

1 July 2022

Enhanced Framework to Support Trustworthy Balanced Federated Learning

Abstract

1. What did you do?

Development of an application to analyse data coming from a federated environment enhancing balancing of data without compromising privacy using zero knowledge proof (ZKP). Unlike classic approaches to federated learning, the model proposed is able to store encrypted data coming from the clients, i.e. workers, to analyse the proportions of the population and use these data to evaluate the fairness of the predictions and mitigate the effect of unbalanced data.

2. Why did you do that (why is it needed based on the SoA)?

Federated learning environments are subject to fairness issues due to the impossibility of measuring data balance.

3. What happened when you did it (highlights of your results)?

We trained a predictive model and measured evaluation metrics (F1) using balanced and unbalanced datasets in a non-federated environment. We noticed a greater deviation of F1 score within subgroups for unbalanced datasets, hence more unfair predictions (but often highest scores) as expected. We used the developed model to train balanced i.e. more fair predictive models.

4. What do the results mean in theory & .5 in practice?

Unbalanced dataset leads to highest F1 score (overall) but also highest variance in subgroups: hence less reliable results for under-represented groups. Using ZKP federate models can be trained, maintaining equal proportions among subgroups and leading to fair results.

6. What is unique to this paper? The most important question?

As far as we researched there is no other data analytics tool that implements the functionalities proposed using the same approach. Other frameworks for balancing federated data make use of mediators (Duan et al., 2019) or other methodologies not involving ZKP.

7. What is left to do (leave)

It is hard to answer this question now... later, with more experience, we could answer this.

Introduction

The general problem area

Federated learning is... the principles of a fed-learn framework are... the advantages are...

The specific problem you address

In a federated environment, the server does not retain any data from the workers, it is thus not possible to evaluate eventual bias introduced by unbalanced sources of data. The framework proposed aims to enhance a federated server implementing the following features:

- A zero knowledge proof (ZKP) protocol is used to be sure that federated data are compliant with the requirements.
- (WIP) workers get a generated random code from an external service to be used in encryption of features, this code must be shared among all workers.
- The server accepts updates from workers only if the required proportions among subgroups is satisfied (can be uniform, normal, etc...).
- The server can retain workers IDs in a data structure to reach them later in case they would not compromise the balancing of the data collected.
- The server can collect encrypted metadata about the proportions of the population measured in various features (ethnicity, gender, age, etc...)

Your research question

- To what extent can we mitigate federated data bias according to EU guidelines for data ethics and trustworthy AI?
- To what extent can zero knowledge proof metadata about the proportions of population clusters generated in a federated learning environment can be used to enhance trustworthiness in AI?

Your technical approach

Demonstrating AI unfairness if dataset is unbalanced

We implemented a predictive model based on an ANN.

We used the UTK Dataset to train the model. We measured the F1 score of the model in a non-federated environment.

We calculated F1 scores for subsets (representing subgroups e.g. only Asians, only White, only Indians, etc...) of the test dataset.

We noticed that training the model with balanced datasets leads to smaller deviance of F1 scores with respect to the general F1 score.

We also noticed that using an unbalanced dataset leads to higher F1 scores (together with higher deviation i.e. unequal treatment among subgroups).

Implementing a federated learning environment and demonstrating that the predictive model used behaves in the same way (under the same conditions) in federated and non-federated frameworks.

We designed a federated framework in which we defined a server and n workers. We implemented some communication protocols to simulate the behaviour of the workers in an actual federated environment. We trained two instances of the same predictive model in a federated and in a non-federated environment. We compared the status of the model in terms of weights and we determined that the two models behave the same.

This way we can use classic evaluation metrics (that make use of data) to measure the performance of the model considering that the federated version of it will behave the same.

implementing ZKP and self balancing features

We extended the functionalities of the server and clients to include the requirements in the section "the specific problem you address".

The contribution of this paper are

- The tool developed will address the problem of unbalanced federated learning without introducing any sort of mediator between server and worker.
- The tool developed can be used to test predictive models before porting them in a federated environment
- The presented tool can be used to keep track of the proportions of the data using different features and can be easily customised to serve different purposes in terms of data analytics in federated frameworks.

Related Works

The following table summarises the related works researched.

ID	Bib	Description	Pros	Cons
ASTRAEA	Duan et al., 2019	Framework that uses mediators to reschedule training process and make the distribution of the data close to uniform. They aggregate data coming from multiple clients and can have a wider view on the data patterns.	Very efficient. If mediators are instantiated server-side, the communication overhead is reduced and this leads to optimal results.	Using mediators risks negating the benefits introduced by a federated framework and may expose latent backdoor to attacks and lead to privacy leakage.
ADRCLIM	Wang et al., 2020	This approach monitors the composition of training data at each training round in a passive way. This approach defines two types of class imbalance in FL: local imbalance and global imbalance, and addresses class imbalance based on a new loss function (Ratio Loss). It is a method that analyse the weights updates to understand if the data is imbalanced.	Secure method, overcomes privacy issues and does not need any proxy/mediator.	The analysis of gradient updates can be done only under certain strict conditions (only a few classes of neural networks). Moreover, this approach does not prevent the model to be imbalanced a priori. It is not a deterministic method.
AGNAPPR	Shen et al., 2022	this approach monitors the composition of training data at	Secure method, overcomes privacy issues and does not need any	As Above

		each training round using primal and dual updates. It is an analytical method that implements ratio-loss and focal-loss to prevent the model to be imbalanced.	proxy/mediator. It is an advancement with respect to ADRCLIM.	
FLREDIM	Yang et al., 2021	this approach monitors the composition of training data at each training round using primal and dual updates. It is an analytical method that implements ratio-loss and focal-loss to prevent the model to be imbalanced.	Secure method, overcome privacy issues and does not need any proxy/mediator. It is an advancement with respect to ADRCLIM.	As above
ONLFEDL	Giorgas and Varlamis, 2020	this approach addresses online federated learning operating central re-training to mitigate the effects of imbalance data.	Secure method, overcome privacy issues and does not need any proxy/mediator. Useful in online learning.	Disadvantages of re-training.

Use case and requirements

Build a FL framework that is able to:

- Distribute data among clients i.e. workers.
- Define a protocol to set up clients participating in federated learning (distributing an encryption key).
- Initialise and set up a server to handle federated data.
- Fit a distributed model following the principles of FL.
- Load metadata regarding the distribution of the data coming from a federated environment into the server with Zero Knowledge.
- Handle imbalance model updates using queue data structures.

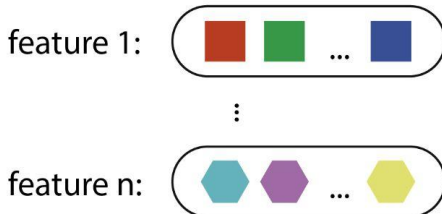
Design

The framework has 3 main server-side tools:


1. Federated server: responsible for federated learning, can make predictions once trained. retains the following data:
 - a. number of updates.
 - b. structure of the possible classes clients can belong to (together with a ZK proof used to verify clients).
 - c. for each class (encrypted) a distribution of the data used to train the model.
 - d. the updated learning model.


2. Server initializer: it generates a number of clients representing each individual class label that the server must record. It is used to make the server able to verify if clients are able to prove if they belong to a certain class label or not.
3. Client initializer: This service is used to provide clients with a code that will be used for labels encryption

FL Server knowledge



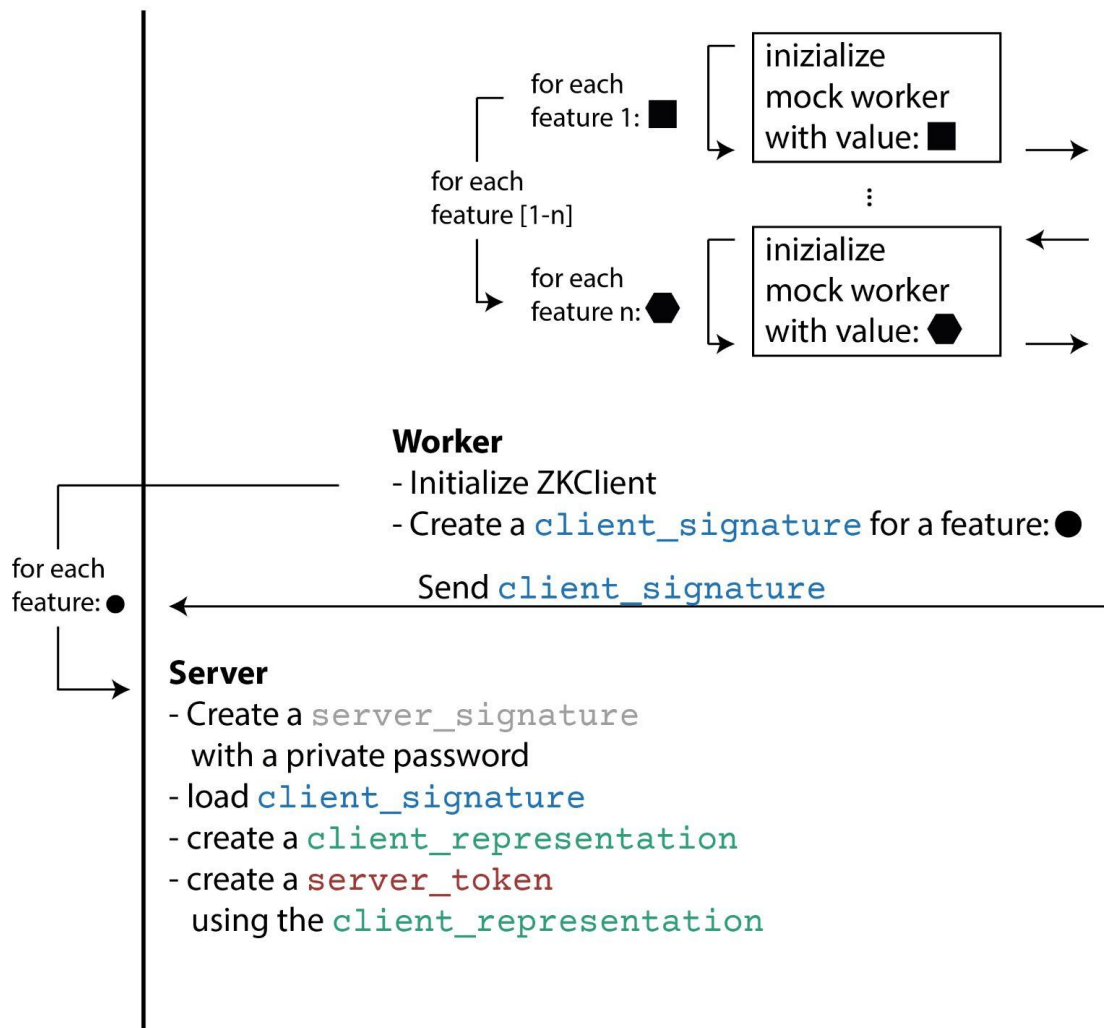
Legend

 feature 1 possible labels

 feature n possible labels

FL Server

Server Initializer



References

- Duan, M., Liu, D., Chen, X., Tan, Y., Ren, J., Qiao, L., & Liang, L. (2019). Astraea: Self-balancing federated learning for improving classification accuracy of mobile deep learning applications. 2019 IEEE 37th International Conference on Computer Design (ICCD). <https://doi.org/10.1109/iccd46524.2019.00038>
- Giorgas, K., & Varlamis, I. (2020). Online federated learning with imbalanced class distribution. 24th Pan-Hellenic Conference on Informatics, 91–95. <https://doi.org/10.1145/3437120.3437282>
- Shen, Z., Cervino, J., Hassani, H., & Ribeiro, A. (2022). An agnostic approach to federated learning with class imbalance. International Conference on Learning Representations. <https://openreview.net/forum?id=Xo0IbDt975>
- Wang, L., Xu, S., Wang, X., & Zhu, Q. (2020). Addressing class imbalance in federated learning. <https://doi.org/10.48550/ARXIV.2008.06217>
- Yang, M., Wang, X., Zhu, H., Wang, H., & Qian, H. (2021). Federated learning with class imbalance reduction. 2021 29th European Signal Processing Conference (EUSIPCO), 2174–2178. <https://doi.org/10.23919/EUSIPCO54536.2021.9616052>