Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.055557

ARTICLE

Blockchain-Enabled Federated Learning with Differential Privacy for Internet of Vehicles

Chi Cui[1,2], Haiping Du[2], Zhijuan Jia[1,*], Yuchu He[1] and Lipeng Wang[1]

[1]School of Information Science and Technology, Zhengzhou Normal University, Zhengzhou, 450044, China

[2]School of Electrical, Computer and Telecommunications Engineering, University of Wollongong, Wollongong, NSW 2500, Australia

*Corresponding Author: Zhijuan Jia. Email: jzj523@163.com

Received: 01 July 2024 Accepted: 14 September 2024 Published: 15 October 2024

ABSTRACT

The rapid evolution of artificial intelligence (AI) technologies has significantly propelled the advancement of the Internet of Vehicles (IoV). With AI support, represented by machine learning technology, vehicles gain the capability to make intelligent decisions. As a distributed learning paradigm, federated learning (FL) has emerged as a preferred solution in IoV. Compared to traditional centralized machine learning, FL reduces communication overhead and improves privacy protection. Despite these benefits, FL still faces some security and privacy concerns, such as poisoning attacks and inference attacks, prompting exploration into blockchain integration to enhance its security posture. This paper introduces a novel blockchain-enabled federated learning (BCFL) scheme with differential privacy (DP) tailored for IoV. In order to meet the performance demanding IoV environment, the proposed methodology integrates a consortium blockchain with Practical Byzantine Fault Tolerance (PBFT) consensus, which offers superior efficiency over the conventional public blockchains. In addition, the proposed approach utilizes the Differentially Private Stochastic Gradient Descent (DP-SGD) algorithm in the local training process of FL for enhanced privacy protection. Experiment results indicate that the integration of blockchain elevates the security level of FL in that the proposed approach effectively safeguards FL against poisoning attacks. On the other hand, the additional overhead associated with blockchain integration is also limited to a moderate level to meet the efficiency criteria of IoV. Furthermore, by incorporating DP, the proposed approach is shown to have the (ε-δ) privacy guarantee while maintaining an acceptable level of model accuracy. This enhancement effectively mitigates the threat of inference attacks on private information.

KEYWORDS

Blockchain; federated learning; differential privacy; Internet of Vehicles

1 Introduction

The rapid advancement of artificial intelligence (AI) in recent years has significantly propelled the evolution of the Internet of Vehicles (IoV). AI technologies, particularly machine learning, have empowered vehicles to make intelligent decisions. On the other hand, the computation-intensive nature of machine learning technology poses challenges for its application in IoV, given the limited on-board

resources of vehicles. The conventional approach to machine learning is centralized, where all local data is transmitted to a central server for model training [1]. Applying this centralized architecture to IoV introduces several issues. Firstly, the central server may struggle to cope with the massive volume of data, forming a potential performance bottleneck. Secondly, the transmission of substantial data volumes results in high network overhead, a concern exacerbated by the dynamic network environment of IoV. Thirdly, local vehicle data may encompass sensitive information, including locations and driving behaviors, raising privacy concerns in the presence of a malicious central server or unauthorized network access. Lastly, the central server is susceptible to a single point of failure, posing a risk of system breakdown.

Federated learning (FL) [2], introduced by Google teams in 2016, has emerged as a viable alternative to traditional centralized learning to address the aforementioned challenges. In FL, model training takes place in a distributed manner. In each training round, FL participants conduct local training using their own datasets, yielding updated model parameters. These parameters are then transmitted to the central server for the aggregation of a global model, which is subsequently shared with participants for the next training round. This approach ensures that only model parameters traverse the network, significantly alleviating network strain and enhancing privacy protection.

Nevertheless, FL is not without its challenges. The centralization issue persists in model aggregation, leaving the performance bottleneck problem unresolved [3]. Additionally, FL participants may exhibit malicious behaviors, potentially initiating poisoning attacks to compromise the model [4]. Furthermore, FL does not completely eliminate privacy threats, as inference attacks, where privacy information can be reconstructed even from the transmitted model parameters, still cause privacy leakage [5].

As a consequence, blockchain, as a secure and decentralized ledger, is increasingly recognized as a viable solution to enhance the security and performance of FL. The inherently distributed nature of blockchain aligns seamlessly with FL, facilitating their integration. By substituting the aggregation server, blockchain introduces complete decentralization to the model aggregation process. The cryptographic techniques inherent in blockchain enhance resistance against security threats such as poisoning attacks. Given these merits, blockchain-enabled FL (BCFL) has attracted growing attention from researchers.

In this paper, we introduce an innovative BCFL approach tailored for IoV. Our proposed method employs a consortium blockchain with the Practical Byzantine Fault Tolerance (PBFT) consensus mechanism. This implementation significantly mitigates the performance issues commonly associated with conventional public blockchains, making our approach more suitable for the IoV environment. Moreover, we incorporate differential privacy (DP) in the proposed BCFL scheme, which provides enhanced protection against inference attacks on privacy information. Experiment results demonstrate that our proposed approach effectively elevates the security and privacy standards of FL, concurrently meeting the demanding efficiency criteria of the IoV environment.

The remainder of this paper is structured as follows: Section 2 provides an overview of the current state-of-the-art research and related works in this field. Section 3 presents a detailed description of the architecture and key features of the proposed BCFL scheme. Section 4 offers a comprehensive analysis of the experimental results, examining both security and performance aspects of the proposed system. Section 5 concludes the paper by summarizing the key findings and outlining our plans for future research in this area.

2 Related Works

Several studies have explored the integration of blockchain and FL, with varying degrees of coupling between the two. Some studies [6] employ a fully-coupled architecture, where blockchain participants simultaneously act as FL participants. While this design is relatively straightforward to implement, it requires intensive computation on the participants, given that both blockchain and FL are demanding in computation power. As a result, fully-coupled architecture may be time and resource consuming. To address this challenge, some other works have adopted a loosely-coupled architecture, separating mining nodes from training nodes [7,8]. Despite requiring additional coordination, this approach can effectively alleviate communication latency, since blockchain and FL work on separate networks. Furthermore, this design requires fewer computational resources on individual nodes and demonstrates improved overall performance. As a result, the majority of existing BCFL research for the IoV favors a loosely-coupled architecture. This preference stems from the suitability of such designs for IoV scenarios, where onboard resources in vehicles are inherently limited.

In the realm of blockchains, the performance and security level vary with the blockchain types and consensus protocols. Pioneering BCFL studies have explored traditional public blockchains utilizing the Proof-of-Work (PoW) consensus protocols, known for providing a high level of trust without centralized trust management. For instance, a BCFL scheme for autonomous vehicles using PoW is proposed in [9]. However, PoW's energy and time-consuming nature renders it inefficient for vehicle-related applications. To enhance BCFL performance, other blockchain architectures with revised consensus protocols have been introduced. Some works leverage consensus protocols replacing computationally intensive hash puzzles with FL tasks, thereby reducing unnecessary computations. For example, the authors in [10] introduce a novel consensus protocol called Proof-of-Federated Learning (PoFL). In this protocol, the node that completes the FL training task most swiftly earns the right to generate a new block. Similarly, some other knowledge-based consensus mechanisms, including Proof-of-Knowledge (PoK) [11] and Proof-of-Accuracy (PoA) [12], decide the winning node based on local model accuracies. Compared with PoW, these modified consensus protocols offer enhanced efficiency. However, their applicability is restricted to fully-coupled BCFL architectures. This limitation stems from the fact that participants in the consensus process must concurrently serve as FL participants in order to execute such consensus protocols effectively.

Given those public blockchains operate in an untrusted environment, extensive computations are essential for security. Consequently, certain works turn to consortium blockchains to enhance trust among participants, as a predetermined group of participants manages the consensus process. The more trusted environment in consortium blockchains allows for the use of more efficient consensus protocols. Many works adopting consortium blockchains leverage voting-based Practical Byzantine Fault Tolerance (PBFT) consensus [13,14] or Delegated Byzantine Fault Tolerance (DBFT) consensus [15]. In these voting-based consensus protocols, the network is supposed to know the identities of consensus nodes [16]. This characteristic makes such protocols particularly well-suited for implementation in consortium blockchains.

To further enhance efficiency, some works explore the integration of Directed Acyclic Graph (DAG)-based blockchains with FL [17–19]. DAG is a graph-based lightweight blockchain structure that allows multiple transactions to be processed simultaneously, making it significantly more efficient and scalable than conventional linear blockchains. Despite the fact that DAG-based blockchains are highly efficient, their security levels are generally perceived as inferior to those of traditional linear blockchains, especially in their early adoption [17].

Regarding the threat of inference attacks in federated learning (FL), many existing works incorporate additional cryptographic methods for protection. For instance, the authors in [13] propose the use of homomorphic encryption (HE) during model aggregation. HE enables the manipulation of encrypted data while preserving its confidentiality. However, HE operations are computationally intensive and time-consuming, which poses challenges for their practical implementation in real-world scenarios. Another approach is DP [20], which is performed by adding a controlled amount of noise to model parameters. Numerous studies [21,22] have investigated various approaches to implement DP in FL contexts, seeking to balance privacy guarantees with model performance and efficiency. These efforts have contributed significantly to advancing privacy-preserving machine learning methodologies in distributed environments. Generally, DP offers greater efficiency compared to HE. On the other hand, DP's introduction of noise may potentially compromise model accuracy. To achieve optimal results, careful fine-tuning of hyperparameters is necessary. This process involves striking a balance between privacy protection and maintaining the model's predictive performance.

While integrating blockchain with FL offers significant advantages, it also presents notable challenges. The consensus process in blockchain systems requires substantial communication and computational efforts among network nodes, thus introducing additional operational overhead. Consequently, this leads to increased latency and elevated resource consumption. When BCFL is deployed in IoV, the resource-constraint and highly dynamic environment further accentuates these challenges. Firstly, low network latency and high throughput are required. In addition, BCFL must demonstrate efficient scalability to accommodate the increasing number of vehicles and participants. This scalability ensures the system's responsiveness and effectiveness as both the network size and data volume expand [23]. To effectively address these challenges with IoV, it is crucial to minimize the additional overhead introduced by BCFL schemes. This optimization necessitates further refinement of existing algorithms to achieve an improved balance between security and efficiency. A promising direction towards this goal involves implementing a consortium blockchain-enabled FL scheme that utilizes a loosely-coupled architecture. Furthermore, the integration of DP is essential to enhance the scheme's resilience against inference attacks, thereby fortifying the overall security of the system.

3 Methodology

In the BCFL approach that we propose, blockchain is employed to store model information. By housing all local model information on the blockchain, global model aggregation can be performed by mining nodes with access to the blockchain, thereby replacing the central aggregation server. The proposed scheme utilizes a loosely-coupled structure, wherein the blockchain and FL nodes are separated. In our scheme, the road-side units (RSUs) act as the mining nodes, responsible for maintaining the blockchain, while the vehicles are tasked with local training. Each vehicle is associated with an RSU. By operating blockchain and FL on distinct networks, a reduction in communication latency and the computational resources required by a single node can be anticipated.

In general, the proposed BCFL scheme operates as follows:

(1) Initialization: The initial global model is broadcasted to each participating RSU and subsequently to its associated vehicles.

(2) Local Training: Upon receiving the global model, the vehicle conducts local training with its own data to obtain its local model. Subsequently, it transmits the local model to its associated RSU upon completing training.

(3) Consensus: Upon receiving a local model, the RSU communicates with other RSUs for validation and consensus. After that, the leader node in the PBFT consensus generates a new block containing the local model parameters and appends it to the blockchain.

(4) Global Model Aggregation: The RSU accesses the entire blockchain and aggregates a global model from all the local models present in the blockchain. Following this, the RSU broadcasts the global model to all its associated vehicles that are available for the next local training.

(5) Iteration: Steps (2) to (4) are iterated until convergence or the maximum number of iterations is reached.

The architecture of the proposed BCFL scheme is illustrated in Fig. 1. Some specific features of the proposed scheme are discussed in more detail in the following subsections.

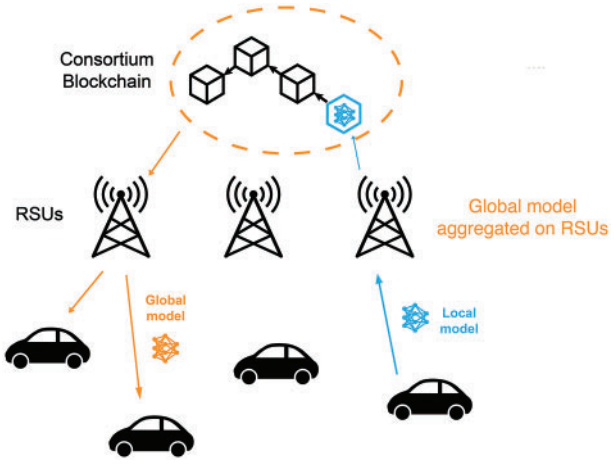

Figure 1: Architecture of the proposed BCFL scheme

3.1 Consortium Blockchain with PBFT Consensus

Blockchains offer significant potential for enhancing IoV security by ensuring trust in an untrusted environment. However, this advantage comes with a cost, as trust establishment among blockchain nodes relies on running consensus protocols, introducing additional overhead in terms of time and energy costs. This poses a challenge when applied in the resource-constrained IoV environment. Consequently, adopting a blockchain architecture and consensus protocol that minimizes this extra overhead while maintaining a reasonable security level is crucial.

Traditional public blockchains are fully decentralized and open to anyone. While they provide high security, they sacrifice efficiency and scalability. To balance the trade-off between security and efficiency, sacrificing some decentralization and accessibility for better performance is a potential direction. Thus, in the proposed BCFL scheme, we utilize a consortium blockchain with the PBFT consensus protocol.

Unlike public blockchains, consortium blockchains are permissioned and maintained by a group of trusted nodes. In the proposed approach, only RSUs act as participating nodes in the blockchain, as RSUs are relatively fixed and more trusted than vehicles. When an RSU attempts to add a new block containing a received local model, the PBFT consensus protocol is executed. PBFT is a voting-based consensus protocol that tolerates Byzantine faults. In a blockchain with $3f + 1$ participating nodes, where f represents the number of fault nodes, consensus can be reached with $2f + 1$ benign nodes.

In PBFT, a node is selected as the leader in each consensus process, and other nodes are replicas. The leader is responsible for generating and appending new blocks to the blockchain. In the proposed scheme, when an RSU receives a local model, it sends the model to the leader node. The consensus procedure of PBFT is then executed, divided into three phases:

(1) Pre-Prepare Phase: The leader node validates the model and broadcasts a *PrePrepare* message, denoted by $< PrePrepare, v, n, h, m, s >$, to all replica nodes, where v denotes the view number, n denotes the sequence number, h denotes the hash of the proposed block, m denotes the proposed block data, and s denotes the signature. After receiving the *PrePrepare* message, a replica node verifies the message and broadcasts a *Prepare* message $< Prepare, v, n, h, s >$, which stands for its approval of the request.

(2) Prepare Phase: After a node collects $2f + 1$ *Prepare* messages and verifies them, it broadcasts a *Commit* message $< Commit, v, n, h, s >$.

(3) Commit Phase: After a node collects $2f + 1$ *Commit* messages and verifies them, a consensus is reached.

This comprehensive three-phase validation procedure ensures consensus nodes must reach agreement at multiple stages. Benign nodes can identify and disregard any inconsistent or invalid messages, thereby enhancing the system's integrity. Under this mechanism, a new block is appended to the blockchain only when more than two-thirds of the consensus nodes concur. Consequently, this approach effectively neutralizes the potential impact of a small number of malicious or faulty nodes through the collective decision-making process.

To further enhance security, the proposed scheme integrates asymmetric encryption using the Elliptic Curve Digital Signature Algorithm (ECDSA) with a consortium blockchain. In this approach, a vehicle signs a locally trained model using a unique signing key. The signed model is then transmitted to a corresponding RSU, where the model gets verified using a corresponding verifying key before entering the PBFT consensus process. This digital signature mechanism significantly enhances data integrity and authenticity. Additionally, privacy is fortified as potential intruders cannot access model parameters without possessing the requisite verifying key. This multi-layered security approach effectively safeguards the FL process in vehicular networks.

3.2 Differentially Private FL

DP is a mechanism that maintains individual privacy when analyzing data by introducing noise into the data or the analysis process, which obscures individual contributions while preserving overall statistical accuracy. In our work, the Differentially Private Stochastic Gradient Descent (DP-SGD) algorithm [24] is applied in the local training process to achieve differentially private FL to further mitigate the threat of inference attacks. The DP-SGD algorithm begins with gradient clipping, which is a crucial step in limiting the influence of any single training sample on the model updates. For each sample in a minibatch, the algorithm computes the gradient and clips its $L2$ norm to a maximum threshold C. The gradient clipping is represented by Eqs. (1) and (2).

$$g_t(x_i, y_i) = \nabla_{\theta_t}\left(\ell\left(\theta; x_i, y_i\right)\right) \tag{1}$$

$$\hat{g}_t(x_i, y_i) = \frac{g_t(x_i, y_i)}{\max\left(1, \frac{\|g_t(x_i, y_i)\|_2}{C}\right)} \tag{2}$$

In the equations above, $\ell(\theta)$ is the loss function where θ is the model, $g_t(x_i, y_i)$ and $\hat{g}_t(x_i, y_i)$ represent the gradient and the clipped gradient, respectively. By setting a threshold C for the $L2$ norm of gradients, the algorithm ensures that no individual data point can exert a disproportionate influence on the learning process. A smaller value of C results in a more aggressive clipping of gradients, and introduces a larger bias into the gradient estimates, as more gradients are substantially modified. It also necessitates the addition of more noise to maintain the same level of privacy protection.

After gradient clipping, the algorithm then adds elaborated Gaussian noise to the average gradient before updating the model, which is shown in Eq. (3).

$$g_t = \frac{1}{B}\left(\sum_i \hat{g}_t(x_i, y_i) + N\left(0, \sigma^2 C^2 I\right)\right) \tag{3}$$

where B represents the batch size and $N\left(0, \sigma^2 C^2 I\right)$ represents the Gaussian noise, in which 0 is the mean, $\sigma^2 C^2$ is the variance, and I is the identity matrix.

Finally, the local model is updated by Eq. (4), where θ_t represents the model parameters at step t and η is the learning rate.

$$\theta_t = \theta_{t-1} - \eta \tilde{g}_t \tag{4}$$

In this way, DP is realized on each local model, which presents inference attacks from adversaries. The privacy budget of DP, denoted by ε, is given by Eq. (5).

$$\varepsilon = \frac{\sqrt{2\log\frac{1.25}{\delta}}}{\sigma} \tag{5}$$

where δ is a very small probability that the privacy guarantee does not hold and σ is the noise multiplier. Therefore, a higher value of σ corresponds to a smaller privacy budget, indicating stronger privacy protection. However, as shown in Eq. (3), a larger σ leads to increased noise, which can result in reduced model accuracy. As a result, a major challenge in DP is to minimize the impact on model accuracy while maintaining an adequate privacy budget. This balance is typically achieved through careful hyperparameter tuning, which is the approach we adopt in this study.

4 Experiments and Analysis

We perform experiments to test the security and performance of the proposed scheme. In this section, firstly the settings of the experiments are introduced. Then the results of the experiments are discussed in detail.

4.1 Experiment Settings

The experiment program is coded using Python 3.9 with PyTorch and runs on a group of computer nodes that act as vehicles or RSUs to simulate the IoV environment. In the experiments, there are 10 nodes acting as vehicles, which are candidates in FL, and 7 nodes acting as RSUs, which are participating nodes of the consortium blockchain. In each global epoch, 6 out of the 10 vehicles are randomly selected as FL participants. On each participating vehicle, the local training is performed 5 epochs with DP-SGD before the vehicle uploads its local model parameters. The global model aggregation is performed over 50 epochs on RSU nodes using the FedAvg (Federated Averaging) algorithm [2] from the local models stored on the blockchain.

Since the proposed scheme is supposed to be applied in the IoV environment, we use the German Traffic Sign Recognition Benchmark (GTSRB) dataset for model training and evaluation in FL. The dataset contains 43 classes in traffic signs with 39,209 training images and 12,630 testing images. To further increase the size and diversity of the dataset, data augmentation is performed before training by adjusting the brightness, contrast, saturation, etc., of the training images and then appending the processed images to the dataset. After data augmentation, the total number of training images becomes 266,400 and each vehicle possesses 26,640 training samples. For the FL process, the ResNet (Residual Networks)-50 model is adopted as the initial model.

4.2 Security Analysis

The primary security threats associated with FL involve poisoning attacks and inference attacks. In this section, we discuss the resilience of the proposed approach to these two security threats with both theoretical analysis and experiment proof.

4.2.1 Poisoning Attacks

In poisoning attacks, adversaries intentionally contaminate the training data by injecting manipulated samples with crafted perturbations to deceive the model into making erroneous predictions. This threat is particularly concerning in FL, where training occurs in a distributed manner, making it easier for a malicious node to train its local model using poisoned data [4]. Fortunately, the introduction of blockchain offers significant mitigation against poisoning attacks. The resistance to poisoning attacks in the proposed BCFL scheme stems from the following aspects:

(1) Immutability of the Blockchain: The immutability of data is a fundamental characteristic of the blockchain. Once data is added to the blockchain, it becomes unalterable and immune to deletion. This immutability is intrinsic to the structure of the blockchain, where each block contains the Merkle root—a hash of the block data—and the hash of its preceding block. Consequently, any attempt to modify the block data results in hash value mismatches in subsequent blocks, promptly revealing any data tampering. This feature makes it impossible for a malicious node to perform model poisoning towards model information on the blockchain.

(2) Data Validation: Before being appended to the blockchain, the new block containing local model parameters undergoes a validation process, serving as a mechanism to detect poisoning attacks. In our approach, the accuracies of local models are assessed using a testing dataset stored on the RSUs during the data validation phase. In each training round, the accuracies of local models are compared with a threshold, which is determined by the average accuracy of the models trained with benign datasets. For each epoch, the RSU keeps a different threshold since the accuracies in early epochs are obviously lower. If a local model received has its accuracy below the threshold, the RSU will reject the model from being appended to the blockchain.

To evaluate the robustness of the proposed scheme, we conducted experiments by initiating poisoning attacks using the PA-PSOSA (Poisoning Attack Using Hybrid Particle Swarm Optimization with Simulated Annealing) method described in our previous work [25]. In the experiments, one of the participating vehicles in the federated learning (FL) system was designated as malicious and performed a poisoning attack on its own training data. The results of these experiments are presented in Fig. 2. After 50 epochs of FL, the global model's classification accuracy, in the absence of any poisoning attacks, converges to approximately 97%. When the poisoning attack is introduced into the conventional FL system, the accuracy significantly declines to around 85%. However, when the same attack is initiated on the proposed BCFL system, the model accuracy initially stays around 92%

in the early epochs and then converges to approximately 95% as the FL process continues beyond 30 epochs. These results demonstrate that the data validation performed by RSUs can effectively enhance the integrity of the global model aggregation by filtering out poisoned local models. In fact, among all the poisoned local models generated over 50 epochs, only those from the first two epochs evaded detection. This is because the local model accuracies at the initial stage are generally low and gaps in accuracies between benign and malicious models are not obvious, making it challenging to distinguish poisoned models. These findings demonstrate that the proposed BCFL approach effectively mitigates the impact of poisoning attacks on local training, highlighting its robustness against such malicious activities.

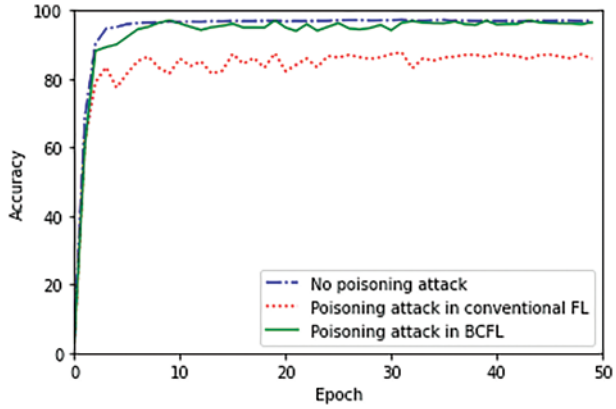

Figure 2: Experimental results on resistance to poisoning attacks

4.2.2 Inference Attacks

Inference attacks occur when adversaries attempt to deduce private training data from local model parameters. The proposed scheme significantly mitigates this threat by incorporating DP-SGD into the local model training process, as detailed in Section 3.2. However, it is crucial to maintain a balance between privacy protection and model performance. With an appropriate privacy budget, the model's utility should be preserved, ensuring that accuracy does not suffer excessively. To evaluate the impact of DP on model accuracy and find the most suitable hyperparameters, we conducted a series of experiments. The experimental result with the highest global model accuracies with DP-SGD is shown in Fig. 3.

From Fig. 3, we can observe that the global model accuracy of BCFL without DP is approximately 97%. Upon the introduction of DP, the model's accuracy initially drops significantly. However, as training progresses, the accuracy gradually improves, ultimately stabilizing at around 91%. This final accuracy demonstrates that the model retains a substantial degree of utility despite the introduction of Gaussian noise. To obtain the results in Fig. 3, the maximum $L2$ norm of gradients has been set to 10, and the noise multiplier σ is set to 0.2. To ensure the (ε-δ) privacy guarantee for each individual step of the SGD process, the value of δ should be set to less than $1/n$, where n is the number of training samples on each vehicle. In this experimental setup, each vehicle contains 26,640 training images. Consequently, the value of δ can be appropriately set to 0.00003. With these parameters established, the privacy budget ε can be calculated using Eq. (5) as presented in Section 3.2. In this case, the value of ε is 23.06, which represents a moderate level of privacy protection. The results suggest that while there is

a modest trade-off between privacy and performance, the DP-enhanced BCFL model still maintains a high level of accuracy, effectively balancing privacy protection and model effectiveness.

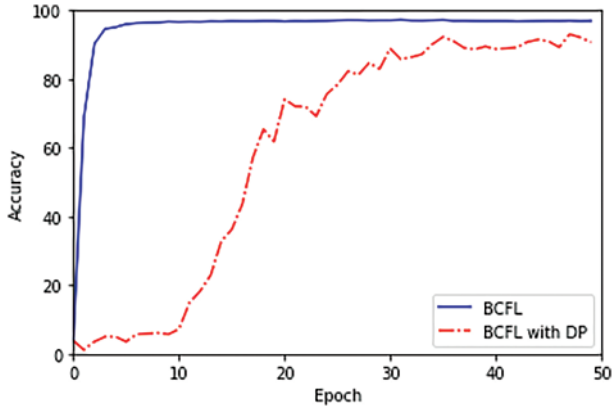

Figure 3: Experimental results on global model accuracy under BCFL with DP

4.3 System Efficiency

While integrating blockchain technology into FL enhances security, it inevitably incurs additional computational costs and reduces overall system efficiency. The consortium blockchain with PBFT consensus is utilized to address the trade-off between security and performance. It offers significantly improved efficiency compared to traditional public blockchains employing PoW consensus.

To evaluate the performance of different FL implementations, experiments were conducted under the settings described in Section 4.1. The study compared the overall running times per epoch for three FL schemes: conventional FL, BCFL with PoW consensus, and the proposed BCFL with PBFT consensus. The results are presented in Fig. 4.

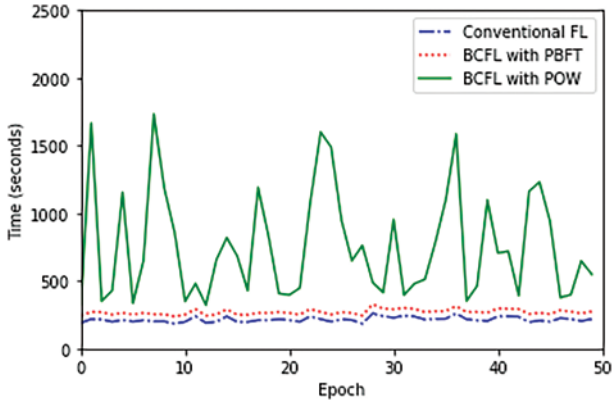

Figure 4: Experimental results showing system operation time

In each round of local model training, the running time for the conventional FL is 209.76 s in average, and the average running time of the proposed BCFL with PBFT consensus scheme is 263.59 s, which still maintains acceptable performance levels under a variety of scenarios. In contrast, BCFL with PoW consensus mechanism exhibits a significantly longer execution time, primarily due to its

computationally intensive mining process. Furthermore, the operation time of the PoW is highly variable, depending on how quickly a mining node can solve the complex hash problem. In the experiment, this duration ranges from approximately 330 to 1800 s. The experiment result suggests that BCFL with PoW can barely meet the requirements of the demanding IoV environment. On the other hand, the proposed BCFL scheme leveraging PBFT consensus involves fewer complex computations compared to PoW-based BCFL. Consequently, it offers superior efficiency while maintaining robust security measures, striking a favorable balance between performance and security enhancements.

5 Conclusion

In this paper, we present the architecture of a novel BCFL scheme designed for IoV. Our proposed BCFL scheme seamlessly integrates a consortium blockchain with FL, aiming to ensure a high-security level while simultaneously enhancing efficiency to meet the demanding requirements of the IoV environment. Experimental results demonstrate that the proposed BCFL scheme effectively protects the global model from poisoning attacks, significantly enhancing the security level of FL. Compared to traditional public blockchains using PoW. the additional overhead incurred by integrating the consortium blockchain with PBFT consensus is acceptable and more suitable for the IoV environment. Furthermore, the implementation of differential privacy enhances privacy protection, with experimental results suggesting an acceptable balance between privacy safeguards and model utility. As part of our future work, we plan to further conduct experiments in a real IoV environment. Subsequent improvements will be made based on the results obtained from experiments from real-life scenarios.

Acknowledgement: We extend our sincere gratitude to all colleagues and research assistants at the Institute of Software Science of Zhengzhou Normal University, for their invaluable assistance and support throughout this research.

Funding Statement: This work was supported in part by the Natural Science Foundation of Henan Province (Grant No. 202300410510), the Consulting Research Project of Chinese Academy of Engineering (Grant No. 2020YNZH7), the Key Scientific Research Project of Colleges and Universities in Henan Province (Grant Nos. 23A520043 and 23B520010), the International Science and Technology Cooperation Project of Henan Province (Grant No. 232102521004), the National Key Research and Development Program of China (Grant No. 2020YFB1005404), and the Henan Provincial Science and Technology Research Project (Grant No. 212102210100).

Author Contributions: The authors confirm contribution to the paper as follows: study conception: Haiping Du; algorithm design: Chi Cui, Zhijuan Jia; data collection: Lipeng Wang; coding of experiment programs and analysis of results: Chi Cui, Yuchu He; draft manuscript preparation: Chi Cui. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: This work uses the GTSRB dataset for the model training and evaluation in FL. The dataset can be downloaded from the Internet.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Liu, J. Tang, Z. Zhang, and J. -L. Gaudiot, "Computer architectures for autonomous driving," *Computer*, vol. 50, no. 8, pp. 18–25, Aug. 2017. doi: 10.1109/MC.2017.3001256.

[2] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Arcas, "Communication-efficient learning of deep networks from decentralized data," in *20th Int. Conf. Artif. Intell. Stat., Ft*, Lauderdale, FL, USA, Apr. 20–22, 2017, pp. 1273–1282.

[3] D. C. Nguyen *et al.*, "Federated learning meets blockchain in edge computing: Opportunities and challenges," *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12806–12825, Apr. 2021. doi: 10.1109/JIOT.2021.3072611.

[4] M. Fang, X. Cao, J. Jia, and N. Gong, "Local model poisoning attacks to byzantine-robust federated learning," in *29th USENIX Secur. Symp.*, Boston, MA, USA, Aug. 12–14, 2020, pp. 1605–1622.

[5] C. Ma *et al.*, "On safeguarding privacy and security in the framework of federated learning," *IEEE Netw.*, vol. 34, no. 4, pp. 242–248, Mar. 2020. doi: 10.1109/MNET.001.1900506.

[6] M. Shayan, C. Fung, C. J. Yoon, and I. Beschastnikh, "Biscotti: A blockchain system for private and secure federated learning," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 7, pp. 1513–1525, Dec. 2020. doi: 10.1109/TPDS.2020.3044223.

[7] H. Kim, J. Park, M. Bennis, and S. -L. Kim, "Blockchained on-device federated learning," *IEEE Commun. Lett.*, vol. 24, no. 6, pp. 1279–1283, Jun. 2019. doi: 10.1109/LCOMM.2019.2921755.

[8] Y. Zhao *et al.*, "Privacy-preserving blockchain-based federated learning for IoT devices," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 1817–1829, Aug. 2020. doi: 10.1109/JIOT.2020.3017377.

[9] S. R. Pokhrel and J. Choi, "Federated learning with blockchain for autonomous vehicles: Analysis and design challenges," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 4734–4746, Apr. 2020. doi: 10.1109/TCOMM.2020.2990686.

[10] F. Ayaz, Z. Sheng, D. Tian, and Y. L. Guan, "A blockchain based federated learning for message dissemination in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 2, pp. 1927–1940, Dec. 2021. doi: 10.1109/TVT.2021.3132226.

[11] H. Chai, S. Leng, Y. Chen, and K. Zhang, "A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 3975–3986, Jun. 2020. doi: 10.1109/TITS.2020.3002712.

[12] H. Liu *et al.*, "Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 6073–6084, Apr. 2021. doi: 10.1109/TVT.2021.3076780.

[13] N. Wang *et al.*, "A blockchain based privacy-preserving federated learning scheme for Internet of Vehicles," *Digit. Commun. Netw.*, vol. 10, no. 1, pp. 126–134, Feb. 2024. doi: 10.1016/j.dcan.2022.05.020.

[14] S. Otoum, I. Al Ridhawi, and H. T. Mouftah, "Blockchain-supported federated learning for trustworthy vehicular networks," in *2020 IEEE Global Commun. Conf.*, Taipei, Taiwan, Dec. 8–10, 2020, pp. 1–6.

[15] Y. Qi, M. S. Hossain, J. Nie, and X. Li, "Privacy-preserving blockchain-based federated learning for traffic flow prediction," *Future Gener. Comput. Syst.*, vol. 117, pp. 328–337, Apr. 2021. doi: 10.1016/j.future.2020.12.003.

[16] Z. Zheng, S. Xie, H. -N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Serv.*, vol. 14, no. 4, pp. 352–375, Oct. 2018. doi: 10.1504/IJWGS.2018.095647.

[17] Q. Wang, J. Yu, S. Chen, and Y. Xiang, "SoK: Dag-based blockchain systems," *ACM Comput. Surv.*, vol. 55, no. 12, pp. 1–38, Mar. 2023. doi: 10.1145/3576899.

[18] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Blockchain empowered asynchronous federated learning for secure data sharing in Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4298–4311, Feb. 2020. doi: 10.1109/TVT.2020.2973651.

[19] H. Chai, S. Leng, F. Wu, and J. He, "Secure and efficient blockchain-based knowledge sharing for intelligent connected vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 9, pp. 14620–14631, Dec. 2021. doi: 10.1109/TITS.2021.3131240.

[20] C. Dwork, "Differential privacy," in *33rd Int. Conf. Autom., Lang. Program.*, Venice, Italy, Jul. 10–14, 2006, pp. 1–12.
[21] K. Wei *et al.*, "Federated learning with differential privacy: Algorithms and performance analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 3454–3469, Apr. 2020. doi: 10.1109/TIFS.2020.2988575.
[22] R. C. Geyer, T. Klein, and M. Nabi, "Differentially private federated learning: A client level perspective," 2017, *arXiv:1712.07557*.
[23] B. Ji *et al.*, "A vision of IoV in 5G HetNets: Architecture, key technologies, applications, challenges, and trends," *IEEE Netw.*, vol. 36, no. 2, pp. 153–161, Apr. 2022. doi: 10.1109/MNET.012.2000527.
[24] M. Abadi *et al.*, "Deep learning with differential privacy," in *23rd ACM Conf. Comput. Commun. Secur.*, Vienna, Austria, Oct. 24–28, 2016, pp. 308–318.
[25] C. Cui, H. Du, Z. Jia, X. Zhang, Y. He and Y. Yang, "Data poisoning attacks with hybrid particle swarm optimization algorithms against federated learning in connected and autonomous vehicles," *IEEE Access*, vol. 11, pp. 136361–136369, Nov. 2023. doi: 10.1109/ACCESS.2023.3337638.