A Long Placeholder Title to Represent Writing an Effective Master's Thesis in the Arts Program

A thesis submitted to the
Graduate College
of the University of Cincinnati
in partial fulfillment of the
requirements for the degree of

Master of Science

in the Department of Communication
of the College of Arts and Sciences
by

Bryan J. Cora
B.A., University of Cincinnati
April 2022

Committee Chair: A. B. Cooper, Ph.D.

Abstract

[Your abstract goes here.]

Acknowledgments

[Your acknowledgments go here.]

Contents

List of Figures

List of Tables

1 Introduction

1.1 Background

Federated learning (FL) is a relatively new approach to machine learning introduced by McMahan et al. (2017) [1]. It allows multiple devices, or c̈lients,̈to work together to train a shared model without sharing their private data. This setup is particularly important in fields like healthcare, finance, and mobile applications, where privacy is a major concern. For example, medical data from hospitals or personal data from smartphones can be used for training without leaving the device. This ability to protect privacy has made federated learning a popular and widely discussed topic.

However, while FL offers exciting possibilities, it also comes with its own set of problems. One of the biggest challenges is dealing with differences in the way data is distributed across clients. In many real-world scenarios, the data on each client does not follow the same pattern, which is referred to as non-independent and identically distributed (non-IID) data. These differences can make it harder for the global model to learn effectively, leading to slower progress, lower accuracy, and biased results [2].

1.2 Problem Statement

When it comes to selecting which clients participate in federated learning, most existing methods rely on random or uniform selection strategies. While these methods are simple and easy to use, they often overlook the differences in data across clients. This can make the learning process less efficient and result in a model that does not fully represent the global population [3]. Additionally, the presence of malicious or untrustworthy clients can further degrade model performance. Malicious clients may intentionally provide misleading updates, while others may have unrepresentative data that skews the global model. Addressing these issues requires a more thoughtful approach to client selection.

This thesis focuses on a new way to select clients by using the known global class distribution of the dataset. By considering how the data is distributed overall, it is possible to create a smarter client selection process that addresses these challenges. Despite the potential benefits, this approach has not been widely explored in existing research, leaving a gap that this work aims to fill.

1.3 Overview of Proposed Methodology

This thesis proposes a client selection algorithm that takes advantage of the global class distribution to improve model training in federated learning. The algorithm works in three main steps:

1. **Elimination Based on Kullback-Leibler (KL) Divergence**: In the first step, clients whose local data distributions are significantly different from the global distribution are removed. This step is motivated by the need to exclude clients that may be malicious or have unrepresentative data, as such clients can harm the overall training process. KL divergence, a common method for comparing probability distributions, is used to measure how much each client's data differs from the global pattern [4]. Only clients with distributions similar to the global one are kept for the next step.

2. **Local Outler Factor (LOF) for Anomaly Detection**: The remaining clients are then evaluated using the local outlier factor (LOF) algorithm to identify potential outliers. Clients with high LOF scores are considered outliers and are removed from the selection process. This step helps to further reduce the impact of untrustworthy or unrepresentative clients on the global model [**?**]. These LOF scores are calculated based on the produced model weights of each client. This step is important to remove the malicious clients that provide misleading updates without altering their local data distribution.

3. **K-Means Clustering for Client Selection**: In the second step, the remaining clients are grouped into clusters using the k-means algorithm. Within each cluster, the client whose data is closest to the cluster center is selected. This ensures that the selected clients are both representative of their cluster and diverse overall [5].

By combining these three steps, the algorithm ensures that the selected clients contribute meaningfully to the global model while reducing the negative effects of non-IID data, unrepresentative clients, and potentially malicious participants.

1.4 Thesis Organization

This thesis is organized into several chapters to guide the reader through the research:

- **Chapter 2: Literature Review** provides an overview of related work in federated learning, focusing on client selection methods and strategies for handling non-IID data.

- **Chapter 3: Methodology** explains the proposed client selection algorithm in detail, including the rationale and technical steps involved.
- **Chapter 4: Experiments and Results** presents the experiments conducted to test the algorithm, along with the results and evaluation metrics used to measure its performance.
- **Chapter 5: Discussion** analyzes the results, discussing their implications, strengths, and limitations.
- **Chapter 6: Conclusion** summarizes the main findings of the research and suggests directions for future work.

This structure ensures that each aspect of the research is covered thoroughly, from the initial background to the final conclusions.

2 Literature Review

[Summarize related work and key references.]

3 Methodology

3.1 Overview

This client selection method consists of two filters: **KL-Divergence on label distribution** and **Local Outlier Factor on model weights**. the first layer is designed to eliminate clients of which have data distributions significantly distinct from the understood distribution of the global population. Such detection is designed to detect both outliers and attackers. The second layer is for further outlier detection, this time focusing on model weights. Local outlier factor produces a mask for removing clients whose model weights are vastly different from everyone else. If a client is marked as an outlier it is highly likely that the model was tampered with so it should be removed. After applying both filters, we perfrom **K-Means clustering** on the model weights to create 5 clusters and pick the two most central clients from each cluster.

3.2 Theoretical Background

3.3 Theoretical Background

This section reviews the theoretical concepts essential to our client selection strategy: the Kullback-Leibler (KL) Divergence and the Local Outlier Factor (LOF).

3.3.1 Kullback-Leibler (KL) Divergence

The KL divergence quantifies the difference between two probability distributions. For distributions P and Q, it is defined as:

$$D_{KL}(P \parallel Q) = \sum_i P(i) \log \frac{P(i)}{Q(i)}$$

In this formulation, P represents the probability distribution derived from a client's data, and Q signifies the expected global distribution. Within our methodology, KL divergence is utilized to pinpoint clients whose data distributions deviate significantly from the global norm, an indicator that they may be outliers or even malicious. For more details on this measure, see [**?**] and [**?**].

3.3.2 Local Outlier Factor (LOF)

The Local Outlier Factor (LOF) is an anomaly detection algorithm that determines the degree of isolation of a data point relative to its neighbors [**?**]. LOF computes a score for each data point, where a high score implies that the point is in a region of lower density compared to its surroundings. In our context, LOF is applied to the model weights received from each client. A high LOF score suggests that a client's model update is anomalously different, indicating potential tampering or discrepancies in its data distribution.

Integrating both KL divergence and LOF enables our system to robustly filter out outliers before performing client selection via K-Means clustering, ensuring that only representative and reliable clients contribute to the global model.

3.4 Algorithm Design

3.5 implementation Details

3.6 Experimental Setup and Evaluation Metrics

4 Experiments and Results

[Present your experimental results and analysis.]

5 Discussion

[Discuss the significance and implications of the results.]

6 Conclusion

[Summarize the main findings and propose future work.]

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. *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS)*, pages 1273–1282, 2017.

[2] Peter Kairouz, H Brendan McMahan, et al. Advances and open problems in federated learning. *Foundations and Trends in Machine Learning*, 14(1–2):1–210, 2021.

[3] Yue Zhao, Meng Li, Liangzhen Lai, Naveen Suda, David Civin, and Vikas Chandra. Federated learning with non-iid data. In *arXiv preprint arXiv:1806.00582*, 2018.

[4] John R Hershey and Peder A Olsen. Approximating the kullback-leibler divergence between gaussian mixture models. *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 317–320, 2007.

[5] Stuart P Lloyd. Least squares quantization in pcm. *IEEE Transactions on Information Theory*, 28(2):129–137, 1982.

References

A Appendix Title

[Include supplementary material, datasets, or additional details.]