분산 환경에서 개인 정보를 보호하는 연합 학습

윤준용[1], 최봉준[2]
[1]숭실대학교 컴퓨터학과 석박통합과정
[2]숭실대학교 컴퓨터학과 교수
wnsdyd1124@soongsil.ac.kr, davidchoi@soongsil.ac.kr

Privacy-Preserving Federated Learning in Decentralized Environments

Jun-Yong Yoon[1], Bong-Jun Choi[2]
[1]School of Computer Science and Engineering, Soongsil University
[2]School of Computer Science and Engineering, Soongsil University

요 약

현대 사회에서 인공지능은 다양한 분야에서 사용되며 발전하고 있다. 특히 의료, 공업, 경제, 농업, 정치 등에 영향을 미치며, 데이터 프라이버시 문제가 빈번히 발생한다. 이를 해결하기 위해 연합학습이 제안되었는데, 이는 로컬 디바이스에서 학습한 모델만을 중앙 서버로 전송하여 프라이버시를 보장하고 효율성을 높인다. 하지만 연합학습은 중앙 서버를 필요로 하므로 탈중앙적인 환경에서는 사용할 수 없는 단점이 있다. 이를 보완하기 위해 본 논문에서는 서버가 없는 다양한 환경에서 연합학습을 적용할 수 있는 비-완전 연결 분산형 연합학습 알고리즘을 소개한다. 비-완전 연결 분산형 연합학습 알고리즘은 모든 노드가 서로 연결 되어있는 상태가 아닌 특정 노드와만 연결 되어있는 형태로 대부분의 실전 분산형 환경에서 사용할 수 있다. 본 방식의 학습 정확도는 일반적인 머신러닝의 정확도와 비교하여 준수한 성능을 보여주고 있다.

1. Introduction

인공지능은 오늘날 현대사회 속 많은 부분에서 사용되며 발전하고 있다. 특히 인공지능 분야는 의료, 공업, 경제, 농업 심지어는 정치까지에도 영향을 끼치며 머신 러닝과 딥러닝을 사용한 AI 솔루션의 유용성은 빠르게 증가하고 있다. 하지만 AI 솔루션의 사용량 증대의 반동으로 다양하고 많은 데이터를 분석해야 하는 머신 러닝의 특성상 데이터 프라이버시가 지켜지지 못하는 경우도 빈번히 발생한다. 이러한 문제점을 해결하기 위하여 많은 인공지능 연구자들은 인공지능 학습에 대한 데이터 프라이버시 보장을 연구하고 있다.

연합학습은 데이터 프라이버시를 보장하는 인공지능 학습 중 대표적인 예시이다. 연합학습(Federated Learning)[1]은 2017년에 McMahan에 의해 처음 발표되었다. 연합학습의 특징은 여러 대의 로컬 디바이스에서 중앙 서버로 모든 데이터를 전송하는 일반적인 인공지능 학습과는 달리 연합학습은 각각의 로컬 디바이스에서 데이터를 학습하고 학습된 결과 모델만 중앙 서버로 전송한 뒤 중앙 서버에서 합쳐서 글로벌 모델을 만드는 학습 방식이다. 이러한 방식을 통해 모든 데이터를 서버로 전송하여 네트워크 트래픽과 서버 내 데이터 저장공간 비용이 증가하는 일반 인공지능 학습에 비해 연합학습은 로컬 모델을 서버로 업데이트 하는 방식으로 통신 비용을 크게 절감함과 동시에 학습 데이터의 외부 유출을 피할 수 있다. 따라서 연합학습은 기존 인공지능 학습과 비교하여 데이터 프라이버시 보장과 통신 효율성 향상이라는 두 가지의 장점을 가지고 있어서 다양한 방면으로 유용하게 사용할 수 있다. 하지만 연합학습의 특성상 중앙 서버는 필수 불가결한 존재이기 때문에 서버가 없는 환경에서는 사용할 수 없다는 단점이 존재한다.

본 논문에서는 서버가 없는 환경에서는 일반적인 연합학습을 사용할 수 없다는 단점을 보안하기 위해 서버가 없는, 즉 탈중앙적인 환경(Decentralized Environments)에서의 연합학습 알고리즘, 즉 분산형 연합학습을 소개한다. 일반적인 탈중앙적 환경은 대게 모든 노드가 서로 연결 되어있는 완전 연결(Fully-Connected) 방식에서 진행되는데 본 논문에서는 완전 연결이 아닌 실전 환경에서 적용 가능한

분산형 연합학습 알고리즘을 제안한다. 이 방식은 일반적인 머신러닝 학습 정확도와 비교하여 좋은 성능을 보여준다.

2. Related Works

분산 연합학습 알고리즘에 대한 몇 가지 논문을 살펴보고자 한다.

“Fully decentralized federated learning”이란 제목의 논문[2]은 2018년에 처음으로 소개된 논문으로 분산형 연합학습이란 무엇인가를 소개한다. 분산형 연합학습은 중앙 집중식 연합학습과 달리 중앙 서버가 필요 없는 분산형 네트워크 아키텍처이며 분산형 연합학습을 사용하면 클라이언트 간에 직접 통신할 수 있으므로 통신 리소스를 크게 절약할 수 있음을 알리고 있다.

탈중앙적인 환경에서의 연합학습 아키텍쳐, 네트워크 토폴로지, 통신 매커니즘, 보안, 핵심 성과지표(KPI), 최적화 기법 등 분산 연합학습의 기본적인 측면(aspects)을 살펴보는 논문도 있다[3]. 이 논문에서는 분산 연합학습의 동향, 배울 점, 과제에 대해 논의하며 정교한 연합 아키텍처, 최적화 기법, 다양한 시나리오에서 사용 가능한 견고한 애플리케이션의 필요성을 강조한다. 또한, 이 논문은 분산 연합학습의 한계를 파악하여 이기종(Heterogeneous) 데이터셋, 사이버 공격, 5G/6G와 같은 첨단 통신 기술 활용 등 향후 연구의 토대를 제시하고 있다.

다양한 방향의 분산형 연합학습에 대한 연구가 이루어지며 다양한 알고리즘이 소개되었다. 그 중 하나인 “Decentralized federated learning through proxy model sharing”이란 논문[4]에서는 ProxyFL이라는 분산형 연합 학습 알고리즘을 제안하며, 이를 통해 다중 기관 간 협력을 가능하게 하고 각 참여자의 데이터 개인 정보 보호를 향상시킬 수 있다고 소개한다. ProxyFL은 각 참여자가 개인 모델과 공개적으로 공유되는 프록시 모델을 유지함으로써 효율적인 정보 교환을 가능하게 하며, 중앙 서버 없이 모델의 다양성을 허용한다. 실험 결과는 ProxyFL이 기존 방법보다 훨씬 적은 통신 오버헤드와 강력한 개인 정보 보호를 제공하며, 이미지 데이터셋과 암 진단 문제에서 우수한 성과를 보여준다.

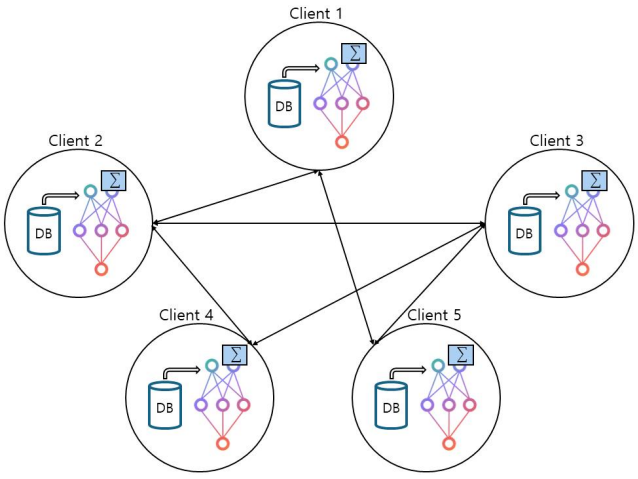
이 연구는 연합 학습 분야에서 혁신적인 접근 방식을 제시하며, 보다 효율적이고 안전한 협업 환경을 제공할 수 있다.

3. Proposed Method

본 논문에서는 실제 환경에서 적용 가능한 분산형 연합학습 알고리즘을 제안한다.

일반적인 분산형 연합학습 알고리즘은 대게 완전 연결로 이루어진 환경에서 적용되어 진다. 하지만 우리가 실생활에서 사용하는 환경은 완전 연결로 이루어진 환경 뿐만 아닌 특정 부분만 연결된 환경 또한 존재한다. 이러한 점에서 착안하여 실제 환경에서 적용 가능한 비-완전 연결 분산형 연합학습 알고리즘을 제안한다.

다음 [그림 1]과 같이 비-완전 연결 분산형 연합학습은 완전 연결 환경이 아닌 특정 부분만 연결된 환경에서 적용된다. 각 노드는 모든 노드와 통신하는 것이 아닌 연결된 노드와만 통신하며 각 노드는 각자 데이터셋으로 학습된 로컬 모델을 연결된 노드에 전송한다. 공유된 모델은 각 노드에서 자체적으로 집계하여 각 노드마다 독립된 글로벌 모델을 만든다. 위 과정을 반복하여 최종적으로는 각 노드의 데이터 유출 없이 각 노드의 독자적인 글로벌 모델을 생성할 수 있다.

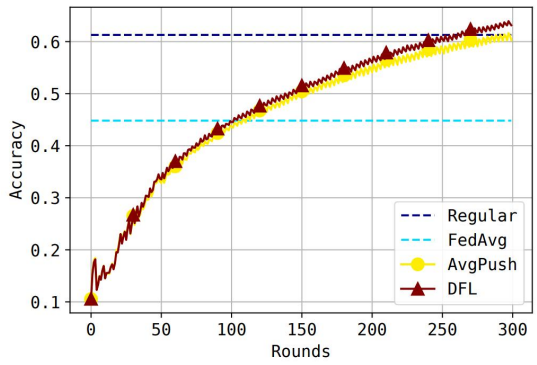


[그림 1] 비-완전 연결 분산형 알고리즘 구조도

4. Experiments

실험에 사용된 데이터셋은 MNIST로 각 노드마

다 28*28 사이즈의 이미지 데이터를 6천개의 학습 데이터와 1천개의 테스트 데이터로 구성하여 총 8개의 노드로 실험을 진행하였다. 실험 방식은 본 논문에서 제안된 메소드를 다양한 머신러닝 학습 메소드와 비교하는 방식으로 진행하였다. 사용된 머신러닝 메소드는 총 4가지로 “FedAvg”, “AvgPush” “Regular”, 그리고 본 논문에서 제안한 “DFL”로 구성되었다. FedAvg는 일반적인 연합학습 메소드이며, AvgPush는 분산형 시스템에서 사용되는 알고리즘인 PushSum 알고리즘을 사용하여 집계한 연합학습 메소드이다. Regular는 일반적인 머신러닝 메소드로 과적합 방지하는 기법을 추가한 메소드이다.



[그림 2] 분산형 연합학습을 적용한 실험 결과

[그림 2]는 분산형 연합학습 알고리즘(DFL)과 다른 연합학습 알고리즘을 비교한 결과이다. Regular와 FedAvg는 각각을 머신러닝과 연합학습의 대표적인 기준으로 삼아 가장 높은 수치의 정확도에 맞추어 표시하였다. AvgPush는 분산형 시스템에서 사용되는 알고리즘이 적용된 만큼 일반적인 FedAvg보다 높은 성능을 보여주고 있다. 본 논문에서 소개한 DFL은 일반적인 연합학습인 FedAvg보다 현저하게 높은 성능을 보여줌과 동시에 일반적인 머신러닝인 Regular보다 나은 성능을 보여주고 있다. 이를 통해 본 논문에서 소개하는 분산형 연합학습 알고리즘이 일반적인 연합학습 알고리즘과 비교해도 손색없는 결과를 보여주고 있음을 알 수 있다.

5. Conclusion

본 논문에서는 서버가 없는 환경에서 데이터 프라이버시를 보장하며 실전 분산형 환경과 유사한 비-완전 연결 분산형 연합학습 알고리즘을 제안한다.

제안된 알고리즘은 특정 노드와만 연결 되어있는 분산 환경에서의 연합학습 알고리즘으로 일반적인 머신러닝 알고리즘의 정확도와 비교하여 비슷하거나 더 높은, 상당히 준수한 성능을 보여주고 있다. 또한, 연합학습 알고리즘을 기반으로 한 만큼 데이터의 유출 없이 클라이언트 내부에서만 학습이 진행되어 개인 정보를 보호하는데 용이하다. 중앙 서버가 존재하는 환경이 아닌 중앙 서버가 없는 환경에서도 적용 가능하며 모든 노드가 서로 연결 되어있지 않은 환경에서도 사용 가능하여 의료, 물류, 군사 등의 다양한 산업 분야에서 사용될 수 있다.

사사문구

본 성과는 과학기술정보통신부의 재원으로 한국연구재단의 지원을 받아 수행된 연구이며 (NRF-2022R1A2C4001270), 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2022-2020-0-01602).

참고문헌

[1] McMahan, Brendan, et al. "Communication-efficient learning of deep networks from decentralized data." Artificial intelligence and statistics. PMLR, 20-22 Apr, 2017.

[2] Lalitha, Anusha, et al. "Fully decentralized federated learning." Third workshop on bayesian deep learning (NeurIPS). Dec. 2018.

[3] E. T. Martínez Beltrán et al., "Decentralized Federated Learning: Fundamentals, State of the Art, Frameworks, Trends, and Challenges," in IEEE Communications Surveys & Tutorials, vol. 25, no. 4, pp. 2983-3013, Fourthquarter 2023,

[4] Kalra, Shivam, et al. "Decentralized federated learning through proxy model sharing." Nature communications 14.1 (2023): 2899.