	84.46
10	89.17
20	89.60
30	89.80
40	89.98
50	90.08

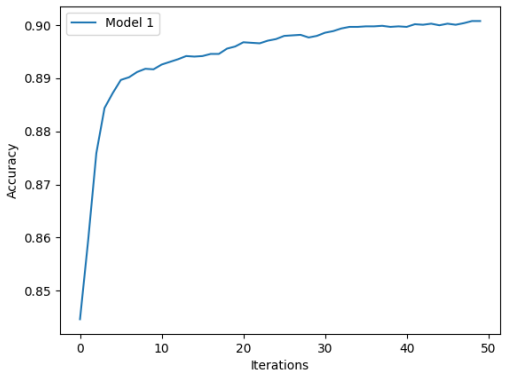

Fig. 1: Accuracy vs Iterations plot for Model 1

[1]Model_04 and Model_59 denote models trained on numbers 0-4 and 5-9, respectively, with Model_merged indicating the merged model. Dataset_04 and Dataset_59 represent datasets for numbers 0-4 and 5-9, respectively.

TABLE IV: Accuracy vs Iteration for Model 2

Iteration	Accuracy (in %)
1	86.96
10	89.36
20	89.43
30	89.61
40	89.93
50	90.06

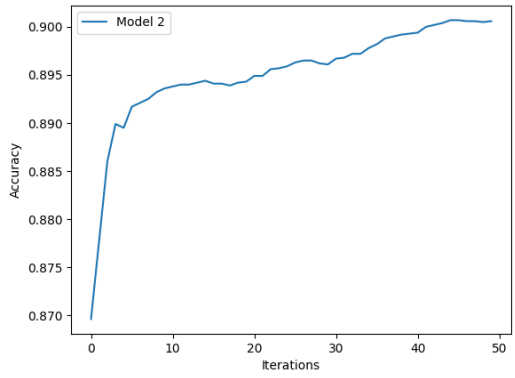

Fig. 2: Accuracy vs Iterations plot for Model 2

D. Approach IV

Following the successful application of iterative Federated Learning using smaller subsets of the MNIST dataset in the last approach, we did some further experimentation to investigate the relationship between dataset correlation and accuracy improvement in collaborative model training. This approach outlines the process, observations, and findings from this extended experiment.

To explore the impact of dataset correlation on Federated Learning, 10 models were trained, each utilizing a dataset comprising 1000 samples, with 100 samples from each of the 10 classes in the MNIST dataset. This expanded dataset allowed for more comprehensive analysis of the correlation and its effects on collaborative learning.

A unique approach was taken this time, involving the implementation of Federated Learning for every pair of models created. This meant that each pair of models underwent collaborative training, with the process repeated across all possible model combinations. Simultaneously, the correlation between the datasets used for training these models was calculated.

During the iterative Federated Learning process for each model pair, an increase in accuracy was observed, as seen in the previous experiments. However, a significant observation emerged when correlating dataset similarity with accuracy improvements. It was noticed that as dataset correlation increased between model pairs, the magnitude of accuracy improvement decreased.

This result aligns with intuitive expectations; as datasets become more highly correlated, the potential for accuracy improvement diminishes. This is due to the nature of Federated Learning, where diverse and less correlated datasets contribute to better generalization. When datasets are highly correlated, the shared information among models is already captured, limiting the potential for significant accuracy gains.

The findings strongly support the hypothesis that dataset correlation plays a crucial role in the effectiveness of Federated Learning. As correlation between datasets increased, the observed increase in accuracy decreased, in line with the expectations based on the intuition that highly correlated datasets limit the potential for substantial accuracy improvements.

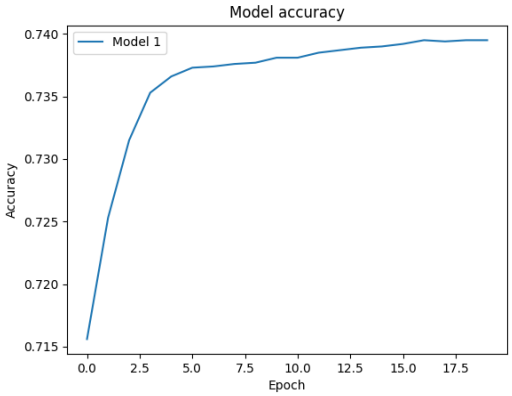

Fig. 3: Accuracy vs Iterations with dataset 1 and 2

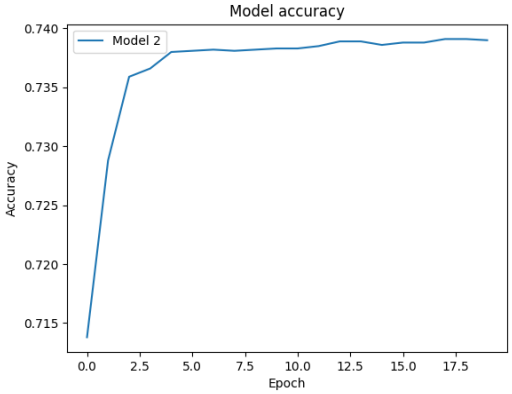

Fig. 4: Accuracy vs Iterations with dataset 1 and 2

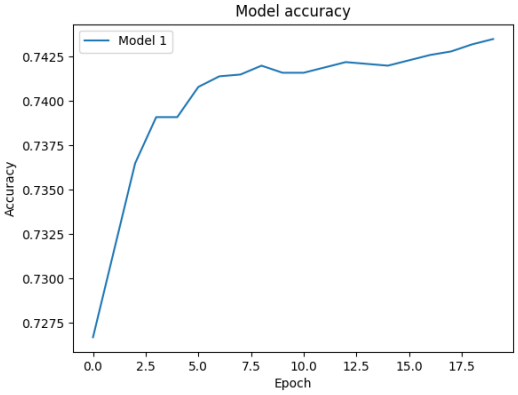

Fig. 5: Accuracy vs Iterations with dataset 2 and 3

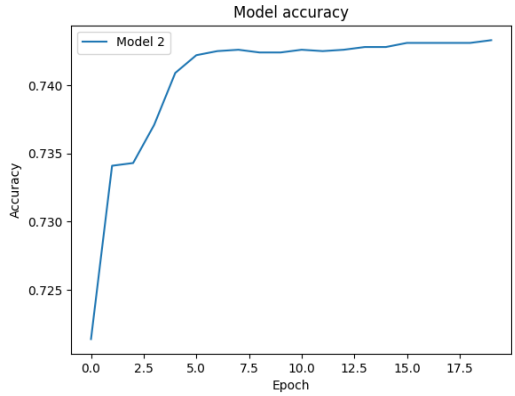

Fig. 6: Accuracy vs Iterations with dataset 2 and 3

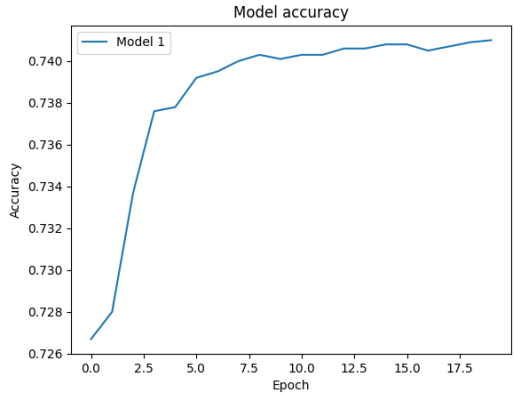

Fig. 7: Accuracy vs Iterations with dataset 5 and 6

IV. Overall Results

The series of experiments conducted to explore Federated Learning with distinct dataset configurations provided insightful observations and valuable lessons in the pursuit of collaborative model training while considering dataset characteristics.

A. Approach 1: Division into Two Mutually Exclusive Datasets

The initial attempt involved splitting the MNIST dataset into two mutually exclusive subsets—0 to 4 and 5 to 9. These subsets were trained independently, but the subsequent weight averaging approach didn't yield evident accuracy improvements. This highlighted the limitation of splitting the data into non-overlapping classes, hindering potential collaborative learning opportunities.

B. Approach 2: Correction with Complete Class Representation

To address the limitations of the first approach, datasets containing samples from all classes (0 to 9) were generated, totaling 10,000 samples with 1,000 samples from each class. However, while applying weight averaging, issues persisted, prompting further investigation.

C. Approach 3: Adoption of Iterative Federated Learning

Inspired by the research paper, the third approach involved creating two datasets with 1,500 samples, distributing

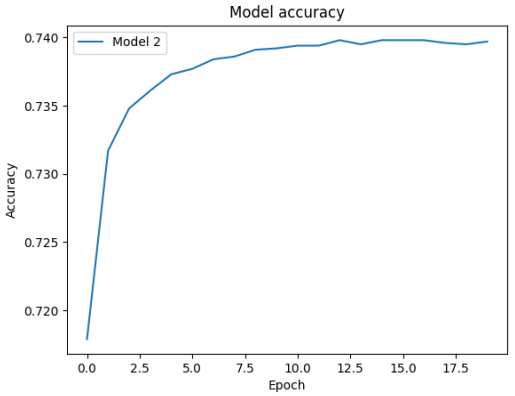

Fig. 8: Accuracy vs Iterations with dataset 5 and 6

150 samples per class. Implementing an iterative Federated Learning approach based on this setup showed promising results. The collaborative learning through iterative updates led to noticeable accuracy improvements in both models, emphasizing the effectiveness of this approach.

D. Approach 4: Correlation Analysis and Its Impact on Accuracy

The final approach explored the correlation between dataset pairs while conducting Federated Learning. Ten datasets, each containing 1,000 samples with 100 samples per class, were used for paired model training. As predicted intuitively and supported by mathematical reasoning, higher dataset correlation inversely affected the increase in accuracy. Higher correlation among datasets led to diminished accuracy improvements due to shared information redundancy.

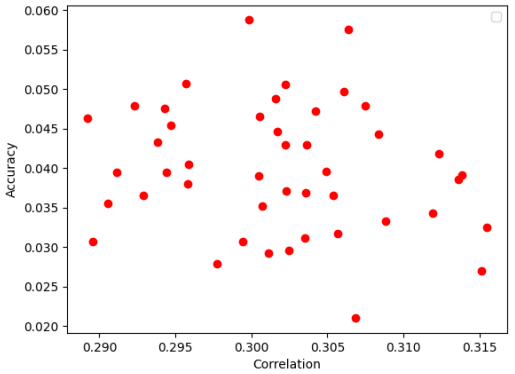

Fig. 9: Correlation vs Accuracy for all pairs

We can see in the plots that as the correlation between the datasets increase we can see a subsequent dip in the difference in the accuracy which is in accordance with what we were expecting from our work.

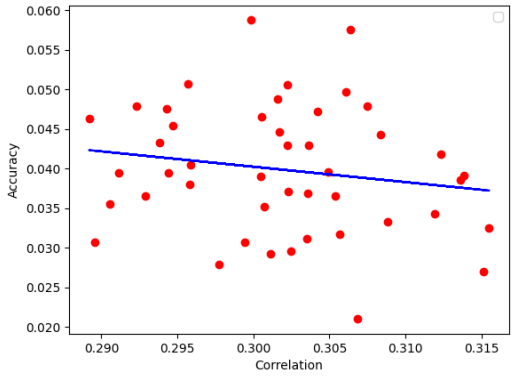

Fig. 10: Trendline for Correlation vs Accuracy

V. Conclusion

We could get some key insights from all these experiments listed below:

- The importance of balanced and diverse datasets in Federated Learning was highlighted, showcasing how complete class representation positively impacted model collaboration
- The success of iterative Federated Learning indicated its potential for enhancing model performance collaboratively, iterating over local updates and global aggregation
- Correlation analysis demonstrated that the degree of dataset similarity directly impacted the effectiveness of collaborative learning. Higher dataset correlation reduced the potential for significant accuracy gains due to shared information redundancy

This comprehensive conclusion encapsulates the insights gained from the different approaches, highlighting the importance of dataset diversity and correlation in Federated Learning's effectiveness while suggesting avenues for future research and improvements.

VI. Future Directions

Future research can focus on:

- Optimizing iterative Federated Learning methodologies for diverse datasets
- Exploring strategies to leverage dataset diversity effectively to enhance collaborative learning outcomes
- Investigating ways to mitigate accuracy limitations in scenarios with highly correlated datasets

References

[1] Yang, K., Jiang, T., Shi, Y. and Ding, Z., 2020. "Federated learning via over-the-air computation". IEEE transactions on wireless communications, 19(3), pp.2022-2035.

[2] Chen Zhang a, Yu Xie b, Hang Bai a, Bin Yu a, Weihong Li a, Yuan Gao c, 2021. "A survey on federated learning". Knowledge-Based Systems, Volume 216, 15 March 2021, 106775

[3] Priyanka Mary Mammen, 2021, "Federated Learning: Opportunities and Challenges", CoRR, abs/2101.05428