Spatio-Temporal Split Learning

Joongheon Kim  
Korea University  
Seoul, Korea  
joongheon@korea.ac.kr

Seunghoon Park  
Korea University  
Seoul, Korea  
psh95king@korea.ac.kr

Soyi Jung  
Korea University  
Seoul, Korea  
jungsoyi@korea.ac.kr

Seehwan Yoo  
Dankook University  
Yongin, Korea  
seehwan.yoo@dankook.ac.kr

Abstract—This paper proposes a novel split learning framework with multiple end-systems in order to realize privacy-preserving deep neural network computation. In conventional split learning frameworks, deep neural network computation is separated into multiple computing systems for hiding entire network architectures. In our proposed framework, multiple computing end-systems are sharing one centralized server in split learning computation, where the multiple end-systems are with input and first hidden layers and the centralized server is with the other hidden layers and output layer. This framework, which is called as spatio-temporal split learning, is spatially separated for gathering data from multiple end-systems and also temporally separated due to the nature of split learning. Our performance evaluation verifies that our proposed framework shows near-optimal accuracy while preserving data privacy.

Index Terms—Split learning, privacy-preserving, deep learning

I. INTRODUCTION

Nowadays, deep neural network computations are widely and actively used in many applications. Therefore, it is obvious that there are a lot of research contributions which aim at privacy-preserving secure deep neural network computation. Among them, federated learning is one of well-known and successful approaches which does not expose training data to the public [1], [2]. According to the privacy-preserving nature in federated learning, it is suitable for medical applications. In distributed medical systems (hospitals, biomedical research institutes, etc.), there exist lots of patients’ data. In addition, the system conducts deep neural network training on such data all of it typically should be in the same space for the training. However, gathering and transporting patient data is strictly regulated by laws due to privacy. As a result, each medical system conducts computations with its own local data. To deal with this issue, this paper proposes a federated learning framework which trains models with the data stored in each end-system locally for privacy-preserving computation while maintaining learning accuracy. Among various federated learning algorithms, this paper considers split learning which separates deep neural network computation into several parts [3]. The basic system architecture for split learning is as illustrated in Fig. 1. As shown in Fig. 1, the training data located in end-system cannot be seen at the centralized server, thus, privacy-preserving deep neural network computation can be available. However, to the best of our knowledge, multiple end-systems are not considered in split learning research contributions, yet. In the case with multiple end-systems, the training data are located in spatially separated individual end-systems and the deep neural network training is temporally separated as shown in Fig. 1, thus our proposed system is named spatio-temporal split learning. In this proposed spatio-temporal split learning, each end-system contains several hidden layers and the results of the last hidden layers of all end-systems will be delivered to the centralized server. The server has the other remaining hidden layers and output layer of our considering deep neural network, thus, centralized computation can be available. Based on our performance evaluation results with cifar10 based classification, it can be observed that our spatio-temporal split learning can show near-optimal performance while preserving data privacy.

II. SPATIO-TEMPORAL SPLIT LEARNING FRAMEWORK

Our proposed spatio-temporal split learning framework is as illustrated in Fig. 2. As shown in Fig. 2, multiple end-systems exist; and the individual results of end-systems’ first hidden layers are delivered to the centralized server. Then, the original raw data is not shared and encoded (due to the first hidden layer computation). Note that sharing the results of first hidden layers at the centralized server does not expose original raw data. Then, deep neural network computation with the other hidden layers and output layer is conducted at the server, thus, all training data is used for single deep neural network training. Therefore, in theory, our proposed spatio-temporal split learning framework achieves near optimal performance by using all data in a single network with certain amount of performance sacrifice due to individual first hidden layers in each end-system. This performance degradation can be larger when more hidden layers are in end-systems while sacrificing certain amounts of learning performance (tradeoff).

The centralized server requires queue while gathering the results of the first hidden layers in end-systems under the consideration of geo-distributed end-systems. If an end-system is located very far from the centralized server, the parameters
from the end-system can arrive at the server lately or sparsely. Then, the learning performance can be biased due to the differences of arrivals from end-systems. Thus, parameter scheduling is required depending on applications, i.e., a queue is conducted with convolutional neural networks (CNN). In our proposed framework, multiple end-systems are sharing one centralized server, where the multiple end-systems are with first hidden layer and the centralized server is with the other layers. This framework is spatially separated for getting data from multiple end-systems and temporally separated for split learning computation. The performance of the proposed framework is evaluated and the results verify that the framework shows near-optimal performance without original raw data sharing for privacy preserving computation.

ACKNOWLEDGMENT

This research was funded by Ministry of Health and Welfare (HI19C0572) and National Research Foundation of Korea (2019R1A2C4070663). S. Jung and S. Yoo are corresponding authors.

REFERENCES

[1] J. Park, S. Samarakoon, A. Elgabli, J. Kim, M. Bennis, S. Kim, and M. Debbah, “Communication-efficient and distributed learning over wireless networks: Principles and applications,” Proc. of the IEEE, 2021.
[2] D. Kwon, J. Jeon, S. Park, J. Kim, and S. Cho, “Multiagent DDPG-based deep learning for smart ocean federated learning IoT networks,” IEEE Internet of Things J., vol. 7, no. 10, pp. 9895–9903, Oct. 2020.
[3] P. Vepakomma, O. Gupta, T. Swedish, and R. Raskar, “Split learning for health: Distributed deep learning without sharing raw patient data,” CoRR, vol. abs/1812.00564, 2018.
[4] J. Jeon, J. Kim, J. Kim, K. Mohaisen, and J. Kim, “Privacy-preserving deep learning computation for geo-distributed medical big-data platforms,” in Proc. IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Portland, OR, USA, June 2019.