독립적인 트랜잭션 연합학습에 관한 연구

산디 라마디카, 이경현*

부경대학교 정보보호학협동과정

*부경대학교 IT융합응응공학과

sandika@pukyong.ac.kr, khrhee@pknu.ac.kr*

Dissacosiation Transactions in Federated Learning

Sandi Rahmadika and Kyung-Hyune Rhee*

Interdiscplinary Program of Information Security, Graduate School PKNU

*Department of IT Convergence and Application Engineering

Pukyong National University, Republic of Korea

Abstract

Segregated learning is disclosed publicly that enables multiple users to improve a global deep learning model gradually. The objective of segregated learning is to preserve privacy for users during training without having to expose their data to the public. However, the system lacks an adequate incentive scheme. A blockchain smart contract can be a credible solution to provide distributed incentives for users since it is self-executing contracts with immutable data records that resistance to failure. Straightforwardly adopting smart contracts in a segregated learning system might break users' privacy. Malicious users can infer the properties of training resources. Therefore, in this paper, we investigate in which case malicious users are likely performing the inference attacks. The preliminary design scheme for dropping the risk of such attacks is also elaborated.

I. Introduction

The decentralized approaches in managing computer commands over the internet have been extensively researched lately by academia, developers, and industries. The key motivation of this approach is to tackle the communication bottleneck issues and memory usage of the conventional centralized system [1]. Therefore, the paradigm of a centralized system for a various implementations also shifted towards decentralized manners such as financial technology, medical records, intellectual property, and to name a few.

Segregated learning is a breakthrough in the deep learning environment. It turns up the from centralized users' raw data for training to a distributed form. The raw data owned by clients are never leaving the devices [2]. Thus, the issues of privacy in centralized learning can be addressed naturally by design.

The contributed parties in the segregated learning system should be incentivized proportionally. The parties use their resources (valuable data and computing power) to improve the global model. Ethereum smart contracts are also well-known as self-executing contracts can be a plausible solution to preserve distributed incentives that also resistance to failure.

A *two-phase commit* protocol is being implemented in order to accommodate more conventional communication between users and the aggregation server. However, during protocol implementation, the information about aggregation values might be inferred by malicious users. By adopting the inference

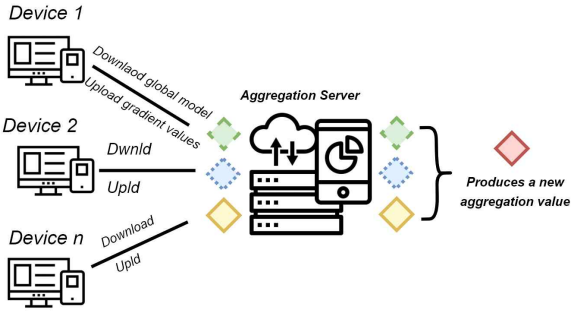
attacks, the observer with certain assumptions can infer and link the presence of specific data features of the users' private dataset. Hence, we outline the segregated learning model along with a decentralized incentive mechanism. We also elaborate on the potential inference attacks that can infer the knowledge between output and the owner.

II. Core System Components

Decent design on cloud services for training a deep learning model provides tangible benefits for providers and clients in the real world. Several convenience features are accomplished with the existence of cloud-based training services. Therefore, the other well-known technologies such as internet-of-things (IoT), virtual machines, artificial intelligence (AI), fifth-generation (5G) mobile networks, and blockchain can be performed remotely in a commercial providers' data center.

Conventional Learning Approaches. In the AI environment, the model providers can offer their original algorithm publicly with certain conditions. Thus, the researchers and developers can use the model directly through cloud services with varied data possessed. Cloud computing is considered essential in guaranteeing the quality of services in the AI model and reducing energy consumption since the workload in many applications is always evolving.

Blockchain in Segregated Learning. One of the most tangible benefits of utilizing blockchain technology is the absence of intermediaries in handling the transactions. This feature is also useful for collaborative intelligence where data is not concentrated. The users' data in a segregated system are unique to each other. In short, there is a set of users with a distinguished dataset in



devices.

Figure 1. High-level of segregated learning

We notice that the aggregation server nor other devices within the maximum waiting time *Tmax* having no knowledge to the local computing data of all parties (AFL is global accuracy). Hence, it preserves data privacy. The computation for upper bound in the general iteration is denoted to be (1). The total execution time respects the number of iterations. It is upper bordered by $O(log(1/\theta))$.

$$K(A_{FL}, \theta) = \frac{\mathcal{O}(log(1/A_{FL}))}{1-\theta} \quad (1)$$

$$\min_{\theta} \ \Omega(\theta) + \frac{1}{n}\sum_{i=1}^{n} \mathcal{L}(y_i, f_\theta(x_i)) \quad (2)$$

The training algorithm T has a set of parameters θ -> $f\theta$ = x -> y. It is applied to minimize a loss function L which penalizes the mismatches between true labels y and predicted labels produces by $f\theta(x)$. With $\Omega(\theta)$ as a regularization term that penalizes model complexity. It helps preventing models from overfitting as shown in (2).

Ethereum platform preserves a decentralized ecosystem for developers to create products using the Ethereum Virtual Machine (EVM) which is powerful and embedded within each full blockchain network as shown in Figure 2. The smart contracts bytecodes are executed through EVM. Interacting with the EVM via smart contracts is likely more costly than traditional servers. However, numerous use cases are favored using EVM rather than conventional servers.

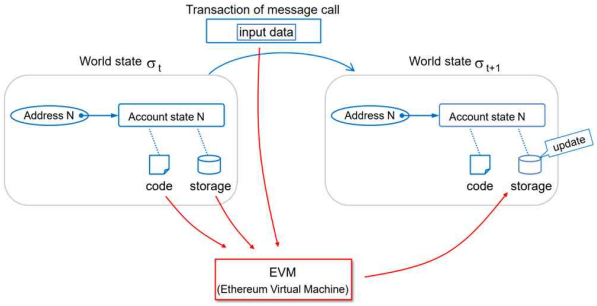


Figure 2. Ethereum virtual machine

III. Secure Collaborative Learning with Blockchain Scheme

A. Segregated Learning Activities and Decentralized Revenue

Segregated Learning Activities. The users are data owners who hold a considerable amount of individual training data, while the AI provider stores the deep learning model that can be accessed by authorized users. The updated gradient are collected by the provider regularly, which later to be employed to calculate the final aggregation value. This process is repeated as long as necessary for improving the global model.

At the beginning of the process for each round, the aggregation server stores a global model in the cloud server. Then, the server roughly mapping the users available in the network along with the dynamic rules.

Eventually, Figure 3 describes the performance of loss over time training from multiple users with the scattered datasets. The loss for the lowest number of devices at 1st epoch is 1.882 and continued to decrease at the 50th epoch by 0.191. The same thing occurred in 15 devices with losses of 1.071 (1st epoch) and 0.206 (50th epoch). Moreover, the average value of loss for all devices is 0.618. The loss decreases as the number of epochs increases for all devices.

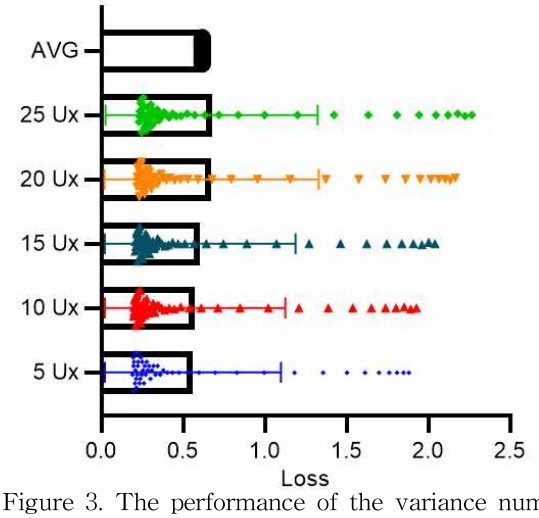


Figure 3. The performance of the variance number of segregated learning users

It can be concluded that most of the losses occurred in the early stages of training per cycle. The differences might be significant if the number of devices implemented is extremely large.

Figure 4 presents the distribution points of an average loss of SL. In short, the average loss for every device is almost identical. The number of devices involved in our scheme slightly affects the loss. Whilst, Fig. 5 depicts the comparison amount of Ethereum gas used between smart contract manager SCx and users Cx. The provider consumes gas stably for every transaction, while the clients produce gas depend on their contribution which is stated in the smart contracts.

B. Traceability and Privacy Concerns with Potenial Solutions

In the segregated learning, when the users deploy their transaction that consists of a cipher to encrypt the information to the AI provider, the observer can impose the dataset knowledge by adopting active and passive inference attacks. Yet, the performance of the adversary decreases with an increasing number of users.

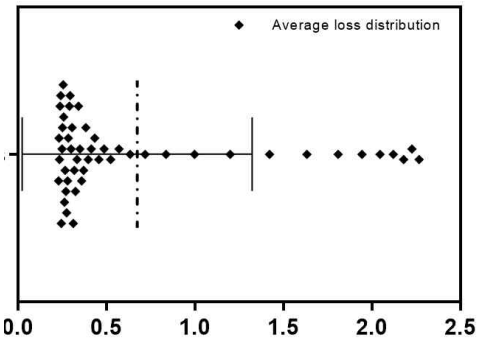


Figure 4. Average loss distribution of SL

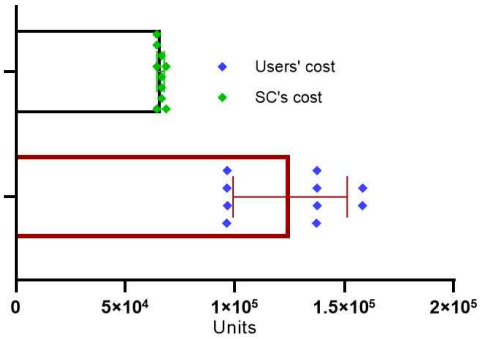


Figure 5. The gas used by users and SC

In short, as batch sizes increase, this type of attack produces more false positives. More promptly, the size of the batch influences the precision of the adversary. The larger the size of a batch, the lower the precision from the adversary's side.

Solutions. In the segregated learning system, every users and model provider have a pair of public keys *(An,Bn)*. The *An* is used to generate a one-time public key for transaction, and *Bn* is attached to the transaction as a tracking pointer.

We assume User *A (Ua)* wants to conduct transactions with User *D (Uδ)*. In concurrent User *C (Uɣ)* and User *B (Uβ)* want to make transactions as well. User *Ua* then wants to use *Mixer* services to hide his identity. The mixer then combines the *A Ua* transaction $TXa = T(U\beta \oplus U\gamma \oplus U\delta \oplus Ua)$.

There are two kinds of pub keys *An* is used to create a stealth address, and *Bn* is used to searching the transaction as shwon in the following equations:.

$$P = Hs(rA\alpha)G + B\alpha$$

$$P' = Hs(a\alpha\, R)G + B\alpha, then$$

$$a\alpha\, R = a\alpha\, rG = rA\alpha;\ P' = P$$

The provider uses P as a destination key for the output and attaches the new value $R = rG$ into the transaction. The data with attachments to P and R values are stored into shared storage after being validated by the miner. The recipient later checks every transaction using his private key $(a\beta, b\beta)$ and calculates the new P', and compares the value P received with the value P'. Finally, an unlinkability transaction is preserved.

IV. Conclusion

Dissacotiation transactions in segregated learning with Ethereum smart contract as an incentive mechanism has been presented in this paper. The system goals are to preserve users' privacy by cutting off the role of a centralized machine to do the training. The provided scheme brings privacy challenges, yet it can be overcome with the solutions that have been outlined in this paper.

Acknowledgment

This research was supported by the Republic of Korea's MSIT (Ministry of Science and ICT), under the High-Potential Individuals Global Training Program) (2020-0-01596) supervised by the IITP (Institute of Information and Communications Technology Planning & Evaluation) and partially supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2018R1D1A1B07048944).

[References]

[1] Koloskova, A., Stich, S. U., & Jaggi, M. (2019). Decentralized stochastic optimization and gossip algorithms with compressed communication. arXiv preprint arXiv:1902.00340.

[2] Weng, Jiasi, et al. "Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive." IEEE Transactions on Dependable and Secure Computing (2019).

[3] Ezhilchelvan, P., Aldweesh, A., & van Moorsel, A. (2020). Non blocking two phase commit using blockchain. Concurrency and Computation: Practice and Experience, 32(12), e5276.

[4] Zhang, Q., Yang, L. T., Yan, Z., Chen, Z., & Li, P. (2018). An efficient deep learning model to predict cloud workload for industry informatics. IEEE Transactions on Industrial Informatics, 14(7), 3170-3178.