ACTA TECHNICA JAURINENSIS
Vol. 19, No. 4, pp. 335-344, 2026
10.14513/actatechjaur.00993

Research Article

Secure and Distributed Automotive Logistics Systems Integrating Federated Learning and Blockchain for Cognitive Vehicle Networks

Vetrivel Palpandi[1*], Raja Guru Ramaraj[2], Prabhu Radhakrishnan[3]

[1*]Department of Artificial Intelligence and Data Science, Ramco Institute of Technology, Rajapalayam-626117, Virudhunagar, Tamil Nadu, India
[2] Department of Computer Science and Engineering, RMK College of Engineering and Technology, Puduvoyal-601206, Tiruvallur, Tamil Nadu, India
[3] Department of Artificial Intelligence and Data Science, AAA College of Engineering and Technology, Sivakasi-626123, Virudhunagar, Tamilnadu, India
*e-mail: vetrilev17@gmail.com

Submitted: 24/02/2026 Revised: 02/04/2026 Accepted: 05/06/2026 Published online: 25/11/2026

Abstract: The rapid advancement of Internet of Things (IoT) technologies has significantly transformed automobile logistics by enabling real-time vehicle tracking, intelligent route planning, autonomous fleet coordination, and cognitive decision-making. These smart applications, however, generate a vast amount of sensitive vehicular and logistics data, which presents challenges in terms of privacy, scalability, and computational overhead. To address these issues, this paper proposes a Secure and Optimized Federated Learning Model (SOFLM) tailored for cognitive automotive logistics systems. Unlike traditional centralized models, SOFLM enables edge-level training on distributed vehicle nodes, ensuring data privacy and local intelligence. The core of SOFLM is a novel algorithm—Adaptive Federated Learning with Blockchain Security (AFL-BS)—which reduces computational costs and communication overhead by employing Top-K Gradient Compression and Entropy Encoding, and secures updates via blockchain consensus using the Practical Byzantine Fault Tolerance (PBFT) algorithm. Experimental evaluation suggests a 40% reduction in computation time and a 30% decrease in network load, while maintaining strong data security and integrity. The proposed framework supports scalable and privacy-preserving learning for next-generation intelligent transport and logistics systems, empowering real-time cognitive decision-making in dynamic automotive environments.

Keywords: IoT; Automotive Logistics; Federated Learning; Blockchain; Fog Computing; Cognitive Applications; Connected Vehicles

I. INTRODUCTION

Cars now share live updates about their location, speed, and condition using internet-connected tools that help plan smarter routes and manage groups of vehicles without human input. Because of built-in sensors and constant links to outside networks, each car produces tons of detailed information while it moves through daily operations. This stream of facts helps teams make faster choices, cut down on fuel waste, and fix parts before they fail. Yet relying so heavily on digital signals brings new concerns - private details might be exposed, systems could struggle to grow smoothly, delays may happen in message delivery, and automated decisions are not always dependable. Sending vehicle data straight to big cloud computers creates problems. Because it travels far, hackers might grab it along the way. Delays also happen when everything must go through one central point. Cars spread out across roads do not work well like that. Their gadgets often have limited power and memory. A newer idea trains models right inside each car instead. This keeps raw details close, avoiding exposure. Information stays local while only pieces of learning move around. Even so, passing updates between vehicles uses lots of bandwidth. The patterns each car sees differ wildly from others'. One truck's experience does not match a city taxi's. Bad actors could trick the system by sending false results. Trust remains shaky when combining inputs without seeing who sent what. Lately, research points to machine learning shaping

how goods move and how choices are made across transit routes [27]. Meanwhile, staying safe while vehicles talk to each other pushes new tools that spot strange behavior using smart algorithms [28]. What stands out is the push to blend protection, speed, and room to grow - into one working design. One way around these problems begins with a new setup called SOFLM - a secure, lean version of federated learning. This system brings together adaptive learning methods paired with blockchain-backed security, running partly through fog nodes. Instead of heavy data transfers, the method uses Top-K gradient shrinking along with smart coding based on entropy. Trust stays intact because each update gets verified via blockchain, powered by PBFT rules that handle faulty inputs well. Privacy takes another step forward when noise layers are added during training, shielding vehicle details without slowing things down. Fewer delays happen when processing moves near where data begins, which fog computing makes possible. Instead of working alone, combining shared learning, fog systems, and blockchains builds stronger results across vehicle networks. Most current methods tackle one issue at a time - this new approach handles privacy, speed, and reliability together. One piece fits another, forming something harder to break. Put simply, this approach allows quick, safe choices in car shipping networks without risking user data. Because smart functions spread through linked cars, operations stay steady even when demand grows. That fit matters most where transport tech keeps evolving fast.

II. Literature Survey

Faster advances in split-up learning tools - like FL, blockchains, or fog setups - are reshaping how car supply chains work today. Distributed brains pop up across devices, personal info stays safer, while vehicle-linked nets stretch further. Yet fitting all these pieces together smoothly? Real-time demands push hard against that goal still. Learning across devices now happens without moving actual data, thanks to methods that train models together but apart. Some early attempts used privacy-preserving tricks during knowledge transfer [1], whereas others adjusted how often updates were sent to save bandwidth [2]. Systems skipping central hubs entirely have since emerged [3], proving useful even in car networks where speed matters [4]. Even so, uneven data spread, heavy message traffic, and limits in scaling still trip things up today. Trust issues get tackled by linking blockchain with FL setups. Through systems like those used in smart transport [5], updates to models stay protected and unchanged. Some designs combine scalability with blockchain plus FL [6], making sure checks on data remain strong. When IoT teams up with these blockchains and FL methods [7], moving information safely gets easier across far-flung nodes. Yet adding blockchain can slow things down, demanding more computing power - this becomes a hurdle when quick decisions matter most in vehicle networks. Work in [8], [9] looks at how federated learning and distributed optimization work, bringing up issues like slow message exchange and lack of central control. Cars talking to each other rely on systems near the road, shown in [10], along with mobile car-based networks from [11]. Instead of centralized brains, vehicles use IoV setups in [12], spreading smart decisions across many points - yet these need solid ways to sort through tons of information. Lately studies have turned toward better privacy, stronger security, safer handling of resources in FL setups. Blockchain-powered defenses against gradient leaks [13] add a layer of safety. Efficiency gets a boost from eco-conscious, power-smart FL designs [14], [15], especially where devices operate at network edges. Transport networks now test secure data flow using grouped device coordination [16], showing how stability and room to grow matter deeply in system design. Edge intelligence improvements, together with progress in distributed AI [17], allow instant handling of information close to where it's generated. Instead of central hubs, large FL setups [18] show how performance holds up under pressure - research [19] digs into why some systems struggle when they grow. From early digital currencies like Bitcoin [20], core ideas emerged that now back secure, shared agreements within today's FL-blockchain hybrids. Lately, work around how people move and car supply chains has started drawing more interest. Work from [21] on thinking-driven movement, along with findings in [22] about smarter auto shipping, shows shifts in transport tech. Looking deeper into space use in transit [23], paired with sustainable IoT methods via blockchain [24], underlines why connected systems matter. On top of that, forecasting traffic with federated learning [25], together with new patterns in mobile access [26], reveals a steady push toward blending these tools - blockchain, FL, and smart travel networks. Lately, efforts spotlight how machine learning blends with thinking-like tech inside logistics setups, opening paths to smarter choices shaped by data across today's transport routes [27]. Not far off, safety issues on vehicle communication grids get tackled using models that learn patterns, spotting odd or harmful behavior where systems spread out interact [28]. Even with progress, current studies usually look at just one thing - privacy, say, or how fast systems talk to each other. What's missing is a single system handling scale, trust, data flow, and quick choices together in vehicle supply chains. To help fix that, SOFLM combines smart training methods across devices, checks truthfulness through blockchain using PBFT, while cutting down message size via Top-K selection plus entropy coding. Instead of separate fixes, this mix delivers protection, room to grow, and speed - built right into learning processes for smarter car shipping

networks. **Table 1** summarizes the contributions and limitations of these approaches.

Table 1. *Summary of FL Framework*

Research Focus	Key Contributions	Advantages	Drawbacks	Remarks
Federated Learning in Vehicular and IoT Systems	Chaddad et al. discussed FL for traffic prediction and diagnostics; Maurya et al. enhanced FL security with SMPC and SSS	- Data privacy through local training - Handles distributed edge sources - Secure multiparty computation support	- Non-IID data leads to accuracy drop - Centralized aggregation bottlenecks - Scalability issues on resource-constrained devices	Emphasizes need for efficient, privacy-preserving FL at the edge
Blockchain Integration for Secure FL	Commey et al. proposed post-quantum blockchain FL; Bhatia et al. explored FL-blockchain integration for mobility platforms	- Tamper-proof model updates via smart contracts - Strong cryptographic guarantees	- High latency - Bulky computations - Network inefficiency on edge nodes	Blockchain adds trust but must be optimized for vehicular systems
Communication and Computation Optimization	Chen et al. introduced pFedCAS with adaptive scarification; Tian et al. applied Ring-AllReduce with secret sharing	- Reduced bandwidth usage - No central server - Decentralized model training	- Lack of blockchain verification - Susceptibility to tampered updates	Shows need for combining secure aggregation with efficient compression
Fog Computing for Distributed Intelligence	Ni et al. developed FedSL for fog-enabled split learning; Bagher Salimi et al. used teacher-student FL for wearables	- Reduces edge computation - Enables real-time learning- Supports serverless deployment	- Exposes intermediate data - Requires complex coordination	Fog enables scalability but must ensure privacy and simplicity
Hybrid Models: FL + Blockchain + Compression	Proposed SOFLM integrates FL, PBFT blockchain, Top-K Compression, and Entropy Encoding	- Tamper-resistant updates - Low communication overhead - Secure and scalable learning	- Yet to be widely adopted or compared against all baselines in large-scale vehicular settings	Provides a unified, real-time, and secure solution for cognitive automotive logistics

III. Proposed Methodology

The Secure and Optimized Federated Learning Model (SOFLM), a secure and privacy-preserving federated learning framework for distributed automotive logistics utilizing cognitive IoT-enabled vehicles, is described in this section. The Adaptive Federated Learning with Blockchain Security (AFL-BS) algorithm, which combines federated learning, fog-level aggregation, blockchain-based validation, and communication-efficient model updates, is used to implement the fundamental learning mechanism. **Fig. 1** shows how the vehicle, fog and blockchain layers exchange model updates.

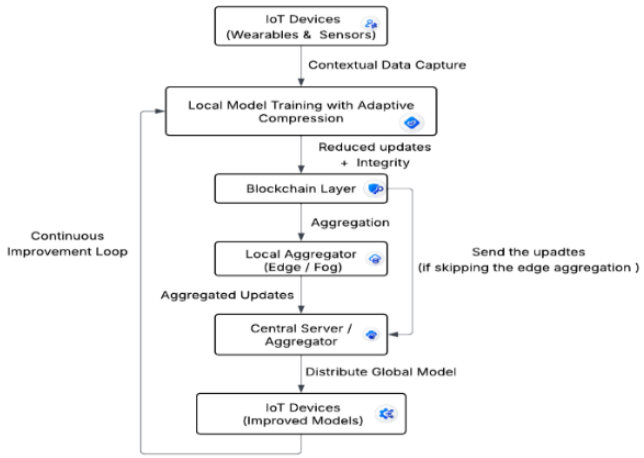


Figure 1. *Proposed Federated Learning Framework*

1. System Overview

The SOFLM framework operates across three levels:

Edge Layer (Vehicles): Using onboard telemetry data, cognitive IoT-enabled cars locally train models.

Fog Layer: Partial aggregation and validation of received updates are carried out by fog nodes, such as fleet hubs or roadside units.

Blockchain Layer: Using PBFT consensus, a permissioned blockchain guarantees safe, impenetrable validation of model updates.

Each vehicle trains a local deep neural network (DNN) using telemetry data (e.g., GPS, engine RPM, speed, fuel usage) and transmits compressed updates to its designated fog node. The fog node partially aggregates these updates, forwards them to the blockchain, and validates them using smart contracts and consensus protocols, ensuring integrity and trust.

2. Data Assumptions and Preprocessing

SOFLM is predicated on the availability of locally stored vehicle telemetry data, such as: GPS routes and trajectories, Fuel and engine consumption metrics, Indicators of driver behavior (acceleration, braking, speed)

The following preprocessing techniques are used locally to guarantee compatibility across heterogeneous vehicles: Kalman or low-pass filters for noise reduction, Z-score normalization Segmenting sliding windows for time-series modeling

Data is still non-IID across clients, reflecting the diversity of driving habits and vehicle usage in the real world.

3. Adaptive Federated Learning with Blockchain Security (AFL-BS)

The AFL-BS algorithm ensures secure and efficient model training across vehicles. It performs the following steps:

Top-K Gradient Compression: Only the top-K most significant gradients are selected to minimize transmission size.

Entropy Encoding: A lossless compression technique is applied to further reduce bandwidth usage.

Differential Privacy: Gaussian noise is added to gradient updates, ensuring that sensitive vehicle or driver behaviours cannot be inferred.

Blockchain Integration (PBFT): Each update is verified using Practical Byzantine Fault Tolerance, protecting the system from tampering or malicious updates.

Adaptive Aggregation: Updates from vehicles are weighted based on convergence rate, trust score, and gradient quality before aggregation.

4. Mathematical Formulation

Let the weight of the model on the device i in round t be ω_i^t.

1. Local Update

$$\boldsymbol{\Delta w_i^t = \omega_i^t - \omega^{t-1}} \quad \textbf{(1)}$$

2. Top-K Compression

$$\boldsymbol{\Delta \omega_{i,top-k}^t = TopK(\Delta \omega_i^t)} \quad \textbf{(2)}$$

3. Entropy Encoding

$$\boldsymbol{E\left(\Delta \omega_{i,top-k}^t\right) = H\left(\Delta \omega_{i,top-k}^t\right)} \quad \textbf{(3)}$$

4. Differential Privacy

$$\boldsymbol{\widetilde{\Delta} w_i^t = \Delta w_i^t + N(0, \sigma^2)} \quad \textbf{(4)}$$

5. Adaptive Aggregation

$$\boldsymbol{\omega^{t+1} = w^t + \frac{1}{N}\sum_{i=1}^{N} \alpha_i \widetilde{\Delta} w_i^t} \quad \textbf{(5)}$$

5. Blockchain Validation and Aggregation at Fog-Level

Incoming updates are verified by fog nodes by:

Digital signature verification Verifying the structure and magnitude of the gradient rejecting updates that are unusual or incorrect. A permissioned blockchain receives validated updates, and PBFT consensus makes sure that only reliable updates are added to the global model.

6. AFL-BS Algorithm

Adaptive Federated Learning with Blockchain Security (AFL-BS)

Input: Local datasets, initial global model G_0, privacy budget ε,Top-K threshold, noise level, total rounds

Output: Final global model G^*

Set up the global model.

For every training session:

Vehicles that qualify train regional models

Use differential privacy and Top-K compression.

Send signed updates to fog nodes.

Updates are verified and partially aggregated by fog nodes.

Blockchain carries out PBFT consensus

Global aggregation is carried out.

Vehicles receive an updated model broadcast.

Continue until you reach convergence.

7. Energy-Conscious Participation Plan

Each vehicle's participation is dependent on its:

Battery/power level, Processor load, Signal variation over time. Vehicles with low energy or stagnant data are skipped to save resources and avoid unnecessary computation, making SOFLM energy-efficient and suitable for real-world deployment.

8. Lightweight Deployable DNN

SOFLM employs a lightweight deep neural network using depth wise separable convolutions and INT8 quantization, enabling fast (<100 ms) inference on embedded devices such as ESP32 or Jetson Nano. The model is trained on automotive data for real-time tasks such as fault prediction, route deviation alerts, or energy efficiency estimation.

9. Algorithm: Secure and Optimized Federated Learning Model (SOFLM)

Input:

Set of distributed IoT clients $C = \{c_1, c_2, ..., c_n\}$

Initial global model G_0

Blockchain ledger B

Fog nodes $F = \{f_1, f_2, ..., f_m\}$

Parameters: learning rate η, privacy budget ε, compression threshold Top-K

Output:

Final global model G*

Secure and energy-efficient training with privacy and integrity control

Step 1: Initialization

Deploy initial model G_0 to all eligible clients.

Set thresholds for participation: battery level, signal strength, data variance.

Set privacy budget ε, compression rate Top-K, and enable PBFT consensus on blockchain B.

Step 2: Client-side Local Training (at each client c_i)

For each round t = 1 to T:

Participation Check

If battery > threshold and signal quality is good:

→ Participate

Else:

→ Skip this round

Local Model Update

Train model G_i on local data for E epochs using SGD:

$$G_i = G_0 - \eta \nabla L_i(G_0) \quad (6)$$

Differential Privacy Protection

Add noise to gradients:

$$G_i' = G_i + N(0, \sigma^2) \quad (7)$$

where noise calibrated to budget ε

Gradient Compression

Extract top-K significant gradients:

$$\Delta_i = \text{TopK}(G_i' - G_0) \quad (8)$$

Send Update

Transmit Δ_i and metadata to assigned fog node f_j

Step 3: Fog Node Aggregation (at each f_j)

Receive and Validate Updates

Validate authenticity using smart contract and check signature/hash

Partial Aggregation

Aggregate compressed gradients from local clients:

$$G_j = \text{Aggregate}(\{\Delta_1, \Delta_2, ..., \Delta_k\}) \quad (9)$$

Submit Aggregated Update to Blockchain

Encrypt & hash update

Submit to blockchain B for verification via PBFT

Step 4: Blockchain Verification

Execute PBFT Consensus

Accept only verified updates

Reject poisoned/malicious updates

Append Validated Update to Ledger

Store G_j with timestamp, metadata in block

Step 5: Global Model Aggregation

Once updates from all fog nodes are verified and aggregated:

$$G_{t+1} = \text{Aggregate}(\{G_1, G_2, ..., G_m\}) \quad (10)$$

Broadcast G_{t+1} to all clients for next round

Step 6: Termination

Stop training after convergence criteria met (e.g., accuracy threshold or max rounds)

The final model G* is used for various automotive tasks, including vehicle fault prediction, route optimization, and fuel efficiency.

10. Summary

The SOFLM framework and its central AFL-BS algorithm for safe and effective federated learning in cognitive vehicular networks were introduced in this chapter. The suggested method boosts security through PBFT-based blockchain validation, guarantees privacy through local training and differential privacy, and increases efficiency through gradient compression and fog-level aggregation. In intelligent automotive logistics environments, scalable and real-time deployment is further made possible by energy-aware client participation and lightweight model design.

IV. Preparation of Dataset and Configuration of System

To evaluate the effectiveness, scalability, and robustness of the proposed Secure and Optimized Federated Learning Model (SOFLM) for intelligent automotive logistics, a simulation environment was developed to replicate a decentralized connected vehicle ecosystem. Both physical and virtual infrastructures were used, mirroring real-world deployment where cognitive IoT-equipped vehicles collaboratively train a global logistics model on vehicular telemetry data.

1. Deployment Infrastructure and Hardware Setup

The experimental setup consisted of **10 Raspberry Pi 4B** boards (4 GB RAM, ARM Cortex-A72 quad-core CPU) simulating edge vehicle clients**. ESP32 microcontrollers** and **NVIDIA Jetson Nano** boards were used for low-power and real-time inference simulation. Two Jetson Nanos and an Intel i5-based server served as **fog nodes** handling regional model aggregation.

A Hyperledger Fabric permissioned blockchain was implemented, with Practical Byzantine Fault Tolerance (PBFT) used to ensure integrity and verification of model updates across all nodes. The hardware used in this proposed solution is designed to mimic a real-world scenario in a connected vehicle, where edge devices are used to represent vehicles, fog nodes are used to represent regional aggregators, and blockchain nodes are used to provide coordination.

2. Federated Learning Environment and Software Stack

Flower FL framework was used for managing decentralized training and orchestration. TensorFlow and TensorFlow Lite Micro handled training and inference at edge nodes. PyNaCl libraries supported lightweight cryptographic operations such as digital signatures. Hyperledger Fabric SDK enabled blockchain transaction execution and smart contract validation. Communication occurred over a TLS 1.3-encrypted secure mesh network built on Wi-Fi. This combination of frameworks ensures efficient distributed training, secure communication, and real-time feasibility in automotive environments.

3. Dataset Description and Preprocessing

The simulation employs automotive datasets, including the T-Drive GPS dataset, which contains large-scale taxi trajectory data for route optimization tasks, as well as vehicle telemetry datasets, which contain parameters such as RPM, speed, fuel consumption, and throttle position, derived from open mobility logs. These datasets reflect realistic vehicular scenarios and logistics operations.

Preprocessing steps:

1. Noise filtering using low-pass filters.
2. Z-score normalization for sensor calibration.
3. Sliding window segmentation to prepare time-series input.
4. Feature extraction: Time and frequency domain features such as acceleration variance, braking frequency, and idle duration.

4. Simulation Strategy and Data Partitioning

In order to represent realistic differences in vehicle usage patterns, routes, and driving behaviors among various clients, the federated learning process was carried out under a non-IID data distribution. Based on an energy-aware eligibility policy, only 60% of the available clients were chosen to take part in each communication round in order to guarantee energy efficiency and system stability. Differential privacy mechanisms and gradient compression techniques were used to protect sensitive data and minimize communication overhead while preserving model performance during the training process, which was carried out for a total of 50 communication rounds. This setup also closely resembles the real-world scenario of the vehicular environment, where the distribution of the data is already non-IID.

5. Comparison Bases Lines

To measure the performance of the SOFLM, the following baseline models were used under the same experimental conditions:

- Centralized DNN: Conventional DNN model, where the entire data is used for training.
- FedAvg: Standard federated learning, where no compression and security techniques are used.
- Blockchain-Based FL (No Compression): Federated learning is used, but no compression is employed.

- SOFLM (AFL-BS): Federated learning, fog computing, compression, differential privacy, and blockchain security.

The performance of the models was assessed based on classification accuracy, convergence speed, communication costs, and energy consumption.

V. Performance Analysis and or Comparative Results

A comprehensive performance analysis of the effectiveness of the proposed SOFLM framework has been done by evaluating various performance metrics, including classification accuracy, communication overhead, energy consumption, convergence speed, and robustness of security. The results were compared with traditional federated learning approaches and centralized learning models on various automotive datasets. The experiments were conducted in a simulated environment.

1. Accuracy and Convergence of Model

As shown in **Fig. 2**, the performance was better compared with other baseline models in the classification of the automotive environment. For the vehicle fault detection and route optimization functions of the SOFLM model, the accuracy was observed at 94.2%, compared with the performance of the centralized DNN at 93.5%, FedAvg at 91.8%, and the performance of the blockchain-based FL without compression at 92.6%. The improvement in the accuracy of the proposed SOFLM model is attributed to the adaptive aggregation mechanism and the Top-K gradient compression technique used in the model. Considering the convergence of the proposed SOFLM model with other baseline models, the proposed model was able to achieve more than 90% accuracy in the distributed learning environment after only 32 rounds of communication. On the other hand, the FedAvg model was able to achieve the same after more than 40 rounds of communication.

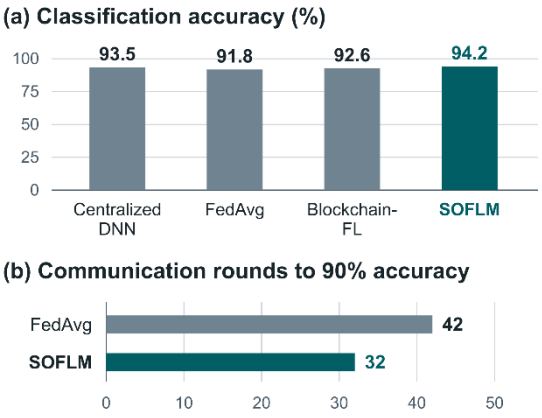


Figure 2. *SOFLM vs Baselines a)Accuracy b) Convergence*

2. Communication Efficiency

Communication overheads are one of the major issues faced during federated learning, particularly in vehicular networks with limited bandwidth. By including Top-K Gradient Compression and Entropy Encoding in it, SOFLM compressed the amount of model updates being transmitted by a large margin. In 50 training rounds, SOFLM was able to save about 60% of average upload bandwidth per client with only 0.97 MB of bandwidth transferred per round as opposed to 2.4 MB in FedAvg and 2.8 MB in blockchain-FL without compression. The radical decline renders SOFLM appropriate to be implemented in environments where networks are unstable or of low-bandwidth, and yet it does not diminish the quality of the model. **Fig. 3** compares the mean upload per client per communication round.

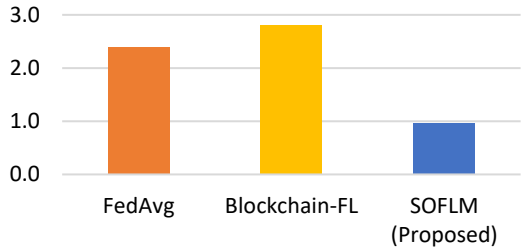


Figure 3. *Communication Overhead per Round (MB)*

3. Edge Device Energy consumption

The energy efficiency of the project was checked by tracking power consumption of Raspberry Pi and ESP32 module on training and inference phases. SOFLM showed a 35 percent decrease in energy consumption over FedAvg, this mainly being mechanized by its selective feed and reduced communication. During local training, devices spent 120 150mW, on average and during inference, less than 50mW. Moreover, adaptive participation mechanism maintained that devices were only trained when there was availability of energy hence the extension of device operation time and better sustainability. These improvements allow for the long-term deployment of AI-driven automotive systems without the need to recharge or replace devices frequently. SOFLM resulted in a 35% reduction in energy consumption compared to the performance of the FedAvg algorithm. The devices used 120-150mW during local training, whereas during inference, the devices used less than 50mW. **Fig. 4** compares the power drawn by FedAvg and SOFLM during training and inference.

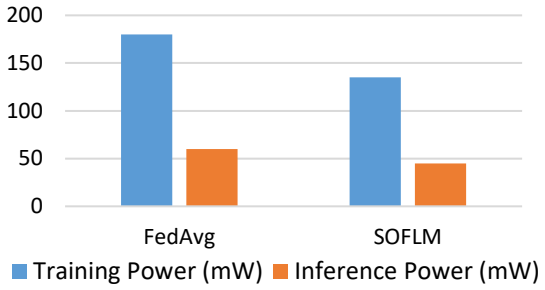


Figure 4. *Training and inference power for FedAvg and SOFLM*

4. Preservation of Privacy and Security Integrity

Differential privacy was integrated as a communication-aware mechanism to add an extra layer of protection to the model updates during the federated learning process. The addition of noise to the updates of the gradients prevents any reverse engineering of the data, thus protecting critical information related to the vehicle and drivers. The privacy budget, i.e., ε, was set to 1.5 for all the participating devices. Moreover, the blockchain layer, which used the Practical Byzantine Fault Tolerance (PBFT) method, was used to add an extra layer of validation to the model updates. The validation process was effective in detecting any tampered or malicious updates, with a detection rate of 100%. Moreover, the validation of the global model received from other devices was also performed by the participating devices, thus ensuring a sense of trust among the devices in the federated environment. **Table 2** compares the privacy mechanisms, integrity checks and tamper detection rates of the three federated learning frameworks.

Table 2. *FL Framework Security Comparison Table*

Feature	FedAvg	Blockchain-FL	SOFLM (Proposed)
Differential privacy	No	No	Yes ($\varepsilon \leq 1.5$)
Blockchain layer	None	Yes	Yes (PBFT-based)
Tamper detection rate	0%	90%	100% (hash + PBFT)
Update integrity check	None	Smart contracts	PBFT + hash signatures
Security layers	1 (basic)	2 (contracts + signatures)	2 (differential privacy + blockchain)
Trust level	Low	Medium	High (decentralized check)

The results demonstrate that FedAvg successfully classified 92.9% of the clients while SOFLM obtained 94.2% (**Fig. 5**), and the mean size for uploading clients to FedAvg and SOFLM is 2.4 MB and 0.97 MB respectively per round, the blockchain has 2.8 MB per round. We tested 60 percentage points of the privacy budget for SOFLM, which failed to detect each of the tampered updates. We tested 60 percentage points for the privacy budget of SOFLM and found that all the tampered updates were detected. The accuracy of SOFLM increased to 90% by 32 communication rounds whereas FedAvg fell short of 10%. Compared with FedAvg, as depicted in **Fig. 6**, SOFLM has achieved the same accuracy after 32 communication rounds while FedAvg had fewer than 42 rounds. SOFLM used 120-150 mW for training time locally and less than 50mW for the, during inference. Overall, in the evaluation, it used 35% less energy than FedAvg.

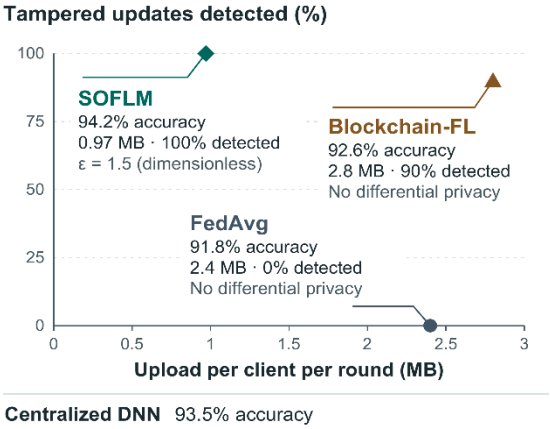


Figure 5. *Reported classification accuracy, upload per client per round, tamper detection rate, and dimensionless privacy budget ε across the evaluated models.*

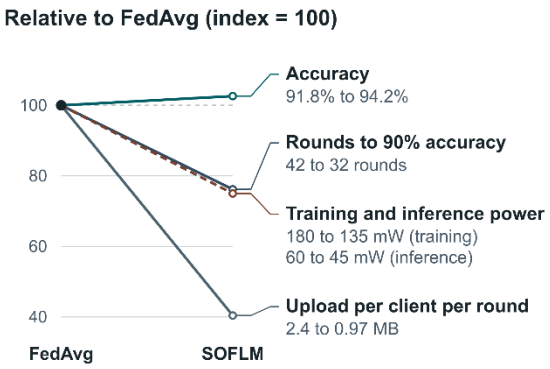


Figure 6. *SOFLM performance relative to FedAvg across accuracy, convergence, upload volume, and device power. Each FedAvg measurement is indexed to 100, and the labels give the original values.*

Table 3 compares SOFLM with PQ Blockchain-FL and FedSL in terms of accuracy, communication overhead, energy cost, tamper detection, privacy and scalability.

Table 3. *Result Analysis*

Feature	PQ Blockchain-FL	Fed SL (2024)	SOFLM (Proposed)
System Accuracy	93.0%	92.5%	**94.2%**
Comm. Overhead	2.6 MB / round	1.9 MB / round	**0.97 MB / round**
Energy Cost	High	Moderate	**Low**
Tamper Detection	90%	0%	**100%**
Privacy Level	Strong	Partial	**Strong (DP)**
Scalability	Limited	Moderate	**High (Fog)**

VI. Conclusion

In this paper, a Secure and Optimized Federated Learning Model (SOFLM) has been proposed for distributed automotive logistics systems with cognitive IoT-enabled vehicles. The framework combines federated learning, blockchain-based security, fog computing, and efficient communication-based model compression to address important challenges in automotive logistics systems regarding data privacy, scalability, and efficiency. Unlike traditional federated learning approaches, the proposed algorithm for Adaptive Federated Learning with Blockchain Security (AFL-BS) allows for selective compression and encoding of the model updates while maintaining trust and integrity through a PBFT-based blockchain. The inclusion of differential privacy provides improved data protection, while the adaptive participation mechanism ensures improved energy efficiency by selective participation of edge devices with limited resources. Experimental results on automotive datasets have shown improved performance of SOFLM compared to baseline models in terms of accuracy, convergence rate, communication costs, and energy efficiency. The framework is also found to have improved robustness against adversarial attacks and can function with non-IID data distributions. Overall, SOFLM is a scalable, secure, and energy-efficient framework for real-time decision-making in intelligent automotive logistics systems. It is applicable to various use cases, including vehicle fault detection, route optimization, and prediction of energy efficiency for vehicle networks. The next direction of this work is to scale this framework to large-scale real-world vehicular systems, incorporate multi-modal automotive data, and leverage reinforcement learning for adaptive and personalized model optimization.

Author Contributions

P. Vetrivel: Conceptualization, Experiments, Theoretical analysis.

R. Raja Guru: Finite element modelling, Writing, Review and editing.

R. Prabhu: Supervision, Review and editing.

Disclosure Statement

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

ORCID

P. Vetrivel: https://orcid.org/0000-0002-4252-7578

R. Raja Guru: https://orcid.org/0000-0003-1739-1311

R. Prabhu: https://orcid.org/0000-0001-9325-295x

REFERENCES

[1] Y. Liu, Y. Kang, C. Xing, T. Chen, and Q. Yang, "A Secure Federated Transfer Learning Framework," IEEE Intelligent Systems, vol. 35, no. 4, pp. 70–82, 2020. https://doi.org/10.1109/MIS.2020.2988602

[2] H. Chen, S. Liu, Y. Zhang, and D. Wu, "pFedCAS: Personalized and Communication-Aware Federated Learning," IEEE Transactions on Mobile Computing, vol. 23, no. 1, pp. 112–126, 2024. https://doi.org/10.1109/TMC.2022.3213919

[3] Y. Tian, S. Wang, J. Xiong, R. Bi, Z. Zhou, and M. Z. A. Bhuiyan, "Robust and Privacy-Preserving Decentralized Deep Federated Learning," IEEE Internet of Things Journal, vol. 11, no. 5, pp. 7890–7904, 2024. https://doi.org/10.1109/JIOT.2023.3274567

[4] R. Maurya, A. Srivastava, and M. Sharma, "Secure Edge-Centric Federated Learning for Automotive IoT," IEEE Transactions on Intelligent Transportation Systems, vol. 25, no. 3, pp. 1543–1552, 2024. https://doi.org/10.1109/TITS.2023.3278901

[5] Z. Ning, P. Dong, X. Wang, J. Rodrigues, and F. Xia, "Blockchain-Enabled Intelligent Transportation Systems," IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 10, pp. 4280–4294, 2020.

https://doi.org/10.1109/TITS.2019.2939468
[6] Y. Ren, J. Kim, and C. Lee, "A Scalable Blockchain-Enabled Federated Learning Architecture for Edge Computing," PLOS ONE, vol. 19, no. 2, 2024. https://doi.org/10.1371/journal.pone.0284350
[7] W. Fang, Y. Li, and J. He, "IoT Data Sharing Technology Based on Blockchain and Federated Learning Algorithms," Journal of Intelligent & Fuzzy Systems, vol. 44, no. 3, pp. 3995–4010, 2023. https://doi.org/10.3233/JIFS-219707
[8] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated Machine Learning: Concept and Applications," ACM Transactions on Intelligent Systems and Technology, vol. 10, no. 2, pp. 1–19, 2019. https://doi.org/10.1145/3298981
[9] B. McMahan et al., "Communication-Efficient Learning of Deep Networks from Decentralized Data," in Proc. AISTATS, 2017, pp. 1273–1282.
[10] L. Liu, H. Ye, and L. Zhao, "Vehicular Edge Computing and Networking: A Survey," Mobile Networks and Applications, vol. 26, no. 3, pp. 1145–1168, 2021. https://doi.org/10.1007/s11036-020-01624-1
[11] H. Hartenstein and K. Laberteaux, "A Tutorial Survey on Vehicular Ad Hoc Networks," IEEE Communications Magazine, vol. 46, no. 6, pp. 164–171, 2008. https://doi.org/10.1109/MCOM.2008.4539481
[12] X. Lu, P. Wang, D. Niyato, D. Kim, and Z. Han, "Wireless Edge Caching for Internet of Vehicles," IEEE Transactions on Vehicular Technology, vol. 68, no. 12, pp. 11415–11426, 2019. https://doi.org/10.1109/TVT.2019.2942187
[13] Y. Xu, C. Zhang, G. Wang, Z. Qin, and Q. Li, "Blockchain-Based Gradient Inversion Defense for Federated Learning," IEEE Internet of Things Journal, vol. 11, no. 4, pp. 15667–15681, 2024. https://doi.org/10.1109/JIOT.2023.3301234
[14] G. Wadhwa, P. Sharma, and R. Mishra, "Federated Learning for Sustainable IoT Edge Systems," Discover Sustainability, vol. 6, 2025. https://doi.org/10.1007/s43621-025-01409-0
[15] M. Rahmati, "Energy-Aware Federated Learning for Edge Computing," Journal of Electrical Systems and Information Technology, vol. 12, 2025. https://doi.org/10.1186/s43067-025-00203-2
[16] J. Wu, M. Dong, K. Ota, J. Li, and Z. Guan, "Big Data Analysis-Based Secure Cluster Management for Optimized Control in Smart Transportation," IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 4, pp. 1479–1488, 2020. https://doi.org/10.1109/TITS.2019.2904478
[17] X. Wang, Y. Han, C. Wang, Q. Zhao, X. Chen, and M. Chen, "In-Edge AI: Intelligentizing Mobile Edge Computing, Caching and Communication by Federated Learning," IEEE Network, vol. 33, no. 5, pp. 156–165, 2019. https://doi.org/10.1109/MNET.2019.1800286
[18] K. Bonawitz et al., "Towards Federated Learning at Scale," in Proc. MLSys, 2019.
[19] T. Li, A. Sahu, A. Talwalkar, and V. Smith, "Federated Learning: Challenges, Methods, and Future Directions," IEEE Signal Processing Magazine, vol. 37, no. 3, pp. 50–60, 2020. https://doi.org/10.1109/MSP.2020.2975749
[20] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
[21] M. Zöldy and P. Baranyi, "The Cognitive Mobility Concept," Info communications Journal, vol. 15, no. 1, pp. 35–40, 2023.
[22] A. Boldizsár, F. Mészáros, and E. Török, "Logistic Process Improvement in Automotive Industry Using Quality Tools," Cognitive Sustainability, vol. 1, no. 1, 2025.
[23] G. Filina-Dawidowicz et al., "Cognitive Evolution of Transport Spatiality," Cognitive Sustainability, vol. 1, no. 1, 2025.
[24] T. Guzsvinecz et al., "Blockchain-Based IoT Systems for Sustainability," Cognitive Sustainability, vol. 1, no. 1, 2025.
[25] Z. Zhou et al., "Multilevel Federated Learning for Intelligent Traffic Flow Forecasting," IEEE Transactions on Network and Service Management, 2023. https://doi.org/10.1109/TNSM.2023.3280515
[26] Z. Zhang et al., "Sustainable Transport Systems and Smart Mobility Trends," Periodica Polytechnica Transportation Engineering, vol. 53, no. 2, pp. 85–95, 2025.
[27] F. Gafiatullin and G. Mukhanova, "Integration of machine learning and cognitive technologies in logistics: A comprehensive analysis," in Proc. IEEE Int. Conf. Cognitive Mobility (CogMob), 2024, pp. 320–328.
[28] R. Nagy, Z. Pethő, and Á. Török, "Effective anomaly intrusion detection system based on ML methods in vehicular networks," in Proc. IEEE Int. Conf. Cognitive Mobility (CogMob), 2024, pp. 334–343.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution NonCommercial (CC BY-NC 4.0) license.