National College of Ireland

Federated Deep Learning for Privacy-Preserving Collaborative Data Sharing and Fault Recovery in Connected Vehicles

Research Project

MSc Cloud Computing

Siranjeevi Muthusamy

Student ID: x22241647

School of Computing

National College of Ireland

Supervisor: Yasantha Samarawickrama

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Siranjeevi Muthusamy
Student ID:	x22241647
Programme:	MSc Cloud Computing **Year:** 2023-2024
Module:	Research Project
Supervisor:	Yasantha Samarawickrama
Submission Due Date:	16-09-2024
Project Title:	Federated Deep Learning for Privacy Preserving Collaborative Data Sharing and Fault Recovery in Connected Vehicles
Word Count:	6851 **Page Count:** 19

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: 

Date: **16th Sep 2024**

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Federated Deep Learning for Privacy-Preserving Collaborative Data Sharing and Fault Recovery in Connected Vehicles

Siranjeevi Muthusamy
x22241647

Abstract

In smart connected internet-of-vehicles (IoVs), locally generated sensory data contains the most important and knowledgeful vehicle-related information captured from onboard units like speedometers, dashboard cameras, and location trackers can offer deeper insights into its status. Through IoV with autonomous driving, this data can be used to optimize and update over-the-air (OTA) driving models from vectors on a cloud or supercomputer that can improve traffic handling dynamically. The current method of using centralized servers for processing vehicle data is limited in its ability to deliver real-time analysis which causes long-lasting vehicle downtimes because it does not consume the common localized information located throughout the IoV network. This research has been influenced to understand if federated learning (FL) can enable privacy-preserving, collaborative use of data from connected intelligent vehicles, while also being robust against vehicle faults. To realize this objective, we propose an FL framework that utilizes deep learning (DL) algorithms such as feed-forward neural networks (FNNs) and convolutional neural networks (CNN), to obtain vital information from vehicular data to collaboratively train models that manage vehicle operations, without the need to share raw vehicle data. The proposed methodology concatenates local model training and global aggregation of the models of every vehicle belonging to the IoV network to overcome security threats, and communication overhead from sharing huge volumes of raw data between vehicles in a high-precision driving scenario. This ensures improved throughput with reduced uplink communications by offering enhanced privacy on large-scale datasets. The proposed FL framework is tested for accuracy, and effectiveness through a case study experiment on the MNIST dataset to diagnose faults and recovery times in the vehicle operation which will not only reduce downtime of the vehicle but will also provide an exquisite driving experience backed with the extracted intelligence from decentralized FL computing models.

Keywords: Federated Learning, Deep Learning, Internet-Of-Vehicles, Collaborative Data Sharing, Fault Diagnosis

1 Introduction

1.1 Problem Background

In connected vehicles, most status analysis needs to be done using the data produced by the sensors local to the vehicle. This data could support in developing real-time route planning,

traffic update systems and driving models for the future IoV. Fault diagnosis in these systems would require dynamic processing as it involves a large amount of data. Current methods and analysis that use centralized servers for all the real-time data from vehicles are not sufficient. They are slow in response time and lead to high downtimes of vehicles because these systems fail to utilize the data distributed across the network. The capabilities of centralized systems to effectively adapt and respond quickly to faults is very much limited because of the ever-changing traffic patterns, unpredicted scenarios, and the variety of hardware configurations in diverse vehicular networks. (Dimitrios Michael Manias, 2021).

Moreover, these systems do not make use of the collectively available local information and the vehicle contextual information that is available across the network. This information can be used to achieve near real-time decentralized fault response time (Posner, 2021). The increasing complexity of vehicular systems and the need for real-time decision-making in autonomous vehicles highlights the importance of fault diagnosis and recovery mechanisms (Dimitrios Michael Manias, 2021). In centralized methods, it takes more time to collect all the data from the nodes of IoV at a central place. Also, the increasing importance of data privacy and security in interconnected vehicles highlights the need for development of solutions that decentralize intelligence sharing without compromising sensitive information (Elbir, 2022).

1.2 Motivation

The recent advancements in federated learning (FL) offer promising solutions for distributed machine learning (ML) models that focus on immediate fault response and data privacy. Its compatibility with IoV ecosystem and the capability of providing privacy-preserving data exchange and allowing fast response times without the need to transfer raw input data from vehicle(s) makes it the ideal solution for facilitating collaborative training across distributed onboard vehicle hardware.

However, only very few works have been done focused on using FL for automotive fault diagnostics, recovery, and restoring vehicle performance at its best. With the increasing complexity and the need for real-time decision-making in autonomous driving, designing efficient fault diagnosis and recovery mechanisms is becoming even more critical (Dimitrios Michael Manias, 2021). FL provides an interesting solution to these issues through decentralized model training and aggregation, which helps in the early detection of faults/recovery while preserving data privacy. Therefore, the goal of this research is to implement an FL framework using FNN and CNN models which can effectively utilize the data collected and shared in a large group of connected vehicles across IoV systems. This helps in analyzing faults as well as taking appropriate actions to reduce vehicle downtime and restoring its performance back into its optimal operational condition, thus providing better reliability than before.

1.3 Research Question

“In decentralized vehicular networks, how well does federated learning works in fault recovery, reducing recovery times, and restoring system performance to optimal levels by leveraging group intelligence?”

1.4 Research Objective

The objective of this research is to explore the capabilities of a federated learning scheme that employs convolutional neural networks (CNN) model and a feed-forward neural network (FNN) model as FL learners. These models utilize collected historical vehicle information in detecting failures, reducing total downtime, and restoring the system performance to optimal condition using a practical scenario case study.

1.5 Research Contributions

The major contributions of this paper are:

- Build a new FL framework for connected vehicular networks allowing vehicles to collectively train deep learning models for fault detection without sharing raw data.
- Compare the performance of CNN and FNN models trained on MNIST dataset in detecting fault patterns and analyzing multi-sensor vehicular data to extract useful insights from them under an FL environment using a case study.
- Our experimental goal is to evaluate the efficiency and feasibility of federated learning for fast recovering from faults, shortening downtimes for unmatched driving performance and improving transportation systems dependability.

1.6 Thesis Organization

Chapter 1: Describes the research problem, motivation, research question, research objective, and unique contributions of the research.
Chapter 2: Literature Review of studies and work in Federated Learning and its Applications in Intelligent Transportation Systems.
Chapter 3: Describes the proposed research methodology with the framework design and discusses its implications in terms of ethics.
Chapter 4: Describes deep learning architecture, optimization strategy development, and how to evaluate these using a case study.
Chapter 5: Implementation Details and Experimental Setup.
Chapter 6: The results are described along with the evaluation and analysis of these findings.
Chapter 7: Summarizes the major findings and limitations of the research.

2 Related Work

This section begins with a literature review of the vehicular network and studies how to integrate advanced technologies into this kind of network, discussing some models related to deep learning, federated learning, and fault recovery that can be adopted. This review also proposes to reveal some research gaps such as privacy models with improved performance and fast fault recovery mechanisms, which this work attempts to bridge using novel learning paradigms of federated learning.

2.1 Deep Learning for Vehicular Networks

The review work by (Hernandez, 2023) presents cloud computing in intelligent vehicles for parallel deep learning model integration with real-time data analysis. The promise of cloud-based solutions to more effectively process the massive volumes of autonomous vehicle data that will need to be managed over vehicular networks is one of the single, useful takeaways from this. Though it offers some of the future research directions to address these problems, it faces difficulties in data privacy and latency. This survey offers a full picture of the cloud technologies within intelligent vehicles, which suggest several effective and secure data handling methods are needed. The work by (Han, 2023) highlighted the integration of deep learning models in intelligent vehicles. The challenges it recognizes include data variety and communication overhead, thus indicating that going forward the research should focus on offering efficient solutions while keeping these in mind. The survey provides significant insights about the state of FL in transportation systems, and future directions towards the adaptive scalable solutions. Yet, we could improve the study in terms of having an in-depth detailed explanation on practical aspects of FL such as incentive mechanisms for participant selection and model aggregation strategy.

The study presented by (Palanisamy, 2019) addresses connected autonomous driving model utilizing a joint control multi agent mechanism that is based on deep reinforcement learning. The goal is to scale autonomous driving beyond geo-fences, using multi-agent interaction for learning control strategies in densely interacted and only partially visible urban intersections. This has implications for decision-making in autonomous vehicles, as cooperative decisions are crucial to ending the monopoly of centralized control imposed by single-agent scenarios. The model was demonstrated to learn different control policies directly from raw sensor inputs in a controlled urban scenario, indicating that DRL could help improve IoV infrastructure. The paper presented by (Altintas, 2020) develop a DRL-based cooperative perception framework for improving safety in connected vehicles. The model can reduce the network load creating a 12% improvement in terms of object detection accuracy with dynamic selection for data transmission. The proposed framework was assessed through both traffic and vehicle simulators to validate that it optimizes data exchanges suitable for a better utilization of network resources. In this paper, we tackle the problem of data selection for transmission in cooperative perception(V2V). The DRL approach proposed here provides a workable solution to the problem of data sharing among all connected vehicles, which enables the smart decision-making agents based on shared perception information. Nonetheless, future work could examine the impact of diverse traffic situations and more importantly on evaluating how well the framework scales to larger vehicular networks.

A collaborative edge computing framework for IoV based on DRL-MDP was proposed in the research paper by (Li, 2020), which can help to achieve effective resource management. This architecture aims to decrease the latency of computing services, enhance security by distributing workloads dynamically and change tasks performance at the edge. This paper verifies its feasibility in a simulative MEC-enabled vehicular network and found that the approach can enhance service reliability, latency as well demonstrate benefits of edge

computing to third-party data processor. With this paper, the authors make a valuable contribution to enhancing edge computing: it introduces an intelligence-based task offloading and scheduling approach for IoV. On the other hand, further research could be conducted with a focus on edge device heterogeneity and vehicle mobility to study the performance of the framework.

2.2 Federated Learning for Vehicular Networks

A blockchain-based decentralized federated learning for connected vehicles was proposed by (Pokhrel, 2020). This model solves both the privacy and efficiency issues of centralized FL models by making use of blockchain technology. The study uses mathematical modelling to regulate parameters for FL, establishing the possibility of decentralized training as an effective solution against high delays and faults. This research establishes a secure and efficient FL framework for vehicular networks with blockchain technology. The research could not be conducted in large-scale vehicular networks due to scalability and computational overhead issues of blockchain for federated learning-based privacy preservation. The recent study (Ye, 2020) proposed a selective model aggregation technique for federated learning in vehicular edge computing. They show that it consistently improves model aggregation for image classification, by providing better utility and efficiency over baseline models such as FedAvg. This approach maintains privacy while improving model utility and illustrates the benefits of selective aggregation in federated learning. This research helps in developing more sophisticated model aggregation algorithm for FL over vehicular environment, as they have low resource. From this work, the study can be carried forward by using other types of datasets to assess out different data-driven approaches and finally implementing the techniques in practical vehicular networks.

A privacy preserving FL architecture for automotive cyber physical systems is introduced by research (Lu, 2020). It describes how to prevent privacy and promote legal security with two-level intelligent data processing and leak detection system. The study justifies the need for enhanced privacy models in vehicular data sharing, and it practically proves its efficiency via an evaluation with a real-world dataset. In this study, a novel FL-based framework for safe data sharing in automotive networks was proposed. Future research can extend considering the effect of data heterogeneity in addition to malicious participants on performance for this proposed framework. (Li X. a.-Y., 2021) discussed about federated learning for collaborative data sharing in vehicular edge networks. The model seems to perform with less system latency and high efficiency in data sharing by deploying additional low-latency MEC servers. The researchers overcame data silo issues and network congestion by using a federated learning approach, as described in the study. The research demonstrates the possibility of achieving efficient and secure data exchange through FL which advances collaborative data sharing mechanisms for vehicular networks. However, the study can be extended to investigate how vehicle mobility and the dynamic nature of vehicular networks affect weather information dissemination performance in their FL-based data sharing framework.

Researchers that have worked on smart public transportation, including (Zhao, 2022), have presented an asynchronous FL model based on blockchain technology and investigated the

difficulties associated with FL. It allows the local models to scale dynamically, earning a better learning performance and resistance against attacks. Existing FL models are vulnerable, as shown in the study and numerical experiments suggest that the proposed approach is beneficial. The study's findings contribute to the development of a strong and secure FL framework for intelligent transportation systems by implementing blockchain-based foundations and asynchronous model updates. However, this study's analysis can be extended to include a more comprehensive assessment of its structure in actual transportation scenarios. (Zhao, 2022) introduced a Collaborative Authentication Protocol for Securely Sharing the Data in Social IoV. In this study, the protocol secures vehicle parameterizing by encryption and authenticates each communication for data transmission more secure and efficient. To enable privacy-preserving data sharing in IoV, they compare the proposed protocol with existing vehicle protocols. This research work, using the advantages of FL presents a protocol suitable for secure authentication schemes in social IoV. Still, more research can be done to find out how the protocol impacts computing overhead and scalability issues in big social IoV networks.

2.3 Fault Recovery Mechanisms in Vehicular Networks

To enable fault tolerance and self-recovery in federated learning systems, (Dautov et al., 2024) proposes the Raft consensus protocol. It uses Raft leader election and log replication behaviours for crawling engines, attempting to resolve the single point of failure issue in FL architectures. This ensures consistency across all the FL nodes and enables seamless training and model convergence by replicating logs. A proof-of-concept implementation was developed leveraging the Flower FL framework along with experiments that analyse aggregator re-election time and evaluate state replication overheads. While iterations cause network overhead as expected, the results prove a robust self-recovering FL system that performs well even in case of node failures maintaining model consistency. In summary, the paper proposes an innovative technique to address these hard real-world problems and provides a solution for preserving FL scalability, fault tolerance as well as maintaining long-term availability of such system.

A model for redundancy-aware collaborative federated learning for automotive networks is presented in the work of Huang et al. (2023). By treating each data value with the enough importance and reducing the number of redundant results, this leads to a better prediction node for the added value model. The study also shows how the redundancy-aware mechanisms that are suggested can be used through numerical simulations; further research is needed to evaluate these mechanisms experimentally in real-world networks. Additionally, a new node collaboration mechanism and data importance evaluation were proposed, which improves the performance of FL frameworks intended for vehicle networks. The study can be expanded to a more comprehensive assessment of the proposed framework on online vehicular networks with unreliable quality and network conditions. (Yan et al., 2023) aims to address this need by presenting an online learning framework for real-time sensor fault diagnosis of cyber-physical systems putting a particular focus on the case study of autonomous vehicles combined with Application independent control system. They designed the framework to be able to effectively detect and classify sensor faults, through a clustering-based data stream fault localization scheme. To address this gap in the literature, they attempt to develop accurate fault signature

generation models that accurately diagnose sensor faults and then establish an efficient robust model (which also works well for time-varying small severity sensor faults) within the study. This paper puts forward a framework for both online learning of fault diagnosis problems on autonomous vehicle and it can also be applied in other sub-systems scenarios. The study presented by (Manias and Shami, 2021) demonstrates that decentralized learning models are useful when minimizing the recovery time and benefiting in restoring system performance. It begins by surveying the existing fault recovery models and argues that federated learning provides a wonderful opportunity. This work presents the potential of using FL for efficient fault diagnosis among automotive systems and paves the way in creating collaborative, privacy-preserving fault recovery techniques. However, the work may be further extended to provide a comprehensive discussion on issues and challenges in terms of FL-based fault recovery mechanisms within resource-constrained vehicular environments. (Chen et al., 2021) proposed a Byzantine-Fault-Tolerant decentralized (BDFL) federated learning approach for autonomous vehicles. The BDFL extends the HydRand protocol, to create a BYzantine Fault Tolerant (BFT) peer-to-peer FL system. The same model security is enforced in all where the Publicly Verifiable Secret Sharing (PVSS) scheme protects its local models, ensuring that encrypted shares of anyone can always be verified. Experiments on MNIST show the potential to adopt decentralized FL in AV by leveraging BDFL against other BFT-based FL methods for our study. Additionally, results on the KITTI dataset confirm that BDFL can improve multi-object recognition for AVs. The simulation results suggest that the proposed PVSS-based data privacy preservation scheme has no side effects on model parameters. BDL offers a secure, robust, and decentralized way of optimizing collaboration learning in AVS whilst taking into capacity utilization with privacy protection, fault tolerance as well.

2.4 Summary

This literature review investigates the design of deep learning, federated learning, and fault recovery models in vehicular networks. Deep Reinforcement Learning and many deep learning techniques have been presented to improve autonomous driving scenarios as well as enhancing the cooperative perception. In vehicular network, work on the fault recovery models like redundancy-aware collaborative federated learning and online learning for sensor faults diagnosis has been identified to enhance their resilience in nature. However, this review illuminates the research gaps in time-critical use cases, less focus on error detection and recovery, exploration of data heterogeneity to name a few. By proposing approaches to handle these pitfalls can open new horizons by incorporating more flexibility into fault diagnosis, and auto-recovery mechanisms without deteriorating vehicle performance. This work is primarily motivated by those gaps and seeks to address them through the development of optimized models for achieving fault resilience by deploying a federated learning framework based on CNN and FNN models to contribute towards data privacy, as well reduce vehicle downtimes by diagnosing faults in decentralized mode. Finally, a real-world case study will be presented to demonstrate the efficiency of this model and show that it is able to reduce recovery time as well as improve accuracy, enhancing vehicular network reliability and performance.

3 Research Methodology

In this paper, we propose comprehensive research to jointly address the fault tolerance of model training and data privacy preservation for connected vehicular networks with FL. The proposed methodology consists of a systematic follow to design, implement and evaluate an FL framework through a case study in object classification tasks performed by Roadside Units (RSUs) of IoT as in Figure 1.

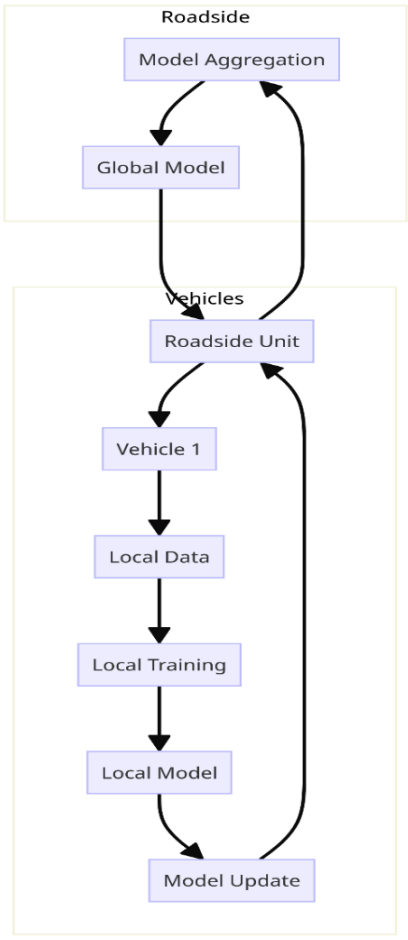


Figure 1: Federated Learning Process Methodology

3.1 Proposed Federated Learning Framework

The FL framework proposes central server and vehicular clients as two main components to perform model training as in Figure 1. The central server starts the FL process that creates an initial global model, aggregates local updates from clients, and checks termination criteria. The local sensors in vehicular clients collect sensor data, the global model is used to train a local model on this data and generate a set of updates that are sent back to the central server for aggregation. The process starts with the first global model sent by the server to all clients. Every client now trains its local model with the global model. We only collect updates from all clients and update a combined global model. This goes on until the termination criteria is met. Instead of Recurrent Neural Networks (RNNs) that was proposed earlier, Feed-forward neural networks (FNN) and CNN will be used for FL training. FNNs are appropriate for modeling

structured data, such as images. They learn hierarchical representations of inputs. Our FNN architecture is specifically engineered to extract important patterns and anomalies from the vehicle sensor data for each type of object classification task. Federated learning using CNNs can be useful in the context of distributed object detection scenarios (e.g., cameras from different cars toward training a shared model), e.g., for autonomous vehicles or surveillance systems. CNNs are frequently used for on-device local inferences (e.g., smartphones or IoT devices). Federated learning makes it possible for all these devices to collaboratively make CNN model performance improve but safeguard the decentralized sensitive data. The proposed FL framework promotes data privacy-preserving such that raw data stays where it is on the vehicular clients and only model updates are transmitted to a central server.

3.2 Object Classification Case Study for Fault Recovery

The proposed FL framework is tested on an example of object classification tasks in a simulated IoV environment conducted by RSUs. The case study presents how the framework permits to train a collaborative model among devices while keeping data privacy and recovering faults in an efficient manner. For the case study scenario, an RSU detects objects (e.g., pedestrian, vehicles, and obstacles) under various traffic conditions. The RSU corrects its local model for these changes, but due to a fault, it loses its own local model. For this purpose, three fault recovery strategies were implemented as follows: retraining the model from scratch using only local data of RSU (referred to as Local Retrain), restore a previous version of the model at RSU, and continue training with its local data going further (Restart Training), or just push down without extra-tuning any new global federated models issued by central server. The handwritten digit images from the MNIST dataset are used to simulate the classification process and measure practices for recovery. It is illustrated that the global federated model can efficiently recover performance to pre-disturbance levels after fault without need of additional local training, hence validating feasibility for applying FL framework in fault recovery on IoV scene.

3.3 Experimental Setup and Evaluation

The proposed FL framework is to be implemented using the Python programming language with commonly used deep learning libraries such as TensorFlow and Keras. Experiments will be performed in a distributed computing environment, which simulates the IoV network for several vehicular clients and one central server. For training and evaluating the FNN and CNN models, the MNIST dataset will be divided into subsets and used for local model training. The dataset will be partitioned across the clients in such a way that every client has separate data to simulate distributed nature of IoV environment. Then, the FNN and CNN models and its hyperparameters will be tuned by validating its performance on a validation set.

The proposed framework will be assessed based on several metrics: classification accuracy for general performance of object classification models, convergence speed to evaluate the time taken by global model in FL to reach a satisfactory level of performance, communication efficiency specifies how much data that is transmitted between clients and server during the FL process, Recovery Time measures duration consumed by RSUs with their default configurations are restored back after evoked under different strategies.

4 Design Specifications

4.1 FL Architecture

The architecture of our FL framework for connected vehicular networks includes three principal parts: the centralized server, roadside units (RSUs), and intelligent vehicles as shown in Figure 2. More generally, the autonomous vehicles themselves gather and process local sensor data for training utilizing FNNs and CNNs. The models or model updates are sent, over a wireless network, to the nearby RSUs where they will be locally trained.

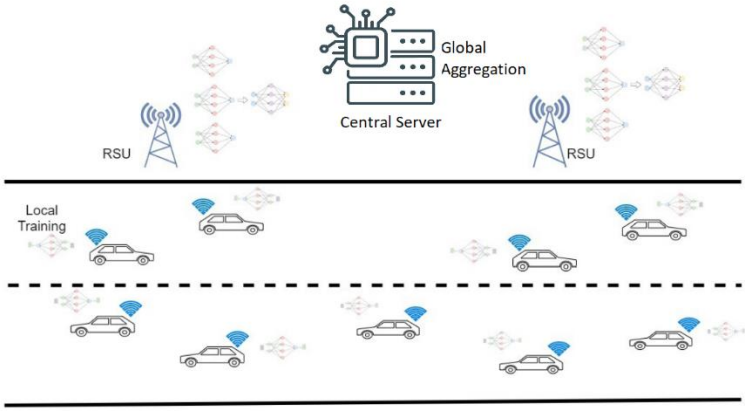


Figure 2: Proposed FL Framework for Autonomous Vehicles

RSUs are in between and act as mediators that collect the updates from vehicles and then relay them to a central server. That global model is being used to update every individual vehicle, and distributed vehicles send back the aggregated result. The central server aggregates the model updates from multiple vehicles via RSUs and globally. The updates are aggregated to form an updated global model, which can then be sent back to the vehicles for cooperative learning or error recovery.

4.2 Deep Learning Models

4.2.1 FNN for FL Model Training

The primary architecture for FL model will be CNN, while FNN will be used instead of RNN. FNNs work well with structured data such as images, natural language text and can learn the hierarchical extraction of input features. For fault diagnosis tasks, the FNN architectures will be tailored for detecting patterns and/or anomalies in vehicular sensor data. Experimentation and hyperparameter tuning will find out the specific architecture details of the FNNs like layers, average neurons per layer, and activation functions. This method can make the model more convenient to adjust combined with vehicle sensor data and fault diagnosis tasks. The FNNs will go through the FL process, where each vehicle trains a local model using its own data and updates are contributed to the global model. This model of learning is called collaborative and preserves privacy as raw data between vehicle does not get shared. Only model updates are shared between nodes, preserving the localization of data on each vehicle.

4.2.2 CNNs for FL Model Training

CNNs work very well for processing grid-like data, like images or spatial sensor data. They employ convolutional layers with filters to learn spatial hierarchies of features without a fixed input size, which is suitable for pattern recognition tasks where structure exists in either the actual space (images) or time domain.

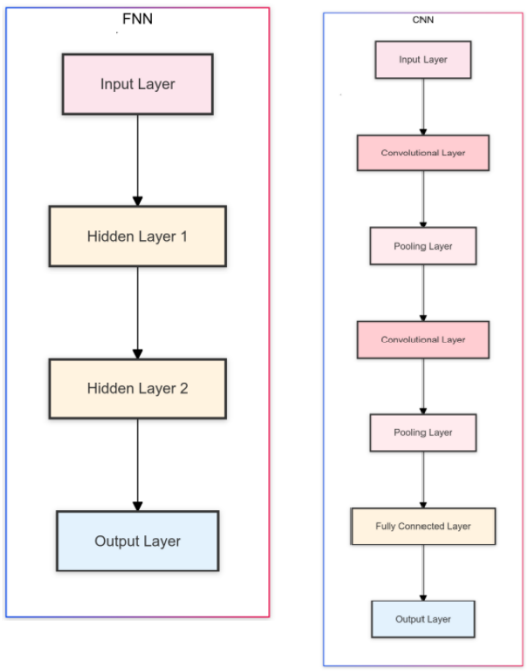


Figure 3: Comparison of FNN and CNN architectures

When it comes to FNNs and CNNs, the differences they lay at an architectural level. In this kind of the model, each neuron is linked to every other neuron in adjacent layers. CNNs on the other hand, add convolutional, pooling layers, and fully connected layer. The convolutional layers use local connectivity and weight sharing, which gives them the capacity to efficiently capture spatial patterns in the data. They can also automatically learn relevant features from raw input data which may obviate manual feature selection preprocessing steps and leading to end-to-end learning. This ability can be particularly useful when working with difficult vehicle sensor data, as crucial patterns might not pop-up right away. Both FNN and CNN architectures could be considered based on the characteristics of vehicle sensor data while transforming it as diagnostic information, to achieve fault diagnosis tasks.

4.3 FL Learning Process

The FL learning process is presented below:

- Initialization: In the beginning, the Central Server generates an initial global model and shares it with all participating vehicles from RSUs.
- Local Training: The local FNN and CNN model of each vehicle is trained using the sensor data collected from that vehicle itself. The vehicles will be used to evaluate advanced variations of their respective locally based models tailored to the dynamically changing operating conditions.

- Update model: Once it is trained locally, every vehicle will send its update (gradients or weights for example) to the closest RSU which in turn sends them to a central server. The raw data is not shared among the RSUs, thus protecting data privacy and only model updates are shared between vehicles.
- Global Aggregation: The central server collects the updates of models from multiple vehicles and aggregates them to create an updated global model. Aggregation methods can be simple, such as taking the average model weights and more complex techniques like Federated Averaging (FedAvg).
- Model Distribution: The newly formed global model is sent back to the vehicles through RSUs. Vehicles could swap out their local models and replace them with the global model or use it to jump start training for an even more locally relevant policy.
- Termination: This can be continued till some stopping criteria tells you that the targeted model performance/number of rounds is reached. The iterative nature of the process also constitutes a method for implementing collaborative learning among the vehicles, so each vehicle in this network learns from it without fully disclosing any data to other partners regardless.

5 Implementation

5.1 Development Environment

The FL framework will be implemented using the Python programming language together with TensorFlow and Keras, two of today's most used deep learning libraries. The code development will be done in Jupyter Notebook, which gives an interactive environment for writing and running a code. A simulated scenario considering a distributed computing environment will be implemented using the case study on fault recovery. The development platform with cloud computing instances support like Google Cloud Platform (GCP) or Amazon Web Services (AWS) Sagemaker Studio can used to deploy the proposed FL framework.

5.2 Dataset Preparation

The object classification task in the case study will be simulated on MNIST dataset i.e., containing handwritten digit images. The workload will be preprocessed and spread over the vehicular clients such that no two vehicles have the same data. The partitioning will be accomplished in such a way that mimics the distributed nature of the IoV environment, where each vehicle can only access its own data locally. The dataset will be divided into training, validation, and testing sets. The training set will be used for local model fitting on the vehicular clients, and validation set are necessary to drive hyperparameters optimization as well as select among models. The final test set is used to assess how good the trained models will perform.

5.3 FL Model Implementation

The process followed to implement federated learning with FNNs and CNNs in the context of object classification tasks is presented below:

The implementation applies TensorFlow Keras Sequential API for both FNN models, and CNN models. The FNN model usually begins with a flattened layer that converts the 2D input images into vectors. This is followed by Dense layers, which are normally a fully connected layers where each neuron in the previous and next layers is interconnected. The number of neurons in these layers and the depth on how deep network has to be is decided by trial experimentation. We use ReLU activation function in the hidden layer and not sigmoid, as this will help us to improve model performance. The output Layer and the number of neurons in the output layer are equal to that of number of prediction classes when you apply the SoftMax activation function for multi-class classification.

CNNs are much deeper and usually better applicable for image classification problems. Model architecture starts with Conv2D layers that use convolutional filters to extract features from input images. These are then subsequently followed by MaxPooling2D layers to lower the spatial dimensions and capture only common attributes. Hierarchical features can be learned by stacking multiple sets of convolutional and pooling layers. Now, the feature maps are flattened and then fed through Dense layers as in FNN structure. For classification the final layer uses SoftMax activation. The loss function for both FNN and CNN models are categorical cross entropy whereas optimizers used with them are Adam or stochastic gradient descent (SGD). Important hyperparameters include the number of epochs, batch size and learning rate as they have a big impact on model performance as well how long training will take.

5.4 Fault Recovery Strategy Implementation

The proposed FL framework will be analyzed for its utility in enabling fast fault recovery in IoV settings. The fault recovery strategies would be integrated as part of the FL framework. We assume that the vehicular clients might fall into fault modes and lose their local model. In particular, the report compares three different fault recovery strategies as in Figure 4:

- Local Retraining: If a vehicle faces an issue and loses its local model, it retrains the entire model from scratch on just its own data locally. This strategy uses only the vehicle's local resources and ignores other vehicles knowledge in system.
- Model Restoration: The vehicle restores a saved version of its local model and continues training on it using its own data. This strategy assumes that the vehicle has a model of its own which could be restored from some previous state.
- Global Model Push: Directly push the latest global model from the central server to faulty vehicles without extra local training. Based on the collective knowledge of the entire network, this strategy can quickly recover from some fault.

We will determine how well these fault recovery strategies work for the case study scenario, based on measurements of e.g. time to recover from faults and ability to regain performance levels in pre-fault condition in the next section.

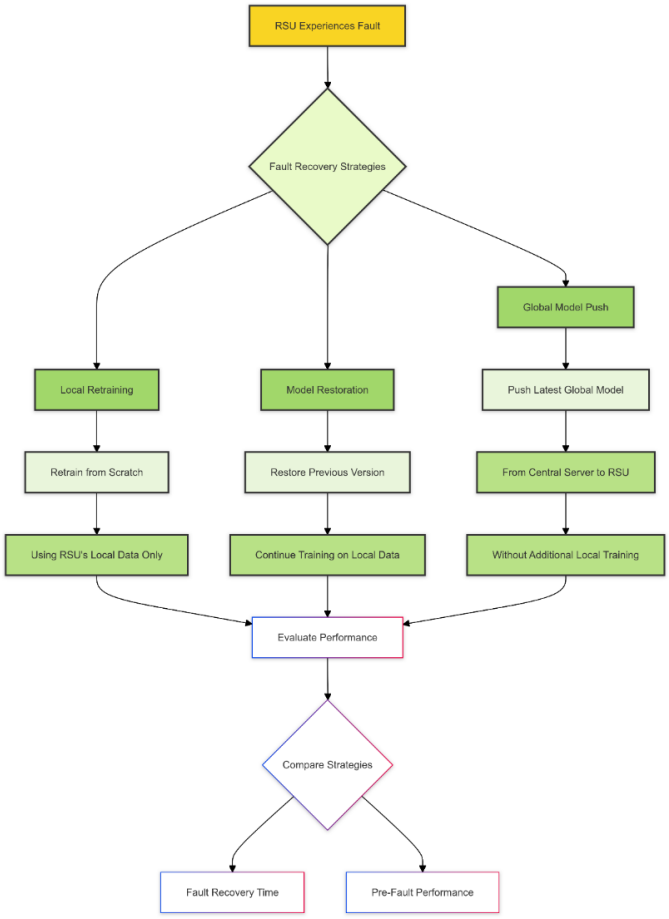


Figure 4: Fault Recovery Strategy Execution

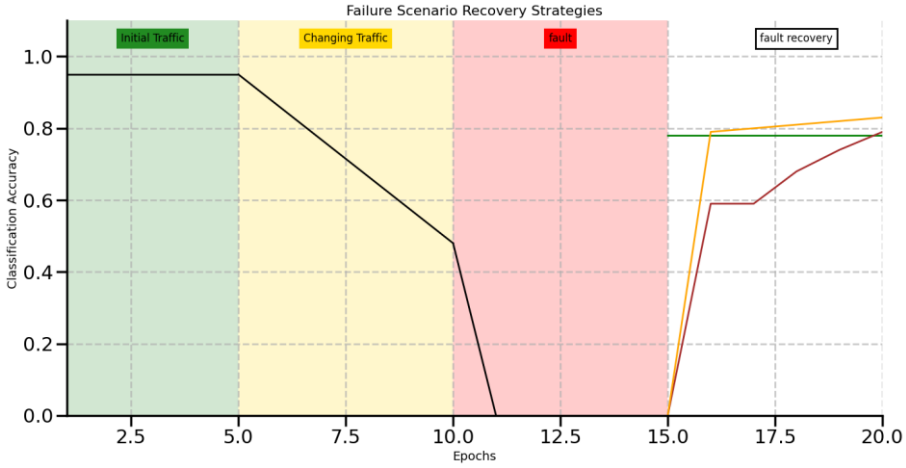
6 Evaluation

In this section, an in-depth study of the results and discussion on the fault recovery strategies implemented using federated learning (FL) for CNN and FNN in a connected vehicle simulation environment is presented.

6.1 Experiment: CNN vs FNN for Fault Recovery

The classification accuracy over training epochs for different fault recovery strategies for both FNN and CNN in presented in Figures 5 and 6, respectively.

Figure 5: FNN Fault Recovery Mechanism



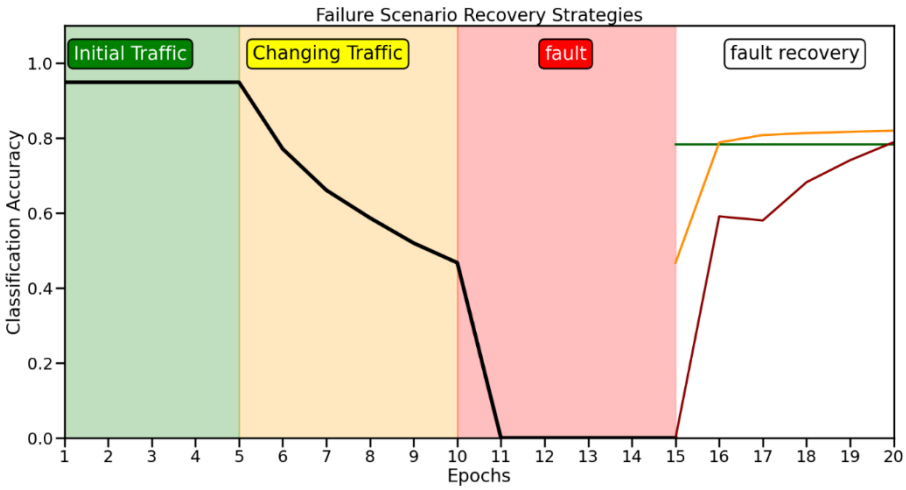


Figure 6: CNN Fault Recovery Mechanism

- Normal Operation: Equivalent High Accuracy (~95%) — Mid to Max at Initial Traffic
- Traffic Shifts: As the pattern of traffic shifts, accuracy decreases over time for both models.
- When fault occurs, accuracy falls to 0% accuracy.
- Fault Recovery:
  1. Local Retrain (red): The slowest but gradually more accurate recovery.

2. Re-training (green line): More rapid re-learning, taking account of previous learned weights.
3. Global Model Push (orange line), which is the fastest recovery and immediately brings back high accuracy.

6.2 Fault Recovery Analysis

- **Federated Recovery:** CNN has the highest AUC with 3.90 and highest peak accuracy at 0.95, fastest recovery time per second for peak performance compared to FNN.
- **Start from Scratch:** CNN AUC (lower is better) = 3.00 score. It went the highest from zero to infinity, immediate recovery was slowest (.59 accuracy). Still, it managed to peak at an accuracy of 0.92 showing that long-term recover could be possible.
- **Continue Training:** Has powerful quick recovery (CNN Performance: 0.79 accuracy) and a trade-off between speed and performance with AUC compared to FNN. FNN follows similar trends as CNN but slightly less effective.

6.3 Statistical Analysis of CNN Performance

- Area Under the Curve (AUC) (Table.1): Federated Recovery has an AUC of 3.90, yielding over two orders higher cumulative sum and therefore global "whole system" recovery performance on the ROC curve better than any other strategy.

Table 1: Area Under the Curve (AUC)

Strategy	Speed
Federated Recovery	0.6121
Start from Scratch	0.1341
Continue Training	0.1343

- Maximum Accuracy/Time: Federated Recovery has the highest peak of any method, with an average accuracy at its best time being 0.95 in approximately 1.5 seconds.
- Recovery Speed: Federated Recovery has one of the highest recovery speeds with perfect accuracy reached at 0.6121s per peak, over 4.5× faster than other strategies on average in this dimension (Refer Table 2).

Table 2: Recovery Speed (Peak Accuracy per second)

Strategy	AUC
Federated Recovery	3.90
Start from Scratch	3.00
Continue Training	3.63

6.4 Discussion

This discussion presents the learnings from the experiments conducted.

- Across numerous metrics, we find that Federated Recovery strategy achieves improved performance over other baselines signifying that decentralized information in connected vehicle networks can indeed be harnessed for mutual benefit.
- While Federated Recovery is ideal along most axes, Continue Training performs strongly when rapid recovery time is of paramount importance hinting that it may serve as an acceptable fallback option if federated learning approaches are not applicable.
- Examining the excellent immediate performance of Continue Training, we find that CNNs appear able to retain useful information in spite faults, thus demonstrating its preservative properties which may be used to maintain productive features whenever possible.
- Federated Recovery combines rapid recovery with high accuracy lineament, which is paramount for connected vehicle real-time use cases.
- CNNS performed very well on all metrics and is an indication that it can efficiently process vehicle sensor data represented as images or grid-like structures.

7 Conclusion and Future Work

In this study, the potential of federated learning scenario that uses FNN and CNN models for fault detection, recovery, or optimal performance restoration in connected vehicular networks. The proposed FL framework enables privacy-preserving collaborative learning with vehicles to minimize downtime by effective fault recovery mechanisms. This indicates the framework's potential in ensuring both high accuracy and speedy fault recovery time as was demonstrated by a case study performed on object classification tasks using the MNIST dataset. The global federated model was able to recover performance equivalent to pre-fault without any additional local training, demonstrating the potential of FL in recovery from faults for IoV applications. The results indicate that FL can improve the data privacy, vehicle downtimes and overall reliability of a vehicular network. That said, there are limitations to the study such as its simulated environment and use of a single data set. This study was focused only on the implementation of the proposed framework. Future work should concentrate on performing a wide range of experiments with diverse and real-world IoV datasets under various traffic contexts. The real application of such FL framework requires investigating how data heterogeneity, scalability, and communication efficiency in large-scale vehicular networks would affect.

References

Manias, D.M. and Shami, A., 2021. Making a case for federated learning on the internet of vehicles and intelligent transportation systems. IEEE network, 35(3), pp.88-94.

Liang, X., Liu, Y., Chen, T., Liu, M. and Yang, Q., 2022. Federated transfer reinforcement learning for autonomous driving. In Federated and Transfer Learning (pp. 357-371). Cham: Springer International Publishing.

Elbir, A.M., Soner, B., Çöleri, S., Gündüz, D. and Bennis, M., 2022, September. Federated learning in vehicular networks. In 2022 IEEE International Mediterranean Conference on Communications and Networking (MeditCom) (pp. 72-77). IEEE.

Posner, J., Tseng, L., Aloqaily, M. and Jararweh, Y., 2021. Federated learning in vehicular networks: Opportunities and solutions. IEEE Network, 35(2), pp.152-159.

Hernandez, L., Hassan, M. and Shukla, V.P., 2023. Applications of Cloud Computing in Intelligent Vehicles: A Survey. Journal of Artificial Intelligence and Machine Learning in Management, 7(1), pp.10-24.

Zhang, S., Li, J., Shi, L., Ding, M., Nguyen, D.C., Tan, W., Weng, J. and Han, Z., 2023. Federated learning in intelligent transportation systems: Recent applications and open problems. IEEE Transactions on Intelligent Transportation Systems.

Palanisamy, P., 2020, July. Multi-agent connected autonomous driving using deep reinforcement learning. In 2020 International Joint Conference on Neural Networks (IJCNN) (pp. 1-7). IEEE.

Aoki, S., Higuchi, T. and Altintas, O., 2020, October. Cooperative perception with deep reinforcement learning for connected vehicles. In 2020 IEEE Intelligent Vehicles Symposium (IV) (pp. 328-334). IEEE.

Li, M., Gao, J., Zhao, L. and Shen, X., 2020. Deep reinforcement learning for collaborative edge computing in vehicular networks. IEEE Transactions on Cognitive Communications and Networking, 6(4), pp.1122-1135.

Pokhrel, S.R. and Choi, J., 2020, April. A decentralized federated learning approach for connected autonomous vehicles. In 2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW) (pp. 1-6). IEEE.

Ye, D., Yu, R., Pan, M. and Han, Z., 2020. Federated learning in vehicular edge computing: A selective model aggregation approach. IEEE Access, 8, pp.23920-23935.

Lu, Y., Huang, X., Dai, Y., Maharjan, S. and Zhang, Y., 2020. Federated learning for data privacy preservation in vehicular cyber-physical systems. IEEE Network, 34(3), pp.50-56.

Li, X., Cheng, L., Sun, C., Lam, K.Y., Wang, X. and Li, F., 2021. Federated-learning-empowered collaborative data sharing for vehicular edge networks. IEEE network, 35(3), pp.116-124.

Zhao, P., Huang, Y., Gao, J., Xing, L., Wu, H. and Ma, H., 2022. Federated learning-based collaborative authentication protocol for shared data in social IoV. IEEE Sensors Journal, 22(7), pp.7385-7398.

Dautov, R. and Husom, E.J., 2024, April. Raft Protocol for Fault Tolerance and Self-Recovery in Federated Learning. In Proceedings of the 19th International Symposium on Software Engineering for Adaptive and Self-Managing Systems (pp. 110-121).

Hui, Y., Hu, J., Cheng, N., Zhao, G., Chen, R., Luan, T.H. and Aldubaikhy, K., 2023. RCFL: Redundancy-Aware Collaborative Federated Learning in Vehicular Networks. IEEE Transactions on Intelligent Transportation Systems.

Yan, X., Sarkar, M., Lartey, B., Gebru, B., Homaifar, A., Karimoddini, A. and Tunstel, E., 2023. An online learning framework for sensor fault diagnosis analysis in autonomous cars. IEEE Transactions on Intelligent Transportation Systems.

Xu, C., Qu, Y., Luan, T.H., Eklund, P.W., Xiang, Y. and Gao, L., 2022. An efficient and reliable asynchronous federated learning scheme for smart public transportation. IEEE Transactions on Vehicular Technology, 72(5), pp.6584-6598.

Manias, D.M. and Shami, A., 2021. Making a case for federated learning on the internet of vehicles and intelligent transportation systems. IEEE network, 35(3), pp.88-94.

Chen, J.H., Chen, M.R., Zeng, G.Q. and Weng, J.S., 2021. BDFL: A byzantine-fault-tolerance decentralized federated learning method for autonomous vehicle. IEEE Transactions on Vehicular Technology, 70(9), pp.8639-8652.