BlockFedML: Blockchained Federated Machine Learning Systems

Shufen Wang
College of Information Engineering
Harbin Institute of Petroleum
Harbin, China
58439782@qq.com

***Abstract*—With the emphasis on security and privacy, Federated Machine Learning (FML) systems have become a research hotspot due to it can perform machine learning models without compromising security and privacy. However, there are two crucial challenges. One is a gradient information leak, and the other is vulnerable to integrity attacks. In this paper, we proposed a Blockchained Federated Machine Learning System, which called "BlockFedML." In BlockFedML, we develop Security Parameter Aggregation Mechanisms, Checkpoint based- Smart Contracts, Incentive Mechanisms, and Transfer Learning. Finally, we outlined the BlockFedML system and its applications and explained our future work.**

Keywords—security and privacy, machine learning, federated learning, blockchain

I. INTRODUCTION

With the improvement of data storage technology and computing power, machine learning (ML) models have achieved unprecedented accuracy in various tasks, e.g., disease prediction [1], image recognition [2], machine translation [3] and speech recognition [4]. However, there are two critical challenges. One is that user data usually exists in the form of "isolated islands," which makes it difficult for ML models to perform parameter aggregation. The other is the strengthening of data privacy and security.

To address the above challenges, Qiang et al. [5] developed a federated machine learning (FedML) framework, which is a new distributed security architecture. FedML is a distributed ML paradigm that has been designed to perform ML models without compromising privacy and security. Therefore, FedML has recently become a research hot-spot and has attracted the attention of many researchers.

This FedML framework, however, cannot protect the privacy of the training data, even the training data is divided and stored separately. The FedML framework is vulnerable to privacy and integrity attacks. Firstly, some researchers have shown that because the intermediate gradient contains rich semantic information, meaningful information about training data can be inferred through reverse engineering [6]. Secondly, D. Harris et al. [7] pointed out that the potential problem was that the ML model would be "poisoned" if the local device submitted "error data".

We propose a possible solution to these problems: BlockFedML: Blockchained Federated Machine Learning Platform. The long-term goal of this research is to develop a system called "BlockFedML," which is a privacy-preserving federated machine learning system based on smart contracts and incentive mechanisms. Specifically, we are addressing these problems using blockchain and smart contract technology. The critical contributions of our paper are as follows.

- Using blockchain to create an immutable audit trail for FedML for more significant trustworthiness in tracking and proving provenance.
- Enhancing encryption and communication strategies between nodes and the FedML to maintain better privacy preservation.
- Demonstrating the use of smart contracts and incentive mechanism for governing the business logic of a FedML platform.

II. RELATED WORK

A. Security and Privacy in Machine Learning

Shokri & Shmatikov et al. [8] first proposed a distributed global neural network model with a privacy-preserving purpose. The author provides a jointly learning model based on a multi-agent system. More specifically, they allow multi-agents participating in the framework to update global models based on their local training. Martín Abadi et al. [9] developed new algorithmic techniques for ML and accurate analysis of privacy costs within differential privacy (DP) framework.

B. Federated Learning

Federated Learning (FL) is an emerging artificial intelligence underlying technology. Google first proposed it in 2016. It was originally used to solve the problem of locally updating models of Android mobile phone end users. Its design goal is to guarantee big data. Under the premise of information security, protecting the privacy of terminal data and personal data, and ensuring legal compliance, develop efficient machine learning between multiple participants or multiple computing nodes.

Among them, the machine learning algorithms that can be used for federal learning are not limited to neural networks, but also include important algorithms such as random forests.

Federated learning is expected to become the basis for the next generation of artificial intelligence, collaborative algorithms, and networks. Qiang et al. [5] proposed a FedML

0-7695-6728-2/19/$31.00 ©2019 IEEE
DOI 10.1109/ICICAS48597.2019.00162

framework that can run ML models without compromising privacy and security.

C. Blockchain

The blockchain originated from Satoshi Nakamoto's Bitcoin. As the underlying technology of Bitcoin, it is essentially a decentralized database [20]. Refers to the technical solution of collectively maintaining a reliable database through decentralization and distrust [21]-[23]. Blockchain technology is a technological solution that does not rely on third parties to store, verify, transfer, and communicate network data through its own distributed nodes. Therefore, from the perspective of financial accounting, some people regard the blockchain technology as a distributed and open decentralized large-scale network bookkeeping book [24]-[27]. Anyone can use the same technical standard to add their information at any time. The blockchain continues to meet the data entry needs brought about by various needs. In simple terms, blockchain technology refers to a way for people to participate in bookkeeping. There is a database behind all the systems; you can think of the database as a big ledger. Then it becomes essential who keeps this ledger. At present, it is the system whose accounts are kept. The account of WeChat is kept by Tencent, and Ali keeps the account of Taobao. But now, in the blockchain system, everyone in the system can have the opportunity to participate in bookkeeping. If there is any data change within a specified period, everyone in the system can come to bookkeeping. The system will judge the person who records the fastest and best time during this period, write his recorded content to the ledger, and write this Within a certain period of time, the contents of the ledger are sent to all others in the system for backup. In this way, everyone in the system has a complete ledger. In this way, we call it blockchain technology. Chen et al. [12] propose a framework called “LearningChain" to preserve the user’s privacy by applying a decentralized version of the Stochastic Gradient Descent (SGD) algorithm and a DP mechanism. Zhu et al. [13] develop a blockchain-based privacy-preserving framework to secure the share of updates in FedML. This framework uses blockchain trading mechanisms to ensure the security of sharing and updating changes. The two core technologies in the blockchain are smart contracts and incentive mechanisms. However, few researchers currently apply the smart contracts and incentive mechanism to FL.

III. METHODOLOGY

A. Federated Machine Learning

FedML is a collaborative ML framework without centralized training data. In the FedML framework, all the training data remains on the local device, and no individual updates are stored in the cloud. To be more specific, the FedML problem involves learning a single, global predicted model from the database stored in dozens to hundreds of organizations [15, 16].

Our goal is to learn this model under the constraints of local storage and processing of data collected by devices in the organization, with a secure parameter aggregation mechanism. Generally, we aim to minimize the objective function as follows:

$$\min_{\omega} f(\omega), where\ f(\omega) := \sum_{i=1}^{m} p_i F_i(\omega) \quad (1)$$

where m is the total number of devices, $p_i \geq 0$, $\sum_i p_i = 1$, and $F_i(\cdot)$ is the local objective function for the i-th device.

B. Smart Contracts

Smart contractz (SCs) is a computer protocol designed to propagate, verify, or execute contracts in an informational manner. Smart contracts allow trusted transactions to be made without third parties, which are traceable and irreversible. The smart contract concept was first proposed by Nick Szabo in 1995. The purpose of smart contracts is to provide a secure method that is superior to traditional contracts and reduce other transaction costs associated with the contract.

The simple understanding of smart contracts is to describe the contract with some code, that is, the execution rules of the machine.

This rule is a program recognized by many parties that runs on the blockchain and can automatically process algorithms according to preset conditions. Its biggest essence is to use program algorithms instead of thinking of arbitration and execution of contracts. Smart contracts have three characteristics : Data is transparent, immutable, and permanently operational.

Data transparency, that is to say, its code and its data processing are public. Because all the code of the blockchain is public, the code of the smart contract must also be public, and any party can view its processing of the data.

All data of the blockchain itself cannot be tampered with. Since all data of the blockchain cannot be tampered with, the code of the smart contract is also tamperable.

Changes in data will inevitably be caused, and the blockchain is distributed, so nodes running smart contracts need not worry about other nodes being maliciously modified code and data.

There are often tens of thousands of nodes that support the blockchain. The failure of some nodes will not lead to the failure of smart contracts. The reliability is theoretically close to permanent operation. This ensures that smart contracts run permanently like paper.

C. Incentive Mechanisms

Incentive mechanisms (IM) encourage contributors to submit good data that will improve the model’s accuracy. The incentive mechanism is divided into three phases: the initialization phase, the contribution phase, and the reward/punishment phase. In the initialization phase, the FedML proposes a baseline with no financial incentives in any form with the goal of reducing the barrier to entry [17]. In the contribution phase, each party follows its SCs to upload its contributions, such as labels, datasets, and so on. In the reward/punishment phase, each party selects a training round to participate in the training. If the accuracy of the model is improved, the party is awarded; otherwise the party is punished.

IV. Current Solution

The long-term goal of this research is to develop a platform called "BlockFedML," which is a privacy-preserving federated machine learning platform based on smart contracts and incentive mechanisms. BlockFedML is defined as an intelligent platform that runs ML models without compromising privacy and security. The objective of the current study is to solve the FL framework with two challenges: one is the possibility of leakage of gradient information, and the other is that the FL framework is vulnerable to "poisoning" attacks.

A. Gradient Information Leakage

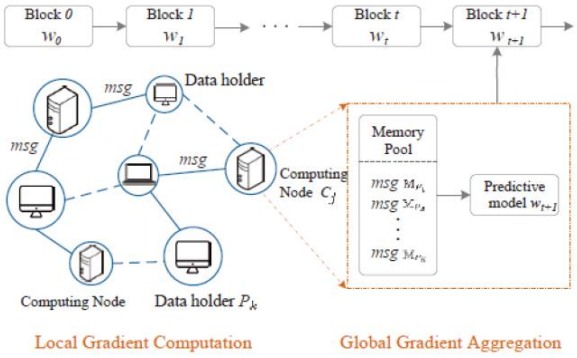

Fig. 1. The Training Process of LearningChain. [12]

For the problem of gradient information leakage, the industry and academia generally adopt a differential privacy (DP) mechanism and blockchain technology in the fedML framework. Taking the most popular "LearningChain" framework as an example, we will analyze its advantages and disadvantages. The training process of LearningChain as shown in Fig. 1. The proposed framework contains three phases: blockchain initialization; local gradient computation; global gradient aggregation. In the core phase, i.e., the local gradient computation phase, the authors introduced the DP mechanism to add well-designed noise to the gradient information to disturb the true distribution of the gradient information. Although this scheme protects the privacy of the gradient information, it increases the network communication overhead and sacrifices the accuracy of the model.

B. "Poisoning" Attacks

For the problem that the FedML framework is vulnerable to "poisoning" attacks, Weng et al. [14] proposed the "DeepChain" framework to solve this problem. DeepChain provides a value-driven incentive mechanism based on Blockchain to force the participants to behave correctly. Meanwhile, DeepChain guarantees data privacy for each participant and provides suitability for the whole training process. The DeepChain model, as shown in Fig. 2.

In Fig. 2, the authors use smart contracts and incentive mechanisms to regulate the behavior of the parties and utilize the workers to audit the parameter information uploaded by the parties. DeepChain first applied smart contracts and incentive mechanisms to FedML. However, DeepChain's audit mechanism is based on 2/3 of the workers are honest and reliable, that is, if the workers are dishonest, then DeepChain cannot prevent "poisoning" attacks. In fact, workers are often dishonest and unreliable. In addition, the DeepChian model is not a distributed learning model in the strict sense.

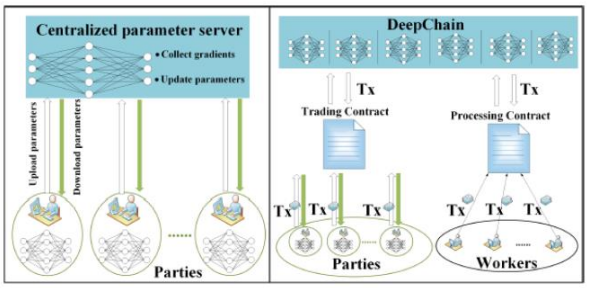

Fig. 2. The left corresponds to traditional distributed deep training framework, while the right is our DeepChain. [14]

In summary, the current solution does not perfectly solve the problems of FedML framework. As people attach importance to privacy rights, it is necessary to develop a powerful privacy-preserving FedML platform.

V. Research Objectives and Approach

BlockFedML is defined as an intelligent platform that runs ML models without compromising privacy and security. The objective of the current research is to solve the FedML framework with two challenges: one is the possibility of leakage of gradient information, and the other is that the FedML framework is vulnerable to integrity attacks. Particularly, the research has the following sub-objectives:

- To propose efficient and robust privacy protection approaches;
- To develop methods to protect the integrity of ML models;
- To develop methods to protect the integrity of the ML model's input (i.e., data, label).

A. Secure Parameter Aggregation Mechanism

For the problem of gradient information leakage, the industry and academia generally adopt a differential privacy (DP) mechanism and blockchain technology in the FedML framework. Taking the most popular "LearningChain" framework as an example, LearningChain utilizes the transaction mechanism in the blockchain to track the parameter information uploaded by local devices and adds well-designed noise to the gradient-based on DP mechanism to disturb the original distribution of gradient information. Although this scheme protects the privacy of the gradient information, it sacrifices the accuracy of the model.

Unlike DP-based methods that cannot keep the accuracy of the model, the secure parameter aggregation mechanism can perform encryption model training without compromising the accuracy.

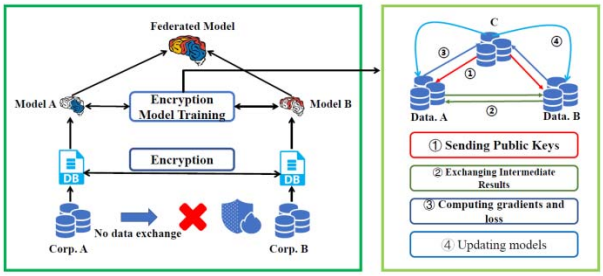

Fig. 3. Secure Parameter Aggregation Mechanism.

Secure Parameter Aggregation Mechanism: After identifying the common entities, we can use the data of these common entities to train machine learning models. To ensure the confidentiality of the data during training, it is necessary to use a third-party collaborator C for encryption. Taking the linear regression model as an example, the training process can be divided into the following four steps (as shown in Figure 3):

- Collaborator C creates encryption pairs, send the public key to A and B; Step
- A and B encrypt and exchange the intermediate results for gradient and loss calculations; Step
- A and B compute encrypted gradients respectively, and B also computes encrypted loss; A and B send encrypted values to C;
- C decrypts and send the decrypted gradients and loss back to A and B; A and B update the model parameters accordingly. Iterations through the above steps continue until the loss function converges, thus completing the entire training process.

During entity alignment and model training, the data of A and B remain local, and the data interaction during training will not cause data privacy leaks. Therefore, the two sides jointly realized the training of the standard model with the help of joint learning.

B. Checkpoint-based Smart Contracts

Before we introduce the Checkpoint-based Smart Contracts, we define model integrity attacks and smart contracts.

Model Integrity Attack: Attackers can influence the integrity of the model by modifying existing training data or adding noise data to the training set.

For example, Weng et al. [11] proposed the "DeepChain" framework to defense this attack. Deepchain utilizes SCs to regulate the behavior of the parties. However, SCs can only regulate parties' behavior and track attackers, but cannot restore the attacked model. To address this shortcoming, I propose the Checkpoint-based Smart Contracts, as shown in Fig. 4.

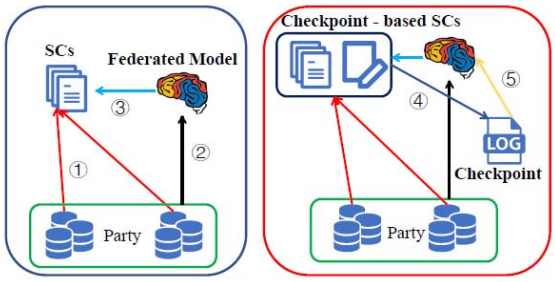

Fig. 4. Smart Contracts (left) and Checkpoint-based Smart Contracts (right).

Step 1 - 3: All parties fulfill the content of the Checkpoint-based SCs, and then parties upload the parameter information to the Federated Model. Checkpoint-based SCs record and track the behavior of parties and Federated Model.

Step 4 - 5: Checkpoint-based SCs store the checkpoint (model parameters) at time t to the database. If the Federated Model loses accuracy by the attacker at time (t + 1), then immediately use the checkpoint from time t to recovery model.

C. Incentive Mechanisms and Transfer Learning

Model's Input Integrity Attack: Party submits malicious data or intentionally loses data.

Incentive mechanisms (IM) encourage contributors to submit good data that will improve the model's accuracy. And transfer learning is a machine learning method that takes the model developed for task A as an initial point and reuses it in the process of developing a model for task B [12]. BlockFedML defends against model's input integrity attacks in two ways, as follows:

1. IM includes a reward system and a punishment system. Contributions such as data and labels submitted by the party are rewarded if the accuracy of the model is improved. On the contrary, it punishes the party and does not even allow participation in the FedML framework.

2. When the Federated Model is not initialized, I introduce an ML model such as Support Vector Machine (SVM) through the transfer learning technique. Before the party submits the data, the party needs to train the SVM locally and submit the results along with the data to the Federated Model. This can detect which are malicious parties.

VI. Overview of the BlockFedML System

Fig. 5 illustrates the envisioned solution. The entire solution is divided into five phases: the selection phase, the configuration phase, the allocation phase, the update phase; and the feedback phase. The specific steps are as follows:

- **The selection phase:** First, each party voluntarily joins the BlockFedML framework with no financial incentives. The cloud sends a copy of the model to each party. Each party initializes the model locally and runs the model locally based on its contributions. Then, each party will upload the result to the cloud (the results are usually binarized, '1' means favorable, '0' means harmful). Finally, the cloud will select eligible parties to participate in this round of training.

- **The configuration phase:** Smart contracts will be sent to each party. Smart contracts standardize the behavior of each party based on a consensus mechanism in the blockchain and can track each transaction through a contract.
- **The allocation phase:** The cloud allocates different FedML tasks according to the categories of contributions (i.e., labels, datasets, and gradient information, etc.) of each party. Therefore, some parties are responsible for updating the labels, some are responsible for updating the data set, and some parties are responsible for updating the gradient.
- **The update phase:** The cloud aggregates the information updated by each party to update the global model. The cloud sends a copy of the updated global model to each party.
- **The feedback phase:** According to the content of the incentive mechanism, the cloud rewards the party that improves the accuracy of the model, and penalizes the party that damages the accuracy of the model or even allows the training after the participation.

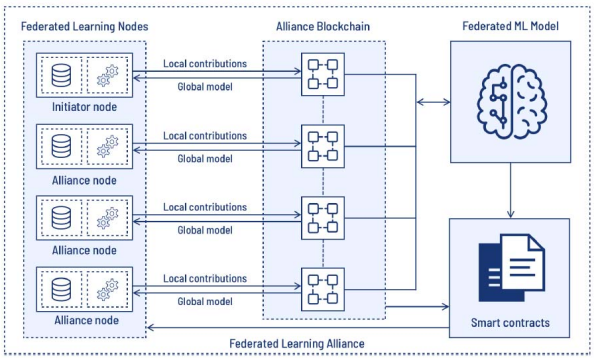

Fig. 5. Overview of the BlockFedML platform.

VII. Applications and Conclusion

Applications of BlockFedML as follows:

- **Intelligent Marketing:** BlockFedML utilizes machine learning technology to bring personalized product services to its customers, including product recommendations and sales services. Because the data involved in the intelligent marketing business is spread across organizations, BlockFedML can federate the organization's data without compromising privacy and security.
- **Intelligent Diagnosis:** The ML model in the medical field is often low inaccuracy due to the lack of data, and BlockFedML can solve this bottleneck.
- Federated Learning and Industry Data Alliance: BlockFedML uses the consensus mechanism and incentive mechanism in the blockchain to aggregate enterprise data into a data alliance. This data alliance can solve the data sharing problems of many industries.

In this paper, we propose a Blockchained Federated Machine Learning System, which called "BlockFedML." In BlockFedML, we develop Security Parameter Aggregation Mechanisms, Checkpoint based- Smart Contracts, Incentive Mechanisms, and Transfer Learning. Finally, we outlined the BlockFedML system and its applications.

Acknowledgment

This work is supported by the special topic of the 13th Five-Year Plan for Education Science in Heilongjiang Province. (Grant No: GBE1317013) The title of the project is "Study on the Cultivation of Innovation and Entrepreneurship of College Students Based on the Dimensions of New Engineering Indicators".

References

[1] P. M. Kumar, S. Lokesh, R. Varatharajan, G. C. Babu, P. Parthasarathy, "Cloud and iot based disease prediction and diagnosis system for healthcare using fuzzy neural classifier", *Future Generation Computer Systems,* vol. 86, pp. 527-534, 2018.

[2] B. Zoph, V. Vasudevan, J. Shlens, Q. V. Le, "Learning transferable architectures for scalable image recognition", *in Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 8697-8710, 2018.

[3] A. Vaswani, S. Bengio, E. Brevdo, F. Chollet, A. N. Gomez, S. Gouws, L. Jones, Ł. Kaiser, N. Kalchbrenner, N. Parmar et al., "Tensor2tensor for neural machine translation," *arXiv preprint arXiv:*1803.07416, 2018.

[4] W. Xiong, L. Wu, F. Alleva, J. Droppo, X. Huang, A. Stolcke, "The microsoft 2017 conversational speech recognition system", *in 2018 IEEE international conference on acoustics, speech and signal processing (ICASSP). IEEE*, pp. 5934-5938, 2018.

[5] Q. Yang, Y. Liu, T. Chen, Y. Tong, "Federated machine learning: Concept and applications", *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 10, no. 2, pp. 12, 2019.

[6] Y. Liu, J. Peng, J.Q. James, Y, Wu. "PPGAN: Privacy-preserving Generative Adversarial Network", *arXiv preprint arXiv*:1910.02007 (2019).

[7] J. D. Harris, B. Waggoner, "Decentralized & collaborative ai on blockchain", *arXiv preprint arXiv:*1907.07247, 2019.

[8] R. Shokri, V. Shmatikov, "Privacy-preserving deep learning", in Proceedings of the 22nd ACM SIGSAC conference on computer and communications security. *ACM*, pp. 1310-1321, 2015.

[9] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, L. Zhang, "Deep learning with differential privacy", in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. *ACM*, pp. 308-318, 2016.

[10] J. Kone˘cn`y, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, D. Bacon, "Federated learning: Strategies for improving communication efficiency", *arXiv preprint arXiv*:1610.05492, 2016.

[11] G. Zyskind, O. Nathan, et al., "Decentralizing privacy: Using blockchain to protect personal data", in 2015 IEEE Security and Privacy Workshops. *IEEE*, pp. 180-184, 2015.

[12] X. Chen, J. Ji, C. Luo, W. Liao, P. Li, "When machine learning meets blockchain: A decentralized, privacypreserving and secure design", in 2018 IEEE International Conference on Big Data (Big Data). *IEEE*, pp. 1178-1187, 2018.

[13] X. Zhu, H. Li, Y. Yu, "Blockchain-based privacy preserving deep learning", in International Conference on Information Security and Cryptology. Springer, pp. 370-383, 2018.

[14] J. S. Weng, J. Weng, M. Li, Y. Zhang, W. Luo, "Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive", IACR Cryptology ePrint Archive, vol. 2018, pp. 679, 2018.

[15] T. Li, A. K. Sahu, A. Talwalkar, V. Smith, "Federated learning: Challenges, methods, and future directions", *arXiv preprint arXiv*:1908.07873, 2019.

[16] M. Ammad-ud din, E. Ivannikova, S. A. Khan, W. Oyomno, Q. Fu, K. E. Tan, A. Flanagan, "Federated collaborative filtering for privacy-preserving personalized recommendation system", *arXiv preprint arXiv*:1901.09888, 2019.

[17] J. Kone˘cn`y, B. McMahan, and D. Ramage, "Federated optimization: Distributed optimization beyond the datacenter," *arXiv preprint arXiv:*1511.03575, 2015.

[18] Y. Wu, Y. Liu, S. H. Ahmed, J. Peng, A. El-Latif, "Dominant Dataset Selection Algorithms for Electricity Consumption Time-Series Data Analysis Based on Affine Transformation", *in IEEE Internet of Things Journal.* doi: 10.1109/JIOT.2019.2946753.

[19] S. J. Pan, Q. Yang, "A survey on transfer learning", IEEE Transactions on knowledge and data engineering, vol. 22, no. 10, pp. 1345-1359, 2009.

[20] Kang J, Yu R, Huang X, et al. Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains [J]. IEEE Transactions on Industrial Informatics, 2017, PP (99):1-1.

[21] Kang J, Xiong Z, Niyato D, et al. Incentive Design for Efficient Federated Learning in Mobile Networks: A Contract Theory Approach [J]. 2019.

[22] Kang J, Xiong Z, Niyato D, et al. Toward Secure Blockchain-Enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory [J]. IEEE Transactions on Vehicular Technology, 2019, PP (99):1-1.

[23] Kang J, Yu R, Huang X, et al. Privacy-Preserved Pseudonym Scheme for Fog Computing Supported Internet of Vehicles [J]. IEEE Transactions on Intelligent Transportation Systems, 2017:1-11.

[24] Huang X, Yu R, Kang J, et al. Distributed Reputation Management for Secure and Efficient Vehicular Edge Computing and Networks [J]. IEEE Access, 2017, PP (99): 1-1.

[25] Huang X, Yu R, Kang J, et al. Software Defined Energy Harvesting Networking for 5G Green Communications [J]. IEEE Wireless Communications, 2017, 24 (4):38-45.

[26] Kang J, Yu R, Huang X, et al. Location privacy attacks and defenses in cloud-enabled internet of vehicles [J]. IEEE Wireless Communications, 2016, 23 (5): 52-59.

[27] Yu R, Kang J, Huang X, et al. MixGroup: Accumulative Pseudonym Exchanging for Location Privacy Preservation in Vehicular Social Networks [J]. IEEE Transactions on Dependable and Secure Computing, 2015:1-1.