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

HDF5: Building on 25 years of success
Birds of Feather at SC23, Denver
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.
TEAM

Zilinghan Li, Shilan He, Minseok Ryu, Kibaek Kim, Ravi Madduri
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 D1 and D2 which differ in one individual’s data.
APPFL – PRIVACY PRESERVING FEDERATED LEARNING FRAMEWORK

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

Creating Secure Federations

Dashboard

Federations

<table>
<thead>
<tr>
<th>Federation Name</th>
<th>Organization</th>
<th>Email</th>
<th>Endpoint Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANL_NCSA_LNL</td>
<td>Cancer Registry of Norway</td>
<td><a href="mailto:jh@washingtonuniversity.edu">jh@washingtonuniversity.edu</a></td>
<td></td>
</tr>
<tr>
<td>Shilan Test1</td>
<td>University of Illinois</td>
<td><a href="mailto:langberg@illinois.edu">langberg@illinois.edu</a></td>
<td></td>
</tr>
<tr>
<td>B2AI/PALISADE-X/MGH</td>
<td>National Center for Supercomputing Applications</td>
<td><a href="mailto:zl@broadinstitute.org">zl@broadinstitute.org</a></td>
<td></td>
</tr>
<tr>
<td>B2AI/PALISADE-X/FLAAS.AWS</td>
<td>Argonne</td>
<td><a href="mailto:mcdonald@anl.gov">mcdonald@anl.gov</a></td>
<td></td>
</tr>
<tr>
<td>APPFLX-Demo</td>
<td>Inova Institute of melt and remelt</td>
<td><a href="mailto:redmond@broadinstitute.org">redmond@broadinstitute.org</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The University of Chicago</td>
<td><a href="mailto:jphoffman@uchicago.edu">jphoffman@uchicago.edu</a></td>
<td></td>
</tr>
</tbody>
</table>

Sites

Site Name

Experiment Information

<table>
<thead>
<tr>
<th>Experiment Name</th>
<th>Experiment ID</th>
<th>Status</th>
<th>Config</th>
<th>Log</th>
<th>Report</th>
<th>Tangent</th>
<th>Endpoint Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>MNB31</td>
<td>1af24b119c13b3c4b3d3c2e873d4e4f5</td>
<td>DONE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MNB32</td>
<td>4af4b144b3c3b3c3b3b3b3b3b3b3b3b3</td>
<td>DNE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MNB33</td>
<td>7f4742b3c3b3b3b3b3b3b3b3b3b3b3b3</td>
<td>DNE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MNB34</td>
<td>5e5b4f5b6b5b6b5b6b5b6b5b6b5b6b6b</td>
<td>DNE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rori_Demo</td>
<td>254b3b5b2b5b2b5b2b5b2b5b2b5b2b5b</td>
<td>DNE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rori_Demo</td>
<td>254b3b5b2b5b2b5b2b5b2b5b2b5b2b5b</td>
<td>DNE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fosti_Demo</td>
<td>2f4b3b3b3b3b3b3b3b3b3b3b3b3b3b3b</td>
<td>DNE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rori_Demo</td>
<td>265b145b4b5b4b5b4b5b4b5b4b5b4b5b</td>
<td>DNE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MNB31_Report_Demo</td>
<td>4af4b144b3c3b3b3b3b3b3b3b3b3b3b3</td>
<td>DNE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MNB32_Report_Demo</td>
<td>5e5b4f5b6b5b6b5b6b5b6b5b6b5b6b6b</td>
<td>DNE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- DONE: Experiment is complete.
- DNE: Experiment not done.
- Config: Configuration changes are needed.
- Log: Log file is available.
- Tangent: Tangent action needed.
# APPFLX CAPABILITIES

## Comprehensive Experiment Reports

### Federation Report

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

### Sites Validation

- Click here to expand explanations:

**MNIST-FedAvg-50Clients**

<table>
<thead>
<tr>
<th></th>
<th>Accuracy vs. Step</th>
<th>Loss vs. Step</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

[Argonne National Laboratory](https://www.anl.gov/)
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.)
RESOURCES

- 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