Cross-OEM Federated Learning for Autonomous Driving

Tanja Schultz
Asst Professor

Abstract

The growing interest in autonomous vehicle technology presents opportunities for manufacturers to pursue plans based on machine learning to develop their own self-driving solutions while maintaining their competitive edge. Collaborative artificial intelligence presents manufacturers with the possibility of cooperation without sharing private user data. Federated learning is a distributed machine-learning framework that enables multiple parties to cooperate on a common model while training locally on their own private data. Despite the similarities in the underlying technology, the application of federated learning for autonomous driving has attracted limited interest. Numerous challenges arise and need to be addressed: Different autonomous driving systems develop independently, and hence their models differ significantly. Vehicle manufacturers may use proprietary data formats that ensure the privacy of user data, and the necessary training data remain in the manufacturer domain. Communication efficiency is critical, as the resources of vehicles are constrained compared with fixed servers. Training data remain local, and agent-specific knowledge cannot be transferred directly.

Collaborative autonomous driving powered by federated learning could fill the perceptual gaps during periods of limited visibility and ensure the safe crossing of busy intersections. A federated-learning framework has been developed that integrates several key components and techniques for training across a multi-manufacture federated vehicular network. It transmits only key information that preserves the privacy of the drivers while enabling safe autonomous driving in a limited-visibility environment. Powers and constraints differ across manufacturers, so establishing a top-level data flow is also necessary.

Keywords: Autonomous Vehicle Technology, Collaborative Artificial Intelligence, Federated Learning Frameworks, Privacy-Preserving Machine Learning, Distributed Model Training, Collaborative Autonomous Driving, Multi-Manufacturer Vehicular Networks, Limited-Visibility Driving Scenarios, Safe Intersection Navigation, Communication-Efficient Learning, Vehicle Resource Constraints, Proprietary Data Formats, Decentralized Data Governance, Local Model Training, Agent-Specific Knowledge, Perception Gap Mitigation, Federated Data Flow Design, Secure Model Aggregation, Intelligent Transportation Systems, Privacy-Aware Autonomous Systems.

1. Introduction

The field of autonomous driving increasingly employs deep neural networks that rely on large amounts of data obtained in natural driving conditions. Such data are shared across manufacturers, often via centralized clouds, raising privacy and security concerns. Federated Learning (FL) addresses this challenge by allowing individual agents to improve their models using local datasets while only broadcasting weight updates to a central server. Data remain on local devices, enhancing privacy. In the case of vehicular networks, the naturally formed network topology and heterogeneous, event-driven driving behaviors motivate the use of FL to enable manufacturers to collaboratively learn models that generalize better across vehicle platforms. Federated Learning (FL) is a distributed ML paradigm that enables learning with decentralized data without compromising privacy and security. FL is especially suitable for connected and collaborative learning across

ISSN: 3067-4190
JOURNAL OF ARTIFICIAL INTELLIGENCE AND BIG DATA DISCIPLINES
Volume: 03 Issue: 02
RECEIVED: APRIL 20 REVISED: MAY 03 ACCEPTED: MAY 21 PUBLISHED: JUNE 04

manufacturers. FL can generalize well across heterogeneous datasets from different agents, enabling multi-manufacturer collaboration in privacy-conscious applications. The unique network topology and behaviors of vehicular networks reduce communication cost, leading to new opportunities in vehicular FL. In a connected-vehicle environment, comprehensive FL algorithms and techniques can better support training efficiency, robustness, privacy, and security. Key drivers and obstacles that a connected-vehicle vehicular FL system must consider.

1.1. Overview of Federated Learning in the Context of Autonomous Driving

Federated learning (FL) enhances the performance and generalization of machine learning tasks in automotive networks by enabling real-time knowledge exchange between different manufacturers while preserving data confidentiality. Despite data generated by multiple vehicles on shared roads, the primary purpose of these connected vehicles is still to serve the individual drivers and travelers. Hence, the amount of locally fast-to-collect data at a vehicle generally outweighs the information it can outsource to the surrounding connected vehicles—and specifically request information from them—over the dedicated short-range communications (DSRC) wireless channels. Supported by federated learning, the collaborative sharing of models rather than raw, personally identifiable, and confidential vehicle data (with its high latency and high bandwidth demand) adds significant driving experience value.

Federated learning facilitates the collective training of a model to optimize a global objective function based on data that remains local at each vehicle and does not need to be shared. This goal is achieved by providing a mathematical framework that guarantees privacy, security, and reliability while remaining mathematically elegant and operationally effective. Nevertheless, data privacy and security are critical requirements of vehicular systems. Although the large majority of data generated by the vehicles during their journey lack any critical personal information, trade-offs between data and privacy must be carefully evaluated in practice. In a federated learning context, where a large variety of vehicles from different manufacturers are collaborating, issues may arise regarding the potential exchange of data.

Fig 1: Privacy-Preserving Collaborative Intelligence: A Federated Learning Framework for Multi-Manufacturer Automotive Networks

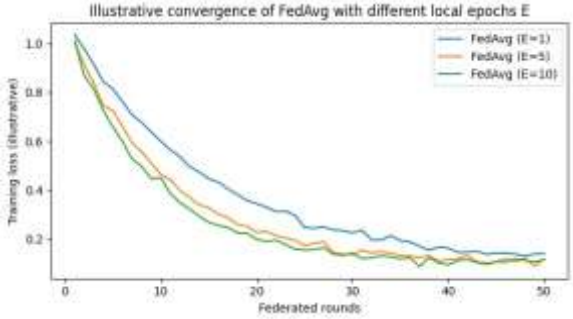
2. Background and Motivation

Privacy and confidentiality concerns have long impeded the success of independent collaborative learning in federated AI. One potentially effective solution to the privacy paradox in these AI tasks involves the local training of separated models on the premises of the collaborating manufacturers, clients or data holders, with stored-available data being transformed to differentially private data. A privacy-preserving vortex-opening means can be detected or not by a privacy-subsidized modifying strategy. The practical advantages are furthermore twofold: on one hand, the collaboration can strengthen the generalization abilities of non-specialists, turn ownership-erroneous models into perfect reconstructors or even detectives. On the other hand, the successful commercial plans of different providers in high-connectivity environments stimulate the business of low cost and higher yield operators, such as the

ISSN: 3067-4190
JOURNAL OF ARTIFICIAL INTELLIGENCE AND BIG DATA DISCIPLINES
Volume: 03 Issue: 02
RECEIVED: APRIL 20 REVISED: MAY 03 ACCEPTED: MAY 21 PUBLISHED: JUNE 04

long-established Unmanned Aerial Vehicle (UAV) companies and supported manufacturers.

A vivid driving example in this sense, already undergoing the pilot testing stages in many world areas, comes from Federated Learning (FL) systems and CAD networks based on Connected and Autonomous Vehicles (CAVs). These new FL technologies reproduce the hyper-parameters of a large data-centric model registered in the thematic space with a much reduced access to the huge amount of training data but using data that cannot be shared directly between the parties. The specification of the CAD users constitutes an additional opportunity for the FL ecosystem. The different manufacturers can own active-modifiable models that combine data from different cars, transferring local knowledge to the specific data-owners that collaborate in the learning process without specializing the services.



2.1. Key Drivers and Challenges in Federated Learning for Autonomous Driving

Federated Learning (FL) is pertinent to the area of connected vehicles, where a lot of data can be shared by the sensors of the vehicles connected via communications, cooperatively supervised by the communications networks, which can therefore improve the performance of FL and speedup its convergence. For autonomous driving, FL presents perhaps the only practical solution to providing machine learning to each of the driverless cars due to the safety and security concerns. These cars are expected to carry critical information about collision situations but at the same time they are manufactured by different vendors; vehicles may be different from the view dimensionality when neighbouring cars go through a scene from different angles. However, there exists safety, security and comfort issues. Privacy protection of the information from a vehicle is the essence when communication game is implemented with other vehicles.

FL also addresses the generalization performance of machine learning models and improve the convergence of DNNs with less information available from the layers in the front delivering less informative latent representations. The speed of private communication between vehicles is limited and thus the shared data can only be transformed at a lower speed than what common practice of deep learning requires. Yet either data compression or bandwidth augmentation is not practically implementable in these play games. Nevertheless, the mutual provision should substantially reduce or even eliminate the danger in autonomous driving.

Equation 1: Global optimization objective (what FL is solving)

Step 1: Define local datasets

- There are N vehicles/clients.
- Vehicle i has dataset D_i with size $n_i = |D_i|$.

Step 2: Define local empirical risk

Let the model parameters be $w \in \mathbb{R}^d$.
Define the per-sample loss $\ell(w; x)$. Then vehicle i's objective is:

$$F_i(w) = \frac{1}{n_i} \sum_{x \in D_i} \ell(w; x)$$

Step 3: Define the global objective (weighted by data size)

Let $n = \sum_{i=1}^{N} n_i$. Then the global FL objective is:

$$F(w) = \sum_{i=1}^{N} \frac{n_i}{n} F_i(w)$$

ISSN: 3067-4190
JOURNAL OF ARTIFICIAL INTELLIGENCE AND BIG DATA DISCIPLINES
Volume: 03 Issue: 02
RECEIVED: APRIL 20 REVISED: MAY 03 ACCEPTED: MAY 21 PUBLISHED: JUNE 04

Step 4: FL training goal

$$w^{\star} = \arg\min_{w} F(w)$$

3. Federated Learning Fundamentals

In the context of collaborative machine learning across mobile devices, Federated Learning (FL) refers to a paradigm in which multiple clients join and contribute in a distributed manner to train a shared model, while retaining their own training data privately on-device. The FL system is depicted in Fig. 3.1. At each iteration, a leader server samples a small subset of clients over the FL communication network (i.e. K-out-of-N sampling). The selected clients download the latest model from the server, train it on their local data, and upload the updates back to the server, which uses the updates to update the global model. Unlike traditional distributed learning where communication typically happens at the parameter-server architecture with workers exchanging model parameters, FL updates the model in an aggregation-based manner. In different variations of communication-efficient FL across mobile devices, a native network communication stack is leveraged and built-in protocol-defined capabilities, happening over data plane and control plane. The PSless hybrid structure enables, on mobile networks, real-time data upload, low-latency service provisioning, two-way service interaction, without introducing additional network overhead. The structure can also well support the event-driven communication of FL by confining the scheduling decision to the control plane during flood/congestion periods.

Symbol	Meaning
N	Total vehicles/clients in the federation
K	Vehicles selected per round (K-out-of-N sampling)
t	Federated round index
S_t	Set of selected vehicles in round t
D_i	Local dataset at vehicle i
n_i	Number of samples at vehicle i
$n = \sum_i n_i$	Total samples across clients (or selected clients, depending on context)
w_t	Global model parameters at round t
$w_{t+1}^{(i)}$	Local model of client i after training in round t
$\Delta_t^{(i)}$	Client update: $\Delta_t^{(i)} = w_{t+1}^{(i)} - w_t$
E	Local epochs per selected vehicle
η	Local learning rate
μ	FedProx proximal strength
ε, δ	Differential privacy parameters
C	Gradient clipping norm bound
σ	Noise multiplier/standard deviation scaling for Gaussian noise

3.1. Privacy and Security Considerations

In Federated Learning, user data never leaves local devices or servers. Only model parameters are exchanged and aggregated. Therefore, data privacy is preserved. Furthermore, the training dataset of any device is inaccessible to other devices during training, thus reducing the risk of unwanted or malicious sharing of sensitive data. Nevertheless, the aggregated global model may still reveal some private information regarding users or their behavior. Defense mechanisms for privacy-preserving Federated Learning find solutions against model inversion attacks, which exploit the fact that the devices contribute more to the global model than those with fewer collected samples, leaking information about the dominating users. To counter this issue, a Privacy-preserving Mechanism against Model Inversion-based Attacks on Federated Learning is implemented, which relies on global model noise infusion. While privacy is an important concern, security measures must also be implemented to ensure that potentially compromised devices do not inject adversarial samples into the system. Devices may get hacked or operate with malicious purposes. Malware attacks alter model weights by node compromise, model poisoning attacks alter the

ISSN: 3067-4190
JOURNAL OF ARTIFICIAL INTELLIGENCE AND BIG DATA DISCIPLINES
Volume: 03 Issue: 02
RECEIVED: APRIL 20 REVISED: MAY 03 ACCEPTED: MAY 21 PUBLISHED: JUNE 04

model update from compromised devices to influence the global model and backdoor attacks implant a hidden trigger in the model. Such malicious threats must be identified and prevented. For example, Secure Federated Learning can identify malware and trigger backdoor attacks, but not model poisoning attacks. Inconsistencies in the updates exchanged among devices can be detected and filtered by secure econometric learning for the communication in Federated Learning without explicit identification and quantification of poisoning samples. Albeit capable of filtering a wide range of attacks without sampling complexity, such approaches have no longer concentrated on Federated Learning.

Fig 2: Securing the Decentralized Frontier: A Hybrid Framework for Noise-Infusion Privacy and Econometric Anomaly Detection in Federated Learning

4. System Architecture for Multi-Manufacturer Collaboration

The federated learning framework can be used to design a system that enables joint testing and verification of autonomous-driving algorithms among a network of vehicles manufactured by different companies. Manufacturers play the leading roles in the setup and orchestration of federated learning tasks. A network of vehicles is formed according to the data owned by the vehicles, with one vehicle serving as the master during the learning operation.

The design of communication-efficient strategies during training heavily influences the performance of federated learning algorithms, especially in a bandwidth-limited vehicular network environment. Therefore, strategies that compress, quantize, asynchronously train, or trigger updates based on event detections significantly improve the training performance and model accuracy. Nevertheless, the certification of a vehicle's data or model privacy remains a challenge. Conventional model-inversion attacks against the central server usually target medical or personas data and cannot be used in the vehicular domain; however, a new kind of attack called model inversion with differential privacy (MDIP) has been specifically developed for a federated-learning-based connected-vehicle application and that consider the threat model.

Item	Equation	What it means
Local loss at client i	$F_i(w) = \frac{1}{n_i}\sum_{x\in D_i} \ell\,(w;x)$	Average loss over local data
Global FL objective	$F(w) = \sum_{i=1}^{N} \frac{n_i}{n} F_i(w)$	Weighted average of client objectives
Training goal	$w^{\star} = \operatorname{argmin}_w F(w)$	Find model minimizing global risk

4.1. Network Topology and Top-Level Roles

Labels for Top-Level Role Nodes in Figure 4: CT Vehicle Group Name; Telematics Service Provider; Cloud Application Service and Data Center Region Provider; and Cloud Operation Center Corporate Manages. The system architecture proposed for collaborative autonomous driving encompasses the vehicles and communication links, as well as two types of non-vehicle sites. Top-level role nodes, with significance that transcends vehicle manufacturers, are the communication link nodes and the nodes at both ends of the communication links. In the architecture, these two types of nodes establish the network topology through

ISSN: 3067-4190
JOURNAL OF ARTIFICIAL INTELLIGENCE AND BIG DATA DISCIPLINES
Volume: 03 Issue: 02
RECEIVED: APRIL 20 REVISED: MAY 03 ACCEPTED: MAY 21 PUBLISHED: JUNE 04

which the vehicles of different manufacturers communicate for federated learning and through which the-used clouds access the federated-aggregated model to meet the telematics service user requirements. In established applications requiring classifying vehicles by their owner manufacturers, these communication links enable collaboration among multiple manufacturers with privacy and security guarantees—data associated with the operation and use of manufacturers' vehicles are processed by their respective manufacturers without being shared with the other manufacturers.

Equation 2: Client sampling (K-out-of-N) and one FL round

Step 1: Select clients

At round t, the server samples a subset:

$$S_t \subseteq \{1,2,\dots,N\}, \quad |S_t| = K$$

Step 2: Broadcast global model

Server sends current global parameters w_t to all $i \in S_t$.

5. Federated Learning Algorithms for Autonomous Driving

Autonomous vehicles are complex distributed systems equipped with multiple sensors and cameras that generate a rich source of training data. Consequently, it is increasingly common to deploy machine learning algorithms onboard the vehicle to enhance road safety and reliability of driving decisions. By processing local data, these on-vehicle learning schemes minimize risk exposure during model training, helping address privacy and security requirements. Nevertheless, a high accident rate among self-driving vehicles indicates that improving safety and reliability remains critical. For this purpose, collaborative learning is promising. Thanks to the presence of high-capacity computing and storage devices, connected vehicles can learn from each other through vehicle-to-infrastructure or vehicle-to-vehicle communications. Real-world driving situations that are infrequently encountered, or even never encountered, can be safely employed for training with the help of surrounding vehicles. Yet, due to the different manufacturers involved in the training process, directly sharing the driving data amongst connected vehicles is no longer acceptable.

As a solution to this issue, recent years have witnessed an increasing interest in federated learning—a distributed learning paradigm that enables multiple organizations to jointly train a shared machine learning model without raw data sharing. Central to this technique is the fact that the participation of clients (i.e., local workers from different manufacturers) in the joint training process is voluntary. Each client can independently determine whether it has completed sufficient local model training and whether the improvements justify the sharing of model updates with others. Consequently, federated learning provides the appropriate approach for connected vehicles. For the specific Federated Averaging and local model update scheme targeting Federated Learning, a vehicle can upload its local model update to the central server for the first time only if its training checkpoint satisfies two conditions: completion of local model training and performance improvement with respect to the previous global model. These features enable those vehicles actively under training to utilize the latest progresses made by others while providing the remaining vehicles with an active model that is as good as possible.

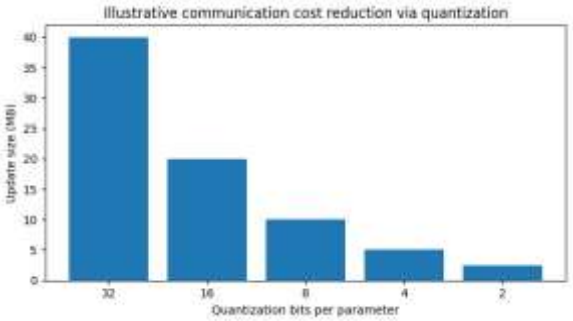
ISSN: 3067-4190
JOURNAL OF ARTIFICIAL INTELLIGENCE AND BIG DATA DISCIPLINES
Volume: 03 Issue: 02
RECEIVED: APRIL 20 REVISED: MAY 03 ACCEPTED: MAY 21 PUBLISHED: JUNE 04

Fig 3: Cross-Manufacturer Collaborative Intelligence: A Federated Averaging Framework for Privacy-Preserving Collective Learning in Connected Autonomous Vehicles

5.1. Federated Averaging and Variants

The standard approach to perform FL in a distributed learning setting is called FedAvg. It is based on the following key steps. A central server randomly selects a subset of connected vehicles and sends the current global model to them. The selected vehicles locally update the parameters on their private datasets for \(E\) epochs and send the updated parameters back to the server. The server then pools the received parameters and updates the global model accordingly. The process is repeated until convergence.

In addition to the basic FedAvg approach, several variants have been proposed that tailor FedAvg to the specific requirements and constraints of vehicular networks, such as heterogeneous data distributions among vehicles, sluggish and intermittent connectivity, lack of communication resources, high delay, and unreliable computing capabilities. For example, FedProx introduces a proximal term in the local objective to stabilize FedAvg training in the presence of non-IID client data. A generalized version adopts a randomly weighted periodic averaging rule that mitigates the need for synchronous aggregation and respects the timing of clients' parameter uploads. Another generalized version employs an asynchronous architecture, thereby permitting the asynchronous execution of local training tasks.



5.2. Personalization and Transfer Learning in Connected Vehicles

To enhance system performance, personalization strategies in the form of transfer or multi-task learning can be introduced in conjunction with FL. Valamouti et al. suggest combining FL with model-domain transfer learning (MDT) in CAV systems where conventional vehicles are present. CAVs are often specialized for certain scenarios or exhibit unique features, and MDT allows knowledge transfer across domains. To tackle heterogeneous CAV features and training samples, Jiang et al. propose a multi-task FL framework that not only trains personalized models locally, but also caters to the entire network through a shared model. The hierarchical structure enables lightweight local models that require minimal sample and communication overhead while optimizing global model training. Personalized FL models have also been considered for V2X markets, where federated learning is used for V2I learning, and different urban scenarios are modeled as user groups. Each vehicle can then play the roles of both local trainer and global learner, enhancing the generalizability of the fast-trained model for surrounding vehicles by fine-tuning it under different scenarios. A federated-multitask-support vector machine approach, where support vector machines are trained for different environments based on local pros/cons, enables multi-task learning capability by exploiting data similarities under a FL setting.

ISSN: 3067-4190
JOURNAL OF ARTIFICIAL INTELLIGENCE AND BIG DATA DISCIPLINES
Volume: 03 Issue: 02
RECEIVED: APRIL 20 REVISED: MAY 03 ACCEPTED: MAY 21 PUBLISHED: JUNE 04

6. Privacy-Preserving Techniques and Threat Models

Although information about the driver and the vehicle itself may not seem sensitive to an individual car owner, leaked data can still bring severe consequences. For instance, knowledge about the start and endpoint of travel can lend support to criminals for robbery, kidnapping, or support for terrorism. Vehicle data becomes even more valuable when data from several surrounding cars are linked together. As a result, automobile manufacturers need to protect not only their own data but also the data from other cars with whom they share information. Even with ideal protection, vehicle data still has to be secured.

For data confidentiality and sensitive information protection of vehicles on the cloud platform in federated machine-learning model training, a new privacy-preserving method integrating personalized differential privacy into FL training with homomorphic encryption is presented. Personalized differential privacy employs different privacy budgets for different datasets to obtain better utility than traditional differential-privacy technology. Based on the analysis of the adversary model, attack surface, the maximum non-colluding server number, and trade-off of model accuracy and user privacy, a new selective decryption strategy is provided to ensure the private model with the highest accuracy.

Equation 3: FedAvg (Federated Averaging) — complete derivation

Server selects vehicles, vehicles train locally for E epochs, send back parameters, server pools and updates.

Step 1: Local training objective on each selected vehicle

Each selected vehicle $i \in S_t$ starts from:

$$w_t^{(i,0)} = w_t$$

Step 2: Local SGD updates (inner loop)

For local step $s = 0,1, \ldots$, SGD does:

$$w_t^{(i,s+1)} = w_t^{(i,s)} - \eta\, g_i\left(w_t^{(i,s)}\right)$$

where $g_i(\cdot)$ is a stochastic gradient estimate on mini-batches from D_i.

After E local epochs (some number of SGD steps), we denote final local parameters:

$$w_{t+1}^{(i)} = \text{LocalTrain}(w_t, D_i, E)$$

Step 3: Convert to a "model delta" form (often used)

Define local update:

$$\Delta_t^{(i)} = w_{t+1}^{(i)} - w_t$$

So equivalently:

$$w_{t+1}^{(i)} = w_t + \Delta_t^{(i)}$$

Step 4: Server aggregation (the "averaging")

Let $n_{S_t} = \sum_{i \in S_t} n_i$.
Server forms weighted average:

$$w_{t+1} = \sum_{i \in S_t} \frac{n_i}{n_{S_t}}\, w_{t+1}^{(i)}$$

Step 5: Substitute the delta form to show it's an averaged update

$$w_{t+1} = \sum_{i \in S_t} \frac{n_i}{n_{S_t}}\left(w_t + \Delta_t^{(i)}\right) = w_t \sum_{i \in S_t} \frac{n_i}{n_{S_t}} + \sum_{i \in S_t} \frac{n_i}{n_{S_t}} \Delta_t^{(i)}$$

But $\sum_{i \in S_t} \frac{n_i}{n_{S_t}} = 1$. So:

$$\boxed{w_{t+1} = w_t + \sum_{i \in S_t} \frac{n_i}{n_{S_t}}\, \Delta_t^{(i)}}$$

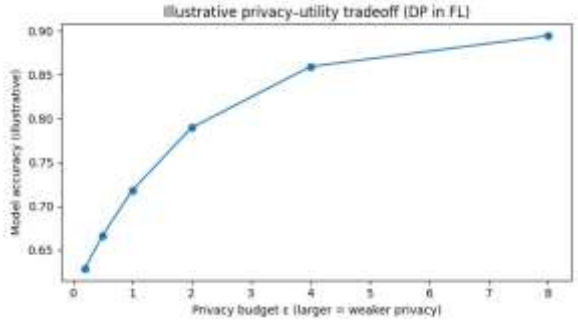
This is the clean "FedAvg update equation".

ISSN: 3067-4190
JOURNAL OF ARTIFICIAL INTELLIGENCE AND BIG DATA DISCIPLINES
Volume: 03 Issue: 02
RECEIVED: APRIL 20 REVISED: MAY 03 ACCEPTED: MAY 21 PUBLISHED: JUNE 04

6.1. Differential Privacy in Vehicle Data

To the best of the existing knowledge base, the introduction of federated learning (FL) into the automotive industry is still developing. FL applied to the vehicular domain brings together data from diverse manufacturers in a collaborative manner within a multi-cloud or multi-server setting, yet each manufacturer maintains control over its data. However, as in other federated learning systems, the information generated by the collected data might leak sensitive data of the vehicles and their drivers in case of adversary access. Recent reports suggest that trajectory prediction models trained with data collected from smart vehicles might expose sensitive information about the trajectories followed. When applied to FL-based autonomous driving, this information leak is dangerous because adversaries might—infer the driving behavior of the vehicles generating the driving models and profile or localizar (using location tracking) the affected vehicles and their drivers. In addition, adversaries might even reconstruct parts of the private training dataset. All the privacy threats identified add motivation for including privacy-preserving mechanisms in FL-based vehicle collaborative training systems.

Differential-privacy (DP) techniques manage to mathematically quantify the privacy guarantee offered to sensitive information by adding noise to data. Digital sharing systems with DP techniques can share models and parameters without leaking private data or exposing the driving behavior of vehicles during prediction. Following a general definition, a system is said to be -differentially private if the outputs of the mechanism are almost equally likely to occur (with a probability ratio of at most e) whether or not any individual's information is included in the input dataset. In a federated learning system, the objective is to protect the parameters generated by each vehicle during the training phase. More specifically, the gradient of the cost functions defined during training is considered to be the sensitive information. Since different vehicles are trained using different datasets, the parameters produced should vary from vehicle to vehicle. Adding noise to the updates of the global model is a strategy to keep it privacy-preserving, keeping the previous definition in mind.



7. Communication-Efficient Training in Vehicular Networks

The significant privacy and security concerns of personal data collection in data-centered ML methods limit their channel selection for collaboration. Therefore, ML solutions that maintain higher privacy and security protection while meeting the specific needs of the connected service-scenario realization are critical. Nonetheless, training these privacy-preserving ML models often involves large communication overhead, making them difficult to deploy in practical vehicle networks. Techniques to decrease the communication cost of the training process should be studied. For instance, gradient compression and quantization may be employed to shrink the model update size for efficient allocation in the vehicular network. Further, asynchronous or event-triggered update strategies may also be integrated into the training process to relax the parameter synchronization constraint among Federated Learning participants. Federated Averaging (FedAvg) and its variants are mostly deployed in autonomous driving scenarios, yet individual vehicle model updates may not equal updates for cloud models due to differences in training dataset diversity and sample size. Consequently, personalization methods are particularly important to better align individual vehicle model updates with their corresponding FedAvg updates in vehicular networks. Beyond simple local fine-tuning or learning within the model parameter space, better transfer learning solutions for connected vehicles can also help to meet the specific driving conditions of each vehicle. Connected vehicle data with a similar driving context but

ISSN: 3067-4190
JOURNAL OF ARTIFICIAL INTELLIGENCE AND BIG DATA DISCIPLINES
Volume: 03 Issue: 02
RECEIVED: APRIL 20 REVISED: MAY 03 ACCEPTED: MAY 21 PUBLISHED: JUNE 04

not strictly the same driving task, e.g. from different brands and different levels of vehicle autonomy, may be spatio-temporally close data. Utilizing these spatio-temporally close datasets from adjacent vehicles may help to train higher-quality models within these connected vehicles even if the models are independently trained.

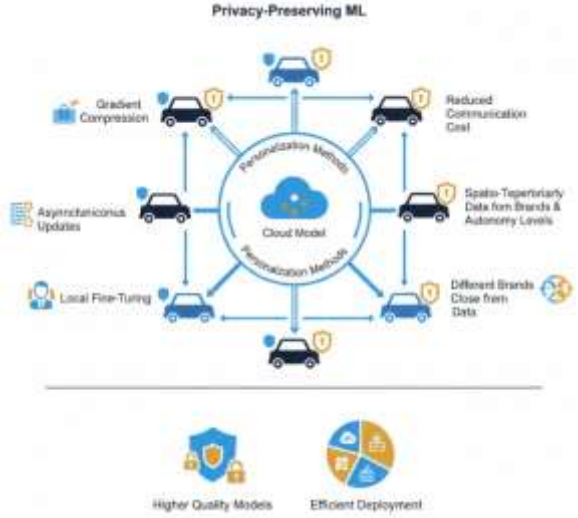


Fig 4: Personalized and Communication-Efficient Federated Learning for Connected Vehicles: A Framework for Spatio-Temporal Data Transfer and Compressed Asynchronous Model Updates

7.1. Model Compression and Quantization

Machine-learning-based methods for intelligent transportation systems (ITS) can benefit from federated learning, providing more accurate models while protecting the privacy of personal information. However, the efficiency of communication throughout the training process should also be considered. Whether traffic signal control based on federated learning or a federated learning approach for connected vehicles is being examined, the communication overhead in sending raw model parameters is significant. Model compression techniques can be applied to compress gradients and achieve improved communication efficiency.

Model compression schemes express the model weight parameters via lower bit precision. For example, in model quantization, the model weight parameters are quantized into a limited number of represented values. In connected vehicle networks with large-scale data, quantization methods based on information theory lead to limited communication overhead. For a federated learning framework in which the system/server aggregates models from client vehicles with limited memory, gradient/weight compression based on low-rank approximation contributes to communication efficiency. It can even achieve improved testing accuracy when the aggregated model is compressed. Quantization can also be employed to convert the models of any client vehicle in a connected vehicle network into a sequence of identical bits through the designed mapping table, hence significantly reducing the communication cost.

7.2. Asynchronous and Event-Driven Updates

Though autonomous vehicles can collect a large amount of data during training, it is still difficult to collect data for each situation of driving, such as rare events. These situations require sufficient samples for model training. Otherwise, the model becomes a “one mark” model and poorly generalizes to other unique situations of driving. In such cases, other participating vehicles can help prediction through appropriate updating. To this end, asynchronous communication updates or an event-driven model training mechanism are implemented.

In the asynchronous cooperation mechanism, each vehicle can conduct local model training on its own sample set periodically. When a model update arrives, it can modify the model by using a partially trained asynchronous optimizer. The complete training can be done at the cloud component when it receives several updates. The communication overhead can be alleviated because not all vehicles need to participate in model updating. It still can cover most of the sample segments. Event-driven cooperation strategy can use other vehicle models as an auxiliary reference when it runs in critical driving events, such as accidents, sudden brake, blind turn with stability, and so on. After model training, the algorithm can store these critical situations as auxiliary triggers. When a vehicle meets these situations, it can take the corresponding auxiliary models through the vehicle-to-vehicle (V2V) communication and make predictions. The model outputs

ISSN: 3067-4190
JOURNAL OF ARTIFICIAL INTELLIGENCE AND BIG DATA DISCIPLINES
Volume: 03 Issue: 02
RECEIVED: APRIL 20 REVISED: MAY 03 ACCEPTED: MAY 21 PUBLISHED: JUNE 04

can be fully considered and discarded based on the knowledge hybrid fusion algorithm.

8. Conclusion

The growing complexity of autonomous driving could be well addressed by collaborative learning methods like Federated Learning (FL). They allow vehicular manufacturers to train their models based on multiple fleets' data without transmitting the vehicle data to a cloud server, effectively solving data privacy and ownership issues. The FL framework for collaborative autonomous driving, and its associated challenges, research branches, and an FL-based model-update method to suit the particular requirements of discrete, gradient- and latency-sensitive vehicular applications are examined. FL aims to pursue a global model by synchronously combining each vehicle's own model and using a small amount of related data from others. Nevertheless, even within such a large swathe of data, the local data of each participating node usually differ semantically, resulting in poor generalization ability of the global model for those vehicles. Personalization and transfer techniques are necessary for enhancing the performance of connected vehicles and also for minimizing model training time when a brand-new vehicle enters the network.

Federated Learning (FL) is a distributed machine learning method that allows multiple parties to collaboratively train an intelligent model without sharing their own private datasets. In its extensive application, an autonomous-driving model can be trained for cars from different manufacturers by aggregating the knowledge gained from various vehicle fleets with different local datasets. It empowers vehicles to share their autonomous-driving experiences with others without data leakage, and even provides the cooperation ability for situations where data-sharing is forbidden by law. The combination of these elements expedites autonomous-driving deep-learning algorithm convergence and model performance. However, the asynchronous nature of the training process also needs to be taken into account as the FL framework is susceptible to model accuracy drop when applied to heterogeneous in-distribution or out-of-distribution data.

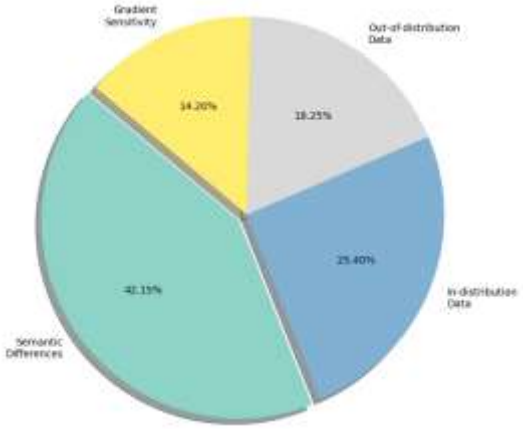


Fig 5: Impact of Heterogeneous Local Datasets

8.1. Final Thoughts and Future Directions

Federated learning enables vehicles manufactured by different companies to collaboratively train machine learning models without revealing sensitive local data. In a federated-learning setting, data owners with similar tasks can train machine-learning models across a decentralized system. The system trains a shared global model on a central server using parameters learned from local updates submitted by distributed data sources, restricting direct exchange of raw data between data owners while still enabling beneficial knowledge sharing.

Multi-manufacturer vehicle collaborations are beneficial for colocated vehicles with similar driving patterns, when data-sharing agreements are difficult to negotiate, or when regulatory requirements prohibit sharing of certain data. Demand for federated-learning approaches to autonomous driving is growing, driven by privacy considerations, local data scarcity, and the high resource consumption of training locally using re-visioned datasets. However, their deployment in vehicle networks necessitates addressing challenges pertaining to privacy leaks at a participating vehicle, communication costs associated with distributed training, and the support of personalization. Solutions to address these difficult challenges exist.

9. References

1. Abad, G., Picek, S., Ramírez-Durán, V. J., & Urbieta, A. (2021). On the security & privacy in federated learning. In Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR).
2. Chellapandi, V. P., Yuan, L., Brinton, C. G., Żak, S. H., & Wang, Z. (2024). Federated learning for connected and automated vehicles: A survey of existing approaches and challenges. IEEE Transactions on Intelligent Vehicles, 9(1), 119–137.
3. Inala, R. (2023). Big Data Architectures for Modernizing Customer Master Systems in Group Insurance and Retirement Planning. Educational Administration: Theory and Practice, 29(4), 5493-5505.
4. Chellapandi, V. P., Yuan, L., Żak, S. H., & Wang, Z. (2023). A survey of federated learning for connected and automated vehicles. In 2023 IEEE 26th International Conference on Intelligent Transportation Systems (ITSC).
5. Cui, Y., Zhu, J., & Li, J. (2024). FLAV: Federated learning for autonomous vehicle privacy protection. Ad Hoc Networks.
6. Dai, R., Shen, L., He, F., Tian, X., & Tao, D. (2022). DisPFL: Towards communication-efficient personalized federated learning via decentralized sparse training. Proceedings of the 39th International Conference on Machine Learning, 162, 4587–4604.
7. Donevski, I., Nielsen, J. J., & Popovski, P. (2021). On addressing heterogeneity in federated learning for autonomous vehicles connected to a drone orchestrator. Frontiers in Communications and Networks, 2, Article 709946.
8. Fu, Y., Tang, X., Li, C., Yu, F. R., & others. (2024). A secure personalized federated learning algorithm for autonomous driving. IEEE Transactions on Intelligent Transportation Systems, 25(12), 20378–20389.
9. Hu, X., Li, R., Ning, Y., Ota, K., & Wang, L. (2023). A data sharing scheme based on federated learning in IoV. IEEE Transactions on Vehicular Technology.
10. Lee, J., Ko, H., & Pack, S. (2022). Adaptive deadline determination for mobile device selection in federated learning. IEEE Transactions on Vehicular Technology, 71(3), 3367–3371.
11. Lee, J., Ko, H., Seo, S., & Pack, S. (2023). Data distribution-aware online client selection algorithm for federated learning in heterogeneous networks. IEEE Transactions on Vehicular Technology, 72(1), 1127–1136.
12. Li, X., Jiang, M., Zhang, X., Kamp, M., & Dou, Q. (2021). FedBN: Federated learning on non-IID features via local batch normalization. In International Conference on Learning Representations.
13. Li, Y., Tao, X., Zhang, X., Liu, J., & Xu, J. (2022). Privacy-preserved federated learning for autonomous driving. IEEE Transactions on Intelligent Transportation Systems, 23(7), 8423–8434.
14. Li, Y., Li, H., Xu, G., Xiang, T., & Lu, R. (2022). Practical privacy-preserving federated learning in vehicular fog computing. IEEE Transactions on Vehicular Technology, 71(5), 4692–4706.
15. Liu, J., Yin, Z., Nie, L., & Zhao, X. (2024). Federated learning enable training of perception model for autonomous driving. SAE Technical Paper, 2024-01-2873.
16. Segireddy, A. R. (2024). Machine Learning-Driven Anomaly Detection in CI/CD Pipelines for Financial Applications. Journal of Computational Analysis and Applications, 33(8).
17. Liu, S., Yu, G., Yin, R., & Yuan, J. (2023). Communication and computation efficient federated learning for Internet of Vehicles with a constrained latency. IEEE Transactions on Vehicular Technology.
18. Ma, L., Liao, Y., Zhou, B., & Xi, W. (2023). PerHeFed: A general framework of personalized federated learning for heterogeneous convolutional neural networks. World Wide Web, 26, 2027–2049.
19. Ma, X., Zhang, J., Guo, S., & Xu, W. (2022). Layer-wised model aggregation for personalized federated learning. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 10092–10101.

20. Marfoq, O., Neglia, G., Vidal, R., & Kameni, L. (2022). Personalized federated learning through local memorization. Proceedings of the 39th International Conference on Machine Learning, 162, 15070–15092.
21. Montazeri, M., Kebriaei, H., Araabi, B. N., Kang, J., & Niyato, D. (2023). Distributed mechanism design in continuous space for federated learning over vehicular networks. IEEE Transactions on Vehicular Technology, 72(4), 4196–4206.
22. Nguyen, A., Do, T., Tran, M., Nguyen, B. X., Duong, C., Phan, T., Tjiputra, E., & Tran, Q. D. (2021). Deep federated learning for autonomous driving.
23. Parekh, R. D., Patel, N., Gupta, R., Jadav, N. K., & others. (2023). GeFL: Gradient encryption-aided privacy preserved federated learning for autonomous vehicles. IEEE Access, 11, 1825–1839.
24. Kumar, K. M., Parasar, A., Walia, A., Inala, R., & Thulasimani, T. (2025, August). Enhancing Risk Management Strategies in Financial Institutions Using CNN and Support Vector Regression. In 2025 5th Asian Conference on Innovation in Technology (ASIANCON) (pp. 1-6). IEEE.
25. Shinde, S. S., Bozorgchenani, A., Tarchi, D., & Ni, Q. (2022). On the design of federated learning in latency and energy constrained computation offloading operations in vehicular edge computing systems. IEEE Transactions on Vehicular Technology, 71(2), 2041–2057.
26. Wang, S., Li, C., Ng, D. W. K., Eldar, Y. C., Poor, H. V., Hao, Q., & Xu, C. (2023). Federated deep learning meets autonomous vehicle perception: Design and verification. IEEE Network, 37(3), 16–25.
27. Wang, S., Hong, Y., Wang, R., Hao, Q., Wu, Y.-C., & Ng, D. W. K. (2022). Edge federated learning via unit-modulus over-the-air computation. IEEE Transactions on Communications, 70(5), 3141–3156.
28. Zeng, T., Semiari, O., Chen, M., Saad, W., & Bennis, M. (2022). Federated learning on the road: Autonomous controller design for connected and autonomous vehicles. IEEE Transactions on Wireless Communications, 21(12), 10407–10423.