IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 20, 2021, accepted June 30, 2021, date of publication July 8, 2021, date of current version July 16, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3095078

Federated Transfer Learning for IIoT Devices With Low Computing Power Based on Blockchain and Edge Computing

PEIYING ZHANG[1,2], HAO SUN[1], JINGYI SITU[3], CHUNXIAO JIANG[3,4], (Senior Member, IEEE), AND DONGLIANG XIE[2], (Member, IEEE)

[1]College of Computer Science and Technology, China University of Petroleum (East China), Qingdao 266580, China
[2]State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
[3]Beijing National Research Center for Information Science and Technology, Tsinghua University, Beijing 100084, China
[4]Tsinghua Space Center, Tsinghua University, Beijing 100084, China

Corresponding authors: Chunxiao Jiang (jchx@tsinghua.edu.cn) and Peiying Zhang (zhangpeiying@upc.edu.cn)

This work was supported in part by the National Key Research and Development Program of China under Grant 2020YFB1804800, in part by the National Natural Science Foundation of China under Grant 61922050, in part by the Shandong Provincial Natural Science Foundation under Grant ZR2020MF006, in part by the Major Scientific and Technological Projects of China National Petroleum Corporation (CNPC) under Grant ZD2019-183-006, and in part by the Open Foundation of State Key Laboratory of Networking and Switching Technology (Beijing University of Posts and Telecommunications) under Grant SKLNST-2021-1-17.

ABSTRACT With the development of artificial intelligence and Internet of Things (IoT), the era of industry 4.0 has come. According to the prediction of IBM, with the continuous popularization of 5G technology, the IoT technology will be more widely used in factories. In recent years, federated learning has become a hot topic for Industrial Internet of Things (IIoT) researchers. However, many devices in the IIoT currently have a problem of low computing power, so these devices cannot perform well facing the tasks of training and updating models in federated learning. In order to solve the above problems, we introduce edge computing into the IIot, so that the device can complete the federated learning operation. In order to ensure the security of data transmission, blockchain is introduced as the main algorithm of equipment authentication in the system. What's more, in order to increase the efficiency and versatility of training model in IIoT, we introduce transfer learning to improve the system performance. The experimental results show that our algorithm can achieve high security and high training accuracy.

INDEX TERMS Federated learning, blockchain, Industrial Internet of Things, transfer learning, Security of Internet of Things.

I. INTRODUCTION

At present, with the rapid development of IoT technology and the arrival of industry 4.0 era, IIoT has begun to enter our production and life [1]. Based on IIoT technology, modern sensors and controllers with sensing and monitoring capabilities can be integrated into the process of industrial production, and then real-time data collection, intelligent analysis and mobile communication can be realized to improve the level of industrial manufacturing, realize the transformation of traditional industrial manufacturing to modernization and intelligence, and achieve a qualitative breakthrough. From the application status of IIoT technology, it shows many advantages, such as security, real-time, automation, embedded, interoperability and interconnection [2].

With the continuous development of artificial intelligence technology in the world, artificial intelligence gives IIoT a broader development space, which is also the development trend of IIoT technology in the future. Based on the technology of IIoT, the robot and automation technology in industrial production will be improved accurately, and the manufacturing factory will eventually develop towards the direction of unmanned factory [2]. As shown in FIGURE 1, it is a schematic diagram of the IIoT. FIGURE 1 is a scene of artificial intelligence learning in three factories. In FIGURE 1, we can see that each time the training is carried out, each factory will transmit its own training data to the cloud server, and then the cloud server will receive The data is trained, and then the training results are distributed to various factories.

The associate editor coordinating the review of this manuscript and approving it for publication was Chi-Yuan Chen.

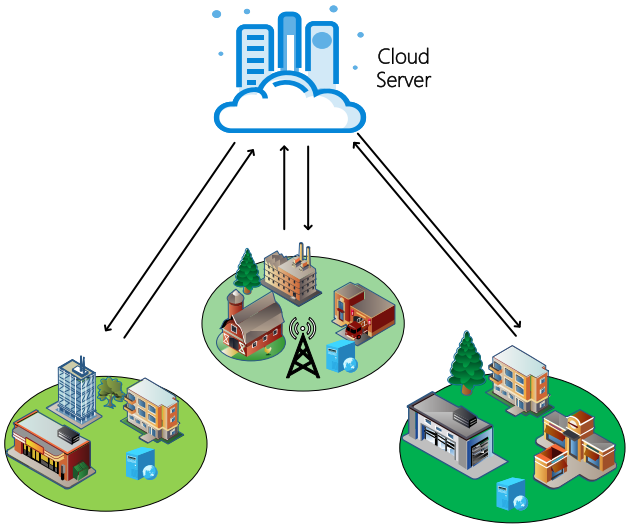

FIGURE 1. Schematic diagram of industrial internet of things.

The traditional machine learning scheme needs to migrate the data collected by each factory from the local equipment to the centralized cloud for training [3]. However, there are still serious problems in transferring data from local devices to centralized cloud. For example, the confidential information of each factory is likely to be leaked to competitors, and the transmission of all data will occupy large bandwidth resources. Therefore, the concept of federated learning is proposed. Federated learning is a new machine learning scheme, which can protect user privacy without transferring data from local devices to centralized cloud. Federated learning shows the viewpoint of distributed learning, rather than collecting the whole data set from users. It enables devices to train models based on local data to protect users' privacy. The global model is updated iteratively by collecting local model updates from the device. Then, the central device feeds back the global model update to the user. This iterative process works until it converges to the accuracy of a global federated learning model [4].

Federated learning has been applied and developed in the IIoT. However, there are still many problems in its application.

1. According to [5], many factories have now applied IoT devices to daily production. But with the development of technology, the performance of these devices will not be able to meet the demands of more and more data processing. However, replacing all of these devices will consume a lot of money.

2. The equipment in the IIoT will generate and process a large amount of data, and it will also make the equipment in the IIoT vulnerable to various attacks [6].

3. In some application scenarios of IIoT, we cannot obtain more scientific and complete data for federated learning, which also makes it difficult for some devices to be intelligent in industrial production. [7].

In the current IIoT environment, the computing power of IoT devices is too low to perform federated learning operation and update model tasks [2]. In order to solve the problem that the IIoT devices cannot optimize the model due to its low computing power, a federated learning mechanism based on edge computing and blockchain is designed in this manuscript to enable multiple factory edge servers to upload parameters and distribute them uniformly after cloud training model. A complete upload training distribution cycle mechanism is formed, which can effectively solve the problem that the fixed effect of the edge model cannot be improved without the user's original data being uploaded.

With the rapid growth of data scale and computing resources, machine learning has made great progress in theory and practice. Traditional machine learning methods usually rely on the basic assumption that the data generation mechanism does not change with the environment. However, in various application fields of machine learning, such as big data analysis, natural language processing, computer vision, bioinformatics, etc., the above assumptions are often difficult to be established because of their strictness. How to analyze and mine large-scale data in non-stationary environment is one of the most challenging frontier directions in modern machine learning [8]. Transfer learning relaxed the constraints that training data and test data must obey independent and distributed constraints in traditional machine learning, so it can mine the unchanging essential features and structures of the domain between two different but interrelated fields, which makes the supervised information such as annotation data can be transferred and reused among the fields. Transfer learning is the basic method to solve the scarcity of target task annotation data, and its research is still in a challenging stage. The purpose of this algorithm is to transfer the existing knowledge to solve the learning problem that there are only a few labeled sample data in the target domain. In the IIoT environment, transfer learning also has a good application prospect. Many training tasks in the IIoT have certain interoperability. If transfer learning is applied to these tasks, it will save a lot of time and computing resources [7].

The essential goal of federated learning is to protect the privacy of users. In the IIoT environment with limited computing power, this paper proposes to transfer the data of low computing power devices to the edge server of the factory intranet for computing. But there is a risk of data leakage in the process of data transmission. Therefore, this paper proposes to use blockchain in data transmission and device verification, so as to ensure that information is not leaked in the process of user data transmission, and user data is only transmitted to specific terminals recognized by users for training.

The main contributions of this manuscript can be highlighted as follows.

1. Aiming at the problem that many devices with low computational power are not suitable for federated learning in IIoT, this manuscript proposes a strategy to submit the data

of low computing power devices to edge computing server in factory intranet for training.

2. In view of the data security problems in the process of data transmission, this manuscript uses blockchain to protect the security of data.

3. This manuscript proposes the combination of federated learning and transfer learning in the IIoT environment to improve the generalization of the training model.

II. RELATED WORKS

A. DEVICE IDENTITY AUTHENTICATION BASED ON BLOCKCHAIN

In recent years, blockchain technology has attracted widespread attention, especially the core supporting technology of the digital cryptocurrency system represented by Bitcoin [9]. The blockchain network provides a ''trustless'' environment where users can conduct transactions without relying on a central trust agency. Currently, blockchain technology has been used in government [10], healthcare [11], digital rights management [12], IoT [13], [14] and other fields. Literature [15] proposed a small decentralized record management system that uses blockchain technology to process EMR. In response to the needs of patients, hospitals and medical researchers, it uses blockchain technology to verify identities, grant permissions, share data and protect privacy. Literature [16] proposed a blockchain-based product ownership management system. Since the forgers cannot prove that they have real products on the system, they cannot clone the real labels. Literature [17] proposed a blockchain-based smart grid data protection system, which uses the features of blockchain to be non-tamperable, traceable and collective maintenance to solve the trust problem between participants on the smart grid. Literature [18] proposed a new automatic food transaction system based on alliance blockchain, which uses alliance blockchain technology to set permissions and authentication for different roles in food transactions to protect the privacy of multiple stakeholders. The above-mentioned studies have proved that the blockchain has good application prospects in data transmission and storage.

Based on the above scheme, this manuscript proposes a secure transmission scheme in the IIoT, which uses the blockchain decentralized architecture to continuously record the transmission data in and out of the node to ensure the security of the data. This solution can realize the identity authentication of IIoT devices and the secure transmission of data, creating conditions for data sharing between devices in federated learning and edge computing.

B. EDGE COMPUTING

In recent years, with the development of sensor technology, electronic technology and industrial automation, most industrial manufacturing processes can be monitored. This also generates a huge amount of data, the complexity of the manufacturing process and the frequency of commercial activities also generate a large amount of data [19]. How to use the data generated in the production process to extract valuable information to improve the production process is the main requirement of intelligent manufacturing, such as fault diagnosis, predictive maintenance and parameter optimization for important equipment [20]–[22]. All intelligent technologies are inseparable from the analysis of data, and data analysis tasks are computationally sensitive tasks that require a lot of computing resources. This is difficult to satisfy in an industrial environment, especially data-driven technology represented by deep learning [23]. Although cloud computing can provide certain computing services remotely, it cannot fully meet industrial needs due to uncertain delays and high communication costs [24]. Therefore, once the concept of edge computing is proposed, it has been widely used in industrial environments [25], [26].

In the industry, edge computing technology has been researched and studied by researchers. Literature [27] outlines the application of edge computing in the IIoT and the possible architecture of the future IIoT. Literature [28] outlines the application, opportunities and challenges of edge computing technology in IIoT under the development of 5G. And came to the view that edge computing technology is an important deployment mode of IIoT in the future. At present, there are few researches on edge computing to provide computing resources for low computing power devices in IIoT.

Based on the above solution, this manuscript proposes to transmit data from low-computing power devices in the IoT to edge computing devices for training and updating. This program improves the efficiency of federated learning and creates excellent conditions for federated learning in the IIoT.

C. TRANSFER LEARNING

In the field of machine learning, traditional machine learning methods are usually limited to solving problems in a single domain, that is, training data and test data are required to obey the same distribution. When the feature distributions of training data and test data are different, it is often necessary to retrain the model on the new data set. However, in practical application, the cost of data reacquisition is very high or sometimes difficult to achieve. It is necessary to transfer useful knowledge learned from the source domain to the target area. Since the rise of transfer learning in 1995, researchers have extended the traditional machine learning methods to the transfer learning, including the transfer learning based on nuclear learning [29]–[34], the transfer learning based on reinforcement learning [35]–[38], the manifold based learning and the deep learning [39]–[42].

At present, transfer learning technology has been widely used, and it is also being integrated with federated learning technology. Based on the above solution, this manuscript proposes an appropriate federated transfer learning method for low performance devices in the IIoT.

III. APPROACH

A. DEVICE IDENTITY AUTHENTICATION BASED ON BLOCKCHAIN

1) BLOCKCHAIN SYSTEM ARCHITECTURE

The IIoT blockchain system designed in this manuscript builds a block network of IIoT devices, edge servers, and cloud servers. In this network, the IoT device node does not undertake data calculation work, we let the existing cloud server be the creation node. We choose the Ripple [43] consensus algorithm as the consensus mechanism. In the blockchain system designed in this manuscript, when a node initiates an application, the billing node will verify the identity of the node and sign it if the verification passes. When the number of signatures in the entire blockchain system is not less than 51% of the total number of summary points in the current blockchain system, the current blockchain system considers that this node has passed the audit of the blockchain system. Otherwise this request will be discarded.

The basic architecture of blockchain is shown in FIGURE 2. Each block refers to the hash of the previous block head and stores it in the linked list to form a blockchain. The block structure includes block head and block body.

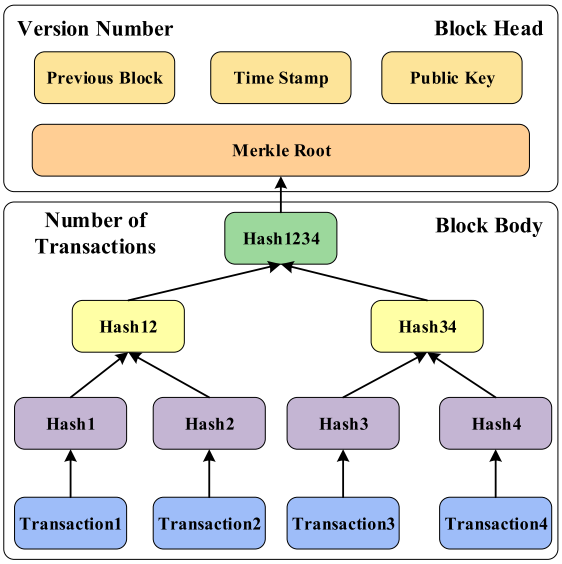

FIGURE 2. The structure of block.

The block header contains the address of the previous block, and its function is to connect the current new block with the previous block. The time stamp indicates the creation time of the block. The Merkle root is generated by the transaction records in the block creation process through the hash process of the Merkle tree. The block body is composed of transactions and the number of transactions. Transaction includes equipment type, data content, data, data generation time, processing node and processing node signature.

2) IDENTITY AUTHENTICATION PROCESS

The main allocation schemes of traditional PKI authentication technology can be divided into centralization and decentralization. The centralized key distribution scheme can be understood as one of the trusted central nodes generating keys and distributing them to the communication parties. Its main function is to issue and manage digital certificate [44].

The IIoT device authentication scheme designed in this manuscript can be improved by the above centralized key distribution scheme. We use the cloud server as the key distribution center through the consensus mechanism to distribute and manage the secret key. We can take a registration process as an example. First of all, IoT devices apply to the cloud server for registration. The cloud server checks the identity of the IoT devices through the consensus mechanism. After the approval, the cloud server will generate a digital certificate containing the public key of the current device and record it into its own account book. Then the cloud server will send the information of the device to other nodes in the blockchain. Other nodes only need to verify the validity of the certificate to know the validity of the current record. After verification, other nodes will record the information in their own account book.

B. EDGE COMPUTING

In this manuscript, for the lack of computing power in the IIoT, the edge computing method is used to solve the problem [45], [46]. In the design of this manuscript, each factory will be equipped with its own edge server. When training is needed, the device uploads its own data and its own device number to the edge server in batches. The edge server sorts all data using Quicksort, compares the data after sorting, and deletes duplicate data. After the edge server has trained the data transmitted by the device, the edge server will combine the model of the same type of equipment in the current factory into a model for training. Finally, the combined training model is uploaded to the cloud server, and the model returned by the cloud server is distributed to the devices.

In this scheme, the edge computing device is located in the factory intranet to ensure the privacy and security of data. In addition, after the edge computing equipment merges and updates the model of the same type of equipment in factory, it can greatly reduce the occupation of public network bandwidth and improve the efficiency of federated learning.

C. FEDERATED TRANSFER LEARNING

We designed a model training framework for federated transfer learning for the scene of IIoT. A common method of unsupervised domain adaptive is to divide the model into two parts: feature extractor and classifier. Feature extractor is used to map data to feature space, and classifier classifies data based on features. In order to achieve better results in the target domain, the distribution difference between source and target regions in feature space need to be reduced. In our framework, in order to measure the difference of the distribution, the alignment loss function is the Maximum Mean Difference (MMD), which is also a common alignment loss function in unsupervised domain adaptation. The training

process of unsupervised domain adaptive training is usually divided into two parts: pretraining and fine tuning. Our framework adopts the same model division method and training process. First, the feature extractor and classifier are pretrained in the source domain; then the source domain sends the weight of the feature extractor to the target domain, and prepares for the fine tuning stage of the cooperation between the two. In the fine tuning stage, the processing of each batch of data can be divided into four steps: feedforward, classification loss function and gradient calculation, MMD loss function and gradient calculation, model parameter updating. The first, second and fourth steps are simple, and the source and target fields can be operated independently without data exchange. Step 3 is the most complex and requires a lot of interaction.

The MMD loss function is defined as:

$$L_{\mathrm{MMD}} = \frac{1}{n_1 (n_1 - 1)} \sum_{i=1}^{n_1} \sum_{i \neq i} k\left(v_i, v_{i'}\right) + \frac{1}{n_2 (n_2 - 1)} \sum_{j=1}^{n_2} \sum_{j \neq j} k\left(v'_j, v'_{j'}\right) - \frac{2}{n_1 n_2} \sum_{i=1}^{n_1} \sum_{j=1}^{n_2} k\left(v_i, v'_j\right),$$

where $k\left(v, v'\right) = \exp\left(-\alpha \left\| v - v' \right\|^2\right)$ is a kernel function. The loss function can be regarded as the sum of three parts. Assuming that v_i and v'_j are the eigenvectors of the source domain and the target domain respectively, the first part of the loss function can be calculated independently, and the second part of the loss function can be calculated independently. The third part needs to use the data of two domains. Therefore, one party needs to encrypt the data and send it to the other party. In order to operate on ciphertext, our framework adopts the Paillier homomorphic encryption algorithm. In addition, the Paillier encryption algorithm does not support exponential function operation, so we carry out Taylor expansion on the exponential function in the kernel function and transform it into polynomial function approximately. The approximate transformed monokernel function can be expressed as:

$$k\left(v, v'\right) = \sum c_m f_m(v) g_m\left(v'\right),$$

In this formula, c_m is a constant, $f_m(v)$ is constant 1 or a polynomial composed of vector elements, $g_m\left(v'\right)$ and $f_m(v)$ have the same meaning. Therefore, in order to calculate Part 3, one party needs to send all FM (V) of each eigenvector to the other party.

For the calculation of MMD gradient of two domains, we take the target domain as an example. For this domain, the gradient of the first part of MMD loss function is 0, and the gradient of the second part can be calculated independently. For the third part, the gradient is actually the sum of the gradients of each kernel function, and the gradient of a single kernel function can be expressed as:

$$\frac{\partial k\left(v, v'\right)}{\partial \theta} = \sum_m c_m f_m(v) \frac{\partial g_m\left(v'\right)}{\partial \theta}.$$

Therefore, similar to the calculation of the loss function in the third part, the calculation of the gradient in the third part also requires the other party (in this case, the source domain) to send all $f_m(v)$ of each eigenvector to the other party.

The detailed steps of Federated transfer learning algorithm are illustrated in Algorithm 1.

Algorithm 1 Federated Transfer Learning Algorithm for IIoT Devices With Low Computing Power Based on Blockchain and Edge Computin

Require: Data generated by each terminal device.

1: **for** Before the trained model is optimal **do**
2: Each terminal device transmits data to the edge server;
3: Edge server deduplication;
4: Edge server training model;
5: Each edge server uploads the trained model to the cloud server;
6: The cloud server aggregates the models uploaded by the edge server;
7: The cloud server transmits the aggregated model to the edge server;
8: The edge server transmits the model to the device;
9: **return** Trained model.

IV. EXPERIMENTS

In this section, we conducted three experiments to verify the security of the blockchain authentication system, the accuracy of federated learning and the accuracy of transfer learning.

A. THE EXPERIMENT OF DEVICE IDENTITY AUTHENTICATION BASED ON BLOCKCHAIN

In this part, in order to verify the security of the algorithm proposed in this manuscript, we mainly carry out the following experiments.

1) NETWORK TRAFFIC TEST

The purpose of network traffic test is to test the difference of network traffic between the protocol and the wireless access point without authentication, so as to measure the increase of network traffic pressure caused by the protocol. Network traffic test uses iftop to test network traffic, compares the query requests sent directly to the blockchain with the request traffic certified by this protocol, constantly changes the query per second (QPS) and calculates the network traffic utilization. In order to respond to the request timely and measure the impact on the network more accurately, the number of randomly selected service nodes is 1. In this case, there is no need to run consensus protocol.

The network traffic test results are shown in Table 1. The observation results show that the impact of this scheme on the network traffic is one thousandth, and the impact on the network performance of the program is negligible.

TABLE 1. Network traffic test results.

QPS	Direct Query Traffic	Encrypted Authentication Traffic	Traffic Utilization
	MB/s	MB/s	%
1	1.000	1.000	100.00
2	2.000	2.001	99.95
5	5.000	5.002	99.96
10	10.001	10.005	99.96
20	20.002	20.011	99.96

2) SECURITY ANALYSIS

Test the camouflage attack: using the private key that does not match the user's address to sign the packet, and then send it to the wireless access point. The access point successfully discards the packet.

Testing forgery attacks:For man-in-the-middle and unauthenticated attacks, this solution relies on digital signature technology to effectively prevent it at all stages. Since the attacker cannot pass the consensus authentication, he cannot join the blockchain, let alone create a request transaction.

Test the replay attack: the same packet is sent to the wireless access point twice, and the wireless access point only makes one request to the blockchain.

For denial of service attacks, the algorithm proposed in this paper can ensure that users and wireless access points cannot manipulate the nodes participating in consensus verification, so that the verification traffic cannot be concentrated on a few nodes, and the denial of service attacks are limited to a certain extent.

To sum up, this scheme can ensure the security of blockchain system, wireless access point and users, and has certain scaling ability, which can balance security and performance.

B. THE EXPERIMENT OF FEDERATED LEARNING

1) USE CASE

The experimental sample data used in this paper is the connection information of network data in the 1999 KDD (knowledge discovery in databases) competition in data mining and network intrusion detection. The data format of KDD99 data set is based on DARPA intrusion detection and evaluation project jointly initiated and conducted by research and projects agency of the US Department of defense and Lincoln Laboratory of Massachusetts Institute of technology in 1998. This batch of data records about 5 million network traffic and connection information in 9 weeks in the simulated network environment of the US air force, including a large amount of normal data and 39 attack connections. Although KDD99 data was collected many years ago, it is still a set of standard data for network security domain research in recent years because of its comprehensive record information and large amount of data. [47] The data set used in this experiment is shown in the following table, which lists the various types of attacks in this experiment and the proportions of various types of attacks in each device.

TABLE 2. Intrusion detection experimental data.

Attack Type	Specific type	Percentage			
		Device1	Device2	Device3	Device4
Normal	normal	20%	18%	16%	21%
Dos	back,land,neptune pod,smurf,teardrop	44%	45%	47%	43%
R2L	ftp_write,guess_password imap,phf,spy,warezclient multihop,warezmaster	20%	19%	19%	22%
U2R	buffer_overflow,loadmodule perl,rootkit	6%	9%	7%	7%
Probe	ipsweep,nmap portsweep,satan	10%	9%	11%	7%

2) EXPERIMENTAL ENVIRONMENT

This manuscript uses multi-client method to test federated learning, and four terminals and one cloud server are set up in the system. Each terminal has 10% of the randomly extracted KDD99 data and ensures that the data stored by four terminals is basically different.

In this experiment, in order to verify the accuracy of our federated learning based on edge computing, we compare the proposed algorithm with CSE and GRAE and FedAvg. In the experiment, the local update of FedAvg algorithm is carried out on the low computing power device (low performance development board), and the machine learning algorithm CSE and GRAE algorithm use the same data set as each device, but only local training, not online update.

3) EXPERIMENTAL RESULT

In 100 rounds of training, we use the common centralized machine learning algorithm CSE and GRAE and the FedAvg to compare with the algorithm proposed in this manuscript. The training mode of FedAvg algorithm is to train directly in local low-performance equipment and then send the training model to the cloud server for joint training, and then the cloud server will feedback the training results to the equipment. The experiment of the algorithm proposed in this manuscript is that the local equipment sends the training data to the edge equipment, the edge equipment sends the training results to the cloud server, and the cloud server sends the results of the joint training to the edge equipment. Then, we tested the experimental results using the same test data set.

The experimental results are shown in FIGURE 3. For example, in FIGURE 3, Device1 represents the accuracy of all the algorithms which were trained and tested based on Device1 dataset. The accuracy of the models tested on clients differs from each other because the data distribution of the respective clients are different. Specifically, for the KDD99 data set, the accuracy rate of testing on Device3 is the best, after 100 rounds of training, the accuracy of the algorithm proposed in this paper can reach more than 99%. While the accuracy rate of federated learning performed on Device4 is the worst. In addition, we also find that the

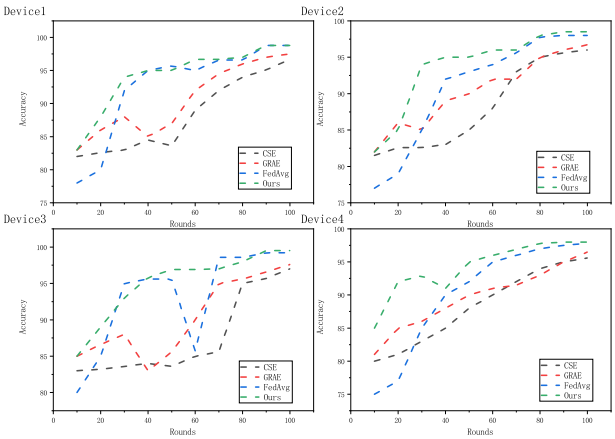

FIGURE 3. The accuracy of each device.

TABLE 3. Confusion matrix for binary classification problems.

two-objective confusion matrix		true value	
		Positive	Negative
predicted value	Positive	TP	FP
	Negative	FN	TN

federated learning approach proposed in this paper performs best in all types of learning. This should be mainly due to the general centralized learning method cannot update the model well, limited by the limited training data set, cannot produce good results. On the other hand, the standard federated learning method is limited by the limited computing power of the device in the environment described in this manuscript, which may have a negative impact on the model and affect the accuracy of the model.

In addition to accuracy, we also measured three other metrics in the experiments, including precision, recall, and F1-Score. These criteria are useful for class wise evaluation of the output of classifier. The precision, recall and F1-Score can be obtained using the following formulas:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN},$$

$$\text{Precision} = \frac{TP}{TP + FP},$$

$$\text{Recall} = \frac{TP}{TP + FN},$$

$$F1 - \text{Score} = \frac{2 * \text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}},$$

The results are illustrated in FIGURE 4. The results show that the proposed federated learning method performed best on Device3, which is similar to the results of accuracy tests. Compared with the standard federated learning method, the proposed federated learning method shows an improvement in FIGURE 4.

In conclusion, the proposed federated learning algorithm achieves higher accuracy than other algorithms. The feasibility of low computing power devices participating in federated learning in IIoT is verified.

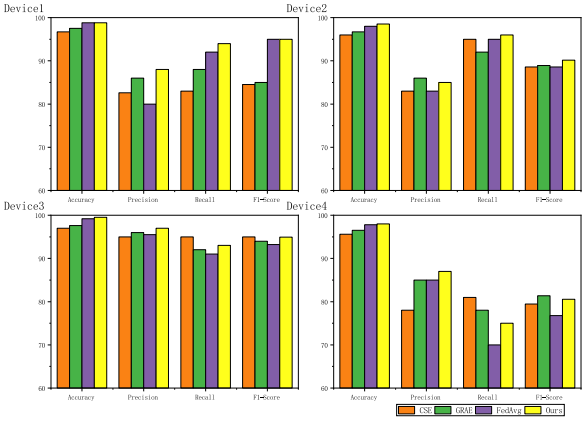

FIGURE 4. The precision, recall, and F1-score of each device.

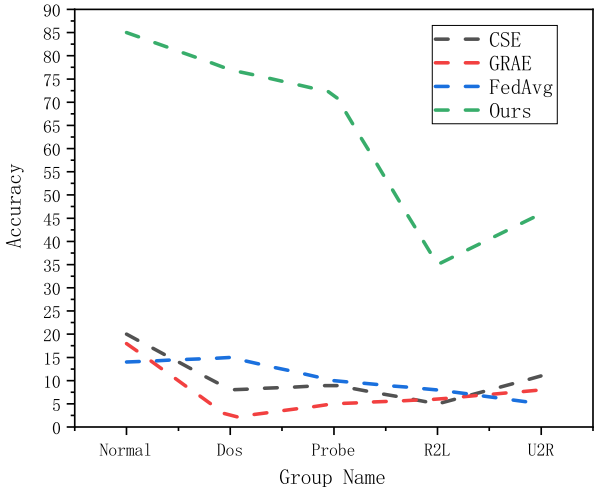

FIGURE 5. The accuracy of each algorithm.

C. THE EXPERIMENT OF TRANSFER LEARNING

In this section, we focus on testing the performance of the transfer learning algorithm proposed in this manuscript. Similar to the previous section, this section still uses the KDD99 data set to test the results. However, different from the previous section, we have different data sets for each device. In this part, we divide the 10% KDD99 dataset into five parts: Normal, DOS, Probe, R2L and U2R, and place them on different nodes. Then the algorithm is trained and tested by using the test data described in the previous section.

The results of several algorithms for the environment described in this manuscript are shown in FIGURE 5 and FIGURE 6. This manuscript mainly lists the accuracy and F1- score of several algorithms. As can be seen from the above two figures, for the Normal, Dos and Probe parts of KDD99 dataset, the accuracy of our algorithm can reach more than 70%, which is far higher than the other three algorithms. Although the accuracy of R2L and U2R parts is not high, it is also far higher than other algorithms. Similarly, the results of the F1-score of the algorithms in FIGURE 6 are similar to this conclusion. From the test results, the algorithm described in this manuscript achieves better transfer learning accuracy. However, the algorithm for R2L and U2R training results of

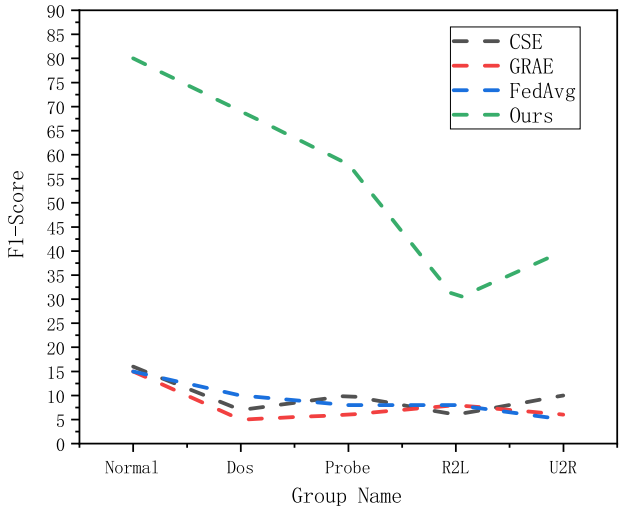

FIGURE 6. The F1-score of each algorithm.

the transfer has no good effect. But in general, the algorithm proposed in this manuscript solves the problem that some scenes in the IIoT lack complete data sets.

V. CONCLUSION AND FUTURE WORKS

This manuscript aims at the problem that the devices in the IIoT are too low to complete the task of model updating in federated learning. This manuscript proposes the use of edge learning to solve the problem of insufficient computing power of devices. At the same time, we also use blockchain technology, and use transfer learning technology to improve the overall performance of the IIoT system. Through experiments, we verify the security and accuracy of our proposed algorithm.

In the current industrial environment, artificial intelligence and IoT will be the future development direction. The algorithm proposed in this paper solves some problems, but there are still some problems need to be improved, such as the accuracy of transfer learning is still not high, the encryption and decryption of data transmission will still consume resources and so on. This is also our future research direction, and we hope that we can have better solutions to these problems.

REFERENCES

[1] P. Zhang, C. Wang, C. Jiang, and Z. Han, "Deep reinforcement learning assisted federated learning algorithm for data management of IIoT," *IEEE Trans. Ind. Informat.*, early access, Mar. 8, 2021, doi: 10.1109/TII.2021.3064351.

[2] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, opportunities, and directions," *IEEE Trans. Ind. Informat.*, vol. 14, no. 11, pp. 4724–4734, Nov. 2018.

[3] G. Carleo, I. Cirac, K. Cranmer, L. Daudet, M. Schuld, N. Tishby, L. Vogt-Maranto, and L. Zdeborová, "Machine learning and the physical sciences," *Rev. Mod. Phys.*, vol. 91, no. 4, 2019, Art. no. 045002.

[4] K. Bonawitz, H. Eichner, W. Grieskamp, D. Huba, A. Ingerman, V. Ivanov, C. Kiddon, J. Konečný, S. Mazzocchi, H. B. McMahan, T. Van Overveldt, D. Petrou, D. Ramage, and J. Roselander, "Towards federated learning at scale: System design," 2019, *arXiv:1902.01046*. [Online]. Available: http://arxiv.org/abs/1902.01046

[5] L. D. Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[6] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in *Proc. 52nd ACM/EDAC/IEEE Annu. Design Autom. Conf. (DAC)*, Jun. 2015, pp. 1–6.

[7] K. Kaur, S. Guo, M. Chen, and D. Rawat, "Transfer learning for 5G-aided industrial Internet of Things," *IEEE Trans. Ind. Informat.*, early access, Apr. 6, 2021, doi: 10.1109/TII.2021.3071310.

[8] M. I. Jordan and T. M. Mitchell, "Machine learning: Trends, perspectives, and prospects," *Science*, vol. 349, no. 6245, pp. 255–260, 2015.

[9] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*. Austin, TX, USA: Satoshi Nakamoto Institute, Apr. 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[10] M. Jun, "Blockchain government—A next form of infrastructure for the twenty-first century," *J. Open Innovation: Technol., Market, Complex.*, vol. 4, no. 1, Dec. 2018.

[11] M. Hölbl, M. Kompara, A. Kamišalić, and L. N. Zlatolas, "A systematic review of the use of blockchain in healthcare," *Symmetry*, vol. 10, no. 10, p. 470, 2018.

[12] Z. Zhang and L. Zhao, "A design of digital rights management mechanism based on blockchain technology," in *Proc. Int. Conf. Blockchain*. Seattle, WA, USA: Springer, 2018, pp. 32–46.

[13] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018.

[14] B. Yu, J. Wright, S. Nepal, L. Zhu, J. Liu, and R. Ranjan, "IoTChain: Establishing trust in the Internet of Things ecosystem using blockchain," *IEEE Cloud Comput.*, vol. 5, no. 4, pp. 12–23, Jul./Aug. 2018.

[15] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, Aug. 2016, pp. 25–30.

[16] K. Toyod, P. T. Mathiopoulo, I. Sasase, and T. Ohtsuk, "A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain," *IEEE Access*, vol. 5, pp. 17465–17477, 2017.

[17] J. Gao, K. O. Asamoah, E. B. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, and G. Dong, "GridMonitoring: Secured sovereign blockchain based monitoring on smart grid," *IEEE Access*, vol. 6, pp. 9917–9925, 2018.

[18] D. Mao, Z. Hao, F. Wang, and H. Li, "Novel automatic food trading system using consortium blockchain," *Arabian J. Sci. Eng.*, vol. 44, no. 4, pp. 3439–3455, 2019.

[19] D. Serpanos and M. Wolf, "Industrial Internet of Things," in *Internet-of-Things (IoT) Systems*. Cham, Switzerland: Springer, 2018, pp. 37–54.

[20] J. Zhou, P. Li, Y. Zhou, B. Wang, J. Zang, and L. Meng, "Toward new-generation intelligent manufacturing," *Engineering*, vol. 4, no. 1, pp. 11–20, 2018.

[21] L. Zhang, L. Zhou, L. Ren, and Y. Laili, "Modeling and simulation in intelligent manufacturing," *Comput. Ind.*, vol. 112, Nov. 2019, Art. no. 103123.

[22] B. He and K.-J. Bai, "Digital twin-based sustainable intelligent manufacturing: A review," *Adv. Manuf.*, vol. 9, no. 1, pp. 1–21, Mar. 2021.

[23] S. Marsland, *Machine Learning: An Algorithmic Perspective*. Boca Raton, FL, USA: CRC Press, 2015.

[24] V. K. Reddy, B. T. Rao, and L. Reddy, "Research issues in cloud computing," *Global J. Comput. Sci. Technol.*, vol. 11, no. 11, pp. 1–8, 2011.

[25] B.-G. Chun, S. Ihm, P. Maniatis, M. Naik, and A. Patti, "CloneCloud: Elastic execution between mobile device and cloud," in *Proc. 6th Conf. Comput. Syst.*, 2011, pp. 301–314.

[26] K. Ha, Z. Chen, W. Hu, W. Richter, P. Pillai, and M. Satyanarayanan, "Towards wearable cognitive assistance," in *Proc. 12th Annu. Int. Conf. Mobile Syst., Appl., Services*, Jun. 2014, pp. 68–81.

[27] T. Qiu, J. Chi, X. Zhou, Z. Ning, M. Atiquzzaman, and D. O. Wu, "Edge computing in industrial Internet of Things: Architecture, advances and challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2462–2488, 4th Quart., 2020.

[28] A. Narayanan, A. S. D. Sena, D. Gutierrez-Rojas, D. C. Melgarejo, H. M. Hussain, M. Ullah, S. Bayhan, and P. H. J. Nardelli, "Key advances in pervasive edge computing for industrial Internet of Things in 5G and beyond," *IEEE Access*, vol. 8, pp. 206734–206754, 2020.

[29] Z. Ming and J. Ren, "Domain transfer dimensionality reduction via discriminant kernel learning," in *Proc. Pacific–Asia Conf. Adv. Knowl. Discovery Data Mining*, 2012, pp. 280–291.

[30] X. Liao, Y. Xue, and L. Carin, "Logistic regression with an auxiliary data source," in *Proc. 22nd Int. Conf. Mach. Learn.*, 2005, pp. 505–512.

[31] Y. Yao and G. Doretto, "Boosting for transfer learning with multiple sources," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, Jun. 2010, pp. 1855–1862.

[32] J. Jiang and C. Zhai, "Instance weighting for domain adaptation in NLP," in *Proc. 45th Annu. Meeting Assoc. Comput. Linguistics*. Stroudsburg, PA, USA: ACL, 2007, pp. 264–271.
[33] S.-I. Lee, V. Chatalbashev, D. Vickrey, and D. Koller, "Learning a meta-level prior for feature relevance from multiple related tasks," in *Proc. 24th Int. Conf. Mach. Learn.*, 2007, pp. 489–496.
[34] N. D. Lawrence and J. C. Platt, "Learning to learn with the informative vector machine," in *Proc. 21st Int. Conf. Mach. Learn.*, 2004, p. 65.
[35] M. E. Taylor, G. Kuhlmann, and P. Stone, "Autonomous transfer for reinforcement learning," in *Proc. Auton. Agents Multi-Agent Syst. Conf.*, 2008, pp. 1–8.
[36] Z. Wang, Y. Song, and C. Zhang, "Transferred dimensionality reduction," in *Proc. Joint Eur. Conf. Mach. Learn. Knowl. Discovery Databases*. Berlin, Germany: Springer, 2008, pp. 550–565.
[37] W. Fengmei, Z. Jianpei, C. Yan, and Y. Jing, "FSFP: Transfer learning from long texts to the short," *Appl. Math. Inf. Sci.*, vol. 8, no. 4, pp. 2033–2040, 2014.
[38] X. Shi, F. Wei, and J. Ren, "Actively transfer domain knowledge," in *Proc. Joint Eur. Conf. Mach. Learn. Knowl. Discovery Databases (ECML/PKDD)*, Antwerp, Belgium, Sep. 2008, pp. 342–357.
[39] B. Cheng, M. Liu, H. I. Suk, D. Shen, and D. Zhang, "Multimodal manifold-regularized transfer learning for MCI conversion prediction," *Brain Imag. Behav.*, vol. 9, no. 4, pp. 913–926, 2015.
[40] M. Long, J. Wang, Y. Cao, J. Sun, and S. Y. Philip, "Deep learning of transferable representation for scalable domain adaptation," *IEEE Trans. Knowl. Data Eng.*, vol. 28, no. 8, pp. 2027–2040, Aug. 2016.
[41] F. Zhuang, P. Luo, Q. He, and Z. Shi, "Inductive transfer learning for unlabeled target-domain via hybrid regularization," *Chin. Sci. Bull.*, vol. 54, no. 14, pp. 2470–2478, 2009.
[42] M. Belkin, P. Niyogi, and V. Sindhwani, "Manifold regularization: A geometric framework for learning from labeled and unlabeled examples," *J. Mach. Learn. Res.*, vol. 7, pp. 2399–2434, Nov. 2006.
[43] D. Schwartz, N. Youngs, and A. Britto, "The ripple protocol consensus algorithm," *Ripple Labs Inc White Paper*, vol. 5, no. 8, p. 151, 2014.
[44] P. Zhang, X. Pang, N. Kumar, G. S. Aujla, and H. Cao, "A reliable data-transmission mechanism using blockchain in edge computing scenarios," *IEEE Internet Things J.*, early access, Sep. 3, 2020, doi: 10.1109/JIOT.2020.3021457.
[45] P. Zhang, C. Jiang, X. Pang, and Y. Qian, "STEC-IoT: A security tactic by virtualizing edge computing on IoT," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2459–2467, 2020.
[46] M. Satyanarayanan, "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30–39, 2017.
[47] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Proc. IEEE Symp. Comput. Intell. Secur. Defense Appl.*, Jul. 2009, pp. 1–6.

PEIYING ZHANG received the Ph.D. degree from the School of Information and Communication Engineering, University of Beijing University of Posts and Telecommunications, in 2019. He is currently an Associate Professor with the College of Computer Science and Technology, China University of Petroleum (East China), and also with the State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications. He has been published multiple IEEE/ACM transactions/journal/magazine articles since 2016, such as IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS (TII), IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS (T-ITS), IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY (TVT), IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING (TNSE), IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT (TNSM), IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING (TETC), IEEE NETWORK, IEEE ACCESS, IEEE INTERNET OF THINGS JOURNAL (IoT-J), *ACM TALLIP*, *Computer Communications*, and *IEEE Communications Magazine*. His research interests include semantic computing, future Internet architecture, network virtualization, and artificial intelligence for networking. He served as the Technical Program Committee of ISCIT 2016, ISCIT 2017, ISCIT 2018, ISCIT 2019, Globecom 2019, COMNETSAT 2020, SoftIoT 2021, CBIoT 2021, IWCMC-Satellite 2019, and IWCMC-Satellite 2020.

HAO SUN is currently a Graduate Student with the College of Computer Science and Technology, China University of Petroleum (East China). His research interests include artificial intelligence and the Internet of Things.

JINGYI SITU received the Bachelor of Science degree in management information system from the Capital University of Economics and Business, Beijing, China, and the Master of Science degree in cybersecurity from Northeastern University, Boston. She is currently a Senior Security and a Privacy Consultant with Protiviti, Beijing, with two years of working and research experience on IT security in China and USA, where she focusing on security operation, security incident investigation and response, security risk assessment, and information security audit. She actively participated and gained excellent results as top 7% in various national cybersecurity competitions and innovation programs in USA, such as National Cyber League, CTF, and MITRE Embedded CTF. Her research interests include data privacy, system and network security, and security governance.

CHUNXIAO JIANG (Senior Member, IEEE) received the B.S. degree (Hons.) in information engineering from Beihang University, Beijing, China, in 2008, and the Ph.D. degree (Hons.) in electronic engineering from Tsinghua University, Beijing, in 2013. He is currently an Associate Professor with the School of Information Science and Technology, Tsinghua University. His research interests include application of game theory, optimization, and statistical theories to communication, networking, and resource allocation problems, in particular space networks and heterogeneous networks. He has also served as a member for the technical program committee and the symposium chair for a number of international conferences. He has served as an Editor for IEEE INTERNET OF THINGS JOURNAL, IEEE NETWORK, and IEEE COMMUNICATIONS LETTERS; and a Guest Editor for *IEEE Communications Magazine*, IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, and IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING.

DONGLIANG XIE (Member, IEEE) received the Ph.D. degree from the Beijing Institute of Technology, Beijing, China, in 2002. He was a Visiting Researcher with the Department of Electrical and Computer Engineering, State University of New York at Stony Brook. He is currently a Full Professor with the State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing. His research interests include resource-constrained wireless communication and information-centric networks, including architecture of ubiquitous and heterogeneous networks, complex network analysis, and content retrieval and service management.