**COMP6130 Data Mining** **Final Project Report**

1. **Introduction**

Our goal is to design a graphical interface. Users could input or select parameters through the interface, view the running progress and results of Papers.

1. **User interface design**

The principle of the design is friendly and simple. The interface contain welcome page and two tabs: welcome and algorithm. Welcome tab will help user to find an algorithm to run according their interesting. The algorithm tab is mainly used to display the process and results of the operation of the method.

The main idea to implement the interface could be divided into three parts: one is used to help user to choose an algorithm. One is designed to show the process and result of the algorithm, and one is supposed to draw the picture according to the requirements of the papers.

**Coding language:** Python Tkinter.

**Other related：**subprocess, PIL, timeit, datetime and warnings

1. **User interface application**

3.1 Paper for numerical experiment: Byzantine-Resilient Federated Machine Learning via Over-the-Air Computation

3.1.1 Paper introduction:

The paper proposes a novel communication efficient robust model aggregation scheme via over-the-air computation (AirComp). This is achieved by applying the Weiszfeld algorithm to obtain the smoothed geometric median aggregation against Byzantine attack.

By setting the number of Byzantine devices, the method of attack and other methods, comparative experiments are designed to prove the effectiveness and correctness of the algorithm.



Picture 3.1.1 the welcome page,click will fade away and go to the topic page



Picture 3.1.2 choose the topic



Picture 3.1.3 choose the paper

3.1.2 Dataset:

EMNIST

MNIST

3.1.3 Experiment setting:

Each method contains three confrontations

no attack

classflip

dataflip

Experimental parameters

[file name] (Dataset name): mnist, emnist

[attack type]: no attack, classflip, dataflip

[method]: agg gm2, var 1e-2

[honestSize]: int num

[byzantineSize]: int num

[round]: int num

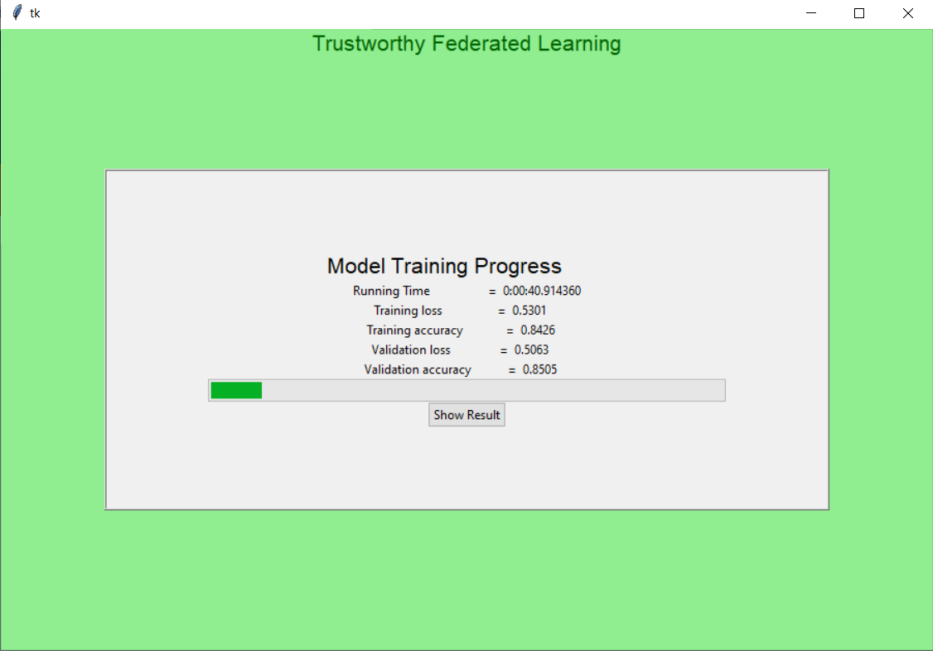
[interval]: int num

[gamma]: 2, 0.01

Graphical user interface

Description automatically generated with medium confidence

Picture 3.1.4 : the interface to input the parameters. Users can select parameters through the drop-down box on the interface



Picture 3.1.5: show the calculation result while processing the data

3.1.4 Result:

We could get the conclusion from the chart, it is almost the same as the chart in the paper, which verifies the correctness of the paper.

Chart

Description automatically generated

Picture 3.1.6 : the picture comes from the interface

Graphical user interface, chart

Description automatically generated

Picture 3.1.7 : the picture comes from the paper

3.2 paper for graphical experiment

3.2.1 Paper introduction:

The paper focus on the possible avenues of attack, analyzed the ability to reconstruct the input to any fully connected layer analytically, propose a general optimization-based attack, and discuss its effectiveness for different types of architectures and network parameters

3.2.2 Dataset:

CIFAR10

3.2.3 Experiment setting:

System requirement:

pytorch=1.4.0

torchvision=0.5.0

Experimental parameters:

Model : ResNet20-4

Cost function : sim

Indices : def

Restart : 1

Targer\_id :-1

Choose\_image : dog

Graphical user interface

Description automatically generated

Picture 3.2.1 : the interface to input the parameters. Users can select parameters through the drop-down box on the interface

A picture containing text, mammal

Description automatically generated

Picture3.2.2 : if the user click the show\_image button, they will see the input picture

Timeline

Description automatically generated with medium confidence

Picture3.2.3 : show the calculation result while processing the data

3.1.5 Result:

Graphical user interface, chart

Description automatically generated

Picture3.2.4 : the result picture

1. Conclusion

We have implemented a numerical and a graphical paper, and left places to insert other papers in the code. In the future, we will add all papers to the GUI program. And59 some detail can be improved such as the input method of parameters, some can be changed from selecting to be filled. Adjust the font size, interface color, etc. to make the style of the interactive interface unified.