기반모델(Foundation Model)과 연합학습(Federated Learning)의 동향

이태환, 윤성환*
울산과학기술원

taehwan@unist.ac.kr, *shyoon8@unist.ac.kr

A Survey on the Foundation Model and Federated Learning

Taehwan Lee, Sung Whan Yoon*
Ulsan National Institute of Science and Technology

요 약

본 논문은 연합 학습(Federated Learning, FL)과 기반 모델(Foundation Model, FM) 사이의 상호작용을 심층적으로 분석하고, 두 기술의 결합을 통해 AI 분야에서 해결할 수 있는 다양한 문제점과 새로운 가능성에 대해 논의한다.

I. 서 론

기반 모델(Foundation Model, FM)은 GPT, BERT, CLIP 와 같은 대규모 사전 학습된 모델들로, 거대한 매개변수와 사전 학습된 지식을 통해 다양한 AI 분야에서 뛰어난 성능을 발휘한다. 이러한 모델들은 자연어 처리, 이미지 생성, 번역 등에서 높은 성과를 보이며, AI 연구와 실무 전반에 걸쳐 큰 변화를 일으켰다. 하지만 FM 을 훈련하기 위해서는 대규모 데이터와 막대한 계산 자원이 필요하며, 이는 데이터 저장과 계산 자원에 대한 비용문제로 이어진다. 연합 학습(Federated Learning, FL)은 분산된 데이터를 활용하여 여러 사용자들이 자신들의 데이터를 공유하지 않고 모델을 훈련할 수 있게 하는 학습 방법이며, 데이터 프라이버시 보호를 위한 기술로, 헬스 케어, 금융, 영상 감시, 개인화 추천 시스템 등에서 점점 더 중요해지고 있다. FL 의 분산학습 및 데이터 프라이버시 보호 특성은 FM 의 훈련에서 발생하는 데이터 부족 문제와 계산 자원 문제를 해결하는 데 기여할 수 있다. 본 논문에서는 FM 과 FL 을 활용해 각각의 기술이 가진 문제점 및 한계를 해결 할 수 있는 방법에 대해 논의한다.

II. Foundation model 과 Federated learning 의 관계

기반 모델(FM)과 연합학습(FL)의 특성을 통해 서로 기여할 수 있는 부분에 대해 제시한다.

FL 이 FM 에 기여하는 부분

1. **데이터 부족 문제 해결**
   FM 은 매우 많은 개수의 모델 파라미터를 가지고 있으며, 이를 학습하기 위해서는 고품질 및 대규모 데이터가 필요하다. 하지만, 이러한 대규모 데이터를 관리하기 위해서는 매우 많은 량의 저장장치를 필요로 한다. 이때, FL 을 통해 사용자들이 가진 데이터를 활용한다면, 서버의 저장장치에 대한 비용문제를 해결할 수 있다. 또한, 각 사용자는 자신이 가진 데이터를 서버에 업로드 하지 않기 때문에, 데이터 프라이버시를 보호하고 FM 의 학습을 위한 데이터 부족 문제를 해결할 수 있다.

2. **계산 자원 공유**
   FM 훈련에는 막대한 계산 자원(CPU, GPU)을 필요로 한다. 예를 들어, LLaMA [1] (65 billion parameters)를 학습하기 위해 2048 개의 NVIDIA A100 GPUs 와 21 일의 학습 시간을 필요로 하는데, 이러한 연산량의 부담을 줄이기 위해 FL 을 활용할 수 있다.
   FL 에서 서버는 자신이 가진 모델을 사용자에게 분배하고, 사용자는 분배 받은 모델을 자신이 가진 데이터에 대해 학습을 진행한다. 즉, 서버의 학습을 위한 연산을 여러 사용자에게 나눠, FM 의 학습에 필요한 연산 부담을 분산할 수 있고, 서버와 각각의 사용자는 자신이 가진 계산 자원을 활용해 더 많은 데이터와 연산을 통해 학습된 FM 을 얻을 수 있다.

FM 이 FL 에 기여하는 부분

1. **성능 향상 및 학습 속도 증가**
   FM 은 사전 학습된 거대 모델로, Downstream task 를 활용해 FL 환경에서 빠른 수렴과 높은 성능을 제공할 수 있다. 특히, FL 환경에서 성능에 치명적인 영향을 미치는 사용자간 데이터 분포의 이질성(non-IID)환경에 취약한 성능을 보이는데, FM 을 작은 모델로 지식

증류(Knowledge Distillation)를 통해, 이질성에 강건한 모델을 학습할 수 있다. 이로 인해 FL 에서의 학습 속도 및 성능을 향상시킬 수 있다.

2. 합성 데이터 생성

모델 학습에 필요한 데이터를 FM 을 활용해 합성 및 생성함으로써 데이터 다양성을 늘리고, 과적합을 줄이며, 민감한 데이터의 프라이버시를 보호할 수 있다. 예를 들어, 새로운 도메인을 위한 Fine tuning 을 진행할 때, FM 을 활용한 데이터 합성을 진행할 수 있고, 의료 데이터나 금융 데이터와 같은 민감한 정보를 학습해야 할 때, FM 이 생성한 합성 데이터를 사용하여 원본 데이터를 직접 노출하지 않고도 학습이 가능하게 만든다.

III. 주요 도전 과제

1. FM 의 자원 소모 문제(메모리 및 계산 자원)

FM 의 크기가 매우 커질수록 FL 환경에서 사용자가 이를 활용하는 데 필요한 메모리, 통신 및 계산 리소스가 증가한다. 예를 들어, GPT-3 는 1,750 억 개의 모델 파라미터를 가지고 있으며, 이를 저장하고 처리하기 위해서는 대규모의 저장 장치 및 연산 자원을 필요로 한다. 하지만, FL 환경의 사용자가 보유한 연산 장치는 이러한 큰 모델을 처리하기 어려울 수 있다.

2. 보안 위협

FL 을 통해 다양한 클라이언트가 참여하면서 악성 공격자가 모델 업데이트 과정에 침투할 수 있는 가능성도 커진다. 이러한 보안 위협을 차단하고 모델의 무결성을 유지하기 위한 보안 메커니즘도 중요하다.

3. 저작권 침해 위험

FM 이 학습한 데이터는 주로 인터넷에서 크롤링된 대규모 데이터이다. 이러한 데이터 중에는 저작권 문제를 일으킬 수 있는 콘텐츠도 포함될 수 있다. 예를 들어, Stable Diffusion [2]과 같은 텍스트-이미지 모델은 LAION-5B [3] 데이터셋을 사용하여 학습하지만, 이 데이터셋에는 저작권 문제가 있는 이미지가 포함되어 있을 가능성이 있다.

IV. 향후 연구 방향

1. 메모리, 통신, 계산 최적화(효율적인 분산 학습 알고리즘)

FL 환경에서 대규모 FM 을 학습하는 데 필요한 메모리, 통신, 계산 자원을 줄이기 위한 효율적인 분산 학습 알고리즘이 필요하다. 예를 들어, Transformer 와 같이 큰 모델학습을 위해 서버와 사용자가 하나의 모델 구조를 여러 부분으로 나눠 [4,5] 사용자의 연산 부담을 줄일 수 있다.

2. 신뢰할 수 있는 FL 시스템 개발

FL 과 FM 이 결합된 시스템에서 프라이버시, 보안 등을 강화하는 기술이 필요합니다. 이를 통해 데이터와 모델의 무결성을 보장하고, 악의적인 사용자가 모델을 훼손할 위험을 차단할 수 있다.

3. 개인화된 연합학습

FL 환경에서 사용자의 데이터가 서로 다른 분포를 따를 때, 이를 효과적으로 처리할 수 있는 개인화된 FL 알고리즘도 중요한 연구 주제이다. 개인화된 모델을 각 클라이언트에게 맞게 조정하여 성능을 높이는 방법이 연구될 필요가 있다.

4. FL 의 법적 및 윤리적 문제

FM 이 생성한 합성 데이터가 실제 데이터를 모방할 경우, 개인정보 침해나 저작권 침해 문제가 발생할 수 있다. 따라서 합성 데이터가 실제 데이터와 충분히 다른지 확인할 수 있는 방법이 필요하다.

5. 인공지능으로부터 잊힐 권리(언러닝, unlearning)

FM 을 학습하기 위해 사용자의 다양한 학습 데이터를 사용한다. 하지만, 학습을 진행 한 이후에 자신이 학습한 데이터를 제거한 상태로 만들고 싶은 경우, 즉, 모델이 자신의 데이터를 학습하지 않은 상태로 만들 수 있는 언러닝에 대한 방법 또한 연구될 필요가 있다.

V. 결론

FM 과 FL 의 결합은 AI 의 새로운 가능성을 열어주며, 데이터 프라이버시, 계산 자원 및 데이터 효율화 등 다양한 이점을 제공한다. 또한, 새로운 도전 과제의 해결을 위한 연구의 필요성을 제시한다.

ACKNOWLEDGMENT

This work was supported by the Institute of Information & communications Technology Planning & evaluation (IITP) grant funded by the Korea government (MSIT) (No. 2021- 0-02201, Federated Learning for Privacy Preserving Video Caching Networks).

참 고 문 헌

[1] Touvron, Hugo, et al. "Llama: Open and efficient foundation language models." *arXiv preprint arXiv:2302.13971* (2023).

[2] Rombach, Robin, et al. "High-resolution image synthesis with latent diffusion models." *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*. 2022.

[3] Schuhmann, Christoph, et al. "Laion-5b: An open large-scale dataset for training next generation image-text models." *Advances in Neural Information Processing Systems* 35 (2022): 25278-25294.

[4] Thapa, Chandra, et al. "Splitfed: When federated learning meets split learning." *Proceedings of the AAAI Conference on Artificial Intelligence*. Vol. 36. No. 8. 2022.

[5] Tian, Yuanyishu, et al. "FedBERT: When federated learning meets pre-training." *ACM Transactions on Intelligent Systems and Technology (TIST)* 13.4 (2022): 1-26