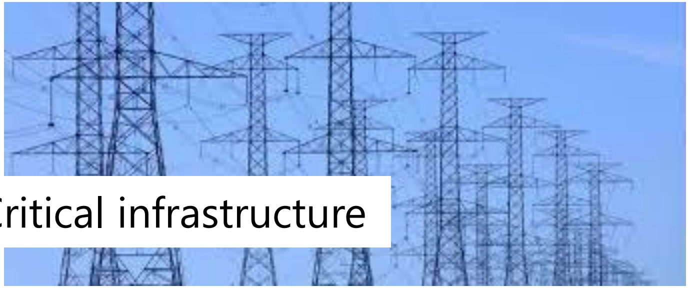
Secure Collaborative Learning for Predictive Maintenance in Optical Networks

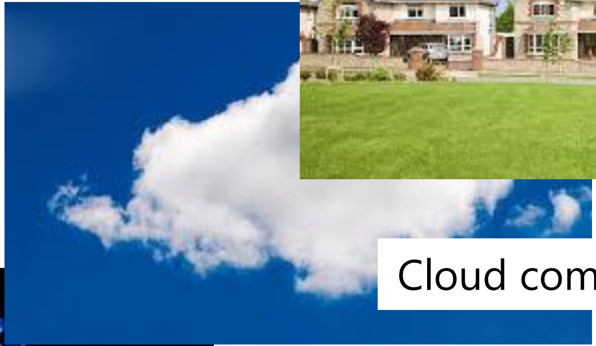
NordSec 2021

Khouloud Abdelli, **Joo Yeon Cho**, and Stephan Pachnicke

30. November 2021

Who Need Optical Networks?





Motivation

How can I estimate the risk of hardware failure?

Fixed optical network as basis for 5G functionality

Network blackout by fire (South Korea, 2018)

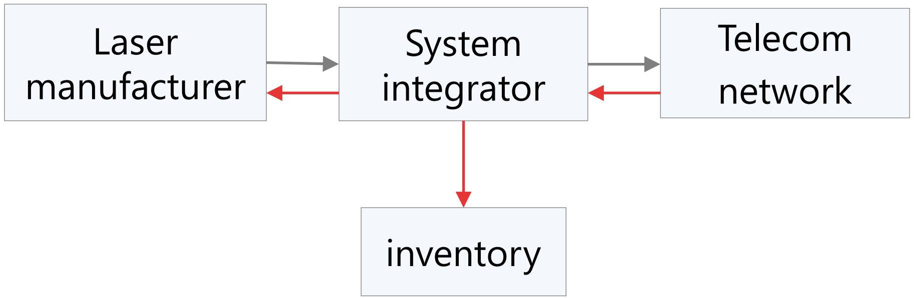
The fire broke out the Korean Telecom site in western Seoul on Saturday (24-Nov-2018), causing massive network damage there and in neighboring regions.

=> Services of mobile phone, restaurant, taxi, supermarket, ATM, hospital, online ordering, etc. were disrupted.

How to evaluate the risk?

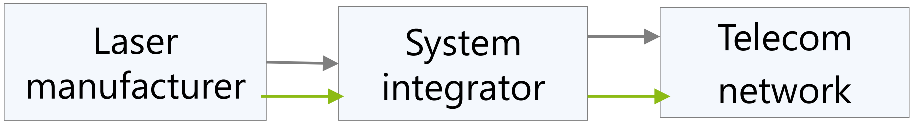
Example of laser manufacturer

Reactive Maintenance



After a hardware fault occurs, the replacement process begins.

Predictive Maintenance



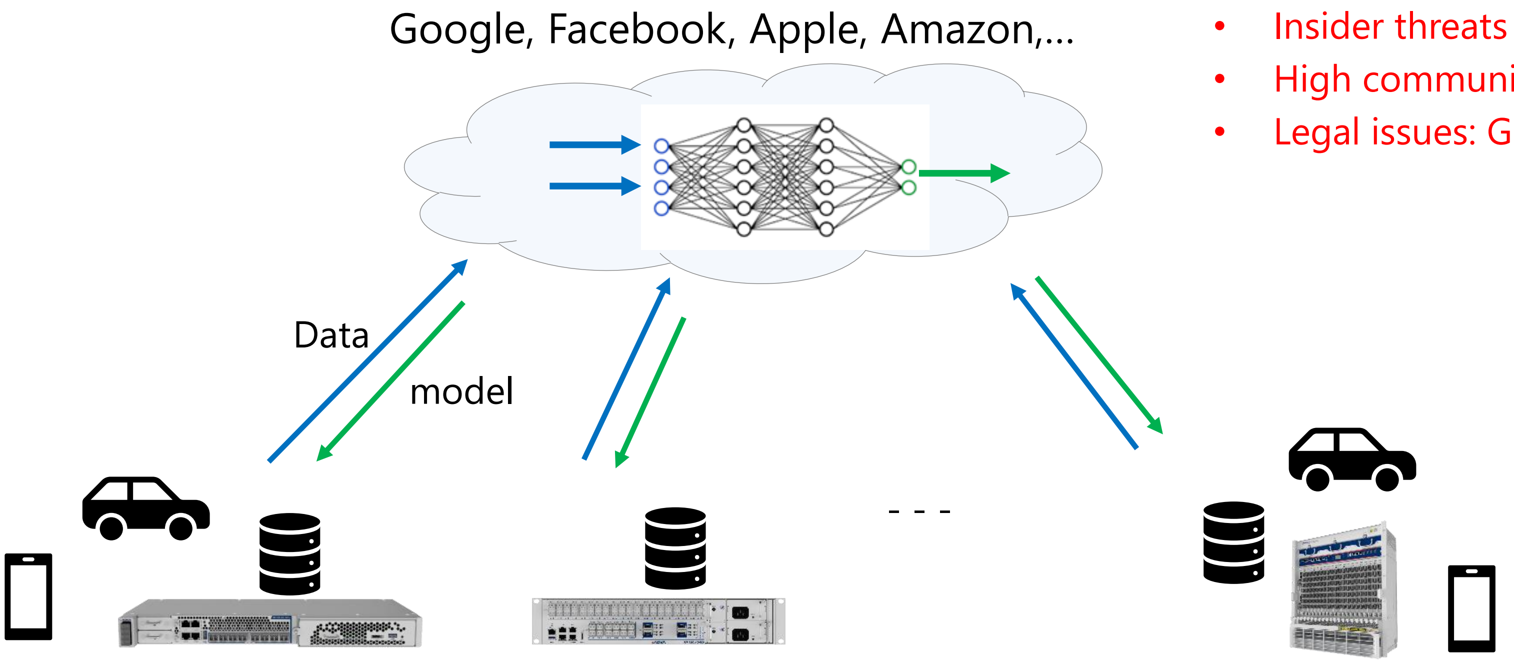
Before a hardware fault occurs, the replacement is prepared.

Minimizing the unplanned downtime and outage of services

PM in the Cloud: Amazon Monitron, Google,…

Global predictive maintenance market is expected more than $13 billion by 2026.

Centralized Machine Learning

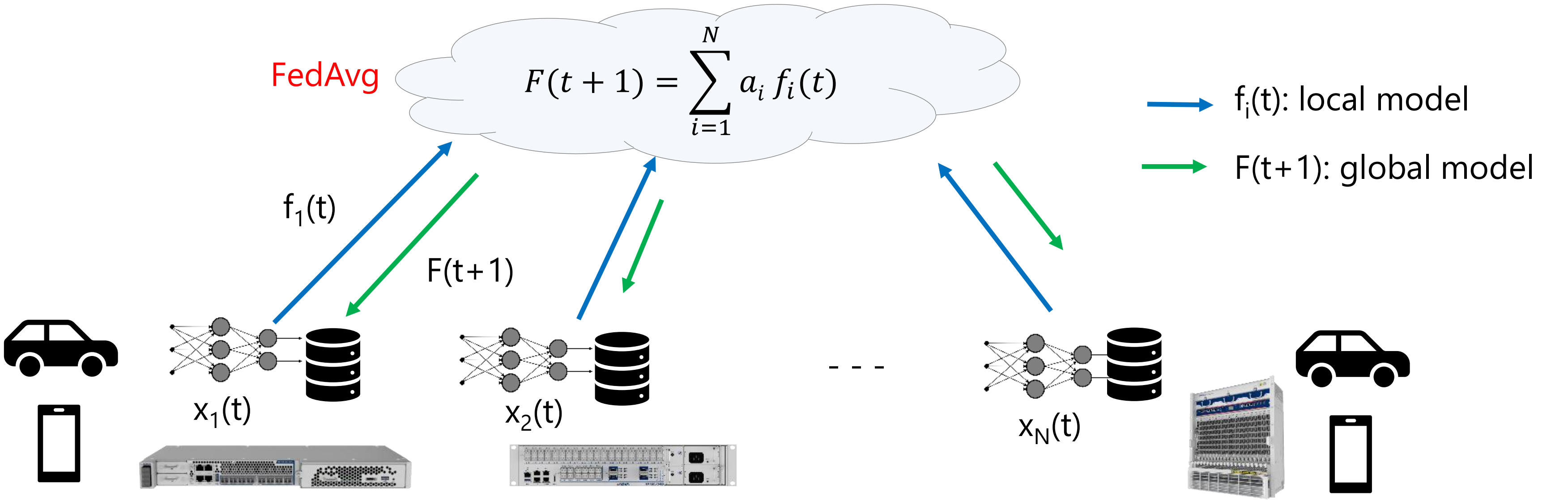


- Data breaches
- Insider threats
- High communication cost
- Legal issues: GDPR,CCPA,...

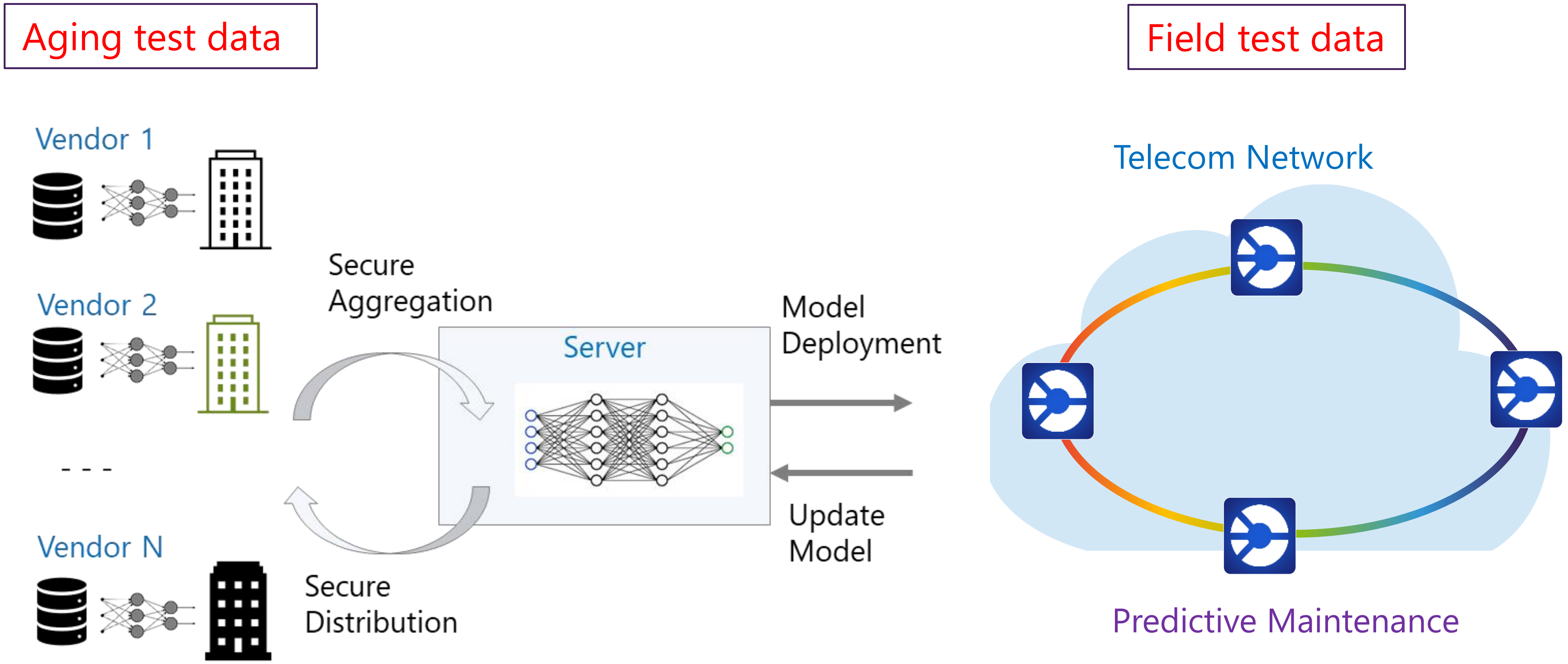
Federated Learning (FL)

- Training an ML model from multiple datasets while keeping training data in place.
- Iterating train rounds which aggregate model updates after local training.

Google introduced the technique in 2017 to test on Android keyboard suggestions.



ML-based predictive maintenance in federated learning



Challenges in Developing Data-driven Prognostics Models

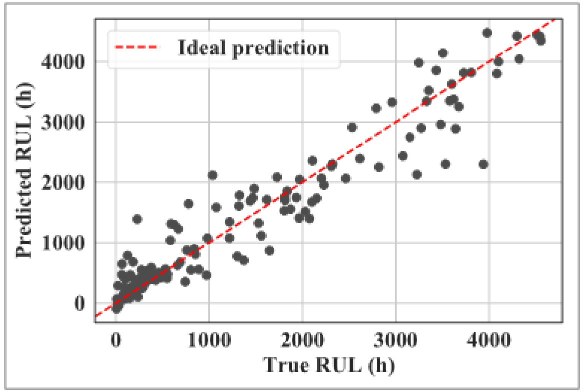
Unavailability of run-to failure data sets (Scarcity of failures during the system operation)

Long time required **to generate a meaningful** reliablity data

Adopting accelerated aging tests to collect reliability data in **shorter time**

- Accelerated aging tests are **expensive**
- Accelerated aging tests carried out for **few devices**

Small amount of data derived from such tests adversely impacting the performance of ML model

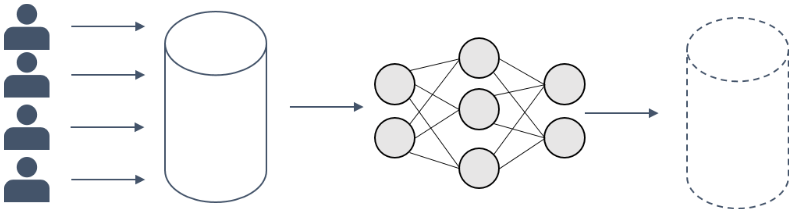


Federated Learning is a promising candidate to tackle the lack of data issue.

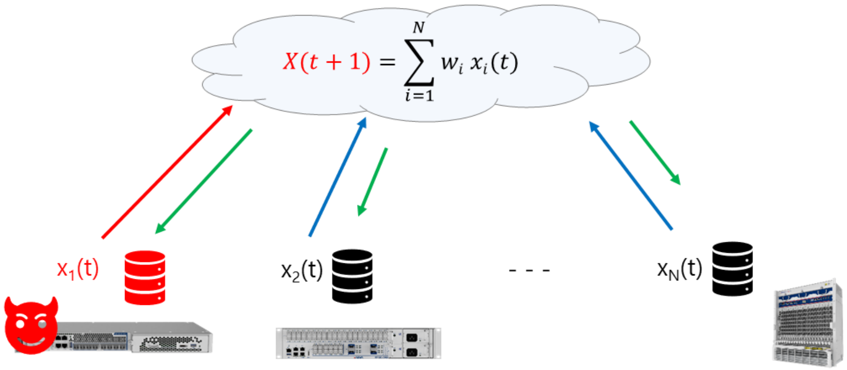
ADVA

Security and Privacy in FL

Model Inversion Attack

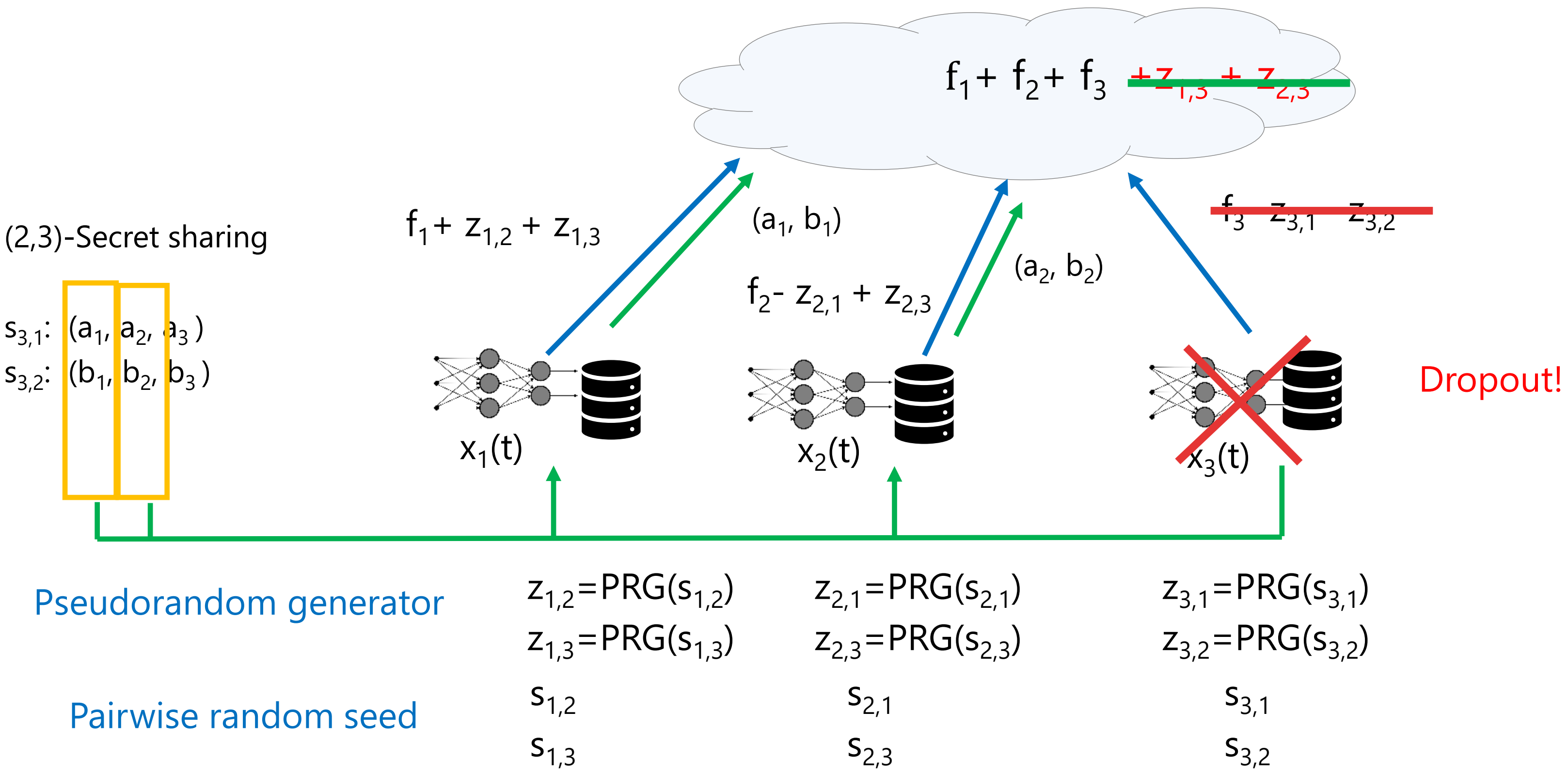


Poisoning attack



[1] Fredrikson, Matt, Somesh Jha, and Thomas Ristenpart. "Model inversion attacks that exploit confidence information and basic countermeasures." In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pp. 1322-1333. 2015.

Secure Aggregation: Example by Google



FL: Secure Aggregation

Practical Secure Aggregation for Privacy-Preserving Machine Learning

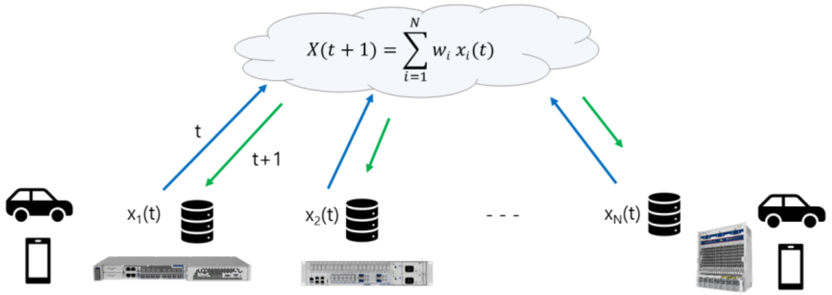
Keith Bonawitz*, Vladimir Ivanov*, Ben Kreuter*,
Antonio Marcedone†‡, H. Brendan McMahan*, Sarvar Patel*,
Daniel Ramage*, Aaron Segal*, and Karn Seth*
*{bonawitz,vlivan,benkreuter,mcmahan,
sarvar,dramage,asegal,karn}@google.com
Google, Mountain View, CA 94043
‡marcedone@cs.cornell.edu
Cornell Tech, 2 West Loop Rd., New York, NY 10044

Threat model

- Honest but curious
- Dropout may occur

$s_{u,v}$: a pairwise shared mask

$$y_u = x_u + \sum_{v \in \mathcal{U}: u<v} s_{u,v} - \sum_{v \in \mathcal{U}: u>v} s_{v,u} \pmod{R}$$



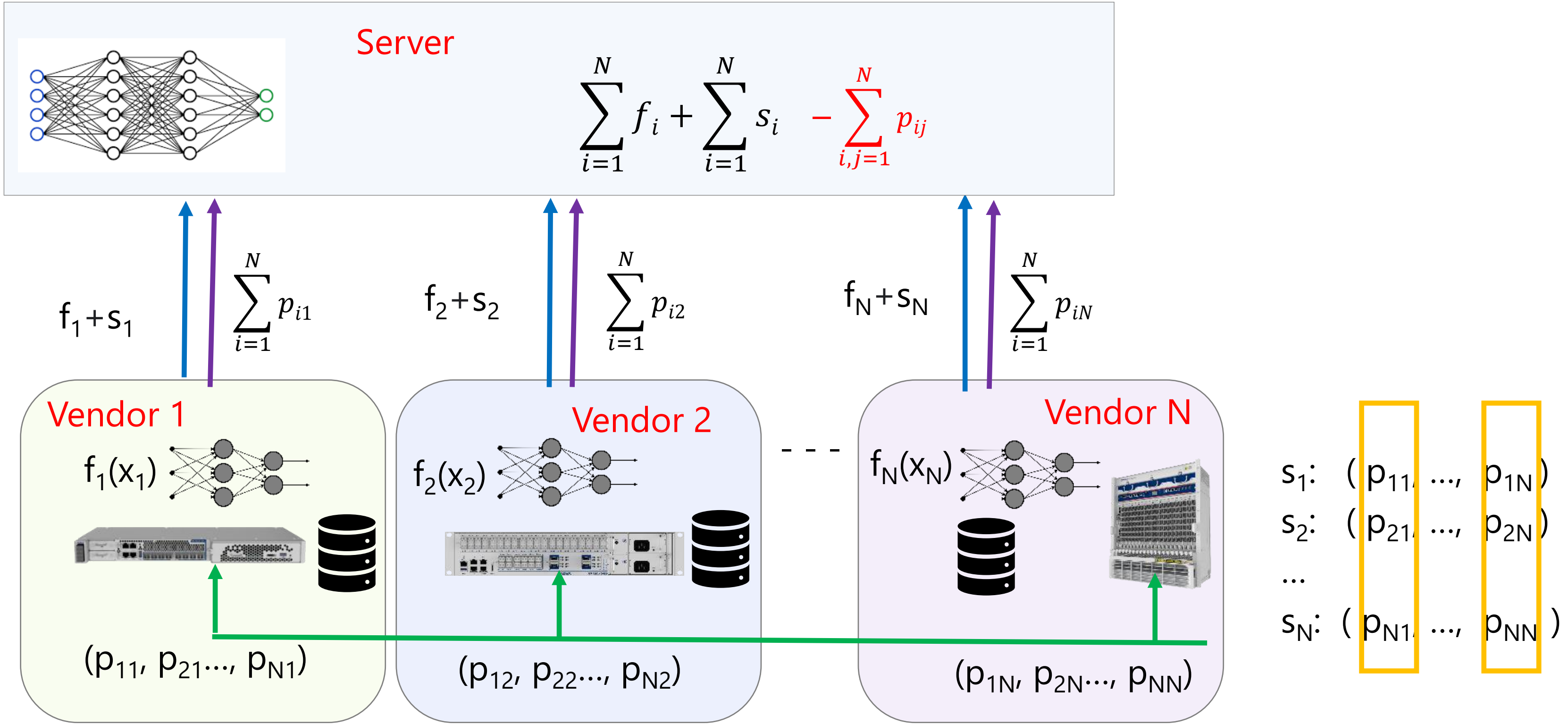
$x_1(t)+s_{1,2}+s_{1,3}+\ldots+s_{1,N}$

$x_2(t)-s_{2,1}+s_{2,3}+\ldots+s_{2,N}$

$x_N(t)-s_{N,1}-s_{N,2}-\ldots-s_{N,N-1}$

CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, October 2017

Private Federated Learning using Additive Masks

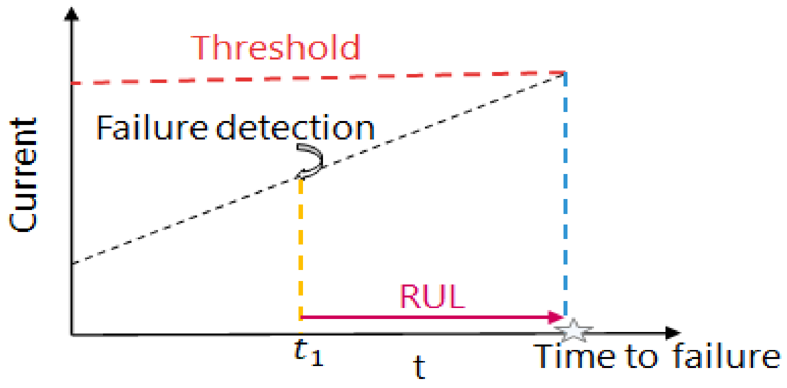


Experiment

Laser Remaining Useful Life (RUL) Prediction

RUL Prediction

RUL defined as the length of time a device is likely to operate before being repaired or replaced.

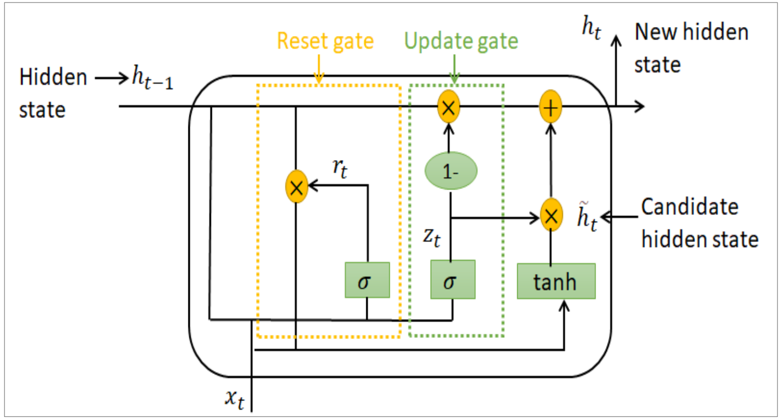


RUL Estimation Approaches

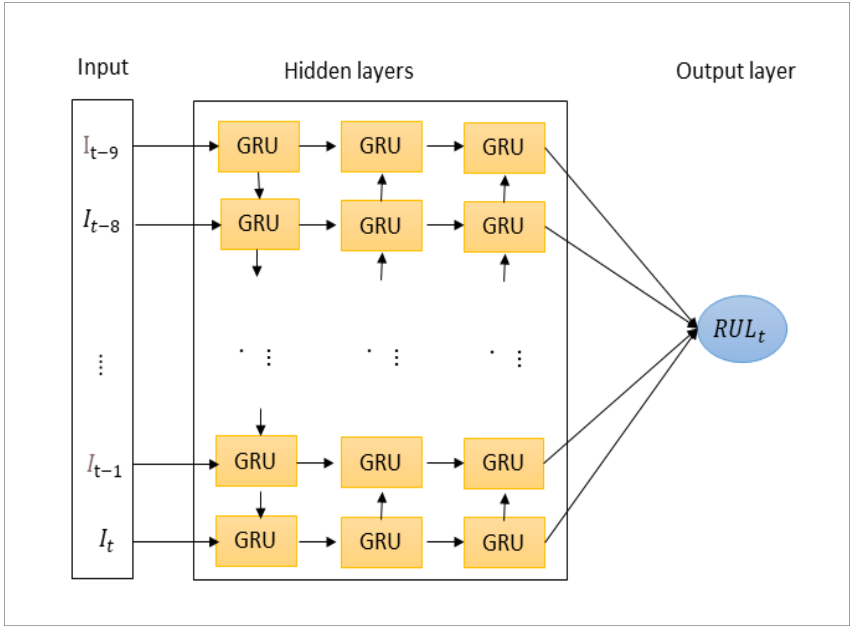
- Physics-based approaches
  - \+ Accurate, precise
  - \- High implementation costs
  - \- Time consuming
  - \- Computionally intensive
- Data-driven approaches
  - \+ Easy and fast implementation
  - \+ No knowledge required about the system
  - \- The need of sufficient amount of data

Local ML Model

GRU



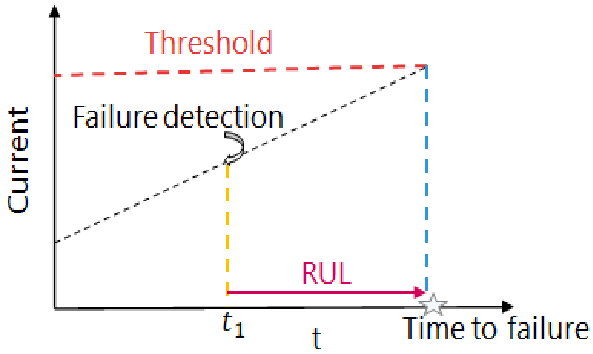
GRU Model for RUL Prediction

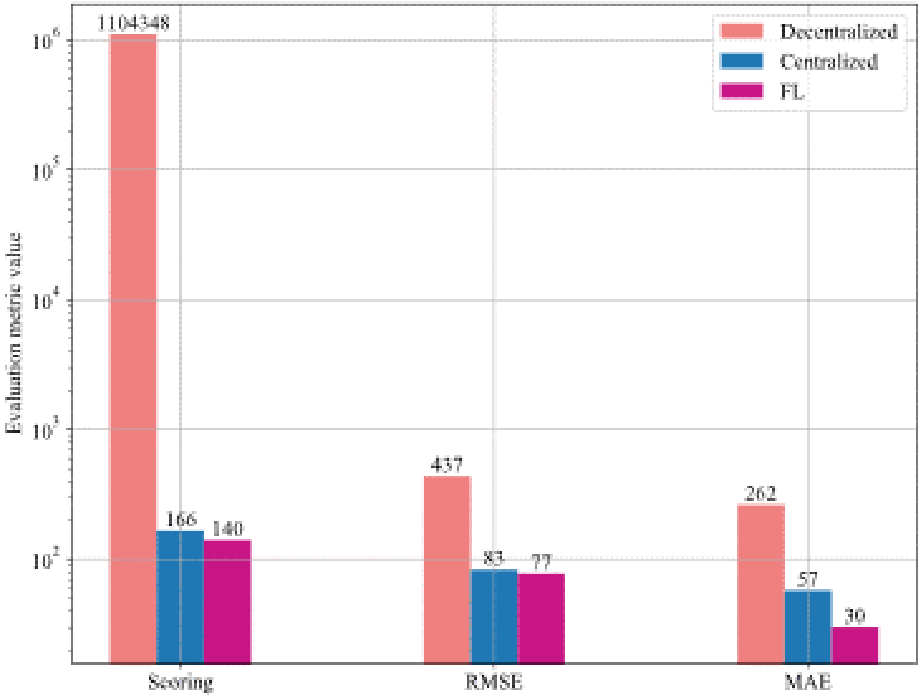


Comparison of FL, Centralized and Local ML

Using RMSE (Root Mean Square Error), MAE (mean absolute error) and scoring metrics

- Decentralized: $x_1, \ldots, x_N$
- Centralized: $X = \sum_{i=1}^{N} x_i$
- FL: $F = \sum_{i=1}^{N} f_i$





Take away

- We demonstrated that the FL framework achieves good prediction capability while ensuring the data privacy and confidentiality.

- The performances of the FL and centralized approaches are very similar in our use case.

- FL is potentially vulnerable for data/model poisoning attacks => Anomaly detection using ML can be applied.

Acknowledgements

This work has been performed in the framework of the CELTIC-NEXT project AI-NET-PROTECT (Project ID C2019/3-4), and it is partly funded by the German Federal Ministry of Education and Research (FKZ16KIS1279K).

Khouloud Abdelli

Research Activities:

Application of Machine Learning in SDN-based Optical Networks

KAbdelli@adva.com

Skills:

Machine learning in Python

Data analysis

Job search:

- Currently PhD candidate
- Probably available from June 2022
- Looking for Post-doc or Industrial position

Thank you

jcho@adva.com