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

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
TEAM

MOTIVATION FOR FEDERATED LEARNING AS A SERVICE

Data Shift in Machine Learning

Privacy Concerns in Biomedical Data
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

---

**Running On:**

- **AWS ECS**
- **Fargate**

**FL Algos:**

- **APPFL**

**FL Client #0**

- Functions
- Results
- Configs

**FL Client #1**

- Functions
- Results

**FL Server Container**

**AWS S3**

**AWS DynamoDB**

**AWS CloudWatch**

---

**Globus Group Authorization Service for Secure Federated Learning**

**Federated Learning Experiment Launch**

- Client Configuration Pages (Group Members)
- Server Configuration Page (Group Admin)

**Globus Compute Endpoint**

**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
**GO BEYOND AN FL FRAMEWORK: WHY “AS-A-SERVICE”?**

### Comparison between a PPFL framework and APPFLx

<table>
<thead>
<tr>
<th></th>
<th>Framework</th>
<th>Service (APPFLx)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Target users:</strong></td>
<td>Developers for developing and simulating FL algorithms.</td>
<td><strong>Target users:</strong> Domain experts for applying FL.</td>
</tr>
<tr>
<td><strong>Authentication:</strong></td>
<td>No client auth for most frameworks.</td>
<td><strong>Authentication:</strong> Clients use institutional credentials via Globus Auth to setup a trust relationship</td>
</tr>
<tr>
<td><strong>Launch Server:</strong></td>
<td>Requires expertise to start federated learning experiments.</td>
<td><strong>Launch Server:</strong> Admin uses web UI to easily launch the FL experiment with different hyperparameters.</td>
</tr>
<tr>
<td><strong>Results:</strong></td>
<td>Server needs to manually share the whole results, which may require further post-process.</td>
<td><strong>Results:</strong> Comprehensive logs, reports, and visualizations shared among all clients on web UI.</td>
</tr>
<tr>
<td><strong>Connection:</strong></td>
<td>Developed algorithms via the framework can be easily adopted to the service.</td>
<td><strong>Connection:</strong> The service is built on the top of the APPFL framework</td>
</tr>
<tr>
<td><strong>Misc:</strong></td>
<td></td>
<td><strong>Misc:</strong> Integrated with HuggingFace, GitHub for pre-trained models and pre-processing.</td>
</tr>
</tbody>
</table>
APPFLX CAPABILITIES
Creating Secure Federations

Dashboard

Federations

Federation Name  

- ANL_NCSA_LLNL  
- Shilan Test1  
- B2AI/PALISADE-X/MGH  
- B2AI/PALISADE-X/MGH_FLAAS_AWS  
- APPFLX-Demo

Sites

Site Name  

- ANL_NCSA_LLNL  
- Shilan Test1  
- B2AI/PALISADE-X/MGH

Federation Configuration

Client Endpoints  

- 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

https://appflx.link/
APPFLX CAPABILITIES

Comprehensive Experiment Reports

Federation Report

Group Name: APPFLX-Demo
Experiment Name: MNIST-FedAvg-M-5Clients

Training Hyperparameters

<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>Federated Average Momentum</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 (TFB)</td>
<td>False</td>
</tr>
<tr>
<td>Clip norm</td>
<td>Clip norm for privacy preserving (TFB)</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</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-M-5Clients

Accuracy vs. Step

Loss vs. Step
RESOURCES

- GitHub for the APPFL framework: https://github.com/APPFL/APPFL/
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