Federated Learning: Evaluating Popular Frameworks and Developing a Sever to Mimic Real Scenarios

Jose Maria Rico Leal

A Thesis Submitted in Partial Fulfilment of the requirements for the

Degree of

Master of Science in Data Analytics



September 2024 Supervisor: Sam Weiss

# Abstract

Accurate hlhafa lhafkahf lk lahrlkah lkhlkahf alk khalfha lh lkfah lfa lahflakh jfa lahflakh falh lhalfalh lahfalh fa.

**GitHub: Wordcount: 15,000**

[Abstract 2](#_Toc172399681)

[1. Introduction 8](#_Toc172399682)

[1.1. Motivation 8](#_Toc172399683)

[1.2. Research Objectives 9](#_Toc172399684)

[1.3. Thesis Overview 9](#_Toc172399685)

[2. Background 9](#_Toc172399686)

[2.1. What is Federated Learning 9](#_Toc172399687)

[2.2. Federated Learning Classification Based on Client Nature 10](#_Toc172399688)

[2.2.1. Cross-device 10](#_Toc172399689)

[2.2.2. Cross-silo 11](#_Toc172399690)

[2.3. Categorization of Federated Learning 11](#_Toc172399691)

[2.3.1. Horizontal Federated Learning 12](#_Toc172399692)

[2.3.2. Vertical Federated Learning 12](#_Toc172399693)

[2.3.3. Federated Transfer Learning 12](#_Toc172399694)

[2.4. Federated Learning vs Distributed training 12](#_Toc172399695)

[3. Literature Review 12](#_Toc172399696)

[3.1. Theme A Federated Learning Frameworks 12](#_Toc172399697)

[3.1.1. Theme AA 12](#_Toc172399698)

[3.2. Theme B Theme 12](#_Toc172399699)

[3.2.1. Theme BB 12](#_Toc172399700)

[3.3. Theme Theme Theme Cc 13](#_Toc172399701)

[3.4. Theme Theme D 13](#_Toc172399702)

[3.4.1. Theme Theme DD 13](#_Toc172399703)

[3.5. Theme Ed 13](#_Toc172399704)

[3.6. Conclusion 13](#_Toc172399705)

[5. State of the Art 13](#_Toc172399706)

[6. Research Methodology 13](#_Toc172399707)

[6.1. Methodology Frameworks 13](#_Toc172399708)

[6.2. Project Management Framework 13](#_Toc172399709)

[6.3. Business Requirements 14](#_Toc172399710)

[6.4. Data Synthetic and Medical 14](#_Toc172399711)

[6.5. Data Preparation 14](#_Toc172399712)

[6.6. Limitations and Ethical Considerations 14](#_Toc172399713)

[7. Data Analysis 14](#_Toc172399714)

[7.1. Data Collection 14](#_Toc172399715)

[7.2. Initial Data Extraction and Exploration 14](#_Toc172399716)

[7.2.1. Data Elaboration 14](#_Toc172399717)

[7.2.2. Data Elaboration 2 14](#_Toc172399718)

[7.3. Conclusion 14](#_Toc172399719)

[8. Data Preparation 14](#_Toc172399720)

[8.1. Data Cleaning 14](#_Toc172399721)

[8.1.1. AAAAA 14](#_Toc172399722)

[9. Experimentation 14](#_Toc172399723)

[9.1. BBBB Option 15](#_Toc172399724)

[9.2. CCCC Option 15](#_Toc172399725)

[9.3. Aaaaaa Option 15](#_Toc172399726)

[9.4. BBBB Option 15](#_Toc172399727)

[9.4.1. CCCCC Option 15](#_Toc172399728)

[10. Validation of the Experimentation’s Results 15](#_Toc172399729)

[10.1. Validation BBBB 15](#_Toc172399730)

[11. Research Conclusion: Summary, Limitations, and Recommendations 15](#_Toc172399731)

[References: 15](#_Toc172399732)

**Abbreviations**

|  |  |
| --- | --- |
| FL | Example of Abbreviation |
| AEA | Another Example Abbreviation |

**Figures**

Figure 1.1. Illustration of a single FL communication round in FL for mobile keyboard prediction.

Figure 2.2.1. Cross-device scenario.

Figure 2.2.2. Cross-silo scenario.

Figure 2.3.1. Horizontal Federated Learning.

Figure 2.3.2. Vertical Federated Learning.

Figure 2.3.3. Federated Transfer Learning.

**Tables**

Table 1.1. XXXXXX.

Table 5.1. XXXXXX.

Table 5.2. XXXXXX.

.

# Introduction

## Motivation

Within the domain of Data Analytics (DA), there is an important field known as Machine Learning (ML), which is embedded in everyday people's lives. A significant topic within this field is Federated Learning (FL). FL occurs when different devices collaborate to build a common model without exchanging their data; instead, the data remains on the devices, and only model updates are sent to a central server where aggregation occurs.

A good example for FL in everyday people’s lives is when phone users are typing a message, and the keyboard predicts words to complete the sentence, a model developed by Google engineers (Hard *et al.*, 2019).

A diagram of a phone system

Description automatically generated  
Figure 1.1. Illustration of a single FL communication round in FL for mobile keyboard prediction.

A different example where FL is helping society move forward is in the healthcare sector. Patients are using wearable devices to track their movements and help doctors monitor their health conditions (Arikumar *et al.*, 2022).

FL is growing rapidly and is helping the technological and medical sectors build robust machine learning models. This significant development motivates the focus of this thesis.

## Research Objectives

The primary purpose of this project is to experiment with FL frameworks to evaluate their implementability and develop a functional FL server. Therefore, the research objectives are:

* **To evaluate the implementability of existing FL frameworks.** This section experiments with popular FL frameworks, such as *TensorFlow Federated* (TFF)*, Flower, EasyFL, IBM Federated* (IBMF)and *FLGo*, by examining their architecture and their applicability to real-world FL scenarios. This evaluation serves as the starting point for the primary research.
* **To develop a FL server**. A practical example of a web Flask FL server will be built, featuring two scenarios: technological and pharmaceutical. Each scenario will run separately, connecting five clients. Each scenario will have its own data, synthetic data for the technological scenario and images for the pharmaceutical scenario. These configurations will be trained, validated, and tested using Neural Networks (NN) that will classify binary outputs. This experiment aims to bridge the gap between popular FL frameworks and real-world FL applications.
* **To compare FL frameworks and the FL server.** This includes discussing the pros and cons each method brings to key industries such as the technological and pharmaceutical sectors. The comparison will focus on the following aspects ease of implementation, scalability, data privacy, and model performance.

## Thesis Overview

# Background

## What is Federated Learning

This concept was introduced in 2016 by Google engineers (McMahan et al., 2016). FL is a shared model that is trained across multiple devices, often referred to as clients. Each client trains its own local model and sends the updates to a central server, where the updates are aggregated to improve the global model. It is important to note that clients do not exchange their data; the data remains private for each client. This principle drove the design of FL, following the concepts of *focused collection* or *data minimization*, which were introduced by the White House in 2013. The intent is to prevent personal data from being sent over the network and potentially being stolen or manipulated by malicious third parties.

## Federated Learning Classification Based on Client Nature

Depending on the nature of client FL can be classified in two types cross-device and cross-silo (Yang *et al.*, 2021).

### Cross-device

The clients for cross-device can be mobile devices, edge devices, Internet of Things (IoT) devices, smartphones, tablets, wearables, etc. Figure 2.2.1. illustrates this scenario.  
The characteristics are, the high number of participants it can be thousands to millions of devices, it may have limited processing power and battery life, datasets tend to be small and network bandwidth may be limited. Devices may also connect and disconnect intermittently.

A diagram of a computer network

Description automatically generated  
Figure 2.2.1. Cross-device scenario.

### Cross-silo

In this scenario, clients can be organizations or institutions such as hospitals, banks, and companies using large data centers. Figure 2.2.2 illustrates a cross-silo ecosystem. Some differences compared to the cross-device scenario include, clients are no longer small devices, there are fewer clients, clients have high computational power and large datasets, and the network is reliable with stable communication.

A diagram of a server

Description automatically generated  
Figure 2.2.2. Cross-silo scenario.

## Categorization of Federated Learning

FL can be categorized according to the distribution of the data held by the clients participating in the modelling. These categories help to understand the different methodologies and use cases for FL (Yang *et al.*, 2019).

### Horizontal Federated Learning

Horizontal Federated Learning (HFL) or sample-based FL, occurs when different clients have datasets that share the same feature space but differ in the samples they hold (see Figure 2.3.1). A practical example of HFL is when two hospitals in different regions each have patient records with the same features (e.g., age, height, weight, diagnosis) but for different patients. These hospitals can collaborate to train a model to predict disease outcomes without sharing patient data.

A diagram of a dataset

Description automatically generated with medium confidence  
Figure 2.3.1. Horizontal Federated Learning.

### Vertical Federated Learning

Vertical Federated Learning (VFL), or feature-based FL, occurs when different clients have datasets that share the same sample IDs but differ in the feature space. An example of this is a bank and an e-commerce company that have data on the same set of customers. The bank has financial information such as credit scores and loan histories, while the e-commerce company has purchase behaviours and browsing records. By combining their data, they can build a model to predict customer credit without sharing raw data.

A diagram of a dataset

Description automatically generated with medium confidence  
Figure 2.3.2. Vertical Federated Learning.

### Federated Transfer Learning

Federated Transfer Learning (FTL) is applicable when the datasets of different clients differ in both samples and features, and the overlap between both is minimal. To clarify, a good example is a European pharmaceutical company and a healthcare research institution in China collaborating using FTL. The pharmaceutical company has drug efficacy data, while the healthcare institution has patient health records. Even though they have different types of data, it is possible to train a global model to predict drug effectiveness on certain health conditions.

A diagram of dataset and dataset

Description automatically generated  
Figure 2.3.3. Federated Transfer Learning.

## Federated Learning vs Distributed training

# Literature Review

## Theme A Federated Learning Frameworks

### Theme AA

## Theme B Theme

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

### Theme BB

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

## Theme Theme Theme Cc

## Theme Theme D

### Theme Theme DD

## Theme Ed

## Conclusion

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Identification of gaps

# State of the Art

# Research Methodology

## Methodology Frameworks

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

## Project Management Framework

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

## Business Requirements

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

## Data Synthetic and Medical

## Data Preparation

## Limitations and Ethical Considerations

# Data Analysis

## Data Collection

## Initial Data Extraction and Exploration

### Data Elaboration

### Data Elaboration 2

## Conclusion

# Data Preparation

## Data Cleaning

### AAAAA

# Experimentation

## BBBB Option

## CCCC Option

## Aaaaaa Option

## BBBB Option

### CCCCC Option

# Validation of the Experimentation’s Results

## Validation BBBB

# Research Conclusion: Summary, Limitations, and Recommendations

# References:

Arikumar, K.S., Prathiba, S.B., Alazab, M., Gadekallu, T.R., Pandya, S., Khan, J.M. and Moorthy, R.S. (2022) ‘FL-PMI: Federated Learning-Based Person Movement Identification through Wearable Devices in Smart Healthcare Systems’, *Sensors*, 22(4), p. 1377. Available at: https://doi.org/10.3390/s22041377.

Hard, A., Rao, K., Mathews, R., Ramaswamy, S., Beaufays, F., Augenstein, S., Eichner, H., Kiddon, C. and Ramage, D. (2019) ‘Federated Learning for Mobile Keyboard Prediction’. arXiv. Available at: http://arxiv.org/abs/1811.03604 (Accessed: 18 July 2024).

Yang, Q., Liu, Y., Chen, T. and Tong, Y. (2019) ‘Federated Machine Learning: Concept and Applications’. arXiv. Available at: http://arxiv.org/abs/1902.04885 (Accessed: 20 July 2024).

Yang, X., Feng, Y., Fang, W., Shao, J., Tang, X., Xia, S.-T. and Lu, R. (2021) ‘An Accuracy-Lossless Perturbation Method for Defending Privacy Attacks in Federated Learning’. arXiv. Available at: http://arxiv.org/abs/2002.09843 (Accessed: 20 July 2024).