프라이버시 보호 딥러닝 서비스 개발

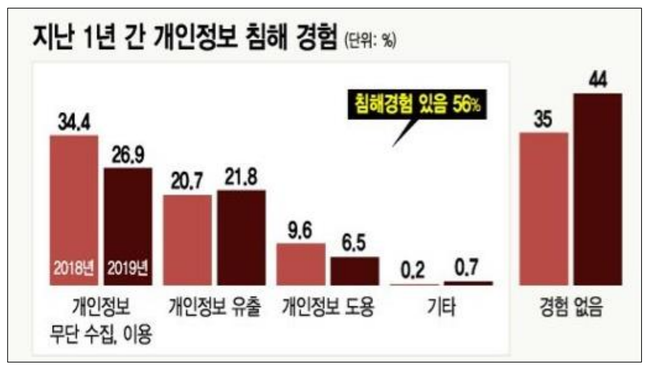
컴퓨터공학과 [사그램]

14 조 승 현, 14 이 상 화, 17 김 수 민, 17 김 주 희

지도교수 : 임 성 수 멘토 : ㈜노타 채 명 수 대표

배경

- 빅데이터의 축적 및 활용
- 개인정보 관련 산업 급성장
- 개인의 프라이버시 침해 논란 발생
- 해결방법 요구



*자료 : 개인정보보호위원회 / 그래픽: 유정수 디자인기자

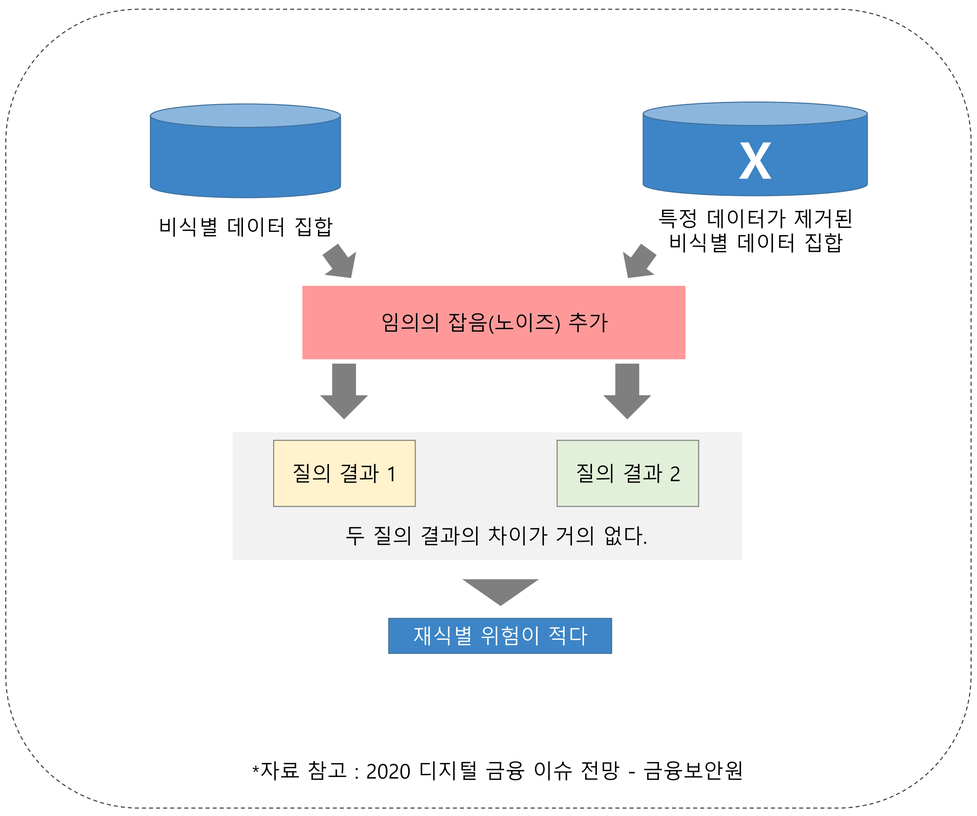
목표

✓ 데이터 보호 알고리즘 도입을 통한 개인정보 침해 방지

✓ 높은 성능의 AI기반 추천시스템 개발

주요개념

- 차등 프라이버시 보호 (Differential Privacy)



*자료 참고 : 2020 디지털 금융 이슈 전망 - 금융보안원

- 기존 개인정보 비식별화 기술과의 차이점

구분	개별화 가능성	연결 가능성	추론 가능성
K-익명성	No	Yes	Yes
L-다양성	No	Yes	May not
차등 프라이버시 보호	May not	May not	May not
해싱/토큰화	Yes	Yes	May not

* 자료: ARTICLE 29 DATA PROTECTION WORKING PARTY, “Opinion on Anonymisation Techniques”, 2014.4.10

설계

- 사용 도구

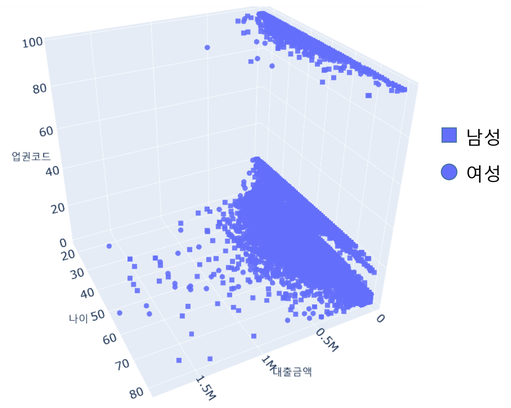
프로그래밍 언어로 Python을 사용했으며 개발 환경으로 Jupyter Notebook을 활용했다.
차등 프라이버시 알고리즘이 적용된 K-means Clustering은 IBM의 Diffprivlib 라이브러리를 사용했다.

- 사용 데이터

한국신용정보원 빅데이터 센터를 통해 신용거래 차주들의 신용정보를 데이터셋으로 활용했다.
그 중 의미 있는 속성인 나이, 성별, 업권코드, 대출금액 값으로 clustering을 수행했다.

생년	성별	업권코드	대출금액	대출상품
1974	2(여성)	5	100	0
1980	1(남성)	1	25000	100
1989	2(여성)	1	87000	220
1949	1(남성)	5	5100	0
1977	1(남성)	5	1500	0
1975	1(남성)	5	26000	240
1952	1(남성)	3	12000	100
⋮				

< 차주 신용정보 데이터 57677 건 >



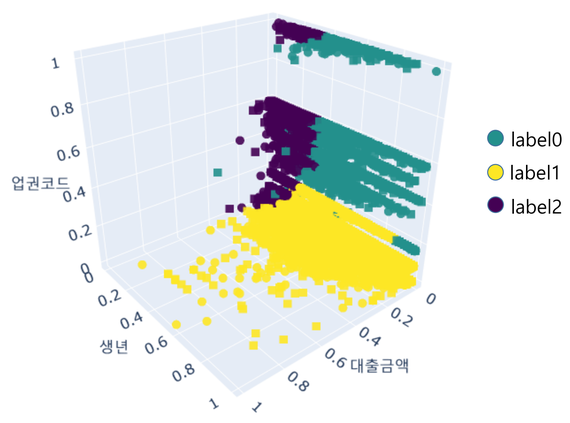
< 4차원 데이터 분포 그래프 >

- 수행 과정

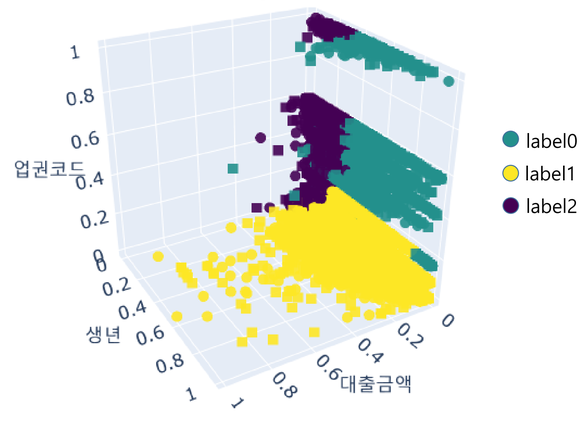
Process
차등 프라이버시 보호가 적용된 K-means Clustering를 수행한다.
추천 받고자 하는 차주의 cluster를 예측한다.
예측된 cluster에서 가장 많이 사용되는 상품을 추천해주는 recommend 함수를 수행한다.
차등 프라이버시 보호가 적용된 K-means Clustering 알고리즘을 수행한 추천 상품 결과와 차등 프라이버시 보호가 적용되지 않은 K-means Clustering 알고리즘을 수행한 추천 상품 결과를 비교/확인한다.

결과

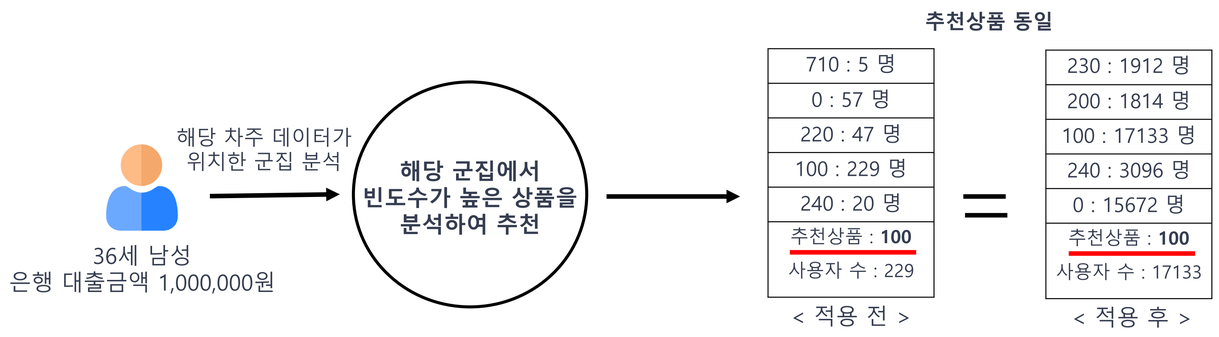
차등 프라이버시 보호 적용 전/후 K-means Clustering 결과



< 적용 전 K-means clustering 결과 >



< 적용 후 K-means clustering 결과 >



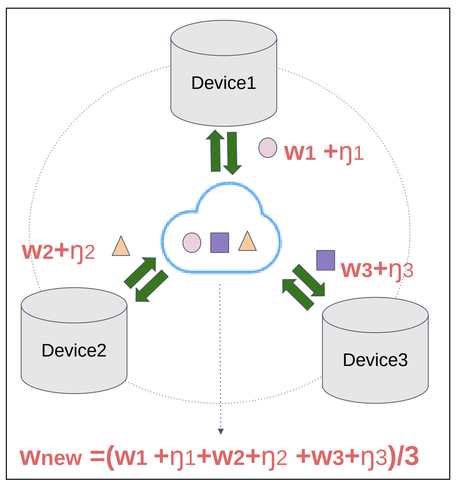
✓ 차등 프라이버시 보호에 의한 비식별화 데이터는 민감한 정보를 보호하여 안전성을 높이면서도 적용 전/후의 결과값에는 영향을 주지 않아 데이터의 유용성은 훼손시키지 않음

✓ 비슷한 속성을 가진 고객들의 데이터를 기반으로 사용자에게 맞춤형 상품을 보다 안전하고 정확하게 제공할 수 있음

향후계획

차등 프라이버시를 적용한 연합학습 도입(9~11월)

- 목적 : 데이터 역추적을 방지하여 프라이버시 보호 강화
- 기존 시스템 : 서버에 가중치 전송, 서버에서 학습 후 장치로 재 배포
- 목표 시스템 : 서버로 전송되는 가중치에 차등 프라이버시 적용
- 장점 : ① 데이터를 서버로 전송하지 않아 보안 우수
  ② 중간 통계 값에 의한 프라이버시 누출 방지



개발일정

	3월	4월	5월	6월	7월	8월	9월	10월	11월
1) 프라이버시 보호 기법 학습	■	■	■	■					
2) 클러스터링 기반 추천 알고리즘 구현			■	■	■	■			
3) 연합학습 시스템 구현							■	■	
4) 차등 프라이버시 적용 연합학습 구현								■	■

* 자료: UNIST 이정혜 교수 , 프라이버시와 인공지능 양립 가능 솔루션 연합학습에 대하여, 2020.05.27