Enhanced Data Catalog to Support Trustworthy Federated Learning

Next Steps

Development of the experiments

- **Demonstrate Federated Learning** to have a starting point for comparison.
- **Showing the results** in case of unbalanced i.e. under-representative datasets.
- **Using existing metrics** it is possible to calculate the fairness of the predictions (this requires direct access to data, hence this practice is not suitable for Federated Learning).

- **Implementing Zero Knowledge Proof** (non-interactive) to store metadata about groups proportions in the dataset.
- **Integrate ZKP into Federated Learning** to be able to produce metadata about the fairness of a dataset with no knowledge of it.
- **Compare** this newly developed method with the benchmark non-federated results.

- **Deploy** of the tool into the CKAN platform.

Demonstrate Federated Learning

- **Fit a FedLearn model** with data coming from a public collection. Keep in mind that the dataset is a single table of persons structured as follows (only relevant fields showed):
  - **[age]** is an integer from 0 to 116, indicating the age
  - **[gender]** is either 0 (male) or 1 (female)
  - **[race]** is an integer from 0 to 4, denoting White, Black, Asian, Indian, and Others.
  - **[img_pixels]** bitmap of B&W picture of the person

- **Show the results** that can be obtained in case of a well balanced dataset.

HELP! How can we design experiments? Which features shall we consider? Train - Test split?

Manipulate the Dataset to Simulate Unfairness

- By **Manipulating the Dataset** it is possible to create under-represented groups.
- Fit a FedLearn Model and **measure the lack of fairness** (assuming to have actual access to the whole dataset).
- Keeping in mind that this measurements could not be taken in an actual federated environment, can we **find a significant difference** between the predictions generated by the “balanced” model and the “unbalanced” one?

Implementing Zero Knowledge Proof

- **Is it possible to store metadata about the population without accessing their actual features?**
- We can do this by "**encoding**" certain features (nominal only: Gender, Ethnicity) with a simple **hash** function (the server will never know the encoded value).
- For **binary features** (Gender in our case), it is possible to implement **Zero Knowledge Proof** (**iterative**: easy but computationally expensive, **non-iterative**: COMPLEX).
- For **interval** features (Age) it is possible to implement an **Efficient Range Proof** to estimate accurately the age of a person without knowing it.

- Is it possible to create a ZKP representation of the population?

A synergy between FedLearn and ZKP

- Developing of a method to **collect data from a federated environment** but also recording metadata about the **population proportions using ZKP**.
- Perform the **experiments and measure the fairness the predictions**, compared to the previous experiments.
- Can we significantly **mitigate the effect of unbalanced dataset** by collecting ZKP metadata?

Having it as a CKAN tool

- Development of a CKAN plugin implementing ZKP FedLearn.
- Executing the experiments within the CKAN platform.
- Conclusion of the project.