# Federated Black-Box Adaptation for Semantic Segmentation

Jay Paranjape
Shameema Sikder
S. Swaroop Vedula
Vishal M. Patel

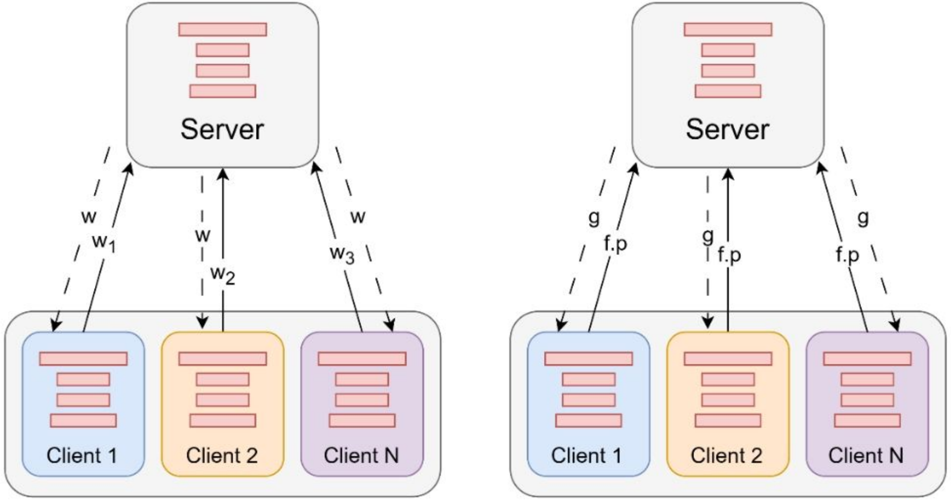
# Federated Learning (FL) - Concept

- FL refers to collaborative learning efforts between centers without explicitly sharing data
- Goal - Learn from data from all centers to maximize performance
- Setup usually consists of N centers and 1 server to aggregate the information

# Traditional Federated Learning

1) Client trains own model, shares weights. Server aggregates weights and sends them back

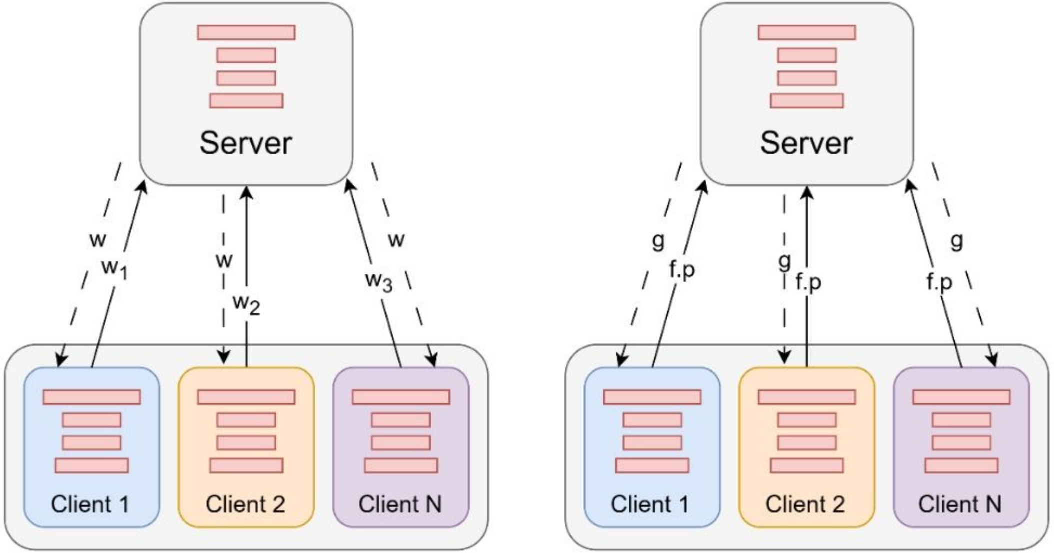
2) Client performs part of the computation. Server finishes the rest, sends gradient back to each client. Server model common among all centers.



Traditional FL
eg. FedAvg

FL with Vanilla Split-nn
(Whitebox)

# Traditional Federated Learning

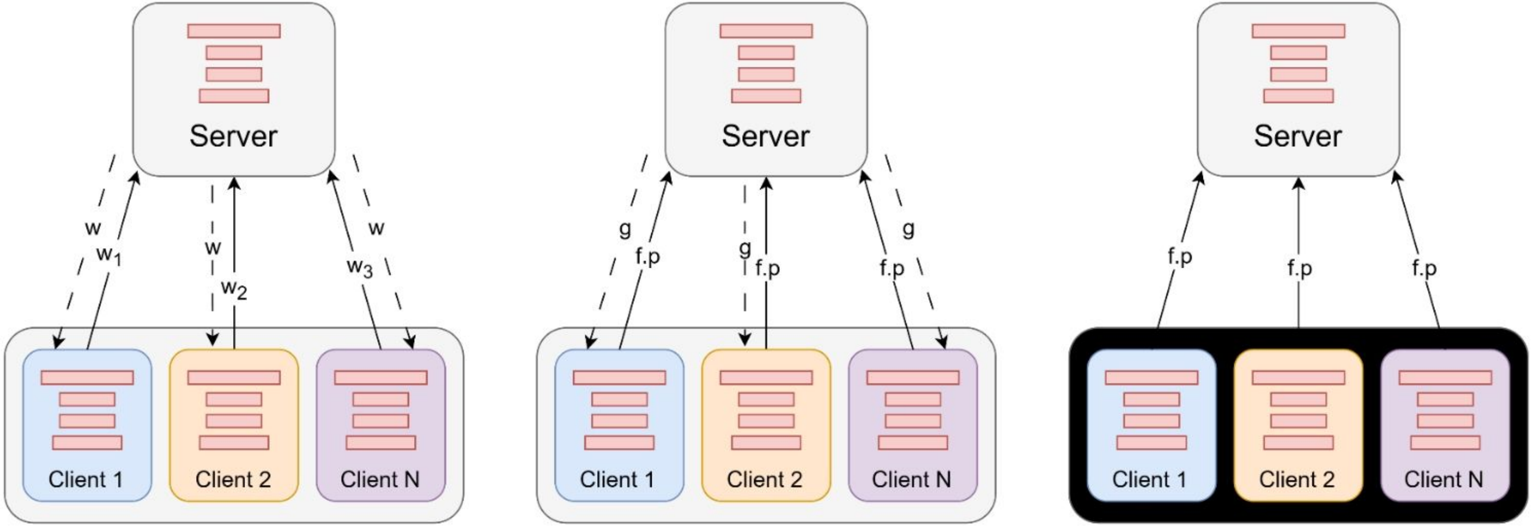


Traditional FL
eg. FedAvg

FL with Vanilla Split-nn
(Whitebox)

Weight Sharing ← Can be Attacked → Gradient Sharing

# BlackFed - Proposed Method



Legend

$w_i$ - client weights

w - aggregated server weights

g - gradients

f.p - forward pass

Traditional FL
eg. FedAvg
Weight Sharing

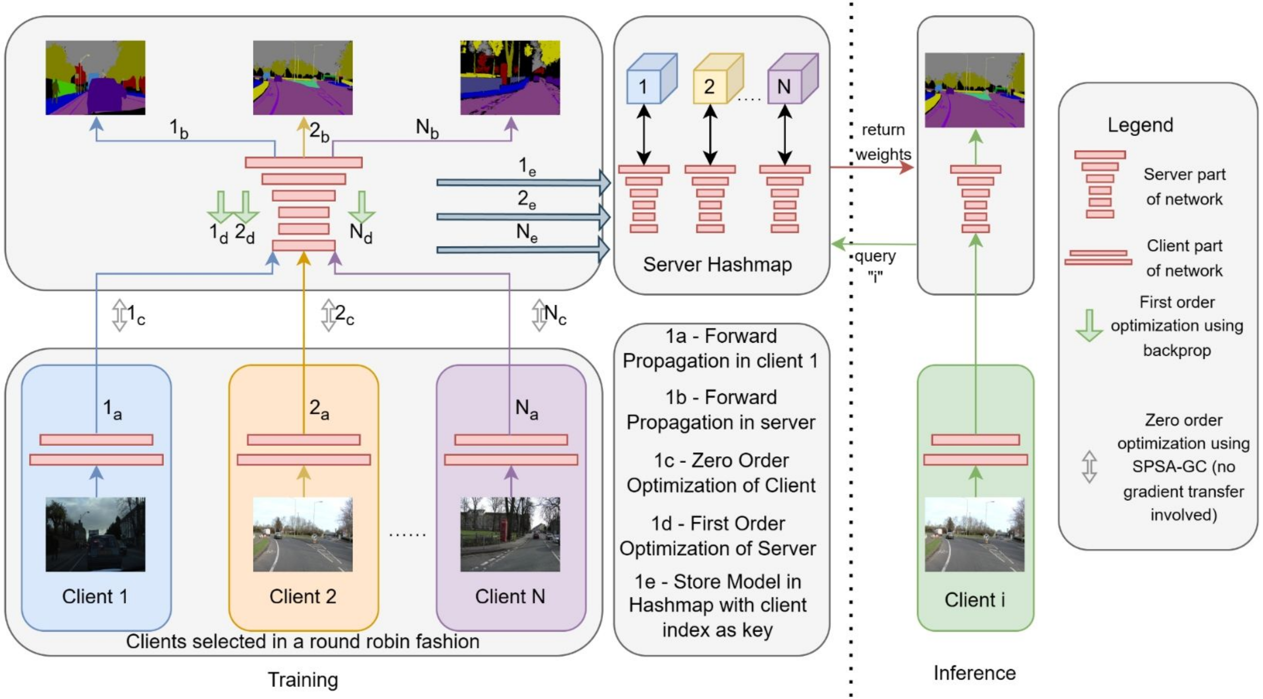
Can be Attacked

FL with Vanilla Split-nn
(Whitebox)
Gradient Sharing

BlackFed (Ours)
(Blackbox)
No Weight Sharing
No Gradient Sharing

# Method

- Select client in round robin fashion
- Update client weights
- Update server weights
- Store server weights in a hashmap indexed by client index. (prevents catastrophic forgetting)
- During inference, get the correct weights, run client and server.



1a - Forward Propagation in client 1

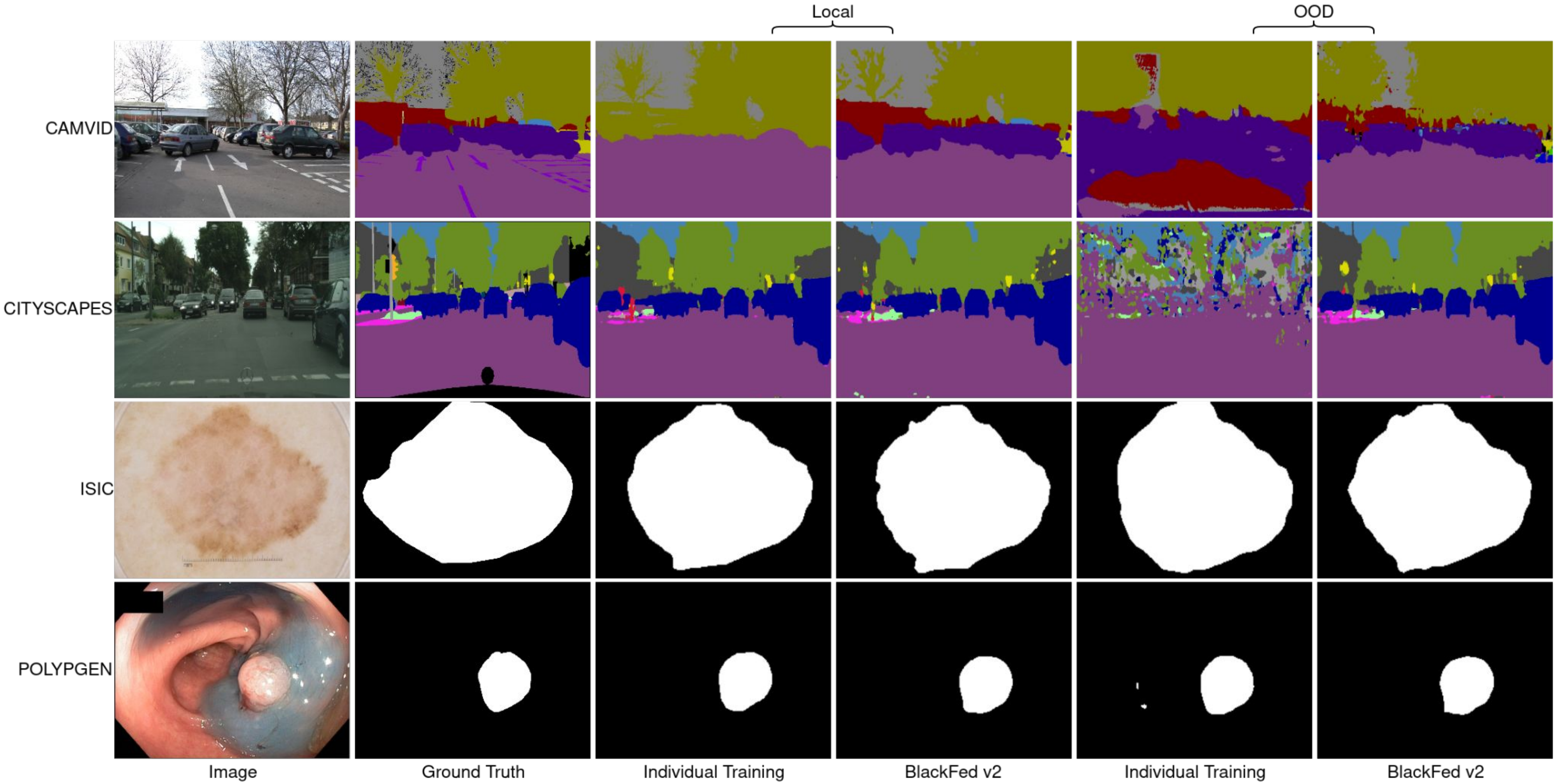
1b - Forward Propagation in server

1c - Zero Order Optimization of Client

1d - First Order Optimization of Server

1e - Store Model in Hashmap with client index as key

# Results


Local
OOD
CAMVID
CITYSCAPES
ISIC
POLYPGEN
Image
Ground Truth
Individual Training
BlackFed v2
Individual Training
BlackFed v2

# Thanks!

Please reach out for further questions and comments