

PRIVACY PRESERVING FEDERATED LEARNING AS A SERVICE - A KEY CAPABILITY FOR BUILDING ROBUST AI MODELS FOR SCIENCE



RAVI MADDURI

Computer Scientist

Data Science and Learning Division

madduri@anl.gov

FUNDING ACKNOWLEDGEMENTS

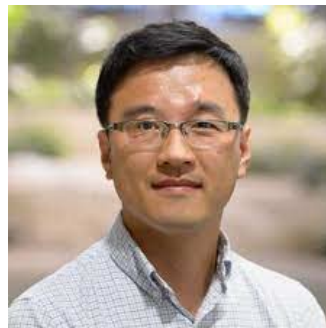
THIS MATERIAL IS BASED UPON WORK SUPPORTED BY THE U.S. DEPARTMENT OF ENERGY, OFFICE OF SCIENCE, UNDER CONTRACT NUMBER DE-AC02-06CH11357.



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



TEAM



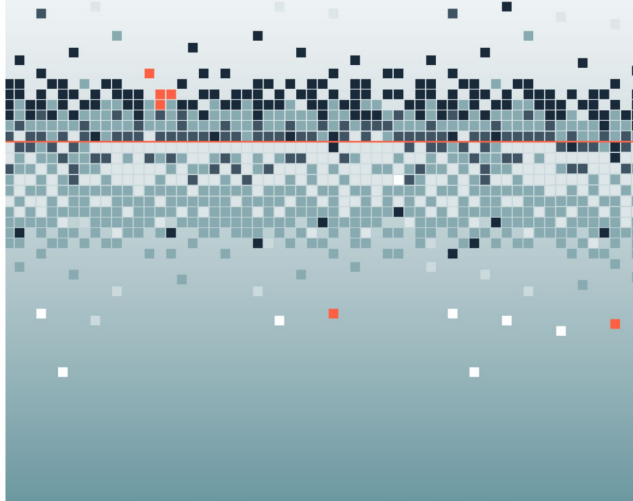
Zilinghan Li, Shilan He, Minseok Ryu, Kibaek Kim, Ravi Madduri

MOTIVATION FOR FEDERATED LEARNING

THE LANCET
Digital Health

DATASET SHIFT IN MACHINE LEARNING

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



ARTICLES | VOLUME 4, ISSUE 6, E406-E414, JUNE 01, 2022

AI recognition of patient race in medical imaging: a modelling study

THE NEW ENGLAND JOURNAL of MEDICINE

CORRESPONDENCE



The Clinician and Dataset Shift in Artificial Intelligence

Source: PMID: 34260843 DOI: [10.1056/NEJMc2104626](https://doi.org/10.1056/NEJMc2104626)

LAB REPORT Kelly Malcom June 21, 2021 11:41 AM

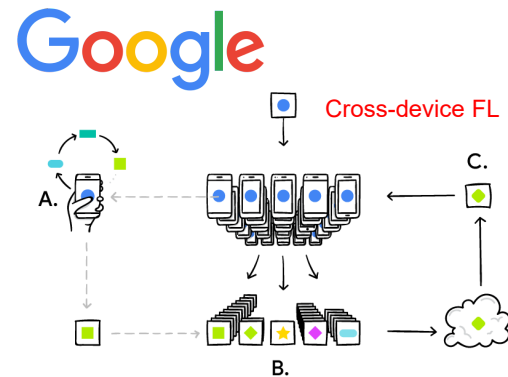
Popular sepsis prediction tool less accurate than claimed

The algorithm is currently implemented at hundreds of U.S. hospitals.

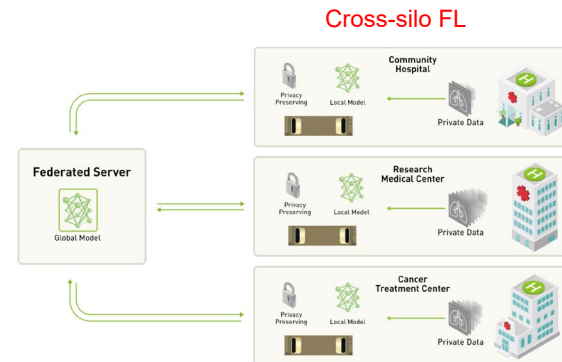
Source: <https://labblog.uofmhealth.org/lab-report/popular-sepsis-prediction-tool-less-accurate-than-claimed>

FEDERATED LEARNING (FL)

- Machine learning without centralizing training data
 - No direct data sharing or storing
 - Training at local and transferring model information
 - Finding a global model
- More benefits
 - Learning a global/shared model
 - Utilizing a localized model at each client side
 - Personalization
- Two settings:
 - Cross-device FL (1000s and 1Ms of small devices)
 - Cross-silo FL (a few large data repositories)
- Challenges in algorithm design



Your phone personalizes the model locally, based on your usage (A). Many users' updates are aggregated (B) to form a consensus change (C) to the shared model, after which the procedure is repeated. (image from Google)



Federated learning on decentralized medical datasets (image from NVIDIA)

PRIVACY-PRESERVING TECHNIQUES

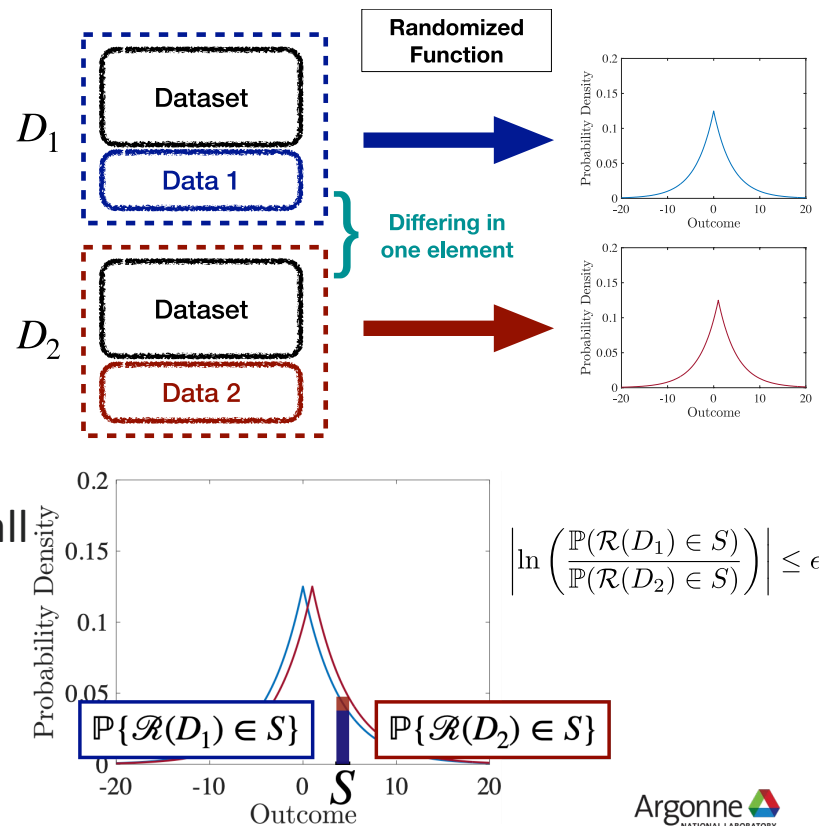


■ Some techniques in FL

- Homomorphic encryption: limited to certain operations
- Secure multi-party computation: computationally expensive
- Differential privacy: potential accuracy loss

■ Differential Privacy

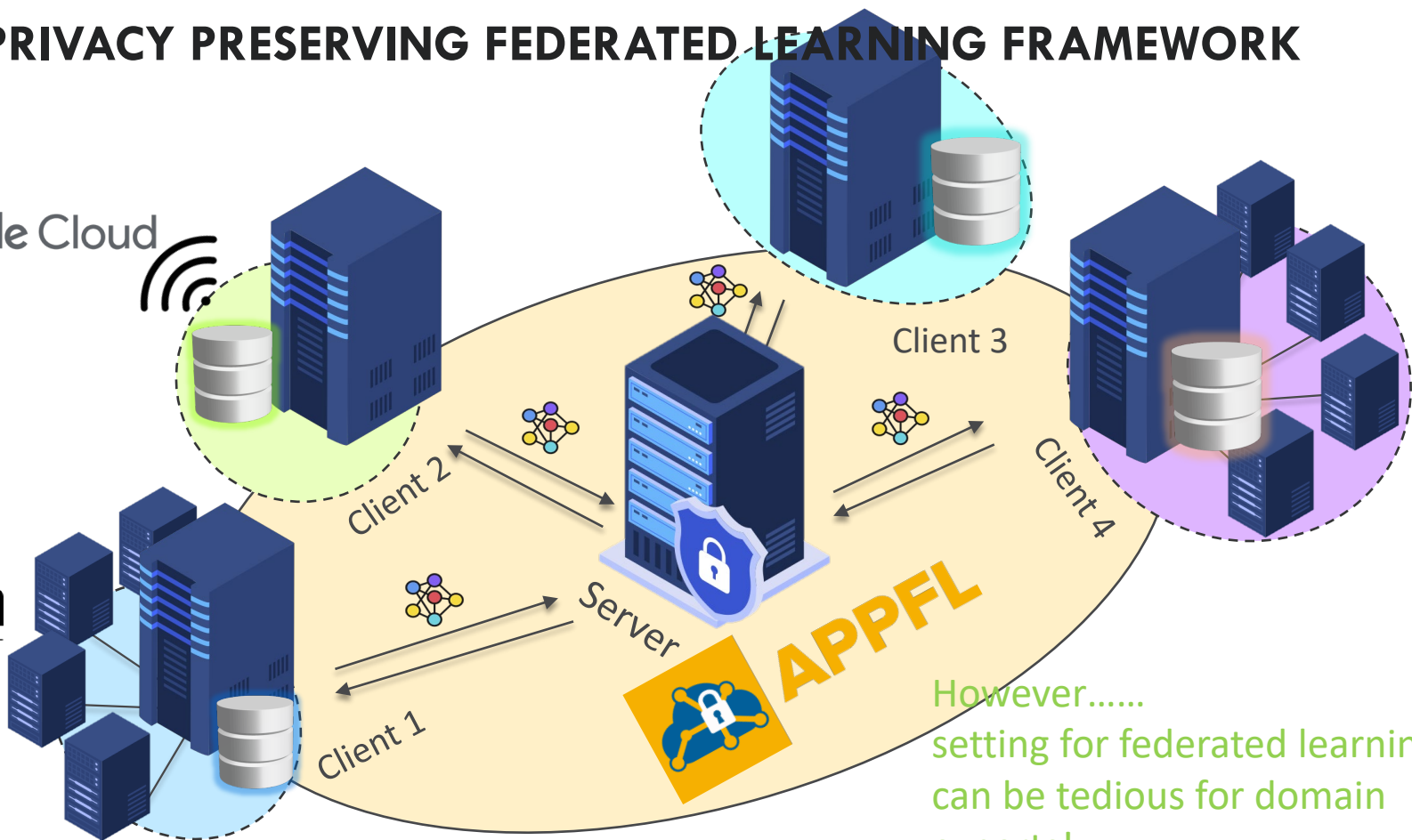
- The two outcomes are indistinguishable for all D_1 and D_2 which differ in one individual's data.



APPFL – PRIVACY PRESERVING FEDERATED LEARNING FRAMEWORK

 Google Cloud


slurm
workload manager



However.....
setting for federated learning
can be tedious for domain
experts!

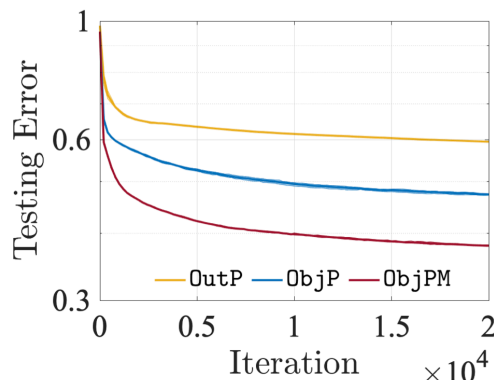
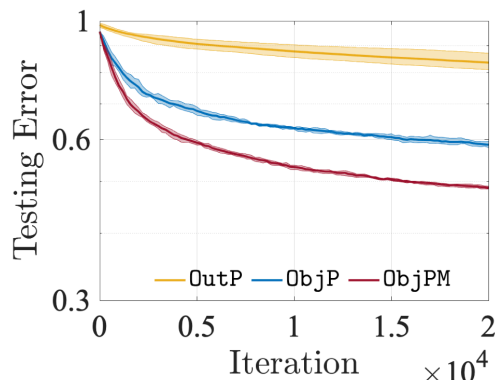
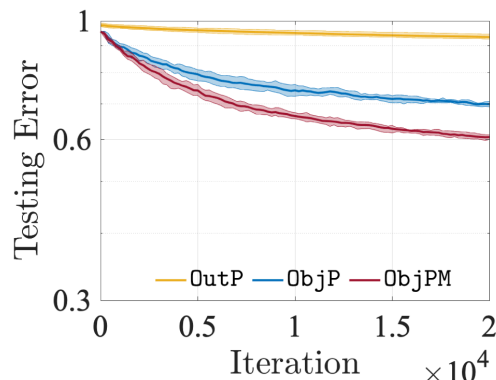
IMPACT OF ADVANCED ALGORITHMS IN PPFL

Implementation of novel training algorithms

- (state-of-the-art) OutP: Inexact ADMM (IADMM) + output perturbation
- (APPFL) ObjP: IADMM + objective perturbation
- **(APPFL) ObjPM:** IADMM + objective perturbation + multiple local updates

Stronger privacy
Weaker learning

Weaker privacy
Stronger learning

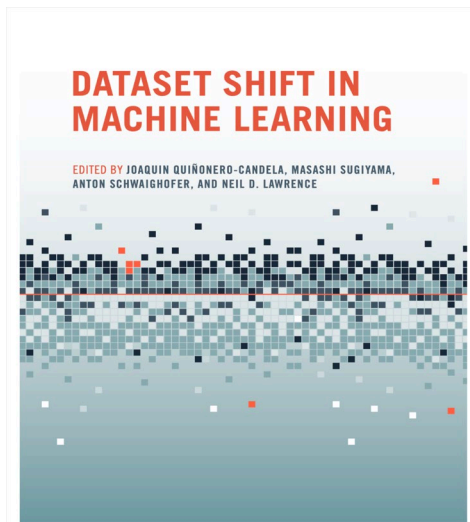


Algorithms developed in APPFL result in lower testing errors in any range of privacy budget, from weak privacy to strong privacy

MAJOR COMPONENTS OF APPFL

- **Training algorithms:**
 - IIADMM, FedAvg [McMahan et al., 2017], ICEADMM [Zhou and Li, 2021]
 - Any user-defined FL algorithms can be added.
- **Privacy-preserving schemes:**
 - Differential privacy mechanisms [Dwork et al., 2006]
 - Other schemes (e.g., homomorphic encryption) to be added.
- **Communication protocols:**
 - gRPC: communication between multiple platforms and languages
 - MPI: efficient communication in a cluster environment
- **User-defined model and data:**
 - Inherits PyTorch's neural network module, `torch.nn.Module`
 - Dataset class that inherits the PyTorch's Dataset

MOTIVATION FOR FEDERATED LEARNING AS A SERVICE



Data Shift in
Machine Learning



Privacy Concerns in
Biomedical Data



Tedious Federated
Learning Setup

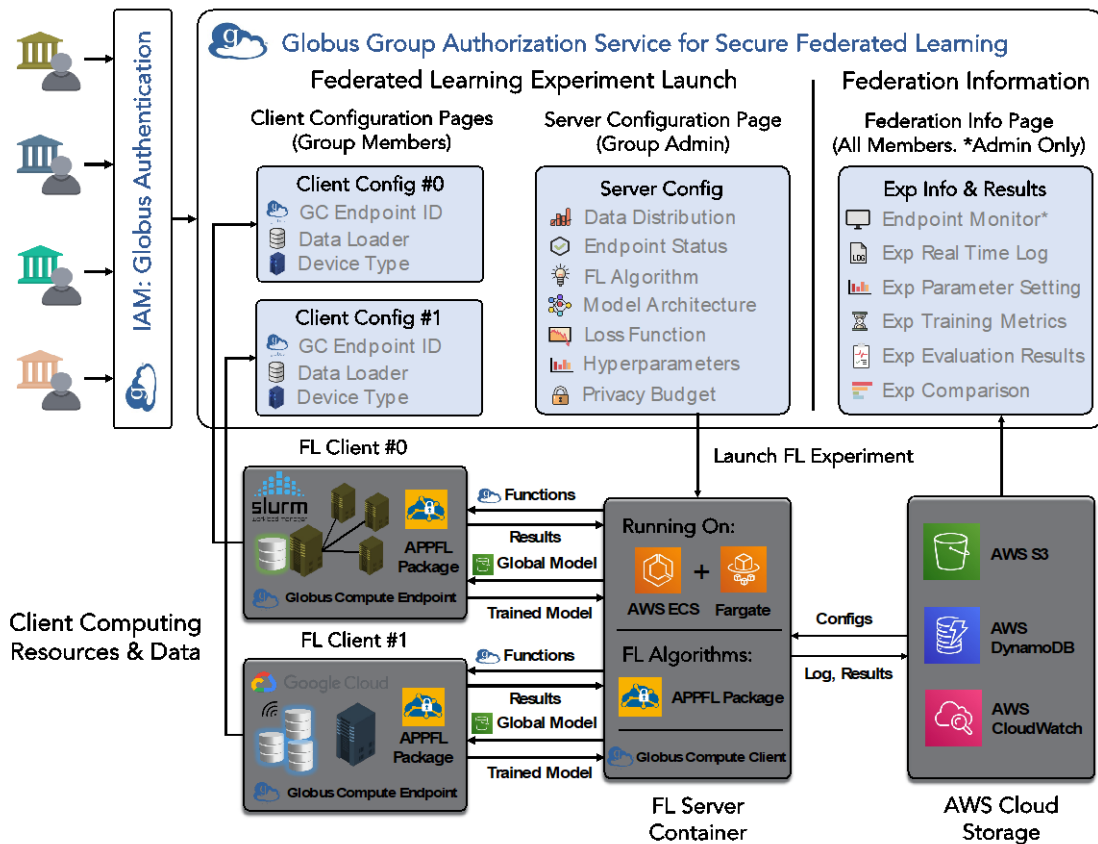
KEY CAPABILITIES OF APPFLX

To Build Models that are Fair and Trustworthy using PPFL easily

- Simple but effective user experience to design, run, share FL experiments with FAIR ideas applied to ML
 - Visualize training data distributions at different participating sites
- End-to-End strong IAM
 - Enable setting up Secure Federation across organizational boundaries
- Easy to leverage HPC for training
 - Integrate heterogeneous computing resources and monitor usage
- Ability to leverage novel Federation strategies
 - Creation of FedCompass Efficient Cross-Silo Federated Learning on Heterogeneous Client Devices using a Computing Power Aware Schedule
- Framework to rapidly run experiments with different hyper-parameters and measure performance with Tensorboard and visualize data distributions in different sites
- Integration with HuggingFace, GitHub for pre-trained models and uniform pre-processing
- APIs and Plug-and-Play architecture
 - To integrate into existing services and add new capabilities/algorithms

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



GOING 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

Federation Information

Endpoint Information

Client	Organization	Email	Endpoint Status
Jan F Nygld	Cancer Registry of Norway	 jfn@krefregisteret.no	
Severin Langberg	Cancer Registry of Norway	 Langberg91@gmail.com	
Zilinghan Li (You)	University of Illinois	 1250976113@qq.com	
Zilinghan Li - NCSA	National Center for Supercomputing Applications	 zli52@illinois.edu	
Ravi Madduri	Argonne	 madduri@anl.gov	
Marcus Klarqvist	broad institute of mit and harvard	 mklarqvist@broadinstitute.org	
Jordan Fuhrman	The University of Chicago	 jdfuhrman@uchicago.edu	

Experiment Information

Experiment Name	Experiment ID	Status	Config	Log	Report	Tensorboard
MINIST1	5a525a61353a4a5a82b3ee895773eedf	DONE				
MINIST2	4c1ee4409b04db89bbc1b210f7699b1	DONE				
MINIST3	75474c0d2bbe4c2481e766b1166b6672	DONE				
MINIST4	be5eb91f8e9e4e8ca647f061b52ccb93	DONE				
Ravi_Demo	23e0bc8fa234130a4a99917e759b928	DONE				
MINIST5	de7ffbb6d2a42bba205158e22bdbfa	DONE				
Demo_Polaris	57d2605794d744f6b7dd08147cafb3c6	DONE				
Demo_Polaris_New	922ddcfe9ecf4ad2b912a5eb14cf720f	DONE				
Ravi_Demo_Latest	7151875c342747169a6707af62ebf21d	DONE				
Final_Demo	4e4432e25b2d4eb6ab4c3f5c1c86d87	DONE				
Ravi_Demo1	06f501225b694a459b3591fec6b69e23	DONE				
MINIST-Report-Demo	fec4ff7c793ae4027bb23d1fe5ab7e97	DONE				
MINIST-Report-Demo2	dfd328dc940346ea87cd4168a2600773	DONE				
MINIST-Demo	27e6ad17a07d4d3f83385e7660078895	DONE				

APPFLX CAPABILITIES

Comprehensive Experiment Reports

Federation Report

Print as PDF

Group Name: APPFLX-Demo

Experiment Name: MNIST-FedAvgM-5Clients

Training Hyperparameters

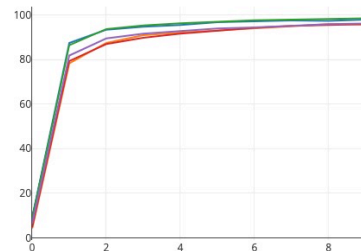
hyperparameter	explanation	value
Federation Algorithm	Server algorithm for the federated learning	Federated Average Momentum
Global training epochs	Number of global training epochs for the federation server	10
Local training epochs	Number of local training epochs for each federation site/endpoint	2
Privacy 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

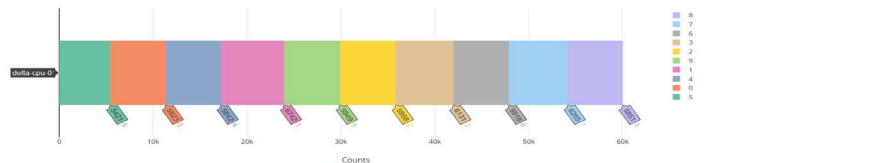
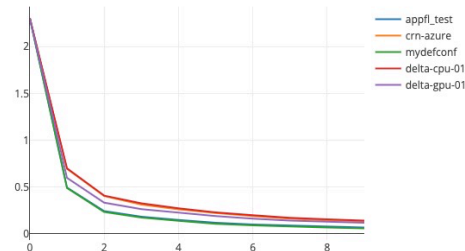
▶ Click here to expand explanations:

MNIST-FedAvg-5Clients

Accuracy vs. Step



Loss vs. Step



ADDITIONAL ONGOING WORK

- Systematic evaluation of different attack modalities
 - Joint work with Miao Li and Mihai Anitescu
 - Attack models include inverse gradient approach, Optimization-based approach like Deep Leakage from Gradients (DLG) and Solving a sequence of linear equations in the R-Gap(Recursive Gradient Attack On Privacy)
- Continuous Learning and Feedback Loop
 - Federated Learning allows for continuous learning and feedback from the local devices. As the models are trained on local data, the devices can provide feedback on the performance and accuracy of the models. This feedback loop helps in identifying data quality issues, model biases, or other issues that can be addressed to improve the overall quality of the training data and the resulting models
- Develop and apply a methodology for providing tiered levels of privacy assurance for a privacy-preserving federated learning framework, while validating the security of the overall system against risks such as model poisoning/corruption, denial of service, or intentional prevention of convergence
 - Joint work with Argonne's Cyber team (Blakely et al.)

APPLYING APPFL IN BIOMEDICINE APPLICATIONS & CHALLENGES

BIOMEDICAL APPLICATIONS

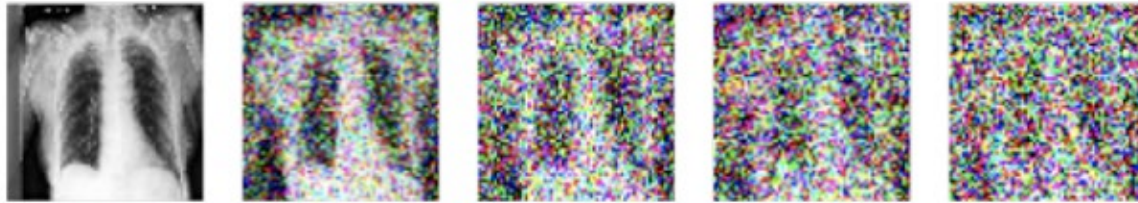
Detection of COVID-19 from Chest X-Rays

**Prediction of age from ECGs to use in models
predicting risk for a CVD event**

USE CASE

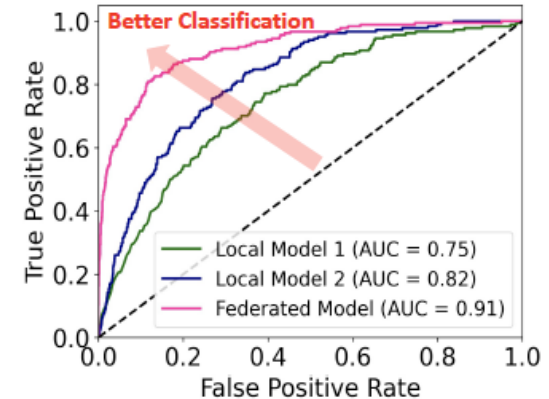
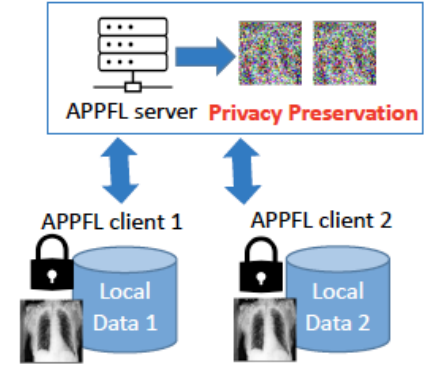
Chest X-ray classification for COVID-19 cases

- FL can produce more accurate model, compared to the models trained on local datasets.
- DP is applied to protect chest X-ray data from reverse-engineering the model gradients communicated during training.
- Collaborations with UChicago Medical School and Broad Institute



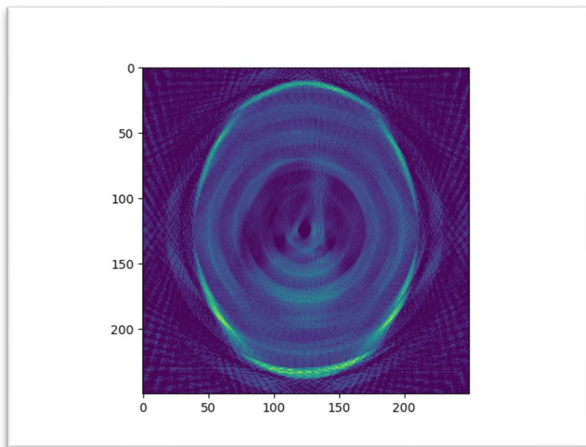
Weaker Privacy

Stronger Privacy



FEDERATED RECONSTRUCTION USING MULTIMODAL DATA

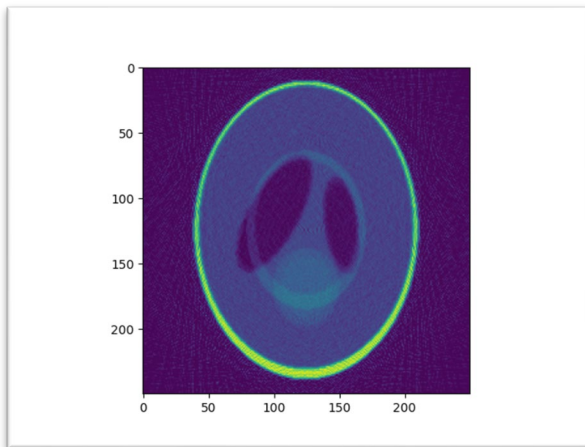
Reconstruction using Unimodal vs Multimodal Data



Reconstruction using **XRT**
unimodal data only

$$w^u = \operatorname{argmin} \|Aw - b\|^2$$

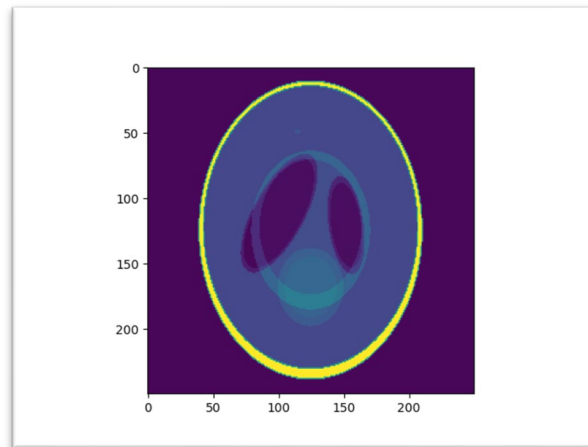
$$\operatorname{MSE}(w^u) = 0.0146$$



Reconstruction using **XRT+XRF**
multimodal data sources

$$w^m = \operatorname{argmin} \|Aw - b\|^2 + f^{XRF}(w)$$

$$\operatorname{MSE}(w^m) = 0.0028 \text{ (better)}$$



Ground truth w^*

$$\operatorname{MSE}(w) := \operatorname{avg}(\|w - w^*\|^2)$$

OVERVIEW OF ECG USECASE



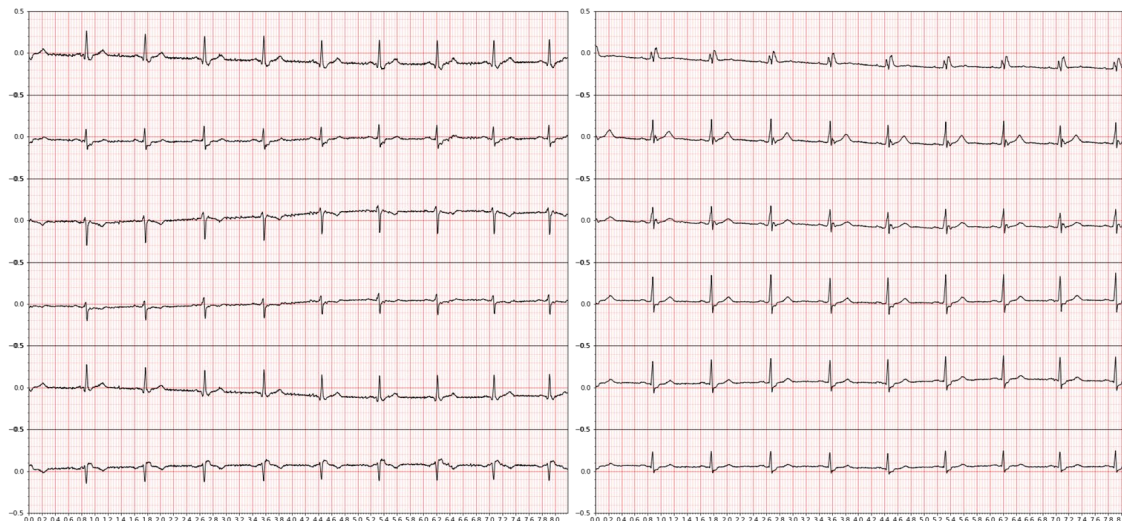
- Chronologic age can be a poor predictor of lifetime CVD risk, particularly among younger individuals
- Augmenting with additional variables can help to refine these estimates, but still ignore the component of variation explained by age
- Replacing with more biological proxies for age, such as from ECGs, can resolve these issues
- ECGs are typically not shared across, or sometimes even within, institutions

WORST PERFORMING ECG: 21-22 YEARS OLDER COMPARED TO CHRONOLOGICAL AGE



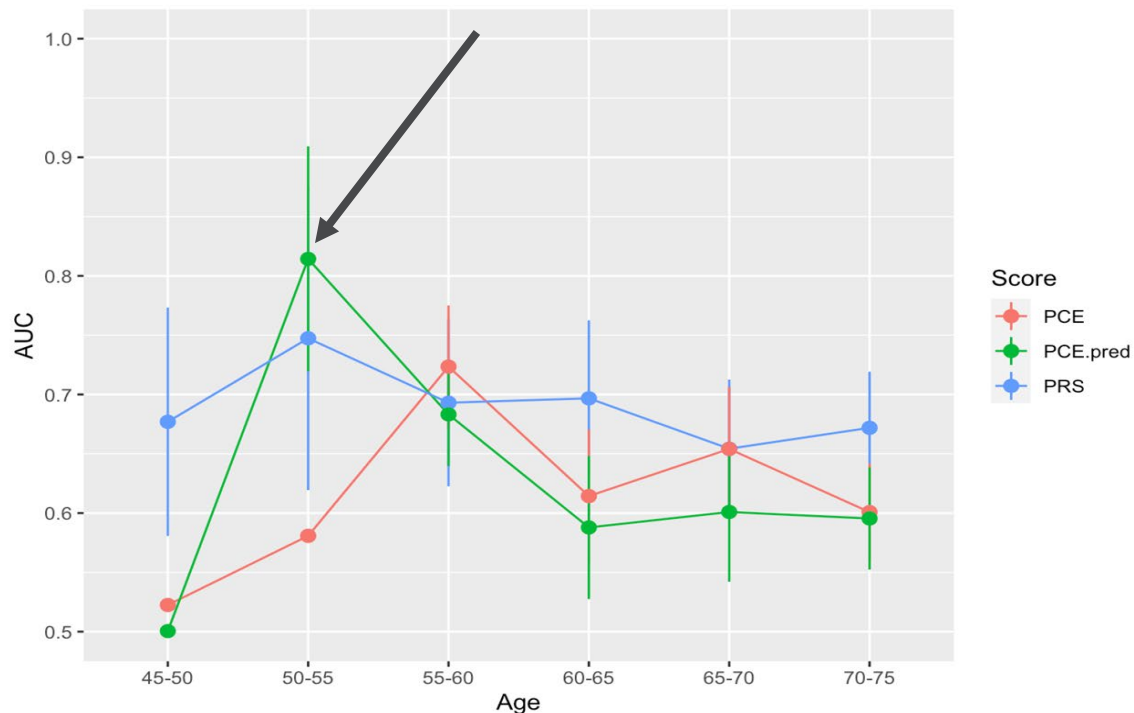
Predicted: 78.342468

Real: 56.861546



How does this age-proxy affect disease risk?

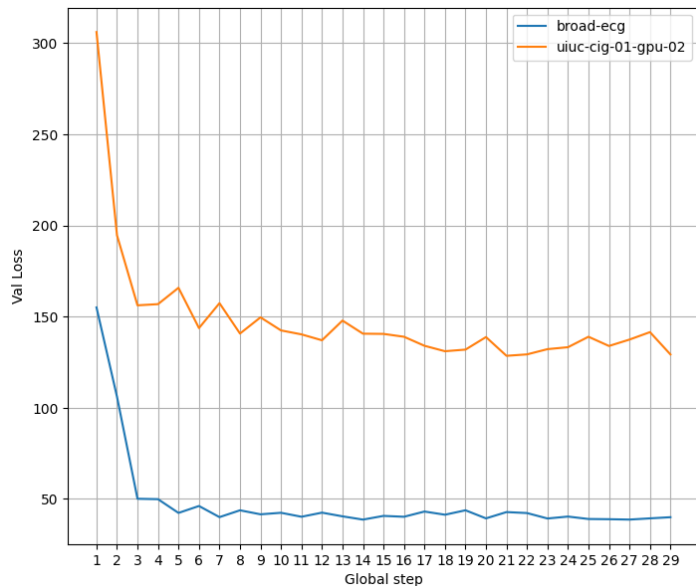
REGRESSED AGE IMPROVES PREDICTIVE POWER FOR YOUNGER AND HARDER-TO-PREDICT SUBJECTS



Urbut et al. (In preparation)

BIOLOGICAL AGING PREDICTION FROM ECG SIGNAL

Training with FL on two clients



Best MSE on ECG-ANL = 125.00

Best MSE on ECG-Broad = 41.70

FL can learn a global model that performs relative well on both datasets

Table 1. Statistic of the datasets used in the biological aging prediction from ECG signal experiment.

Dataset	Train	Val	Test	Total
ECG-ANL	64518	7905	7905	80328
ECG-Broad	33140	4143	4143	41426

Table 2. Testing MSE error of the biological aging prediction from ECG signal models.

Training Dataset	Testing Set	
	ECG-ANL	ECG-Broad
ECG-ANL (<i>single</i>)	109.95	224.48
ECG-Broad (<i>single</i>)	225.41	38.93
ECG-ANL+Broad (<i>FedAvg</i>)	125.00	41.70

CONCLUSION

- Dataset Shift challenge in AI are real
 - Models don't do well when applying in settings different from settings and data used in training
 - Bigger challenge in Biomedicine where data is not shared because of policy issues
- We presented APPFLx where we
 - Developed APPFL (Argonne Privacy-Preserving Federated Learning) framework that implements end-to-end secure framework that leverages *differential privacy algorithms* along with capabilities to leverage heterogeneous HPC resources easily
 - We discussed how we integrated APPFL framework with our existing computing and data infrastructure (i.e., ABLE, SEAL, HPCrypt, funcX, and DLHub) with focus on validating and evaluating APPFL framework by using the multi-institutional biomedical datasets
- We presented results and lessons learned when applying APPFL to Biomedical datasets

RESOURCES

- Privacy Preserving Federated Learning as a Service APPFLx - <https://appflx.link/> and instructions <https://ppflaas.readthedocs.io/en/latest/>
- GitHub Repo: <https://github.com/APPFL>
- Pre-print for APPFLx: <https://arxiv.org/pdf/2308.08786.pdf>
- FedCompass pre-print: <https://arxiv.org/abs/2309.14675>

Q&A



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