

컴퓨터공학과 사그램조

프라이버시 보호 딥러닝 서비스 개발

14 조승현

14 이상화

17 김수민

17 김주희



주제

프라이버시 보호 딥러닝 서비스 개발

사용자의 신용정보를 분석하여 적절한 대출 상품을 추천

목차

1

배경

동기
추진 배경
해결 방법

2

설계 및 결과

개발 일정
구현 방법
구현 결과

3

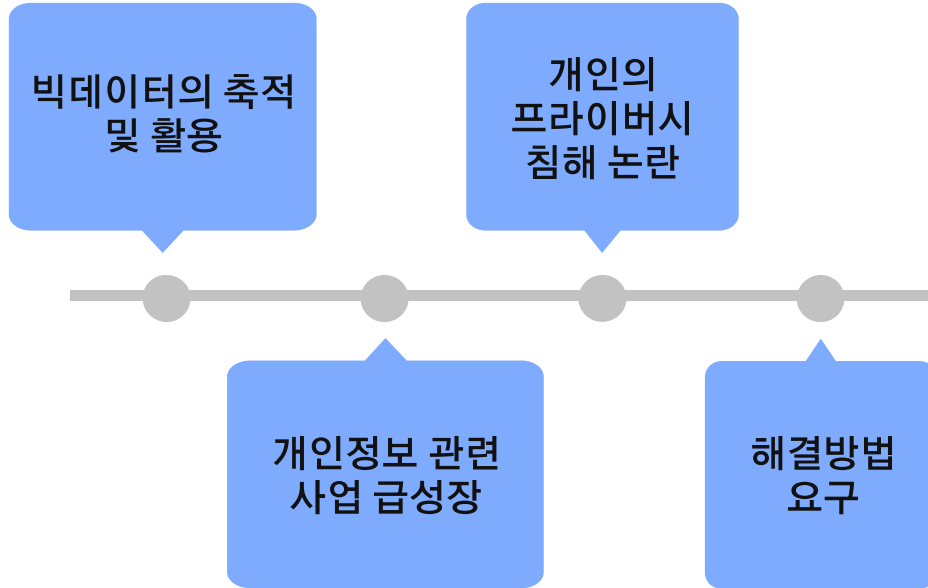
향후 계획

개발 방향

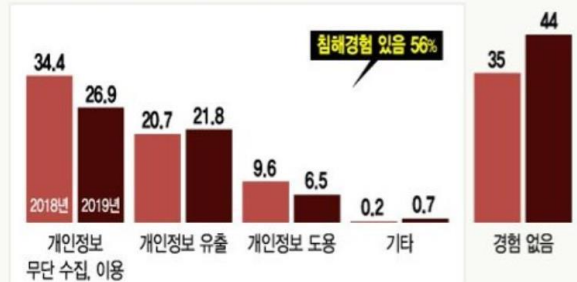
1. 배경

- 동기
- 추진 배경
- 해결 방법

동기



지난 1년 간 개인정보 침해 경험 (단위: %)



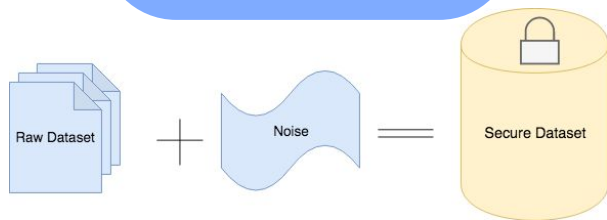
추진 배경



해결 방법

프라이버시 보호 딥러닝

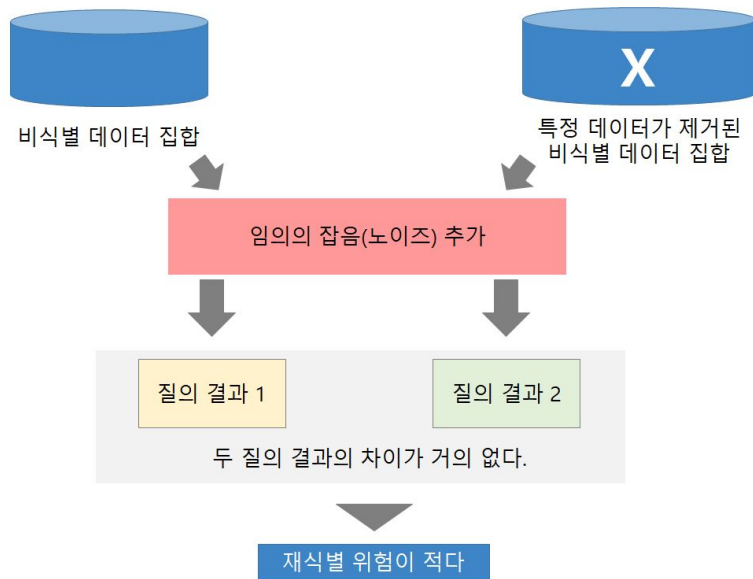
차등 프라이버시



연합학습



해결방법 1 - 차등 프라이버시 보호



*자료 : 2020 디지털 금융 이슈 전망 - 금융보안원

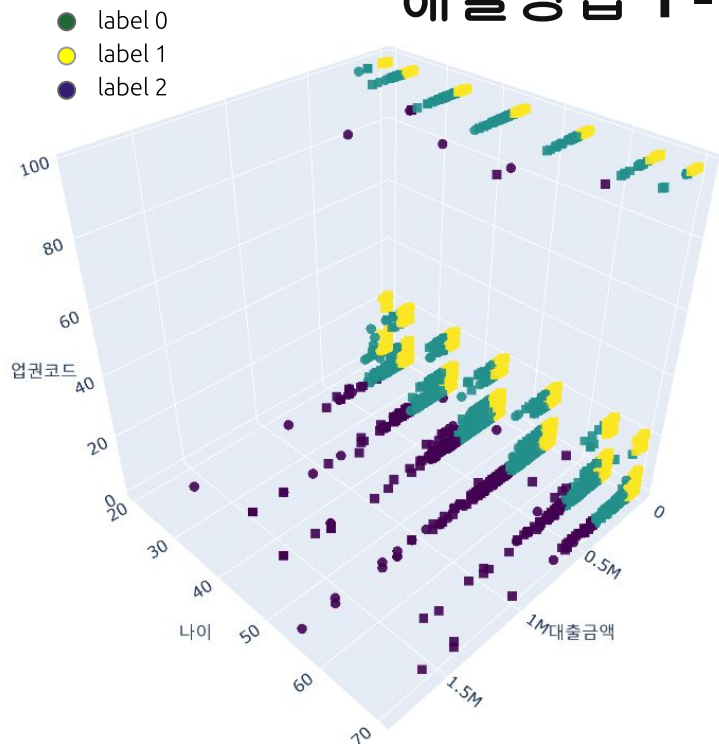
해결방법 1 - 차등 프라이버시 보호

기존 방법들과 재식별 가능성 여부 비교

구분	개별화 가능성	연결 가능성	추론 가능성
K - 익명성	X	O	O
I - 다양성	X	O	△
차등 프라이버시 보호	△	△	△
해싱/토큰화	O	O	△

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

해결방법 1 - 차등 프라이버시 보호



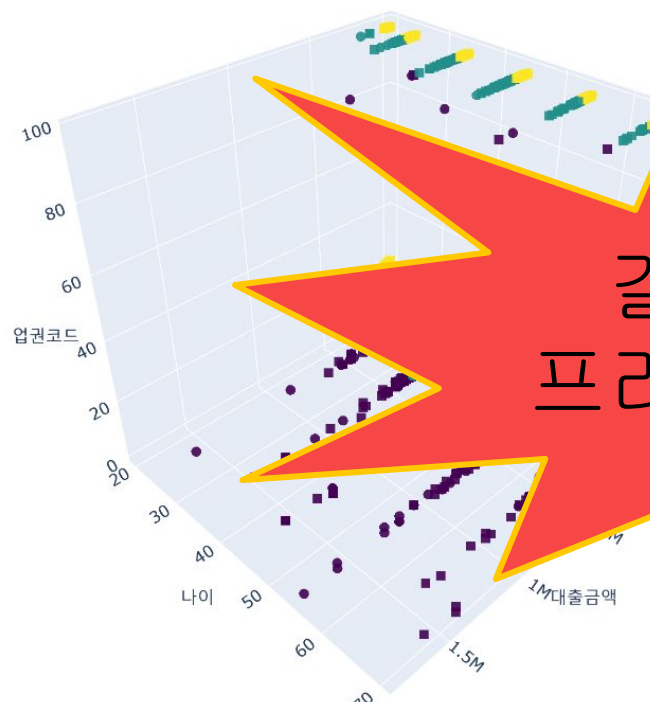
<k-익명성 적용을 위하여 age 값을 범주화한 그래프>

기존 방법 : 비식별화 (k-익명성)

- 준식별자의 값을 범주화하는 k-익명성 기법을 통하여 데이터가 비식별화 되는 것처럼 보일 수 있음.
ex) age : 25 \Rightarrow age : 21-30
- 그러나 정보들이 유출될 시 특정 사람을 유추할 수 있는 '연결 가능성' 등 문제점이 여전히 존재.

구분	개별화 가능성	연결 가능성	추론 가능성
K - 익명성	X	○	○
차등 프라이버시 보호	△	△	△

해결방법 1 - 차등 프라이버시 보호



결론은 차등
프라이버시 보호

방법 : 비식별화 (k-익명성)

화하는 k-익명성 기법을 통하여
보일 수 있음.

유추할 수
문제점이 여전히 존재.

	개별화 가능성	연결 가능성	추론 가능성
K-익명	X	○	○
차등 프라이버시 보호	△	△	△

<k-익명성 적용을 위하여 age 값을 범주화한 그래프>

해결방법 2 - 연합 학습

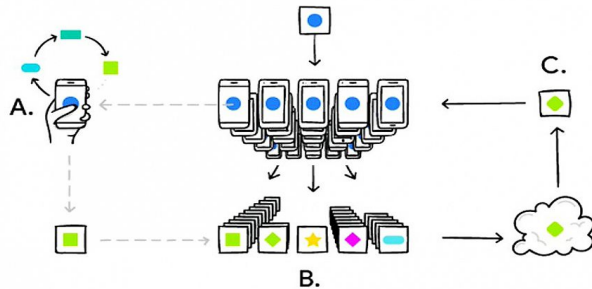
기존 방식의 한계

- 중앙 데이터베이스에 저장 문제
- 분산 데이터를 한 곳에 모으는 비용이 큼
- 데이터 관련 프라이버시 이슈

해결 방안



연합학습

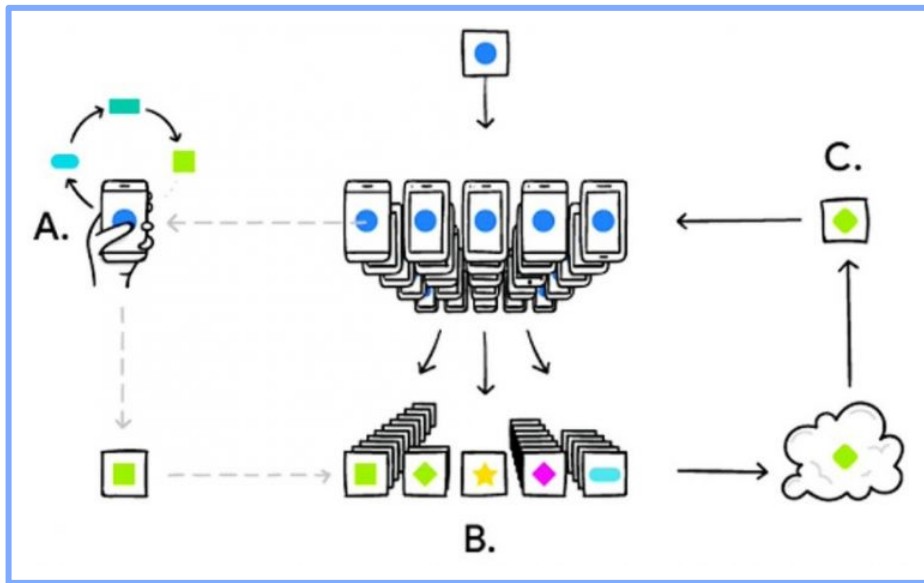


구글에서 제안된 방식, 프라이버시 보호 방안으로 급부상

학습 피라미터만을 서버에 공유하여 모델을 학습시키므로
원본 데이터를 유추할 수 없음

⇒ 프라이버시 이슈에 대한 대안이 될 수 있다.

해결방법 2 - 연합 학습



*자료 : Google AI

A. 단말이 학습을 통해 알고리즘 성능 강화

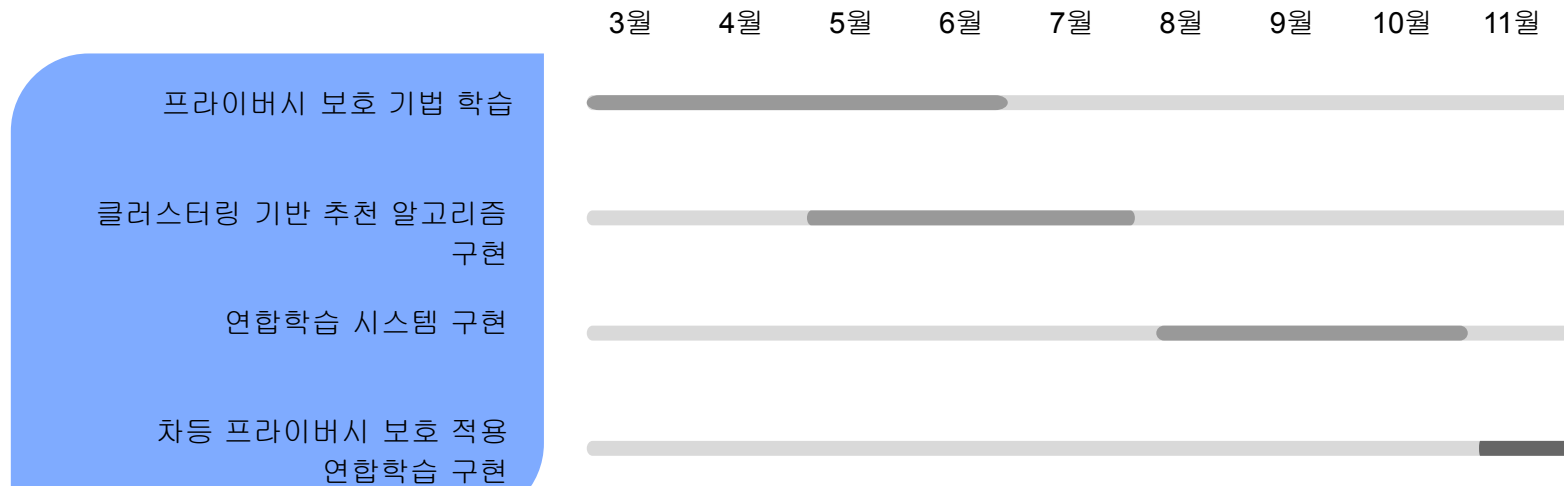
B. 학습한 알고리즘을 클라우드 데이터 센터로 전송

C. 공통 성능 개선 요소를 생성해 각 단말에 전송

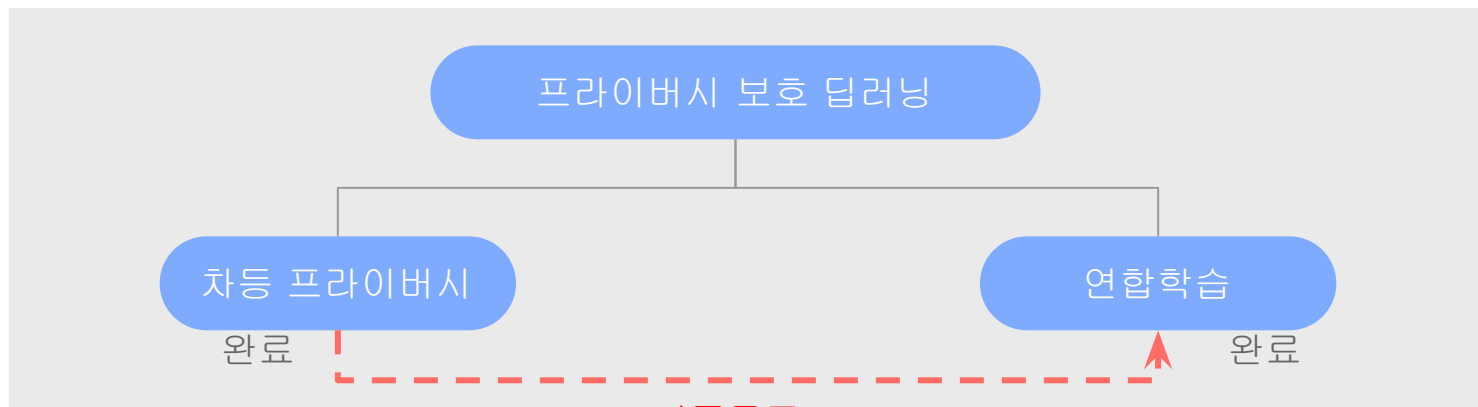
2. 설계 및 결과

- 개발 일정
- 구현 방법
- 구현 결과

개발 일정



해결방법



연합학습에 차등프라이버시를 적용하여 프라이버시를 보호

구현 방법



개발 언어

Python



개발 환경

Jupyter Notebook
Linux



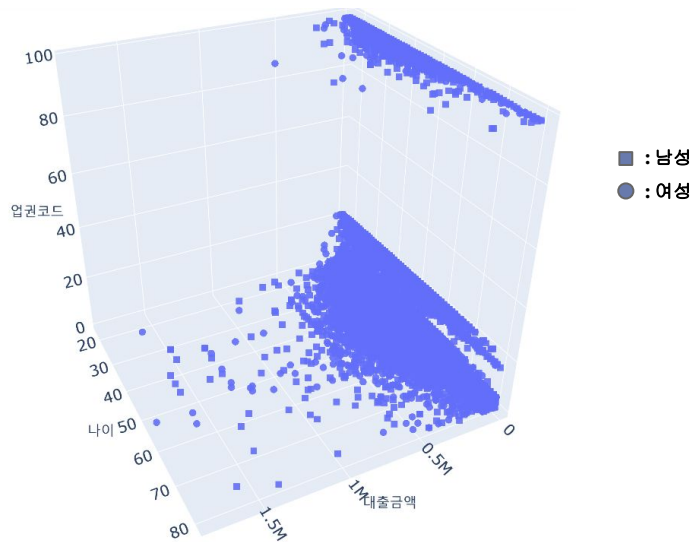
라이브러리

IBM - Diffprivlib
Tensorflow - Tensorflow_federated
Sherpa.ai - shfl

데이터

생년	성별	업권코드	대출금액	대출상품코드
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
⋮				

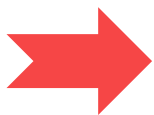
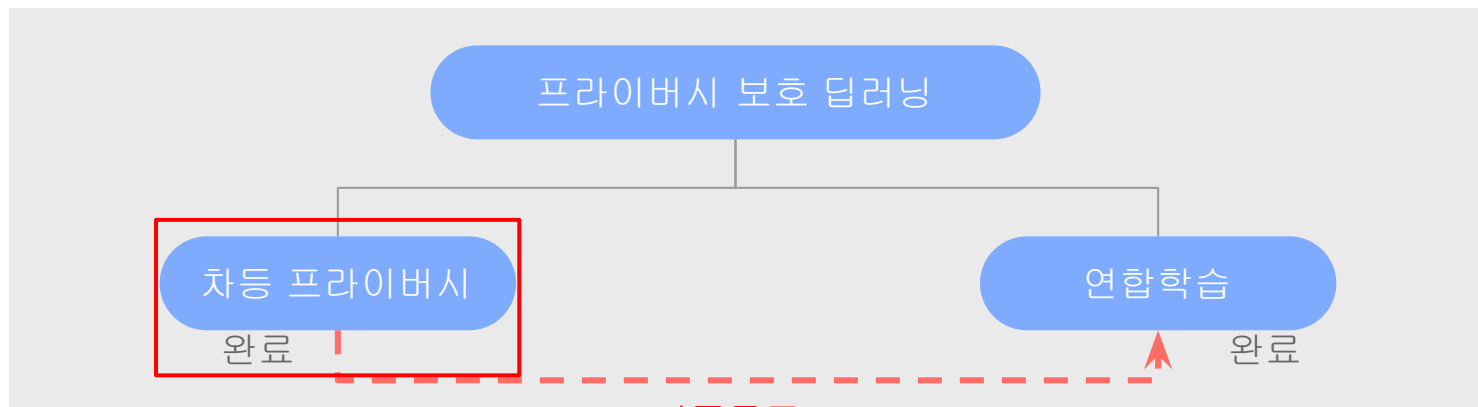
< 차주 신용 데이터 57677건 >



< 4차원 데이터 분포 그래프 >

정제 및 정규화를 수행한 데이터 분포 그래프

해결방법



연합학습에 차등프라이버시를 적용하여 프라이버시를 보호

K-means clustering

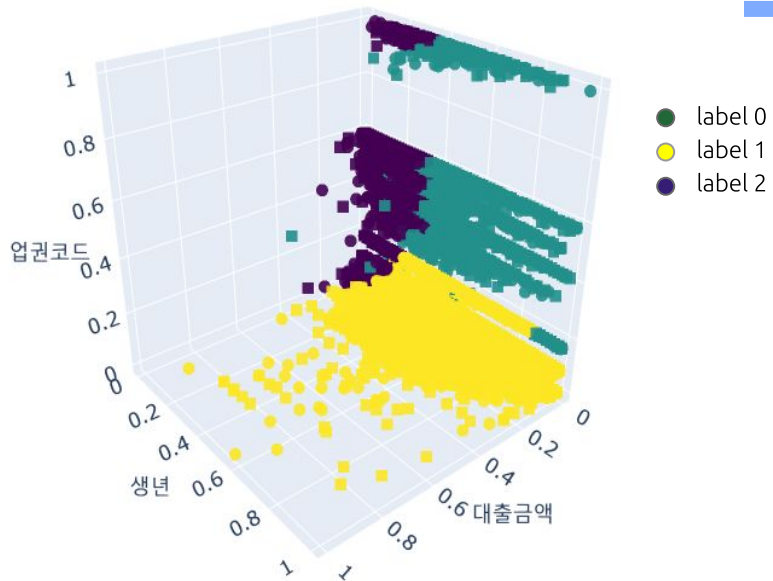
Clustering

- 비슷한 속성을 가진 사람들을 그룹으로 묶어주는 방법
- Clustering의 대표로 K-means 군집화 방식을 사용

K-means

- 효율적이고 해석이 쉬움
- 군집의 수도 자동화하여 결정해줄 수 있는 편리한 방식

K-means clustering



< K-means 수행 결과 데이터 분포 그래프 >

수행 결과

그룹이 label 0,1,2로 나뉘게 됨

그룹 특성

성별보다는 업권, 나이가 중요한 특성

- 해당 결과를 이용해 추천 과정을 진행

K-means clustering

해당 클러스터에서 가장 많이 가지는
상품을 추천하는 함수

```
def recommend(x): # x는 예측된 결과 데이터
    array = []
    for i in range(len(X_train)):
        if x[0] == X_train['cluster'][i]:
            array.append(y_train['LN_CD_2'][i])
    result = Counter(array)
    i = 0
    a = 0
    for key in result:
        if i < result[key]:
            i = result[key]
            a = key
    print(key, ': ', result[key], "명")
    print("")
    print("추천상품: " + str(a))
    print("고객님과 비슷한 수입, 나이대의 사람이 이 대출 상품을 "+str(i)+" 명 사용합니다.")
```

```
print("test 값의 cluster label은"+str(predict_1[0])+" 입니다.")
```

test 값의 cluster label은 2 입니다.

test 데이터의 cluster를 예측한다.



결과

200 : 834 명
100 : 6384 명
240 : 1156 명
0 : 7908 명
270 : 365 명
220 : 3410 명
230 : 764 명
245 : 49 명
500 : 809 명
590 : 125 명
510 : 237 명
710 : 41 명
290 : 257 명
210 : 91 명
170 : 11 명
250 : 122 명
150 : 14 명
700 : 18 명
271 : 5 명

추천상품: 0

고객님과 비슷한 수입, 나이대의 사람이 이 대출 상품을 7908 명 사용합니다.



test

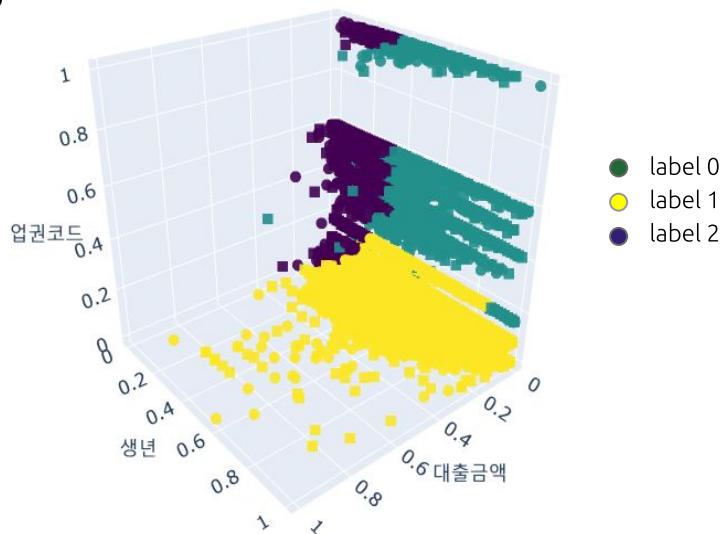
36세 남성
은행 대출금액 1,000,000원

가장 많은 7908명이 사용하는 대출 상품 0을 추천해준다.

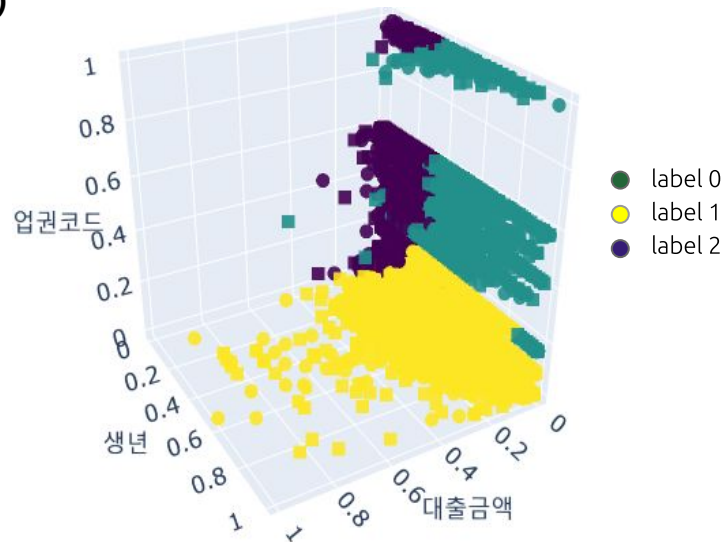
K-means clustering with DP

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

(전)

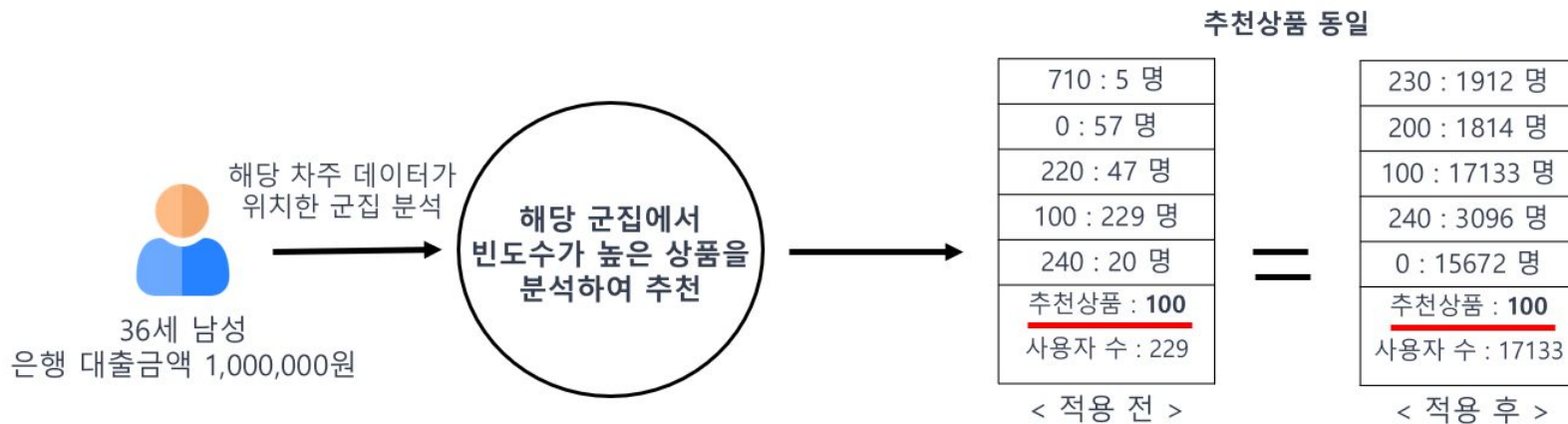


(후)



차등 프라이버시 적용으로 일부 cluster의 값이 변경됨

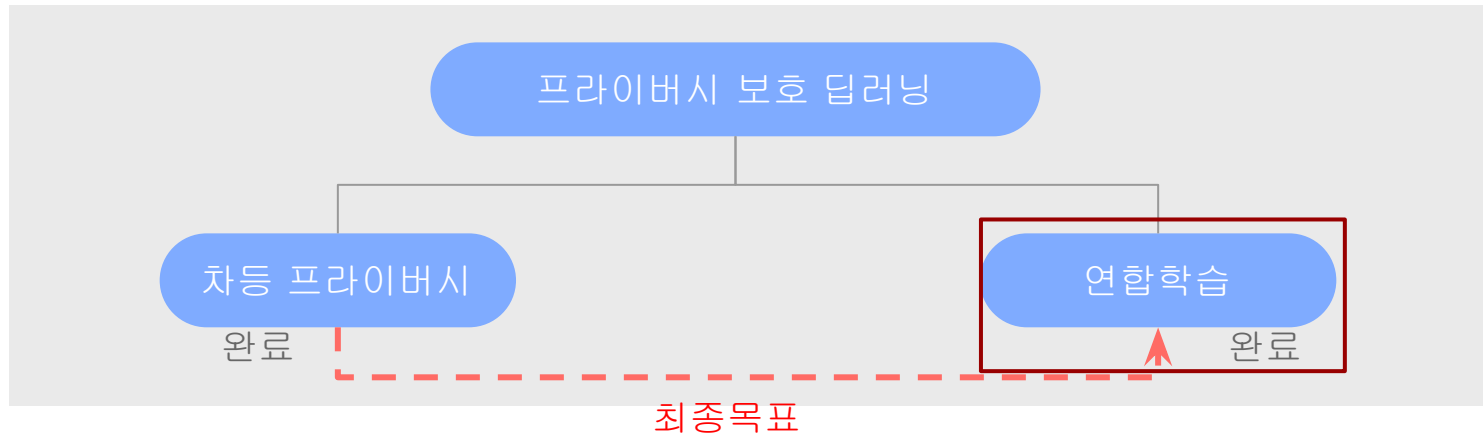
K-means clustering with DP

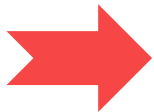


결과

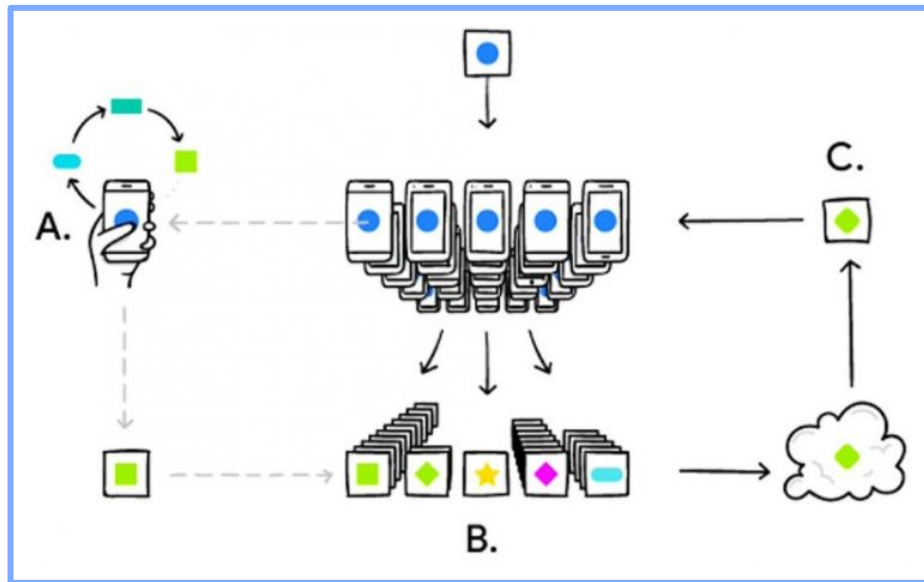
- ✔ 차등 프라이버시 적용 데이터는 비식별화를 통하여 데이터를 보호하여 안전성을 높임
- ✔ 차등 프라이버시 적용 전/후 결과는 변화가 없어 데이터 유용성은 훼손시키지 않음
- ✔ 고객 데이터를 기반으로 사용자에게 맞춤형 상품을 안전하고 정확하게 제공할 수 있음

해결방법



 연합학습에 차등프라이버시를 적용하여 프라이버시를 보호

해결방법 2 - 연합 학습



*자료 : Google AI

A. 단말이 학습을 통해 알고리즘 성능 강화

B. 학습한 알고리즘을 클라우드 데이터 센터로 전송

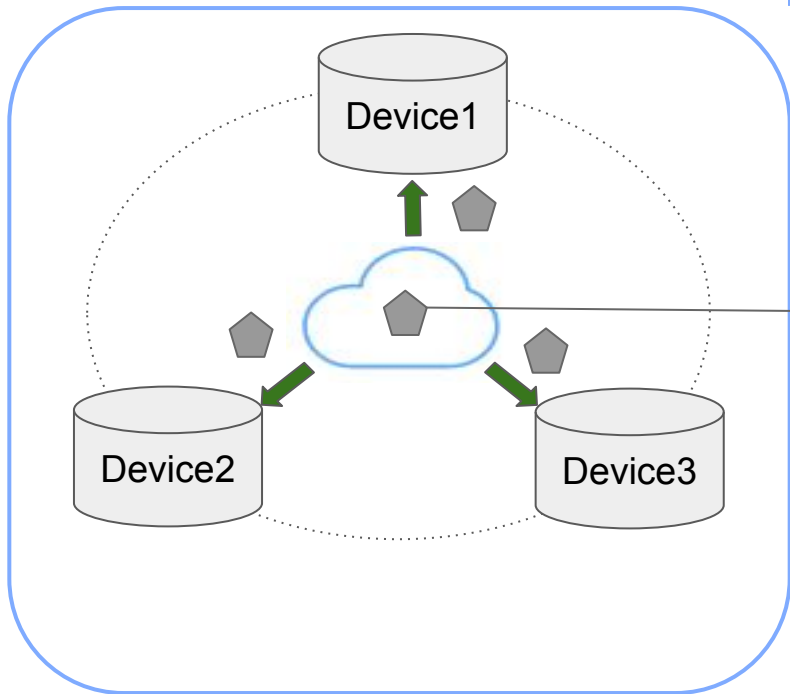
C. 공통 성능 개선 요소를 생성해 각 단말에 전송

Federated Learning

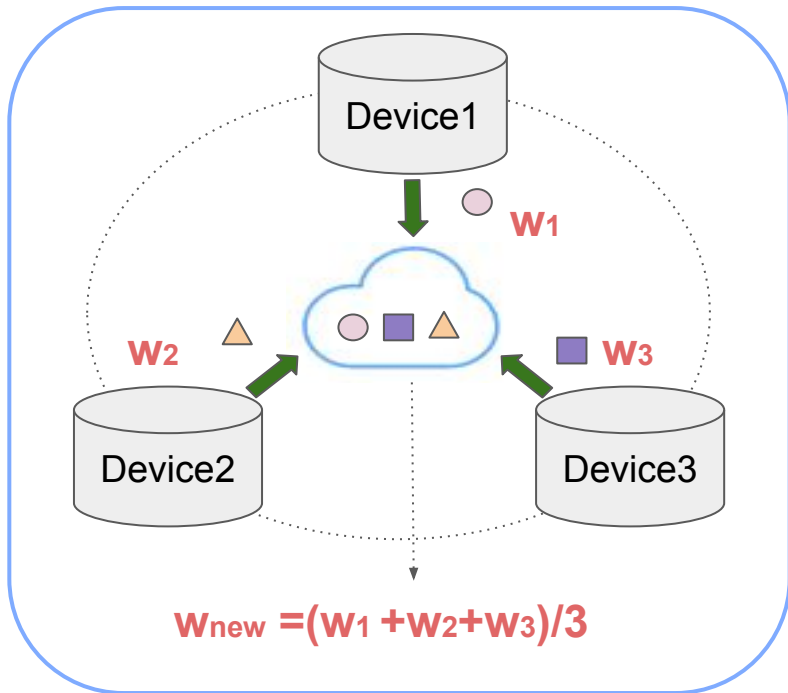
A. 단말이 학습을 통해 알고리즘 성능 강화

< 초기 모델의 낮은 정확도 >

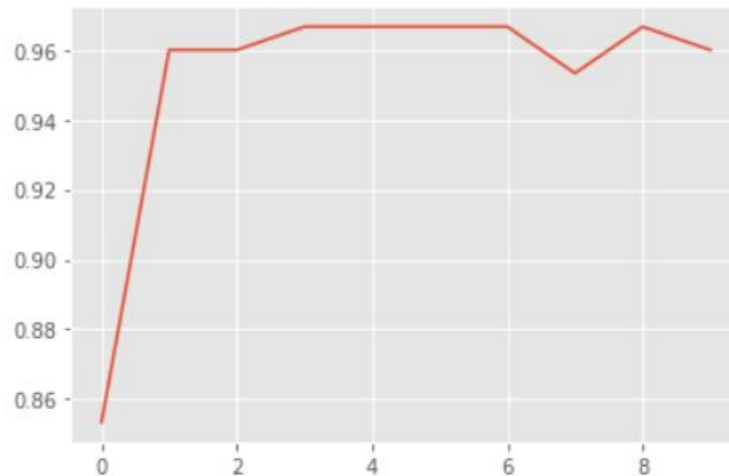
→ **accuracy: 0.773**



Federated Learning



B. 학습한 알고리즘을 클라우드 데이터 센터로 전송



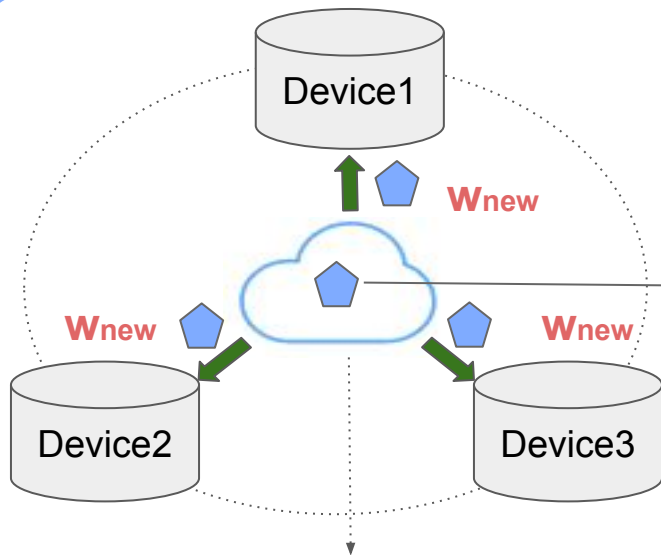
클라우드에서는 단말의 학습 파라미터만으로 모델 업데이트

Federated Learning

C. 공통 성능 개선 요소를 생성해 각 단말에 전송

< 연합학습 후 얻은 높은 정확도 >

accuracy: 0.96

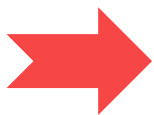
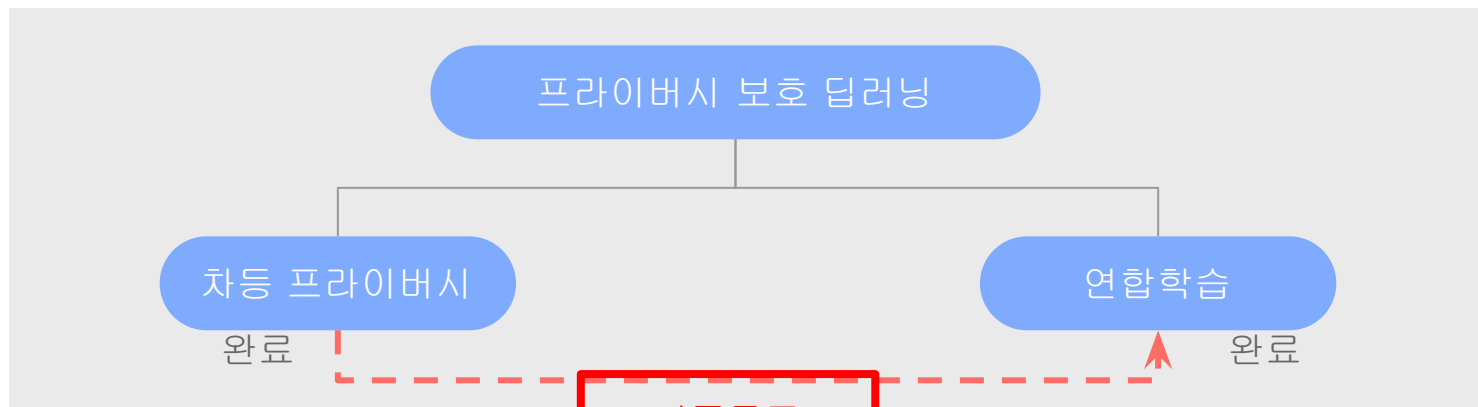


$$W_{new} = (w_1 + w_2 + w_3) / 3$$

결과

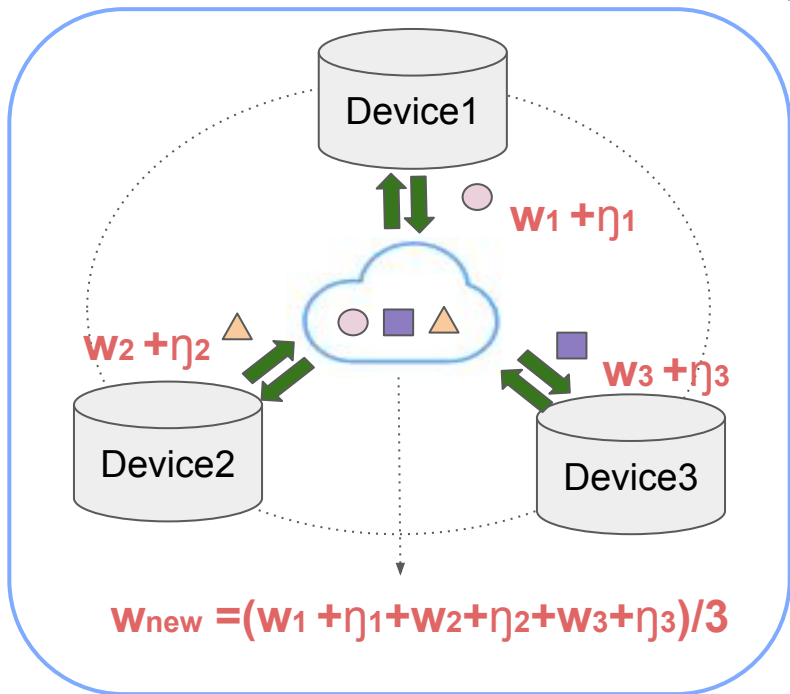
- ✓ 데이터를 학습하는 역할을 사용자들이 나눔으로써 중앙 컴퓨터 파워 부하량이 감소함
- ✓ 민감한 데이터를 중앙으로 수집하지 않아 프라이버시 문제를 해결할 수 있음
- ✓ 프라이버시 문제를 해결하여 사용자로부터 데이터를 수집하기 용이함

해결방법



연합학습에 차등프라이버시를 적용하여 프라이버시를 보호

차등프라이버시를 적용한 연합학습 구현



목적

모델의 역추적을 통한 데이터 예측 방지

기존 시스템

서버에 가중치 전송

목표 시스템

가중치에 차등 프라이버시 적용

기대효과

중간 통계값에 의한 프라이버시 노출을 방지 하면서 연합학습 수행

차등프라이버시를 적용한 연합학습 구현

A. 간단한 MLP 훈련

Model: "sequential_1"

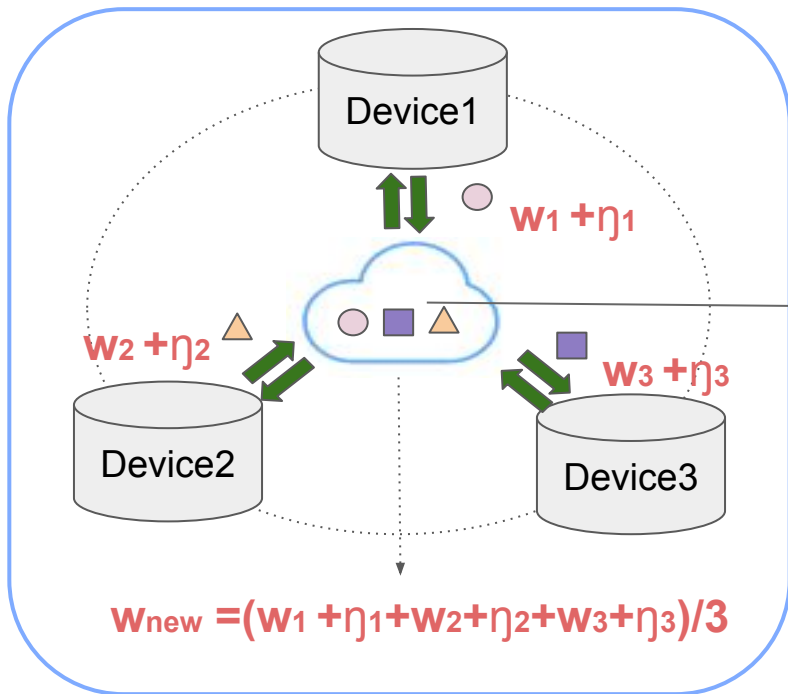
Layer (type)	Output Shape	Param #
dense_2 (Dense)	(None, 1000)	11000
dense_3 (Dense)	(None, 20)	20020

Total params: 31,020
Trainable params: 31,020
Non-trainable params: 0

< 100 EPOCH 의 훈련 >

→ **accuracy: 0.92**

차등프라이버시를 적용한 연합학습 구현



B. 연합학습

< 100 ROUND 의 훈련 >

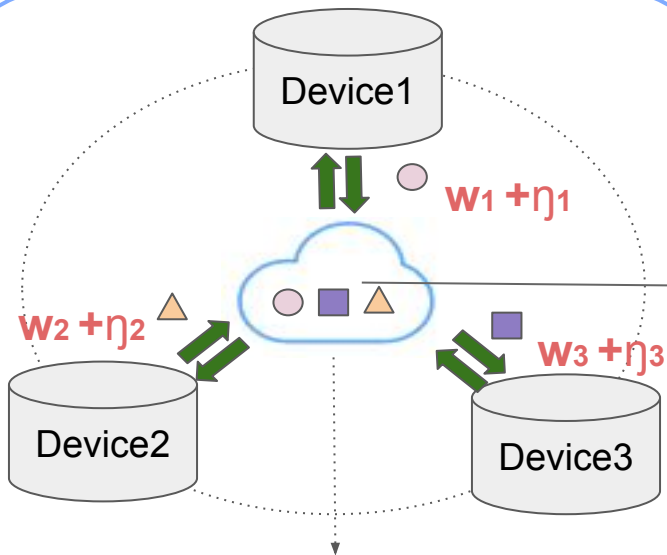
accuracy: 0.82

차등프라이버시를 적용한 연합학습 구현

C. 차등프라이버시를 적용한 연합학습

< 200 ROUND 의 훈련 >

accuracy: 0.79



$$w_{\text{new}} = (w_1 + \eta_1 + w_2 + \eta_2 + w_3 + \eta_3) / 3$$

결과

- ✓ 전송되는 가중치에 차등프라이버시를 적용함으로써 모델 역추적을 통한 데이터 유출 방지
- ✓ 모델의 정확도는 추가적인 학습을 통해 문제점이 해결 가능하다는 것을 확인
- ✓ 프라이버시 문제를 해결하여 사용자로부터 데이터를 수집하기 용이함

감사합니다!