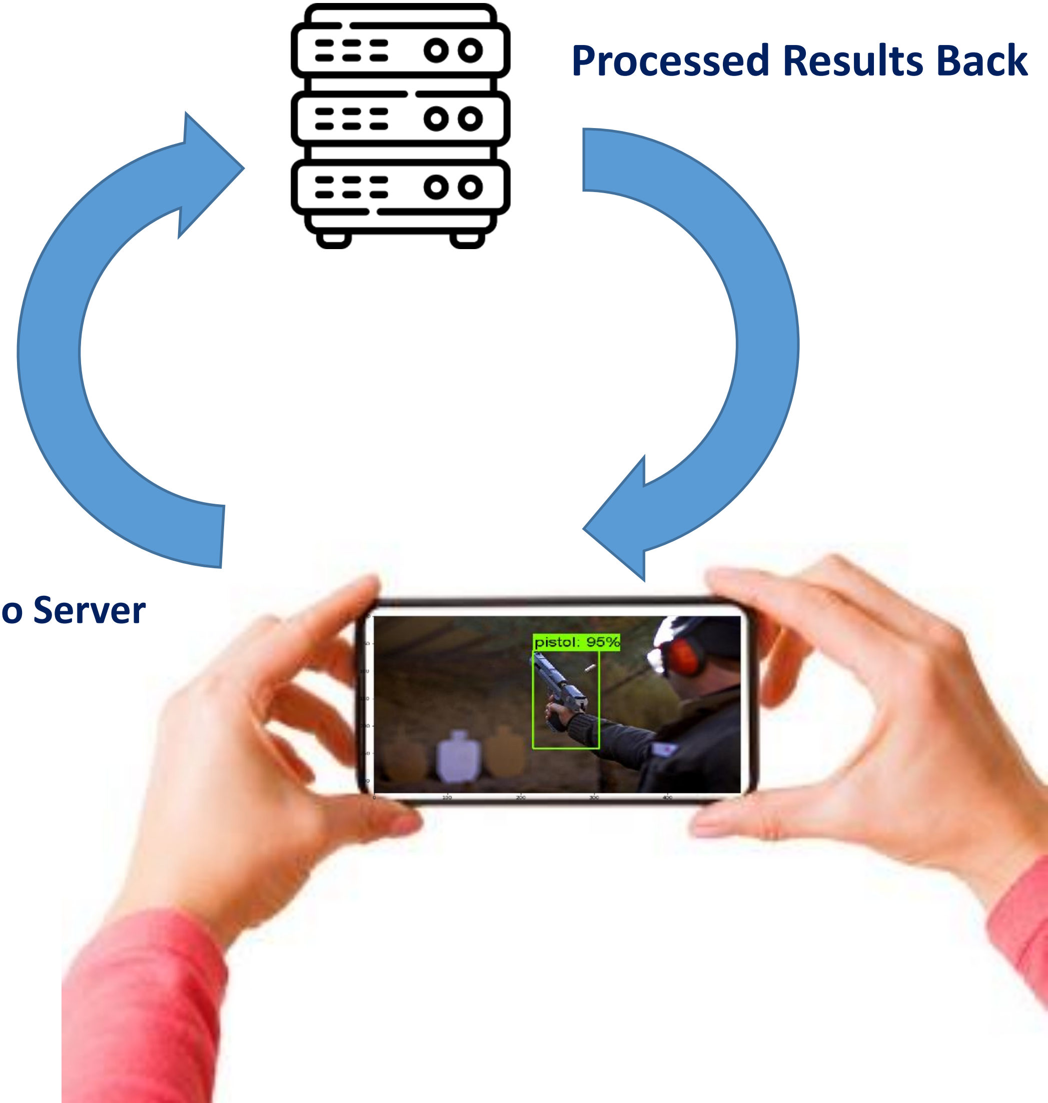
Introduction to Federated Learning

Tools & Techniques for Data Science

Course Instructor: Dr. Farrukh Hasan Syed

Conventional Methods Widely Adopted

- We usually keep our models on main server
- We usually experience applications with **I/O capabilities**
- All model are deployed on centralized server usually
- Data can often be highly private and sensitive



Processed Results Back

Data (Frame) is sent to Server

International Organizations Earning

The Professional Companies using the Cloud Based Services:

www.viAct.ai

The company is providing cloud based accident detection services to the clients.

https://www.intelli-vision.com/intelligent-video-analytics/

AI-Based Video Analytics

www.eyedius.com

Eyedius Smart Security System receives images from the RTSP (Real-time stream protocol) band

https://smartsentry.ai/

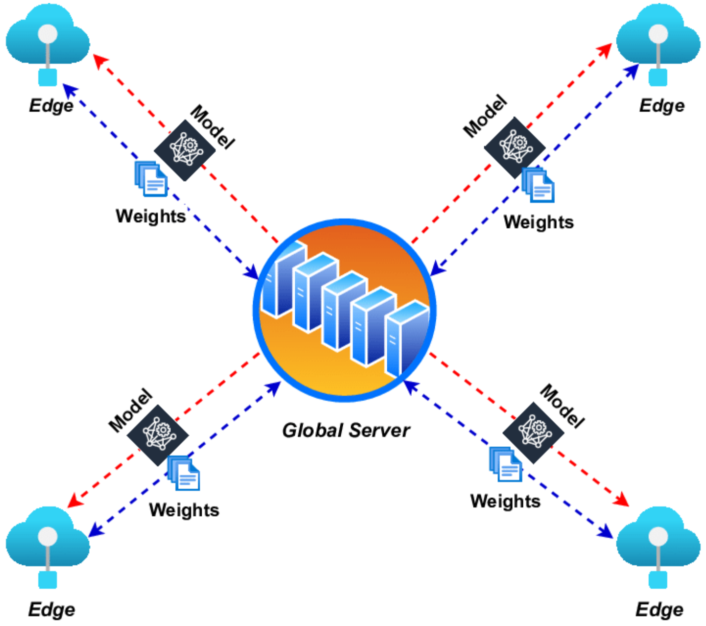
Connect your system now with our seamless integration. Mentioned about SMTP/ONVIF protocols.

In Federated Learning …

- Trained a model locally on individual device without having training on central server

- Its decentralized learning completely, Your data and model right on the device

- User data is never sent to the server ensuring the security



Collaborative Learning without Centralized Training Data

- The data used to train the model on device never leaves the device
- The weights, biases and parameters leave only
- The new parameters are pruned in the master model
- Server averages the individuals and do make the combined model
- The smart keyboard shows signs of Intelligence

How it Works ?

- Your Phone First Downloads a generic Machine Learning Model
- On basis of daily data, Your phone personalizes and improves the model and compute daily summaries
- These summaries are sent daily to the global model at night
- These provides the global improvement to the model without having a threat to data security

- Whenever we search for the specific things or place

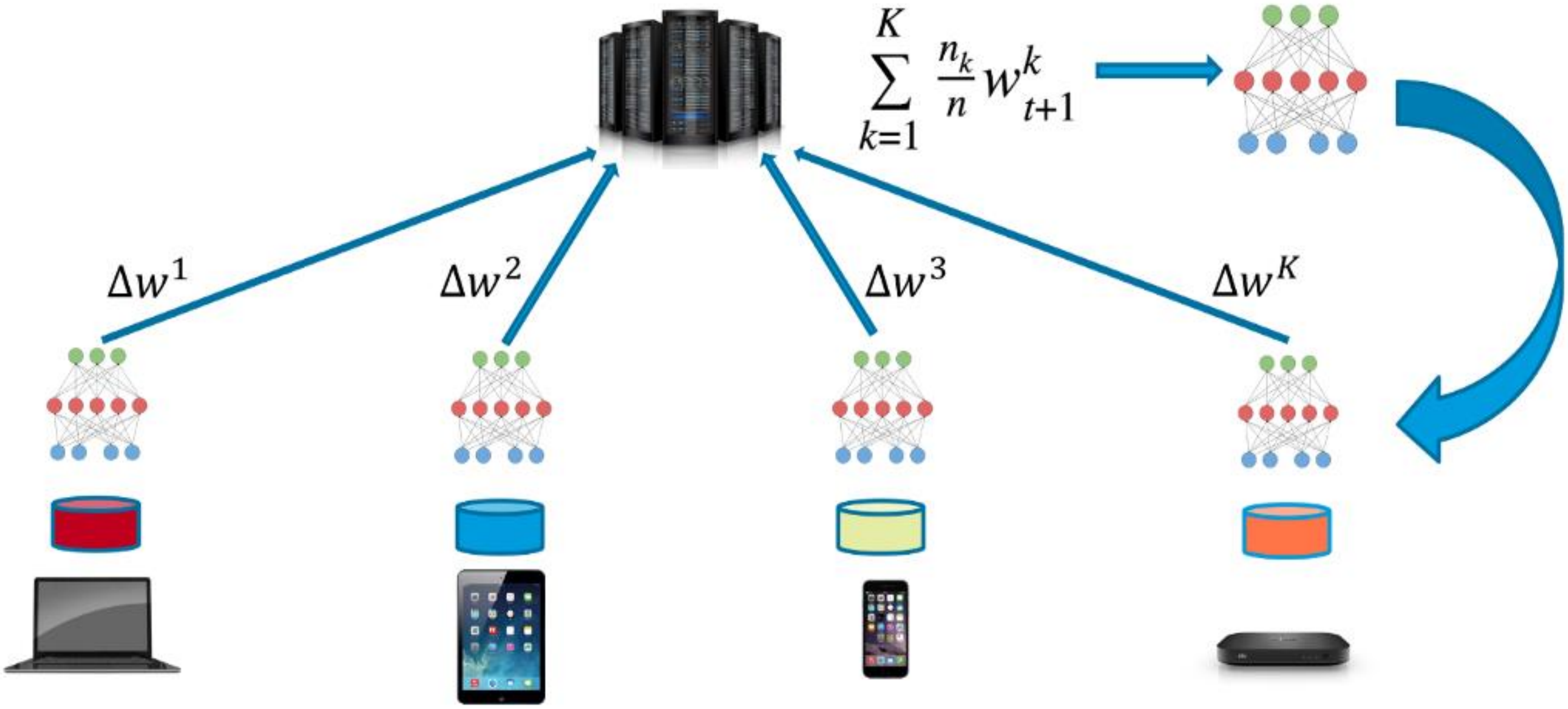
- The device stores the information locally and used it as suggestion for further

- No data is sent to the cloud, we send the models on device and models are trained on individual device

- The things sent on the server are the model updates (no the data)

- The global (combined) model auto updates itself

How it works?



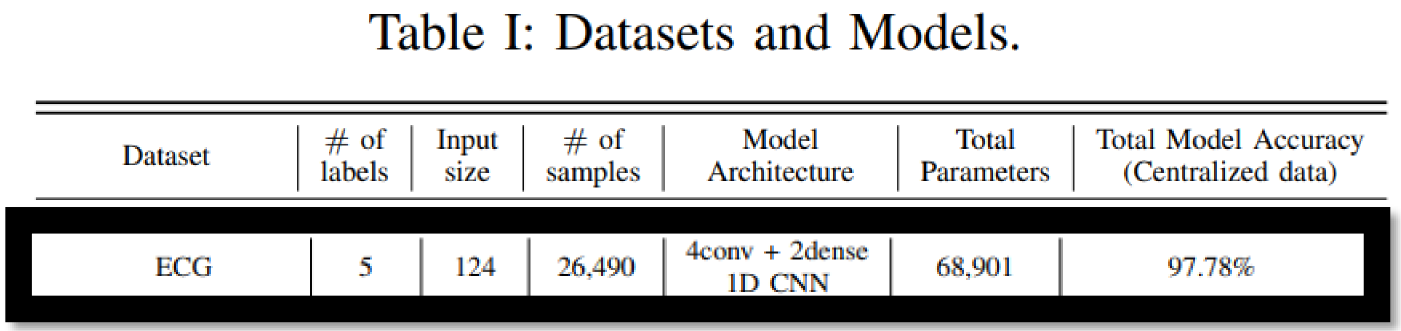
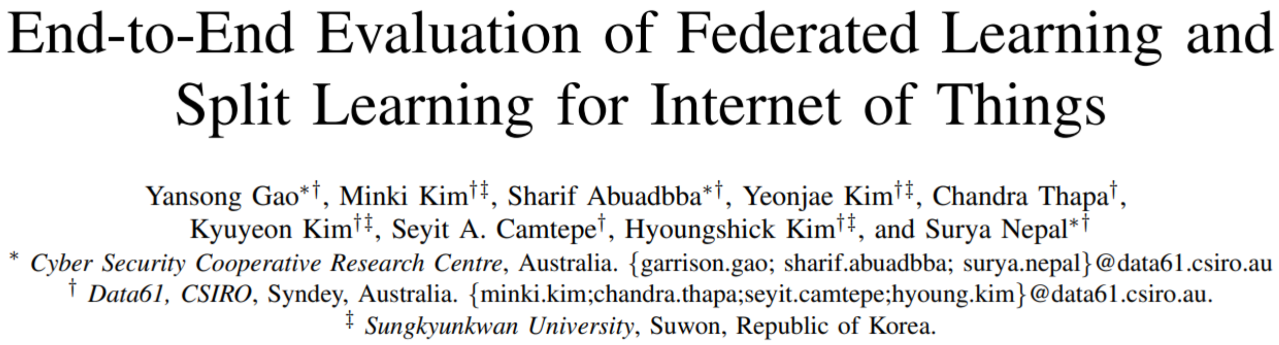


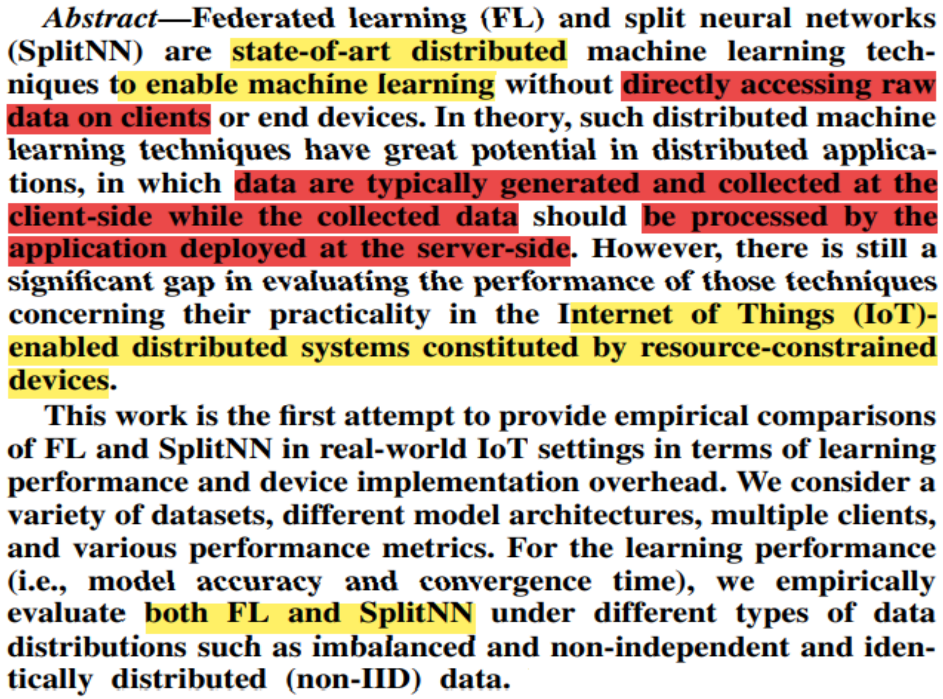
Table I: Datasets and Models.

Dataset	# of labels	Input size	# of samples	Model Architecture	Total Parameters	Total Model Accuracy (Centralized data)
ECG	5	124	26,490	4conv + 2dense 1D CNN	68,901	97.78%



End-to-End Evaluation of Federated Learning and Split Learning for Internet of Things

Yansong Gao*†, Minki Kim†‡, Sharif Abuadbba*†, Yeonjae Kim†‡, Chandra Thapa†,
Kyuyeon Kim†‡, Seyit A. Camtepe†, Hyoungshick Kim†‡, and Surya Nepal*†
* *Cyber Security Cooperative Research Centre*, Australia. {garrison.gao; sharif.abuadbba; surya.nepal}@data61.csiro.au
† *Data61, CSIRO*, Syndey, Australia. {minki.kim;chandra.thapa;seyit.camtepe;hyoung.kim}@data61.csiro.au.
‡ *Sungkyunkwan University*, Suwon, Republic of Korea.



***Abstract*—Federated learning (FL) and split neural networks (SplitNN) are state-of-art distributed machine learning techniques to enable machine learning without directly accessing raw data on clients or end devices. In theory, such distributed machine learning techniques have great potential in distributed applications, in which data are typically generated and collected at the client-side while the collected data should be processed by the application deployed at the server-side. However, there is still a significant gap in evaluating the performance of those techniques concerning their practicality in the Internet of Things (IoT)-enabled distributed systems constituted by resource-constrained devices.**

This work is the first attempt to provide empirical comparisons of FL and SplitNN in real-world IoT settings in terms of learning performance and device implementation overhead. We consider a variety of datasets, different model architectures, multiple clients, and various performance metrics. For the learning performance (i.e., model accuracy and convergence time), we empirically evaluate both FL and SplitNN under different types of data distributions such as imbalanced and non-independent and identically distributed (non-IID) data.

Courses Link:

Course 1:

Federated Learning at Udemy:

https://www.udemy.com/course/federated_learning/

Course 2:

Federated Learning at Coursera:

https://www.coursera.org/learn/advanced-deployment-scenarios-tensorflow/