기계 학습용 다자간 연산과 연합 학습에 대한 비교 연구

A Comparative Study on Multi-Party Computation for Machine Learning and Federated Learning

Seong-Hyeon Bae, Su-Jeong Yu, Won-Yong Shin
Yonsei University

baesh2756@gmail.com, sujeong.yu@yonsei.ac.kr, wy.shin@yonsei.ac.kr

요 약

본 논문은 개인 정보 보호 기계 학습 (privacy preserving machine learning, PPML)의 대표적인 접근법인 서버 측 보안 다자간연산 (server-side secure multi-party computation, SMPC)와 수평적 연합 학습 (horizontal federated learning, HFL) 방법 간 차이를 비교한다. SMPC 는 참여자가 데이터를 비밀 분할하여 서버에게 전송 후 서버가 복호화 없이 모델을 학습하며, HFL 은 각 참여자가 로컬에서 학습한 모델 파라미터만을 서버에 공유하여 글로벌 모델을 업데이트한다. SMPC 는 계산 및 통신 비용이 크지만 높은 보안성과 참여자간 데이터 분포 불균형에 강한 반면, FL 은 모델 파라미터로부터 원본 데이터가 유출될 위험이 있지만 학습 속도가 빠르다는 각각의 특징이 있다.

Ⅰ. 서 론

본 논문에서는 PPML 을 수행하는 대표적인 기법인 SMPC 기반 기계 학습 방법 [1]과 HFL 방법 [2]에 대한 비교 분석을 다룬다.

Ⅱ. 방법론

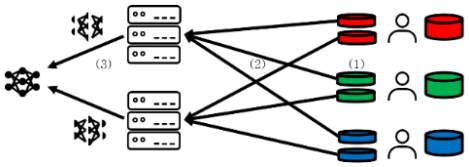

그림 1. SMPC 기반 PPML 구조

먼저, SMPC 는 참여자들의 비밀 분할된 데이터를 둘 이상의 서버가 나누어 전송 받아, 하나의 연산 결과를 공동으로 계산하는 암호학 프로토콜이다. SMPC 를 기계 학습에 적용하면, 참여자의 데이터를 안전하게 처리하면서도 협력적인 학습이 가능하다. 각 참여자는 그림 1 과 같이 (1) 자신의 데이터를 비밀 분할 (secret share)을 통해 암호화하여 (2) 서버에 전달하고, (3) 서버는 비밀 분할된 데이터를 복원하지 않고 연산을 진행하여 글로벌 모델을 학습시킨다.

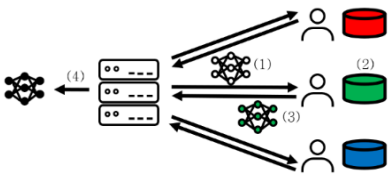

그림 2. HFL 의 구조

다음으로, HFL 은 동일한 데이터 특성을 가진 여러 분산된 데이터가 각 참여자의 로컬 기기에 비공개로 저장된 채로 학습하는 방식이다. 그림 2 와 같이 HFL 에서는 (1) 하나의 서버에서 여러 개의 로컬 기기로 초기 모델을 전송하고, (2) 로컬에서 각자의 데이터로 모델을 학습 후 (3) 학습시킨 모델 파라미터를 서버로 전송한다. 서버는 (4) 전송받은 파라미터를 통합하여 글로벌 모델을 업데이트한다. 각 참여자의 데이터는 로컬에 존재하고, 서버에게 파라미터 정보만 전달하므로 데이터가 노출되지 않는 효과가 있다.

Ⅲ. 비교 및 분석

	SMPC 기반 PPML	Horizontal FL
서버 구성	두개 이상의 non-colluding 서버	단일 중앙 서버
학습 주체	여러 서버가 협력하여 학습	참여자가 각자 로컬에서 학습
서버가 받는 정보	비밀 분할된 데이터 조각	참여자가 학습한 모델의 파라미터
데이터 보안성	데이터가 암호화되어 원본 노출 불가	모델 파라미터로부터 데이터 유추 위험 문제
데이터 분포 문제	모든 데이터를 단일 학습에 포함하므로 분포 편향에 강함	참여자마다 학습 데이터의 분포가 달라 수렴이 어려움
병렬성 및 속도	병렬화가 제한되고 통신량이 많아 느림	참여자마다 병렬적으로 학습이 가능하여 빠름

표 1. SMPC 기반 PPML 과 Horizontal FL 의 특징 비교

표 1 과 같이 데이터의 절대적인 보안이 요구되고 각 유저의 데이터 분포가 다양한 경우에는 SMPC 기반 PPML 이 적합하다. 반면, 학습 속도가 중요한 경우에는 병렬 학습이 가능하고 통신량이 적은 FL 이 효과적이다.

ACKNOWLEDGMENTS

This work was supported by the National Research Foundation of Korea (NRF), Republic of Korea through the Korean Government through MSIT under Grant 2021R1A2C3004345 and Grant RS-2023-00220762 by the Institute of Information and Communications Technology Planning and Evaluation (IITP), Republic of Korea through by the Korean Government through MSIT (6G Post-MAC—POsitioning and Spectrum-Aware intelligent MAC for Computing and Communication Convergence) under Grant 2021-0-00347.

참 고 문 헌

[1] I. Zhou *et al.*, Secure multi-party computation for machine learning: A survey. IEEE Access, April 2024.

[2] Q. Yang *et al.*, Federated machine learning: Concept and applications. ACM TIST, January 2019.