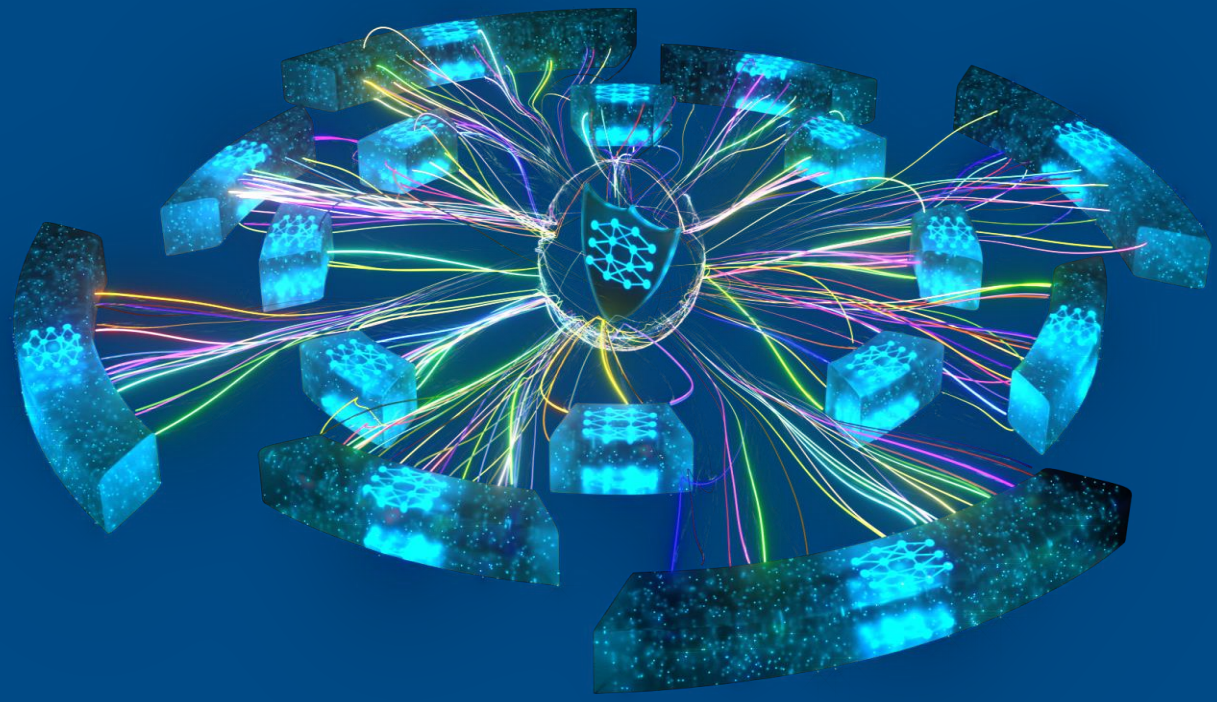
The ***COFE*** Ecosystem

GaNDLF	OpenVINO	HF Hub	OpenFL	MedPerf
Generally Nuanced Deep Learning Framework	Model optimization for inference on low-resource environments	Model deployment across multiple platforms & ecosystems	Federated Learning Library	Governance & Orchestration
gandlf.org	**openvino.ai**	**hf.co**	**openfl.io**	**medperf.org**
ML Commons	intel.	🤗	OPENFL	ML Commons
S. Pati, et al., *Nature Communications Engineering*, 2(23), 2023	A. Demidovskij, et al.; *ICCV Workshop*, 783-787, 2019	S.M. Jain, *Introduction to Transformers for NLP*, 51-67, Berkeley, 2022	P. Foley, et al., *Phys Med Biol (ITCR Special Issue)*, 67(21), 214001, 2022	A. Karargyris, et al.; *Nature Machine Intelligence* 5:799-810, 2023

https://www.linkedin.com/in/psfoley/
patrick.foley@intel.com

OpenFL

Building Better AI Models with Private Data



Patrick Foley

Chief Architect and Engineering Manager for OpenFL

intel®

Financial Disclosure of Commercial Interests

Speaker Name: Patrick Foley

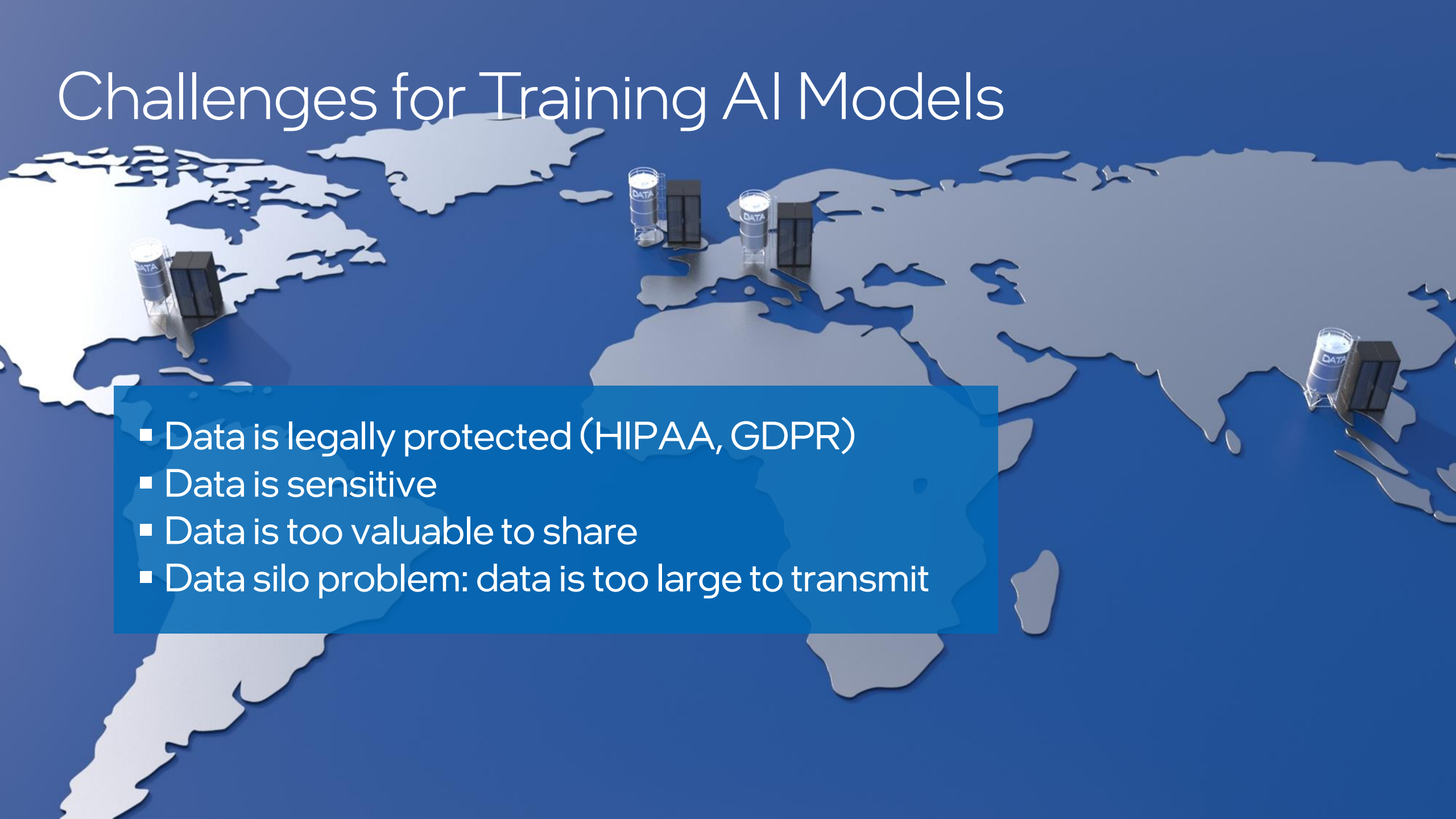
OpenFL and its derivatives may be commercialized by Intel or Intel's partners in the future

https://www.linkedin.com/in/psfoley/
patrick.foley@intel.com

Topics

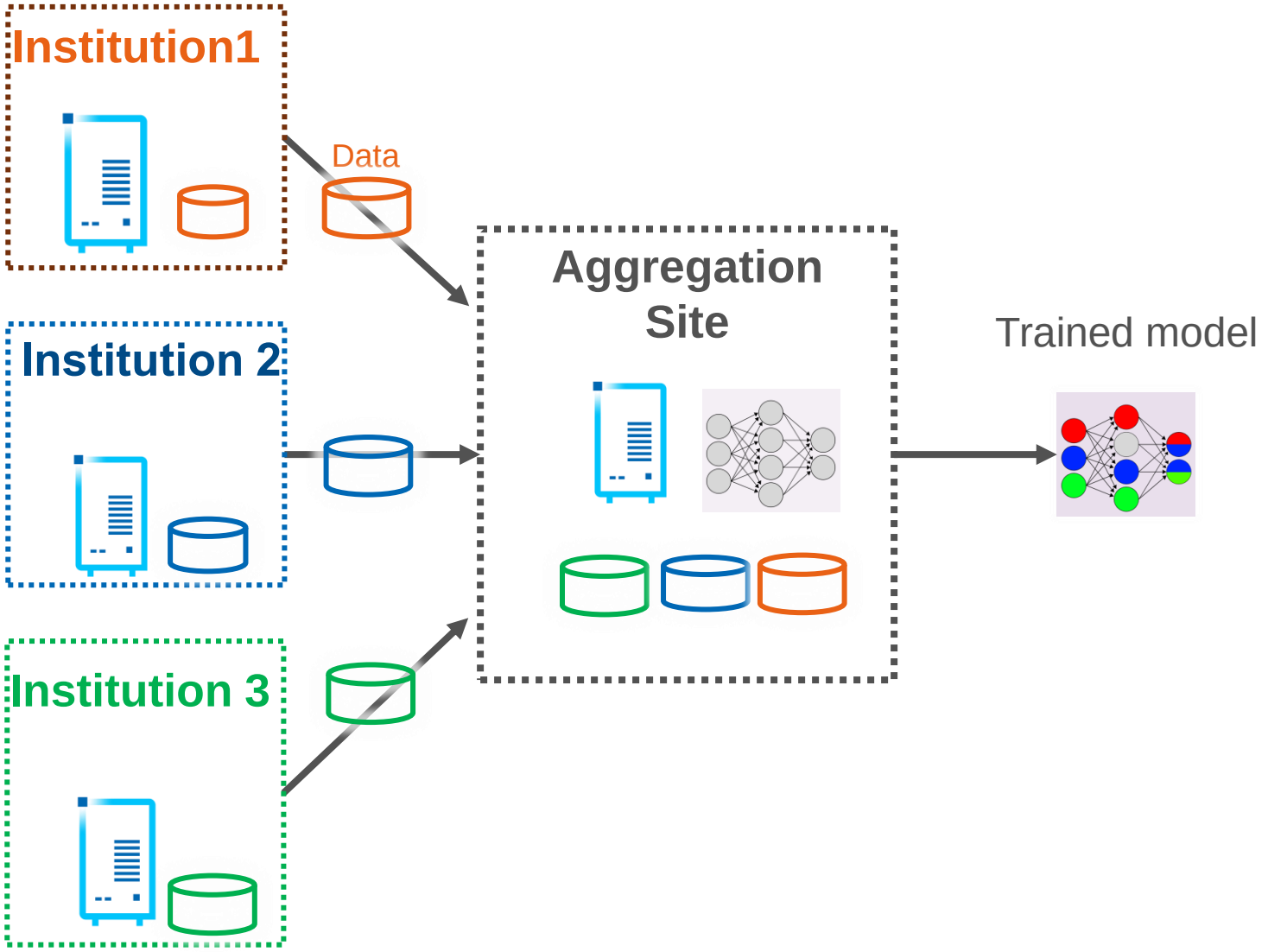
1. Introduction to Federated Learning and OpenFL
2. FL security and privacy challenges addressed using Intel SGX
3. Additional real world usage of OpenFL
4. How to get involved

Challenges for Training AI Models

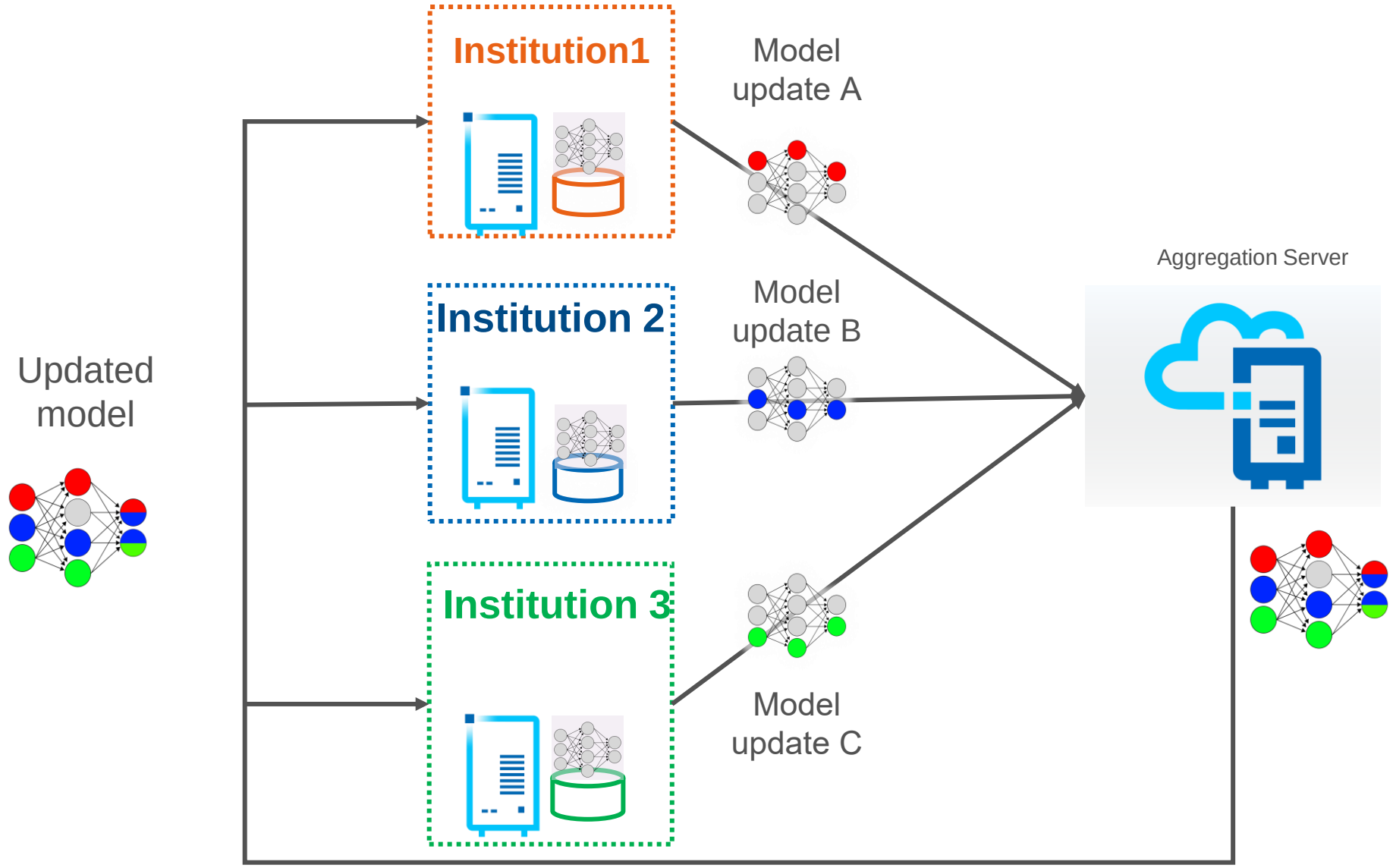


- Data is legally protected (HIPAA, GDPR)
- Data is sensitive
- Data is too valuable to share
- Data silo problem: data is too large to transmit

Traditional Centralized learning

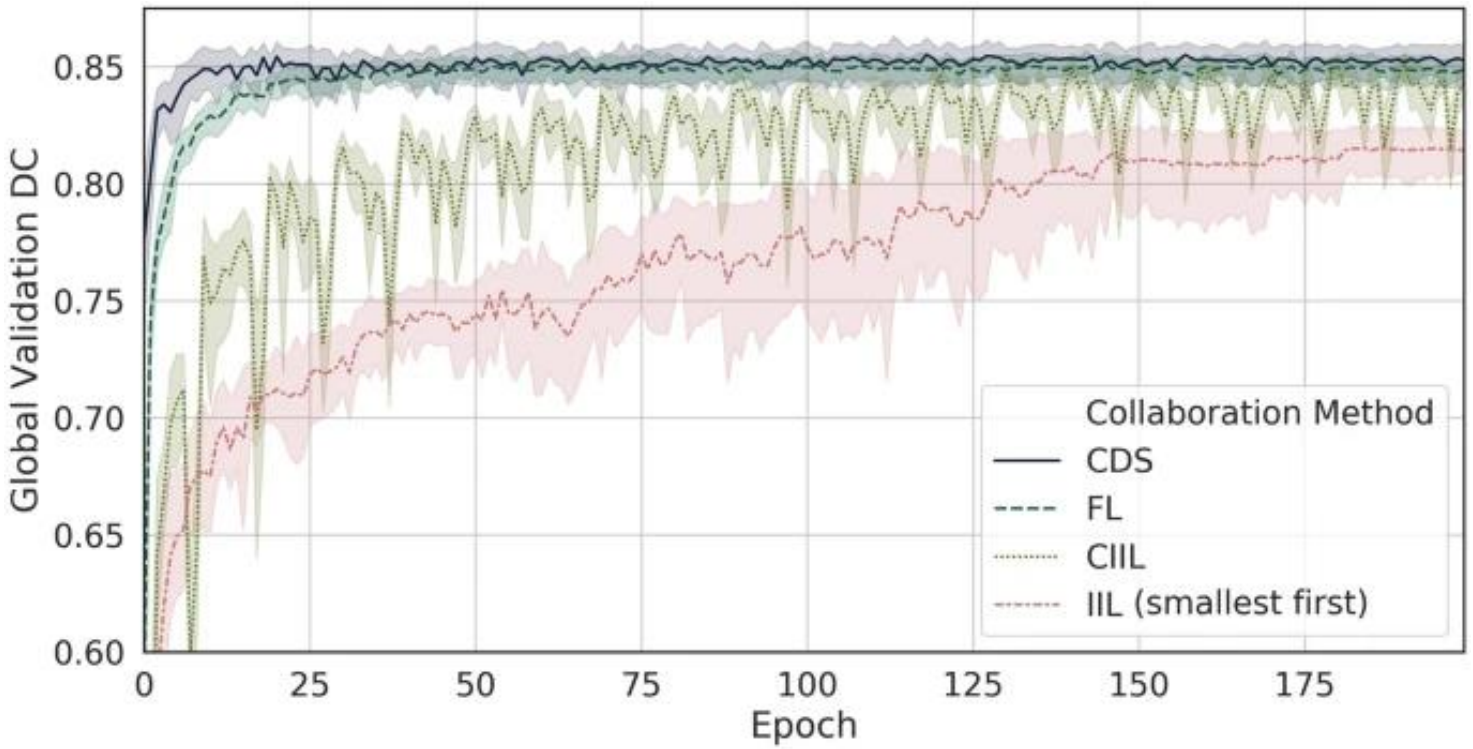


Federated Learning



https://www.linkedin.com/in/psfoley/
patrick.foley@intel.com

Centralized Learning versus Federated Learning



scientific reports

Explore our content | Journal information

nature > scientific reports > articles > article

Article | Open Access | Published: 28 July 2020

Federated learning in medicine: facilitating multi-institutional collaborations without sharing patient data

Micah J. Sheller, Brandon Edwards, G. Anthony Reina, Jason Martin, Sarthak Pati, Aikaterini Kotrotsou, Mikhail Milchenko, Weilin Xu, Daniel Marcus, Rivka R. Colen & Spyridon Bakas

Scientific Reports **10**, Article number: 12598 (2020) | Cite this article

3140 Accesses | **119** Altmetric | Metrics

Abstract

Several studies underscore the potential of deep learning in identifying complex patterns, leading to diagnostic and prognostic biomarkers. Identifying sufficiently large and diverse datasets, required for training, is a significant challenge in medicine and can rarely be found in

SCIENTIFIC REPORTS

intel

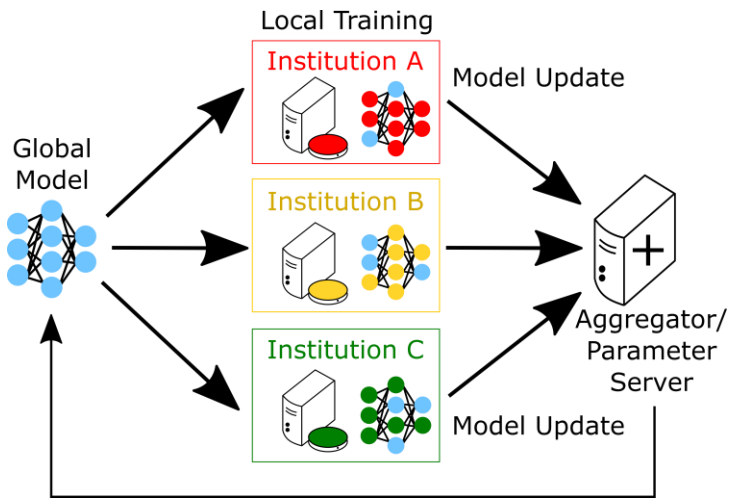
Perelman School of Medicine University of Pennsylvania

nature.com/articles/s41598-020-69250-1

https://www.linkedin.com/in/psfoley/
patrick.foley@intel.com

OpenFL

- Open-source software for a complete Federated Learning System Architecture
- Privacy preserved Machine Learning for Data/Model in transit, use and storage
- OpenFL is easy to use and scalable and manageable for large federations



License Apache 2.0

Keras

TensorFlow

PyTorch

OpenFL Solves the data silo problem with software that accelerates time to market deployment of Federated Learning. It provides the greatest access to data through enabling secure, privacy preserved data.

GitHub

github.com/intel/openfl

pypi

pip install openfl

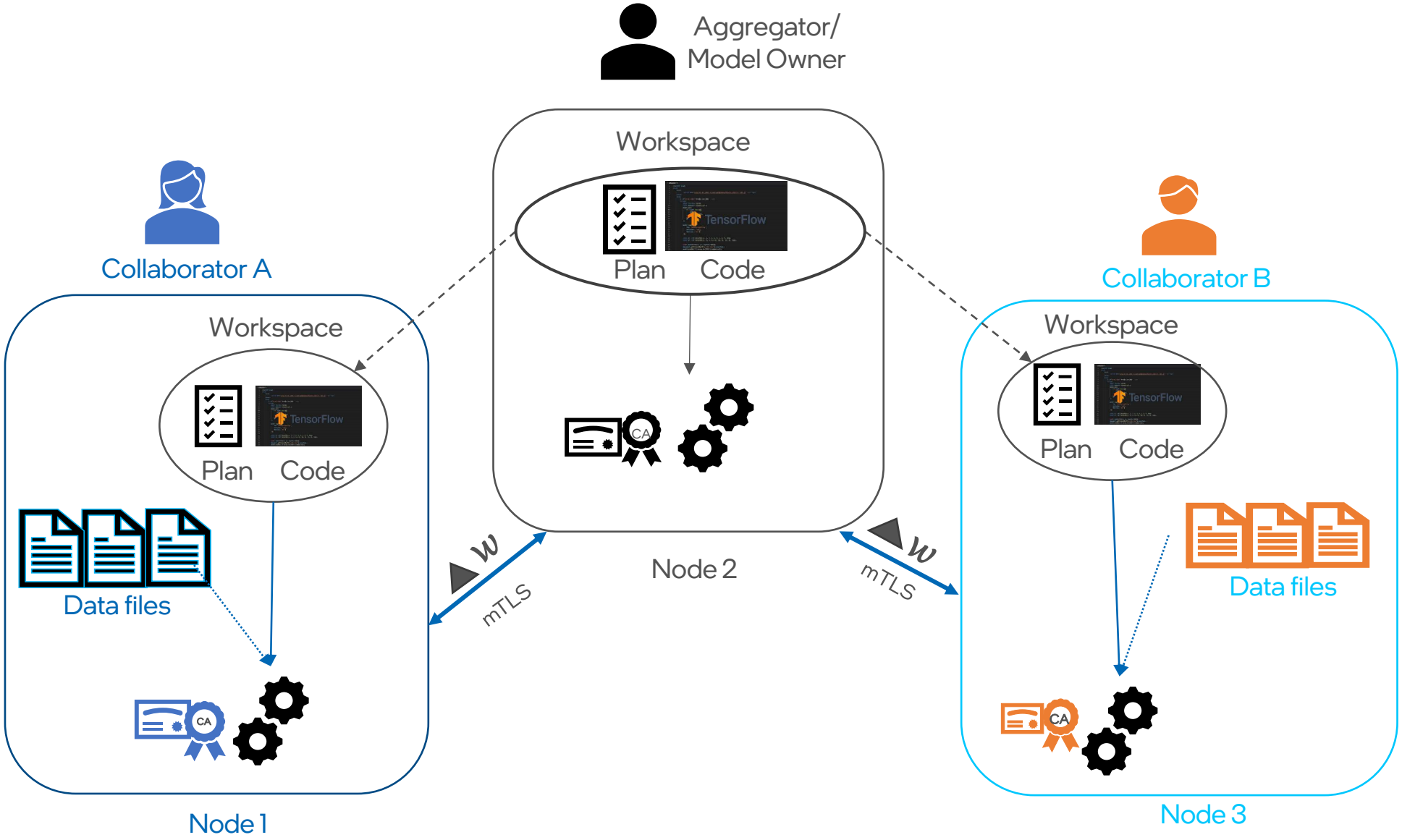
docker hub

docker pull intel/openfl

https://www.linkedin.com/in/psfoley/
patrick.foley@intel.com

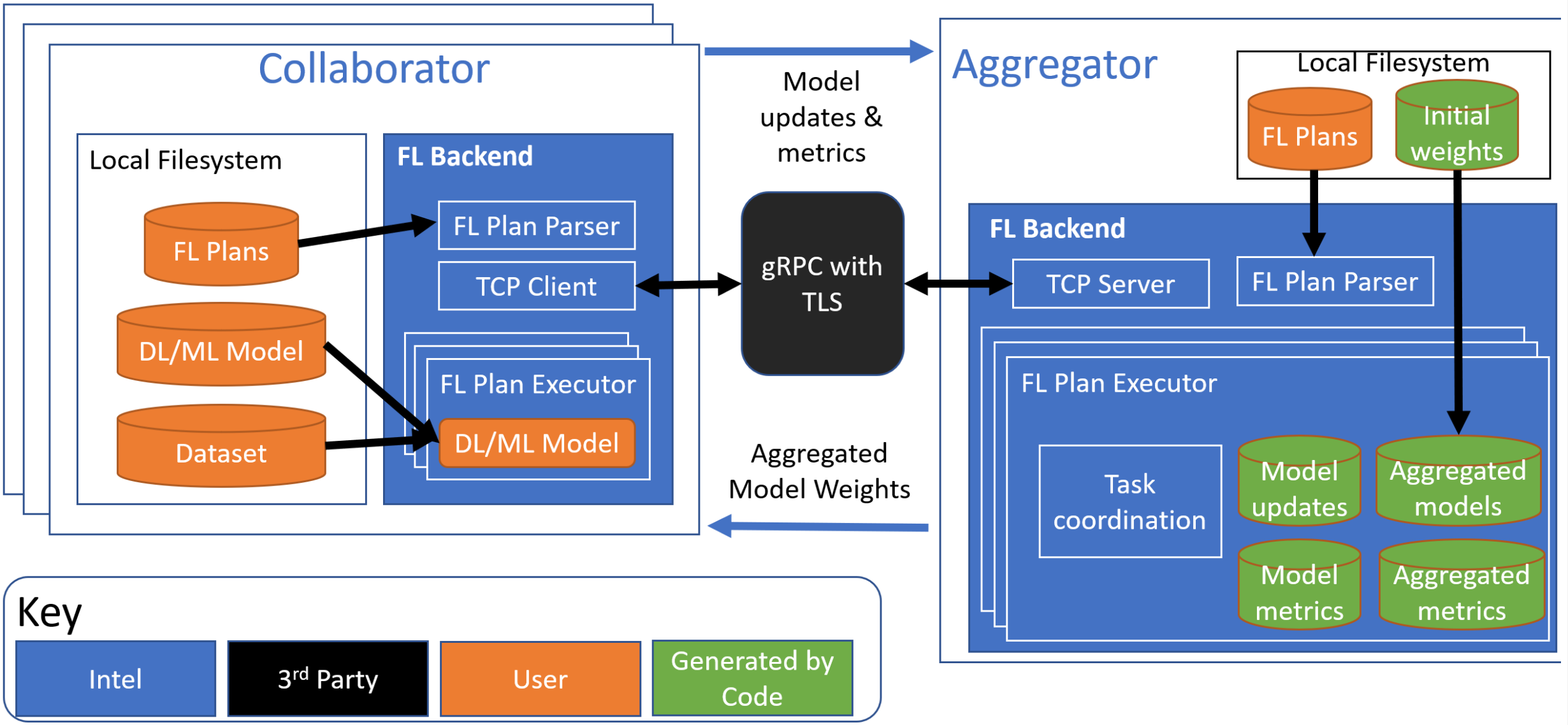
P. Foley, *et Int*, S. Bakas, *Phys Med Biol*, 67(21):214001, 2022

OpenFL Architecture



https://www.linkedin.com/in/psfoley/
patrick.foley@intel.com

OpenFL Architecture (cont.)

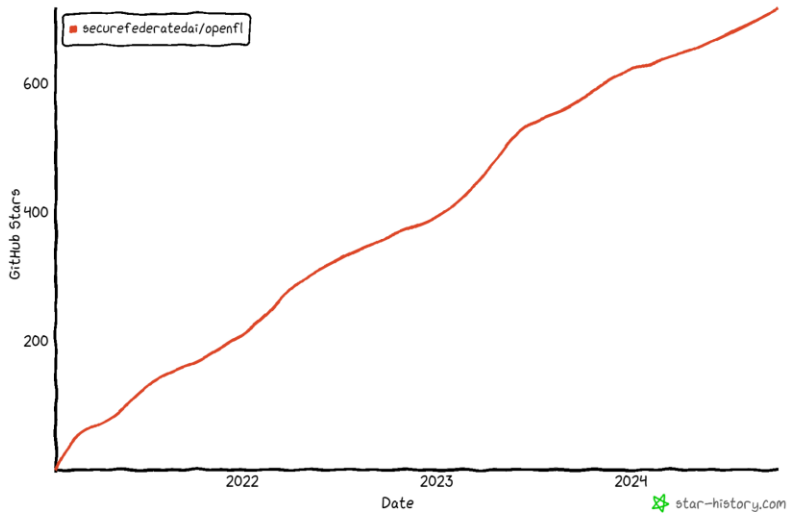


https://www.linkedin.com/in/psfoley/
patrick.foley@intel.com

OpenFL: progress summary

- **Intel Labs' & UPenn** initial research and contribution in 2018-2020
- **Public Release** on GitHub: Feb 1, 2021
- **7 major releases**: OpenFL 1.0 – OpenFL 1.6

Star History Statistics (10.04.2024)

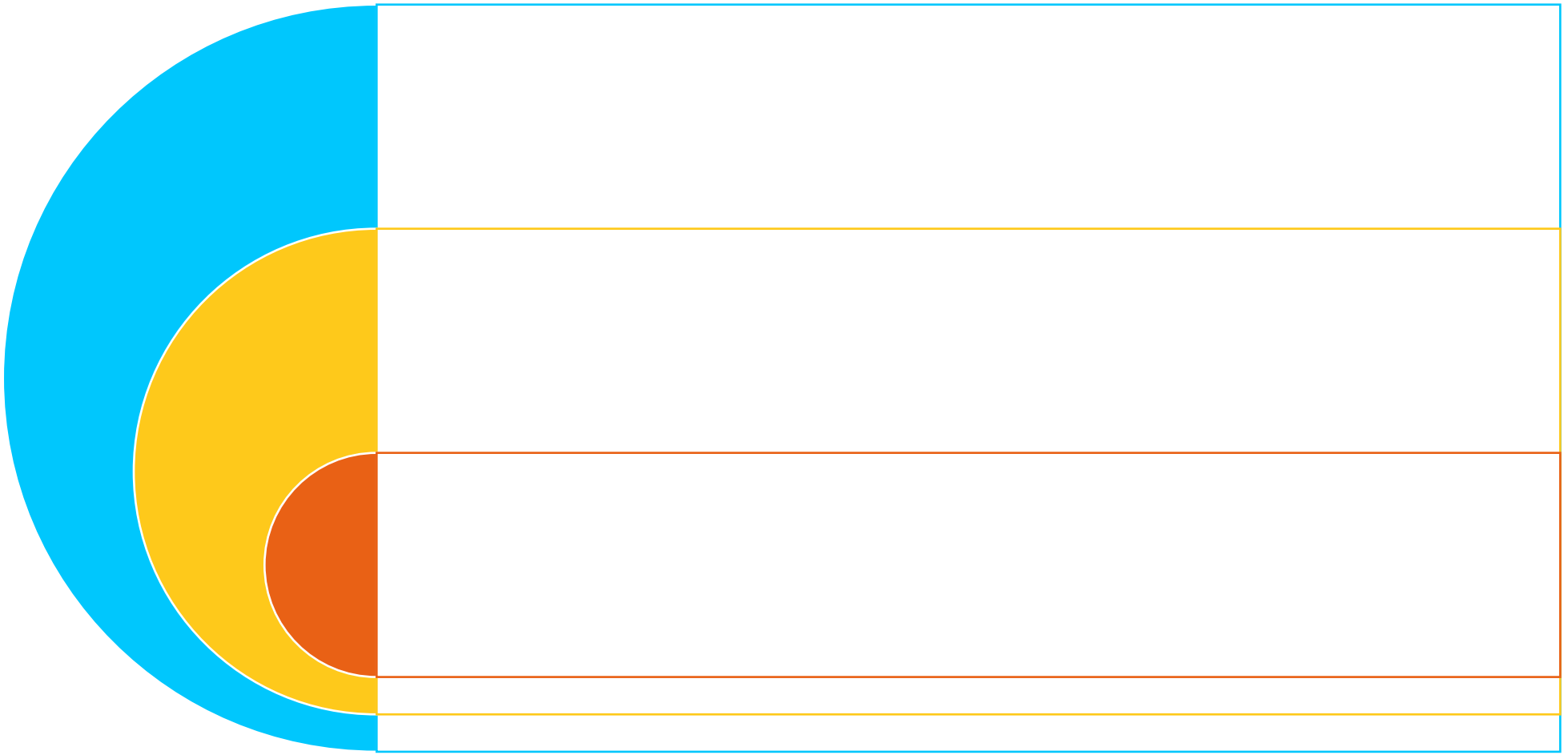


pypi Statistics (10.04.2024)

docker hub Statistics (10.04.2024)

https://www.linkedin.com/in/psfoley/
patrick.foley@intel.com

OpenFL core values



OpenFL 1.6: highlights

OpenFL: how to get started

OpenFL is distributed through GitHub, PyPI and Docker Hub

github.com/securefederatedai/openfl

pypi.org/project/openfl

pip install openfl

hub.docker.com/r/intel/openfl

docker pull intel/openfl

OpenFL supports all the popular machine learning frameworks

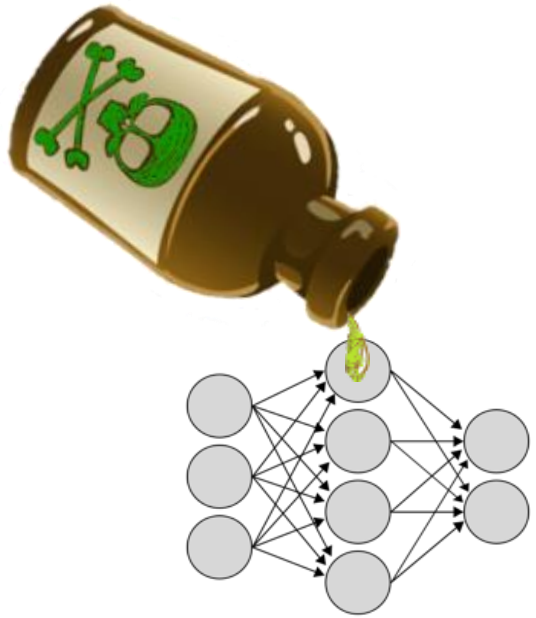
OpenFL Keras Tutorial

OpenFL PyTorch Tutorial

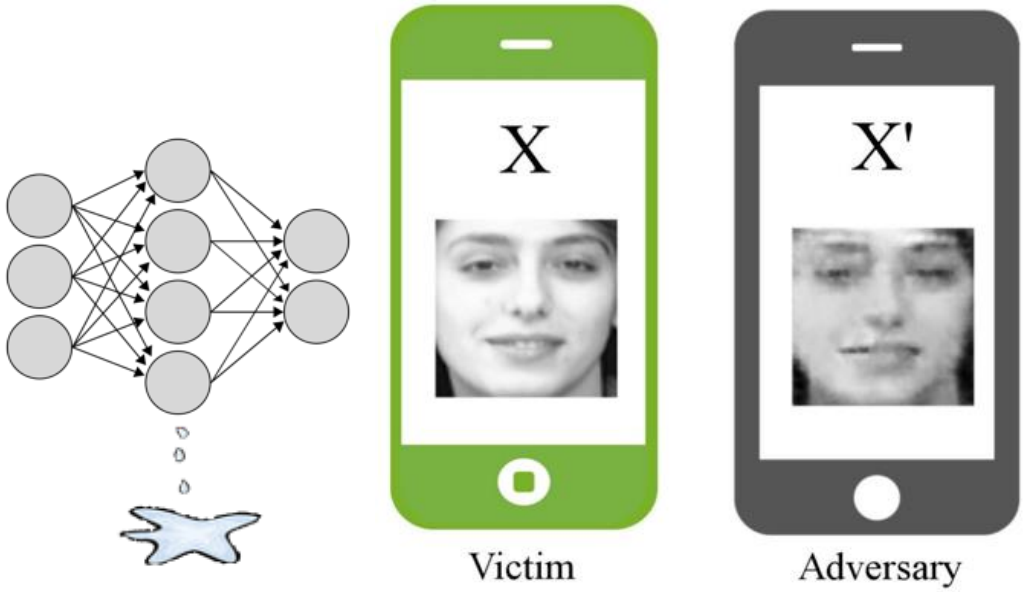
OpenFL documentation

https://www.linkedin.com/in/psfoley/
patrick.foley@intel.com

Security and Privacy Challenges



Poisoning attacks may maliciously alter models.



Extraction attacks recover training data from models.

Federated learning frameworks need to have additional **security** to manage these risks

https://www.linkedin.com/in/psfoley/
patrick.foley@intel.com

FL with Trusted Execution Environments

* Additional SGX Services needed to verify remote code integrity

Confidentiality

- Data never leave the premise of data owners.
- Model IP protected end-to-end in use and at rest.

Integrity & Attestation

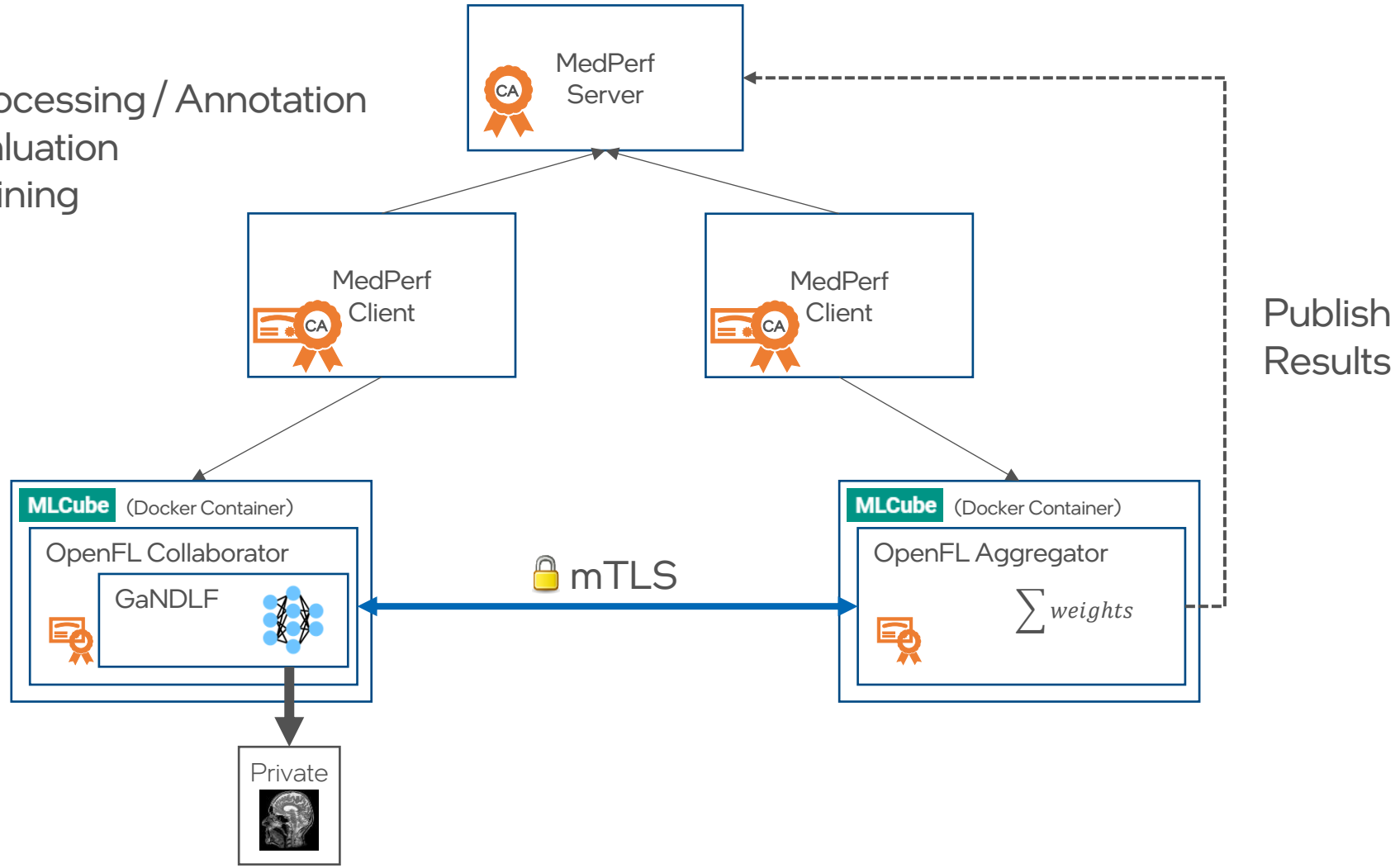
- Only verified and approved ML models.
- Participants can not insert unapproved code at any time.

Provides a mechanism to prevent stealing the model or reverse-engineering data distribution.

https://www.linkedin.com/in/psfoley/
patrick.foley@intel.com

How OpenFL / Medperf / GaNDLF connect

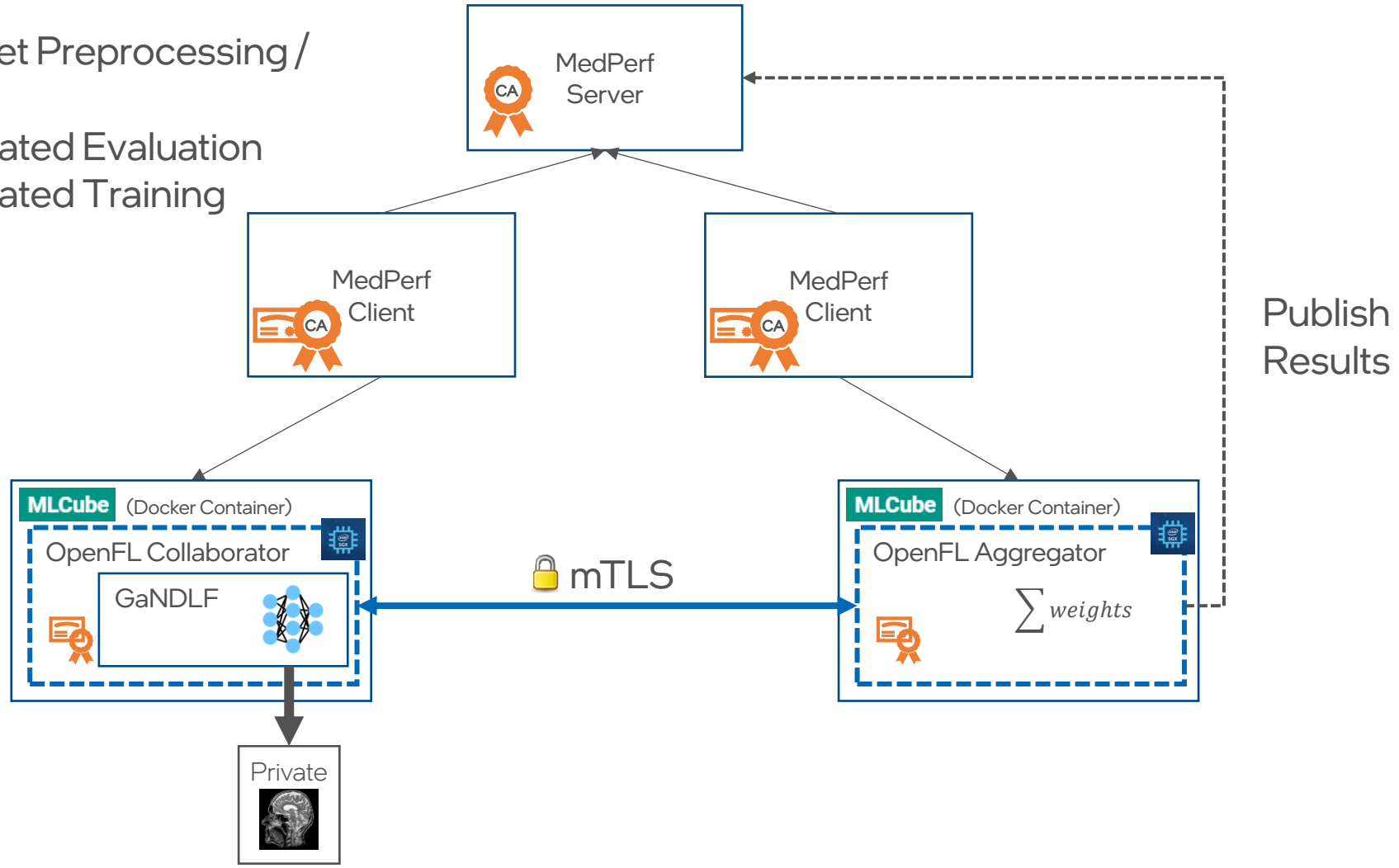
Enables:
- Dataset Preprocessing / Annotation
- Federated Evaluation
- Federated Training



https://www.linkedin.com/in/psfoley/
patrick.foley@intel.com

How do TEE's improve this system?

- **Verified** Dataset Preprocessing / Annotation
- **Verified** Federated Evaluation
- **Verified** Federated Training



https://www.linkedin.com/in/psfoley/
patrick.foley@intel.com

Who is using OpenFL?

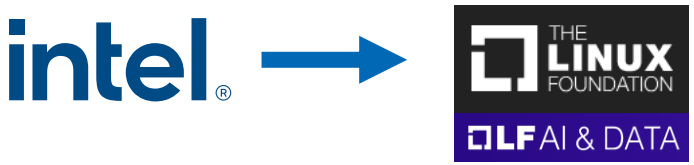
- University of Pennsylvania created the first real-life and largest federation of healthcare institutions.
- Federated Tumor Segmentation Challenge the first federated learning competition.
- Center for Federated Learning in Precision Medicine
  Looking into the incorporation of OpenFL for clinical trials
- Targeting large, persistent federations. Extends work from FeTS Initiative.

- Frontier Development Lab: NASA, Mayo Clinic and Intel used federated learning to understand the effect of cosmic radiation on humans
- NASA: with the FLUID project. OpenFL became the first FL Framework to run in space
- Montefiore used OpenFL to simultaneously tap data from multiple hospitals to predict likelihood of Acute Respiratory Distress Syndrome (ARDS) and Death in Covid-19 patients
- VMware used OpenFL for Microservices Applications and contributed EDEN, a new compression pipeline designed for federated learning, to OpenFL.

https://www.linkedin.com/in/psfoley/
patrick.foley@intel.com

How you can get involved

- Use OpenFL, contribute back!
  - github.com/securefederatedai/openfl
- OpenFL just moved to a new home at the Linux Foundation
  - Joined by *VMWare, Leidos, UPenn / IU, Flower Labs* in driving future of project
  - **Looking for active contributors of all skill levels!**
- OpenFL Contrib Repo
  - Community governed and contributed:
    - Aggregation algorithms
    - Compression algorithms
    - Experimental use cases and examples



https://www.linkedin.com/in/psfoley/
patrick.foley@intel.com

github.com/securefederatedai/openfl

bit.ly/2MKAyAv