Research on Data Sharing and Privacy Protection Mechanism in Federated Learning Based on Blockchain

Yi Liu

Abstract—**With the development of the times, how to share data safely on the basis of protecting users' privacy has attracted extensive attention. As a new machine learning technology, federated learning can use the local data set of nodes for distributed model training, and only share the model without uploading the original training data during the training update process, so as to achieve the safe sharing of the model. However, the data provider will not share the local data out of concern about the risk of data security and privacy disclosure, resulting in data sharing failure; There may be malicious workers in federal learning that will destroy learning, affect the overall model, and lead to unreliable data sharing; In the process of model updating, intermediate parameters may be stolen by attackers, leading to the privacy disclosure of data providers.To address the above issues, this paper introduces blockchain technology to further study data sharing and privacy protection in federated learning.**

Index Terms—**Federal Learning; Blockchain; Data sharing; Privacy protection; Consensus algorithm**

I. Introduction

With the rapid development of the Internet, the process of socialization is faster and faster, and a large number of data are generated. The potential value of data can be mined through machine learning technology. However, traditional ML schemes require aggregation on the centralized cloud to train data, which causes users to worry about privacy disclosure of personal data and possible misuse of data [1].

Federated Learning (FL) [2], a collaborative approach of distributed ML, can solve the problem of data islands through mutual collaboration. Its core idea is to conduct distributed model training among multiple data sources with local data. In the training process, the global model under virtual fusion data is constructed only by exchanging model parameters or intermediate results without exchanging local individuals or sample data. This can ensure that the user data privacy in FL remains unchanged, because no original data is transmitted from the user equipment. The central server receives the local models of different devices and updates them continuously, so as to aggregate the updated local models and update the global model. The mobile device obtains the updated global model to calculate the local model of its next version [3]. In order to ensure the reliability of federal learning tasks and improve the accuracy of model training, blockchain technology can be used to realize the security management of data in the federal learning process by using the tamper proof and traceability of blockchain.

"Blockchain" first appeared in the article [4] "Bitcoin: Decentralized, a peer-to-peer electronic cash system" published by Bencong in 2008, which described how to establish a new, decentralized, trust independent peer-to-peer trading system. Blockchain technology is the core supporting technology of the digital cryptocurrency system represented by Bitcoin. On January 3, 2009, the first decentralized virtual crypto digital currency, Bitcoin, was officially launched, and the first Bitcoin block, Genesis Block, was born. In 2013, Vitalik Buterin developed a distributed computing platform based on blockchain technology - Ethereum. Since 2014, the huge potential application value of the underlying supporting technology blockchain of Bitcoin has been discovered, which has triggered the development of distributed ledger technology. Nowadays, blockchain has become a kind of ledger technology that is chronological, decentralized, original and unchanging [5]. In order to reduce the security problem involving FL central server, the blockchain can be organically integrated with FL. [6]

II. RELATED WORK

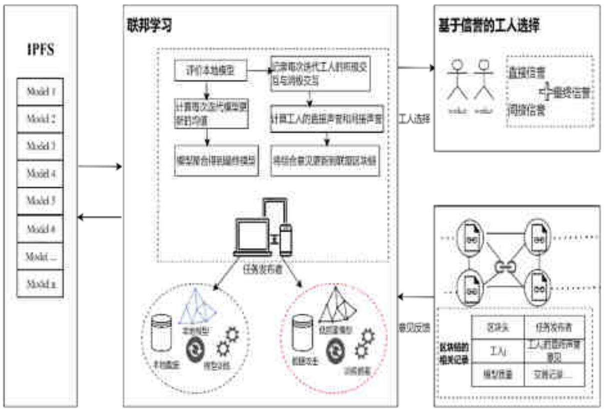
In order to avoid being attacked by malicious workers during federal learning tasks and the risk that model training is the disclosure of intermediate parameter privacy, a common, multi-party distributed data sharing mechanism is designed in this paper. In this mechanism, each participant has its own data. In order to enable participants to make better use of data, data can be merged for collaborative tasks. This paper aims to design a Secure data sharing mechanism, which can effectively maintain data privacy (DSPM for short). In this process, task publishers can not directly access and obtain data, thus protection the privacy of nodes. Before starting the federal learning task, each task publisher will select appropriate workers according to the task needs and feedback after previous training. The selected worker nodes will form a shared global model through repeated training.

The local data is also constantly updating the local model. All workers will submit the updated local model to the task publisher, who will update the global model. The task publisher evaluates the reputation of workers based on their training behavior and the model uploaded by workers [7], and evaluates whether workers can be trusted to express their opinions and whether they contribute to the model update. In order to ensure the reliability and safety of federal learning, a

Manuscript received December 07, 2022

Yi Liu School of Software,Tiangong University,China

multi weight subjective logic model is used to evaluate the reputation of workers, and a reputation based worker selection scheme is designed. The multi weight subjective logic model is used to calculate the reputation of workers. Taking advantage of the tamper proof and traceability of the blockchain, an alliance blockchain is designed to store and manage workers' reputation and contribution opinions in a decentralized and secure way.In order to reduce the storage pressure and storage cost of the blockchain, IPFS technology and storage training model are introduced.



Federal Learning Module

Step 1: Publish federal learning tasks: Task publishers first broadcast within a certain range according to the joint learning tasks they are required to complete and specific resource requirements (such as data type, size and time range, accuracy). The node that meets the requirements can become a candidate to participate in the model training of the federated learning task, respond to the task publisher, send the connection request to the task publisher, and send its identity information to the task publisher together through encryption.

Step 2: Calculate the reputation and contribution comments of the candidate worker nodes participating in the task: Step 1, the task publisher first decrypts the identity information of the workers who want to participate in the learning task, confirms whether the information they provide is legal, and includes the qualified nodes in the list of federal learning workers. The task publisher then based on the direct reputation evaluation of the interaction history, that is, the local evaluation, and the indirect reputation evaluation opinions of other task publishers, that is, the recommended reputation evaluation, through the multi weight subjective logic model [8], from the four aspects of interaction frequency, interaction effect, interaction time and interaction location, we can get the reputation value of the candidate workers. Both direct and indirect opinions are saved on the reputation blockchain, and the reputation evaluation of candidate workers is recorded in each data block for the task publisher to access at any time. When selecting candidate workers, the task publisher will first download the latest indirect evaluation on reputation, that is, recommendations, from the blockchain. Finally, the direct reputation opinion is combined with the recommended reputation opinion to form a final opinion value for reference by each task publisher.

Step 3: Select workers for joint learning: Reputation thresholds are preset by task publishers according to their own needs, usually by the average level of workers. Of course, different publishers can also set the same threshold. Then, we calculate the reputation. According to the different reputation, we select workers with higher reputation as the workers of federal learning tasks.

Step 4: Perform federal learning tasks. After determining the workers, the task publisher will randomly select an initial model from the predetermined range according to the requirements of the federal learning task, and regard it as a shared global model of the whole. The initial model is trained using various optimization algorithms. For example: SGD algorithm. Then, the task publisher sends the shared global model to the selected workers. After receiving the model, the workers use their local data to conduct collaborative training on the model, and send its local model updates to the task publisher. During this period, the task publisher will record the updated results of the local model uploaded by the workers after each repeated training. When the model is aggregated, the performance degradation of local model updates exceeds the threshold set by the system, and the local model updates will be rejected. Finally, the local model after each training is tested according to the test data set, and the worker's behavior is judged according to its accuracy in the test data set. So as to determine whether the data interaction between task publishers and workers is a positive event or a negative event. In each iteration, the interaction with reliable workers is regarded as positive interaction, and the interaction with unreliable workers is regarded as negative interaction, which is recorded by the task publisher.

Blockchain and IPFS module

This paper uses the Alliance Blockchain to store the reputation opinions of workers. The federation chain combines the public chain with the private chain. It can control some nodes, making the nodes on the chain open and transparent. After the federal learning task is completed, the task publisher updates the latest reputation opinions of workers through historical interactive opinions, places all reputation opinions in a data block, and adds the block to the chain using block verification and consensus algorithm. In this way, the task publisher can screen federal learning workers through the blockchain and improve the work efficiency of the blockchain.

Although we know the identity of each node of the alliance chain, in order to prevent internal nodes from stealing the privacy of other nodes, the blockchain only stores the reputation opinions and model training records of workers, while the real model will be saved in IPFS. After the task publisher uploads the model to IPFS, IPFS will return a unique hash value to protect the security and privacy of the uploaded file.

III. REPUTATION-BASED WORKER SELECTION SCHEME WITH CONSORTIUM BLOCKCHAIN.

In this paper, reputation opinion evaluation is used to evaluate workers in federal learning tasks. The reputation opinion of workers is to evaluate the credibility of workers. Four factors, including interaction frequency, effect, location and time, are considered. The reliability of opinion evaluation can be improved by considering multiple weights. When excluding malicious workers, task publishers can set a threshold for reputation comments.

Taking advantage of the openness, transparency and tamper resistance of the blockchain, the design alliance chain stores the comments and interactive records of workers on the chain to achieve the opinion management of workers' safety, thus training a reliable model.

When using the subjective logic model, opinion evaluation is often affected by their own factors. As a result, their evaluation of opinions is not objective and comprehensive enough. Therefore, in order to obtain an objective and comprehensive evaluation of workers, it is necessary to take into account the influence of many factors. When using the weighted operation, the traditional subjective logic model is evolved into a multi weight subjective logic model [9]. The application of the multi weight subjective logic model should be considered from all aspects of the transaction. Finally, combine the local opinions of the workers with the recommendations to generate a final opinion. Task publishers select workers with high final opinions to conduct model training of federal learning.

This paper mainly considers the weight from the following four aspects: interaction frequency, interaction effect, interaction time and interaction location.

(1)Interaction frequency: higher interaction frequency means that task publishers have more prior knowledge of federal learning workers. The interaction frequency between task publishers and federal learning workers is the ratio of the number of interactions between task publishers and federal learning workers to the average number of interactions between task publishers and other federal learning workers in the time window. Therefore, the higher the interaction frequency, the higher the reputation.

(2)Interaction effect: the interaction effect between task publishers and workers has both positive and negative effects. Different influences will bring different evaluations to workers. For example, workers with good behavior or high contributions upload better models in the process of federal learning and training, which improves the efficiency of model aggregation. This is called positive interaction. However, the updating effect of models uploaded by selfish workers or workers with low contributions is not good, so it will have an impact on the overall aggregation of models, which is a negative interaction. Positive interaction will improve the reputation of federal learning workers, while negative interaction will reduce the reputation of federal learning workers. Compared with positive interaction, negative interaction has a greater impact on workers.

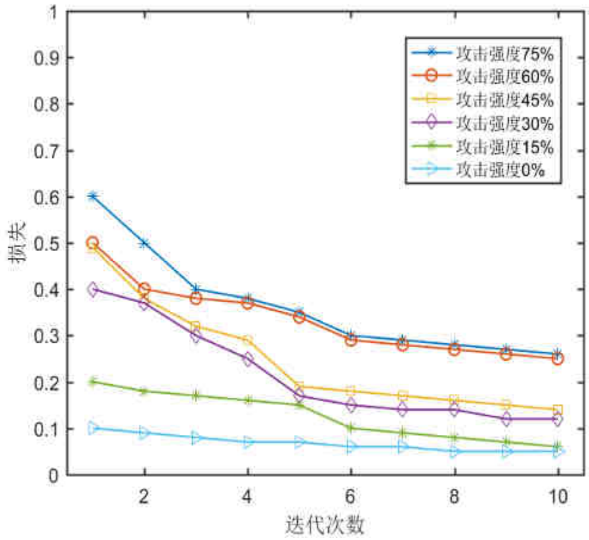
(3)Interaction time: Workers are not always credible and reliable in federal learning. Workers who behave well at the beginning may also become malicious workers later. Therefore, the trust and reputation of task publishers will change over time. The recent interaction will have a greater impact on the local opinions of the task issuer about the federal learning workers.

(4)Interaction location: the data transmission between the task issuer and workers is affected by the interaction location. Due to different environments, the distance of data transmission will be different. The closer the distance is, the smaller the impact on data transmission will be. The farther the distance is, the greater the impact on data transmission will be. Therefore, the closer the worker is to the task publisher, the higher the rating will be, and the farther away the worker will be, the lower the rating will be.

IV. FEASIBILITY ANALYSIS

In the federal learning task, 150 workers are set in this paper. Suppose that 15 workers are selected for each federal learning task. By default, the positions of all workers are evenly distributed. Among the 150 workers, there are 3 malicious workers, 12 workers with low contribution, and the rest are workers with good behavior. Malicious workers mislead model training by deliberately modifying some labels of training examples. The percentage of label modification of training example indicates the attack strength. The higher the percentage of tag modifications, the stronger the attack.

In terms of opinion calculation, the initial credit opinion and initial contribution opinion of all federal learning workers are set as 0.5, ranging from 0 to 1. In this paper, the number of interactions between task publishers and workers on federal learning tasks is set as 10 to 30 times a week. During information interaction, set the probability of successful transmission of data packets to 40% to 60%. For task publishers, this article is composed of 10 honest task publishers and 5 dishonest task publishers. Dishonest task publishers provide false recommendations to other task publishers, resulting in errors in reputation calculation results. This paper compares the proposed multi weight subjective logic scheme with the traditional subjective logic (TSL) scheme proposed in other papers.



As shown in Figure, a malicious worker in a federal learning task, by changing the label of the worker's training example, launched attacks of 0%, 15%, 30%, 45%, 60% and 75%, respectively. From this, we can find that whether there is an attack and the strength of the attack have different effects on its loss function in the federal learning task. When there is no attack, the loss function of federated learning reaches 0.023 after 10 iterations. When the attack intensity is 45%, the loss function of federated learning reaches 0.165 after 10 iterations. When the attack intensity is 75%, the loss function of federated learning reaches 0.267 in 10 iterations. When the attack intensity of malicious workers is higher, the loss function of federated learning is larger. It can be seen from this that attacks by malicious workers greatly affect federal learning tasks. Therefore, how to avoid malicious workers when selecting workers is crucial.

In the storage experiment, we adopted a general federated learning strategy, conducted the same training cycle with the proposed blockchain based federated learning plan, and compared the training results of the two methods. In the joint training, each round has about 1.8 M model, each round has four nodes and an overall model, so each round will consume about 7.2 M model storage cost. In this scheme, upload the model to IPFS, and IPFS will return a hash value of 45 B, and use the public key to encrypt it.

In the storage experiment, set the same training cycle for the general federated learning scheme and the blockchain based federated learning scheme proposed in this paper, so as to compare the block costs generated by the two methods of training. In the process of federated learning training, each round of model size is about 1.8M, each round has four nodes and a global model, and each round will generate a model storage cost of about 7.2M. In this scheme, the model is uploaded to IPFS, and IPFS will return a hash value of 45B, and use the public key to encrypt it. After encryption, a H (Vi, j) of 346B is obtained. After encapsulation, it is encapsulated into a trans i, j (Vi) of 3160B, and placed in a block. Under the scheme proposed in this paper, the size of five models stored in the block in each round is about 15.8KB.

V. Conclusion

With the rise and development of blockchain technology, a trusted data storage and communication infrastructure has been created for the society. Federated learning is a distributed machine learning method, which stores data on each participating node to ensure the privacy of data. In order to prevent the centralized parameter server from being attacked maliciously and parameter privacy leakage, blockchain technology is introduced to upload the trained model to IPFS to ensure the security of the model.

In order to avoid malicious workers in federal learning, which may lead to failure in the learning process, an alliance chain is established to store the evaluation opinions and interaction processes of workers on the chain for task publishers to select workers.

References

[1] Zhao J, Chen Y, Zhang W. Differential privacy preservation in deep learning: Challenges, opportunities and solutions[J]. IEEE Access, 2019, 7: 48901-48911.

[2] Liang Y, Guo Y, Gong Y, et al. An isolated data island benchmark suite for federated learning[J]. arXiv preprint arXiv:2008.07257, 2020.

[3] Wachter S. Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR[J]. Computer law & security review, 2018, 34(3): 436-449.

[4] Nakamoto S. Nakamoto, S, Bitcoin: A peer-to-peer electronic cash system[J]. 2009.

[5] Zappone A, Di Renzo M, Debbah M. Wireless networks design in the era of deep learning: Model-based, AI-based, or both?[J]. IEEE Transactions on Communications, 2019, 67(10): 7331-7376.

[6] Wang S. BlockFedML: Blockchained federated machine learning systems[C]//2019 International Conference on Intelligent Computing, Automation and Systems (ICICAS). IEEE, 2019: 751-756.

[7] Delgado-Segura S, Tanas C, Herrera-Joancomartí J. Reputation and reward: Two sides of the same bitcoin[J]. Sensors, 2016, 16(6): 776.

[8] Ramkissoon A N, Goodridge W. An Energy-Efficient Ensemble-Based Computational Social System for Fake News Detection in MANET Messaging[C]//2022 IEEE Eighth International Conference on Big Data Computing Service and Applications (BigDataService). IEEE, 2022: 182-183.

[9] Kang J, Xiong Z, Niyato D, et al. Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory[J]. IEEE Internet of Things Journal, 2019, 6(6): 10700-10714.