Federated Learning

BARGAVA SUBRAMANIAN
TUHIN SHARMA

Binaize

AGENDA

1

CURRENT LEARNING PARADIGM

2

FEDERATED LEARNING

3

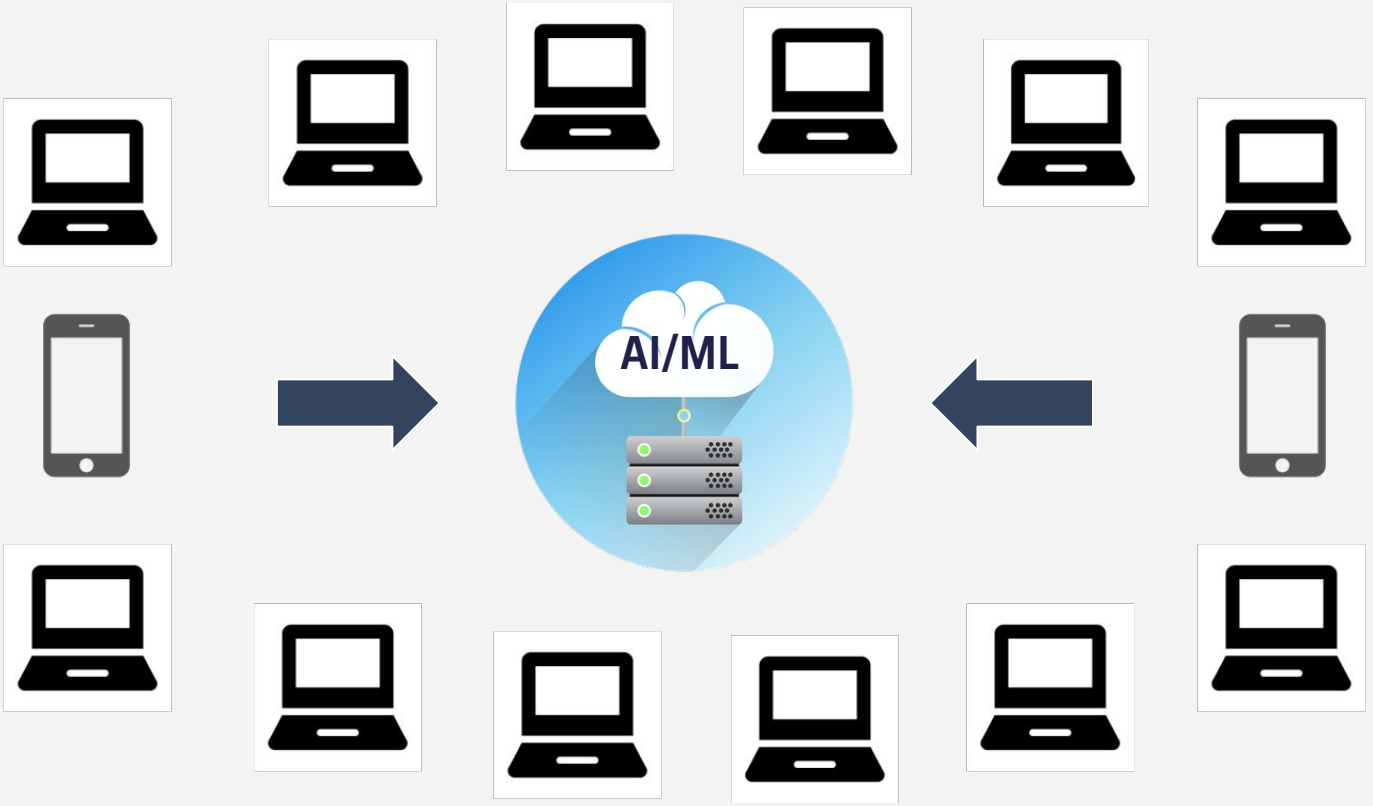
TOOLS & CHALLENGES

4

DEMO

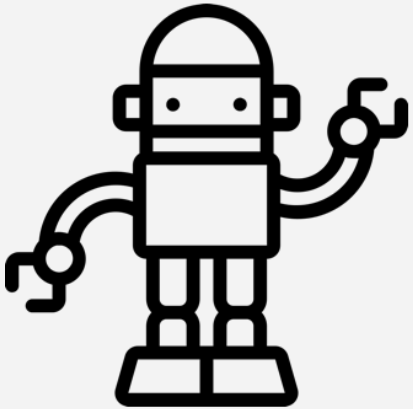
(notebook)

Centralized Machine Learning

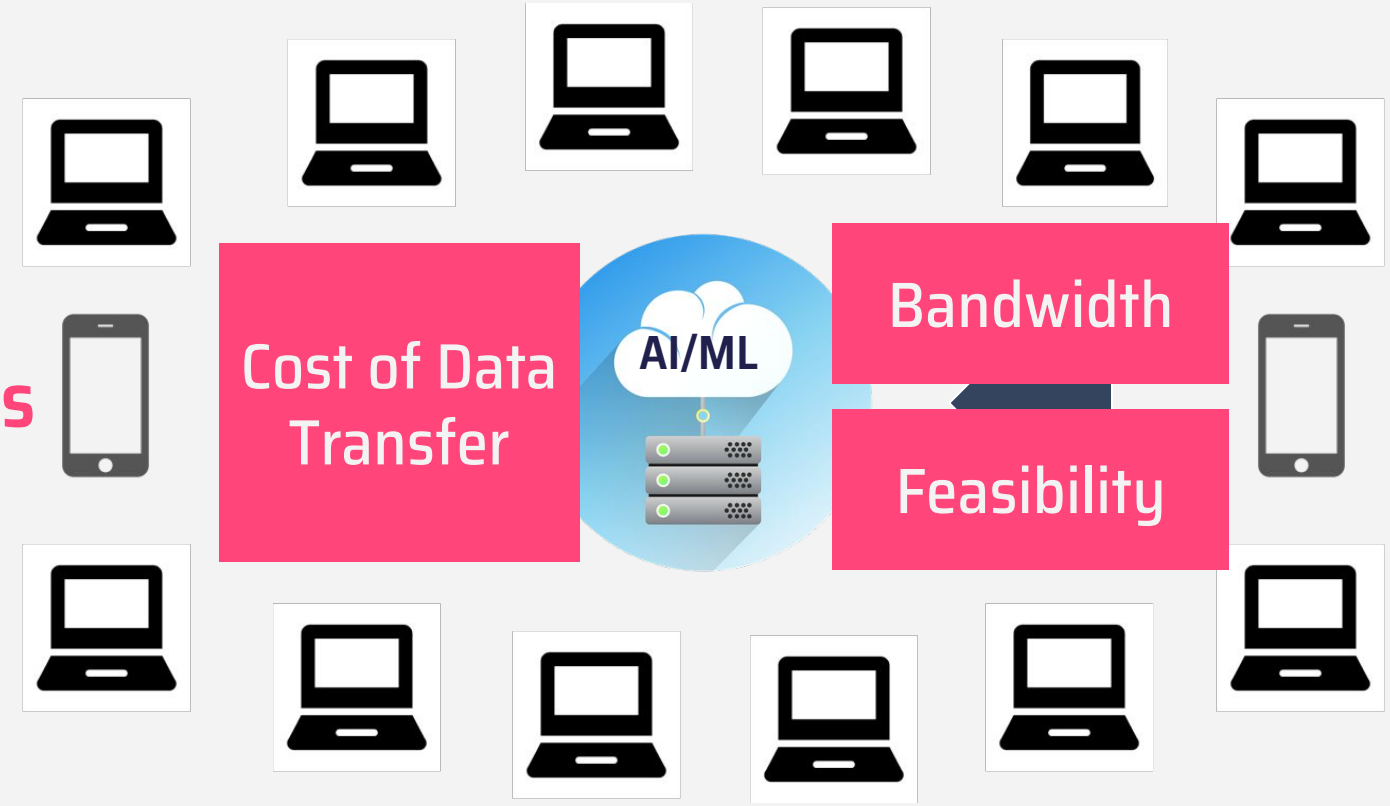


BUT

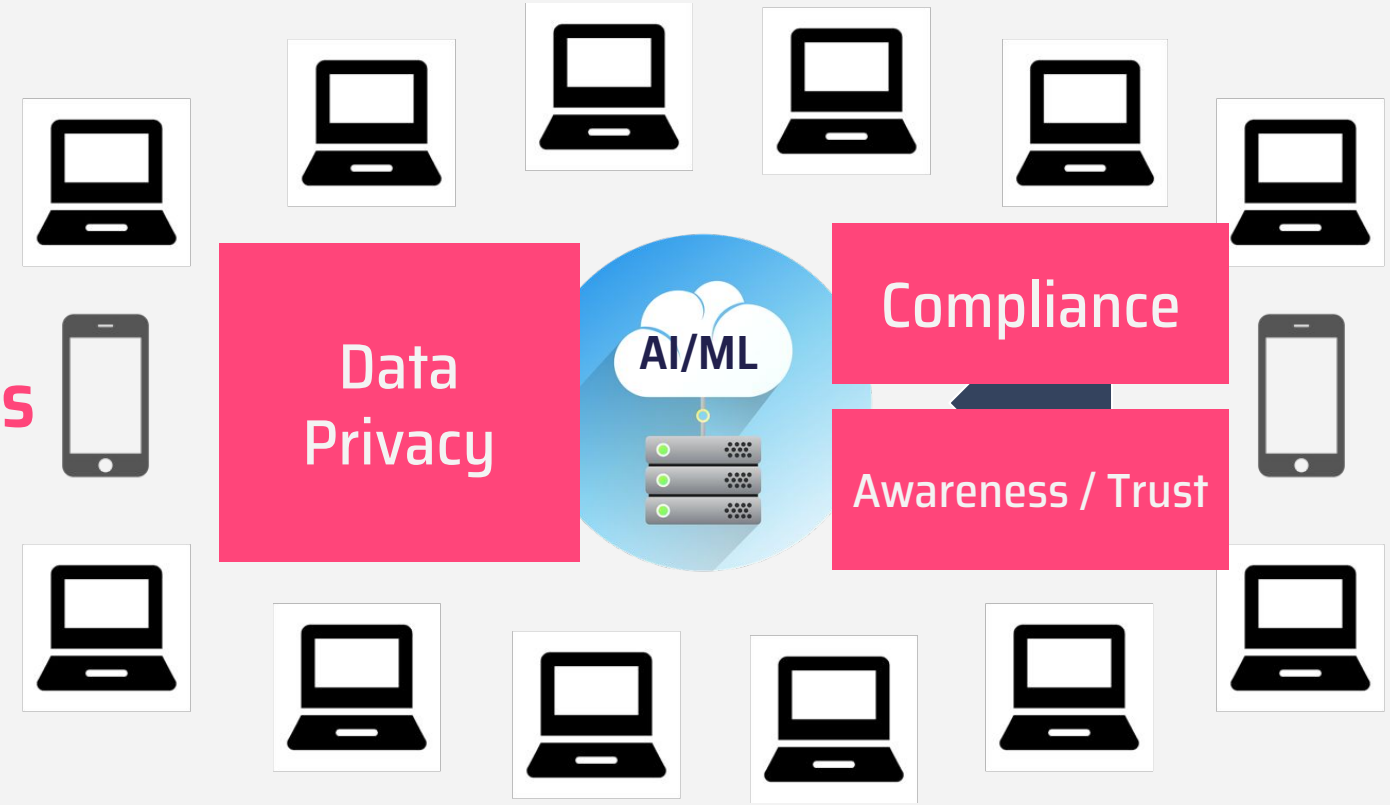
We live in a
Smart
Connected
World



Challenges



Challenges



Anomaly Detection

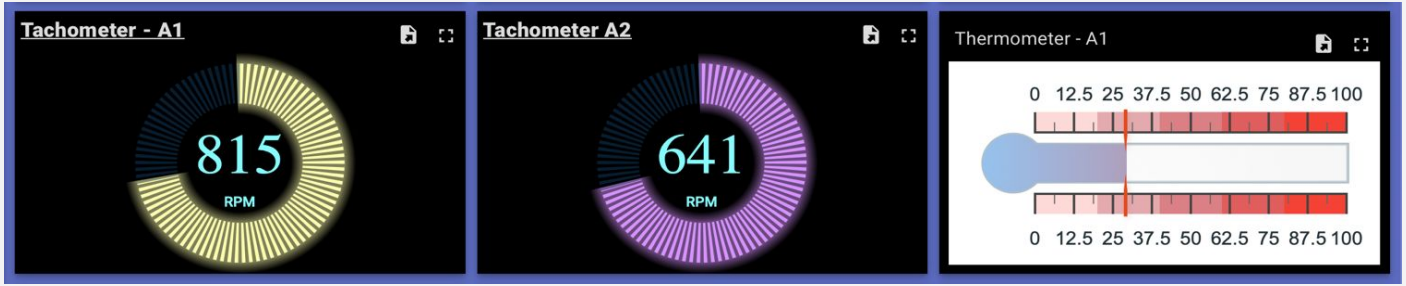
USE CASES

- Cybersecurity
- Preventive Maintenance
- Sales & Marketing

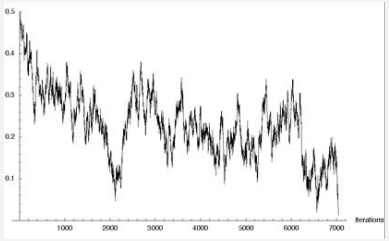
GOAL

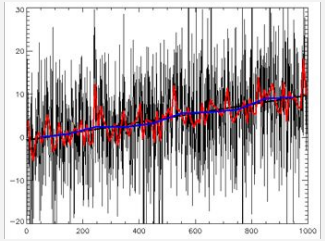
Find anomalies across a stream of time series events

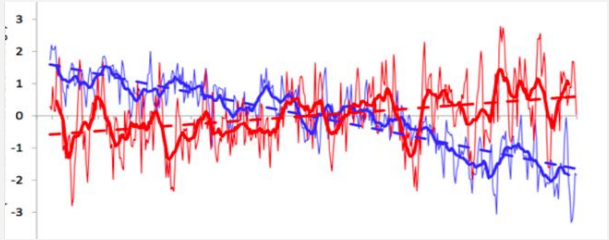
Sensor Data



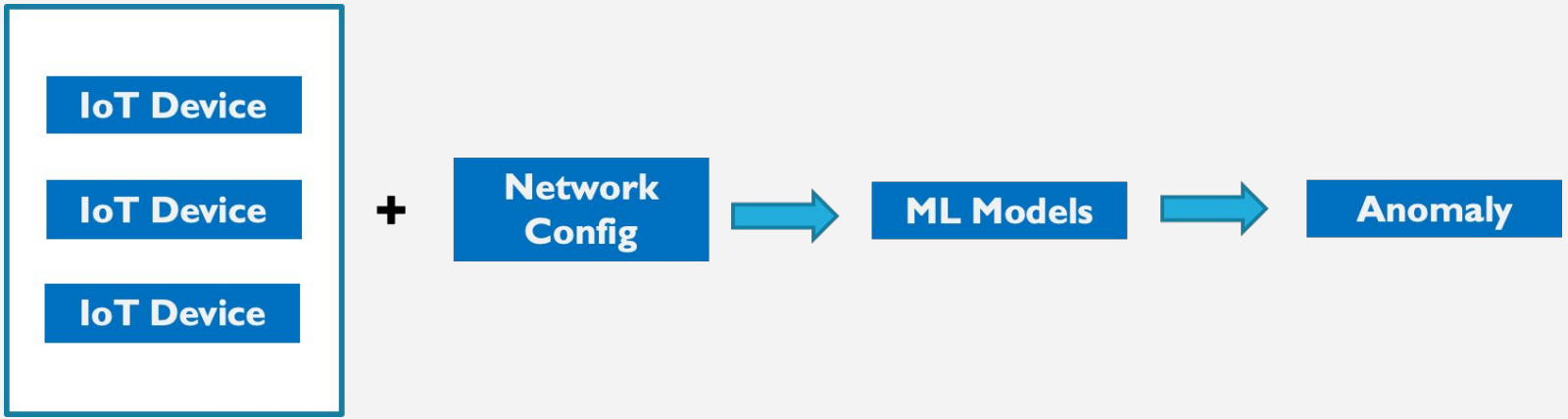
Network Data



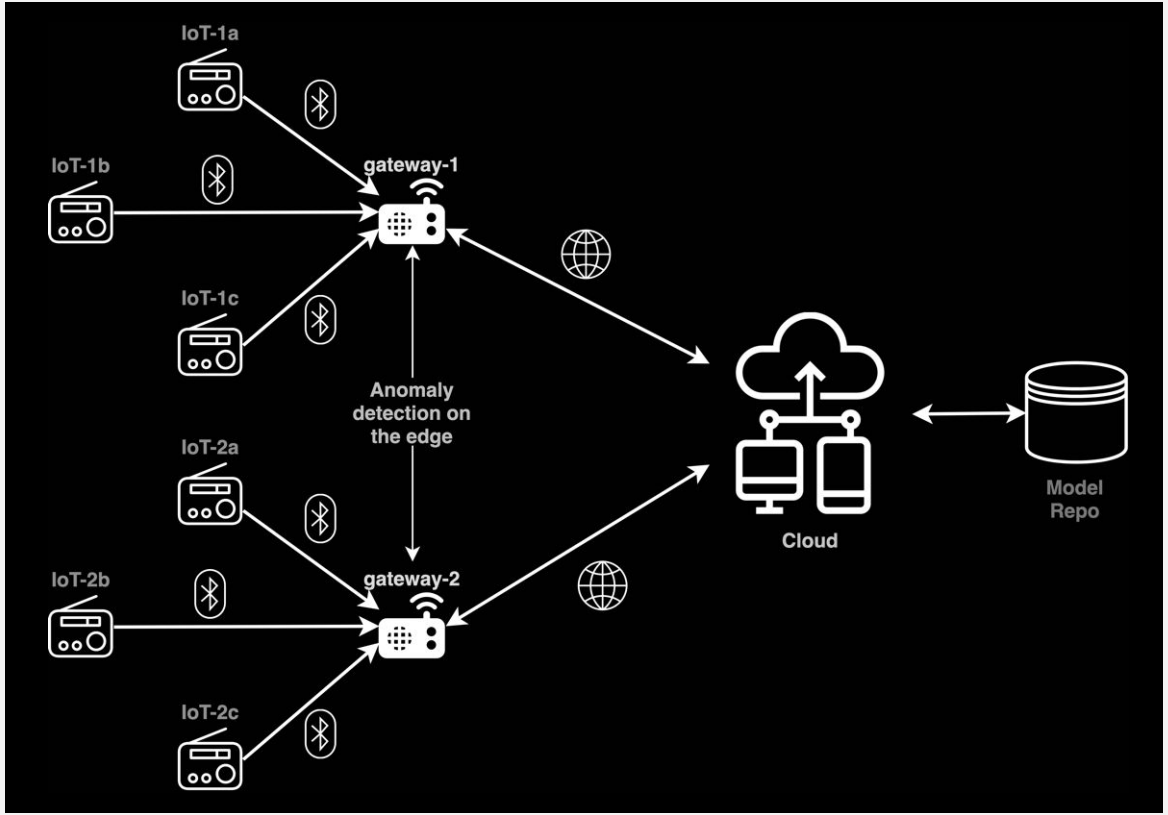




DATA FLOW


IoT Device
IoT Device
IoT Device
+
Network Config
ML Models
Anomaly

NETWORK SETUP



HOW FEDERATED LEARNING SOLVES THIS?

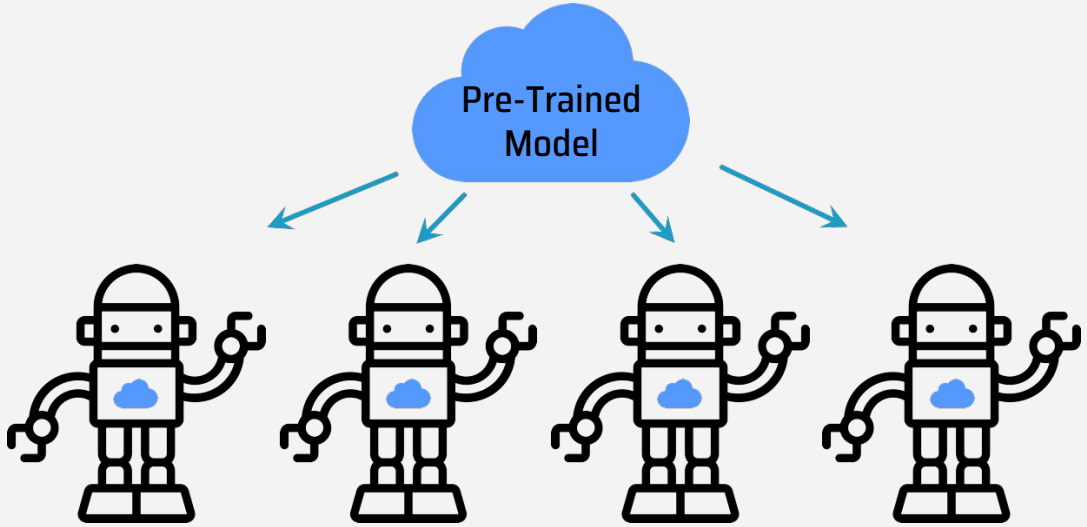
DECENTRALIZED LEARNING

PRESERVE PRIVACY

SECURE COMPUTING

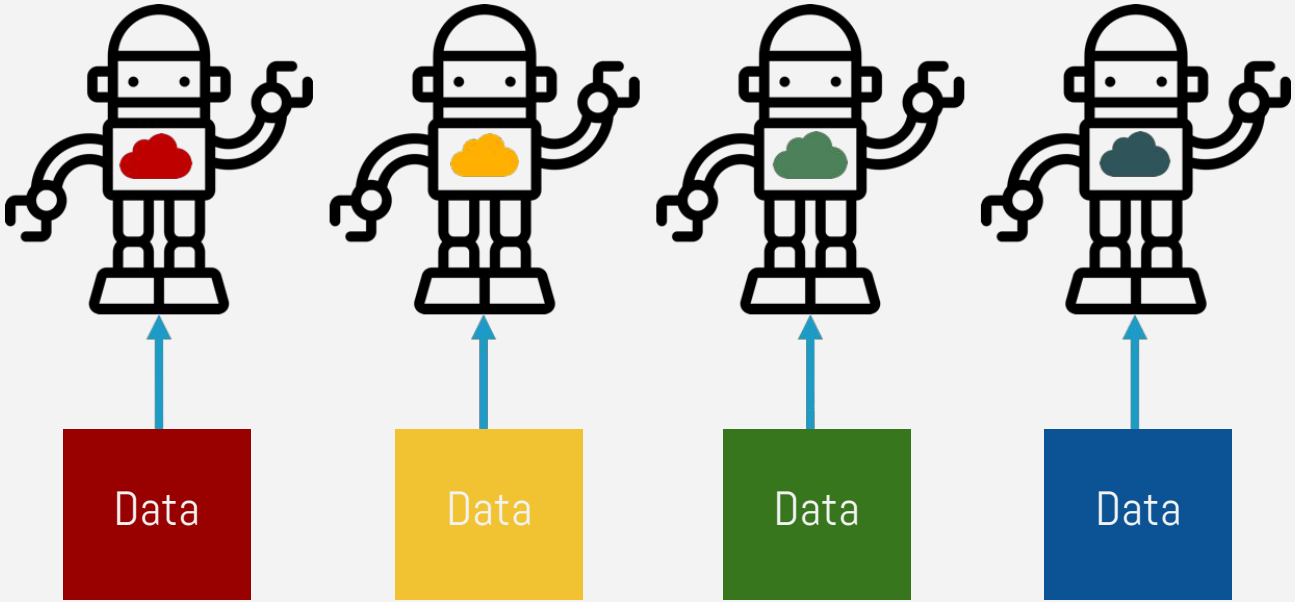
Decentralized Learning

Federated Construction



Decentralized Learning

Decentralized Training

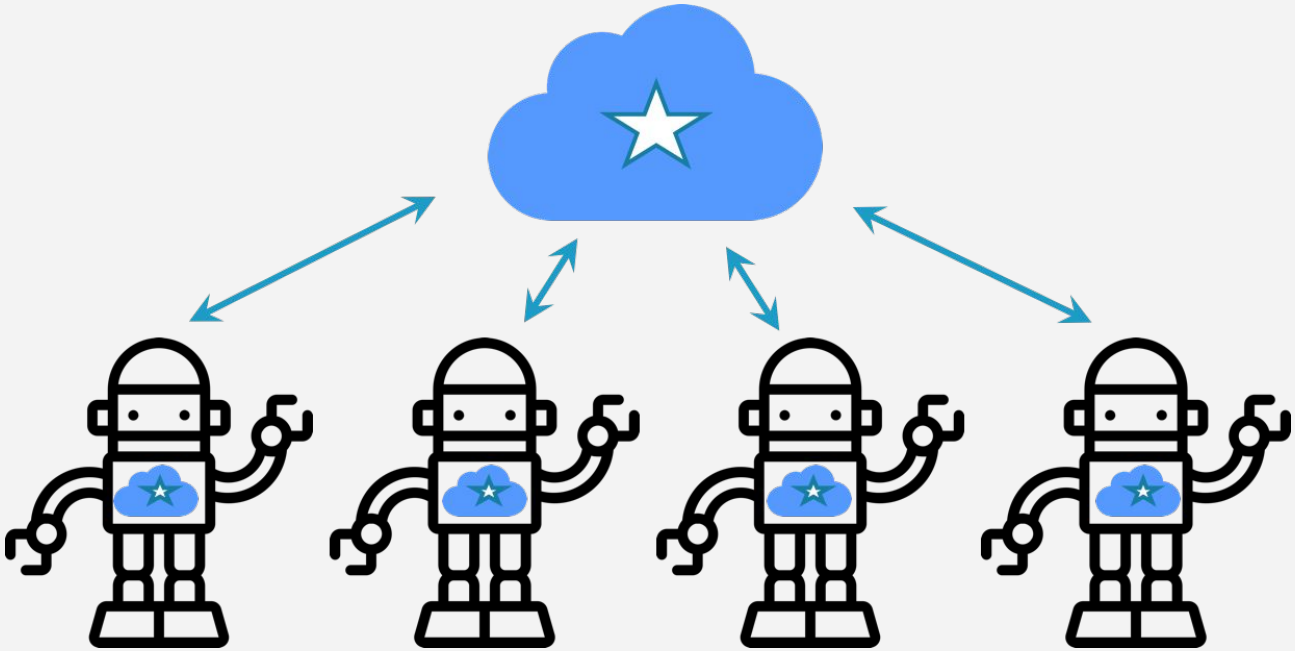


Decentralized Learning

Aggregation

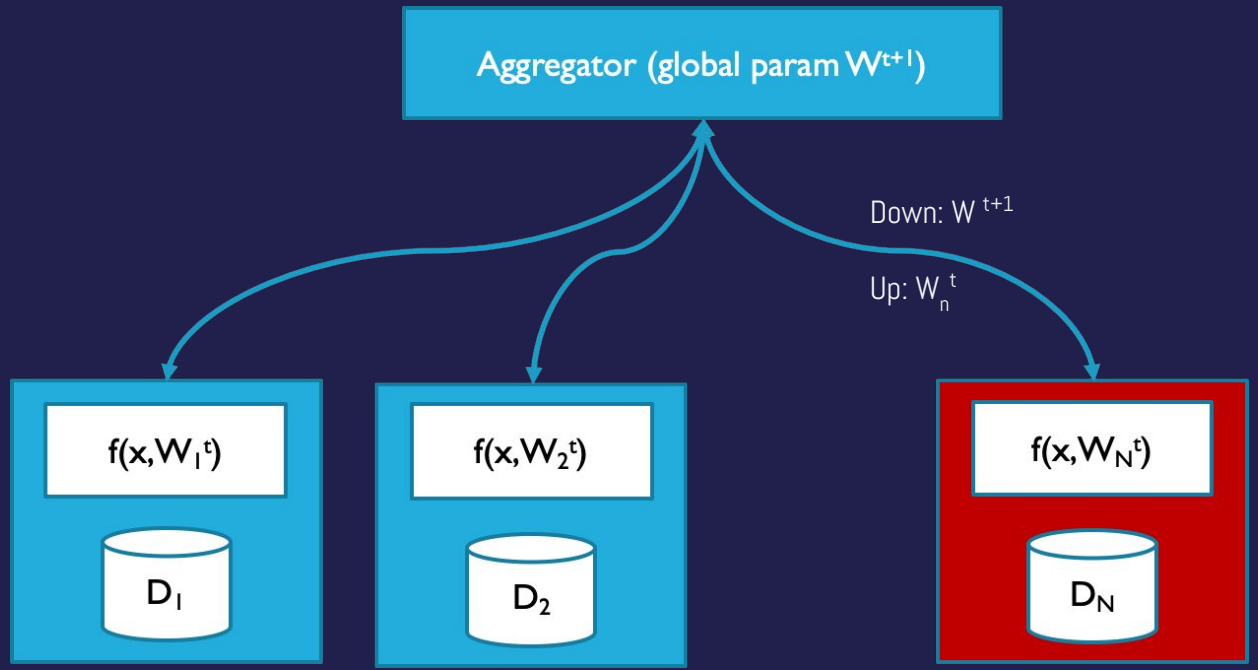
Decentralized Learning

Rinse - Repeat



PROBLEM!

Inference Attack

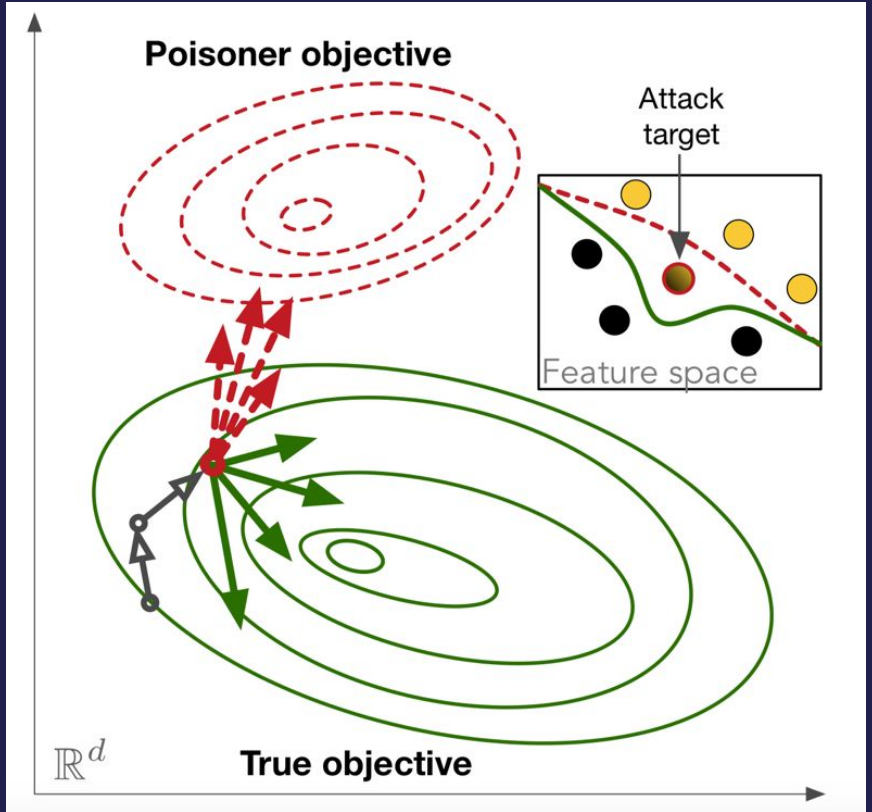


~~Inference Attack~~

Differential Privacy

Clip Gradients + Noise + Average

Model Poisoning



~~Model Poisoning~~

Sybil Detection

- Adaptive Learning per Client

- Adversarial Network

Secure Computing

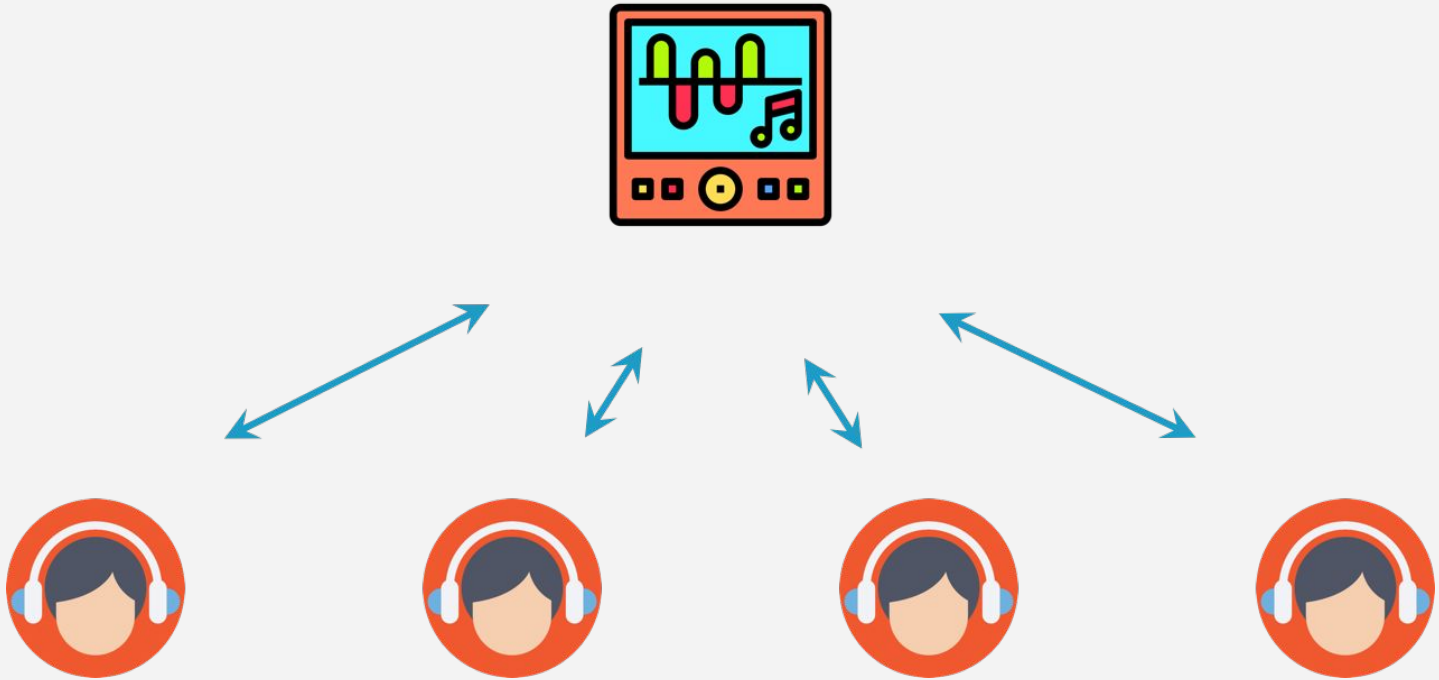
Train on Encrypted Data

Types of Federated Learning

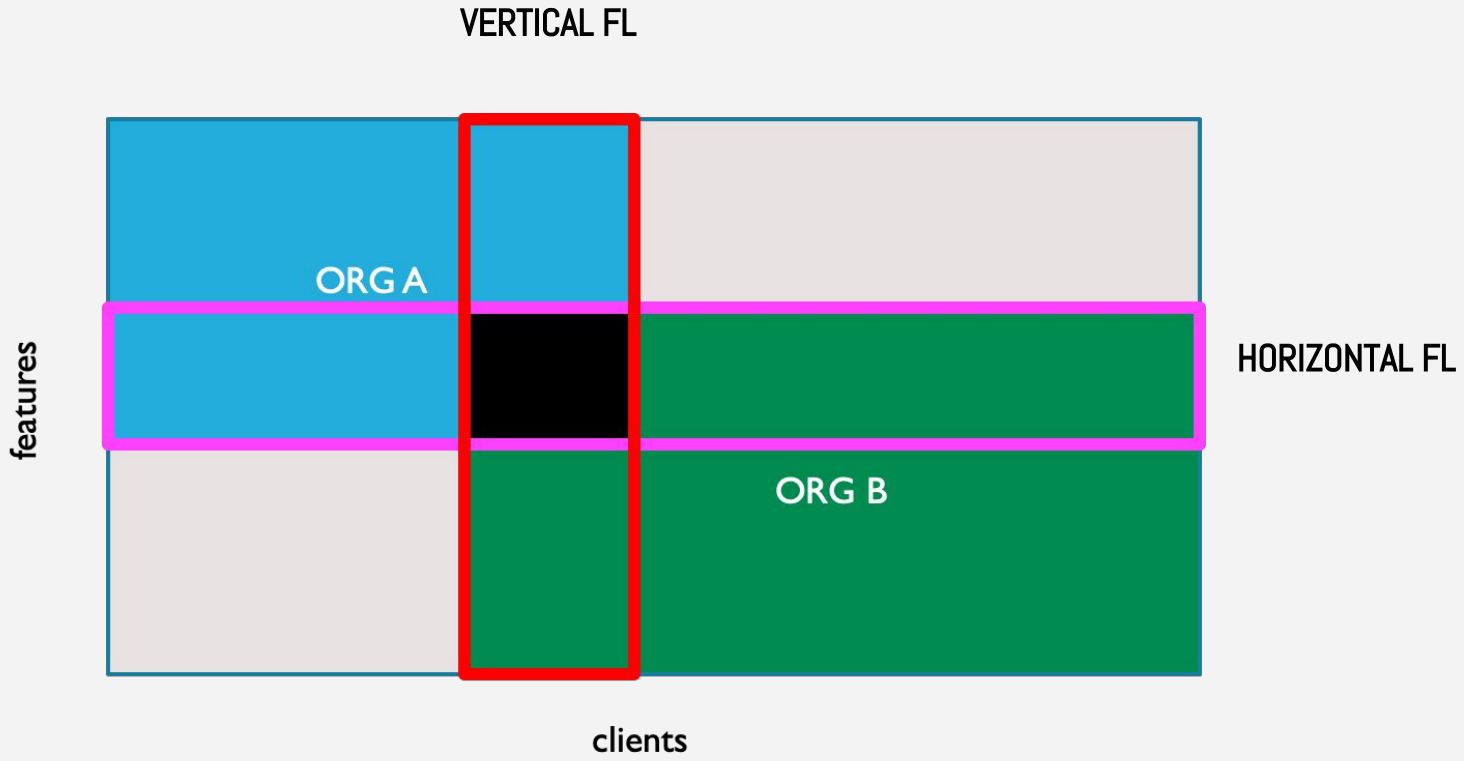
SINGLE PARTY

MULTI PARTY

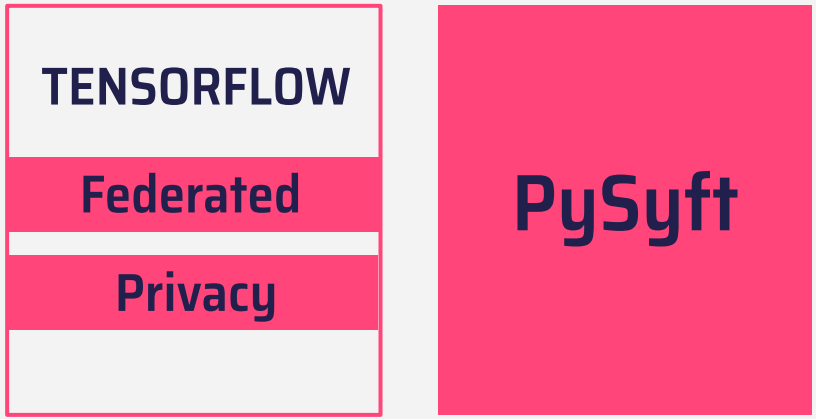
SINGLE PARTY



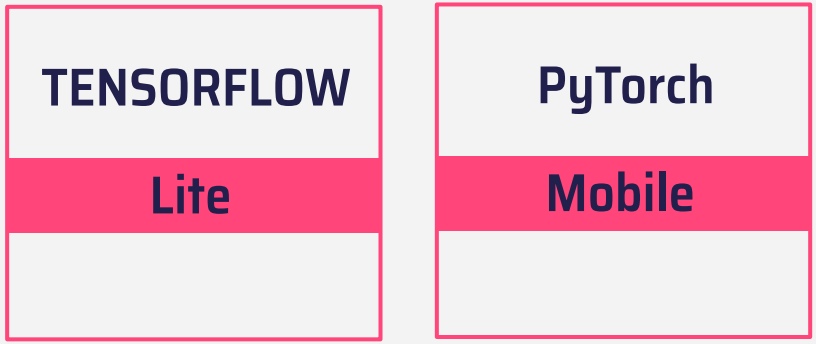
MULTI PARTY



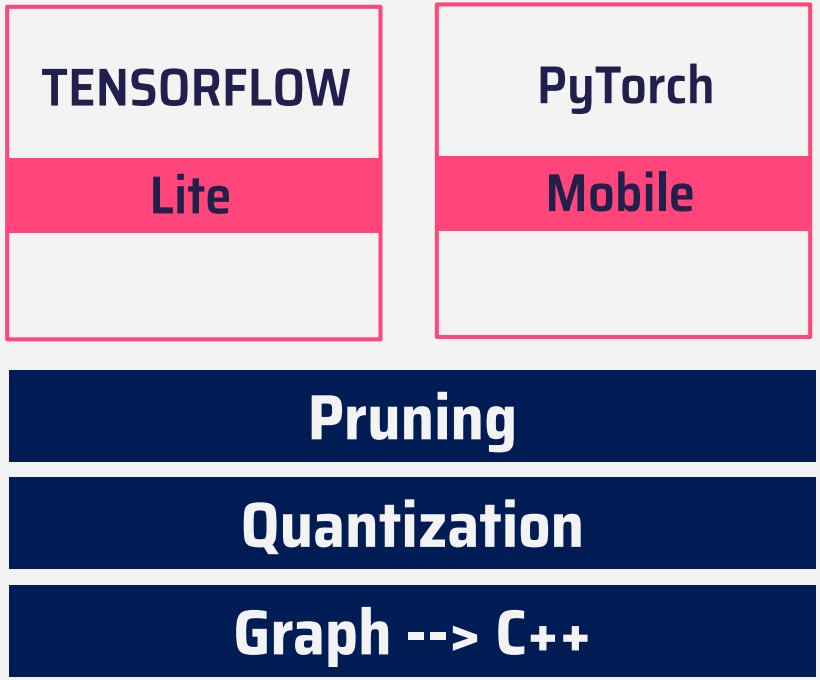
TOOLS



Deployment
TOOLS



Deployment
TOOLS



Challenges

- Not IID
- Model Convergence Time
- Limited Deployment Choices

DEMO

BENEFITS

- Better model accuracy
- Lower latency
- Lesser power consumption
- Lesser network load
- Privacy
- Can be used across organizations*
- Can be used immediately*

BENEFITS

- Better model accuracy
- Lower latency
- Lesser power consumption
- Lesser network load
- Privacy
- Can be used across organizations*
- Can be used immediately*

Resources

- https://github.com/tuhinsharma121/federated-ml/
- https://www.tensorflow.org/federated
- https://github.com/tensorflow/privacy
- https://github.com/uTensor/uTensor
- https://github.com/OpenMined/PySyft
- https://pytorch.org/mobile/home/

THANKS!

TUHIN SHARMA
@tuhinsharma121

BARGAVA SUBRAMANIAN
@bargava