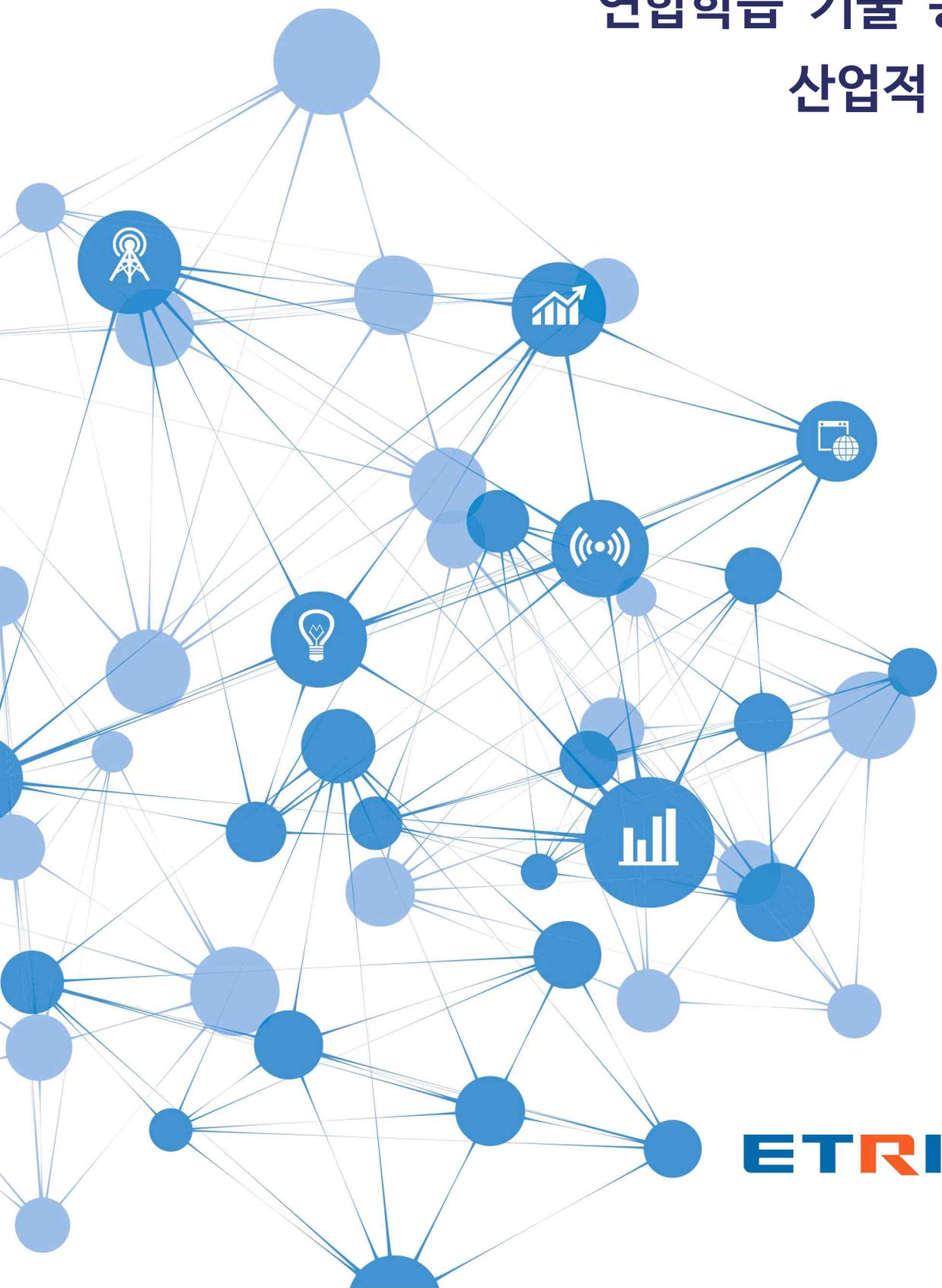
ETRI Insight

기술정책 트렌드 2020-06

연합학습 기술 동향 및 산업적 시사점

이승민



ETRI 한국전자통신연구원
Electronics and Telecommunications Research Institute

본 보고서는 ETRI 기술정책연구본부 주요사업인 **“국가 지능화 기술정책 및 표준화 연구”**를 통해 작성된 결과물입니다.

목 차

요 약

AI를 이용한 데이터 활용에 대한 요구가 증가하면서, 최근 기존 법적 규제와 충돌하지 않으면서 이를 해결하고자 하는 방안으로 연합학습이 급부상하고 있다. 특히 구글이 차세대 AI 학습으로 '연합학습'을 선택했다는 소식이 알려지면서 더욱 큰 주목을 받고 있다. AI 연합학습은 기존 분산 학습 개념과 유사하지만 분산된 데이터 자체를 보호하면서 협업 모델을 생성할 수 있다는 점에서 큰 차이가 있다.

분산형 데이터로는 스마트폰에서 생산되는 개인의 활동, 앱 사용 데이터뿐만 아니라 자동차의 주행 정보, 개인의 병원 진료 기록 등 다양하다. 그러나 이를 활용하는 과정에서 기존 분산형 학습 기술만으로는 해결할 수 없는 문제가 있다. 바로 프라이버시다. 연합학습은 프라이버시에 대한 '보호'와 '활용'이 양립할 수 있는 해법을 제시하고 있다는 점에서 의미가 크다.

본 보고서에서는 연합학습의 기술 동향과 산업적 활용 가능성에 대해서 살펴보았다. 첫째, 기술적 관점에서 연합학습의 기본 개념과 작동 원리를 알아보고 FedSGD, FedAVG 등 주요 알고리즘의 특징을 분석하였다. 또한, 연합학습 알고리즘의 프라이버시 보호와 보안성을 강화하기 위해 함께 사용하는 차등정보보호, 동형암호, 안전한 다자간 계산 알고리즘 등의 원리와 적용 방법을 살펴보았다. 연합학습을 현장에 적용하는 과정에서 해결해야 할 기술 이슈가 무엇인지, 그리고 이를 해결하기 위해 진행되는 연구 방향에 대해서도 간략하게 정리하였다.

둘째, 산업적 관점에서 연합학습이 적용되고 있는 현황을 분석하였다. 먼저, 데이터 3법의 주요 내용과 최근 연합학습의 적용이 가장 활발하게 진행되고 있는 의료 데이터의 특징 및 활용 현황을 살펴보았다. 연합학습은 여러 병원에 흩어져 있는 특정 질환에 대해 환자 데이터나 임상 데이터를 직접 공유하지 않고도, 프라이버시 노출 위험을 줄이면서 모든 데이터를 한곳으로 모아서 분석한 것과 같은 효과를 얻을 수 있다. 이런 장점으로 인해, 의료 영역은 연합학습의 활용이 가장 기대되는 분야이다. 관련하여 인텔과 엔비디아 등 ICT 기업과 글로벌 의료기관 간의 협력 현황과 연구 결과를 살펴보았다.

연합학습 방법은 향후 디지털 기술의 발전과 함께 사회적 이슈로 부상할 데이터의 소유권 강화와 데이터 활용을 위한 공유 문제를 해결할 대안으로 더욱 주목받을 것으로 보인다. 특히 전이학습, 암호화 알고리즘, 블록체인 등 기존 기술과 결합하여 다양한 산업 분야에서 의미 있는 결과를 낼 수 있을 것으로 전망된다.

Ⅰ 등장 배경

1 분산형 데이터의 증가

스마트 기기, 사물인터넷, 엣지 컴퓨팅 등 디지털 기술의 발전에 힘입어 개별 기기와 기관에서 독립적으로 생산, 수집, 저장하는 데이터양이 급속도로 증가하고 있다. 여기에는 개인의 활동, 앱 사용 정보 등 스마트폰에 축적되는 사용자 데이터와 가정 내 각종 디지털 제품에서 수집되는 생활 데이터, 자동차의 운행 데이터 등이 포함된다. 또한, 병원, 은행, 연구소 등 동일 목적을 위해 생산된 데이터[1)]가 유사한 형태로 저장되는 경우도 많다. 앞으로 초고속(5G), 초연결(IoT), 초지능(AI) 시대가 되면서 이런 분산형 데이터의 종류와 규모는 기하급수적으로 증가할 것으로 보인다. 특히 엣지 컴퓨팅의 발전은 분산형 데이터 생산을 가속할 것이다.

분산형 데이터의 증가는 데이터 '활용' 측면에서 새로운 요구를 만들고 있다. 첫째, 개인 맞춤형 서비스에 관한 것이다. 나에게 맞는 스마트폰 사용 환경, 온라인 쇼핑 추천, 건강 관리, 최적의 홈 에너지 관리 등이다. 둘째, 여러 사용자와 기관이 보유한 데이터를 통합·공유함으로써 새로운 비즈니스 기회와 지식을 발견하는 것이다. 여러 병원에 흩어져 있는 난치성 질환이나 신종 감염병 데이터를 공유하거나, 서로 다른 기관에서 동일 목적을 가지고 비슷한 시기에 진행되는 실험데이터를 통합하여 의미 있는 결과를 도출하고자 하는 경우이다.

이와 같은 목적을 달성하기 위해서 지금까지는 분산형 데이터를 중앙에 있는 클라우드 서버에서 모아서 AI 알고리즘을 이용하여 전체 데이터를 한꺼번에 처리(Centralized Learning 등)하였다. 그러나 흩어진 데이터를 한곳으로 모아 분석하기 위해서는 참여자의 이해관계, 효율성, 분석 시간, 비용 등 많은 제약이 따른다.

연합학습을 이용하면 분산된 로컬 데이터를 한곳으로 모으지 않고 데이터를 보유하고 있는 다양한 장치, 기관 등에서 독립적으로 데이터를 처리하되, 전체 데이터를 한꺼번에 처리하는 것과 비슷한 효과를 얻을 수 있다.

1) 병원의 진료·임상 데이터, 은행의 결재 데이터, 연구소의 실험 데이터 등

2 프라이버시 '보호'와 '활용' 양립 가능

AI는 데이터를 먹으며 성장한다. 그러나 AI 접근이 매우 제한된 영역이 있다. 개인의 의료 데이터, 금융데이터 등 개인정보 영역이다. 과연 AI 활용과 개인정보보호는 양립할 수 있는가? 이 무겁고 오래된 질문은 최근 세계가 경험하고 있는 코로나19 대응 과정에서 또다시 뜨거운 이슈로 부상하고 있다. 코로나19 확진자의 동선을 추적하기 위해서 프라이버시를 침해하는 것이 과연 바람직한지에 대한 논란이 그것이다. 그러나 개인정보 활용에 대한 일시적인 조치가 영구히 정착되거나 다른 산업 분야로 확산하는 데에는 적지 않은 반발이 예상된다.

유럽 연합은 EU 회원국에 속한 국민의 사생활 보호와 개인정보를 보호하는 규제인 '일반 데이터 보호 규칙(GDPR)'을 이미 2018년 5월 25일부터 적용하고 있다. 우리나라는 개인정보보호법, 정보통신망법, 신용정보법 등으로 구성된 '데이터 3법'이 2020년 1월 9일 국회 본회의를 통과한 후 하반기부터 본격 시행되고 있다. '데이터 3법'의 핵심은 사업자가 개인식별정보를 '가명화'하여 개인정보를 활용할 수 있도록 허용하겠다는 것이다. 그러나, 가명정보처리의 허용범위, 가명정보의 활용 및 결합 조건 등이 매우 모호하거나 엄격하게 규정되어 있어 개인정보 활용의 실효성 논란이 커지고 있다. 특히, 서로 다른 기관에서 보유하고 있는 개인정보를 결합하는 문제는 데이터 활용에 있어 또 다른 제약이 되고 있다. 이렇듯 개인 데이터 '보호'와 '활용'의 양립 가능성은 실현되기 매우 어려운 것으로 알려졌다.

최근 이러한 문제를 해결하는 데 연합학습(Federated Learning)이 새로운 가능성을 제시하고 있다. 각종 기기와 개별 기관에 흩어져 있는 개인 데이터를 '보호'하면서, 서로 협력하여 공유하는 효과를 낼 수 있는 AI 학습 '활용'이 가능하기 때문이다. 이뿐만 아니라 연합학습은 중앙에서 한꺼번에 처리하는 방법에 비해 학습 소요 시간을 줄일 수 있는 등 다양한 활용 가치를 보여주고 있다.[2)3)] 특히 의료 데이터를 중심으로 최근 활발히 진행되고 있는 연합학습 활용은 의료 데이터 혁신을 통해 서비스의 질적 수준을 한 단계 끌어올릴 것으로 기대된다.[4)]

---

2) H. B. McMahan et al., (2016), Federated Learning of Deep Networks using Model Averaging, arXiv:1602.05629v1.
3) J. Konečný et al. (2016), Federated learning: Strategies for improving communication efficiency, arXiv:1610.05492.
4) Karen Hao (2019), A little-known AI method can train on your health data without threatening your privacy, MIT Technology Review.

Ⅱ 연합학습 기술 동향

1 개념 및 작동 원리

연합학습이란 기기나 기관 등 여러 위치에 분산 저장된 데이터를 직접 공유하지 않으면서, 서로 협력하며 AI 모델을 학습할 수 있는 분산형 머신러닝 기법이다. 일반적으로 AI 모델을 만들기 위해서는 각 클라이언트(개인 기기, 개별 기관 등)가 보유한 데이터를 중앙서버에 모아서 일괄적으로 학습하게 된다. 반면, 연합학습에서는 클라언트 개별 데이터를 중앙서버로 전달하지 않고, 중앙서버의 AI 모델을 클라언트로 보내 각각의 데이터로 모델을 훈련한다. 그리고 클라우드인 중앙서버는[5] 개별 클라이언트에서 학습한 로컬 AI 모델을 모두 합쳐 글로벌 AI 모델을 만든다. 이 과정을 반복함으로써 중앙서버의 글로벌 AI 모델은 점점 일반화되고 클라이언트의 로컬 AI 모델의 정확도는 향상된다.

최근 연합학습이 주목받게 된 데에는 구글이 있다. 2017년 구글은 차세대 AI 학습 방법으로 연합학습을 선택하고, 스마트폰 사용자의 맞춤형 학습모델 개발에 연합학습 활용 방법을 제시했다.[6][7] 스마트폰에 저장된 데이터는 사진, 위치 정보, 비밀번호, 검색 단어, 대화 내용 등 민감한 개인정보를 담고 있어 가명화하기 어렵고 중앙서버에서 저장할 수 없기 때문이다.

로컬 단말(개별 스마트폰)이 평소에는 서버와 통신하지 않고 단말에 저장된 개인 데이터를 사용하여 로컬 AI 모델을 생성한다. 하지만, 단말의 전원이 연결되고 와이파이가 접속되는 등 특정 조건을 만족하면, 단말은 생성한 로컬 AI 모델의 결과값(파라미터)을 압축·암호화하여 클라우드 서버로 전달한다. 클라우드에서는 여러 사용자의 스마트폰에서 학습한 로컬 AI 모델의 정보를 결합하여 글로벌 AI 모델을 업데이트한다. 이렇게 개선된 글로벌 AI 모델은 다시 개인 스마트폰에 전송되어 기존 모델을 업데이트함으로써 점점 예측력이 높은 로컬 모델이 만들어진다. 구글은 이 방법을 자사의 안드로이드 기반 키보드 지보드(Gboard)에 사용했다. 스마트폰 사용

5) 중앙서버는 연합학습에 대한 횟수, 참여 클라이언트 결정 등 전반적인 통제권을 가진다.
6) 연합뉴스 (2019.8.22.), 당신이 잠들면 구글 AI는 학습을 시작한다.
7) Google (2017), Federated Learning: Collaborative Machine Learning without Centralized Training Data, Google AI Blog (https://ai.googleblog.com/2017/04/federated-learning-collaborative.html)

자의 정보를 서버에 전송하지 않고 개인의 단말에서 지보드 AI 모델을 학습한 것이다. 연합학습을 통해 지보드는 단어를 추천하고 검색어를 제안해준다. 단말은 서버로 사용자 데이터 원본을 보내는 것이 아니라 단말에서 학습한 결과값을 압축·암호화등을 거친 값을 전달한다. 이를 통해 단말에 저장된 사용자의 프라이버시 침해 가능성을 현저히 낮출 수 있다고 강조한다.

(그림-1) 구글이 제시한 스마트폰의 연합학습 활용 예

* 출처 : Google(2017)

스마트폰뿐만 아니라 개별 기관에서 독립적으로 보유하고 있는 데이터에 대해 연합학습을 적용하고자 할 경우에도 작동 원리는 비슷하다. 다만, 연합학습에 참여하는 전체 단말의 수가 적고 컴퓨팅 자원 등의 제약 조건이 다를 수 있다. 또한, 개별 기관의 시스템과 데이터의 통계적 이질성 등의 문제가 추가로 발생할 수 있다.

기존 분산학습과 차이점을 포함하여, 스마트폰 등 로컬 디바이스가 참여하는 연합학습과 기업, 조직 등 개별 기관들이 협업하는 연합학습의 특징을 살펴보면 다음 표와 같다. 단, 표에서 분산학습은 데이터센터 내 분산된 서버에 데이터가 저장된 환경에서 모델을 학습하는 경우이고, Cross-silo는 의료, 금융 기관 등 다양한 기업과 조직으로 구성된 경우, Cross-device는 매우 많은 수의 모바일 기기로 구성되어 연합학습에 참여하는 경우를 의미한다.

〈 표-1 〉 연합학습과 분산학습 비교

구분	분산학습 (Datacenter)	연합학습	
		Cross-silo	Cross-device
참여 환경	- 클라이언트가 하나의 클러스터나 데이터센터 내에 있는 컴퓨터 노드들로 구성	- 서로 다른 기업, 조직 (의료, 금융 등)단위에서 연합학습 클라이언트로 참여	- 매우 많은 수의 모바일 기기, IoT 기기 단위로 구성된 클라이언트가 연합학습에 참여
데이터 분포	- 데이터는 중앙에 저장 - 어떤 클라이언트라도 다른 클라이언트의 데이터를 읽을 수 있음	- **데이터가 로컬에서 생성되고, 분산되어 존재** - 각 클라이언트는 자신이 데이터를 저장하고, 다른 클라이언트의 데이터에는 접근할 수 없음 - Non-IID(Independent & Identically Distributed) Data	
통합 조정	- 중앙에서 통합하고 관리	- **중앙서버에서 전체 학습을 조정하고 관리** - 그러나, 중앙서버는 원본 데이터(raw data)를 볼 수 없음	
통신	- 하나의 데이터센터/클러스터 내의 모든 클라이언트는 연결됨	- Hub-and-spoke 형태로 구성 - Hub는 전체 학습을 조정(원본 데이터 없이)하고, 각 클라이언트에 연결	
데이터 가용성	- 모든 클라이언트는 거의 항상 가용		- 일부 클라이언트는 특정 순간(예: 주간)에만 가용
규모	- 1~1,000개 클라이언트	- 2~100개 클라이언트	- 대규모 병렬로 10^{10}개의 클라이언트까지 가능
주요 병목점	- 데이터센터 내 연산 능력(고속통신망 가정)	- 연산 능력과 통신 속도 모두	- 통신 속도(wi-fi 또는 느린 통신환경에서 작동)
주소 지정	- 클라이언트는 고유 ID 또는 이름을 지정		- 클라이언트 ID 없음(직접 인덱싱할 수 없음)
상태 유지	- 모든 클라이언트는 매 라운드에 참여하고 상태를 전달		- 클라이언트가 작업에 한 번만 참여할 수 있음(매 라운드에 새로운 클라이언트 참여 가능)
신뢰성	- 클라이언트 참여 실패 가능성이 적음		- 매 라운드에서 클라이언트 5%이상 실패가능(배터리, 통신 불안정 등)
데이터 분할	- 클라이언트 간 임의 분할/재분할 가능	- 수평(horizontal) 또는 수직(vertical)적[8] 고정 분할	- 수평(horizontal)적 고정 분할

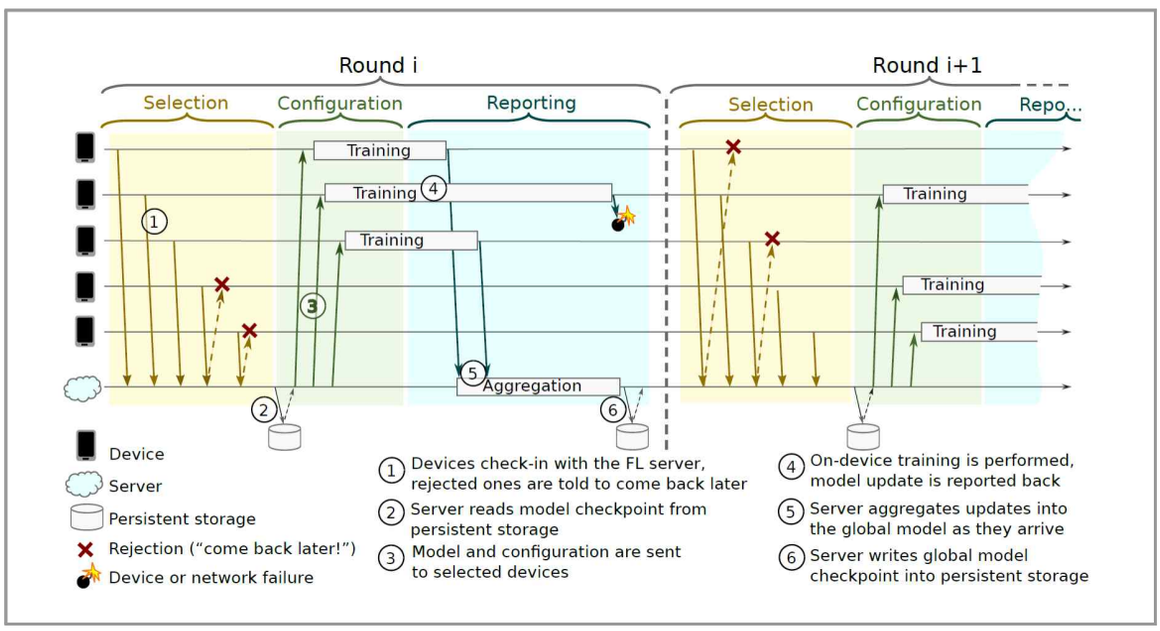
* 출처 : Peter Kairouz et al.(2019) 참고하여 재작성

8) 일반적으로 학습 데이터의 샘플 수를 늘리기 위한 조직 또는 단말 간 수평적 분할이 주로 사용되며, 수직적 분할은 동일 샘플의 특징값을 늘리기 위해 데이터를 공유하는 방법으로 동형암호, Secure Multi-Party Computation 등의 알고리즘과 함께 사용됨(Qiang Yang et al., 2019 참고).

2 프로토콜 및 주요 알고리즘

일반적인 연합학습 프로토콜은 다음과 같다.[9] AI 모델을 학습하기 위해서는 많은 양의 컴퓨팅과 통신 자원이 필요하기에 학습 가능 시간, 통신 상태 등 특정 조건이 만족 되어야만 연합학습이 진행된다. 조건을 만족한 단말은 우선 연합학습 참여자로 등록할 준비가 되었다고 서버에 통보한다. 참여자는 수십에서 수백만까지 가능하며, 서버는 서전에 정의된 최적의 참여자를 선정한 후 각 단말로 수행해야 할 작업 관련 정보를 전달한다. 단말은 서버로부터 전달받은 글로벌 AI 모델을 기반으로 로컬 AI 모델을 학습한다. 학습이 완료된 로컬 모델의 결과는 서버로 전달되고 서버는 글로벌 AI 모델을 업데이트한다. 이 과정이 (그림-2)의 Round i에 해당한다.

(그림-2) 연합학습 프로토콜

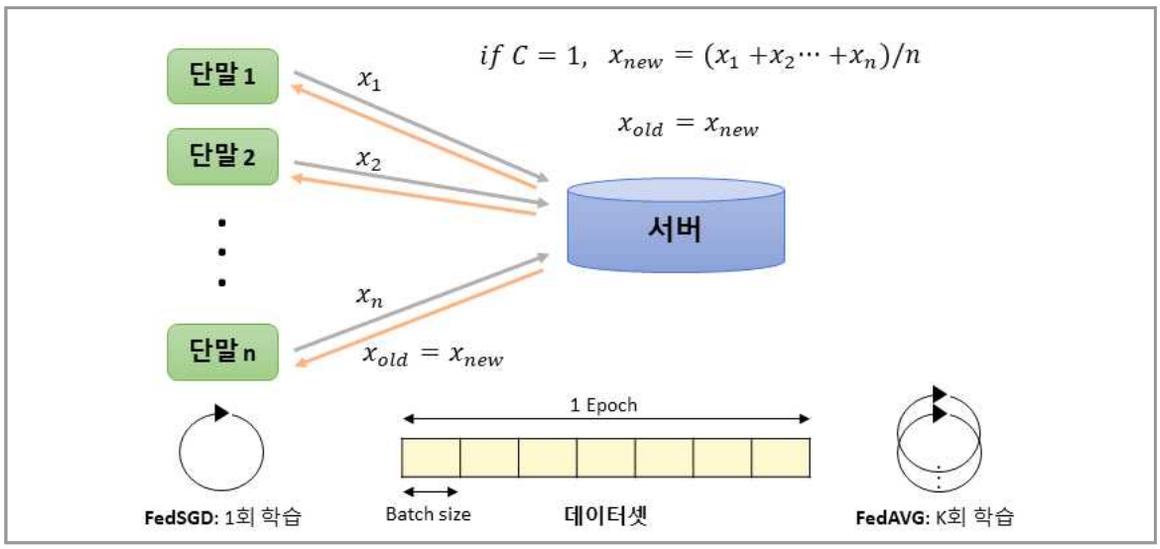


* 출처 : K. Bonawitz et al.(2019)

연합학습의 주요 알고리즘에는 FedSGD(Federated Stochastic Gradient Descent), FedAVG(Federated Averaging) 등이 있으며 다음과 같은 특징이 있다.

9) K. Bonawitz, et. al. (2019), Towards Federated Learning at Scale: System Design, arXiv: 1902.01046.

(그림-3) 연합학습 주요 알고리즘



* 출처 : 저자 작성

『 FedSGD (Federated Stochastic Gradient Descent)[10] 』

각 단말(엣지, 클라이언트)은 자신이 한번 학습한 파라미터 값(그림-3의 X: 딥러닝의 Gradient, W 등)을 중앙서버(클라우드)로 전달하고, 중앙서버는 취합한 모든 클라이언트의 로컬 파라미터 값의 평균을 계산하여 글로벌 파라미터를 업데이트하고 이 결과를 다시 모든 단말로 전달한다. 파라미터의 수렴 조건이 만족될 때까지 이 과정을 반복한다. (이때, 그림-3에서 하이퍼 파라미터 C는 서버에서 글로벌 파라미터를 계산할 때 사용할 단말의 비율이다. 예를 들어, C=1이면 모든 참여 단말을 사용하고 C=0.5이면 참여 단말의 50%만 사용한다)

『 FedAVG (Federated Averaging)[11] 』

각 단말이 일정한 횟수 K만큼 반복적으로 학습을 수행한 후의 파라미터 값을 서버로 전달하는 방식이다. 각 단말에서 batch size 크기로 나눠서 학습하여 minibatch 효과를 줌으로써 글로벌 파라미터가 수렴에 이르는 시간을 단축할 수 있다. 이 경우 최종 결과에 크게 영향을 미치는 변수로 하이퍼 파라미터 C, epoch와 batch size이

10) H. Brendan McMahan et al., Communication-efficient learning of deep networks from decentralized data, arXiv:1602.05629, 2016.
11) Xiang Li et al., On the convergence of fedavg on non-iid data, ICLR 2020.

다.[12] 즉, 설정된 이들 값에 따라 수렴에 이르는 시간이 오히려 길어질 수도 있다.

최근 연구에 따르면 앞서 설명한 연합학습 알고리즘만으로는 프라이버시 보호로부터 완전히 자유로울 수는 없다는 사실들이 증명되고 있다. 예를 들어, 단말에서 서버로 전달하는 Gradient 값을 통해 특정 속성을 가진 샘플이 어느 batch에 있는지를 확인할 수 있거나, GAN을 통해 학습 데이터와 유사한 데이터를 생성할 수 있을 뿐만 아니라, 심지어 원래의 학습 데이터까지도 복원 가능[13]하다는 논문이 발표되었다.

연합학습이 가진 이러한 프라이버시 및 보안 문제를 해결하기 위해 최근 다양한 알고리즘 연구가 진행되고 있다. 프라이버시 보장형 연합학습(Privacy-Preserving FL), 보안 연합학습(Secure FL), 보안 및 프라이버시 보장형 연합학습(Secure and Privacy-Preserving FL) 등 대표적이다. 기존 연합학습 과정에 다른 알고리즘을 추가 적용하여 프라이버시와 보안을 강화하려는 시도다. 이와 관련하여 차등정보보호(Differential Privacy), 동형암호(Homomorphic Encryption), 안전한 다자간 계산(Secure Multi-Party Computation) 등이 최근 주목받고 있다. 각각의 개념과 연합학습 적용 방안에 대해 살펴보면 다음과 같다.

『 차등정보보호 (Differential Privacy) 』

차등정보보호는 원래의 데이터에 수학적 노이즈를 추가하여 프라이버시 노출 위험을 낮추려는 기술이다. 이 개념은 Dwork(2016)가 제안한 것으로, 공개된 자료에 특정인의 정보가 포함되지 않은 경우에도 그 사람의 개인정보가 노출될 수 있다는 주장에서 비롯됐다.[14] Dwork는 하나의 개인정보가 전체 자료에 추가로 포함될 때 증가하는 노출 위험을 '차등정보보호'라고 정의하고 이를 수학적으로 측정하는 방법을 제안하였다. 즉, 차등정보보호란 주어진 질의(query)를 하나의 개인정보만 차이가 있는 두 개의 데이터베이스에 적용했을 때, 질의 결과의 차이를 제어함으로써 해당 개인정보에 대한 노출 위험을 제한할 수 있다는 것이다.

---

12) 1 Epoch: 모든 데이터셋을 한번 학습, 1 iteration: 1회 학습, minibatch: 데이터셋을 batch size 크기로 나눠서 학습 (예: 데이터셋이 100개, batch size가 20이면, 1 iteration = 20개 데이터에 대해 학습, 1 Epoch = 100/batch size = 5 iteration)

13) Ligeng Zhu et al. (2019), Deep leakage from gradients, NeurIPS 2019, p.14747-14756.

14) Dwork(2016)가 예로 든 사례는 다음과 같다. "Terry Gross는 리투아니아 여자의 평균 키보다 2인치 작다. 국가별 남녀의 평균 키를 제공하는 자료가 존재한다면 Terry Gross의 키는 노출될 수 있다."

◎ **차등정보보호의 수학적 정의**[15)]

Dwork(2016)는 $k: Y \rightarrow k(Y)$를 어떤 랜덤화 함수라고 정의하고, 어떤 두 개의 데이터베이스 Y_1과 Y_2간에 오직 한 명의 개인정보만 다르고 다른 개인들의 정보는 모두 동일하다고 가정한다. 만약 모든 경우의 집합 $S \subset Range(k)$에 대해서

$$\log\left(\frac{\Pr[k(Y_1) \in S]}{\Pr[k(Y_2) \in S]}\right) \leq \epsilon$$

이 성립한다면, 랜덤화 함수 k는 ϵ-차등정보보호를 보장한다. ϵ가 작을수록 강한 수준의 정보보호 상태가 유지된다.

차등정보보호 기술은 FedSDG, FedAVG 등 연합학습 알고리즘을 사용하여 단말에서 학습한 결과값을 서버로 전달하는 과정에 적용된다. 즉, 파라미터에 노이즈를 줘서 프라이버시 노출을 방지하려는 것이다.

차등정보보호 기술은 2020년 MIT 10대 혁신 기술 가운데 하나로 선정되었고[16)], 올해 미국 인구 조사국은 3억 3천만 명의 미국인 데이터를 수집하는 과정에 이를 사용하고 있다. 애플은 이미 2016년 프라이버시를 침해하지 않고 이용자들의 행동 패턴을 파악하기 위해 차등정보호호 기술을 도입했다.[17)] 구글, 페이스북 등도 특정 사용자를 식별하지 않고 집계 데이터를 수집하는 등 개인정보가 포함된 데이터를 통합하고 사용자 현황과 패턴을 찾기 위해 차등정보보호 기술을 사용하고 있다고 밝혔다.

『 동형암호 (Homomorphic Encryption) 』

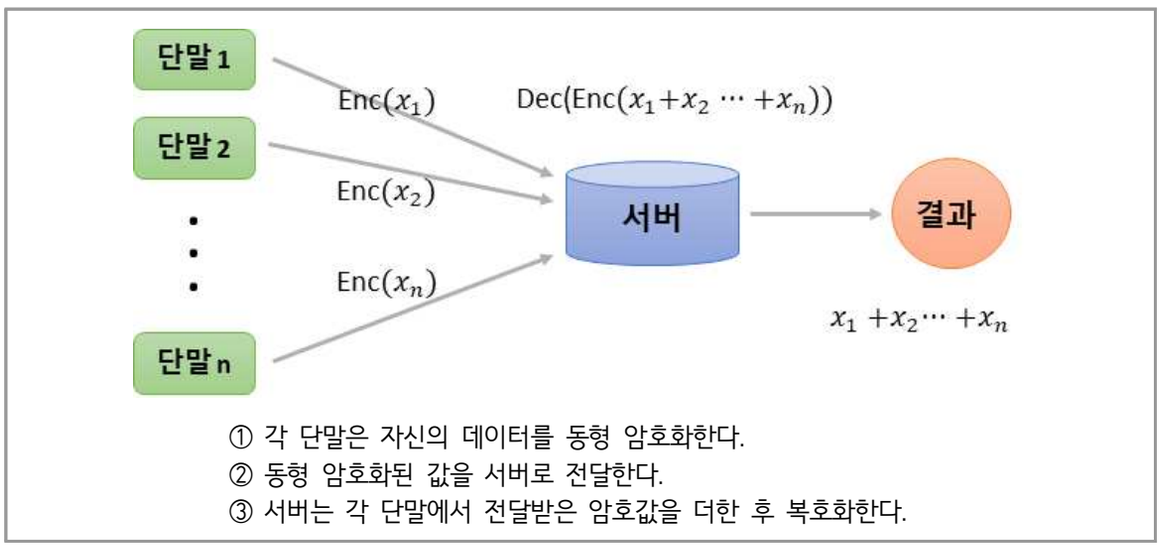
동형암호는 암호화된 데이터를 복호화 없이도 연산할 수 있는 암호기술이다. 즉, 평문을 암호화한 상태에서 각종 연산을 했을 때, 그 결과가 암호화하지 않은 상태의 연산 결과와 동일하게 나오는 암호 알고리즘이다. 동형암호는 1978년 Rivest, Addleman, Dertouzous 등이 제안하였고, 2009년 Gentry에 의해 동형암호의 안전성이 난제로 환원됨을 증명하였다.[18)] 2011년 MIT 10대 유망기술[19)] 가운데 하나로

15) Park, M-J., & Kim, H. J. (2016), Statistical disclosure control for public micro data: present and future, The Korean Journal of Applied Statistics, 29(6), 1041-1059.
16) MIT Technology Review (2020), 10 Breakthrough Technologies 2020.
17) 애플 시리(Siri)는 사용자의 목소리에만 활성화되도록 음성인식 기술을 개선하는 데 연합학습 기술을 사용했고, IOS 13에서는 퀵타입(Quick Type) 키보드 단어예측, 저장되지 않은 전화번호 예측 등에 연합학습을 적용했으며, 이 과정에서 '차등정보보호' 기술을 통합 적용함으로써 이중으로 프라이버시를 강화함.

선정된 동형암호는 최근 실용화를 앞두는 있는 등 활발한 연구가 진행되고 있다.

FedSDG, FedAVG 등 연합학습 알고리즘은 동형암호를 추가 사용함으로써 보안성을 한층 강화할 수 있다. 즉, 그림과 같이 엣지 단말에서 학습한 결과값의 동형암호화한 값을 서버로 전달하면, 서버는 암호화한 값에 대한 합을 구한 후 복호화하여 사용할 수 있다.

(그림-4) 연합학습에서 동형암호 적용 예



* 출처 : 저자 작성

『 안전한 다자간 계산 (Secure Multi-Party Computation 』

다자간 계산은 동형암호와 경쟁적인 알고리즘이다. 다자간 계산 알고리즘은 동형암호와 유사하게 각 단말에서 서버로 전달하는 원래의 값을 노출하지 않으면서 전체 합을 알 수 있도록 하는 방법이다. 즉, 다수의 사용자가 각자의 비밀값을 입력값으로 하여 함수값을 함께 계산하는 기술로서 관련 개념은 1982년에 양자간 계산으로 제안되었고 이후 다자간 계산으로 발전했다. 연합학습에 사용되는 가장 대표적인 다자간 계산 알고리즘으로 Secure Aggregation이 있다.[20] 이는 보안성과 프라이버시를 강화하면서 서버에 대한 공격에도 강인한 방법을 포함하고 있다.

18) 천정희 외 (2019.2.28.), 개인정보가 보호되는 동형암호기반 금융데이터분석, 한국금융정보학회.
19) MIT Technology Review (2011), 10 Emerging Technologies of 2011.
20) K. Bonawitz, et al. (2016), Practical Secure Aggregation for Federated Learning on User-Held Data, arXiv:1611.04482.

3 주요 이슈 및 해결 과제

연합학습은 기존 분산 학습과 유사한 개념이지만 이와 다른 기술적 해결 과제가 있다. 연합학습에서 다루고 있는 대표적인 분산 최적화 이슈는 다음과 같다.[21)]

〈 표-2 〉 연합학습 이슈 및 해결 과제

구분	주요 내용
통신 비용	- 로컬 단말과 중앙서버 간의 통신은 연합학습을 위해 구성된 전체 네트워크(연합 네트워크)에서 중요한 병목 현상을 유발 - 실제로 연합 네트워크는 수백만 대의 스마트폰으로 구성되는 경우, 네트워크 통신 속도는 로컬 컴퓨터보다 수십 배 느릴 수 있음 - 글로벌 모델을 업데이트하고 단말과 서버 간 데이터 전달 과정에서 통신 효율적인 방법을 개발해야 함 - 이때, 고려해야 할 두 가지 요소는 단말과 서버간 통신 횟수와 회당 전송되는 데이터 크기를 줄이는 것
시스템 이질성	- 연합학습에 참여한 로컬 단말(장치)는 저장공간, 계산 및 통신 성능, 배터리 수준 등이 매우 다양함 - 각 단말의 시스템과 네트워크의 제약으로 인해서 특정 시간에 참여할 수 있는 단말의 수가 신뢰할 수 없거나 학습 과정에서 사라질 수 있음 - 따라서 참여한 단말의 수의 변화, 이기종 하드웨어 등에 강인한 연합학습 메커니즘이 개발되어야 함
통계적 이질성	- 연합학습은 참여한 단말이 수집한 데이터가 독립적이고 동일한 확률 분포(IID: independent and identically distributed)라고 가정함 - 그러나 스마트폰 사용자의 사용 언어, 데이터 연결점의 개수 등이 다를 수 있어 모델 생성 및 분석 과정에서 복잡성이 매우 높아질 수 있음 - 각 단말에서 수집하는 데이터의 통계적 이질성을 다룰 수 있는 연합학습 방법 연구가 필요함
프라이버시 문제	- 연합학습의 프라이버시 보호를 강화하기 위해서 차등정보보호, 동형암호, 안전한 다자간 계산 등의 알고리즘을 추가 사용하고 있으나, 이것은 학습 모델의 성능 저하나 시스템의 효율성을 낮추는 문제가 발생함 - 이론적으로나 경험에 비추어 프라이버시 강화와 시스템 효율성 간 최적의 균형점을 찾는 방안 모색 필요

* 출처 : Tian Li et al.(2019) 참고하여 재작성

21) Tian Li et al. (2019), Federated Learning: Challenges, Methods, and Future Directions, arXiv:1908.07873v1.

연합학습에 대한 최적화 이슈 외에도 머신러닝 시스템으로써 사이버 공격 문제가 있다.(Qiang Yang et al., 2019) 연합학습 알고리즘의 보안성을 강화하기 위해 도입된 차등정보보호, 동형암호, 안전한 다자간 계산 등의 알고리즘으로는 해결하기 어려운 보안 이슈다.

일반적으로 머신러닝 시스템은 블랙박스(Black-box) 모형이다. 즉, 외부 공격자가 머신러닝 시스템이 학습하는 파라미터를 직접 관찰할 수 없다. 단지 입력값과 출력값만을 관측하여 모델을 추론한다. 하지만, 연합학습은 중앙서버와 클라이언트 간 전송되는 학습 파라미터를 외부 공격자가 관측할 수 있는 화이트박스(White-box) 모형이다. 연합학습에서는 기존 머신러닝 시스템에 대한 공격 취약성에 더해 다음과 같은 사이버 공격에 대한 안전성 문제를 해결해야 한다.

첫째, 학습 모델의 파라미터 업데이트 공격(Model update poisoning)이다. 연합학습에 참여한 클라이언트의 업데이트 정보에 직접 손상을 가하거나 중간자 공격(man-in-the-middle attack)를 수행할 수 있다. 즉, 공격자가 일부 클라이언트를 직접 제어함으로써 학습모델의 파라미터 값을 편향되도록 한다. 파라미터 값만을 공유하는 연합학습에서 외부 공격을 탐지하기 쉽지 않다.

둘째, 학습 데이터 공격(Data poisoning)이다. 학습 단계 전에 데이터 자체를 오염시켜 학습 결과가 달라진다. 이 공격은 일반적인 머신러닝 시스템에 적용되는 경우와 유사하나, 공격 대응이 사실상 불가능하다. 왜냐하면, 연합학습은 전체 학습 메커니즘을 관리하는 중앙서버가 클라이언트 데이터에 직접 접근할 수 없으므로, 오염된 데이터를 제거(Data sanitization)하는 방법을 사용할 수 없다.

셋째, 회피 공격(Evasion attack)이다. 사람의 눈으로는 구별할 수 없는 미세한 노이즈를 학습 데이터(음성, 텍스트 등)에 추가하여 데이터를 교란하는 방법이다. 이 공격은 일반적인 머신러닝 시스템보다 연합학습에 훨씬 쉽게 수행될 수 있다. 연합학습은 화이트박스 모형을 가지기에 외부 공격자가 전체 학습 과정에서 공유되는 학습 파라미터를 관측할 수 있기 때문이다.

한편, 연합학습에서는 기존 머신러닝 과정에서 드러난 공정성(Fairness)과 편향성(Bias) 문제 또한 고려해야 있다. 즉, 연합학습에 사용된 학습 데이터가 특정 클라이언트가 가진 데이터 속성에 너무 편향되어 학습 결과가 공정성을 잃게 되는 경우다.

Ⅲ 산업적 활용 가능성

1 데이터 3법과 의료 데이터

지난 1월 9일 국회 본회의를 통과한 '데이터 3법'은 '개인정보보호법', '정보통신망법', '신용정보법' 등 3가지 법률을 포함한다. 이번 '데이터 3법'에서는 데이터 활용을 제고하기 위해 '가명정보' 개념을 도입하고, 가명정보 '활용'과 '결합'에 관한 방안을 제시한 것이 특징이다. 또한, 데이터 활용에 따른 '개인정보' 판단 기준과 관리 체계를 명확히 하고 책임을 강화했다.

〈 표-3 〉 데이터 3법 주요 내용

구분	주요 내용
개인정보보호법	• 가명정보 도입을 통한 데이터 활용 제고 - 가명정보는 통계작성, 과학적 연구, 공익적 기록 보존 목적으로 정보주체의 동의 없이 처리 허용 - 서로 다른 기업이 보유하고 있는 가명정보를 보안 시설을 갖춘 전문기관에서 결합할 수 있도록 함 • 개인정보 범위 명확화 및 합리적 사용 허용 - 다른 정보와 결합해 특정 개인을 알아볼 수 없는 정보(익명정보)의 법 적용 배제 명확화 - 합리적 범위에서 동의없이 처리할 수 있는 개인정보의 추가적인 이용·제공 허용
정보통신망법	• 개인정보 보호 관련 사항을 '개인정보보호법'으로 이관 - 정보통신망법에 규정된 개인정보 보호에 관한 사항을 '개인정보보호법'으로 이관하고, 규제 및 감독 주체를 '방송통신위원회'에서 '개인정보보호위원회'로 변경
신용정보법	• 금융 데이터 활용의 법적 근거 명확화 - 가명정보는 통계작성, 연구(산업적 목적 포함), 공익적 기록 보존으로 정보주체의 동의 없이 활용 가능 - 가명정보 활용과 결합에 대한 안전장치 및 사후 통제 수단 마련 • 금융분야 마이데이터 산업 도입 - 본인정보 통합조회, 신용·자산관리 등의 서비스를 제공하는 MyData 도입 • 금융 데이터 개인정보보호 강화 - 기계화·자동화된 데이터처리(프로파일링)에 대해 금융회사 등에 설명요구·이의제기 등 프로파일링 대응권 도입 등

* 출처 : 정부자료, 언론보도 등 참고하여 저자 작성

하지만 산업계를 중심으로 '데이터 3법'을 둘러싼 현실적인 문제를 지적하고 있다. 먼저, 개인정보보호법 시행령 개정안의 제14조 2항에 따르면, 정보 주체의 동의 없이 개인정보를 추가 이용·제공할 때 '당초 목적과의 상당한 관련성', '추가 이용 예측 가능성', '제3자 이익 침해 방지', '가명처리 의무' 등 4가지 요건을 모두 갖춰야 한다. 유럽연합의 GDPR보다 엄격할 뿐만 아니라 시행령 내에 포함된 단어의 모호성이 있어 활용에 제한적일 수 있다.

무엇보다, 가명정보의 결합과 관련된 제29조 2항의 규정에 대한 문제가 크다. 가명정보 결합을 전문기관이 수행하고, 결합된 정보를 결합정보기관 내 물리적 공간으로 한정했기 때문이다. 또한, 다양한 정보가 결합될 경우 가명정보의 재식별 가능성이 있음에도 결합의 허용범위가 구체적으로 마련되지 않았다.

한편, 데이터 3법 통과로 가장 기대되는 의료 데이터 현황을 살펴보면, 국내의 경우 〈표-4〉와 같이 관리 주체별로 다양한 의료 데이터가 존재한다. 하지만, 의료 데이터를 활용한 의료 산업의 혁신을 이끌기 위해서는 풀어야 할 과제가 많다. 먼저, 가명화된 의료 개인정보 활용 분야가 R&D 영역 등으로 매우 제한적이다. 또한, 환자의 의료정보에 대한 구체적인 활용 지침이 없다. 무엇보다, 현행 의료법과 국민건강보험법에서 의료 데이터가 별도 관리되고 있어, 데이터 3법에 포함된 개인정보보호법 개정안과 충돌할 경우, 해결방안이 필요하다. 관리 주체별로 관리되는 동일한 의료 데이터나 주체 간 이질적인 데이터를 결합하는 문제 또한 풀어야 할 숙제다.

〈 표-4 〉 관리 주체별 의료 데이터 종류

구분	관리 주체	데이터 종류
건강데이터 (Lifelog Data)	개인	- 웨어러블 기기, 스마트폰, 개인 헬스케어 기기(체온계, 혈압계 등) 등을 통해 생성, 수집되는 개인 라이프로그 데이터
유전데이터 (Gene Data)	유전자 분석기관	- 유전자 분석기관이 생성하는 유전체 데이터로 선천적 유전형(Genotype), 후천적 표현형(Phenotype) 데이터를 총칭 - 1인당 약 30억개의 유전자 염기서열 정보가 있음
전자의무기록 (EMR)	의료기관	- 의료기관에서 생성되고 관리되는 환자의 진료, 검사, 영상 등 전자의무기록 의료데이터
국민건강정보	공공기관	- 건강보험공단, 건강보험심사평가원 등에서 관리하는 진료내역, 건강검진결과, 의료급여, 보험료 등 공공데이터

* 출처 : 한국산업기술평가관리원(2020), 삼정KPMG 경제연구원(2020) 등 참고하여 저자 작성

2 연합학습과 의료혁신

최근 연합학습 활용이 가장 활발히 진행되고 있는 분야는 단연 의료 데이터다. 지금까지 의료기관은 풍부한 개인 의료 데이터를 보유하고 있어도 법적 규제에 묶여 AI 활용은 극히 제한되었다. 의료 현장에서 한 사람의 의료 데이터는 여러 병원에 분산되어 저장되어 있고, 같은 질병의 의료 데이터도 여러 병원에 흩어져 있다. 그러나 프라이버시와 현행 의료법 등으로 인해 병원 간 데이터 공유를 통한 협업은 어려운 실정이다. 연합학습은 여러 병원에 흩어져 있는 특정 질환에 대한 환자 데이터나 임상 데이터를 직접 공유하지 않고도(프라이버시 우려 없이) 모든 데이터를 한곳으로 모아서 분석한 것과 같은 효과를 얻을 수 있다.

이런 이유로 인텔, 엔비디아 등 ICT 기업은 글로벌 의료기관이 협력하여 의료 현장에서 연합학습의 실증실험을 진행하고 있다.

『 인텔 랩 & 펜 메디슨 』

인텔 랩은 펜실베니아 대학교 페럴만 의과대학(주관: 펜 메디슨)과 협력하여, 29개 국제 보건의료 및 연구 기관 연합체가 프라이버시 보장형 AI 학습모델을 만들 수 있는 기술을 개발하고 있다.[22] 목표 기술은 뇌종양을 조기에 식별하기 위해 29개 참여 기관이 각기 보유한 환자의 의료 데이터를 공유하지 않고도 서로 협력하여 AI 모델을 훈련할 수 있는 연합학습에 기반을 두고 있다.[23] AI는 뇌종양을 조기에 발견하는 데 큰 가능성이 있지만 한 기관에서 보유한 데이터로는 한계가 있다. 이를 극복하기 위해서는 다양한 기관들이 보유한 개인 의료 데이터의 보안을 유지하면서 AI 학습모델을 생성할 수 있어야 한다.

인텔 랩은 이미 2018년 의료 영상 기술 학회(MICCAI 2018)에서 연합학습 기반 뇌종양 식별 정확도가 프라이버시를 고려하지 않은 기존 AI 학습 방법의 99% 이상의 정확도에 근접함을 입증한 논문을 발표한 바 있다.[24] 2020년에는 크게 확장된

22) Intel (2020), Intel Works with University of Pennsylvania in Using Privacy-Preserving AI to Identify Brain Tumors.

23) 본 연구를 주도하는 펜 메디슨은 펜실베니아 대학교, 스피리돈 바카스 박사에게 3년 동안 120만 달러 연구비를 지원(국립 보건원(NIH) 산하 국립암연구소의 암 연구를 위한 정보 기술학(ITRC) 프로그램의 일부)

국제 뇌종양 분할 시험(BraTS challenge) 데이터셋을 이용하여 개선된 뇌종양 식별 알고리즘을 개발 중이다.

(그림-5) 인텔의 연합학습 시스템 구조

* 출처 : Intel(2020)

『 엔비디아 & 킹스 칼리지 런던 』

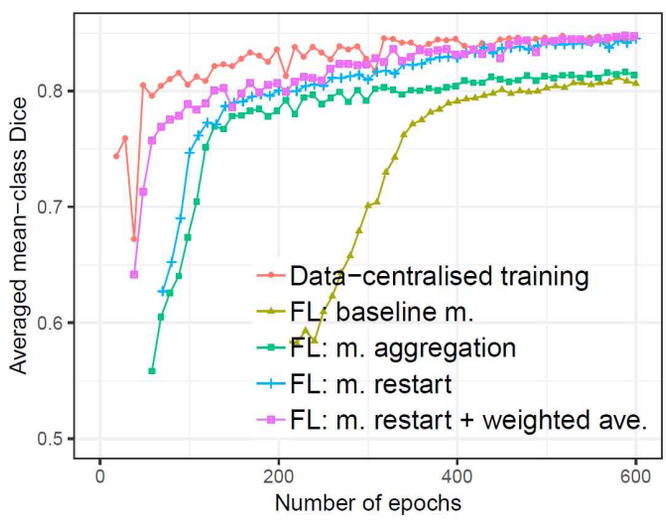
엔비디아는 2019년 10월 의료 영상 기술 학회(MICCAI 2019)에서 킹스 칼리지 런던과 공동으로 뇌종양 식별을 위한 연합학습 신경망 논문을 발표하였다.[25] 본 연구는 285명의 뇌종양 환자 MRI 스캔을 포함한 'BraTS 2018' 데이터셋을 대상으로 수행되었다. 결과적으로 연합학습을 활용한 제안 방법이 기존 방법과 비교하여 환자의 개인정보를 보호하면서도 비슷한 성능에 근접함을 보여주었다.

24) Micah J. Sheller et al. (2019), Multi-institutional Deep Learning Modeling Without Sharing Patient Data: A Feasibility Study on Brain Tumor Segmentation, LNCS, Vol. 11383, (Presenting at MICCAI 2018)
25) W. Li et al. (2019), Privacy-preserving Federated Brain Tumour Segmentation, arXiv: 1910.00962v1.

엔비디아는 2019년 12월 북미방사선의학회(RSNA 2019)에서 AI 의료 시스템 '클라라 FL(연합학습)'을 발표하였다. 구체적으로 EGX 지능형 엣지 컴퓨팅 플랫폼(NVIDIA EGX intelligent edge computing platform)이다. 실제로 엔비디아는 미국 영상의학회(ACR), UCLA 방사선학과, 뉴잉글랜드 파트너스 헬스케어, 캘리포니아 대학교 등에서 '클라라 FL'를 시범 운용 중이다. 또한, 영국의 킹스 칼리지 런던, 오우킨(Owkin)[26] 등과 제휴하여 국가보건서비스를 위해 연합학습 플랫폼을 구축하고 있다.

한편, 2020년 4월 엔비디아는 미 의료계[27]와 협업하여 '클라라 FL'을 활용하여 유방종양 및 조직밀도 평가와 성능을 개선한 연구 결과를 발표했다.[28] 본 연구에서 연구팀은 약 3만 3,000개의 유방 촬영 사진에서 1만 3,000개 이상의 이미지를 사용해 연합학습 기반 AI 모델을 생성하였다.

(그림-6) 뇌종양 식별 성능 비교: 연합학습 vs. 非연합학습



FL(연합학습) vs Data-centralised training(非연합학습)

* 출처 : W. Li et al.(2019)

26) 엔비디아는 연합학습의 안전성을 높이기 위해 차등정보보호와 최신 프라이버시 보호기술을 Owkin 구조에 내장(https://news.developer.nvidia.com/first-privacy-preserving-federated-learning-system/).
27) American College of Radiology, Brazilian imaging center Diagnosticos da America, Partners HealthCare, Ohio State University, and Stanford Medicine.
28) Venturebeat (2020), Health care organizations use Nvidia's Clara federated learning to improve mammogram analysis AI.

3 연합학습의 또 다른 가능성

앞서 살펴본 바와 같이 현재 연합학습이 가장 활발히 활용되고 있는 분야는 의료 산업이다. 연합학습을 사용하면 서로 다른 기관에서 보유하고 있는 의료 데이터를 직접 공유하지 않고도 통합된 AI 모델을 생성할 수 있기 때문이다. 특히 보건·의료 분야는 개인 데이터를 관리하는 주체가 다양하기에 앞으로 연합학습을 이용한 서비스 개발이 더욱 활발해질 것으로 전망된다.

의료 분야 외에도 개인이 정보 관리의 주체가 되는 '마이데이터 사업' 분야에도 연합학습의 활용이 기대된다. 금융과 교육 등에서 연합학습을 이용한 개인 맞춤형 비즈니스 모델이 만들어질 수 있다. 또한, 제조, 물류, 에너지 등 서로 다른 위치에서 생성된 데이터를 통합하여 최적의 해법을 찾는 과정에서도 연합학습이 활용될 수 있다. 특히 서로 다른 기관에서 같은 목표를 가지고 있으나, 개별 실험과 연구가 진행된 결과 데이터를 통합하여, 의미 있는 새로운 결과를 도출하고자 할 때[29] 연합학습의 활용성은 크다. 여기에는 국가 간 데이터 공유를 통한 공동연구도 포함된다. 즉, 연합학습을 통해 확장된 데이터 파트너십과 생태계 구축이 가능하다.

앞으로 스마트폰, 웨어러블기기, 스마트홈 장치(AI 스피커, 지능형 전자제품), 자동차 등 개인화된 제품과 장치는 더욱 많아질 것이다. 이런 환경에서 개인의 정보를 '보호'하면서 '활용'이 가능한 개인 맞춤형 서비스 발굴에 대한 시장의 요구는 증가할 수밖에 없다. 연합학습은 현실적으로 데이터 공유에 제약이 있는 분산된 환경에서 기업의 경쟁력을 차별화할 수 있는 강력한 도구가 될 수 있다. 딥러닝 이후 주목받고 있는 생성적 적대 신경망(GAN), 전이학습, 심층강화학습 등에 이어 연합학습의 산업적 활용이 크게 기대되는 이유다.

연합학습 방법은 향후 디지털 기술의 발전과 함께 급증하는 데이터의 소유권과 활용의 문제를 해결하는 대안으로 더욱 주목받을 것으로 보인다. 특히, 이종 산업 간 데이터를 공유하는 과정에서 드러난 데이터의 이질성 등 효율성 문제와 신뢰성을 높이기 위해 전이학습, 암호화 알고리즘, 블록체인 등의 접목이 필요하다. 이러한 노력은 결과적으로 연합학습이 단순히 프라이버시 '활용'과 '보호'를 문제 해결을 넘어 완전히 새로운 수준의 비즈니스 모델을 만들 수 있을 것이다.

29) 신종 감염병 확산 방지를 위한 병원, 금융기업, 공공기관 등이 보유한 데이터 통합 분석 등이 대표적.

참고문헌

◆ 국내자료

삼정KPMG 경제연구원(2020.3.), 데이터 3법 통과: 의료 데이터, 개방을 넘어 활용으로.

연합뉴스 (2019.8.22.), 당신이 잠들면 구글 AI는 학습을 시작한다, 연합뉴스, 2019.8.22.

이정혜 (2020), 연합학습이란? 프라이버시와 인공지능 양립 가능 솔루션 연합학습에 대하여, https://www.youtube.com/watch?v=UEidxYeNPng

전주형 외 (2019.6.), 연합학습(Federated Learning) 기술동향, OSIA S&TR Journal Vol. 32, No. 2.

천정희 외 (2019.2.28.), 개인정보가 보호되는 동형암호기반 금융데이터분석, 한국금융정보학회.

한국산업기술평가원 (2020), 디지털치료제 기술동향과 산업전망.

◆ 국외자료

Google (2017), Federated Learning: Collaborative Machine Learning without Centralized Training Data, Google AI Blog,

https://ai.googleblog.com/2017/04/federated-learning-collaborative.html

H. B. McMahan et al. (2016), Federated Learning of Deep Networks using Model Averaging, arXiv:1602.05629v1.

H. B. McMahan et al. (2016), Communication-efficient learning of deep networks from decentralized data, arXiv:1602.05629.

Intel (2020), Intel Works with University of Pennsylvania in Using Privacy-Preserving AI to Identify Brain Tumors.

J. Konečný et al. (2016), Federated learning: Strategies for improving communication efficiency, arXiv:1610.05492.

Karen Hao (2019), A little-known AI method can train on your health data without threatening your privacy, MIT Technology Review.

K. Bonawitz, et al. (2016), Practical Secure Aggregation for Federated Learning on User-Held Data, arXiv:1611.04482.

K. Bonawitz, et al. (2019), Towards Federated Learning at Scale: System Design, arXiv: 1902.01046.

Ligeng Zhu et al. (2019), Deep leakage from gradients, NeurIPS 2019, p.14747-14756.

Micah J. Sheller et al. (2019), Multi-institutional Deep Learning Modeling Without Sharing Patient Data: A Feasibility Study on Brain Tumor Segmentation, LNCS, Vol. 11383, (Presenting at MICCAI 2018)

MIT Technology Review (2011), 10 Emerging Technologies of 2011.

MIT Technology Review (2020), 10 Breakthrough Technologies 2020.

Peter Kairouz et al. (2019), Advances and Open Problems in Federated Learning, arXiv:1912.04977v1.

Park, M-J., & Kim, H. J. (2016), Statistical disclosure control for public micro data: present and future, The Korean Journal of Applied Statistics, 29(6), 1041-1059.

Qiang Yang et al. (2019), Federated Learning: Concept and Applications, arXiv: 1902.04885v1.

Tian Li et al. (2019), Federated Learning: Challenges, Methods, and Future Directions, arXiv:1908.07873v1.

Venturebeat (2020), Health care organizations use Nvidia's Clara federated learning to improve mammogram analysis AI.

W. Li et al. (2019), Privacy-preserving Federated Brain Tumour Segmentation, arXiv: 1910.00962v1.

Xiang Li et al. (2020), On the convergence of fedavg on non-iid data, ICLR 2020.

저자소개

이승민 ETRI 지능화융합연구소 기술정책연구본부 경제사회연구실 책임연구원
e-mail: todtom@etri.re.kr Tel. 042-860-1775

연합학습 기술 동향 및 산업적 시사점

발행인 이 지 형
발행처 한국전자통신연구원 지능화융합연구소 기술정책연구본부
발행일 2020년 11월 30일

www.etri.re.kr

Electronics and Telecommunications Research Institute
34129 대전광역시 유성구 가정로 218
TEL. (042) 860-6114 FAX. (042) 860-6504

비매품/무료
93560
9 788955 192827
ISBN 978-89-5519-282-7