멘토링 결과 보고서

과 제 명	프라이버시 보호 딥러닝 서비스 개발
참여인원	4 명 201402433 조승현 201402392 이상화 201704144 김수민 201704145 김주희
수행기간	2020년 3월 ~ 2020년 6월

추진배경

데이터의 전성기 시대가 도래하면서 빅데이터의 축적 및 활용으로 개인에 관한 각종 정보(의료정보, 위치정보, 신용정보 등)와 관련된 산업이 급성장하고 있다. 기업이나 기관에서 이를 분석하고 활용하는 과정 속에 개인의 프라이버시가 침해되는지에 관한 논란이 발생하게 되었고 이를 해결하기 위한 방법이 요구되어진다.

본 과제를 수행하면서 이러한 민감한 정보를 보호할 수 있는 기술 연구를 통해 기업이나 기관은 업무 생산성을 향상시키고 정보의 주체자들은 정보 유출의 염려를 덜어 안심할 수 있도록 즉, 모두가 win-win 할 수 있는 서비스를 개발하고자 한다.

목표 및 내용

- 인공지능의 자체적인 학습(딥러닝)을 통한 서비스를 개발한다.
- 프라이버시 침해 우려가 있는 민감한 데이터 정보를 감추면서도 데이터 기반의 다양한 활용을 가능케 해주는 개인정보 비식별화 기술인 '차등 정보보호(Differential Privacy)'를 연구한다.
- 사용자의 기기에서 데이터를 학습하여 모델을 추출하는 연합학습(Federated Learning)을 통해 개인의 민감한 데이터에 대한 우려를 줄일 수 있다.

위의 내용을 바탕으로 차등 정보보호(Differential Privacy) 기술로 사용자의 개인정보를 보호하고 기기 내에서 AI 학습이 수행되는 연합학습(Federated Learning) 방식을 적용한 맞춤형 금융상품 소개 서비스를 개발한다.

더하여 사용자 맞춤형 상품 추천 기능을 위해서는 사용자의 분류를 판별할 수 있어야 하는데 이를 위해 클러스터링 기법을 이용한다. 사용자들의 데이터에 대해 클러스터링 기법을 적용하

여 유사도를 기준으로 동질 유형을 분류하게 되며 이를 통해 고객의 특성과 상품 유형을 고려하여 세분화한 것을 기준삼아 상품을 추천 해주는 서비스를 구현할 수 있다.

결과적으로 사용자들에게 보다 안전한 서비스를 제공할 수 있을 뿐만 아니라 차별화된 개인 맞춤형 서비스로 편의성과 만족도까지 향상시킬 수 있다.

수행결과

1-1) 프라이버시 보호가 되는 딥러닝 vs 프라이버시 보호가 되지 않는 딥러닝

프라이버시 보호를 잘 고려하지 않은 딥러닝은 분석 결과를 통해 민감한 정보를 복원할 수 있었다. 그리고 기존의 프라이버시 보호(k-익명성, l-다양성 등)는 다양한 자료의 연결을 통해 특정 개인의 정보를 추론할 수 있는 가능성이 여전히 존재한다. 하지만 차등 프라이버시 모델은 k-익명성, l-다양성의 취약한 부분을 보완하기 위해 제안된 모델로, 단순한 숫자의 변화가 아니라 레코드들 자체의 확률적 변형을 통해 프라이버시에 대한 식별 가능성을 제한하는 향상된 프라이버시 보호 모델이다.

1-2) 차등 프라이버시 보호 알고리즘 개선점 혹은 사그램만의 아이디어

금융이나 의료 같은 분야에 차등 프라이버시 보호 알고리즘 외의 다른 프라이버시 보호 알고리즘은 간간히 쓰이지만 차등 프라이버시 보호는 현재 잘 쓰이지 않기 때문에 이에 대한 개선점이나 아이디어는 아직 명시하기 힘들다.

1-3) db언급을 했는데 db에서 이미 사용자 개인정보가 들어가기 때문에 프라이버시 침해요소가 발생할 수 있다?

연합 학습, 차등 프라이버시를 이용하여 데이터베이스의 프라이버시 침해를 방지할 수 있다. 연합 학습은 데이터를 중앙에 모아서 학습하는 것이 아니라 사용자 기기에서 학습한 모델을 중앙으로 취합하는 학습 모델이다. 데이터를 중앙으로 수집하는 것이 아니기 때문에 사생활 침해 소지가 적다. 그리고 차등 프라이버시 보호는 데이터베이스에 쿼리를 요청할 때 그에 대한 응답에 적절한 분포의 noise를 섞어 프라이버시 보호를 할 수 있다.