APPFLX: PROVIDING PRIVACY-PRESERVING CROSS-SILO FEDERATED LEARNING AS A SERVICE

APPFL

globus

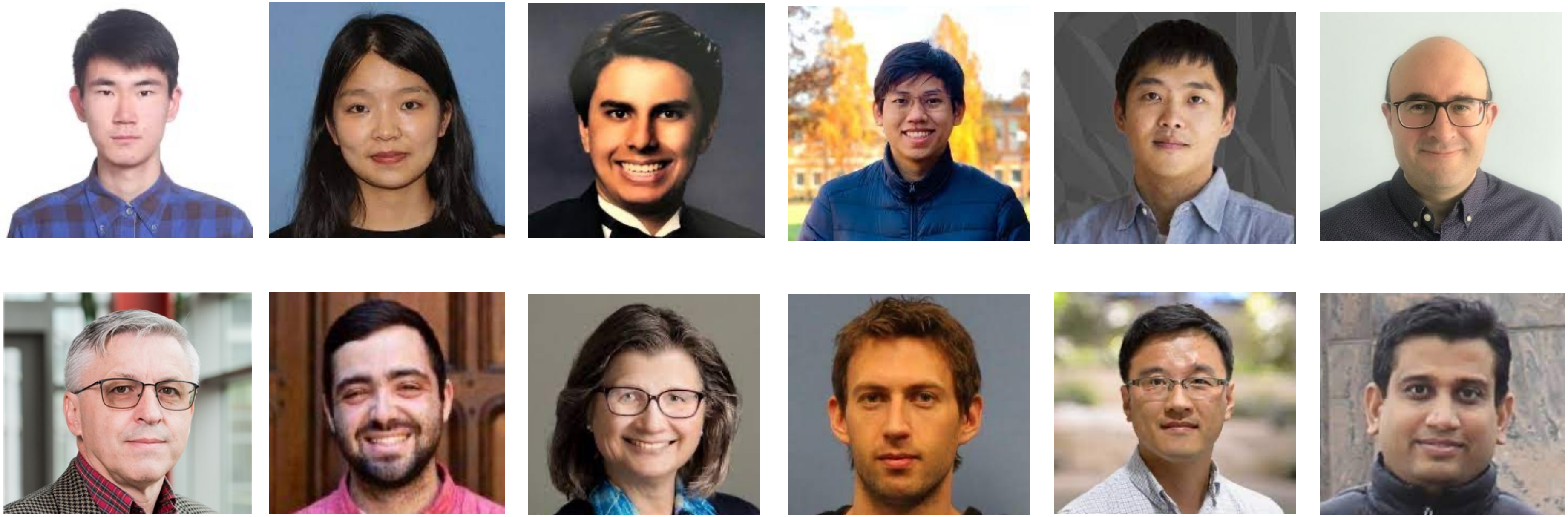
ZILINGHAN LI

Research Associate
Data Science and Learning Division, Argonne National Laboratory
Department of Computer Science, University of Illinois at Urbana-Champaign
zilinghan.li@anl.gov, zl52@Illinois.edu

U.S. DEPARTMENT OF ENERGY
Argonne National Laboratory is a
U.S. Department of Energy laboratory
managed by UChicago Argonne, LLC.

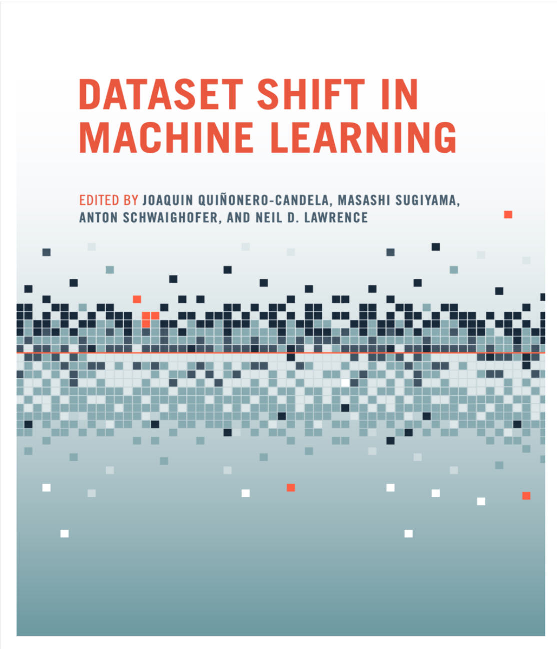
ParslFest 2023

TEAM



Zilinghan Li, Shilan He, Pranshu Chaturvedi, Trung-Hieu Hoang, Minseok Ryu, E. A. Huerta,
Volodymyr Kindratenko, Jordan Fuhrman, Maryellen Giger, Ryan Chard, Kibaek Kim, Ravi Madduri

MOTIVATION FOR FEDERATED LEARNING AS A SERVICE



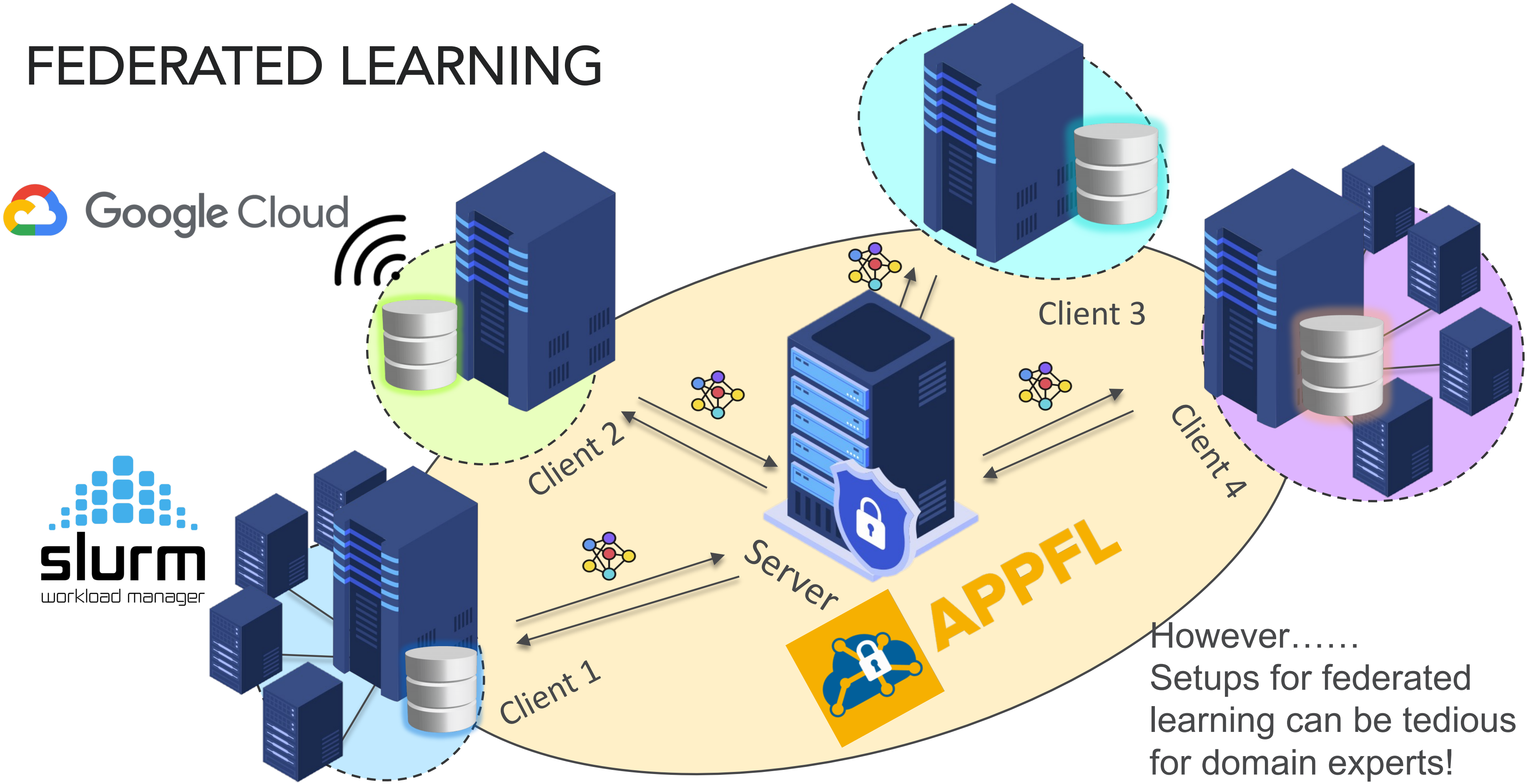
DATASET SHIFT IN MACHINE LEARNING

EDITED BY JOAQUIN QUIÑONERO-CANDELA, MASASHI SUGIYAMA, ANTON SCHWAIGHOFER, AND NEIL D. LAWRENCE

Data Shift in Machine Learning

Privacy Concerns in Biomedical Data

FEDERATED LEARNING

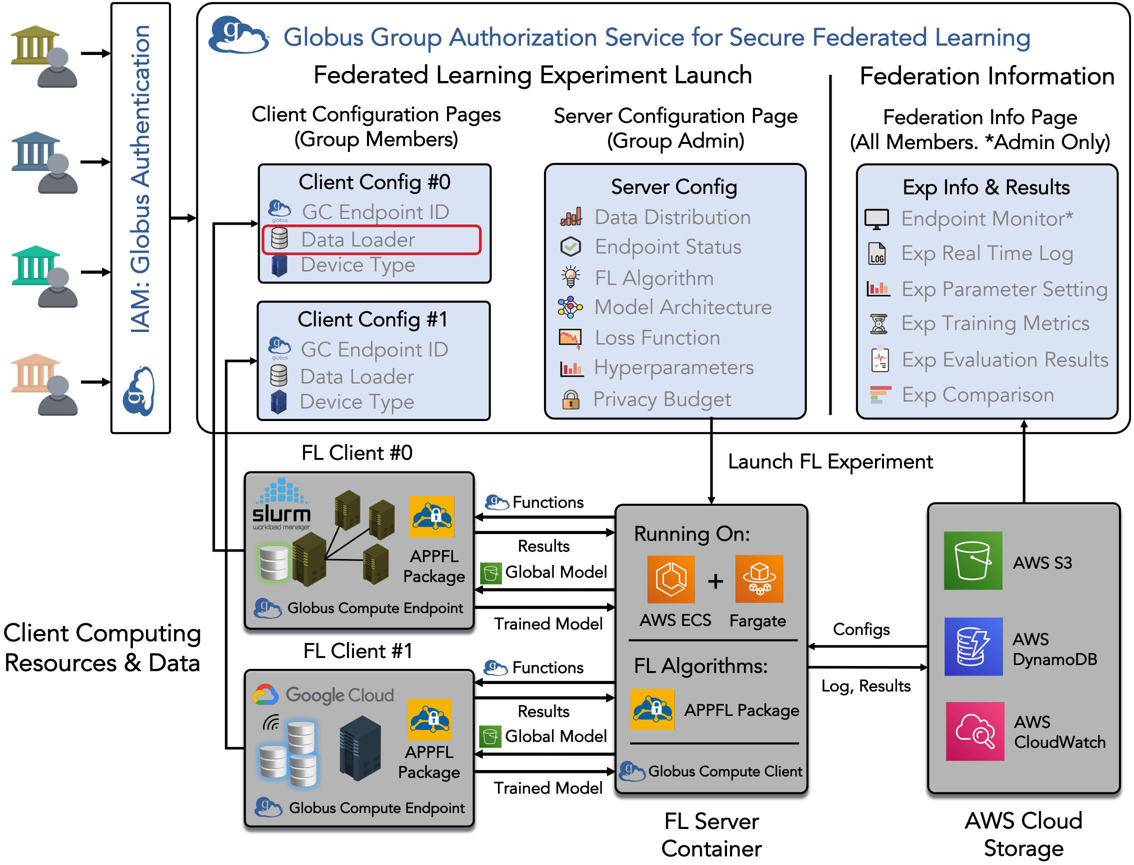


However……
Setups for federated learning can be tedious for domain experts!

APPFLX WORKFLOW

- Login via Globus using institutional credentials
- Create a federation (FL group)
- Invite collaborators using institutional credentials
- Collaborators setup the globus compute endpoint
- Collaborators provide endpoint id and load data loader
- Configure and launch different FL experiments
- Monitor training in real-time, and obtain comprehensive reports
- Reason using data distribution visualization

Minimal code!



IAM: Globus Authentication

Globus Group Authorization Service for Secure Federated Learning

Federated Learning Experiment Launch

Client Configuration Pages (Group Members)

Client Config #0
- GC Endpoint ID
- Data Loader
- Device Type

Client Config #1
- GC Endpoint ID
- Data Loader
- Device Type

Server Configuration Page (Group Admin)

Server Config
- Data Distribution
- Endpoint Status
- FL Algorithm
- Model Architecture
- Loss Function
- Hyperparameters
- Privacy Budget

Federation Information

Federation Info Page (All Members. *Admin Only)

Exp Info & Results
- Endpoint Monitor*
- Exp Real Time Log
- Exp Parameter Setting
- Exp Training Metrics
- Exp Evaluation Results
- Exp Comparison

Launch FL Experiment

Client Computing Resources & Data

FL Client #0: slurm workload manager; APPFL Package; Globus Compute Endpoint

FL Client #1: Google Cloud; APPFL Package; Globus Compute Endpoint

Functions, Results, Global Model, Trained Model

FL Server Container: Running On: AWS ECS + Fargate; FL Algorithms: APPFL Package; Globus Compute Client

Configs; Log, Results

AWS Cloud Storage: AWS S3; AWS DynamoDB; AWS CloudWatch

GO BEYOND AN FL FRAMEWORK: WHY "AS-A-SERVICE"?

Comparison between a PPFL framework and APPFLx

Framework

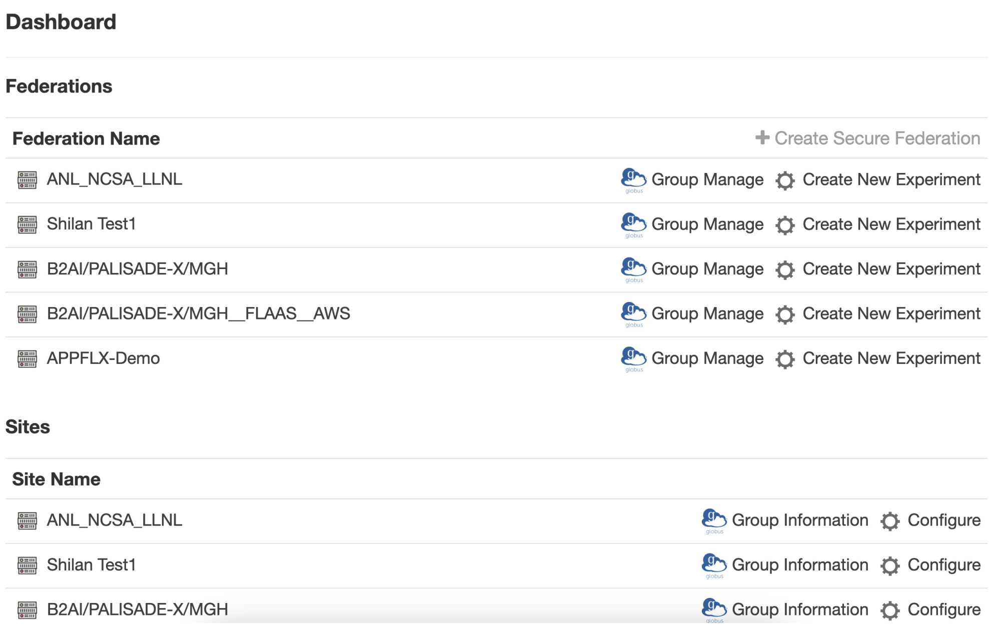
- **Target users:** Developers for developing and simulating FL algorithms.
- **Authentication:** No client auth for most frameworks.
- **Launch Server:** Requires expertise to start federated learning experiments.
- **Results:** Server needs to manually share the whole results, which may require further post-process.
- **Connection:** Developed algorithms via the framework can be easily adopted to the service.

Service (APPFLx)

- **Target users:** Domain experts for applying FL.
- **Authentication:** Clients use institutional credentials via Globus Auth to setup a trust relationship
- **Launch Server:** Admin uses web UI to easily launch the FL experiment with different hyperparameters.
- **Results:** Comprehensive logs, reports, and visualizations shared among all clients on web UI.
- **Connection:** The service is built on the top of the APPFL framework
- **Misc:** Integrated with HuggingFace, GitHub for pre-trained models and pre-processing.

APPFLX CAPABILITIES

Creating Secure Federations



Dashboard

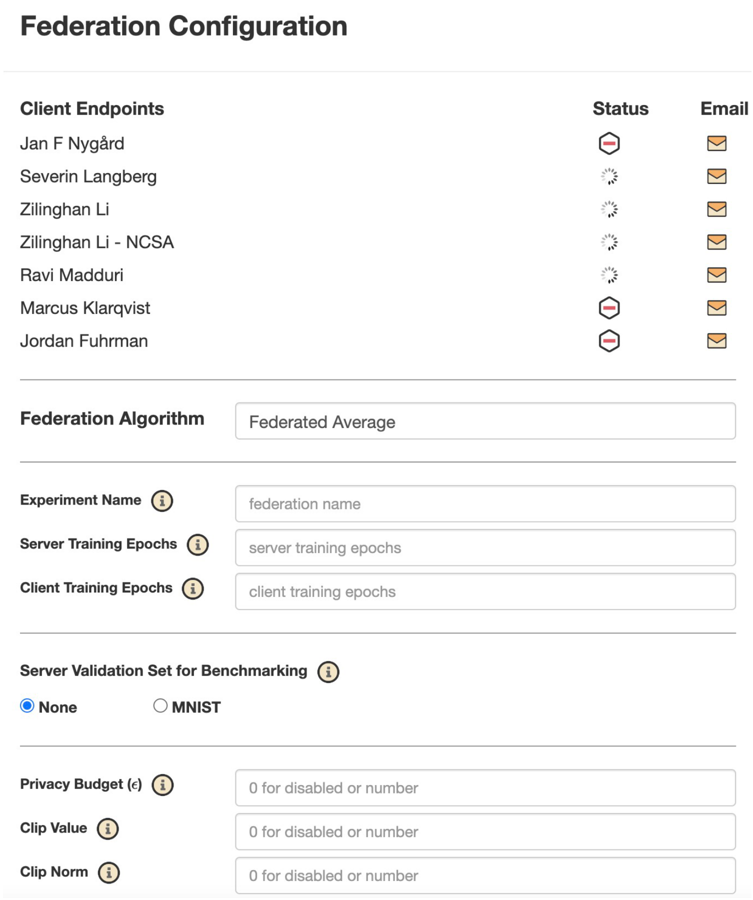
Federations

Federation Name	+ Create Secure Federation
ANL_NCSA_LLNL	Group Manage · Create New Experiment
Shilan Test1	Group Manage · Create New Experiment
B2AI/PALISADE-X/MGH	Group Manage · Create New Experiment
B2AI/PALISADE-X/MGH__FLAAS__AWS	Group Manage · Create New Experiment
APPFLX-Demo	Group Manage · Create New Experiment

Sites

Site Name	
ANL_NCSA_LLNL	Group Information · Configure
Shilan Test1	Group Information · Configure
B2AI/PALISADE-X/MGH	Group Information · Configure

https://appflx.link/



Federation Configuration

Client Endpoints	Status	Email
Jan F Nygård	⊖	✉
Severin Langberg	⟳	✉
Zilinghan Li	⟳	✉
Zilinghan Li - NCSA	⟳	✉
Ravi Madduri	⟳	✉
Marcus Klarqvist	⊖	✉
Jordan Fuhrman	⊖	✉

Federation Algorithm: Federated Average

Experiment Name ⓘ: federation name

Server Training Epochs ⓘ: server training epochs

Client Training Epochs ⓘ: client training epochs

Server Validation Set for Benchmarking ⓘ

● None ○ MNIST

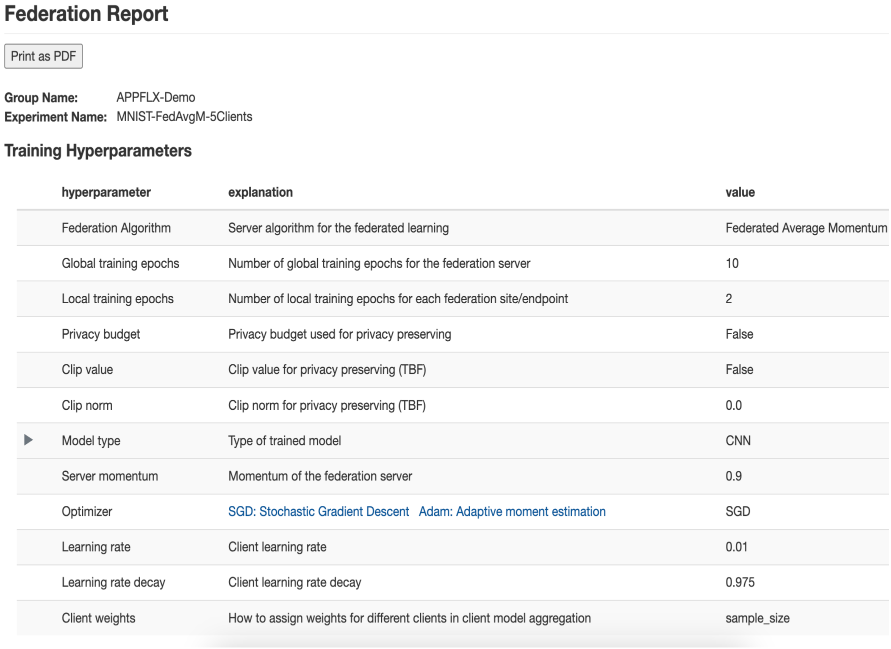
Privacy Budget (ϵ) ⓘ: 0 for disabled or number

Clip Value ⓘ: 0 for disabled or number

Clip Norm ⓘ: 0 for disabled or number

APPFLX CAPABILITIES

Comprehensive Experiment Reports



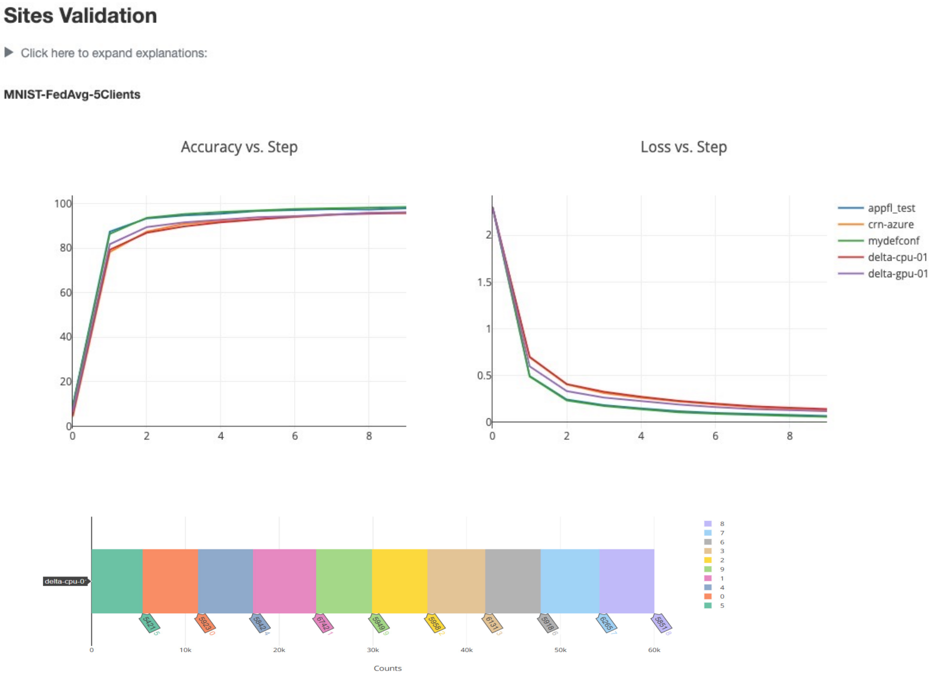
Federation Report

Print as PDF

Group Name: APPFLX-Demo
Experiment Name: MNIST-FedAvgM-5Clients

Training Hyperparameters

	hyperparameter	explanation	value
	Federation Algorithm	Server algorithm for the federated learning	Federated Average Momentum
	Global training epochs	Number of global training epochs for the federation server	10
	Local training epochs	Number of local training epochs for each federation site/endpoint	2
	Privacy budget	Privacy budget used for privacy preserving	False
	Clip value	Clip value for privacy preserving (TBF)	False
	Clip norm	Clip norm for privacy preserving (TBF)	0.0
▶	Model type	Type of trained model	CNN
	Server momentum	Momentum of the federation server	0.9
	Optimizer	SGD: Stochastic Gradient Descent Adam: Adaptive moment estimation	SGD
	Learning rate	Client learning rate	0.01
	Learning rate decay	Client learning rate decay	0.975
	Client weights	How to assign weights for different clients in client model aggregation	sample_size



Sites Validation

▶ Click here to expand explanations:

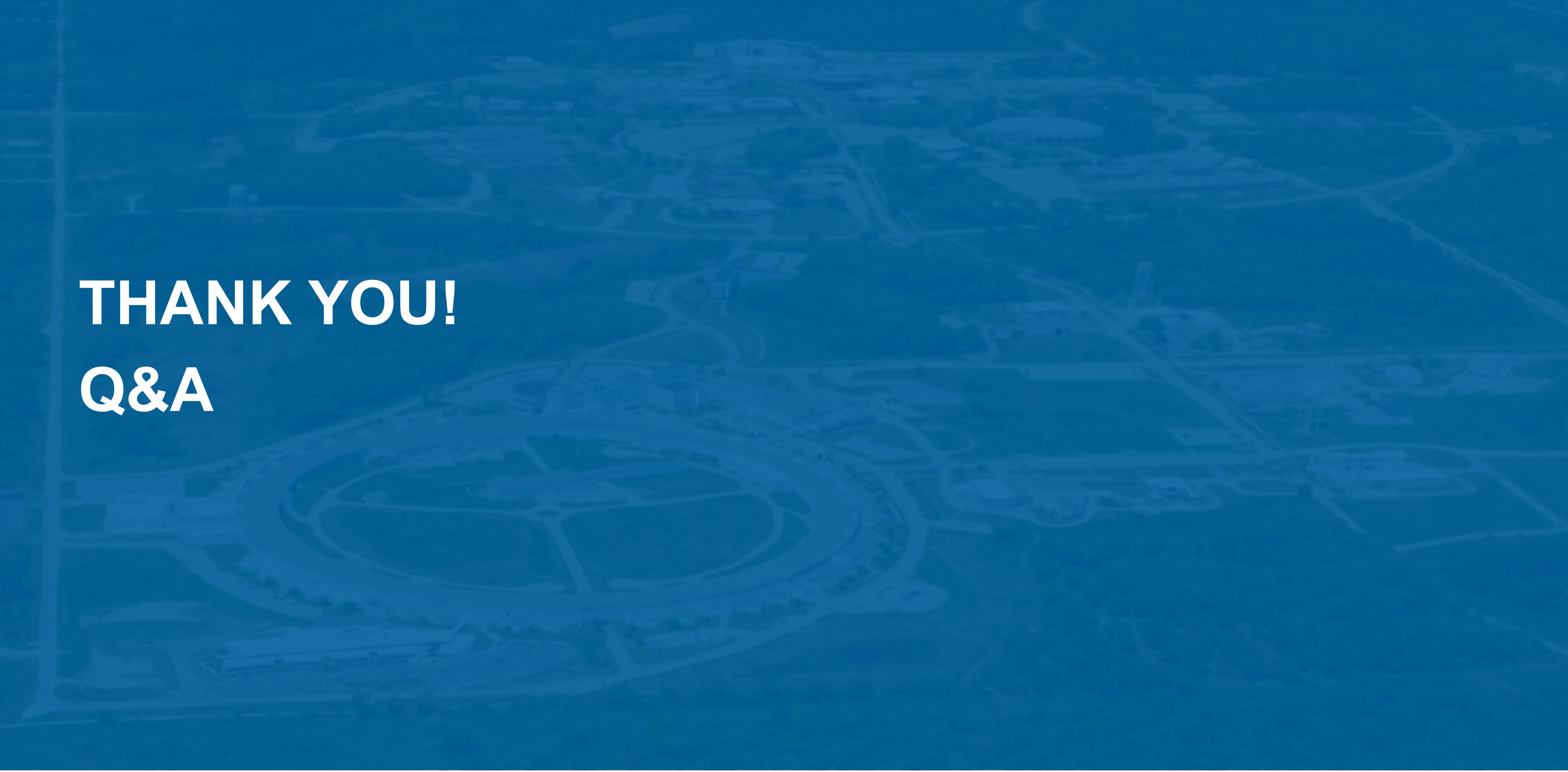
MNIST-FedAvg-5Clients

RESOURCES

- Privacy Preserving Federated Learning as a Service APPFLx - https://appflx.link/ and instructions https://ppflaas.readthedocs.io/en/latest/
- GitHub for the APPFL framework: https://github.com/APPFL/APPFL/
- Globus Compute Communicator: https://github.com/APPFL/APPFL/tree/main/src/appfl/comm/globus_compute
- APPFLx paper: https://arxiv.org/pdf/2308.08786.pdf
- FedCompass preprint: https://arxiv.org/pdf/2309.14675.pdf

FUNDING ACKNOWLEDGEMENTS

THIS MATERIAL IS BASED UPON WORK SUPPORTED BY THE U.S. DEPARTMENT OF ENERGY, OFFICE OF SCIENCE, UNDER CONTRACT NUMBER DE-AC02-06CH11357.



THANK YOU!

Q&A