JOURNAL OF INTERNATIONAL CRISIS AND RISK COMMUNICATION RESEARCH
ISSN: 2576-0017
2025, VOL 8, NO S11

Distributed Learning Systems For Autonomous Vehicles

Venkata Surya Teja Batchu

Independent Researcher, USA

Abstract

The rapid evolution of autonomous vehicle technology has created unprecedented demands for sophisticated machine learning models capable of real-time decision-making while preserving user privacy. This article presents a comprehensive analysis of Federated Learning architectures specifically designed for autonomous vehicle applications, examining how these distributed learning paradigms enable collaborative model training without compromising sensitive data privacy. It explores the integration of cloud-edge computing frameworks, advanced cryptographic protocols, and geospatial intelligence systems that collectively enable privacy-preserving AI deployment at scale. The article systematically reviews recent implementations and case studies from leading automotive manufacturers, demonstrating how federated architectures achieve enhanced vehicle safety, improved route optimization, and robust privacy protection while addressing the unique challenges of vehicular networks. The article examines core architectural principles including distributed computation, secure aggregation, and privacy preservation mechanisms that form the foundation of vehicular federated learning systems. It analyzes hierarchical federated learning architectures that leverage multi-tier cloud-edge integration, enabling efficient resource utilization while maintaining model consistency across diverse operational environments. The article covers advanced privacy-preserving mechanisms including differential privacy integration and cryptographic protocols that provide mathematical guarantees against privacy leakage. Additionally, it explores geospatial intelligence integration and location-aware learning approaches that address the spatial heterogeneity inherent in vehicular data. Through a comprehensive evaluation of real-world deployment challenges and performance metrics, this article provides essential insights for implementing scalable, privacy-preserving federated learning systems in production autonomous vehicle environments.

Keywords: Federated Learning, Autonomous Vehicles, Privacy-Preserving AI, Cloud-Edge Computing, Differential Privacy.

1. Introduction

The autonomous vehicle industry stands at a critical juncture where the demand for intelligent, adaptive AI systems intersects with increasingly stringent privacy regulations and user expectations. Traditional centralized machine learning approaches, while effective for model accuracy, present significant challenges in handling the sensitive nature of vehicular data, including precise location histories, driving patterns, and personal mobility preferences. The exponential growth in connected and automated vehicles has intensified concerns about data privacy and security, particularly as these systems require continuous data collection and processing to maintain optimal performance [2]. Conventional approaches necessitate the transmission

of raw sensor data to centralized servers, creating substantial privacy vulnerabilities and regulatory compliance challenges across different jurisdictions.

Federated Learning emerges as a paradigm-shifting solution that fundamentally reimagines how autonomous vehicles can collectively improve their intelligence without sacrificing individual privacy. The federated learning process operates through a distributed architecture where a central server initializes a global model with a set of starting weights, which is then distributed to participating vehicles [1]. Each vehicle performs local training using its own dataset, subsequently transmitting only the updated model parameters back to the central server for aggregation, ensuring that sensitive raw data never leaves the originating device [1]. This collaborative training methodology enables the development of robust machine learning models while maintaining strict data locality requirements and preserving user privacy throughout the learning process.

The significance of this architectural innovation extends beyond privacy preservation, addressing the fundamental challenges of autonomous vehicle operation in dynamic environments. Connected and automated vehicles must continuously adapt to varying traffic conditions, weather patterns, road infrastructure changes, and evolving safety regulations while maintaining consistent performance across diverse geographical regions [2]. The heterogeneous nature of vehicular environments creates unique challenges for machine learning systems, as models must generalize effectively across different driving scenarios while maintaining personalized decision-making capabilities for individual vehicles. Federated Learning architectures provide the foundational framework for achieving collaborative intelligence that benefits from collective knowledge while respecting individual privacy constraints and regulatory requirements.

Furthermore, the scalability requirements of modern autonomous vehicle deployments demand innovative approaches to distributed learning that can accommodate massive fleets while maintaining communication efficiency and computational feasibility. The federated learning paradigm addresses these scalability challenges by enabling hierarchical aggregation strategies, adaptive communication protocols, and resource-aware training schedules that optimize both learning effectiveness and operational efficiency [2]. This distributed approach becomes increasingly critical as the automotive industry transitions toward fully autonomous systems requiring continuous model updates and real-time adaptation capabilities.

References

2. Federated Learning Fundamentals in Vehicular Context

2.1 Core Architectural Principles

Federated Learning in autonomous vehicles operates on three fundamental architectural pillars: distributed computation, secure aggregation, and privacy preservation. Each participating vehicle maintains its local dataset comprising sensor readings, navigation decisions, traffic interactions, and environmental observations. Rather than transmitting this sensitive information to central servers, vehicles execute local training processes on their onboard computing systems, addressing the fundamental challenge of statistical heterogeneity inherent in distributed learning environments [3]. The federated optimization framework enables collaborative model development through iterative parameter sharing, where each vehicle contributes to global model improvement while maintaining strict data locality constraints and preserving individual privacy requirements throughout the training process.

The distributed computation model leverages the substantial processing capabilities of modern autonomous vehicles, which typically incorporate multiple GPUs, specialized AI accelerators, and high-performance computing units originally designed for real-time perception and decision-making tasks. This computational infrastructure provides the necessary resources for local model training without requiring additional hardware investments. The federated learning paradigm transforms these individual computing resources into a coordinated distributed system, where communication efficiency becomes paramount due to bandwidth limitations and intermittent connectivity challenges [3]. Advanced scheduling algorithms optimize the balance between local computation and global communication, ensuring that federated

learning processes do not interfere with safety-critical autonomous driving functions while maximizing learning effectiveness across the vehicular network.

2.2 Data Characteristics and Challenges

Autonomous vehicle data presents unique characteristics that influence federated learning design decisions. Vehicular datasets are inherently heterogeneous, reflecting diverse driving environments, weather conditions, traffic patterns, and individual driving behaviors. This heterogeneity creates significant challenges for model convergence and performance consistency, as traditional federated averaging algorithms may struggle with the non-uniform data distributions across participating vehicles [4]. The spatial and temporal variations in vehicular data require specialized aggregation techniques that can effectively handle the inherent biases and skewness present in distributed automotive datasets while maintaining global model coherence.

Temporal dynamics represent another critical consideration in vehicular federated learning implementations. Vehicle-generated data exhibits strong temporal correlations, with driving patterns varying significantly based on time of day, seasonal variations, and special events. These temporal patterns introduce concept drift and model staleness issues that can significantly impact learning performance and safety-critical decision-making capabilities [4]. Federated learning architectures must incorporate adaptive mechanisms to address these temporal challenges, including dynamic weighting schemes, incremental learning strategies, and robust aggregation methods that can effectively manage the evolving nature of vehicular operational environments while preventing catastrophic forgetting of essential safety behaviors.

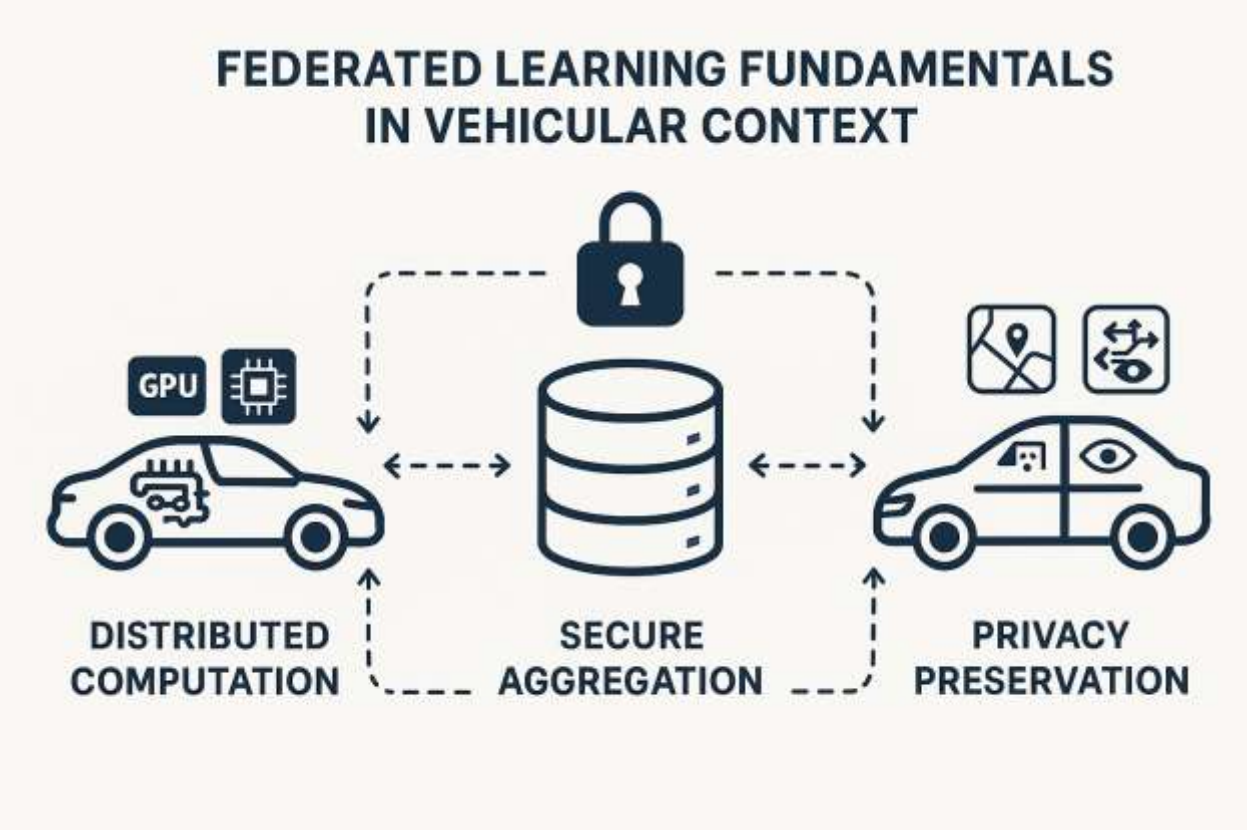

Fig. 1: Federated Learning Fundamentals in Vehicular Context [3, 4]

3. Cloud-Edge Integration Architectures

3.1 Hierarchical Federated Learning Systems

Modern federated learning implementations for autonomous vehicles employ sophisticated hierarchical architectures that leverage both edge computing resources and cloud infrastructure capabilities. These multi-tier systems typically consist of three primary layers: vehicle-level edge computing, regional aggregation nodes, and global cloud-based coordination systems. The hierarchical approach addresses the fundamental challenge of resource constraints in edge computing environments, where limited computational power, memory capacity, and energy availability necessitate adaptive learning strategies that can dynamically adjust to varying system conditions [5]. This tiered architecture enables efficient resource utilization by distributing computational loads across multiple levels while maintaining model consistency and learning effectiveness throughout the federated network.

At the vehicle level, edge computing units perform local model training, feature extraction, and preliminary aggregation of sensor data. These systems must operate under strict latency constraints while managing limited computational resources and power consumption requirements. The adaptive federated learning framework enables intelligent resource allocation by monitoring system performance and automatically adjusting training parameters, communication frequencies, and model complexity based on available computational capacity [5]. Advanced scheduling algorithms ensure that federated learning tasks are executed during optimal periods, such as when vehicles are stationary or operating under reduced computational loads, thereby minimizing interference with safety-critical autonomous driving functions.

Regional aggregation nodes, often implemented through roadside infrastructure or mobile network base stations, serve as intermediate coordination points for geographically proximate vehicles. These nodes perform preliminary model aggregation, reducing communication overhead with centralized cloud systems while enabling rapid knowledge sharing among vehicles operating in similar environments. The hierarchical aggregation strategy significantly improves system scalability by reducing the number of direct connections to central servers while maintaining collaborative learning benefits across diverse operational contexts [6].

3.2 Cloud Infrastructure Requirements

The cloud layer in federated learning architectures serves multiple critical functions beyond simple model aggregation. Advanced cloud platforms provide sophisticated orchestration capabilities, managing the complex coordination required for large-scale federated learning deployments involving millions of connected vehicles. These systems must handle dynamic participant enrollment, model version management, aggregation scheduling, and quality assurance processes while ensuring robust security and privacy protection throughout the learning lifecycle [6]. The cloud infrastructure implements comprehensive threat detection and mitigation strategies to protect against various adversarial attacks and privacy breaches that could compromise the integrity of the federated learning system.

Scalability represents a paramount concern given the exponential growth in autonomous vehicle deployment and the increasing complexity of AI models required for safe autonomous operation. Cloud infrastructures must accommodate massive numbers of participating vehicles while maintaining low-latency communication channels and ensuring robust fault tolerance across diverse geographic regions and network conditions. Modern implementations leverage containerized microservices architectures, enabling dynamic resource allocation and horizontal scaling based on real-time demand patterns and traffic loads [6].

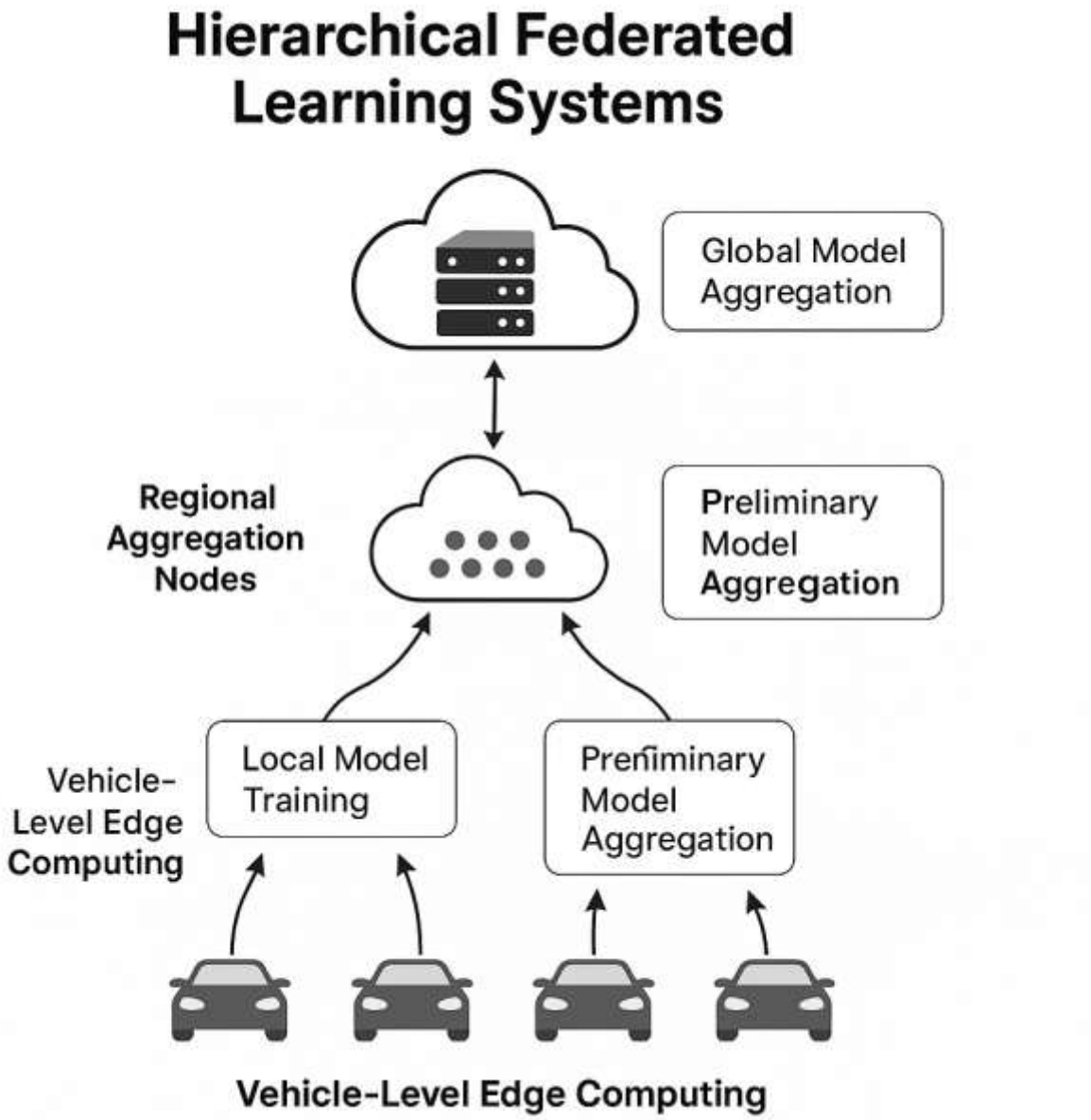

Fig. 2: Hierarchical Cloud-Edge Integration for Federated Learning in Autonomous Vehicles [5, 6]

4. Privacy-Preserving Mechanisms

4.1 Differential Privacy Integration

Differential privacy mechanisms play a crucial role in federated learning architectures for autonomous vehicles, providing mathematical guarantees against privacy leakage even in the presence of sophisticated adversarial attacks. These techniques introduce carefully calibrated noise into model parameters before transmission, ensuring that individual vehicle contributions cannot be reverse-engineered from aggregated models. The differential privacy framework provides rigorous theoretical foundations through epsilon-differential privacy, where the privacy parameter epsilon quantifies the maximum information leakage about any individual's data contribution to the learning process [7]. This mathematical rigor enables autonomous vehicle systems to provide provable privacy guarantees that are essential for regulatory compliance and maintaining user trust in sensitive mobility applications.

The implementation of differential privacy in vehicular contexts requires careful balance between privacy protection and model utility. Autonomous vehicle applications demand high accuracy for safety-critical functions, necessitating sophisticated privacy budget allocation strategies that maximize learning effectiveness while maintaining strong privacy guarantees. The challenge of applying differential privacy to complex machine learning models, particularly in distributed settings like federated learning, requires advanced noise calibration techniques that account for the sensitivity of different model parameters [7]. Vehicular federated learning systems must carefully manage the privacy-utility trade-off to ensure that safety-critical functions such as obstacle detection and collision avoidance maintain sufficient accuracy while protecting individual driving patterns and location histories from potential privacy breaches.

4.2 Cryptographic Protocols

Advanced cryptographic protocols provide additional layers of security for federated learning communications. Homomorphic encryption enables secure aggregation of model parameters without requiring decryption at intermediate nodes, preventing potential data exposure during transmission and processing phases. These protocols are particularly important in vehicular networks where communication channels may traverse multiple network operators and geographic jurisdictions. The implementation of secure multiparty computation enables multiple parties to jointly compute functions over their private inputs without revealing those inputs to each other, which is fundamental for maintaining confidentiality in federated learning scenarios [8]. This cryptographic approach ensures that even the aggregation server cannot access individual model updates from participating vehicles, providing an additional layer of privacy protection beyond differential privacy mechanisms.

Secure multi-party computation protocols enable collaborative model training scenarios where multiple stakeholders, including vehicle manufacturers, fleet operators, and infrastructure providers, can contribute to federated learning processes without revealing proprietary algorithms or sensitive business intelligence. The theoretical foundations of secure multiparty computation provide provable security guarantees against both semi-honest and malicious adversaries, ensuring robust protection even when some participants deviate from the protocol or attempt to extract unauthorized information [8]. These protocols become particularly critical in automotive industry applications where competitive considerations and intellectual property protection requirements necessitate strict confidentiality measures while enabling beneficial collaborative learning that improves overall vehicle safety and performance across the entire ecosystem.

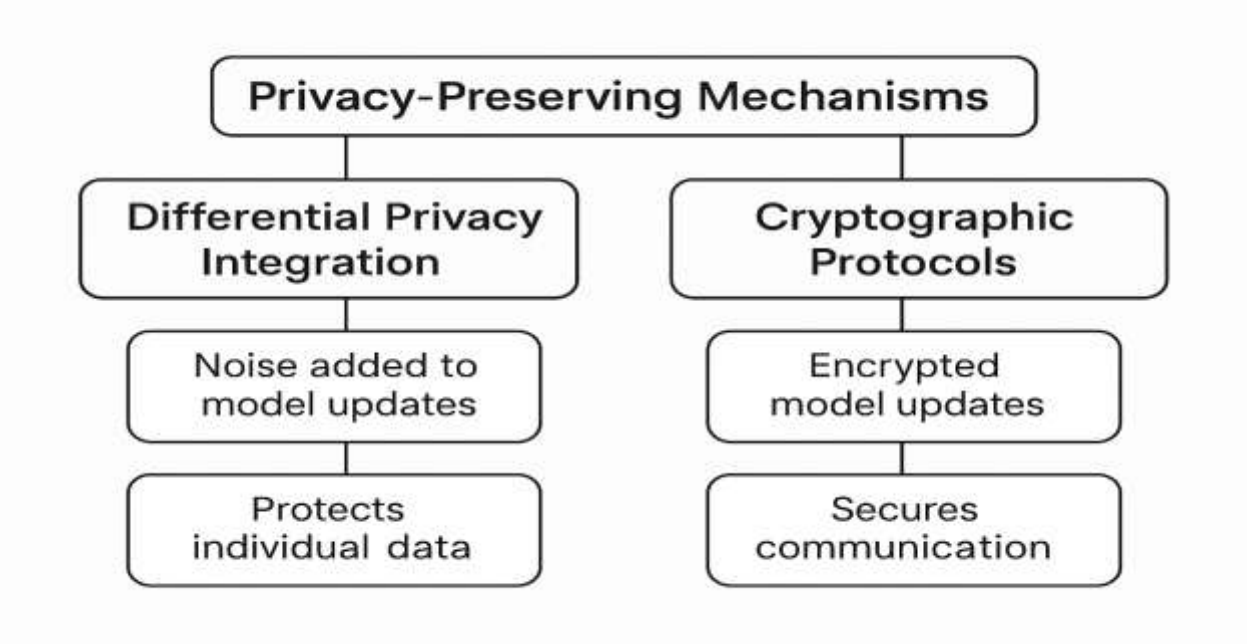

Fig. 3: Privacy-Preserving Mechanisms in Federated Learning for Autonomous Vehicles [7, 8]

5. Geospatial Intelligence and Location-Aware Learning

5.1 Spatial Federated Learning Models

Geospatial considerations introduce unique requirements for federated learning architectures in autonomous vehicles. Traditional federated learning assumes that data distributions across participants are independent, but vehicular data exhibits strong spatial correlations that must be explicitly modeled to achieve optimal performance. The spatial heterogeneity of vehicular data stems from diverse geographical characteristics, including urban versus rural environments, varying road infrastructure, local traffic regulations, and region-specific driving cultures that create distinct data patterns across different locations [9]. This spatial non-uniformity necessitates specialized federated learning approaches that can effectively leverage geographical context to improve model performance while maintaining collaborative learning benefits across the entire vehicular network.

Spatial federated learning approaches partition the global model space based on geographic regions, enabling specialized models that capture location-specific driving patterns, traffic behaviors, and environmental conditions. These spatially-aware architectures improve model accuracy for region-specific scenarios while maintaining global knowledge sharing for common driving tasks such as object detection and basic navigation. The implementation of spatial clustering techniques enables the identification of geographically coherent groups of vehicles that share similar operational environments and data characteristics [9]. This geographical partitioning allows for the development of specialized sub-models that capture local nuances while contributing to global model knowledge, thereby achieving superior performance compared to traditional location-agnostic federated learning approaches that fail to account for spatial heterogeneity in vehicular data.

5.2 Dynamic Spatial Aggregation

Advanced implementations employ dynamic spatial aggregation strategies that adapt model sharing patterns based on real-time traffic conditions, seasonal variations, and special events. During major sporting events or natural disasters, for example, aggregation patterns may temporarily prioritize knowledge sharing among vehicles in affected areas while maintaining broader model synchronization for long-term learning stability. The dynamic spatial aggregation framework incorporates real-time contextual information to optimize federated learning performance by adapting communication patterns and model sharing strategies based on current operational conditions [10]. This adaptive approach enables more efficient resource utilization and improved learning outcomes by prioritizing knowledge exchange among vehicles experiencing similar environmental conditions or operational challenges.

The implementation of location-aware federated learning requires sophisticated algorithms that can balance local specialization with global generalization while managing the computational and communication overhead associated with spatial clustering and dynamic aggregation. Advanced spatial aggregation techniques leverage geographical proximity, traffic density patterns, and environmental similarity metrics to determine optimal grouping strategies that maximize learning effectiveness [10]. These systems must also address privacy concerns related to location data, implementing techniques such as location obfuscation and differential privacy to protect sensitive geographical information while maintaining the benefits of spatial awareness in federated learning processes. The integration of geospatial intelligence with federated learning creates opportunities for more personalized and context-aware autonomous vehicle systems that can adapt to local conditions while benefiting from collective knowledge across the entire vehicular network.

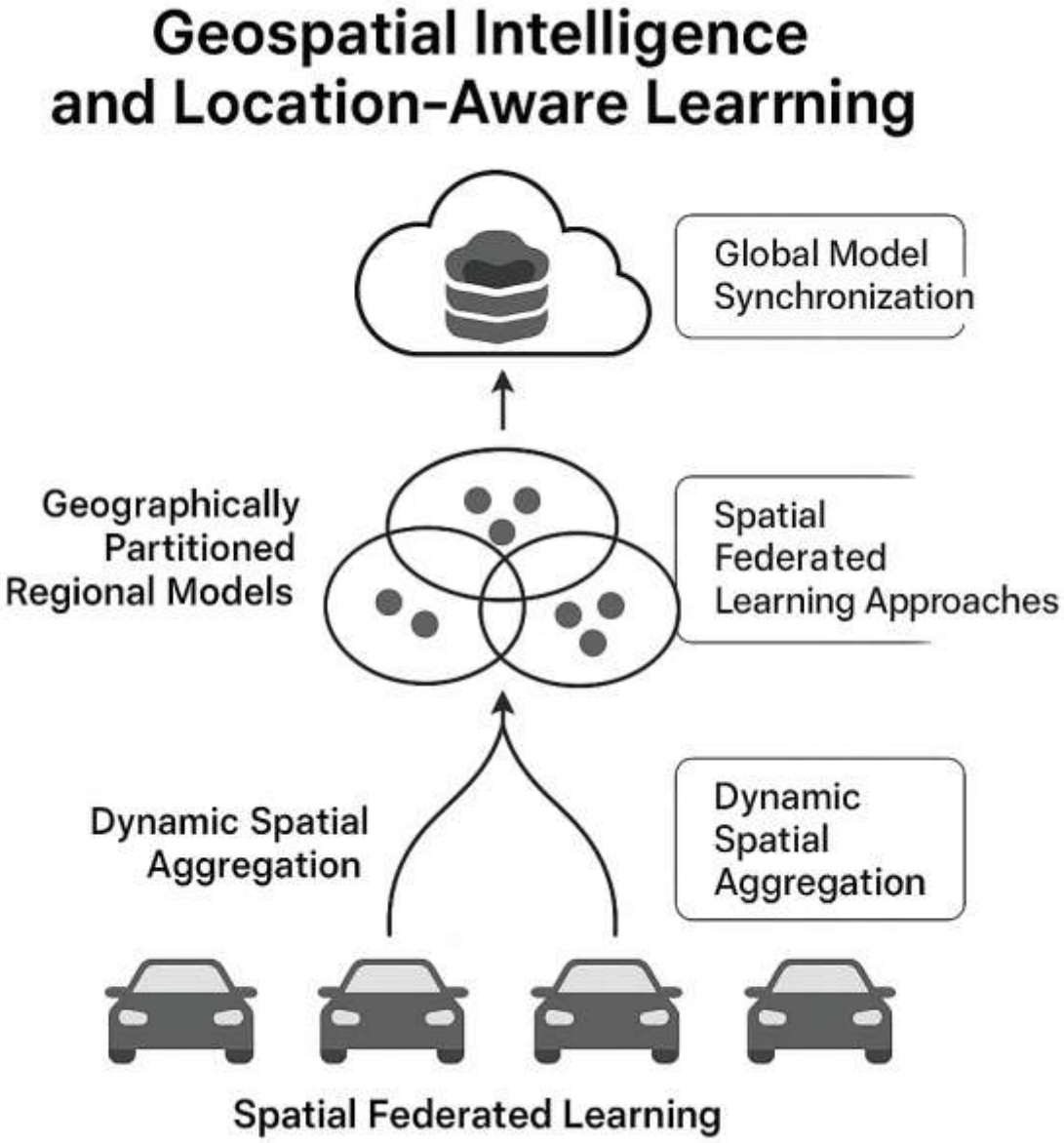

Fig. 4: Geospatially-Aware Federated Learning for Autonomous Vehicles [9, 10]

6. Real-World Implementation Case Studies

6.1 Automotive Industry Deployments

Leading automotive manufacturers have begun implementing federated learning architectures in production autonomous vehicle systems, providing valuable insights into practical deployment challenges and solutions. These implementations demonstrate significant improvements in model accuracy, privacy preservation, and system scalability compared to traditional centralized approaches. The transition from laboratory research to real-world deployment has revealed critical insights about the practical challenges of implementing federated learning in production autonomous vehicle systems, including communication reliability, computational resource management, and integration with existing vehicle architectures [11]. These industrial implementations have validated the feasibility of federated learning approaches while

highlighting the importance of robust system design and comprehensive testing frameworks for safety-critical automotive applications.

Automotive manufacturers have developed sophisticated federated learning platforms that leverage the distributed computational resources of their vehicle fleets to enable continuous model improvement without compromising individual privacy or overwhelming communication networks. The implementation of federated learning in production vehicles requires careful consideration of computational scheduling, network optimization, and integration with existing safety systems to ensure that collaborative learning processes do not interfere with critical autonomous driving functions [11]. These real-world deployments have demonstrated the practical benefits of federated approaches, including reduced data transmission costs, improved model personalization, and enhanced privacy protection, while also revealing the technical challenges associated with managing heterogeneous vehicle populations and maintaining model consistency across diverse operational environments.

6.2 Performance Metrics and Evaluation

Comprehensive evaluation of federated learning systems requires multi-dimensional performance metrics that capture accuracy, privacy, efficiency, and scalability characteristics. Standard machine learning metrics such as precision, recall, and F1-scores provide baseline performance indicators, but vehicular applications require additional safety-focused metrics including false positive rates for critical scenarios and response time distributions for emergencies. The evaluation of federated learning systems in autonomous vehicle contexts necessitates specialized benchmarking frameworks that can assess both individual model performance and system-wide collaborative learning effectiveness under realistic operational conditions [12]. These evaluation methodologies must account for the unique characteristics of vehicular data, including temporal dynamics, spatial heterogeneity, and the critical importance of maintaining consistent performance across diverse driving scenarios.

Privacy metrics must quantify the effectiveness of differential privacy and cryptographic protection mechanisms, typically measured through information-theoretic approaches such as mutual information analysis and adversarial attack resistance testing. Communication efficiency metrics evaluate bandwidth utilization, aggregation latency, and network resource consumption patterns. The development of comprehensive evaluation frameworks for vehicular federated learning requires integration of multiple performance dimensions, including model accuracy under various environmental conditions, privacy preservation effectiveness against sophisticated attacks, communication efficiency across different network topologies, and system scalability under varying participant loads [12]. These evaluation methodologies enable systematic comparison of different federated learning approaches and provide essential feedback for optimizing system performance in real-world automotive deployments, ensuring that federated learning implementations meet the stringent requirements of safety-critical autonomous vehicle applications.

7. Future Research Directions

7.1 Quantum-Enhanced Security

The emergence of quantum computing technologies presents both opportunities and challenges for federated learning security. Quantum-resistant cryptographic protocols are being developed to ensure long-term security against potential quantum computing attacks on current encryption methods. The advent of quantum computing poses significant threats to existing cryptographic foundations used in federated learning systems, necessitating the development of post-quantum cryptographic algorithms that can withstand attacks from both classical and quantum adversaries [13]. The transition to quantum-resistant security protocols becomes particularly critical for autonomous vehicle systems, where long-term data protection requirements and the extended operational lifespan of vehicular infrastructure demand cryptographic solutions that remain secure even as quantum computing capabilities advance over the coming decades.

Quantum machine learning techniques may eventually enable more efficient federated learning algorithms with superior privacy guarantees and computational performance. However, these technologies remain in

early research phases and require significant development before practical implementation. The potential integration of quantum computing principles with federated learning could revolutionize privacy preservation through quantum cryptographic protocols such as quantum key distribution and quantum secure multi-party computation [13]. These quantum-enhanced approaches promise theoretically unbreakable security guarantees based on fundamental quantum mechanical principles, potentially providing unprecedented privacy protection for sensitive vehicular data while enabling more efficient collaborative learning algorithms that leverage quantum computational advantages for complex optimization problems inherent in large-scale federated learning deployments.

7.2 Autonomous Fleet Orchestration

Future research focuses on fully autonomous federated learning systems that can self-organize, adapt aggregation strategies, and optimize resource allocation without human intervention. These systems would leverage artificial intelligence techniques to continuously improve their own federated learning processes, creating recursive learning capabilities that adapt to changing vehicle populations, network conditions, and performance requirements. The development of autonomous orchestration systems requires sophisticated meta-learning algorithms that can dynamically adjust federated learning parameters, participant selection strategies, and communication protocols based on real-time system performance metrics and environmental conditions [14]. These self-adaptive systems must incorporate advanced decision-making capabilities that enable automatic optimization of trade-offs between learning effectiveness, privacy protection, communication efficiency, and computational resource utilization across diverse operational scenarios.

The implementation of autonomous fleet orchestration involves complex multi-objective optimization problems that must balance competing requirements such as model accuracy, convergence speed, energy consumption, and network resource utilization while maintaining robust performance under varying operational conditions. Advanced reinforcement learning and evolutionary optimization techniques show promise for developing autonomous systems capable of continuous self-improvement and adaptation to dynamic vehicular network environments [14]. These autonomous orchestration systems would enable federated learning deployments to automatically scale and adapt to changing fleet compositions, varying network topologies, and evolving performance requirements without requiring manual intervention, thereby reducing operational complexity and enabling more efficient utilization of distributed computational resources across large-scale autonomous vehicle deployments while maintaining optimal learning performance and privacy protection.

Conclusion

Federated Learning architectures represent a transformative approach to privacy-preserving AI development in autonomous vehicles, successfully addressing the fundamental tension between model accuracy requirements and privacy protection needs. Through sophisticated cloud-edge integration, advanced cryptographic protocols, and geospatially-aware learning mechanisms, these systems enable unprecedented levels of collaborative intelligence while maintaining strict data privacy controls. The comprehensive analysis presented in this research demonstrates that federated learning frameworks provide viable solutions for the complex challenges of distributed machine learning in vehicular environments, including statistical heterogeneity, communication constraints, and temporal dynamics inherent in automotive data. The successful implementation of federated learning in production autonomous vehicle systems validates the practical viability of these approaches, with demonstrated improvements in model accuracy, privacy preservation, and system scalability compared to traditional centralized methodologies. The integration of hierarchical architectures, differential privacy mechanisms, and secure multiparty computation protocols creates robust frameworks that protect individual privacy while enabling collective intelligence advancement across vehicular networks. As the autonomous vehicle industry continues its rapid evolution toward fully automated transportation systems, federated learning architectures will play an increasingly critical role in enabling safe, intelligent, and privacy-respecting mobility solutions. Future developments in quantum-enhanced security, autonomous fleet orchestration, and advanced communication technologies will further expand the capabilities of federated learning systems, creating

new opportunities for collaborative intelligence that extends beyond individual vehicle optimization to encompass entire transportation ecosystems. The continued research and development of these technologies will be essential for realizing the full potential of autonomous vehicle systems while maintaining the privacy rights and security expectations of users in an increasingly connected automotive landscape.

References

[1] Mohab M. Eid Kishawy et al., "Federated learning system on autonomous vehicles for lane segmentation," Scientific Reports, 2024. [Online]. Available: https://www.nature.com/articles/s41598-024-71187-8

[2] Vishnu Pandi et al., "Federated Learning for Connected and Automated Vehicles: A Survey of Existing Approaches and Challenges," Research Gate, 2023. [Online]. Available: https://www.researchgate.net/publication/373263350_Federated_Learning_for_Connected_and_Automated_Vehicles_A_Survey_of_Existing_Approaches_and_Challenges

[3] Tian Li et al., "Federated Learning: Challenges, Methods, and Future Directions," IEEE Signal Processing Magazine, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9084352

[4] Shiying Zhang et al., "Federated Learning in Intelligent Transportation Systems: Recent Applications and Open Problems," arXiv:2309.11039, 2023. [Online]. Available: https://arxiv.org/abs/2309.11039

[5] Shiqiang Wang et al., "Adaptive Federated Learning in Resource Constrained Edge Computing Systems," arXiv:1804.05271v3, 2019. [Online]. Available: https://arxiv.org/pdf/1804.05271

[6] Yi Liu et al., "Privacy-Preserving Traffic Flow Prediction: A Federated Learning Approach," IEEE Internet of Things Journal, Volume 7, Issue 8, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9082655

[7] Cynthia Dwork, "Differential Privacy: A Survey of Results," Springer, 2008. [Online]. Available: https://web.cs.ucdavis.edu/~franklin/ecs289/2010/dwork_2008.pdf

[8] Daniel Escudero, “An Introduction to Secret-Sharing-Based Secure Multiparty Computation,” 2023. [Online]. Available: https://eprint.iacr.org/2022/062.pdf

[9] Yue Zhao et al., "Federated Learning with Non-IID Data," arXiv:1806.00582, 2018. [Online]. Available: https://arxiv.org/abs/1806.00582

[10] Takayuki Nishio and Ryo Yonetani, "Client selection for federated learning with heterogeneous resources in mobile edge," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8761315

[11] Andrew Hard et al., "Federated learning for mobile keyboard prediction," arXiv:1811.03604, 2019. [Online]. Available: https://arxiv.org/abs/1811.03604

[12] Peter Kairouz et al., "Advances and open problems in federated learning," arXiv:1912.04977, 2021. [Online]. Available: https://arxiv.org/abs/1912.04977

[13] John Preskill, "Quantum computing in the NISQ era and beyond," arXiv:1801.00862v3, 2018. [Online]. Available: https://quantum-journal.org/papers/q-2018-08-06-79/

[14] Virginia Smith et al., "Federated multi-task learning," arXiv:1705.10467, 2018. [Online]. Available: https://arxiv.org/abs/1705.10467