Blockchain-Driven Federated Learning for Advanced Vehicular Network Intelligence

***Abstract*—In the evolving landscape of vehicular networks, it is crucial to ensure robust security and efficient data handling. In this work, we introduce a novel federated learning (FL) algorithm, enhanced by an innovative blockchain consensus mechanism, tailored specifically for vehicular networks. Motivated by the pressing need for improved data privacy and security in the Internet of Vehicles (IoVs), our approach can not only prioritize these aspects but also enhance the efficiency and accuracy of distributed machine learning. The proposed consensus mechanism, by integrating Proof-of-Knowledge (PoK) with Practical Byzantine Fault Tolerance (PBFT), is crafted to be lightweight, making it suitable for the dynamic and resource-constrained vehicular environments. Our evaluation findings demonstrate the algorithm's superior performance and scalability, suggesting its applicability in diverse IoV scenarios and its potential to facilitate secure, robust, and efficient collaborative learning.**

***Index Terms*—Blockchain, Federated Learning, Consensus mechanism, Knowledge sharing, Internet of Vehicles, Data privacy and security**

I. Introduction

With the evolution of smart transportation systems, machine learning techniques powered by artificial intelligence (AI) have supported extensive applications in the realm of the Internet of Vehicles (IoVs) [1], [2]. Vehicles equipped with AI-driven onboard units and advanced sensors are increasingly inclined to disseminate data amongst themselves and with infrastructural elements. This data dissemination extends beyond mere computational, communicational, and spectral resources and encompasses the transfer of knowledge during the machine learning phase. Such knowledge transfer [3] enables a set of vehicles to share their learning insights, facilitating a faster learning curve and enhancing decision-making abilities. A practical instance of this can be seen when referring to the mutual sensing capabilities of vehicles, where the shared knowledge might pertain to acquire traffic flow patterns.

If a vehicle can utilize the data collected for individual model training, and then aggregate these individually trained models to derive a comprehensive model, it can hold a significant potential for knowledge sharing across the entire vehicular region. Such an approach would be of paramount importance for the future of intelligent transportation systems and traffic flow control [4], [5].

While knowledge sharing process offers numerous advantages, it also presents a myriad of challenges.

- **Security and Reliability:** Current vehicular systems cannot guarantee the security and reliability of knowledge data during the sharing process [6]. For example, malicious vehicles can compromise the knowledge sharing system by transmitting false knowledge or tampering with received models [7].
- **Privacy Concerns:** Due to the decentralized nature of vehicular networks, most vehicular networks may adopt distributed machine learning techniques during knowledge sharing [8]. This could lead to severe privacy concerns. During knowledge sharing, private information of vehicles, such as coordinates, driving preferences, owner details, and the datasets collected by the vehicle, could be at risk of exposure [9].

Blockchain technology offers a promising solution to the security challenges faced in vehicular knowledge sharing. As a distributed ledger, blockchain ensures that knowledge sharing between vehicles can be represented as transactions. These transactions are then audited and recorded by all peers in the network through a consensus process [10]. One of the defining features of blockchain is its immutability, which aids in maintaining the reliability of knowledge sharing [11]. In the context of vehicular networks, the high-speed movement of vehicles can lead to unstable connections [12].

Federated learning offers a solution to the issue of privacy breaches within the Internet of Vehicles (IoV) network. As an innovative distributed machine learning approach, federated learning enables all nodes to participate in the global model training in a distributed and collaborative manner. During the federated learning process, nodes are required to share only the trained models or model parameters with the server, rather than the entire datasets, thereby mitigating privacy risks and breaking down data silos [2]. In this study, due to the inability of a universal learning model to adapt to multiple regions with distinct business characteristics, traditional FL methods are not suitable for vehicular networks [13].

Identify applicable funding agency here. If none, delete this.

To address the aforementioned challenges, we propose a novel blockchain consensus mechanism that enhances the sharing of knowledge within the federated learning network, where knowledge is shared in the form of model parameters. FL-enabled vehicles, as users, collect data from their surroundings, train their models, and share this knowledge with the network, while blockchain ensures the security of the sharing process. The entire vehicular network is divided into several regions by Road-Side Units (RSUs), and federated learning is conducted within these regions. The consensus mechanism then disseminates the optimal model to all participants (FL vehicles). The proposed new consensus mechanism is adaptable to the varying characteristics of different traffic regions. The contributions of this paper can be summarized as follows:

- Unlike existing consensus mechanisms, we propose a new lightweight Proof-of-Knowledge (PoK) combined with the Practical Byzantine Fault Tolerance (PBFT) consensus mechanism. Compared to traditional consensus mechanisms, our approach significantly reduces computational consumption and is more suitable for dynamic vehicular scenarios. The advantage of PBFT is also leveraged to address the issue of cross-domain consensus among vehicles.
- With the integration of the new consensus mechanism, we made improvements to the federated learning algorithm. For the first time, accuracy is used as a reference standard, and compared to traditional federated learning algorithms, this algorithm shows a clear advantage in learning precision.

The paper structure includes a review of federated learning and blockchain in vehicular networks (Section II), a detailed methodology of our blockchain-based learning architecture and KEBA consensus mechanism (Section III), performance evaluation using MNIST and EMNIST datasets and scalability tests (Section IV), and a summary and future research directions (Section V).

II. Related Work

Federated Learning facilitates decentralized machine learning, with nodes jointly learning a predictive model while ensuring data remains private, thus effectively sharing knowledge [14]. It employs 'workers' for local training and 'servers' for aggregating updates, thereby boosting the learning accuracy. This approach pools varied data, enhancing model strength and data security, and reduces sensitive data exposure risks [15], [16]. FL is set to transform distributed machine learning training, offering a secure, scalable, and efficient method over conventional centralized techniques.

The integration of blockchain technology with federated learning in vehicular networks has been a subject of increasing interest in recent years. This section reviews some of the latest research in this area.In the field of blockchain in vehicular networks and federated learning, recent studies have made significant contributions. Lin et al. [17] proposed an adaptive blockchain-enabled Federated Learning (FL) framework for Intelligent Transportation Systems (ITS), addressing challenges like fixed parameters in vehicular blockchains and high communication costs in two-layer blockchain-based FL frameworks. Their design, which includes a streamline-based shard transmission mechanism and an adaptive sharding mechanism using Deep Reinforcement Learning, shows promise for efficient and scalable data interactions among intelligent vehicles.

Wang et al. [18] focused on the Wireless Computing Power Network (WCPN), proposing a secure and decentralized federated learning approach based on blockchain. Their design includes a blockchain with a proof-of-accuracy consensus scheme, which prioritizes high-accuracy local models for aggregation, thereby enhancing the efficiency and security of federated learning in WCPN. Boualouache et al. [19] introduced a secure and privacy-preserving on-demand framework for building Machine Learning attack detection models in 5G and Beyond (5GB) vehicular networks. Combining FL, blockchain, and smart contracts, their framework ensures fair and trusted interactions between FL servers and workers, with an efficient consensus algorithm and an intelligent incentive mechanism.Rajan et al. [20] presented a Blockchain-based Multi-Layer Federated Extreme Learning Machines (MLFEM) enabled Intrusion Detection System (IDS) for vehicular networks. Their approach leverages federated learning for generating multi-layered extreme learning machines, offloaded to vehicular edge devices, ensuring network security and efficient resource use.

Recently, Federated Learning algorithms have been seen a significant progress. Shen et al. [21] introduced DPFEDREP to address privacy leakage, achieving differential privacy and convergence in non-convex settings. Chen et al. [22] developed MOON, an algorithm that mitigates data heterogeneity and enhances learning accuracy and speed. Yang [23] analyzed techniques for improving FL communication efficiency, while Huang and Hu [24] presented FedMix, which adjusts federated learning for heterogeneous data, outperforming traditional algorithms in certain scenarios. These advancements underline the ongoing effort to refine FL algorithms for distributed environments.

III. METHODOLOGY

A blockchain-based federated learning architecture for knowledge sharing is depicted in Fig. 1, where vehicles are responsible for collecting environmental data from their vicinity, and Road-Side Units (RSUs) undertake the task of processing this data information. Federated learning is employed to construct a shared information model, thereby preserving the privacy of each participant. Meanwhile, blockchain serves as a distributed ledger, recording all collected data and thereby enhancing the security of the data.The definitions is shown in Table 1.

A. Blockchain Framework for Knowledge Sharing

1) Federated Learning Vehicle (FV): In Federated Learning, vehicles act as the primary workers, colloquially

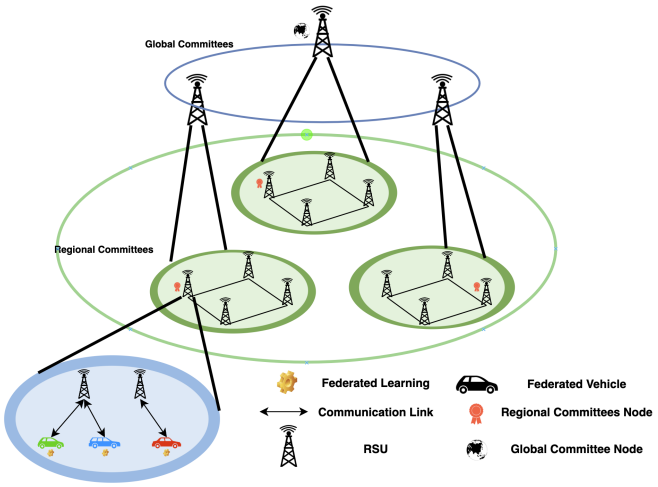


Fig. 1: Architecture for knowledge sharing

TABLE I: Notations and their descriptions

Notation	Description
D_n	Datasets of the surrounding environment collected by FV
Acc_n	Accuracy of FV after local training
P_n	Model parameters after FV local training
WA_{FV_n}	Wallet address for FV vehicles
WA_{RSU_m}	Wallet address for RSU
Sig_n	Signature of FV
Sig_m	Signature of RSU
$tx_{n,m}$	Transactions passed from FV to RSU
$tx^{\gamma}_{m,n}$	Transactions after RSU validation passes
$Cost$	Specific loss function chosen
θ	threshold parameter defines acceptable model performance
agg_param	Parameters of the aggregator
fv_param	parameters of FV

referred to as Federated Vehicles. Their main task involves collecting environmental data surrounding their vehicle to serve as the training set for FL. The learned model parameters are then transmitted to nearby RSUs in the form of transactions. Upon successful transactions, FVs receive a certain number of rewards. The specific workflow is as follows: FVs collect data from around their vehicle, receive the latest version of model parameters from RSUs, engage in federated learning using the collected data, trade the learned model parameters with RSUs, and upon verification, FVs are rewarded with tokens. Subsequently, they continue to collect data, accept the latest model, and prepare for the next transaction.

2) Road Side Unit (RSU):Road-Side Unit are critical nodes within the federated learning architecture of this vehicular framework. They are not tasked with collecting surrounding data but are responsible for receiving data transmitted by nearby FVs. RSUs are equipped with built-in test sets and federated learning model parameters; the built-in dataset serves to verify the authenticity of the data during transactions with FVs, checking for any potential data falsification. Given that RSUs typically possess superior computational capabilities compared to FVs, are stationary, and have more reliable transmission signals, they are chosen as the mining nodes in this structure. The specific workflow for RSUs is as follows: they distribute the latest model parameters to nearby FVs, receive transactions from nearby FVs, use the built-in dataset to validate these transactions, and upon successful validation, the transactions enter a pool awaiting packaging. Subsequently, RSUs issue rewards to the corresponding FVs.

3) Regional and Global Node Committees: Our architecture utilizes a dual-layer committee system, comprising Regional and Global Node Committees, to enhance network integrity and efficiency. Regional Committees are tasked with local transaction validation and data sharing, reducing latency and bolstering security against malicious threats within specific geographic zones. The overarching Global Node Committee ensures adherence to network protocols during the consensus process, maintaining rule compliance across regional divisions. This two-tiered structure ensures the network is scalable, responsive, and robust, catering to the dynamic nature of vehicular networks.

B. Federated Transaction Process

Federated Vehicles, denoted as FV_n, are responsible for gathering environmental data to form a dataset D_n. Upon completion of the Federated Learning (FL) process, FV_n compiles the learned model parameters P_n, along with the locally computed accuracy Acc_n, into a transaction. In this context, FV_n constructs a transaction that encapsulates P_n, Acc_n, and the signature of FV_n, denoted as Sign_{FV_n}. Consequently, the structure of the learning transaction generated by FV_n can be formally represented as follows:

$$tx^{t}_{n,m} = \{WA_{FV_n} \parallel P_n, Acc_n \parallel 0 \parallel WA_{RSU_m} \parallel Sig_n\} \tag{1}$$

where WA_{FV_n}, WA_{RSU_m} denotes the wallet addresses of the FV and RSU. The term P_n represents the model parameters, while Acc_n indicates the accuracy level obtained post-local federated learning within FV_n. A value of 0 signifies that the transaction has not passed the RSU's verification and is therefore not yet eligible for entry into the transaction pool. The signature Sig_n is the digital endorsement by the FV, authenticating the transaction in question.

Upon receipt of the transaction, referred to as $tx^{t}_{n,m}$, the RSU commences a procedure to verify the transaction's validity. Subsequent to this verification, the RSU is tasked with generating a new transaction, the specifics of which are delineated below.

$$tx^{v}_{m,n} = \{WA_{RSU_m} \parallel P_n, Acc_n \parallel 1 \parallel WA_{FV_n} \parallel Sig_m\} \tag{2}$$

A value of 1 indicates that the transaction has passed the RSU verification process. The RSU signature, represented by Sig_m , is affixed to the transaction as evidence of this validation. Following the successful authentication, the RSU will proceed to deposit the transaction, denoted as $tx^v_{m,n}$, into the transaction pool.

C. Knowledge-Ensured Byzantine Agreement Consensus Mechanism (KEBA)

During each global iteration of the federated learning process, the RSUs within regional committees can collect model parameters from the transactions of nearby vehicles, subsequently training the model, and then the global committees elect the model with the highest accuracy to be distributed back to the various Federated Vehicles (FVs) for the next round of iteration. In our framework, the collection of local models is executed by the consensus process.

Utilizing popular consensus mechanisms such as Proof of Work (PoW) for knowledge sharing can either lead to a significant waste of computational resources or introduce additional consensus delays, both of which are detrimental for high-speed vehicular environments. To address this issue, we introduce a new consensus mechanism named Knowledge-Ensured Byzantine Agreement (KEBA), which amalgamates the features of Proof of Knowledge (PoK) [2] and Practical Byzantine Fault Tolerance (PBFT), taking into account the computational efforts of the federated learning process within the structure.

The PoK integrates machine learning with blockchain consensus, replacing complex hashing puzzles with the learning process [25], thereby enhancing the efficiency of energy utilization. KEBA maintains network integrity even in the presence of underperforming or malicious nodes, as PBFT can tolerate a certain proportion of node failures. Unlike conventional PBFT, KEBA allows nodes to participate in the consensus based on the quality of data they contribute, enabling more nodes to join the network without compromising security, thus improving the system's scalability. We will describe this in four steps as below.

1) Collecting and Verifying Transactions: Each RSU continuously gathers transactions $tx^t_{n,m}$ from the surrounding FVs, which include the model parameters P_n and accuracy Acc_n post federated learning. This step is crucial to prevent the propagation of false knowledge by FVs, which could compromise the integrity of the entire federated learning structure. To ensure the authenticity of the knowledge, RSUs initially test the model parameters using a pre-stored test set $\{(x, y)\}$. The validation outcome is determined through a loss function, expressed as:

$$Loss^R = Cost(f_{P_n}(x) - y) \tag{3}$$

where $Cost()$ denotes the specific loss function chosen, such as Cross-Entropy Loss or Mean Squared Error (MSE). Here, f_{P_n} represents the model inference using parameters received from the FV.

$$|L^R - Acc_n| \leq \theta. \tag{4}$$

Where Acc_n represents the accuracy metric as reported by the FV, and θ is a threshold parameter established by human-determined to delineate the bounds of acceptable model performance.If the L^R falls within a certain acceptable range, it is deemed reliable. Following the validation process, the RSU transforms the transaction into a verified transaction $tx^v_{m,n}$ and subsequently packages it into the transaction pool.The format of candidate block is shown in fig.2.

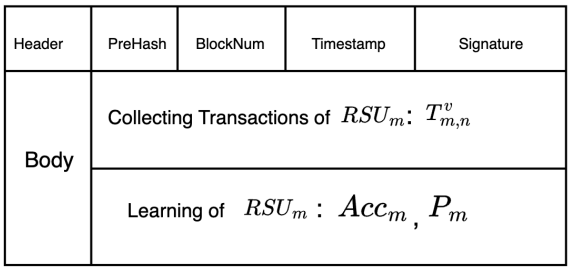


Fig. 2: Format of candidate block

2) Consensus Process: In the dynamic and distributed context of the Internet of Vehicles (IoV), traditional centralized data processing methods confront challenges of inefficiency and insufficient reliability. To address these issues, our proposed consensus mechanism includes a structure based on regional and global committee architecture. This mechanism initially forms regional committees among RSUs that are geographically proximate. Each committee is composed of $3n + 1$ RSUs, where n represents the number of fault-tolerant nodes. This structure allows the system to efficiently manage data exchange and consensus processes within local areas, thereby reducing dependence on central processing points. Such an architecture also ensures the scalability of the blockchain.
Within these regional committees, we use an accuracy-based method to elect representative nodes. Specifically, the RSU providing the highest accuracy data is chosen as the regional representative node. As a testament to the knowledge learned, learning precision is indicative of the RSU's contribution to the global model. This approach not only guarantees the quality and reliability of the data but is also crucial for maintaining the integrity and trustworthiness of data throughout the entire network.
Furthermore, representative nodes from each region can form a global committee, tasked with consensus decision-making on a wider scale. This design aids in maintaining consistency and synchronization across a larger network area, enhancing the scalability and flexibility of the entire system.

In terms of transaction processing, our mechanism ranks transactions based on accuracy Acc_n and assigns the packaging responsibility to RSU nodes elected by the global nodes. This not only improves processing efficiency but also ensures the quality of data transmitted across the network. Moreover, the optimal model parameters can be disseminated to all participating nodes via broadcasting or uploaded to the blockchain for FVs to download. This completes a round of global consensus, followed by the commencement of a new learning cycle. This method not only facilitates the sharing of knowledge and resources, but also increases the system's transparency and traceability.

D. Security Performance

This section delves into the security performance of our proposed system, focusing on its resilience against various types of cyber attacks. We evaluate the system's robustness against integrity attacks, double spending attacks, dishonest behaviors, Sybil attacks, and the notorious 51% attacks. Each type of attack is analyzed in the context of our system's unique consensus mechanisms. These mechanisms collectively enhance the security of our federated learning-based blockchain framework, ensuring data integrity, preventing fraudulent activities, and maintaining network stability even in the presence of potential threats.

1) Integrity Attack: In an integrity attack, data tampering is mitigated by the Proof of Knowledge (PoK) mechanism, which deters attackers by requiring high-accuracy data for consensus participation. Practical Byzantine Fault Tolerance (PBFT) further ensures data consistency through its comprehensive verification process, securing data integrity against compromised nodes as long as a majority remains honest.
2) Double Spending Attack: In digital currency systems, the double spending attack, where the same asset is used multiple times, is thwarted in the KEBA mechanism. Here, each transaction must pass through federated learning accuracy verification and PBFT nodes' confirmation, ensuring once a transaction is verified by one node, it's broadcast for additional validation, effectively preventing fund reuse.
3) Dishonest Behaviours: This includes providing false data, denial of service, etc. In the PoK mechanism, low-quality data from dishonest nodes will not be used for consensus, thus diminishing their influence. The PBFT mechanism requires agreement from more than two-thirds of the nodes to confirm a transaction, reducing the impact of a minority of dishonest nodes.
4) Sybil Attack: The KEBA mechanism counters Sybil attacks, where attackers use fake identities to influence networks, by basing consensus on data quality, not node quantity. This makes sustaining multiple high-quality false identities impractical. Additionally, PBFT's multi-node verification further impedes attackers' ability to influence consensus, reinforcing network security against such attacks.
5) 51% Attack: The KEBA mechanism mitigates the risk of a 51% attack, common in PoW blockchain systems, by basing consensus on data quality rather than computational power. This shift reduces the impact of singular computational dominance on consensus, diminishing the likelihood of such attacks. PBFT's multi-stage consensus process further reinforces defense against 51% attacks.

E. Weighted Accuracy Average Updating Federated Learning (Fed_WAAvg)

In the advanced federated learning algorithm tailored for a multi-server knowledge-sharing architecture, the workflow is methodically structured as follows:

Step 1. Data Collection and Local Training by FVs: Local FVs are tasked with the continuous collection of environmental data, a critical component in the federated learning process. Post the data collection phase, these vehicles engage in the local training. The culmination of this phase is the uploading of the resultant model parameters and the associated accuracy metrics to the RSUs. This upload is executed in the form of structured transactions, ensuring systematic data management and traceability.

Step 2. Data Verification by RSUs: Upon receiving the data, RSUs perform a crucial verification process. This step involves a thorough examination of the data's accuracy, ensuring that only high-quality information is integrated into the system. Transactions that successfully meet the accuracy criteria are then incorporated into the transaction pool, each endorsed with the RSU's signature. This signature is a mark of data authenticity and validation within the system.

Step 3. Handling of Non-Verified Transactions: Transactions that do not pass the verification process are not immediately discarded. Instead, they may be considered for analysis in a prospective reputation system. This system, aimed at enhancing the network's security, would evaluate such transactions to identify and mitigate potential threats or attacks on the system. The implementation of such a system would contribute to the overall robustness and reliability of the federated learning framework, ensuring a secure and efficient knowledge-sharing environment.

Step 4. The algorithm proceeds to calculate the overall accuracy and determine the relative contribution weight of each FV within the RSU. This calculation involves a systematic process as outlined below:

1) Weight Computation for Each FV: The algorithm iterates over each federated vehicle data vector collected by the RSU. The weight for each federated vehicle is computed by dividing the accuracy of the FV by the total accuracy. This step ensures that each federated vehicle's contribution is proportionally represented in the final model.
2) Aggregated Parameter Update: The algorithm then enters a phase of parameter aggregation. For each pair of aggregated parameters and model parameters of the

federated vehicle , the algorithm iterates to perform the update. In each iteration, the aggregated parameter is recalculated by adding the product of the federated vehicle's model parameter and its computed weight to the existing aggregated parameter. This process effectively combines the contributions of all federated vehicles into a cohesive set of model parameters.

3) Model Parameter Update in RSUs: Upon completion of the iteration process, the Roadside Unit updates its model parameters to reflect the newly aggregated parameters. This update signifies the integration of individual contributions from each federated vehicle, culminating in a refined and collective model that embodies the shared knowledge and insights of the entire network.

Algorithm 1 Weighted Accuracy Average Updating Federated Learning

Each RSU Server Aggregation:
initialize agg_param
total_acc = sum(rsu.fvs_acc)
for each fv in rsu.fvs **do**
  weight = fv_acc / total_acc
  for each (agg_param, fv_param) in zip(agg_params, fv.model_params) **do**
    Update agg_param=agg_param + weight $\times$ fv_param
  end for
end for
Update rsu.model_params as agg_params
Return agg_params
FV executes:
(get param from global node)
$D_s \leftarrow$ fv collects surrounding data as local training set
for each local epoch **do**
  for each $B \in D_s$ epoch **do**
    learning model
    Update model fv_param, fv_acc
  end for
end for
Return fv_param, fv_acc to rsu

IV. PERFORMANCE EVALUATION

In this section, we aim to conduct a comparative analysis of the newly proposed federated learning algorithm, focusing on its accuracy and loss metrics. This evaluation will be carried out on two public datasets: MNIST and EMNIST. Additionally, we will explore the scalability of the Fed_WAAvg algorithm through a set of experiments. This comprehensive assessment aims to validate the effectiveness and robustness of our proposed algorithm in diverse scenarios, providing insights into its practical applicability and potential for broader implementation in federated learning environments.

A. Dataset

For the algorithm evaluation, we conducted assessments on two real-world datasets that are extensively utilized in data classification tasks. The first dataset is MNIST, a classic benchmark in the field of machine learning and computer vision. It comprises 60,000 training examples and 10,000 test examples, each being a 28x28 pixel grayscale image of handwritten digits from 0 to 9. This dataset is renowned for its simplicity and is often used as an introductory dataset for algorithm testing in image recognition tasks.

The second dataset–Extended MNIST (EMNIST)–enhances MNIST by including a wider array of handwritten characters, encompassing both digits and letters. This expansion increases data complexity, making EMNIST ideal for testing machine learning algorithms on more diverse and challenging classification tasks. Using EMNIST helps assess the robustness and adaptability of our federated learning algorithm in handling various data types.

TABLE II: The configuration of PC

Name	**Detail**
CPU	Intel(R) Xeon(R) CPU @ 2.20GHz
Memory	12.67GB
GPU	Tesla T4-PCIE-15GB
Operating System	Ubuntu 22.04.2 LTS
Python Environment	3.10.12
Development Framework	Pytorch

B. Experimental Settings

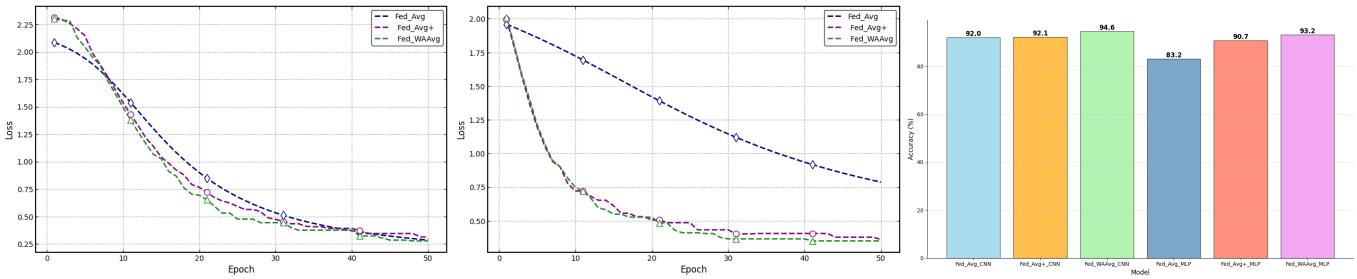
In this work, Fed_WAAvg, Fed_Avg+, Fed_Avg was trained by using the Pytorch deep learning framework. The Fed_Avg+ algorithm is based on the Fed_Avg algorithm, which is improved for the data sharing framework. The learning rate was set to 0.003, beta1=0.9, beta2=0.999. The model was trained for 50 epochs. The experimental equipment has GPU support. The specific hardware configuration of a node is summarized in Table II.

C. Accuracy Results

In Figure 3a, the CNN-based network showcases the loss function trajectories for various federated learning algorithms. The Fed_Avg algorithm provides a consistent benchmark, while Fed_Avg+ indicates a trend towards faster convergence. The Fed_WAAvg algorithm stands out with its rapid decrease in loss, evidencing an advanced aggregation strategy that may substantially bolster learning efficiency.

Figure 3b reflects a similar trend in the MLP-based network, with Fed_WAAvg demonstrating a pronounced and swift reduction in loss. This suggests its potential superiority in handling the intricacies of MLP structures.

Figure 3c then compares the learning accuracies, where Fed_WAAvg's performance supersedes the others in both network types. Specifically, for the CNN model, Fed_WAAvg's accuracy peaks at accuracy 94.6%, outperforming Fed_Avg and Fed_Avg+ by 2.6% and 2.5%, respectively. For the MLP model, it reaches 93.2% accuracy, which is a significant 10%



(a) Loss Function of CNN-based Network (b) Loss Function of MLP-based Network (c) Learning Accuracy

Fig. 3: Learning performance of MNIST dataset.

and 2.5% improvement over Fed_Avg and Fed_Avg+, respectively. These figures underscore the efficacy of Fed_WAAvg's weighted averaging in federated learning environments, confirming its capability to enhance model performance markedly.

Figures 4a and 4b present an intriguing scenario where the Fed_Avg algorithm, expectedly the baseline, reports lower loss values than the Fed_WAAvg for the CNN and MLP networks on the EMNIST dataset. This anomaly could be attributed to a myriad of factors such as the Fed_Avg's simpler mechanism fortuitously matching the dataset's profile, or a hyperparameter configuration that is more suited to the characteristics of the EMNIST dataset. Conversely, the sophistication of Fed_WAAvg with its weight adjustments might not be conducive to the specific distribution of the EMNIST data, highlighting the complexity of federated learning systems and the necessity for tailored algorithm configurations.

Figure 4c contrasts the learning accuracies, with the CNN model, showing a slight decrease in accuracy using Fed_WAAvg at 74.7% compared to Fed_Avg at 75.3%. Meanwhile, the MLP model's accuracy under Fed_WAAvg is 71.2%, significantly trailing Fed_Avg's 79.3% while substantially outperforming Fed_Avg+'s 61.1%. These figures highlight the nuanced effects that different federated learning algorithms can have on varying model architectures.

D. Scalability experiments

The figures present a study on the scalability of federated learning systems using a CNN model on the MNIST dataset, with a focus on the loss and accuracy as the number of FVs and RSUs varies. The notation "fv_x_rsu_y" represents the experimental setup with 'x' number of FVs and 'y' RSUs. The results indicate that systems with more RSUs, particularly fv_40_rsu_20 and fv_50_rsu_20, demonstrate lower loss and improved accuracy, highlighting effective scalability. Even as the number of participating nodes increases, the system upholds strong learning performance, showcasing its capacity to manage larger federated learning environments without compromising on the learning efficacy. This suggests that the proposed federated learning framework is well-equipped to handle growth in network size, making it a robust solution for large-scale distributed learning applications.

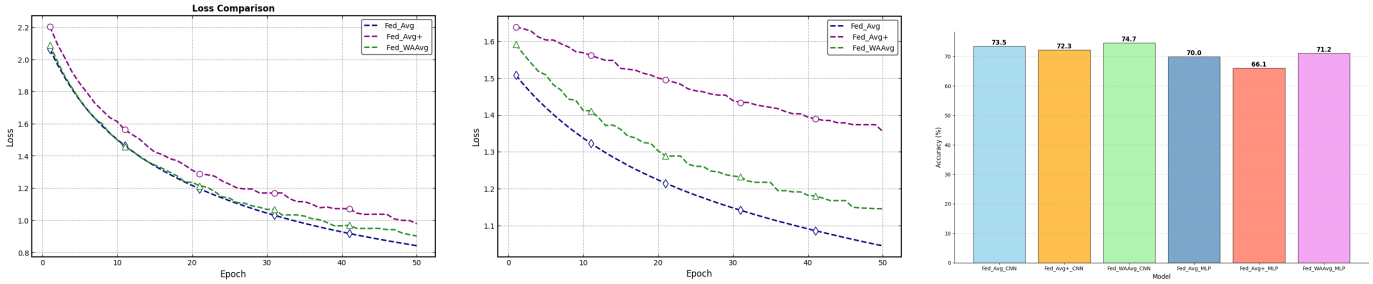
The presented figures offer a clear insight into the scalability of the federated learning system deployed on the MNIST dataset. Despite the variations in the number of vehicles and RSUs, the system exhibits a strong ability to maintain efficient learning, as evidenced by the sustained reduction in loss and improvement in accuracy. The data suggests that the system architecture can effectively accommodate an increasing number of nodes without significant degradation in performance, showcasing its well-designed scalability features. The trends affirm that the system can handle growth in the federated network, making it a viable solution for expansive and diverse real-world applications.

E. Comprehensive analysis of the KEBA consensus mechanism

The KEBA consensus mechanism presents a unique and innovative approach in the blockchain domain, distinguishing itself from traditional mechanisms like PoW and PoS. Unlike PoW, which relies on energy-intensive computational tasks and often leads to centralization due to the dominance of entities with greater computational resources, KEBA emphasizes model accuracy in federated learning as the basis for consensus. This not only aligns the network's objectives with performance improvements but also fosters a collaborative environment incentivizing high-quality data and model contributions. In contrast to PoS, known for its energy efficiency but criticized for potential wealth concentration and security concerns like the 'nothing at stake' problem, KEBA offers a more balanced solution. It combines the energy efficiency of PoS with a meritocratic governance model, where influence is based on contributions to model accuracy rather than wealth or computational power. Additionally, the integration of PBFT enhances network security against Byzantine faults, ensuring resilience even in the presence of malicious or failing nodes. This dual focus on model performance and fault tolerance addresses several limitations of PoW and PoS, such as high energy consumption, centralization, and security vulnerabilities, making KEBA a compelling alternative for blockchain networks, especially those integrated with AI and machine learning functionalities.

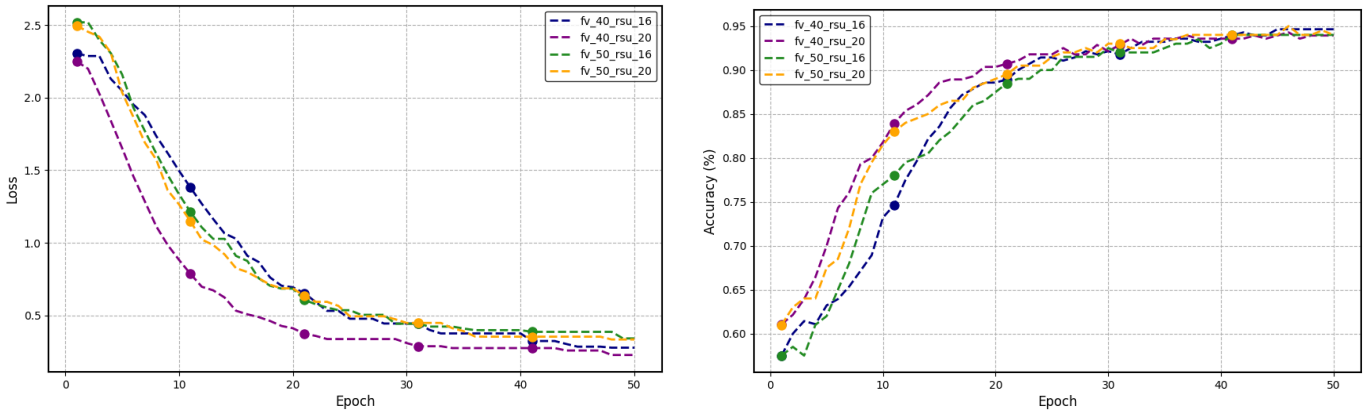
Building further on this foundation, KEBA refines its advantages when compared individually to PBFT and PoK. PBFT, while robust against Byzantine faults and offering a high degree of fault tolerance, faces scalability challenges in larger networks due to intensive communication overhead.

7



(a) EMNIST Loss Function of CNN Network (b) EMNIST Loss Function of MLP Network (c) EMNIST Learning Accuracy

Fig. 4: Learning performance of EMNIST dataset.



(a) MNIST Scalability of Loss Function (b) MNIST Scalability of Accuracy

Fig. 5: Scalability experiments for MNIST dataset.

KEBA addresses this by integrating the PoK aspect, which emphasizes the quality of contributions in a federated learning context. This integration not only enhances scalability but also aligns the network's incentives with the improvement of the federated model's accuracy.

On the other hand, PoK as a standalone consensus mechanism, while innovative in its approach to valuing knowledge contribution, might lack the robust security features necessary for a decentralized network. By combining PoK with PBFT, the KEBA mechanism inherits the security strengths of PBFT, ensuring network resilience against malicious activities while still promoting a knowledge-driven environment. This synergy creates a more balanced and secure framework, where contributions towards the federated model's accuracy are crucial, but not at the expense of network security and stability. Thus, KEBA emerges as a holistic approach, addressing the limitations of both PBFT and PoK when used independently, and making it particularly suitable for blockchain networks that heavily rely on data integrity and model accuracy.

V. CONCLUSION AND FUTURE WORKS

The research conducted provides compelling evidence that the newly proposed federated learning algorithm, coupled with a robust consensus mechanism, significantly advances the state-of-the-art in knowledge sharing within vehicular networks. The integration of PoK with PBFT within the FL framework offers a dual enhancement—fortifying the security of distributed learning while concurrently optimizing learning outcomes. The performance on benchmark datasets showcases an improvement in learning efficiency and model accuracy, affirming the algorithm's capability to adeptly manage a spectrum of network sizes and complexities.

Our future work could include exploring more intricate blockchain consensus mechanisms and expanding the application of federated learning algorithm to a larger and more diverse dataset. It also includes enhancing the algorithm's adaptability under different vehicular network scenarios and the integration of emerging technologies for further optimization.

REFERENCES

[1] W. Y. B. Lim, J. Huang, Z. Xiong, J. Kang, D. Niyato, X.-S. Hua, C. Leung, and C. Miao, "Towards federated learning in uav-enabled internet of vehicles: A multi-dimensional contract-matching approach," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 5140–5154, 2021.

[2] H. Chai, S. Leng, Y. Chen, and K. Zhang, "A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 3975–3986, 2020.

[3] E. S. Ali, M. K. Hasan, R. Hassan, R. A. Saeed, M. B. Hassan, S. Islam, N. S. Nafi, and S. Bevinakoppa, "Machine learning technologies for secure vehicular communication in internet of vehicles: recent advances

and applications," *Security and Communication Networks*, vol. 2021, pp. 1–23, 2021.

[4] B. Sliwa, T. Liebig, T. Vranken, M. Schreckenberg, and C. Wietfeld, "System-of-systems modeling, analysis and optimization of hybrid vehicular traffic," in *2019 IEEE International Systems Conference (SysCon)*. IEEE, 2019, pp. 1–8.

[5] C.-H. Lin, Y.-C. Lin, Y.-J. Wu, W.-H. Chung, and T.-S. Lee, "A survey on deep learning-based vehicular communication applications," *Journal of Signal Processing Systems*, vol. 93, pp. 369–388, 2021.

[6] T. Zhang and Q. Zhu, "Distributed privacy-preserving collaborative intrusion detection systems for vanets," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 148–161, 2018.

[7] H. Chai, S. Leng, Y. Chen, and K. Zhang, "A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 3975–3986, 2021.

[8] G. Raja, S. Anbalagan, G. Vijayaraghavan, S. Theerthagiri, S. V. Suryanarayan, and X.-W. Wu, "Sp-cids: Secure and private collaborative ids for vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4385–4393, 2021.

[9] T. Zhang and Q. Zhu, "Differentially private collaborative intrusion detection systems for vanets," *arXiv preprint arXiv:2005.00703*, 2020.

[10] N. Malik, P. Nanda, A. Arora, X. He, and D. Puthal, "Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 2018, pp. 674–679.

[11] U. Divakarala, K. Chandrasekaran, and K. H. K. Reddy, "A hierarchical blockchain architecture for secure data sharing for vehicular networks," *International Journal of Information Technology*, vol. 15, no. 3, pp. 1689–1697, 2023.

[12] Z. Ma, F. R. Yu, X. Jiang, and A. Boukerche, "Trustworthy traffic information sharing secured via blockchain in vanets," in *Proceedings of the 10th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, 2020, pp. 33–40.

[13] X. Zhou, W. Liang, J. She, Z. Yan, I. Kevin, and K. Wang, "Two-layer federated learning with heterogeneous model aggregation for 6g supported internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 5308–5317, 2021.

[14] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Artificial intelligence and statistics*. PMLR, 2017, pp. 1273–1282.

[15] R. Gosselin, L. Vieu, F. Loukil, and A. Benoit, "Privacy and security in federated learning: A survey," *Applied Sciences*, vol. 12, no. 19, p. 9901, 2022.

[16] T. Wittkopp and A. Acker, "Decentralized federated learning preserves model and data privacy," in *International Conference on Service-Oriented Computing*. Springer, 2020, pp. 176–187.

[17] Y. Lin, Z. Gao, H. Du, J. Kang, D. Niyato, Q. Wang, J. Ruan, and S. Wan, "Drl-based adaptive sharding for blockchain-based federated learning," *IEEE Transactions on Communications*, 2023.

[18] P. Wang, W. Sun, H. Zhang, W. Ma, and Y. Zhang, "Distributed and secure federated learning for wireless computing power networks," *IEEE Transactions on Vehicular Technology*, 2023.

[19] A. Boualouache, B. Brik, S.-M. Senouci, and T. Engel, "On-demand security framework for 5gb vehicular networks," *IEEE Internet of Things Magazine*, vol. 6, no. 2, pp. 26–31, 2023.

[20] D. Rajan, P. Eswaran, G. Srivastava, K. Ramana, and C. Iwendi, "Blockchain-based multi-layered federated extreme learning networks in connected vehicles," *Expert Systems*, vol. 40, no. 6, p. e13222, 2023.

[21] Z. Shen, J. Ye, A. Kang, H. Hassani, and R. Shokri, "Share your representation only: Guaranteed improvement of the privacy-utility tradeoff in federated learning," *arXiv preprint arXiv:2309.05505*, 2023.

[22] S. Chen, Z. Lin, and J. Ma, "The effect of hyper-parameters in model-contrastive federated learning algorithm," in *2023 IEEE International Conference on Sensors, Electronics and Computer Engineering (ICSECE)*. IEEE, 2023, pp. 1170–1174.

[23] Y. Yang, "The improvement of federated learning in communication efficiency," *Highlights in Science, Engineering and Technology*, vol. 34, pp. 183–190, 2023.

[24] Y. Huang and C. Hu, "Toward data heterogeneity of federated learning," *arXiv preprint arXiv:2212.08944*, 2022.

[25] C. H. Liu, Q. Lin, and S. Wen, "Blockchain-enabled data collection and sharing for industrial iot with deep reinforcement learning," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3516–3526, 2018.