This article has been accepted for publication in IEEE Network. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MNET.2024.3369406

Towards Secure and Robust Federated Distillation in Distributed Cloud: Challenges and Design Issues

Xiaodong Wang, Zhitao Guan, Longfei Wu, and Keke Gai

***Abstract*—**Federated learning (FL) offers a promising solution for effectively leveraging the data scattered across the distributed cloud system. Despite its potential, the huge communication overhead greatly burdens the distributed cloud system. Federated distillation (FD) is a novel distributed learning technique with low communication cost, in which the clients communicate only the model logits rather than the model parameters. However, FD faces challenges related to data heterogeneity and security. Additionally, the conventional aggregation method in FD is vulnerable to malicious uploads. In this article, we discuss the limitations of FL and the challenges of FD in the context of distributed cloud system. To address these issues, we propose a blockchain-based framework to achieve secure and robust FD. Specifically, we develop a pre-training data preparation method to reduce data distribution heterogeneity and an aggregation method to enhance the robustness of the aggregation process. Moreover, a committee/workers selection strategy is devised to optimize the task allocation among clients. Experimental evaluations are conducted to evaluate the effectiveness of the proposed framework.

INTRODUCTION

In recent years, the rapid advance of information and communication technologies has given rise to the prevalence of compact and intelligent internet-connected devices which are application-oriented. According to a recent report from Statista [1], the amount of Internet of Things (IoT) devices worldwide is projected to nearly triple from 9.7 billion in 2020 to more than 29 billion by 2030. This trend would bring an explosive growth in demands for data processing and storage, posing a significant challenge to existing cloud services. Notably, certain applications generate tasks with requirements such as substantial computation capacity, low latency, high throughput, data confidentiality, and/or regulatory compliance. To satisfy the needs of these applications, the geographically distributed cloud servers, fog nodes, edge devices, along with the end devices can together constitute a distributed cloud system, working collaboratively on tasks. Federated learning (FL) [2] provides a distributed learning paradigm where cloud servers can collaborate to train a global model that benefits all participants without directly sharing their local data [3].

The most common FL framework consists of an aggregator (server) and multiple participants (clients). In conventional FL, the sharing of model parameters between the aggregator and clients during the training process introduces a significant communication overhead. The communication cost scales proportional with the number of global parameters [4], impeding clients in FL from using lager-sized models. Model heterogeneity is another limitation of FL. Typically, local models held by clients share the same architecture as the global model produced by the aggregator, limiting the degree of personalization. Privacy leakage is the third limitation of conventional FL. Although the local data of clients in FL are not exposed, the parameters of deep learning models may still leak the privacy of the clients. For example, with the target model's parameters, an adversary can launch membership inference attack against FL to infer whether a given data point is in the training set, thereby obtaining private information about the composition of the target model's training set [5].

Federated distillation (FD) [4], a novel distributed training paradigm, provides a promising approach to tackle these challenges. Inspired by knowledge distillation (KD), FD allows multiple clients to jointly train the global model by sharing the logits (prediction results) of their local models rather than the model parameters. In FD, each client takes its local model as the student model and views the aggregated model outputs of all other clients as the teacher model output. The frameworks of FL and FD are presented in Fig. 1. Compared to FL, FD enables the cloud servers in the distributed cloud system to perform federated training with low communication overhead and the flexibility to design their own local models. However, FD faces certain challenges. The first is the distillation dataset issue. In conventional KD, the teacher model and the student model transfer knowledge from the same distillation dataset. When it comes to FD, due to the concerns on the privacy and security of sensitive data, clients are reluctant to share their local data, Consequently, they have no knowledge about the local data of each other. Data heterogeneity is another important issue. Similar to FL, the local data of clients in FD are non-identically and independently distributed (non-IID), which can lead to slow convergence and degraded performance [6]. Lastly, there are also robustness and security issues in FD. The malicious aggregator or clients may attack the training process, resulting in poor training performance.

To resolve the above challenges, we design a secure and robust FD framework for collaborative learning in the distributed cloud system. In order to enhance the security, we employ the blockchain technology to build a secure and trustworthy environment for all parties participating the FD. To tackle the data distribution heterogeneity issue and the lack of distillation data, a novel pre-training data preparation method is devised. This method searches for overlap data via

▪ *Xiaodong Wang and Zhitao Guan are with School of Control and Computer Engineering, North China Electric Power University, Beijing, 102206, China.*
▪ *Longfei Wu is with Department of Mathematics & Computer Science, Fayetteville State University, Fayetteville, 28301, USA.*
▪ *Keke Gai (Corresponding author) is with School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing, 100081, China.*

Authorized licensed use limited to: Iowa State University Library. Downloaded on March 06,2024 at 23:25:47 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

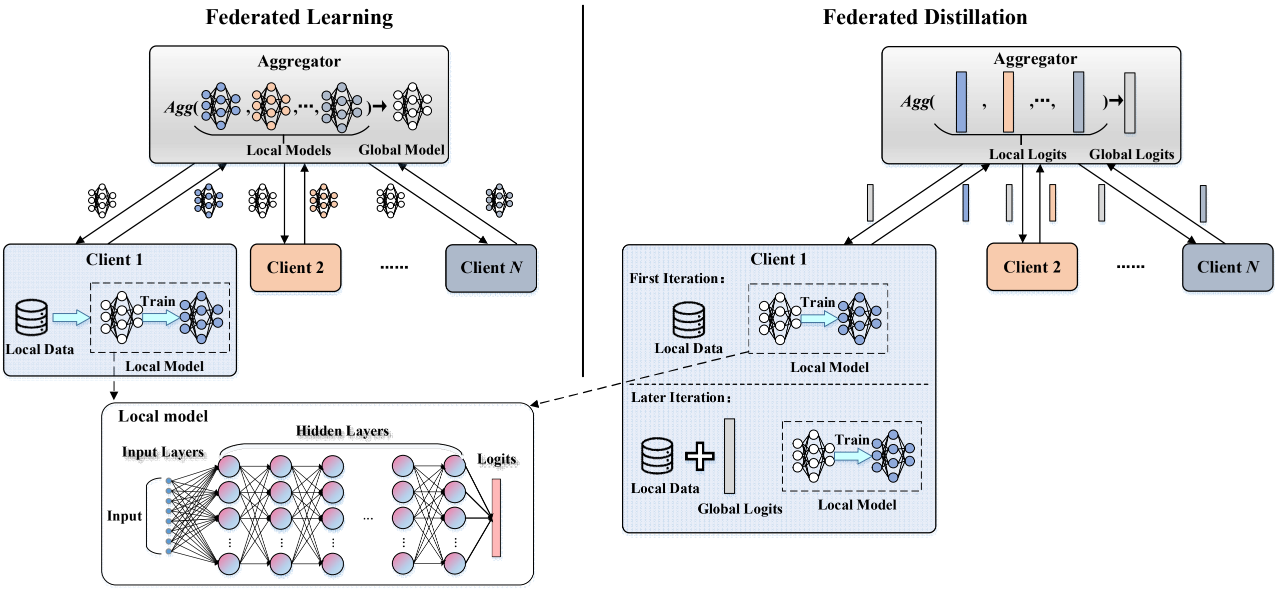


Fig. 1. The frameworks of FL and FD.

the private set intersection (PSI) technique, then the overlap data are augmented to reduce the distance between local data distributions. In addition, the aggregator performs robust aggregation using the weighted average algorithm with dynamic weights. Furthermore, to optimize the task allocation, a committee/workers selection strategy is employed for cloud servers to alternately play the roles of clients in FD and nodes in blockchain. The main contributions of our study are summarized as follows:

- We investigate the application of FD in the distribution cloud system and analyze its advantages and challenges.
- We propose a novel FD framework that integrates a modified federated training process with blockchain technology, which can improve the model accuracy and enhance the security and robustness of FD.
- We conduct experimental evaluations on our proposed framework to demonstrate its effectiveness. The results show that our framework can achieve a performance advantage over the conventional FD and decrease the communication cost compared to FL.

Federated Distillation for Distributed Cloud Computing

In this section, we first describe the workflow of FD, and then we discuss the main design challenges of FD in the distributed cloud system.

Workflow and Key Features of FD in Distributed Cloud

FD is a novel algorithmic framework derived from FL to address its limitations. In FD, the aggregator and clients communicate model logits instead of model parameters during federated training. In the context of distributed cloud system, the cloud servers play the role of clients in FD and a centralized server functions as the aggregator.

Workflow: The workflow of FD can be simply summarized as follows:

Step 1: The clients build their own local models and updates the model parameters according to their own loss functions on the local data.

Step 2: The clients store the averaged model logits of each label. Then, the label-wise local logits are uploaded to the aggregator.

Step 3: The aggregator calculates the global logits via the received local logits. Then, the aggregator selects K from all N clients to participate in next iteration.

Step 4: The clients receive the global logits distributed by the aggregator and update the local parameters according to the loss function and distillation regularizer.

Step 5: Repeat Steps 2-4 during the training iterations.

Key Features: We highlight two key features of FD in the distributed cloud system.

Reduced communication overhead: The communication overhead during federated training is greatly reduced, since only the model logits are communicated instead of the model parameters. Consequently, the clients can employ large-sized models.

Training heterogenous models: FD provides a solution to heterogenous FL. Without the need to share model parameters, the clients can choose their own personalized models as the local models for their specific tasks, which can enhance the efficacy of federated training.

Design Challenges

While FD can mitigate the shortcomings of FL, it also faces its own problems. The primary issues with FD are discussed below.

Distillation Data: In KD, the student model and the teacher model distill knowledge on the same dataset. However, in FD, the clients are reluctant to share their local data. One way for

Authorized licensed use limited to: Iowa State University Library. Downloaded on March 06,2024 at 23:25:47 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Network. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MNET.2024.3369406

clients to evaluate the logit gap is to share the average logits of each label. Then, clients store the logit vectors label-wise and upload these local logits to the aggregator. Another way is to employ an extra distillation dataset, called proxy dataset [6]. The proxy dataset is usually a public dataset [7-8] or a generative dataset [9-10]. As for the former, it is assumed that the aggregator and the clients have access to a public dataset to calculate the logits, while for the latter, the distillation dataset is created by a generative model trained by the aggregator or clients. In practical scenarios, the public dataset may not always be available. Additionally, training a generative model needs extra knowledge of the clients' local data, potentially compromising FL's primary goal of privacy preserving.

Data Heterogeneity: Data heterogeneity includes data feature heterogeneity and data distribution heterogeneity. The former is associated with the problem of model heterogeneity, which we have discussed before. Here, we focus on the data distribution heterogeneity. Generally, the model trained on the non-IID data performs worse than the model trained on the IID data. Some existing works use a public dataset (e.g., an unlabeled public dataset) to mitigate the effect of non-IID data [11]. However, as we have just mentioned, the availability of a public dataset is not guaranteed in all scenarios.

Security and Robustness: The issue of security and model robustness remains in FD. Under the traditional assumption that the aggregator is trustworthy, the clients may be dishonest and/or lazy during the federated training. Even worse, a malicious client can modify the uploaded local logits to obtain private information about other clients' local data. Breaking out of the traditional assumption, the aggregator may also be curious about the private information about the clients' local data.

A Blockchain-Based Federated Distillation in Distribution Cloud

In this section, we present a framework of blockchain-based FD to resolve the remaining challenges in the distributed cloud system. We first give an overview of the framework. Then, we describe the detailed design for secure and robust federated training.

A Blockchain Enhanced FD Framework

Trust model: We consider the following trust model and assumptions of entities in the proposed framework:

Honest-but-curious aggregator: We assume that the aggregator (centralized server) will honestly follow the federated training protocol, but it may attempt to gain additional information from the exchanged messages.

Malicious clients: We assume that a malicious client may attempt to infer private information about honest clients by analyzing the exchanged information. Additionally, a malicious client may tamper the local model weights before submitting the local logits.

Benefits of blockchain: Blockchain plays an important role in realizing supervised and trusted FL schemes [12]. Likewise, the incorporation of blockchain in our framework can mitigate the security concerns in FD. The benefits of integrating blockchain with FD are listed as follows.

Immutability: The blockchain records the whole process of federated training in FD through the immutable ledger, ensuring a transparent and unalterable history of model updates. This feature is crucial for auditing and accountability, as it allows participants and supervisors to trace the federated training process. Moreover, the immutable nature of the ledger acts as a deterrent against clients' dishonest behavior and laziness, fostering a cooperative and trustworthy environment in which participants are motivated to contribute to the federated training.

Smart contracts: Smart contracts are the self-enforcing programs stored in the blockchain which are executed automatically. Blockchain employs smart contracts to enhance the trust management and automation, as the smart contracts cannot be tempered after deployment. Smart contracts can be employed to make the recording of the training process automatic and more efficient.

Storage: FD also alleviates the storage burden on blockchain nodes. In the blockchain-based FL framework, the blockchain nodes are obligated to store the communicated model parameters when recording the training process. In contrast, in the blockchain-based FD framework, the nodes only need to record the model logits. Additionally, the blockchain nodes can choose to preserve the whole ledger with the block body or merely the block header depending on their resource availability [13]. Hence, the storage cost is greatly lowered in the FD context.

Framework: In our proposed framework, FD is conducted by a number of distributed cloud servers and a powerful centralized server. The cloud servers act as the clients in FD and also as the nodes in blockchain. The central server acts as the aggregator. Each cloud server is connected to various kinds of devices (e.g., fog/edge devices). By default, the communication messages between the server and clients are encrypted using homomorphic encryption, ensuring that the server computes global logits without knowing the plaintext of logits. Therefore, a curious server cannot infer the private information from the exchanged messages.

As shown in Fig. 2, we take the medical system as an example, where the hospitals have their own cloud servers that are connected to medical devices. These hospitals are managed by a central server for federated training. We describe the workflow of our proposed blockchain-based FD as follows.

Step 1: The clients prepare the local data and initialize the local models which are built on their own. The method of pre-training data preparation used will be introduced in detail shortly.

Step 2: The clients update their local models upon the local data using only the loss function.

Step 3: The clients input the local training data into the local model and average the model logits on each label. Then the clients store the mean logits of each label as the local logits. The local logits are uploaded to the aggregator.

Step 4: The nodes of the committee in this iteration are

Authorized licensed use limited to: Iowa State University Library. Downloaded on March 06,2024 at 23:25:47 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Network. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MNET.2024.3369406

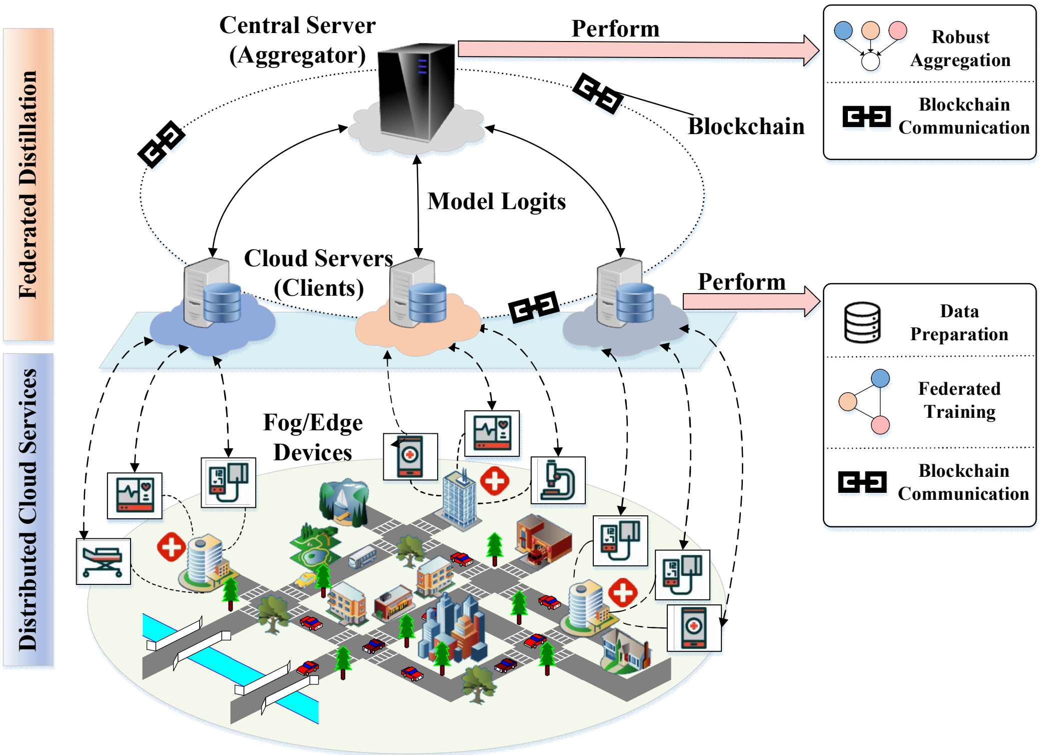


Fig. 2. The architecture of the blockchain-based FD in the distributed cloud system.

selected from the clients. The committee generates a new block and links it to the end of the blockchain. The newly created block contains the information of the clients participating in this iteration, the local logits uploaded by the clients. The committee selection method will be described later in this section.

Step 5: The aggregator calculates the global logits by aggregating the clients' local logits. The robust aggregation method will be presented later in this section.

Step 6: The *K* clients who participate in the next iteration are selected, and we denote these clients as workers. Then, the aggregator sends the global logits to the workers. The worker selection strategy will be presented later in this section.

Step 7: The committee creates a new block which involves the information of the iteration and the global logits.

Step 8: The selected clients receive the global logits and update the local parameters using the loss function and the distillation regularizer.

Step 9: Repeat Steps 3-8 in each iteration.

In addition, the committee and the workers selection methods are written into respective smart contracts which are loaded in all nodes. Also, smart contracts are used to record the training process in the blockchain, as in Step 4 and Step 7.

PRE-TRAINING DATA PREPARATION

One method to enrich the clients' local datasets is data augmentation. However, blind data augmentation on non-IID local data may aggravate data distribution heterogeneity. To address this, we consider scenarios where overlaps exist between clients' local datasets. For instance, in a medical system, cloud servers in different hospitals may share data about patients who visit two or more of these hospitals for examinations, diagnosis, and treatment. We propose a pre-training data preparation method to handle data distribution heterogeneity. The key strategy to mitigate non-IID issues is to augment the overlap data, minimizing distribution disparities between datasets. To find the overlap between datasets without revealing the actual data, private set intersection (PSI) [14] is performed on the local datasets between every two clients. Specifically, we employ is the server-aided PSI in [15], which ensures security against malicious adversaries attempting to violate the protocol. If an intersection exists between local datasets, the corresponding clients will apply data augmentation to the overlapped data points. Although conducting PSI between every two clients seems to be tedious, it can work when a public dataset is unavailable and can avoid privacy leakage. Moreover, once the overlap data among all local datasets are found, they can be used as distillation data. Then, the clients upload the local logits by concatenating the logits of overlap data and the logits of each label.

COMMITTEE/WORKERS SELECTION STRATEGY BASED ON WEIGHTED RANDOM SAMPLING

In the conventional FD, the aggregator randomly selects clients for each iteration, overlooking critical distinctions among clients, such as the volume of their local data. It is generally acknowledged that models trained with larger datasets yield better performance. Hence, it is rational to prioritize clients with larger size of local data to participate more often in federated training. Another motivation of the selection strategy is to optimize the task allocation. In the

Authorized licensed use limited to: Iowa State University Library. Downloaded on March 06,2024 at 23:25:47 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Network. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MNET.2024.3369406

blockchain-based FD framework, clients also serve as nodes in the blockchain system. It is reasonable to offload the tasks of the committee in the blockchain from clients with larger datasets to those with smaller datasets. Therefore, we propose a committee/workers selection strategy using Weighted Random Sample (WRS) based on the size of the clients' local training datasets. The more local data a client has, the more likely the client is to be selected as a worker. Meanwhile, the smaller a client's local dataset is, the more likely the client is to be selected as a node of the committee. The weights in the WRS are proportional to the quantity of local data. To prevent scenarios where clients with smaller local datasets never get selected as workers in federated training, we set a minimal participation frequency for clients. That is, each client is mandated to participate at least T_{min} iterations throughout the training process. T_{min} can be set as t percentile of the total number of iterations (t as a hyperparameter, e.g., t=5, 10 or 20).

Robust Aggregation Method with Dynamic Weights

The aggregator averages the local logits uploaded by the clients (workers) to calculate the global logits. The global logits sent to a client exclude the local logits uploaded by that client. The aggregation via averaging is vulnerable to attacks from malicious clients. We propose a weighted average aggregation method with dynamic weights to achieve robust aggregation. Specifically, the aggregator calculates global logits using a weighted average algorithm with dynamic weights. In each iteration, we assume that the clients' local datasets have L labels and the aggregator receives local logits from K clients. For the i-th client's local logit matrix (consisting of L logit vectors), the aggregator calculates Euclidean distances between this logit matrix and other K-1 logit matrixes. The sum of these distances is denoted as d_i. Then, the aggregator calculates the sum of d_1^{-1} (the inverse of d_1, $1/d_1$), d_2^{-1}, …… and d_K^{-1}, denoted as D. The weight assigned to the i-th client's logit vector is equal to d_i^{-1}/D. As we can see, the weight of the i-th client's local logits in the weighted average is greater when d_i and the sum of the distances are small, emphasizing the importance of logit vectors from clients whose local data distributions align closely with others. Therefore, this dynamic weighting strategy can enhance the robustness of the aggregation process.

Experimental Evaluation

In this section, we evaluate the performance of the proposed blockchain-based FD framework. The major goal of FD is to dramatically reduce the communication cost of FL by sharing the model logits rather than the model parameters. Hence, it is acceptable for FD schemes to have a small performance loss in terms of accuracy compared to FL schemes. In our experiments, we take the conventional FD scheme [4] and the conventional FL scheme FedAvg [2] as benchmarks.

Experimental Settings

The experiments are conducted on a PC running Windows 11 OS and equipped with 16GB RAM, Intel(R) Core(TM) i7-12700F CPU @ 2.10GHz, NVIDIA GeForce RTX 3060 12GB GPU, Python(3.8.13), and torch(1.8.0).

We use accuracy as the primary metric. Accuracy is the ratio of the number of correct predictions to the total number of predicted samples, typically expressed as a percentage. We set up 10 cloud servers (clients) in a distributed cloud system to perform collaborative learning on their local datasets without sharing data with each other. We conduct the experiments on a real-world dataset, CIFAR-10. CIFAR-10 is an image dataset widely used in the field of image recognition, which contains a total of 60,000 color images from 10 classes. To assess the impact of data distribution, we explore both IID and non-IID settings. In the IID setting, data points with the same label are evenly distributed among clients; while in the non-IID setting, the distribution of data points with the same label varies across clients. We also evaluate the performances when the clients' local datasets overlap and do not overlap. To avoid the inference of difference types of models, we employ the fully connected networks (FCN) for all clients. The clients start communicating with the aggregator after 200 iterations of local training (local iterations), with the aggregator performing 25 iterations of aggregation (global iteration).

Evaluation Analysis

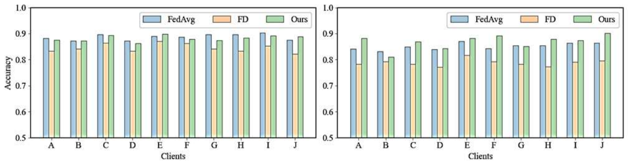
In all experiments, we measure the accuracy in the last iteration for each of the ten clients (named A to J). Under both the IID and non-IID settings, we compare the accuracy of our proposed framework with that of FedAvg and conventional FD (labeled as FD in the figures). In the first group of evaluation, we consider the scenario where there are overlaps in the clients' local datasets. The results are shown in Fig. 3. As we can see, in both the IID and non-IID settings, our proposed blockchain-based FD framework outperforms the conventional FD as all clients achieve a higher accuracy. In comparison to FedAvg, the performance of our method under the IID setting is slightly lower than FedAvg but they are overall very close. Under the non-IID setting, the performance of our approach exceeds FedAvg for the majority of clients. In the second group of evaluation, we explore the ideal situation where the clients' local datasets do not overlap, which corresponds to the performance of our framework without pre-training data preparation. In other words, the results of this group of evaluation show the effectiveness of the committee/workers selection strategy and the robust aggregation strategy we proposed. As shown in Fig. 4, the accuracy of FedAvg is higher than our approach when no overlap exists between the clients' local data. However, our approach still achieves an apparently higher accuracy than the conventional FD for most clients. Regarding communication overhead, in FedAvg, clients share the FCN architecture with 950,083,200 model parameters. In each global iteration, each client exchanges the doubled amount of model parameters for upload and download. In contrast, our proposed framework only requires clients to upload 10 logit vectors every global iteration. Each of the logit vectors consists of 10 elements of the confidence scores. This significantly reduces the communication burden compared to traditional FL,

Authorized licensed use limited to: Iowa State University Library. Downloaded on March 06,2024 at 23:25:47 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Network. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MNET.2024.3369406

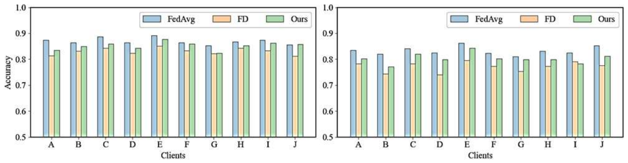
demonstrating the efficiency of our approach.

To sum up, our proposed framework can achieve a remarkable advantage in overall accuracy performance (across all clients) over the conventional FD scheme. And it can significantly reduce the communication overhead compared to the conventional FL scheme at the cost of a little loss in accuracy. Notably, the pre-training data preparation method proposed in our framework demonstrates a significant contribution as our framework outperforms the conventional FD scheme in both accuracy and communication overhead in the practical situation of overlapping local datasets and non-IID data setting.



a) IID setting b) Non-IID setting

Fig. 3. Accuracy of the three different frameworks when the overlaps in local datasets exist.



a) IID setting b) Non-IID setting

Fig. 4. Accuracy of the three different frameworks when no overlap in local datasets exists.

Discussions

There remain some challenges in our proposed schemes that need to be further addressed. We discuss the technical challenges and future research directions below.

Remaining Challenges

Overhead of PSI: The server-aided PSI offloads computation tasks to a centralized server, alleviating challenges for resource-constrained devices especially when dealing with large-scale datasets. However, the computational and communication costs increase accordingly.

Communication and efficiency of blockchain: In the blockchain-based FD system, the need for decentralized communication among participants introduces communication overhead. The process of exchanging information through the blockchain network consensus mechanism can lead to increased communication costs and latency.

Privacy leakage assessment: Although FD offers improved privacy compared to FL, potential privacy threats persist. Specifically, the black-box membership inference attack (MIA) against machine learning models poses a threat to FD theoretically. One of the primary challenges in the proposed FD scheme lies in the absence of a privacy leakage assessment with existing MIA methods.

Future Directions

Efficient communications: While FD reduces the communication overhead cost by sharing model logits, the proposed FD requires additional communications due to the integration of blockchain and the usage of server-aided PSI. One of the future directions is to optimize communication protocols and leverage intelligent compression algorithms to enhance efficiency.

Comprehensive performance evaluation: The experimentation conducted is limited. Future efforts will be made on a more comprehensive investigation on the performance of the proposed scheme under different federated settings, including different non-IID cases and different numbers of clients. Moreover, the effectiveness the proposed FD in mitigating privacy leakage will also be the focus our future research.

Conclusion

In this article, we present a blockchain-based FD framework to establish secure and robust distributed learning in distributed cloud systems. We design a novel pre-training data preparation method to avoid the requirements on a public dataset and training a generator to create the public data. In order to enhance the robustness of aggregation process, we propose a new robust aggregation strategy. We also develop the committee/workers selection strategy to optimize data utilization and task allocation. Experimental evaluations are conducted to demonstrate the effectiveness of our proposed framework. We also discuss the challenges of the proposed FD framework and our future research directions.

Acknowledgment

The work is partially supported by the National Natural Science Foundation of China under Grant 62372173.

References

[1] Statista, "Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030," 2022. [Online]. Available: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/, accessed Dec. 9, 2022.

[2] B. McMahan et al., "Communication-Efficient Learning of Deep Networks from Decentralized Data," Proc. AISTATS, 2017, pp. 1273–82.

[3] A. Tak and S. Cherkaoui, "Federated edge learning: design issues and challenges," *IEEE Network*, vol. 35, no. 2, Mar./Apr. 2021, pp. 252–58.

[4] E. Jeong, S. Oh, H. Kim, J. Park, M. Bennis, and S.-L. Kim, "Communication-efficient on-device machine learning: Federated distillation and augmentation under non-IID private data," *Proc. NIPS Workshop*, 2018.

[5] M. Nasr, R. Shokri, and A. Houmansadr, "Comprehensive Privacy Analysis of Deep Learning: Passive and Active White-Box Inference Attacks Against Centralized and Federated Learning," *Proc. IEEE S&P*, 2019, pp. 739–53.

[6] L. Zhang, L. Shen, L. Ding, D. Tao, and L.-Y. Duan, "Fine-tuning global model via data-free knowledge distillation for non-iid federated learning," *Proc. IEEE Conf. Computer Vision and Pattern Recognition*, 2022, pp. 10174–10183.

[7] D. Sui, Y. Chen, J. Zhao, Y. Jia, Y. Xie, and W. Sun, "FedED: Federated learning via ensemble distillation for medical relation extraction," *Proc. EMNLP*, 2020, pp. 2118–2128.

[8] J.-H. Ahn, O. Simeone and J. Kang, "Wireless federated distillation for distributed edge learning with heterogeneous data", *Proc. IEEE PIMRC*, pp. 1-6, 2019.

[9] T. Lin, L. Kong, S. U. Stich, and M. Jaggi, "Ensemble distillation for robust model fusion in federated learning," *Proc. NIPS*, vol. 33, 2020, pp. 1–26.

Authorized licensed use limited to: Iowa State University Library. Downloaded on March 06,2024 at 23:25:47 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Network. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MNET.2024.3369406

[10]Z. Zhu, J. Hong, and J. Zhou, "Data-free knowledge distillation for heterogeneous federated learning," *Proc. ICML*, 2021, pp. 12878–12889.

[11]X. Gong et al., "Ensemble attention distillation for privacy-preserving federated learning," *Proc. IEEE/CVF ICCV*, 2021, pp. 15 076–15 086.

[12]N. Wang et al., "A blockchain based privacy-preserving federated learning scheme for Internet of Vehicles." *Digital Communications and Networks*, early access, doi: 10.1016/j.dcan.2020.06.002.

[13]G. D. Putra, V. Dedeoglu, S. S. Kanhere and R. Jurdak, "Toward Blockchain-Based Trust and Reputation Management for Trustworthy 6G Networks," *IEEE Network*, vol. 36, no. 4, July/Aug. 2022, pp. 112-119.

[14]C. Hazay and M. Venkitasubramaniam, "Scalable Multi-party Private Set-Intersection", Proc. Public-Key Cryptography, 2017, vol. 10174, pp. 175-203.

[15]Kamara, S., Mohassel, P., Raykova, M., Sadeghian, S., "Scaling Private Set Intersection to Billion-Element Sets," 18th International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 2014: 195–215.

BIOGRAPHIES

XIAODONG WANG (swithunwang@ncepu.edu.cn) is currently a PhD student with the School of Control and Computer Engineering, North China Electric Power University. He received his B.S. degree from North China Electric Power University in 2021. His current research interests include blockchain and federated learning. He is a Student Member of IEEE.

ZHITAO GUAN (guan@ncepu.edu.cn) is currently a Professor at the School of Control and Computer Engineering, North China Electric Power University. He received his BEng degree and PhD in Computer Application from Beijing Institute of Technology, China, in 2002 and 2008, respectively. His current research focuses on smart grid security, AI security and privacy computing. He is a Member of IEEE.

LONGFEI WU (lwu@uncfsu.edu) is currently an assistant professor in the Department of Mathematics and Computer Science at Fayetteville State University. He received his Ph.D. degree in computer and information sciences from Temple University in July 2017. He obtained his B.E. degree from Beijing University of Posts and Telecommunications in July 2012. His research interests are the security and privacy of networked systems and modern computing devices, including mobile devices, IoT, implantable medical devices, and wireless networks.

KEKE GAI (gaikeke@bit.edu.cn) received the Ph.D. degree in computer science from Pace University, New York, NY, USA. He is currently a Professor at the School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing, China. He has published 5 books and more than 180 peer-reviewed journal/conference papers, including 10 best paper awards. He serves as an Editor-in-Chief of the journal Blockchains and Associate Editors for a number of decent journals, including IEEE Transactions on Dependable and Secure Computing, Journal of Parallel and Distributed Computing, etc. He also serves as a co-chair of IEEE Technology and Engineering Management Society's Technical Committee on Blockchain and Distributed Ledger Technologies, a Standing Committee Member at China Computer Federation - Blockchain Committee, a Secretary-General at IEEE Special Technical Community in Smart Computing. His research interests include cyber security, blockchain, privacy-preserving computation, decentralized identity, and artificial intelligence security.

Authorized licensed use limited to: Iowa State University Library. Downloaded on March 06,2024 at 23:25:47 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.