Blockchain Assisted Decentralized Federated Learning (BLADE-FL) with Lazy Clients

Jun Li[1], Yumeng Shao[1], Ming Ding[2], Chuan Ma[1], Kang Wei[1], Zhu Han[3], H. Vincent Poor[4]

1. Nanjing University of Science and Technology, China. E-mail: shaoyumeng@njust.edu.cn.
2. Data61, CSIRO, Sydney, Australia.
3. University of Houston, Houston, TX, USA.
4. Princeton University, NJ, USA.

Introduction

In recent years, Federated Learning (FL) shows an inherent advantage in privacy preservation, since users' raw data are processed locally. However, it relies on a centralized server to perform model aggregation. Therefore, FL is vulnerable to server malfunctions and external attacks.

In this paper, we propose a novel framework by integrating blockchain into FL, namely, blockchain assisted decentralized federated learning (BLADE-FL), to resolve this single-point-failure. However, it gives rise to a new problem of training deficiency, caused by lazy clients who plagiarize others' trained models and add artificial noises to conceal their cheating behaviors.

The lazy clients can't be detected from the lack of penalization mechanism in an unsupervised network, such as blockchain, but we can reduce its influence by adjusting the computational resources allocation strategy.

References

[1] C. Xu, K. Wang, P. Li, S. Guo, J. Luo, B. Ye, and M. Guo. (2019) Making big data open in edges: A resource-efficient blockchain-based approach. In IEEE Transactions on Parallel and Distributed Systems, vol.30, no. 4, pp. 870–882.

[2] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang. (2019) Blockchain and federated learning for privacy-preserved data sharing in industrial iot. IEEE Transactions on Industrial Informatics

[3] S. Wang, T. Tuor, T. Salonidis, K. K. Leung, C. Makaya, T. He, and K. Chan. (2018) Adaptive federated learning in resource constrained edge computing systems.

Framework

- Local Training
- Model Uploading
- Model Downloading
- Mining
- Block Verification
- Local Updating

A lazy client can plagiarize other models directly before generating a new block and add artificial noises to the model weights to cancel its behavior.

$$\boldsymbol{w}_{i'}^k = \boldsymbol{w}_i^k + \mathbf{n}_i, \quad i' \subseteq \mathcal{M}, i \notin \mathcal{M}$$

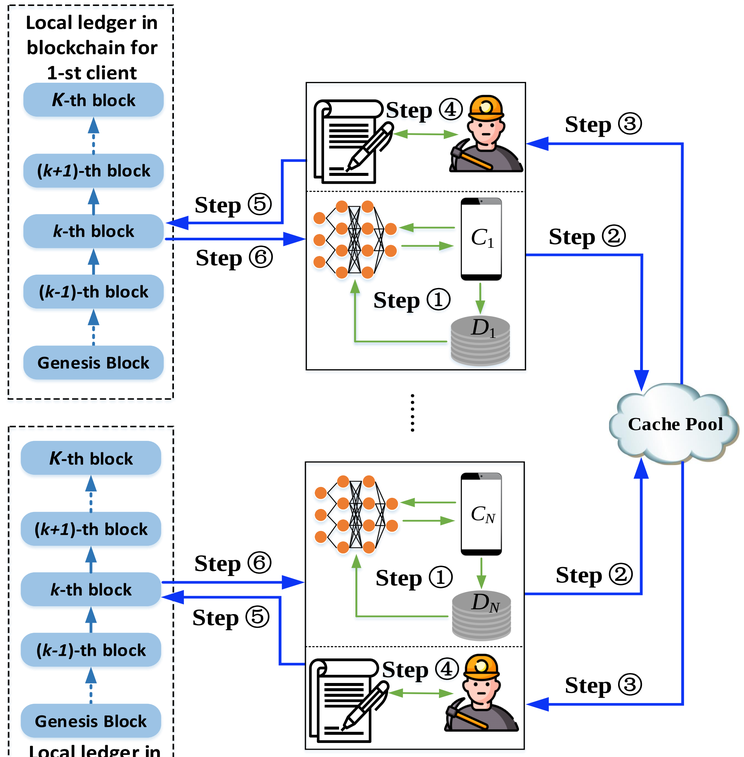

Fig. 1 The framework of BLADE-FL

Main Theorem

The upper bound of BLADE-FL is given by

$$F(\boldsymbol{w}^K) - F(\boldsymbol{w}^*) \leq \frac{1}{\gamma\left(\eta\phi - \frac{\frac{\delta\xi K}{L}\left(\lambda^{\frac{\gamma}{K}}-1\right) - \eta\xi\delta\gamma + \xi\frac{M}{N}\theta + \xi\frac{\sqrt{M}}{N}\sigma^2}{\varepsilon^2\gamma}\right)}$$

- The developed upper bound is a convex function with respect to K.
- The optimal K that minimizes the loss function value decreases as the lazy client ratio M/N or the noise variance σ^2 grows.

Results

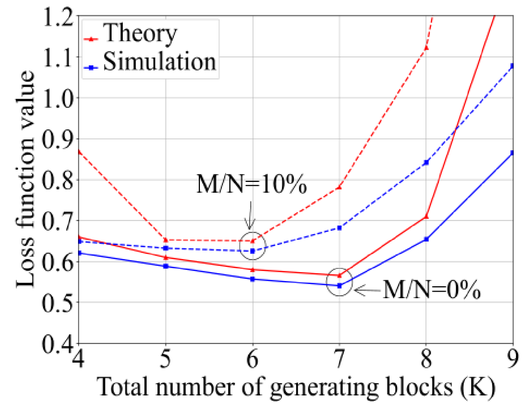

Fig. 2 Numerical results and experimental results on MNIST

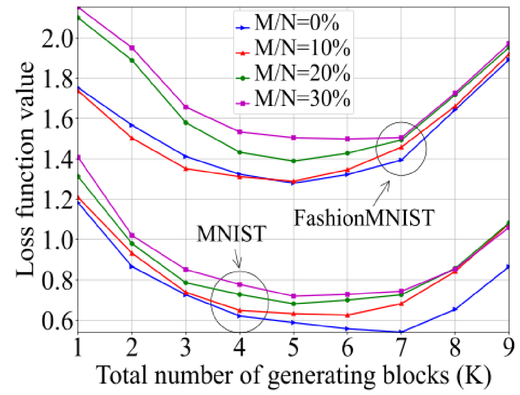

Fig. 3 Value of the loss function and accuracy under various K and M/N values

Nanjing University of Science & Technology