2024 embedded VISION SUMMIT®

Federated ML Architecture for Computer Vision in the IoT Edge

Akram Sheriff

Senior Engineering Manager AI_ML Engineering

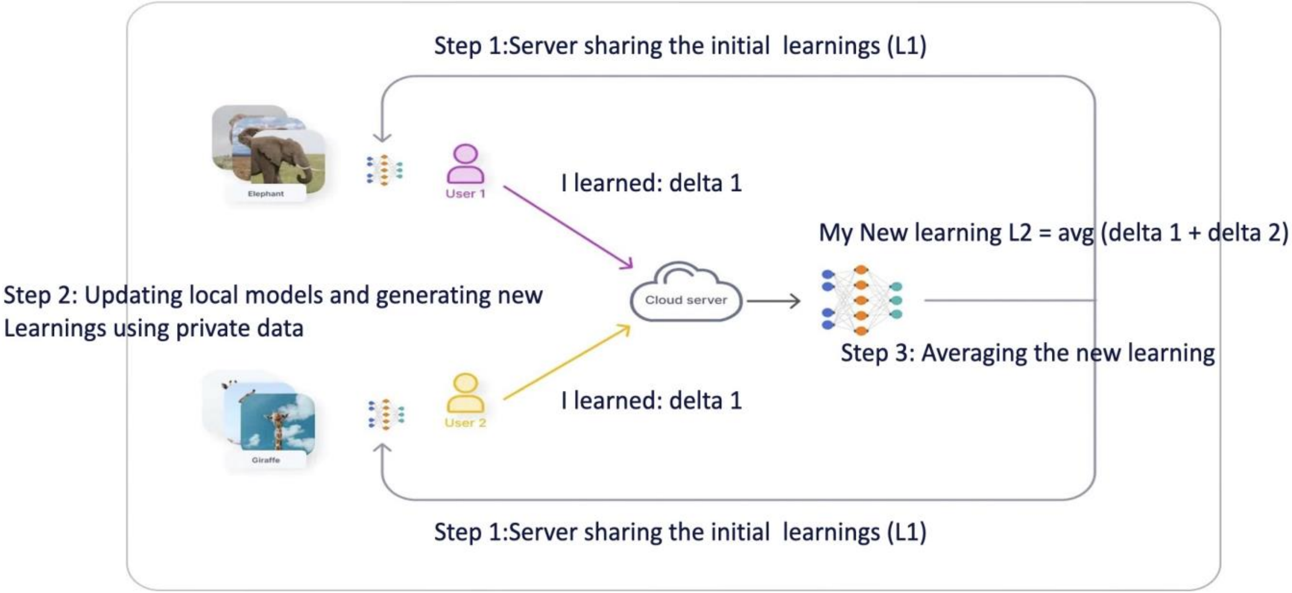
Cisco Systems

Agenda

- Introduction to federated learning in computer vision
- Federated learning architectural patterns for deployment
- Existing federated learning architectural challenges in computer vision
- Proposed federated learning with hybrid models for computer vision use cases
- Advantages of the proposed approach and merits of the architecture
- Real world example of federated learning in healthcare computer vision use case.
- Summary and key takeaways

Introduction to Federated Learning in Computer Vision

- Federated learning involves multiple nodes collaboratively training a model in a distributed manner.
- Federated learning normally involves a decentralization of the data by the nodes.



Step 1:Server sharing the initial learnings (L1)

I learned: delta 1

My New learning L2 = avg (delta 1 + delta 2)

Step 2: Updating local models and generating new Learnings using private data

Step 3: Averaging the new learning

I learned: delta 1

Step 1:Server sharing the initial learnings (L1)

Illustration of FL in Computer Vision use case

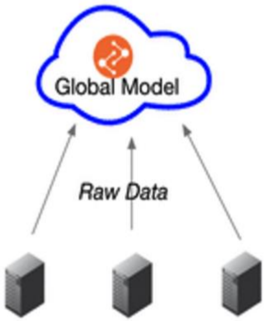
Federated Learning Architectural Patterns for Deployment

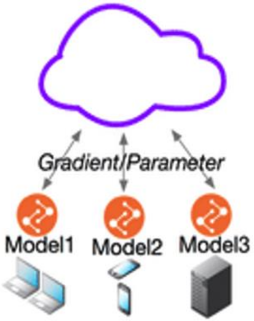
a) Centralized/global federated learning

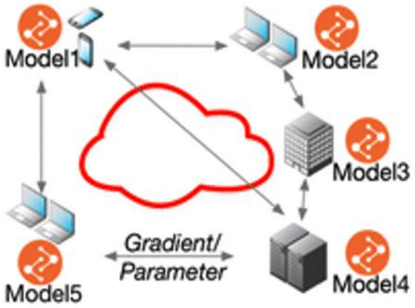
b) Cloud-based distributed federated learning

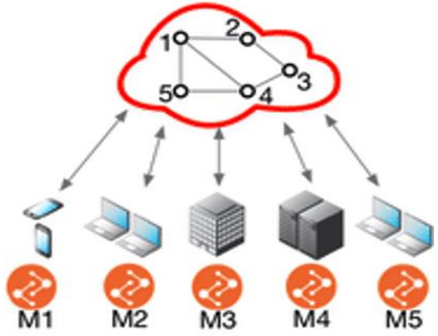
c) Decentralized federated learning

d) Multi-task with de-centralized parameter exchanging federated learning



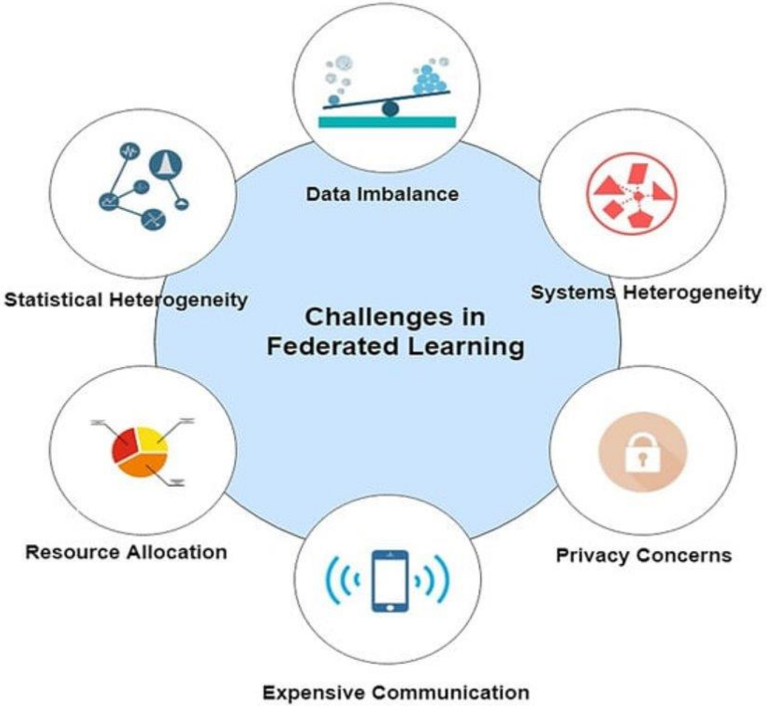






Existing Federated Learning Challenges in Computer Vision (CV)

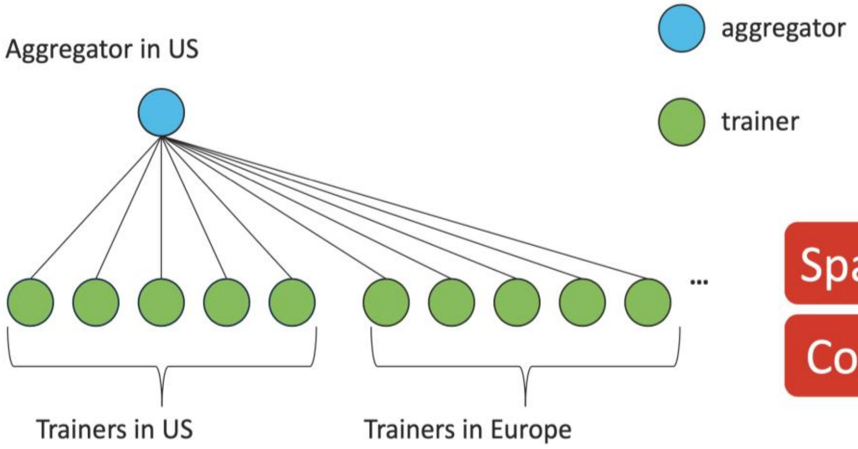
- Unbalanced local datasets:
- Statistical differences in datasets:
- Larger number of worker nodes:
- Heterogeneous Network connectivity:
- Heterogeneous Computer power:
- Data Privacy Concerns



More Challenges

- For computer vision/CV tasks such as object detection the size of model would be large.
- Data Aggregation, Data sovereignty and Data provenance issues.
- Spatial Data Heterogeneity across the Training Nodes.

Classical FL Topology



Spatial Data Heterogeneity

Communication Overhead

Proposed Federated learning with Hierarchical FL for Computer Vision(CV) with FedCV framework

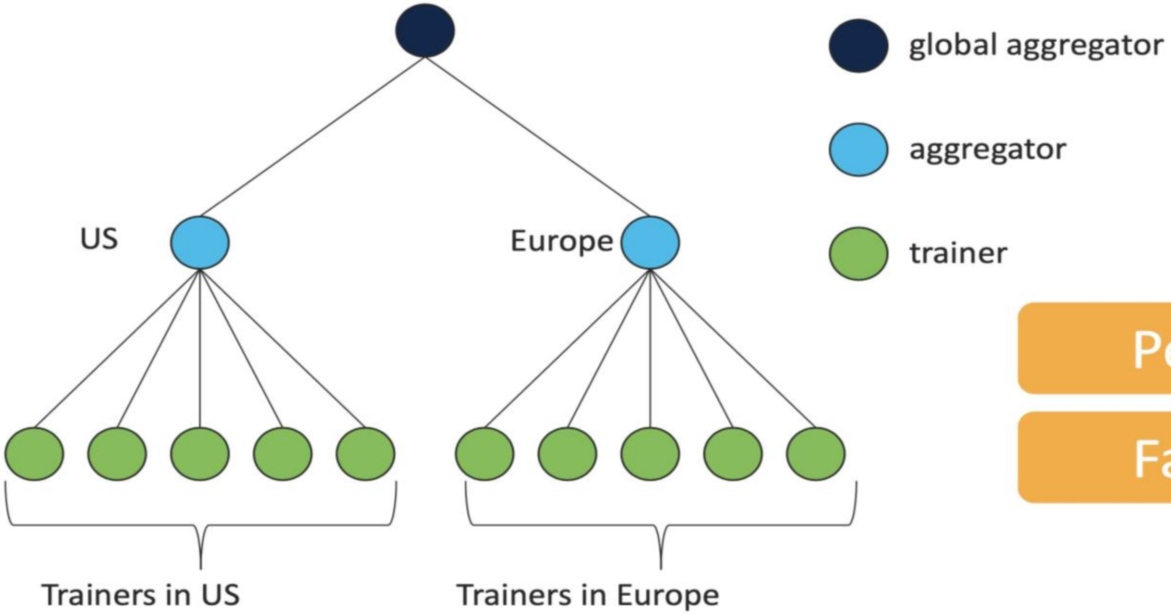
- FedCV framework is FL topology, architecture variants agnostic.
- Ease of use FedCV API's
- FedCV is a distributed training toolkit for analysis, benchmarking, library and platform for executing CV applications.
- FedCV helps in bridging gaps between SOTA algorithms and facilitating the development of different variant of FL techniques.
- FedCV reduces engineering development effort with multiple embedded features.

Proposed Hierarchical FL Technique

Proposed Hierarchical FL learning layer has the following advantages

- By doing the learning in these smaller Micro-batches based training.
- Nodes then perform small batches of training on their local data.
- Periodically, each training node submits ML model parameter/weight updates to the central node.
- Holistic view during FL based model weights update and convergence.
- This process can either take place indefinitely or be repeated until the FL model converges with respect to some evaluation metric (e.g., mean average error, accuracy).

Proposed Hierarchical FL Topology



Personalized Model

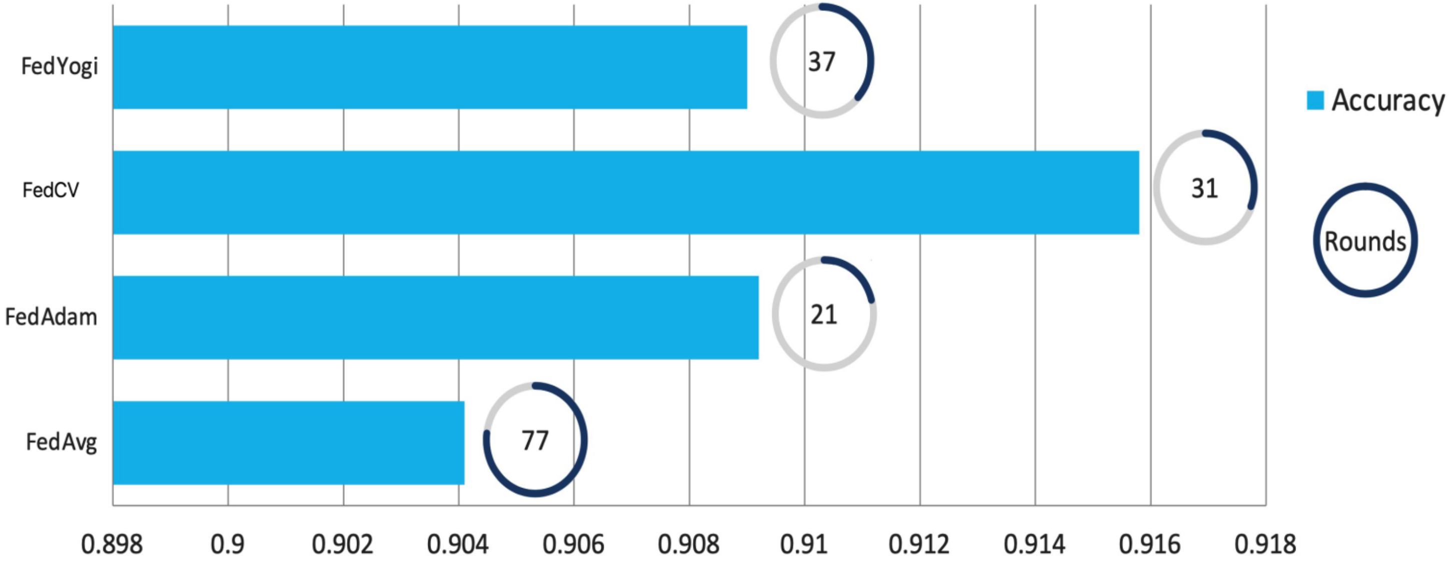
Faster Convergence

Advantages

- Multi node and Multi layered architecture with FL technique.
- Failure of operation of FL architecture is minimal
- CV application context and data specific significance given to the creation of FL weights.
- Tree based Hierarchical FL improves the convergence performance.
- The location of aggregator nodes need not be pre-determined in an H-FL architecture which gives flexibility
- Network Topology specific routing of incoming inferencing API requests.
- No fixed location of aggregator and Non-aggregator nodes.
- Aggregator nodes may be dynamically placed within the network to improve model accuracy and execution performance.

Performance Improvements Results — FedCV based Training and Evaluation

Results



Rounds: # of rounds to >90% test accuracy.

Federated Learning in Healthcare — Real world usecase

Problem:

Medical data and Healthcare vertical faced insurmountable hurdles with patient privacy concerns, data silos, and ethical issues.

Solution:

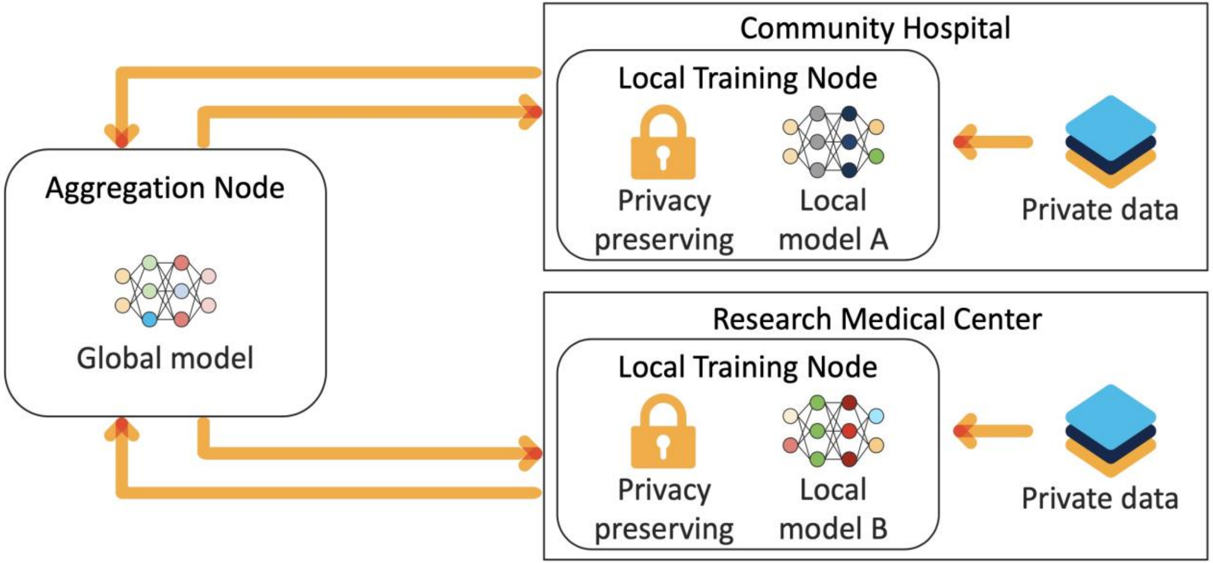
- Federated learning empowers individual devices and institutions to collaboratively train AI models.
- Federated learning offers network of hospitals, each holding unique clinical datasets.
- Patient privacy, Data sovereignty, Data lineage ensured with FL

Advantages of Federated Learning in Healthcare:

- FL could be used to provide Targeted Precision medicine for a Patient to cure from Fatal diseases.
- Patient's privacy ensured but at the same time real time data collected and monitored locally in a FL architecture.
- Country, Region specific Medical data Compliance could be achieved with FL architecture.
- FL scalable across a Global chain of Hospitals, Medical research Institutions with data loss and ensuring data Privacy.
- Democratization of Vaccine and Medical IP to enable low cost medicine in a specific region/Country.

Federated Learning in Healthcare — Reference Architecture

Real-world Example in Healthcare



Summary and Key Takeaways

- Federated learning (FL) is a decentralized approach to training machine learning models.
- Federated learning gives advantages of privacy protection, data security, and access to heterogeneous data.
- Federated learning architectural paradigm complies with data sovereignty norms.
- Federated learning with good architectural patterns can be used for CV use cases.
- Selection of the right FL software framework (FedCV), API's, hierarchical architectural design pattern is important for CV use case.
- Ongoing research and industry work in the intersection of FedCV based FL techniques and LLM's to build different Multi-modal LLM applications.

References

A Field Guide to Federated Optimization
https://arxiv.org/abs/2107.06917

Optimization in Federated Learning
https://ceur-ws.org/Vol-2473/paper13.pdf

Reddi, S. et al. Adaptive Federated Optimization. Arxiv (2020)
https://openreview.net/forum?id=LkFG3lB13U5

https://www.v7labs.com/blog/federated-learning-guide

https://arxiv.org/pdf/2308.13558.pdf

https://github.com/OliverStoll/Anomaly-Detection-IIoT

https://github.com/izakariyya/testbed-fl-iot

https://github.com/FedML-AI/FedIoT

https://github.com/topics/federated-learning

https://github.com/qub-blesson/FedAdapt

https://github.com/qub-blesson

Thanks (Q&A)