크라우드 소싱 연합학습 모델 서비스 설계

문현수○ 이영석
충남대학교
munhyunsu@cnu.ac.kr, lee@cnu.ac.kr

Design a Crowd-sourcing Federated Learning Model Service

Hyunsu Mun○ Youngseok Lee
Chungnam National University

요 약

사용하기 쉬운 API를 가진 딥러닝 라이브러리가 공개됨에 따라서 비전문가들도 손쉽게 예측 모델을 학습시키고 사용할 수 있게 되었다. 하지만, 민감 정보가 포함된 데이터를 보유한 기관들은 정확도가 높은 모델을 위하여 더 많은 데이터가 필요하지만 각 기관이 서로 데이터를 공유하기 어렵다. 전이 학습을 통하여 적은 양의 데이터로도 높은 정확도의 모델을 학습시킬 수 있으나, 이것은 단방향 (1-way) 학습 응용이기 때문에 각 기관의 데이터를 모두 학습한 모델이 생성되지는 않는다. 본 논문에서는 기존 단방향 학습 모델 공유와 달리 다양한 기관 또는 사용자가 규모에 상관없이 양방향 (2-way) 으로 모델을 학습 및 활용할 수 있도록 연합학습을 활용한 크라우드 소싱 연합학습 서비스에 대한 설계를 제안한다. 실험에서는 전체 분류 클래스 중 부분적인 데이터만 가진 학습 참여자 10명이 이미지 분류 모델에 기여하는 시나리오를 진행하였다. 크라우드 소싱 모델이 중앙 학습 기준 모델 대비 정확도 1%밖에 차이가 나지 않음을 보였다. 이 결과는 기존 단방향 학습 모델을 연합학습을 통해 양방향 학습 모델로 개선하여 각 개인 또는 기관이 보유한 데이터를 하나로 모은 것처럼 모델을 학습하는 방법에 기여한다.

1. 서 론

최근 TensorFlow, Keras, PyTorch 와 같은 딥러닝 라이브러리가 학습을 위한 API를 지원함에 따라 비전문가들도 손쉽게 예측 모델을 사용할 수 있게 되었다. 또한, 전이 학습 (Transfer learning)이 활발히 연구되면서 ImageNet 같은 양질의 데이터로 학습된 모델을 통해 적은 데이터로도 높은 정확도의 모델 학습을 수행할 수 있게 되었다 [1]. MNIST, Tensorflow Datasets 등 다양한 공개 데이터와 ResNet, Inception 등 공개 모델을 사용하여 서비스 개발자가 직접 학습할 수도 있지만, 학습을 위한 컴퓨팅 파워와 시간이 많이 소요되어 Google, IBM과 같은 기관이 학습한 결과를 다운로드받아 활용한다. 이러한 구조는 큰 기관이 하나의 모델을 공유하고, 각 개발자는 모델을 활용해 자신의 서비스를 만드는 단방향 (1-way) 학습 응용이라고 할 수 있다 [2].

민감 정보가 포함된 의료, 주행, 음성, 얼굴 데이터 등을 보유한 기관들은 정확도가 높은 모델을 위하여 더 많은 데이터가 필요하지만 각 기관이 서로 데이터를 공유하기 어렵다 [3]. 정부 사업이나 기관 간 협약을 통해 학습을 위한 데이터를 공유하는 등 민감 정보를 학습해야 하는 영역에서도 딥러닝 활용을 시도하고 있으나 데이터 및 컴퓨팅 자원이 많은 기관에서만 사용 가능한 성과가 나오고 있다 [4]. 소규모 기관 또는 개인의 경우 적지만 양질의 데이터를 보유하고 있더라도 데이터 편향이 발생하여 모델을 학습하기 쉽지 않다.

본 논문에서는 연합학습을 활용한 크라우드 소싱 모델 학습 서비스 설계를 제안한다. 제안 방법을 통하여 기존 단방향 학습 모델 공유와 달리 다양한 기관 또는 사용자가 규모에 상관없이 양방향 (2-way) 으로 모델을 학습 및 활용할 수 있다. 특히, 데이터를 공유하지 않고 모델 학습 결과만 공유하는 연합학습을 활용하여 민감 정보가 포함된 데이터도 개인정보 노출 우려 없이 학습에 사용할 수 있다. 연합학습에 참여하는 클라이언트마다 보유한 데이터양과 컴퓨팅 파워가 다르므로 학습이 비동기로 완료되는 것을 고려하였다 [5].

제안 서비스가 양방향 학습을 제공할 수 있음을 보이기 위하여 gRPC를 활용한 TensorFlow 크라우드 소싱 모델 API 개발 및 이미지 분류 모델 연합학습을 수행하였다. 크라우드 소싱 모델 학습 서비스는 다양한 개발자 또는 기관이 쉽게 접근할 수 있도록 쉬운 API를 제공하였다. 구현 서비스 활용 실험에서는 전체 20개의 클래스 중 최대 10개 클래스에 대한 데이터만 보유한 학습 참여자 10명이 이미지 분류 모델에 기여하는 시나리오를 살펴보았다. 실험 결과 크라우드 소싱 이미지 분류 모델이 중앙 학습 기준 모델 대비 정확도 1%밖에 차이가 나지 않았다. 이 결과는 기존 단방향 학습 모델을 양방향 학습 모델로 개선하여 각 개인 또는 기관이 보유한 데이터를 하나로 모은 것처럼 모델을 학습하는 방법에 기여한다. 크라우드 소싱을 통해 다양한 데이터가 학습된 모델은 소규모 기관에서 쉽게 나타나던 편향성을 없앨 수 있고, 대규모 기관에서도 소규모 기관이 보유한 양질의 데이터를 활용할 수 있게 된다.

2. 크라우드 소싱 연합학습 모델 서비스

그림 3은 크라우드 소싱 모델 학습 서비스의 구조로 gRPC 기반의 앱 서버와 데이터베이스로 구성된다. 서비스를 이용하는 사용자는 크게 모델 관리자와 학습 참여

이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(IITP-2019-0-01343)

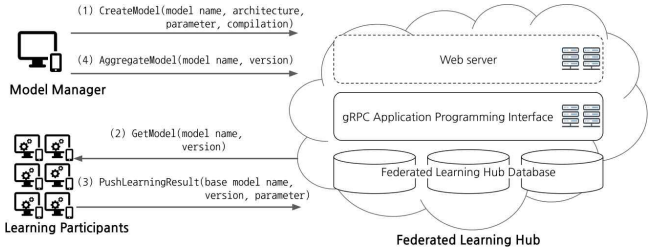

그림 3. Federated Learning Hub architecture and simple scenario.

자로 나누어지는데 각 역할에 맞추어 다른 기능이 제공된다. 모델 관리자는 모델의 생성과 병합을 담당하며 학습 참여자는 특정 모델에 대하여 자신의 데이터로 학습한 결과를 반환한다. 이때, 학습 참여자마다 학습 결과를 반환하는 시점이 다르므로 모델 관리자는 서비스에 업로드된 학습 결과 현황을 살펴보고 병합 명령을 내린다.

제안 서비스의 가장 간단한 사용 시나리오는 4단계로 이루어진다 (그림 3). (1) 모델 관리자는 본 서비스에 모델 이름과 형태, 초기 가중치, 학습 방법을 업로드하여 새로운 모델을 생성한다. (2) 이미지 분류 데이터셋을 가지고 있는 학습 참여자는 서버에서 모델을 다운로드받아 자신의 데이터로 모델을 학습시킨다. (3) 학습 참여자가 비동기적으로 모델 학습을 완료하고 나면 학습 결과를 서버로 전송하고, 서버는 해당 학습 결과를 데이터베이스에 기록한다. (4) 모델 관리자는 적당한 시간이 지나 모델에 대한 학습 기여가 충분히 이루어졌다고 판단되었을 때 모델 이름과 기준 버전을 인자로 모델 병합 명령을 내린다. 모델 병합 명령을 받은 앱 서버는 해당 모델 이름과 기준 버전에 기여된 학습 결과를 데이터베이스에서 불러와 연합 병합 (Federated average) 연산을 수행한 후 증가된 버전과 함께 데이터베이스에 기록한다.

본 서비스에서 모델 이름과 모델 버전은 동시에 여러 개의 모델을 서비스하고 비동기적으로 반환되는 학습 결과를 처리하기 위하여 필수적인 요소이다. 모델 이름은 모델 관리자 및 학습 참여자가 대상 모델을 식별하기 위하여 사용된다. 모델 버전은 보통 연합 병합이 진행될 때마다 증가하게 되어 모델에 학습 결과가 적용되었는지 구분할 수 있게 한다. 또한, 학습 참여자는 자신이 학습에 참여한 모델의 이름과 버전을 기록함으로써 중복 학습 참여를 방지할 수 있다. 학습 관리자는 학습 참여자가 학습 결과를 업로드할 때 함께 알려주는 기준 버전을 통하여 비동기적으로 반환되는 학습 결과를 처리할 수 있다. 예를 들어, 연합 병합을 수행하여 새로운 가중치로 개선이 이루어진 모델에 과거 버전을 기준으로 한 학습 결과가 반환되었을 때 학습 관리자는 해당 학습 결과를 무시할 수 있다.

서버와 모델 관리자 또는 학습 참여자는 다양한 프로그래밍 언어에 대한 제약 없이 사용할 수 있도록 gRPC에서 지원하는 데이터 타입으로 정보를 주고받는다. 제안 서비스가 제공하는 gRPC 메시지 및 Protocol Buffer로 서비스에서 제공하는 모델의 이름과 학습 현황을 확인하거나 TensorFlow 모델을 다운로드받을 수 있다. 모델에 기여된 학습 결과 현황을 요청하고, 연합 병합 지시와

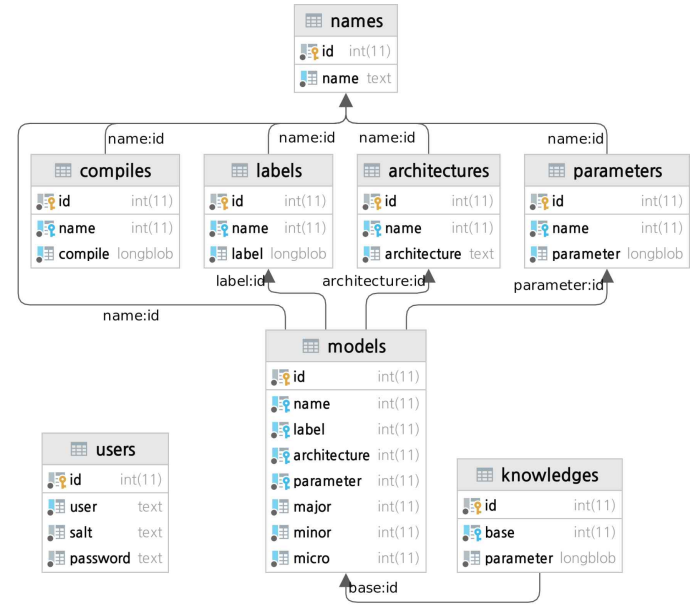

그림 4. Relational database schema for Federated Learning Hub

같은 모델 관리 메시지는 gRPC 메시지에 API key를 함께 전송하여 인증을 수행한다. 제안 서비스가 gRPC로 구현되어있기 때문에 사용자가 웹을 통해 모델을 다운로드받고 학습 결과를 업로드할 수 있는 웹 서버를 쉽게 연결할 수 있다.

본 서비스에서 제공하는 모델과 업로드되는 학습 결과를 쉽게 관리하고 규모확장성을 보장하기 위해서는 정보를 데이터베이스에 저장하여야 한다. TensorFlow, PyTorch 와 같은 딥러닝 라이브러리는 학습 모델을 파일로 저장하는 API만 제공되기 때문에 모델의 정보와 학습 결과, 학습 정보 등을 데이터베이스에 저장할 수 있는 자료형으로 변환하였다. 그림 4는 제안 서비스의 관계형

표 1. Dataset metadata for experiments

Train datasets	MNIST fashion 60,000 images CIFAR10 50,000 images
Test datasets	MNIST fashion 10,000 images CIFAR10 10,000 images
Classes	'Airplane', 'Ankle boot', 'Automobile', 'Bag', 'Bird', 'Cat', 'Coat', 'Deer', 'Dog', 'Dress', 'Frog', 'Horse', 'Pullover', 'Sandal', 'Ship', 'Shirt', 'Sneaker', 'T-shirt', 'Trouser', 'Truck'
Clients	5 with MNIST fashion 5 with CIFAR10
Dataset distribution	Random sampling of 6,400 images per round

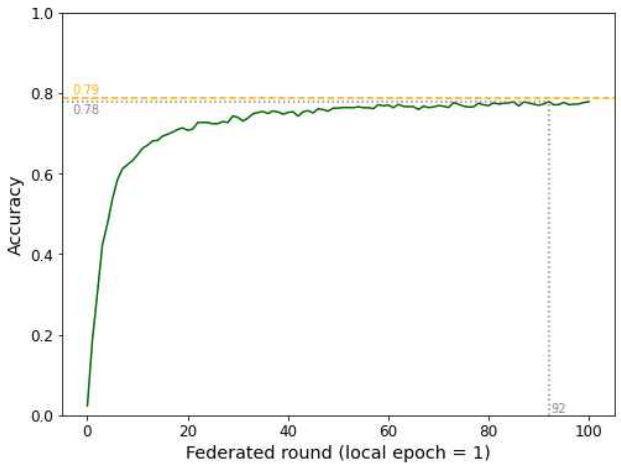

그림 5. Crowd-sourcing CNN model accuracy (baseline: centralized learning)

데이터베이스 (RDB) 구조로 모델 구조 (architecture) 와 가중치 정보 (parameter)가 각각 JavaScript object notation (JSON)과 Binary large object (BLOB) 형태로 저장한다. 모델 및 학습 정보를 RDBMS 에 저장함으로써 데이터베이스 서버를 독립적으로 관리하고 확장할 수 있도록 하였다.

3. 이미지 분류 모델 크라우드 소싱 연합학습 실험

본 논문이 제안하는 크라우드 소싱 모델 학습 서비스가 딥러닝 모델을 양방향으로 학습 및 기여할 수 있음을 보이기 위하여 활용 실험을 수행하였다. 실험은 이미지 분류 모델에 대하여 학습 참여자가 각각 다른 데이터셋으로 모델을 학습시켰다. 표 1은 실험 시나리오 및 데이터셋에 대한 설명으로 MNIST fashion 데이터셋을 가진 학습 참여자 5명과 CIFAR10 데이터셋을 가진 학습 참여자 5명이 본 서비스의 간단 이미지 분류 모델을 크라우드 소싱으로 기여한다. 학습 참여자들은 각자 자신의 학습 데이터셋에서 무작위로 샘플링하였는데, 예를 들어 MNIST fashion 데이터셋을 가진 학습 참여자들은 MNIST fashion 데이터셋에서 각자 샘플링하였다. 현실 환경에서는 학습 참여자가 항상 같은 데이터를 가지고 있을 수 없으므로 매 라운드에 모든 학습 참여자들이 새롭게 데이터를 샘플링하여 기여하였다. 모델 관리자는 학습 참여자 10명이 모두 기여하면 모델 병합 명령을 내렸다. 서비스 소스코드 및 학습 참여자 코드는 Github에 공개되어 있다[1].

그림 3은 모델이 새로 생성되었을 때부터 라운드에 따른 정확도를 나타낸다. 비교 기준 모델은 같은 모델 구조에 대하여 모든 학습 참여자가 보유한 데이터를 하나의 서버에서 중앙 학습으로 얻어진 정확도이다. 서버에 생성된 모델에 대하여 각 학습 참여자들이 자신의 데이터로 기여한 결과 학습 정확도가 기준 모델과 비교해 1% 차이가 났다. 전체적인 정확도는 조금 낮아졌지만, 학습 참여자 중 누구도 20개 클래스 모든 데이터를 가지고 기여하지 않았음에도 불구하고 모든 클래스를 분류할 수 있게 되었다. 이는 모델 관리자가 목표 레이블(Label)을 적절하게 설정하면 Non independent and identically distributed dataset (Non-IID dataset) 환경에서도 학습이 잘 완료됨을 나타낸다.

gRPC를 통해 모델을 다운로드 받는 본 제안 서비스는 TensorFlow에서 직접 모델을 생성하는 학습 코드와 크게 차이 나지 않아 사용하기 쉽다. 서버에서 생성이 완료된 모델 객체를 전송하기 때문에 Bytes 데이터를 TensorFlow Model 객체로 변환하기만 하면 바로 사용할 수 있다. 학습 결과를 반환할 때도 연합 병합과 같은 복잡한 작업은 서버에서 수행하기 때문에 학습 참여자는 gRPC를 이용하여 학습 결과만 반환하면 된다.

4. 결론

본 논문은 데이터가 많고 컴퓨팅 자원이 풍부한 기관에서 딥러닝 모델을 학습한 후, 소규모 개발자 또는 기관에서는 해당 모델을 이용하기만 하는 단방향 (1-way) 문제를 해결하기 위하여 크라우드 소싱 모델 학습 서비스 설계를 제안하였다. 연합학습을 활용한 양방향 (2-way) 모델 학습을 통하여 양질의 적은 데이터가 있는 학습 참여자들이 하나의 공통 모델을 학습시키고 개선해 나갈 수 있음을 보였다. 전체 모델의 분류 클래스 20개 중에서 최대 10개 클래스의 부분적인 데이터만 가진 학습 참여자 10명이 크라우드 소싱으로 이미지 분류 모델을 학습하는 실험을 통하여 모든 데이터를 가진 중앙 학습 모델과 비교해 정확도가 1%밖에 차이가 나지 않음을 보였다. 전체적인 정확도는 조금 낮아졌지만, 학습 참여자 중 누구도 20개 클래스 모든 데이터를 가지고 기여하지 않았음에도 불구하고 모든 클래스를 분류할 수 있었다. 본 제안은 크라우드 소싱을 통해 규모에 상관없이 모든 개인 또는 기관이 좋은 공통의 모델을 만들기 위하여 연합하는 방법에 기여한다.

참고 문헌

[1] S. J. Pan and Q. Yang, “A survey on transfer learning,” IEEETransactions on knowledge and data engineering, vol. 22,no. 10, pp. 1345-1359, 2009.
[2] B. Neyshabur, H. Sedghi, and C. Zhang, “What is being trans-ferred in transfer learning?,” arXiv preprint arXiv:2008.11687,2020.
[3] N. Rieke, J. Hancox, W. Li, F. Milletari, H. R. Roth, S. Al-barqouni, S. Bakas, M. N. Galtier, B. A. Landman, K. Maier-Hein,et al., “The future of digital health with federated learn-ing,” NPJ digital medicine, vol. 3, no. 1, pp. 1-7, 2020.
[4] T. Li, S. Hu, A. Beirami, and V. Smith, “Ditto: Fair and robustfederated learning through personalization,” inInternationalConference on Machine Learning, pp. 6357-6368, PMLR,2021.
[5] C. Park, S. Lee, and N. Lee, “Asynchronous federated learn-ing algorithm with decentralized data (in korean),” Communi-cations of the Korean Institute of Information Scientists andEngineers, vol. 38, no. 12, pp. 29-33, 2020.

1) https://github.com/munhyunsu/tff-app