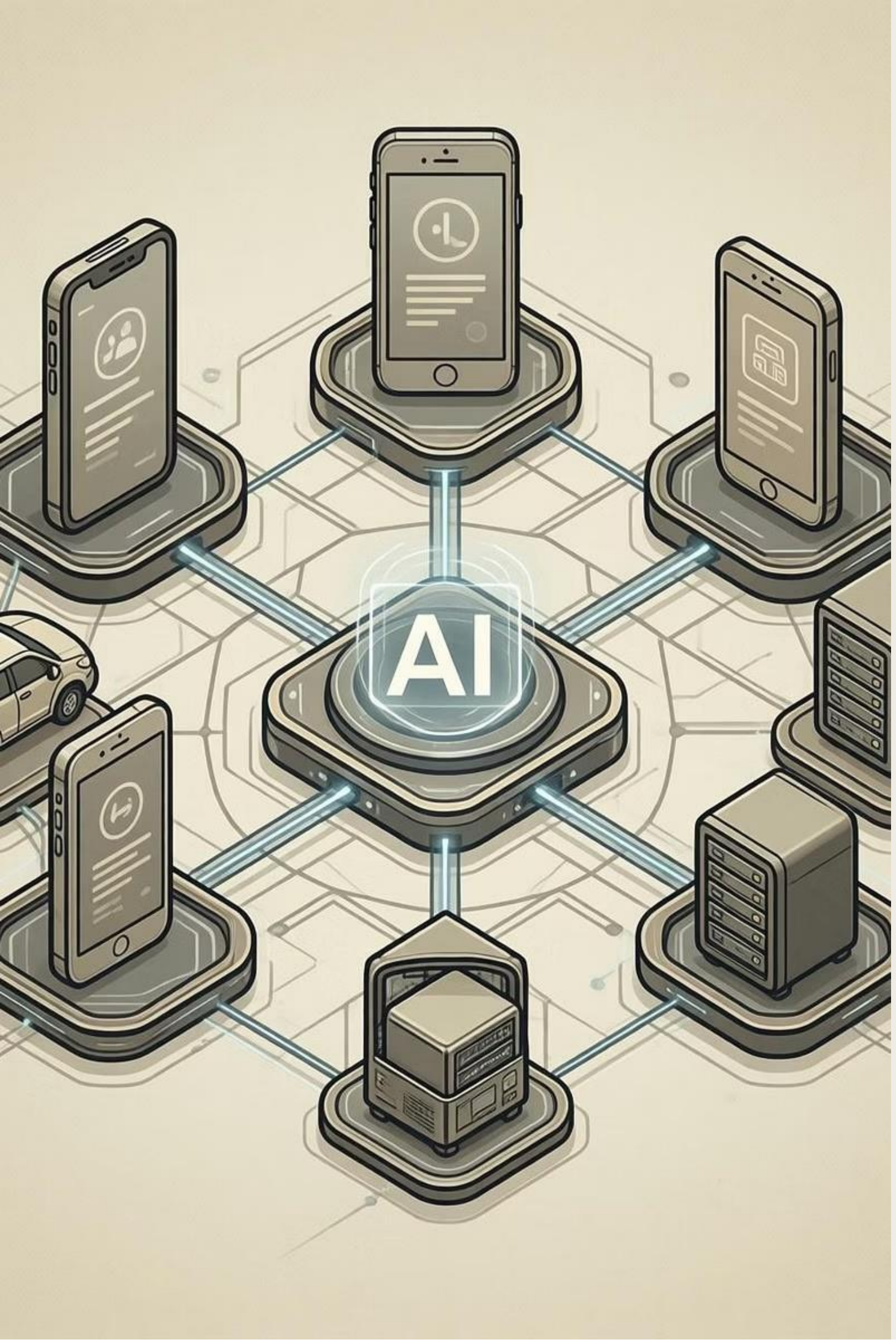


Federated Learning in Intelligent Systems & ITS

This presentation explores the application of Federated Learning(FL) in real-world intelligent systems and specifically within Intelligent Transportation Systems(ITS), highlighting its benefits, challenges ,and future directions.

Outline

Introduction to Federated Learning

What This Paper Is About

- Focuses on applying FL in real-world intelligent systems.
  Emphasizes privacy-preserving machine learning.
- Addresses distributed data environments and edge systems.
- Application-oriented, studying deployment and challenges.
- Evaluates accuracy, communication cost, and privacy.
- Reviews existing research for ITS applications.

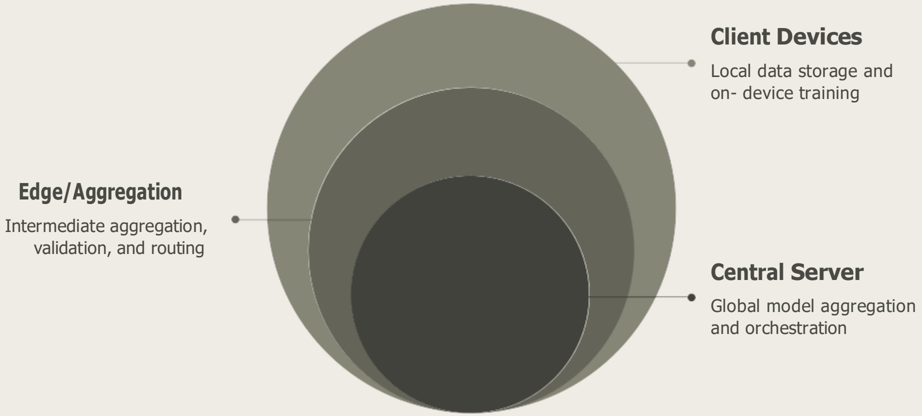
Motivation:WhyFLisNeeded

- **Centralized Data Collection Is Risky:** Personal and location data lead to privacy leakage and regulatory issues(GDPR, HIPAA).
- **Distributed Data Can not Be Easily Merged:**

  Data on edge/mobile devices is expensive, slow, and energy-consuming to transfer.
- **Resource Constraints at the Edge:** Limited CPU, memory, and battery make heavy models impractical.
- **High Response Latency in ITS:** Cloud-based decisions are too slow for real-time tasks like collision avoidance.
- **Privacy and Security Issues in ITS:** Sensitive vehicle data risks leakage and attacks when sent to the cloud.
- **Low Decision-Making Accuracy in ITS:** Uneven, incomplete, and Non-IID data leads to poor model generalization.

FL System Architecture & Workflow

- **Three-Tier Architecture :**Client, Edge/Aggregation, and Central Server layers.
- **Client Layer:** Edge devices store local data, perform local training and feature extraction.
- **Edge/Aggregation Layer:** Optional intermediate layer reduces latency and communication cost, support spartial aggregation.
- **Central Server:** Coordinates training rounds, performs model aggregation and global synchronization.
- **Training Workflow:** Server initializes global model, sends to clients for local training, clients send updates, server aggregates using Fed Avg.
- **ITS Architecture :**Cloud server (global model), RSUs/Edge servers(partial aggregation),Vehicles(local models).



This architecture is scalable, fault-tolerant, and suitable for ITS environments.

Algorithms and Techniques Used

1

Federated Averaging (FedAvg)

Main aggregation algorithm: simple, communication-efficient,but sensitive to non-IID data and client heterogeneity.

2

Local Training Algorithms

Clients use CNNs, DNNs, or light weight models with SGD and mini-batch training for edge efficiency.

3

Non-IID Data Handling

Addresses model drift and slower convergence due to differing client data distributions via adaptive weights

Privacy & Communication Optimization

- **Differential Privacy(DP):**Adds noise to model updates to prevent inference attacks, with a privacy-accuracy trade-off.
- **Secure Aggregation :**Server only sees aggregated model, protecting individual updates from honest-but-curious servers.
- **Model Compression:** Techniques like parameter pruning and quantization reduce communication overhead.
- **Client Selection :**Not all clients participate every round; selection base don network quality and resource availability.
- **Update frequency Control:** Fewer communication rounds with more local computation to optimize communication.
- **Blockchain Integration:** Provides trust and trace ability for data and model updates in FL systems.

FL in Intelligent Transportation Systems(ITS)

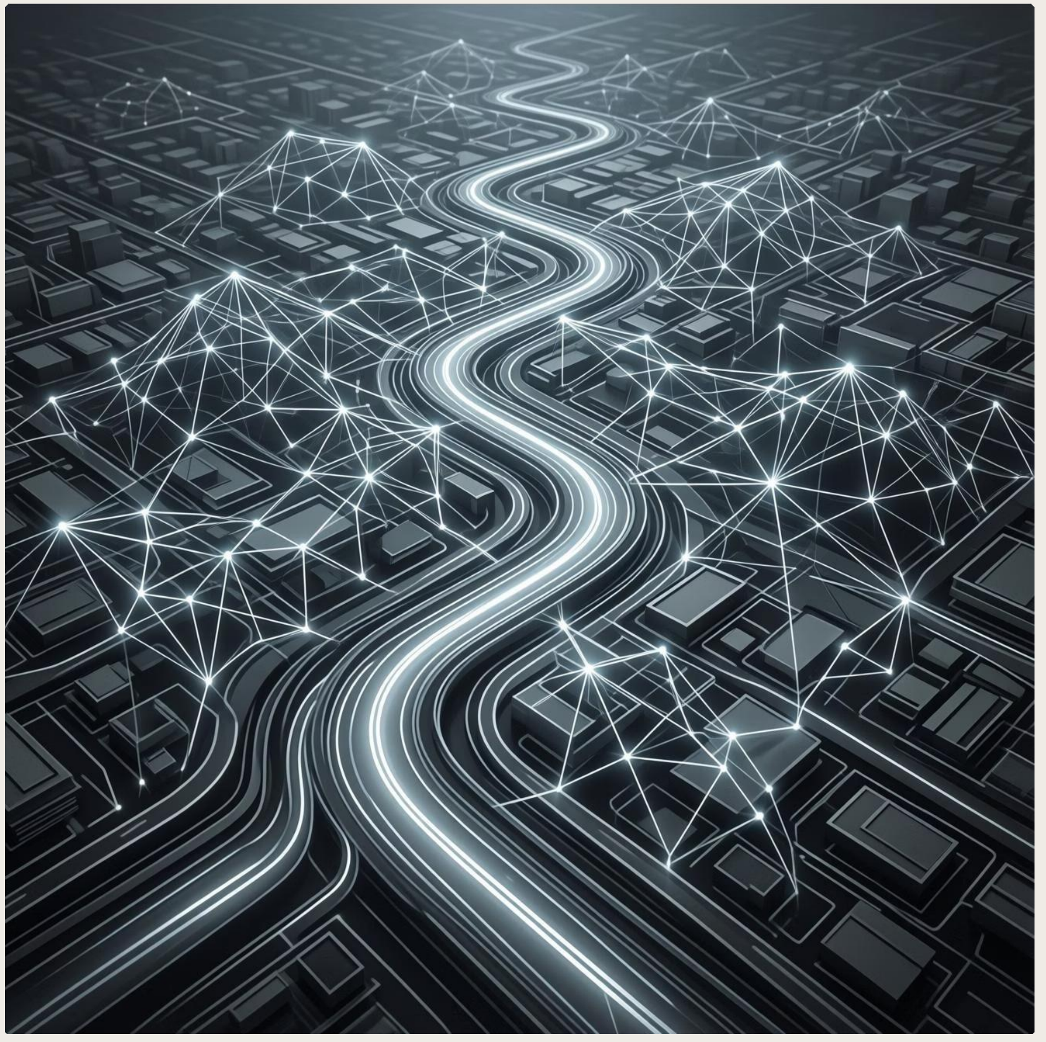
- **Lower Communication Cost:** Only light weight model updates are shared, not raw data, ideal for limited bandwidth.
- **Enhanced Privacy Protection:** Data stays local within vehicles, combined with DP and secure aggregation.
- **Improved Scalability:** Supports large-scale ITS with dynamic vehicle populations, as vehicle scan join and leave.
- **Increased Robustness:** System continues to function even if some vehicles disconnect, avoiding single points of failure.
- **Non-IID Data Handling:** FL is designed for un even data distributions common in ITS, using personalized and grouped aggregation.
- **Support for Local Personalized Decisions:** Each vehicle can adapt the global model for better local performance and real-time responses.

ITS Application Scenarios

- **Object Recognition (Perception):** Obstacle detection, traffic sign recognition using CNNs, YOLO, Mask R-CNN.
- **Traffic Status Identification(Perception + Prediction):** Vehicle positioning, traffic flow prediction using DNN,LSTM, TCN.
- **Traffic Management (Decision):** Parking management, traffic signal control using FL+ Reinforcement Learning.
- **Service Providing Tasks:** EV charging services, route planning using graph search, DRL.
- **Challenges :**High-speed mobility, limited storage/computing, high information sensitivity.
- **Solutions:** Asynchronous FL, edge computing, model compression, blockchain, DP, anomaly detection.

Future Directions & Conclusion

- **Lightweight FL Models:** Essential for resource-constrained edge devices.
- **Adaptive Aggregation Strategies:** To better handle non-IID data and client heterogeneity.
- **Cross-Layer Optimization:** Integrating network and learning optimizations for better performance.
- **Real-World Deployment:** Benchmarking and commercial deployment using platforms like Open Daylight.
- **Generalized FL for Multiple ITS Scenarios:** One FL system serving diverse tasks efficiently.
- **Deep Integration of FL and ITS:** Developing task-specific FL architectures for optimal performance.



Federated Learning is a strong candidate for future ITS, solving privacy, communication, and scalability issues, but requires continued research in to security, resource limitations,and deployment challenges.