

2. 개인 정보 보호 기술

2.1. 연합학습 (Federated Learning): 데이터는 각자 보관, 인공지능은 함께 성장

① 왜 나오게 되었는가?

연합학습은 개인정보 보호와 AI 발전이라는 두 마리 토끼를 잡기 위해 등장했다. AI를 발전시키려면 많은 데이터가 필요하지만, 이를 한 곳에 모으면 개인정보 유출 위험이 커진다. 이는 마치 여러 사람의 비밀 일기를 한 곳에 모아두는 것과 같아서 위험하다. 특히 병원 기록이나 은행 거래 내역 같은 민감한 정보는 더욱 조심스럽게 다뤄야 한다. 또한, 엄청난 양의 데이터를 한 곳으로 옮기는 것은 시간과 비용이 많이 든다. 이런 문제들을 해결하면서도 AI를 효과적으로 발전시킬 방법이 필요했고, 그 해답으로 연합학습이 탄생했다.

② 쉽게 설명하면?

연합학습은 ‘함께 공부하되, 각자의 노트는 공개하지 않는’ 방식이라고 할 수 있다. 여러 기기나 서버가 각자 가진 데이터로 AI를 학습시키고, 그 결과만을 중앙에 보내 종합한다. 이는 마치 여러 학생이 각자 공부한 내용을 발표하고, 선생님이 이를 정리해 더 좋은 수업 자료를 만드는 것과 비슷하다. 이 과정에서 학생들의 개인적인 공부 노트는 공개되지 않는다. 마찬가지로 연합학습에서는 개인의 원본 데이터가 자신의 기기나 서버에 남아있어 개인정보가 안전하게 보호된다.

③ 예시와 함께 좀 더 자세히 알아볼까?

연합학습의 실제 활용 예를 들어보자. 여러분이 스마트폰에서 사용하는 키보드 앱을 생각해보자. 이 앱은 여러분의 단어 사용 패턴을 학습해 더 정확한 자동완성 기능을 제공한다. 연합학습을 사용하면, 이 과정이 다음과 같이 진행된다:

- 여러분의 스마트폰에서 키보드 앱이 여러분의 입력 패턴을 학습한다.
- 이 학습 결과(예: “사용자는 ‘안녕’이라는 단어 다음에 ‘하세요’를 자주 입력한다”)만 중앙 서버로 전송된다.
- 중앙 서버는 수많은 사용자로부터 받은 이런 정보들을 종합해 더 똑똑한 키보드 모델을 만든다.
- 이 개선된 모델이 다시 모든 사용자의 스마트폰으로 전송되어 적용된다.

이 과정에서 여러분이 실제로 입력한 메시지 내용은 절대 외부로 전송되지 않는다. 단지 입력 패턴에 대한 정보만 공유되어 개인정보가 안전하게 보호된다.

④ 왜 중요한가?

연합학습의 중요성은 ‘개인정보 보호’와 ‘AI 발전’이라는 두 가지 목표를 동시에 달성할 수 있다는 점에 있다. 이는 마치 케이크를 먹으면서도 다이어트에 성공하는 것과 같은 이상적인 상황이다. 개인정보 유출 걱정 없이 대규모 데이터를 활용해 AI를 발전시킬 수 있어, 더 많은 분야에서 AI 기술을 안전하게 적용할 수 있다.

특히, 의료나 금융 같은 민감한 정보를 다루는 분야에서 연합학습은 혁신적인 해결책이 될 수 있다. 예를 들어, 여러 병원이 환자 정보를 직접 공유하지 않고도 함께 더 정확한 질병 예측 모델을 만들 수 있게 된다. 이는 개인의 프라이버시를 지키면서도 의료 기술의 발전을 가속화할 수 있는 중요한 방법이다.

⑤ 어디에 활용되는가?

연합학습은 우리 일상 곳곳에서 활용되고 있다. 앞서 언급한 스마트폰 키보드 앱 외에도 다양한 분야에서 사용된다. 예를 들어:

- 음성 인식: 스마트 스피커가 여러분의 말을 더 잘 알아들을 수 있게 만드는데 사용된다. 개인의 음성 데이터는 기기에 남아있고, 학습 결과만 공유되어 모든 기기의 성능이 향상된다.
- 의료 분야: 여러 병원이 협력하여 희귀 질병의 진단 모델을 개발할 때 활용된다. 각 병원의 환자 정보는 외부로 나가지 않으면서도, 함께 더 정확한 진단 모델을 만들 수 있다.
- 금융 사기 탐지: 은행들이 고객의 거래 내역을 직접 공유하지 않고도 함께 더 효과적인 사기 탐지 시스템을 개발할 수 있게 한다.
- 자율주행차: 여러 자동차 회사가 각자의 주행 데이터를 공유하지 않으면서도 함께 더 안전한 자율주행 시스템을 개발할 수 있다.

2.2. TEE (Trusted Execution Environment): 데이터의 안전 자킴이, 기기 속 작은 금고

① 왜 나오게 되었는가?

TEE, 즉 신뢰 실행 환경(Trusted Execution Environment)은 우리의 개인정보를 더욱 안전하게 보호하기 위해 탄생했다. 스마트폰, 스마트워치, 스마트 TV 등 우리 주변의 모든 기기들이 점점 더 많은 개인정보를 다루게 되면서, 이를 안전하게 보호할 필요성이 커졌다. 기존의 방식은 마치 집 안의 모든 물건을 그냥 놓아두는 것과 같아서, 누군가 집에 들어오면 모든 것이 노출될 위험이 있었다. TEE는 이런 문제를 해결하기 위해, 기기 안에 아무나 열 수 없는 특별한 금고를 만드는 것과 같은 기술이다.

② 쉽게 설명하면?

TEE는 우리가 사용하는 기기 안에 만들어진 특별한 안전 영역이다. 이는 마치 집 안에 있는 금고와 같다. 일반적인 데이터는 집 안 여기저기에 놓여있지만, 정말 중요한 것들은 이 금고 안에 넣어둔다. 이 금고는 특별한 잠금장치가 있어서 허가받지 않은 사람은 절대 열 수 없다. TEE도 이와 같이 작동한다. 기기 안에서 암호키, 지문 정보, 신용카드 정보 같은 민감한 데이터를 이 특별한 영역에 보관하고 처리하여, 해커들이 접근할 수 없게 만든다.

③ 예시와 함께 좀 더 자세히 알아볼까?

TEE의 실제 활용 예를 들어보자. 여러분이 스마트폰으로 모바일 뱅킹을 사용할 때를 상상해보자. 앱을 실행하고 지문으로 로그인한 후, 송금을 하려고 한다. 이 과정에서 TEE는 다음과 같이 작동한다:

- 지문 인식: 여러분의 지문 정보는 TEE 안에 안전하게 보관되어 있다. 지문을 스캔하면, 이 정보는 TEE 안에서만 처리되어 외부로 유출될 위험이 없다.
- 계좌 정보 확인: 여러분의 계좌 번호, 비밀번호 등은 TEE 안에서 암호화되어 저장된다. 앱이 이 정보를 확인할 때도 TEE 안에서만 처리된다.
- 송금 처리: 송금 과정에서 사용되는 암호화 키도 TEE 안에 보관되어 있다. 송금 정보는 이 키를 사용해 TEE 안에서 암호화된 후 은행 서버로 전송된다.

이 모든 과정에서 중요한 정보들은 TEE라는 안전한 금고 안에서만 처리되므로, 해커가 스마트폰을 해킹하더라도 이 정보들에는 접근할 수 없다.

④ 왜 중요한가?

TEE의 중요성은 우리의 디지털 생활을 더욱 안전하게 만든다는 점에 있다. 이는 마치 집 안에 견고한 금고를 설치하는 것과 같아서, 중요한 물건을 안심하고 보관할 수 있게 해준다. 특히 요즘처럼 스마트폰으로 모든 것을 하는 시대에, TEE는 우리의 개인정보와 재산을 지키는 파수꾼 역할을 한다.

또한, TEE는 AI 기술과 결합하여 더욱 강력해질 수 있다. 예를 들어, 스마트폰에서 작동하는 AI 비서가 우리의 개인정보를 이용할 때, 이 정보들을 TEE 안에서 안전하게 처리할 수 있다. 이로써 AI의 편리함은 그대로 누리면서도 privacy는 완벽하게 보호받을 수 있는 것이다.

⑤ 어디에 활용되는가?

TEE는 우리 일상 곳곳에서 활용되고 있다. 가장 흔한 예로는 스마트폰의 지문인식이나 안면인식 기능을 들 수 있다. 여러분이 지문으로 스마트폰 잠금을 해제할 때마다 TEE가 작동하고 있는 것이다.

또한, 신용카드 정보를 이용한 모바일 결제 시스템에서도 TEE가 중요한 역할을 한다. 애플페이 같은 서비스들이 안전하게 작동할 수 있는 것은 TEE 덕분이다.

최근에는 자동차 산업에서도 TEE의 활용도가 높아지고 있다. 자율주행차의 경우, 차량의 제어 시스템이나 사용자의 위치 정보 등 중요한 데이터를 TEE에 저장하고 처리하여 해킹을 방지한다.

심지어 스마트 TV에서 넷플릭스나 왓챠 같은 스트리밍 서비스를 이용할 때도 TEE가 사용된다. 영화나 드라마의 불법 복제를 막기 위해 콘텐츠를 암호화하는 데 TEE가 활용되는 것이다.