World Journal of Engineering Research and Technology

WJERT

www.wjert.org **SJIF Impact Factor: 7.029**

FEDERATED HD MAP UPDATING FRAMEWORK FOR PRIVACY-PRESERVING COLLABORATIVE AUTONOMOUS NAVIGATION

Mohammed Sharfuddin*

MS in Computer Science, Campbellsville University, KY, USA.

Article Received on 21/07/2025 **Article Revised on 12/08/2025** **Article Accepted on 01/09/2025**

***Corresponding Author**
Mohammed Sharfuddin
MS in Computer Science,
Campbellsville University,
KY, USA.

ABSTRACT

High-definition (HD) maps are essential for safe and efficient autonomous vehicle (AV) navigation. However, centralized HD map updating frameworks face limitations such as high latency, single points of failure, and user privacy concerns. In this paper, we propose a federated HD map updating framework that enables real-time, privacy-preserving collaboration between autonomous vehicles. Each vehicle detects road environment changes using AI-powered feature extraction and securely shares minimal metadata with a central map server using differential privacy and homomorphic encryption techniques. This federated approach ensures faster updates, distributed intelligence, and robust protection of sensitive location data. Our framework builds prior work in real-time HD map monitoring, AI-based change detection, and V2X security, and demonstrates improved map accuracy and update efficiency across a simulated AV fleet.

1. INTRODUCTION

Autonomous vehicles (AVs) rely heavily on high-definition (HD) maps to accurately perceive and interpret their surroundings. Unlike traditional navigation maps, HD maps offer centimeter-level precision and dynamic semantic layers, including road edges, traffic signs, lane-level geometry, and 3D objects. These maps complement real- time sensors like LiDAR and camera, enabling safe lane changes, path planning, and obstacle avoidance. However, HD maps are only as effective as their freshness and accuracy.

The current approach to updating HD maps often involves centralized data collection and processing, where vehicles upload large datasets to a central server for offline analysis and integration. While this model provides control and consistency, it suffers from major limitations, especially in the context of real-time and large-scale deployment. Centralized pipelines introduce latency, bandwidth bottlenecks, and expose sensitive vehicle data, raising privacy concerns and potential cybersecurity risks.

Recent advancements in federated learning (FL) and edge AI provide a promising alternative. Federated learning enables multiple agents (vehicles, in this case) to collaboratively train models or share updates without exposing raw data. When applied to HD map updates, this concept allows vehicles to locally detect changes in road environments and contribute securely to a shared map without compromising privacy.

In this research, we present a novel Federated HD Map Updating Framework designed to address the challenges of scalability, privacy, and real-time responsiveness. Each autonomous vehicle acts as an intelligent agent that detects changes using AI-based feature extraction models, and sends minimal encrypted deltas to the cloud. These deltas are processed using secure aggregation techniques such as homomorphic encryption and differential privacy, ensuring that sensitive geospatial or driving behavior data remains protected.

This paper builds upon our earlier work on:

- Real-time HD map change detection using sensor fusion and AI,
- Data structure optimization for low-latency map access,
- Quality monitoring pipelines using big data frameworks, and
- V2X security techniques in autonomous navigation systems.

Through simulation experiments and architectural modeling, we demonstrate that our proposed framework enables timely, accurate, and privacy-preserving HD map updates for large-scale AV networks.

2. Related Work

The development and maintenance of high-definition (HD) maps for autonomous vehicles (AVs) have been the subject of extensive research over the last decade.

Traditional methods rely on periodic mapping vehicles and manual annotation, which are time-consuming and prone to obsolescence. More recent efforts focus on automation through

AI and distributed sensing. In this section, we review key prior works relevant to HD map data collection, real-time updates, privacy concerns, and collaborative intelligence in autonomous systems — including strategic references to our own research contributions.

2.1 Real-Time HD Map Change Detection

HD maps require frequent updates to reflect dynamic changes such as new road constructions, lane closures, or altered traffic signs. In our earlier work, AI-Powered Change Detection for High-Definition Map Updates in Autonomous Driving, we proposed a deep learning pipeline that integrates LiDAR, camera, and GNSS/IMU data to identify environmental changes. This model proved effective in automatically detecting and classifying scene modifications without relying on centralized validation processes.

2.2 HD Map Quality Monitoring at Scale

In Scalable Data Mining Pipeline for Real-Time HD Map Quality Monitoring, we presented a distributed pipeline capable of processing map tiles in real time to detect anomalies, data gaps, and quality degradations. This work laid the foundation for implementing real-time feedback loops within large-scale AV ecosystems. The insights from this system highlighted the importance of integrating quality validation directly into the update cycle.

2.3 Optimized Data Access and Map Structuring

Efficient data structures are crucial for both storage and in-vehicle retrieval of HD maps. In Optimizing Data Structures for Real-Time HD Map Processing in Autonomous Driving Systems, we demonstrated that advanced indexing strategies and modular data representations could reduce latency by up to 60%. These techniques ensure that vehicles can quickly retrieve and update only relevant segments of the map, which is particularly relevant for federated models.

2.4 Secure HD Map Transmission in Connected Vehicles

AV networks are exposed to various cybersecurity threats, especially during data transmission. In Security Challenges in Connected Autonomous Vehicles: A Case Study of HD Map Transmission, we explored potential vulnerabilities in V2X-based map exchange and proposed layered security models combining symmetric encryption, TLS tunnels, and vehicular authentication protocols.

2.5 Federated Learning in AV Systems

Federated learning has gained attention for its ability to decentralize intelligence across distributed nodes. Notable studies such as Li et al. (2021) have applied FL to vehicle trajectory prediction and object detection, showing promising results in reducing data leakage. However, the application of FL in map update scenarios remains underexplored, particularly with the integration of privacy-preserving techniques like homomorphic encryption or differential privacy.

2.6 Privacy and Trust in Collaborative Mapping

With AVs continuously scanning their environments, concerns around driver tracking, behavior profiling, and unauthorized surveillance arise. Previous research has proposed cryptographic protocols and trusted execution environments to mitigate such risks. Our proposed framework builds upon these insights by applying differential privacy to geo-temporal map deltas and using secure aggregation to anonymize vehicle contributions.

3. METHODOLOGY

To address the limitations of centralized HD map updating in autonomous vehicles, we propose a Federated HD Map Updating Framework that enables collaborative, secure, and privacy-preserving map refinement using distributed intelligence across vehicle fleets. The framework comprises four key components: local perception and detection, map delta generation, privacy-preserving communication, and central aggregation and validation.

3.1 Local Change Detection Using Onboard AI

Each autonomous vehicle is equipped with a sensor fusion system combining LiDAR, camera, and GNSS/IMU data. An AI-based perception module — pre-trained and incrementally refined — continuously analyzes sensor data to detect environmental changes. These changes may include lane shifts or newly painted markings, construction zones or temporary obstacles, and signage updates or missing infrastructure. This process builds upon the system we developed in previous research, where multi-sensor data is processed through a convolutional neural network (CNN) for spatial feature extraction and scene comparison against the local HD map cache.

3.2 Generation of Encrypted Map Deltas

When a change is detected, the vehicle generates a map delta, a lightweight record summarizing change type, GPS coordinates (rounded for privacy), confidence score of detection, timestamp, and sensor source. Rather than uploading raw sensor data, only this delta is prepared for transmission. Each delta is encrypted locally using either homomorphic encryption or a hybrid approach involving symmetric AES encryption with secure key exchange.

3.3 Privacy-Preserving Communication Protocol

To ensure anonymity and security, the framework employs differential privacy (adding noise to GPS coordinates and metadata), secure aggregation protocols (aggregating encrypted deltas before decryption), and trusted execution environments (TEEs) on edge servers for isolated processing of sensitive computations. This architecture improves upon traditional TLS-based communication by integrating content privacy and identity abstraction.

3.4 Central Aggregation and Consensus

On the cloud side, encrypted deltas are decrypted after aggregation and cross-verified using consensus from multiple vehicle submissions, historical map data, and real-time road authority feeds. Updates are approved when confidence exceeds a predefined threshold and consistency is validated. The central system does not store identifying vehicle data.

3.5 Federated Learning for AI Model Improvement

Alongside map deltas, vehicles participate in federated model training for change detection. Each vehicle trains locally on recent data and shares encrypted gradient updates, which are aggregated centrally and redistributed as updated AI models. This allows the change detection model to continuously improve without compromising local data privacy.

3.6 Framework Architecture Diagram

(A diagram showing vehicle nodes with AI change detection → encrypted delta → cloud aggregator → HD map update system.)

4. Experimental Setup

To evaluate the proposed Federated HD Map Updating Framework, we designed a series of experiments simulating a fleet of autonomous vehicles operating in a dynamic urban environment. The primary goals of this evaluation were to measure update latency compared to centralized methods, accuracy of detected map changes and integration, effectiveness of privacy-preserving techniques, and impact on federated model convergence and performance.

4.1 Simulation Environment

A virtual urban scenario was created using the CARLA simulator (version 0.9.13), modeling a 5 km^2 city grid with roads, traffic signals, construction zones, and variable weather conditions. Fifty AV agents were deployed, each equipped with simulated LiDAR, camera, GPS/IMU, and onboard computing resources capable of running AI- based perception algorithms.

4.2 Dataset and Ground Truth

We used a baseline HD map generated from initial survey data and maintained a dynamic log of map changes including lane closures due to construction, newly installed traffic signs, and temporary obstacles such as parked vehicles and road debris. Ground truth annotations were created manually for these events to evaluate detection accuracy.

4.3 Federated Learning Setup

Each vehicle hosted a local AI model based on a lightweight CNN architecture trained to detect changes in point cloud and camera data. Model updates were shared every 10 minutes with a simulated cloud aggregator using secure aggregation protocols.

4.4 Privacy Parameters

Differential privacy noise magnitude was set to $\varepsilon = 0.5$ for geospatial data perturbation. Homomorphic encryption used Paillier cryptosystem with 1024-bit keys for map delta encryption. Secure aggregation enforced minimum batch size of 5 vehicles per aggregation round.

4.5 Baseline Methods for Comparison

We compared our framework with centralized update model (vehicles upload full raw sensor data) and non-encrypted federated model (federated learning and delta uploads without encryption).

4.6 Evaluation Metrics

Update latency, detection accuracy (precision, recall, F1-score), privacy leakage risk, and federated model performance (convergence and detection accuracy over time) were measured.

5. RESULTS AND DISCUSSION

This section presents the findings from the experiments evaluating the performance of our Federated HD Map Updating Framework relative to baseline methods.

5.1 Update Latency

Our framework achieved a mean update latency of 45 seconds, significantly faster than the centralized model's average of 5 minutes. The federated approach reduces the volume of data transmitted by sharing lightweight map deltas instead of raw sensor data, and the privacy-preserving aggregation protocols add minimal overhead (~5 seconds).

5.2 Detection Accuracy

Method	Precision	Recall	F1-Score
Proposed Federated Model	0.92	0.89	0.90
Centralized Update Model	0.95	0.93	0.94
Non-Encrypted Federated Model	0.91	0.88	0.89

While the centralized model slightly outperforms in accuracy, the federated model's performance remains high and acceptable for practical deployment. Privacy measures introduce negligible accuracy degradation.

5.3 Privacy Preservation Effectiveness

Location re-identification attacks on the federated system showed a successful re-identification rate below 3%, demonstrating strong resistance to privacy leakage, compared to over 25% for non-encrypted federated models.

5.4 Federated Learning Model Performance

The federated AI model converged to 90% of centralized training accuracy within 15 aggregation rounds, demonstrating efficient learning with privacy constraints.

5.5 DISCUSSION

The results validate the proposed framework's capability to maintain near-real-time HD map updates with strong privacy guarantees. Though a slight trade-off in detection accuracy exists compared to centralized models, the framework's scalability and security benefits make it well-suited for large autonomous fleets.

Potential limitations include computational overhead on vehicle nodes and dependency on reliable V2X communication. Future work could explore blockchain integration for decentralized consensus and extend privacy techniques with trusted hardware enclaves.

6. CONCLUSION AND FUTURE WORK

In this paper, we proposed a novel Federated HD Map Updating Framework that addresses key challenges in real-time, privacy-preserving collaboration for autonomous vehicle navigation. By combining onboard AI-based change detection with secure, privacy-enhancing communication protocols such as differential privacy and homomorphic encryption, our framework enables autonomous vehicles to collaboratively maintain fresh, accurate, and secure HD maps.

Simulation experiments demonstrated that our framework achieves a significant reduction in map update latency compared to centralized systems while maintaining high detection accuracy and robust privacy guarantees. Federated learning techniques effectively enhanced the change detection model across the vehicle fleet without exposing raw sensor data.

Our work bridges multiple research areas—HD mapping, autonomous systems security, and federated AI—and opens several avenues for future exploration. Future work will focus on integrating blockchain-based consensus mechanisms to further decentralize map validation, optimizing computational resource usage on edge devices, and testing in real- world AV fleets.

Overall, this research advances the state-of-the-art in collaborative autonomous navigation and provides a secure, scalable foundation for next-generation HD map updating systems.

REFERENCES

1. Sharfuddin Mohammed. "AI-Powered Change Detection for High-Definition Map Updates in Autonomous Driving. DOI: 10.13140/RG.2.2.22018.80320 https://www.researchgate.net/publication/392364113_AI-POWERED_CHANGE_DETECTION_FOR_HIGH-DEFINITION_MAP_UPDATES_IN_AUTONOMOUS_DRIVING
2. Sharfuddin Mohammed. "Scalable Data Mining Pipeline for Real-Time HD Map Quality Monitoring. DOI: 10.13140/RG.2.2.35440.57602 https://www.researchgate.net/publication/392526167_SCALABLE_DATA_MINING_PIPELI NE_FOR_REAL-TIME_HD_MAP_QUALITY_MONITORING
3. Sharfuddin Mohammed. "Optimizing Data Structures for Real-Time HD Map Processing in Autonomous Driving Systems. DOI : 10.13140/RG.2.2.27228.91528 https://www.researchgate.net/publication/392526316_Optimizing_Data_Structures_for_Re

al-Time_HD_Map_Processing_in_Autonomous_Driving_Systems/citations

4. Sharfuddin Mohammed. "Security Challenges in Connected Autonomous Vehicles: A Case Study of HD Map Transmission.
   DOI: 10.13140/RG.2.2.31397.00481
   https://www.researchgate.net/publication/392526073_SECURITY_CHALLENGES_IN_C
   ONN
   ECTED_AUTONOMOUS_VEHICLES_A_CASE_STUDY_OF_HD_MAP_TRANSMIS
   SION
5. T. Li, A. K. Sahu, A. Talwalkar, V. Smith, "Federated Learning: Challenges, Methods, and Future Directions," IEEE Signal Processing Magazine, 2021; 37(3): 50–60.
6. J. Zhao et al., "Privacy-Preserving Vehicle Collaboration via Secure Federated Learning," ACM Transactions on Intelligent Systems and Technology, 2022; 13(4): 1–21.
7. B. Bonawitz et al., "Practical Secure Aggregation for Privacy-Preserving Machine Learning," Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017.