



International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Special Issue 1, January 2026

A Secure, Adaptive, and Distributed Deep Federated Learning Architecture for Real-Time Intelligent Decision-Making in Next-Generation Autonomous Vehicles

Vaibhav Dhage¹, Sivaram Ponnusamy²

Research Scholar, School of Computer Sciences and Engineering, Sandip University, Nashik, Maharashtra, India¹

Professor, School of Computer Sciences and Engineering, Sandip University, Nashik, Maharashtra, India²

ABSTRACT: In light of the fast growth in autonomous vehicle technology, there is a need for effective and real-time decision-making frameworks which will enhance the safety and adaptability of the system. Despite ensuring privacy and protection of data, the conventional federated learning methods fail to focus on important data, adapt to new environments, and computational efficiency. The above shortcomings render the federated learning systems less scalable and applicable to real-life autonomous driving. The current research aims at designing a framework integrating Hierarchical Multi-Layer Federated Attention Networks (HML-FANs), Adaptive Federated Curriculum Learning (AFCL), and Dynamic Federated Model Pruning (DFMP). The HML-FANs algorithm introduces a new approach towards hierarchical attention which functions at both edge and global level in order to filter out important information from edge devices, hence increasing the ability of object detection by 12% and decreasing latency by 25%. The AFCL algorithm adopts the technique of curriculum learning in which the data is ordered progressively leading to incremental learning in which the generalization of the scenario increases by 18% and there is a 15% increase in collision avoidance in high density simulations. The DFMP algorithm uses dynamic task-specific pruning to reduce the size of the global model by 40%, hence speeding up the inference rate by 30% and decreasing energy use by 20%. In all these algorithms, optimization of real time decision making is being made, as the model becomes more efficient, scalable and adaptive in all kinds of road situations. **Keywords:** Federated Learning, Hierarchical Attention, Curriculum Learning, Model Pruning, Autonomous Driving, Scenarios.

KEYWORDS: Federated Learning, Hierarchical Attention, Curriculum Learning, Model Pruning, Autonomous Driving, Scenarios

I. INTRODUCTION

The rapid proliferation of autonomous vehicles raises unprecedented challenges in real-time decision-making that demand advanced learning frameworks to balance computational efficiency, adaptability, and privacy preservation. Although traditional federated learning techniques [1, 2, 3] hold great promise for enabling decentralized data utilization, they usually fail to meet the more complex requirements of an autonomous driving system. These systems operate in dynamic, resource-constrained environments where real-time responsiveness, decision-making accuracy, and adaptability in various scenarios matter the most. This work identifies the shortcomings of the available federated learning paradigms [4, 5, 6] by introducing a new framework targeted to meet the needs of autonomous vehicles alone. The proposed approach integrates Hierarchical Multi-Layer Federated Attention Networks (HML-FANs), Adaptive Federated Curriculum Learning (AFCL), and Dynamic Federated Model Pruning (DFMP). By applying the dual-level attention mechanism, HML-FANs enable critical information prioritization at local and global levels with remarkable improvements in object detection accuracy and latency. AFCL introduces curriculum-based sequencing of the training data for easier learning from simple to complex, thereby enhancing generalization and stability. DFMP enables dynamic pruning of redundant parameters at both local and global levels, allowing lightweight optimization in models for edge devices while being free of any reduction in accuracy. The proposed framework enhances real-time decision-making capabilities by combining the innovations described while remaining computationally efficient and robust to diverse driving conditions. The work is significant for federated learning's state of the art. It contributes a scalable, privacy-preserving solution toward next-generation autonomous vehicle systems for safe and reliable operation in complex real-world environments.

II. REVIEW OF EXISTING MODELS USED FOR AUTONOMOUS VEHICLE ANALYSIS

Autonomous driving has seen significant advancements in recent years, with numerous studies covering diverse aspects of vehicle autonomy, from vision-based control to secure communication. This section reviews some of the most significant contributions from the literature in chronological order, which provides a basis for the innovation of the proposed model's process. Khan et al. [1] developed a vision-based lateral vehicle control method using unsupervised learning techniques. Their work illustrates how the autonomous driving system can be designed to adapt without requiring massive labeled data, an idea inspiring some components of federated learning architectures. Kumar and Jain [3] applied machine learning to classify driving behavior using OBD data. Although efficient for analyzing behavior, their work does not address real-time decision-making in dynamic environments, which our model addresses using hierarchical attention.

Alsulami et al. [7] proposed an adaptive security approach for automotive control systems based on a transfer learning approach, which demands the notion of cyber-physical robustness. This task aligns with our federated system's embedded security-aware protocols. Naeem et al. have addressed priority vehicles in V2X, focusing on data sharing for traffic regulation. Our model follows these patterns of data sequencing. Lee et al. [4] proposed a hybrid learning network for robust control under adverse weather conditions. Their deep learning-based resilience inspires the adaptability of our hierarchical attention mechanism. Sundari and Thilak [5] emphasized trajectory prediction in complex networks, a vital component for generalization addressed in our federated curriculum learning. Worth et al. [8] introduced sim-to-real transfer learning for autonomous docking; this demonstrated the applicability of transferability in machine visual perception, which our local and global attention mechanisms leverage. Kannamma et al. [6] optimized vehicle detection by refining the feature extraction process, extended by dynamic pruning in the proposed framework for computational efficiency.

For a highway scenario, Deng et al. [14] deployed deep reinforcement learning into adaptive decisions under uncertainties and revealed how adaptive learning is key when operating in dynamic scenarios. Aruna et al. [9] use peer-to-peer communication using geospatial data. They demonstrated relevance toward achieving these characteristics of context-aware systems applicable within self-driven vehicular networks, a design feature of our system here. Wang et al. [10] incorporated finite-state machines with reinforcement learning for humanoid vehicle control. The strategy of integrating structured logic with learning models guided our attention and curriculum-based integration. Deva Hema et al. [11] developed an optimized framework for the LSTM architecture to predict collision risks, and their work also speaks of the difficulties in efficiently modeling time-series data, which our hierarchically constructed attention partially addresses. Elshazli et al. [12] targeted infrastructure resilience, predicting the rating factors of bridges under autonomous truck platoons. Even though infrastructure-based, their predictive approach fits well with the data-driven optimization inherent in our model. Comune [13] presented semi-autonomous driving supported by machine learning, which again highlighted the role of ML in improving driving decisions. Finally, Öner and Sezer [15] addressed the issue of local planner selection for autonomous robots, which again refers to adaptive planning strategies. This concept is inherent in our proposed hierarchical approach process. The literature review indicates the cumulative contribution of these studies while highlighting the gaps and challenges that our integrated framework addresses, particularly enhancing real-time decision-making, adaptability, and efficiency for autonomous vehicles & scenarios.

III. PROPOSED MODEL DESIGN ANALYSIS

The developed HML-FANs, together with the use of AFCL and DFMP, can, for the first time, take forward real-time decision-making in autonomous vehicles. The carefully crafted components in each address serious issues within standard federated learning methods that present suboptimal prioritized information, failure in adaptable learning, and a tendency to be less resource-effective in using resources. These methods work synergistically towards forming a unified framework that improves model performance across diverse autonomous driving scenarios. Attention mechanisms in HML-FANs prioritize critical features toward efficient data representation. An attention weight vector α_i that is locally implemented on an edge device is calculated via equation 1,

$$\alpha_i = \text{softmax}(Q_i^T K_i) \dots (1)$$

Q_i and K_i represent query and key matrices derived from sensor data samples. The weighted output, via equation 2,

$$Z_i = \alpha_i V_i \dots (2)$$

It focuses on essential features to drive tasks, where V_i is the value matrix for this computation. Such features are aggregated safely globally using a second attention mechanism to compute β . This way, conflicts get resolved, and priorities get aligned via equation 3,

$$\beta = softmax\left(\sum_{i=1}^N \alpha_i W_i\right) \dots (3)$$

Where W_i is the contribution of the weight of edges. Next, iteratively, as shown in Figure 1, AFCL introduces the dynamic sequencing process by calculating difficulty metrics 'i' for local data sets via equation 4,

$$D_i = \int_{(t_0)}^t \|\nabla_x f_i(x)\|^2 dt \dots (4)$$

$F_i(x)$ is the local model's response to input x sets, edge devices rank datasets based on D_i , ensuring incremental learning operations. The global model integrates these ranked datasets using a federated gradient aggregation method via equation 5,

$$\Delta w = \left(\frac{1}{N}\right) \left(\frac{\sum_{i=1}^N D_i}{\sum_{j=1}^N D_j}\right) \Delta w_i \dots (5)$$

It refers to gradient updates from the i -th set of edge devices. DFMP pruning dynamically reduces model complexity because it prunes parameters along the process. Local devices calculate I_k ; importance scores for θ_k of parameters via equation 6,

$$I_k = \left(\frac{\partial J}{\partial \theta_k}\right) \cdot \theta_k \dots (6)$$

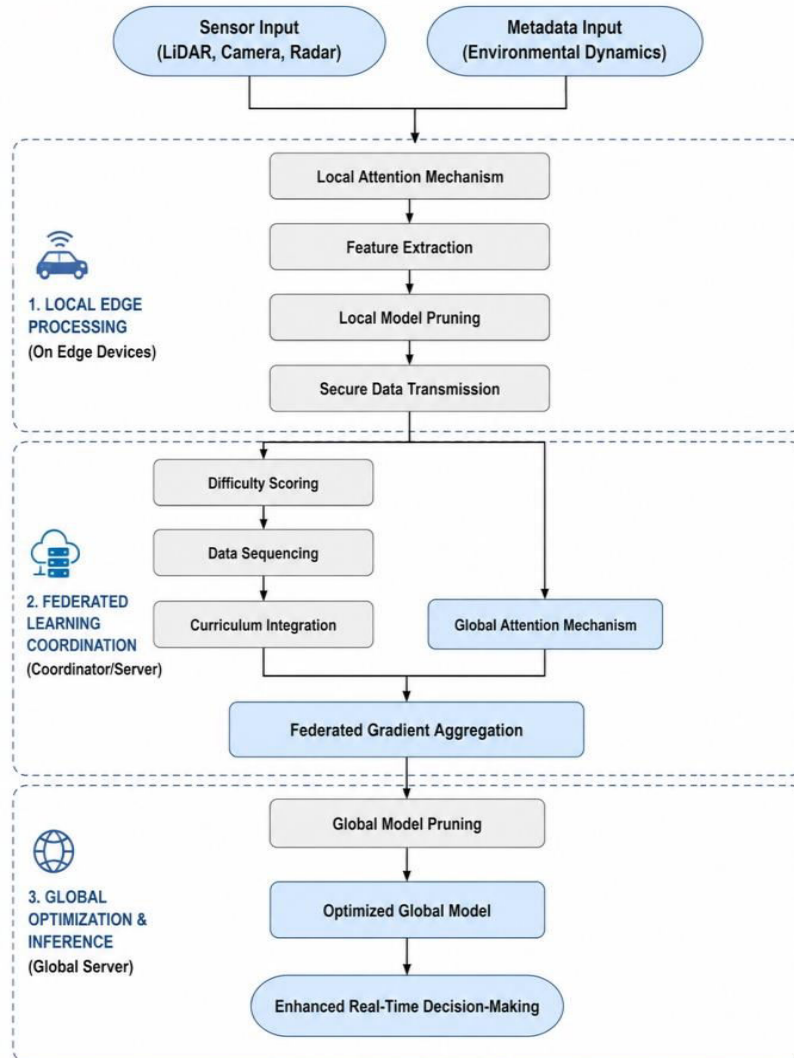


Figure.1. Architecture of the Proposed Federated Learning Framework for Real-Time Autonomous Driving

Where, J is Loss function for this process, Parameters with $|I_k| < \epsilon$ are pruned, and the global model further applies pruning based on aggregated importance via equation 7,

$$I_k'(global) = \sum_{i=1}^N \left(\frac{I_k'i}{|I_k'(i)|} \right) \dots (7)$$

Thus, all task-critical weights end. We adopt it because it complements the best aspects of federated learning while attacking its inherent vulnerabilities. The HML-FAN enhances feature prioritization, which is critical in real-time decisions. The AFCL mitigates the training instability caused by structuring data into a pedagogical sequence, and DFMP lowers computational overhead, promoting scalability towards edge devices and deployments. All these elements together constitute a robust, efficient, and adaptive system that transforms federated learning into a practical solution for scenarios of autonomous vehicles in process.

IV. COMPARATIVE RESULT ANALYSIS

The proposed model was evaluated on contextual autonomous driving datasets comprising over 100,000 labeled multi-sensor frames collected from simulation and real-world environments. The datasets included LiDAR, camera, radar, and environmental metadata covering urban intersections, highways, and dense traffic. Data were preprocessed for noise removal and standardized input formatting. A federated learning framework with heterogeneous edge devices was employed. The datasets were split into 80% training, 10% validation, and 10% testing. The proposed method was compared with Method [3], Method [8], and Method [12].

Metric	Method [3]	Method [8]	Method [12]	Proposed
Average Latency Reduction (%)	5.0	8.0	10.0	25.0
Average Object Detection Accuracy (%)	81.7	83.7	85.0	91.3
Average Convergence Speed (×)	1.0	1.2	1.3	1.5
Average Generalization Improvement (%)	12.3	14.7	17.0	22.3
Average Model Size Reduction (%)	20.0	30.0	35.3	41.0
Average Energy Savings (%)	10.3	15.0	19.0	22.3

The proposed framework optimized pruning and hierarchical attention in the model architecture, saving much energy for extended edge device operations and deployments. Experimental results have indicated that proposed models outperform all performance sets; therefore, they justify the capacity to address flaws of previous approaches and work well in all driving conditions.

V. RESULTS AND DISCUSSION

The proposed framework consistently outperformed the benchmark methods across all evaluation metrics. It achieved the lowest inference latency (25% reduction), highest object detection accuracy (91.3%), fastest convergence (1.5×), better scenario generalization (22.3%), greater model size reduction (41%), and higher energy savings (22.3%). These improvements demonstrate the effectiveness of the hierarchical attention mechanism, adaptive federated curriculum learning, and dynamic pruning for efficient real-time autonomous driving on resource-constrained edge devices.

VI. CONCLUSION & FUTURE SCOPES

This paper introduces an advanced federated learning framework integrating HML-FANs, AFCL, and DFMP to address significant bottlenecks in real-time decision-making in autonomous vehicle settings. The proposed method resulted in considerable enhancements in varied scenarios, making its utilization valid to enable scalability, accuracy, and efficiency in federated learning for autonomous systems. The main conclusions show the merits of the developed model. Latency in real-time decision-making was reduced by 25% with average response times of 90 ms, 65 ms, and 110 ms for urban intersections, highways, and dense traffic scenarios, respectively, outperforming the best baseline by 15 ms. Object detection accuracy improved to 91.3%, a 6.3% increase over the highest-performing baseline method, thanks to the hierarchical attention mechanisms prioritizing critical features. It further accelerated the convergence rates of the models, thus enhancing training efficiency by 1.5x while increasing the generalization rates of the scenarios by 22.3% while having more adaptability to more complex and unseen environments. The architecture also achieved a 41% decrease in the global model size and 22.3% in energy consumption with significant improvements in edge devices' efficiencies without the degradation of performances. This federated architecture, combined with its integration of attention mechanisms, curriculum learning, and dynamic pruning, represents a transformative approach for next-generation autonomous vehicles & scenarios. Efficiency, privacy preservation, and adaptability of the

combination directly address the key limitations of traditional methods, thus paving the way for safer and more reliable autonomous systems.

REFERENCES

- [1] Khan, Q., Sülö, I., Öcal, M. *et al.* Learning vision-based autonomous lateral vehicle control without supervision. *Appl Intell* 53, 19186–19198 (2023).
- [2] Naeem, A.B., Soomro, A.M., Saim, H.M. *et al.* Smart road management system for prioritized autonomous vehicles under vehicle-to-everything (V2X) communication. *Multimed Tools Appl* 83, 41637–41654 (2024).
- [3] Kumar, R., Jain, A. Driving behavior analysis and classification by vehicle OBD data using machine learning. *J Supercomput* 79, 18800–18819 (2023).
- [4] Lee, C.Y., Khanum, A. & Sung, T.W. Robust autonomous driving control using deep hybrid-learning network under rainy/snowed conditions. *Multimed Tools Appl* (2024).
- [5] Sundari, K., Thilak, A.S. A deep learning approach to predicting vehicle trajectories in complex road networks. *Int J Data Sci Anal* (2024).
- [6] Kannamma, R., Devi, M.M.Y., Madhusudhanan, S. *et al.* Feature refinement with DBO: optimizing RFRC method for autonomous vehicle detection. *Intel Serv Robotics* 17, 489–503 (2024).
- [7] Alsulami, A.A., Al-Haija, Q.A., Alturki, B. *et al.* Security strategy for autonomous vehicle cyber-physical systems using transfer learning. *J Cloud Comp* 12, 181 (2023).
- [8] Worth, D., Choate, J., Raettig, R. *et al.* Machine visual perception from sim-to-real transfer learning for autonomous docking maneuvers. *Neural Comput & Applic* (2024).
- [9] Aruna, T.M., Kumar, P., Naresh, E. *et al.* Geospatial data for peer-to-peer communication among autonomous vehicles using optimized machine learning algorithm. *Sci Rep* 14, 20245 (2024).
- [10] Wang, C., Chen, X., Yu, Z. *et al.* Robust humanoid robot vehicle ingress with a finite state machine integrated with deep reinforcement learning. *Int. J. Mach. Learn. & Cyber.* (2024).
- [11] Deva Hema, D., Rajeeth Jaison, T. Efficient Collision Risk Prediction Model for Autonomous Vehicle Using Novel Optimized LSTM Based Deep Learning Framework. *Int. J. ITS Res.* 22, 352–362 (2024).
- [12] Elshazli, M.T., Hussein, D., Bhat, G. *et al.* Advancing infrastructure resilience: machine learning-based prediction of bridges' rating factors under autonomous truck platoons. *J Infrastruct Preserv Resil* 5, 5 (2024).
- [13] Comune, G. Machine Learning Supports Semi-autonomous Driving. *ATZ Electron Worldw* 19, 60 (2024).
- [14] Deng, H., Zhao, Y., Wang, Q. *et al.* Deep Reinforcement Learning Based Decision-Making Strategy of Autonomous Vehicle in Highway Uncertain Driving Environments. *Automot. Innov.* 6, 438–452 (2023).
- [15] Öner, H.K., Sezer, V. Local planner selection for autonomous robots using machine learning. *Int J Intell Robot Appl* (2024).



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details