he Journal of the Convergence on Culture Technology (JCCT)
Vol. 10, No. 1, pp.435-441, January 31, 2024. pISSN 2384-0358, eISSN 2384-0366

http://dx.doi.org/10.17703/JCCT.2024.10.1.435

JCCT 2024-1-51

# 개인정보 보호를 고려한 딥러닝 데이터 자동 생성 방안 연구

# A Study of Automatic Deep Learning Data Generation by Considering Private Information Protection

장성봉*

**Sung-Bong Jang***

**요 약** 수집된 대량의 데이터셋이 딥러닝 학습데이터로 사용되기 위해서는 주민번호, 질병 정보등과 같이 민감한 개인정보는 해커에게 노출되지 않도록 값을 변경하거나 암호화해야 하고 구축된 딥러닝 모델의 구조와 일치 하도록 데이터를 재구성 해주어야 한다. 현재, 이러한 작업은 전문가에 의해 수동으로 이루어지기 때문에, 시간과 비용이 많이 소요 된다. 이러한 문제점을 해결하기 위해, 본 논문에서는 딥러닝 과정에서 개인정보 보호를 위한 데이터 처리 작업을 자동으로 수행할 수 있는 기법을 제안한다. 제안된 기법에서는 데이터 일반화에 기반한 개인정보 보호 작업을 수행하고 원형큐를 사용하여 데이터 재구성 작업을 수행한다. 제안된 기법의 타당성을 검증하기 위해, C언어를 사용하여 직접 구현하였다. 검증 결과, 데이터 일반화가 정상적으로 수행되고 딥러닝 모델에 맞는 데이터 재구성이 제대로 수행됨을 확인 할 수 있었다.

**주요어** : 개인 정보 보호, 딥러닝, 데이터 전처리, 기계 학습

**Abstract** In order for the large amount of collected data sets to be used as deep learning training data, sensitive personal information such as resident registration number and disease information must be changed or encrypted to prevent it from being exposed to hackers, and the data must be reconstructed to match the structure of the built deep learning model. Currently, these tasks are performed manually by experts, which takes a lot of time and money. To solve these problems, this paper proposes a technique that can automatically perform data processing tasks to protect personal information during the deep learning process. In the proposed technique, privacy protection tasks are performed based on data generalization and data reconstruction tasks are performed using circular queues. To verify the validity of the proposed technique, it was directly implemented using C language. As a result of the verification, it was confirmed that data generalization was performed normally and data reconstruction suitable for the deep learning model was performed properly.

**Key words :** Privacy Protection, Deep Learning, Data Pre-processing, Machine Learning

## Ⅰ. 서 론

코로나 유행으로 인한 비대면 산업 환경의 도래는 인공지능을 가능하게 하는 딥러닝 기술에 대한 수요를 점점더 증가시키고 있다. 딥러닝은 여러개의 계층을 가진 심층 신경망(Deep Neural Network)을 구성하고 학습 데이터를 이용하여 이를 훈련 시키고 훈련된 신경망을 데이터 분류, 예측에 사용하는 기술이다. 딥러닝 모

*정회원, 금오공과대학교 산학협력단 교수 (제1저자)
접수일: 2023년 10월 15일, 수정완료일: 2023년 11월 9일
게재확정일: 2023년 11월 10일

Received: October 15, 2023 / Revised: November 9, 2023
Accepted: November 10, 2023
*Corresponding Author: sungbong.jang@kumoh.ac.kr
Dept. of Industry-Academy, Kumoh Institute of Technnology, Korea

델을 훈련 시키기 위해서는 대량의 데이터를 적절히 원하는 형태로 구성하고 필요할 경우, 보안을 위해 원래의 데이터를 변경하는 작업이 필요하다[1]. 이러한 데이터 보안 처리 및 구성을 위한 작업은 고도의 전문성을 요구하기 때문에, 시간이 오래 걸리고 비용이 많이 들어가게 된다[2]. 관련 연구를 살펴본 결과, 기존의 딥러닝 기법에서는 다음과 같은 문제점들이 노출되었다. 첫째, 기존의 딥러닝용 도구들 에서는 개인정보 보호를 충분히 고려하지 않았다. 전세계적으로 딥러닝을 위한 학습 데이터는 방대한 양이 실시간으로 축적되고 있으며, 이를 활용하여 각종 AI서비스를 개발하여 마케팅에 활용하고 있다. 하지만, 학습 데이터 속에 포함된 개인정보 및 중요 데이터에 대한 보호가 허술하여, 해커들의 공격에 매우 취약하다[3]. 따라서, 원래의 데이터를 그대로 제공하지 말고 일부 변경한 후, 학습 데이터로 제공해야 한다. 학습 데이터를 변경하는 가장 단순한 방법은 엑셀과 같은 도구를 사용하여 직접 작업을 해주는 것이다. 하지만, 데이터 갯수가 수십만개로 커질경우에는 이를 일일이 수작업으로 작업하는 것은 비효율적이다[4]. 본 연구에서는 이를 쉽게 할 수 있는 소프트웨어 도구를 개발하고자 한다. 둘째, 딥러닝을 위해 구성된 심층 신경망 구조와 일치하는 학습 데이터를 생성하는 과정이 매우 불편하다. 예를 들어, 입력층이 10개이고 출력층이 5개인 심층 신경망을 구성했다고 하자. 그러면, 순차적으로 구성되어 있는 데이터를 15개의 훈련 데이터로 재구성한 후, 이를 모델의 입력 데이터로 사용해야 한다. 이렇게 데이터를 재구성하기 위해서는 사용하는 딥러닝 도구의 데이터 처리 함수를 사용하여 코딩을 해주어야 한다. 전문 프로그래머가 아닐 경우, 이 과정은 조금 복잡하며, 딥러닝 도구마다 처리하는 방법이 너무 다양하다. 본 연구에서 이를 자동으로 수행해 줄 수 있는 도구를 개발하고자 한다.

## II. 이론고찰

R. Podschwadt의 논문[5]에서는 동형 암호와 기법(homomorphic encryption)를 사용한 개인 정보 보호가 가능한 기계 학습(PPML)에 대한 기존의 기법들을 소개하고 있다. 또한, 이 논문에서는 개인정보 보호를 위한 신경망 모델 및 아키텍처 변경이 기계학습 성능에 어떠한 영향을 미치는지 실험을 통해 분석 하고 새로운 성능 평가지표를 제안 하였다. T. Zhang의 논문[6]에서는 개인정보 보호 기반 경사하강법(DP-SGD, Differential Private Stochastic Gradient Descent)을 사용한 딥러닝를 사용할 경우, 정확도의 큰 손실 없이 낮은 식별 수준에서 모델 업데이트 가능성을 제공하기 때문에, 훈련 횟수(learning epoch)가 개인정보 보호 정도와 정확도 간의 균형을 맞추는 중요한 변수라는 것을 밝혀 내었다. 이를 바탕으로, 분석가가 이상적인 균형을 달성하기 위해 모델 훈련을 중지할 최적의 시기를 선택하는 데 도움이 되는 두 가지 다른 조기 중지 기준을 제시 하였다. V. Stephanie 논문[7]에서는 헬스케어 분야에서 사물 인터넷(IoT), 엣지 및 클라우드를 사용한 개인 정보 보호를 고려한 강화 심층 신경망(DNN) 기반 학습 프레임워크를 제안하고 있다.  제안된 프레임워크는 서버에서 손실을 최소화하고 효율성을 높이기 위해 로컬 모델 생성을 위한 전이 학습을 갖춘 차등 개인 정보 보호 기반 기법을 제시하고 있다. M. Shateri 논문[8]에서는 데이터의 전체 시간적 상관 관계를 모델링하여 상호 정보 기반 보상 신호를 추정하고 이를 신경망 모델 학습에 사용하는 기법을 제시하고 있다. 제시된 기법은 실제 데이터셋을 사용하여 경험적으로 성능 평가를 진행하고 간단한 개인 정보 보호 지표값을 측정하여 기존의 방법과 비교 하였다. T. Zhu[9]는 차등 프라이버시(Differential Privacy) 기법의 적용 분야에 대해서 설명하고 있다. 본 기법은 보안을 강화하면서 성능을 보장하여 기계학습 모델을 구축하고 학습하는데 사용될 수 있음 보여주고 있다. 특히,  분산 기계 학습, 딥 러닝 및 다중 에이전트 시스템에서 AI 성능을 향상할 수 있는 다양한 가능성에 대한 새로운 관점을 제공하고 있다. Z. Wu 논문[10] 에서는 스마트폰 카메라 응용 프로그램에서 점정 중요해지고 있는 딥러닝 기반 활동 감지 프로그램에서 적대적 해킹으로부터 개인정보 보호를 위한 기법들에 대해서 서술하고 있다. 또한, 기존의 기법들을 적용하기 위한 최적화 전략 기법에 대해서 서술하고 있다. L. Xiang 논문[11]에서는 모델 매개변수로부터 개인 훈련 데이터를 추론하여 개인 정보를 탈취하는 개인정보 공격을 완화하기 위해 제안된 노이즈 추가 기반 차등 프라이버시(differential privacy) 기법의 문제점인 과다 노이즈 첨가 문제를 해결하기 위한 기법을 제안 하였다. 제안된 기법에서는 노이즈 방향(directional noise) 값을 고려하여 노이즈를 추가하도록 하였다. A. E.

Ouadrhiri 논문[12]에서는 딥러닝과 연합학습에서 사용자의 프라이버시를 보장하기 위한 차등 정보 보호 기법(Differential Privacy)의 주요 아이디어를 분석하고 설명하고 있다. 또한 차등 정보보호 기법의 메커니즘을 충족하는 모든 유형의 확률 분포를 해당 속성 및 사용 사례와 함께 설명하고 있다. R. Parekh 논문[13] 에서는 자율 주행차 분야의 기계 학습에서 암호화에 기반한 개인정보 보호 딥러닝 프레임워크를 제안하고 있다. 제안된 기법에서는 엣지 장치에 존재하는 로컬 딥러닝 모델을 미세 조정하고 전송되는 입력 데이터는 암호화하여 원격에서 딥러닝을 수행하도록 하고 있다. 이 이외에도 딥러닝 데이터셋에 포함된 정보를 암호화-복호화 함으로써, 개인정보를 보장하는 다양한 연구들이 진행 되었다[14-17].

현재까지 살펴본 기존의 연구들에서는 개인정보를 보호하기 위한 다양한 기법들을 제시하고 있지만, 기법을 적용하기 전에 기존의 데이터셋을 딥러닝 모델의 구조에 맞는 데이터 재구성, 전처리, 데이터 일반화에 대한 연구는 진행되지 않았다.

## III. 연구 방법

본 연구에서는 개인정보 보호를 위해 딥러닝 학습 데이터에 포함된 민감정보를 쉽게 변경하고 원래의 데이터를 딥러닝 구조에 맞는 데이터로 자동으로 변경할 수 있는 기법을 제시하고 이를 지원하기 위한 소프트웨어 도구를 개발 하였다. 제시된 기법은 다음과 같다.

### 1. 딥러닝용 원시 데이터 읽기 기능

딥러닝 학습 데이터 형태를 저장하기 위해 가장 많이 사용하는 형태가 쉼표구분 파일(CSV, Comma Separated Value)포맷이다. 이 방법은 데이터 값 사이에 쉼표를 삽입하여 값을 구분한다. 본 연구에서는 개인정보 보호를 고려한 학습 데이터 생성을 위해 CSV형태로 저장된 데이터를 숫자의 형태로 메모리로 읽어와야 한다. 이때, 문제가 되는 부분은 CSV로 저장된 데이터는 숫자가 아니라 텍스트로 저장되어 있다는 점이다. 학습 데이터 재생성을 위해서는 이를 숫자로 변경해야 한다. 이를 위해, 본 연구에서는 다음과 같은 2 단계 과정을 거쳐서 데이터를 읽도록 하였다. 첫 단계에서는 텍스트 형태로 저장된 데이터를 한 바이트씩 읽어서 버퍼에 저장한다. 한 바이트씩 읽기와 저장을 반복하다 쉼표(,)를 만나게 되면, 읽기를 멈춘다. 두 번째, 현재까지 읽은 문자 데이터를 딥러닝이 가능한 숫자 데이터로 변경한 후, 다시 저장 한다. 이를 수행하기 위한 알고리즘은 다음 [그림 1]과 같다.

```
입력데이터 파일과 출력데이터 파일 열기;
for(j=0;j<NUMBER_OF_ML_DATA;j++) {
  i=0;
  do {
       입력파일에서 한글자읽은후 변수 c에저장;
        if(c=파일의끝) 반복문 중단;  // 입력 데이
          c에 저장된 글자를 item에 저장;
      } while(c != ',');
      item의 마지막에 종료문자('\0')추가;
     item에 저장된 문자열을 숫자로 변경;
     원형큐에 숫자로 변경된 데이터값 추가;
}
```

그림 1. 파일로부터 딥러닝 데이터 읽기 위한 알고리즘
Figure 1. An algorithm for reading deep learning data from file

### 2. 딥러닝 모델에 맞는 데이터 생성 기능

본 연구에서는 원형큐를 이용한 학습 데이터 생성 기법을 제안 한다. 제안된 기법에서는 원형큐 버퍼를 사용하여 딥러닝 모델의 입력층과 출력층 개수와 동일한 개수를 갖는 여러줄의 학습 데이터를 생성하도록 하였다. 알고리즘은 [그림 2]와 같다.

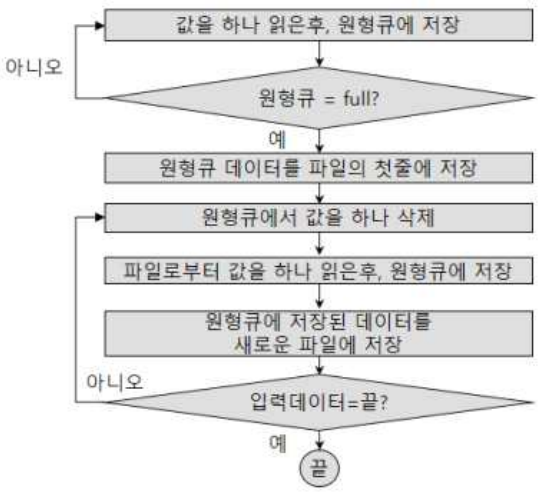


그림 2. 딥러닝 모델 데이터 재생성 알고리즘
Figure 2. An algorithm for regenerating deep learning data

첫째, 값을 하나씩 읽은 후, 원형큐(circular queue)에 저장 한다. 이때, 원형큐의 크기는 딥러닝에서 학습을 한 번 할 때마다 필요한 데이터의 개수만큼 설정하게 된다. 둘째, 원형큐 버퍼가 모두 차게 되면(버퍼풀), 이를 처음

부터 읽어서, 외부 파일의 첫줄에 저장 한다. 셋째, 값들을 하나씩 아래로 이동 저장 하기 위해 원형큐의 맨 뒤에서 값을 하나 삭제하여 새로운 값을 저장할 공간을 확보한다. 넷째, 입력 파일에서 값을 읽은 후, 삭제된 위치에 값을 저장한다. 다섯째, 원형큐 버퍼가 모두 차게 되므로(버퍼풀), 이를 처음부터 읽어서, CSV파일의 둘째줄에 저장 한다. 입력 데이터를 모두 읽을 때까지 단계 5) ~5) 까지 반복한다. 입력데이터를 모두 처리하고 나면, 학습을 위한 여러줄의 데이터가 생성된다. 알고리즘에서 사용되는 자료구조와 API(Application Program Interface) 함수는 [그림 3]과 같다.

```
typedef float element;
typedef struct QueueType {
        element data[NUMBER_OF_ML_DATA];
        int q_f, q_r;
} dlQtype;
void dl_qinit(dlQtype* q);
int dl_empty(dlQtype* q);
int dl_full(dlQtype* q) ;
void dl_enqueue(dlQtype* q, float data) ;
element dl_dequeue(dlQtype* q);
```

그림 3. 딥러닝 데이터 재생성을 위한 자료구조와 API함수
Figure 3. Data structures and API functions for regenerating deep learning data

3. 데이터 일반화에 기반한 개인정보 보호 기능

본 연구에서는 개인 정보 보호를 위해 데이터 일반화에 기반한 딥러닝 데이터 생성 기능을 구현 하였다.

```
if(mode = 3구간일반화) {
    for(j=0;j<25;j++) {
        if( 원래데이터값> (2.0*j) and
            원래데이터값<= ((2.0*j)+2.0))  {
                일반화된데이터값= 2.0*j+1.0;
                반복문중단;
        }
    }
    일반된데이터값을문자데이터로 변경;
    문자 데이터로 변경된 값을 파일에 저장;
}
```

그림 4. 연구에서 사용된 데이터 일반화 알고리즘
Figure 4. Data generalization algorithm used in the research

데이터 일반화 기법은 매우 다양한 방법이 존재하는데, 본 연구에서는 구간별 일반화 기법을 사용하였으며, 그 중에서도 3구간 일반화 기법을 구현하였다. 본 연구에서 구현한 알고리즘은 [그림 4]와 같다.

4. 변경된 데이터를 CSV로 저장하는 기능

일반화된 데이터는 세단계를 거쳐서 CSV파일로 저장하도록 하였다. 첫째, 출력할 파일을 연다. 두 번째, 숫자 데이터를 문자 데이터로 변경한 후, 맨 뒤에 쉼표(,) 문자를 붙인 후, 문자열을 버퍼에 저장한다. 세 번째, 저장된 문자열을 파일에 쓴다.

## Ⅳ. 연구 결과

본 연구에서 제안한 기법에 대한 타당성 검증을 위해 제안된 기법을 C언어로 구현하였다. 또한, 실험을 위해 총 10년간의 미세먼지 데이터셋을 수집하고 구현된 도구를 사용하여 타당성을 검증 하였다.

첫째, 딥러닝 모델 구조에 맞는 데이터 생성기능 실험을 진행 하였다. 실험에서는 입력층이 10개, 출력층이 5개인 딥러닝 모델을 가정하였다. 파일에 순차적으로 저장된 원래의 데이터는 10개의 입력 데이터와 5개의 정답 데이터가 한줄씩 순차적으로 저장된 구조로 재생성 되어야 하며, 재생성된 값들은 하나씩 오른쪽으로 이동 되어서 배치되어야 한다. [그림 5]는 실험에서 사용된 원래의 데이터셋을 보여주고 있다.

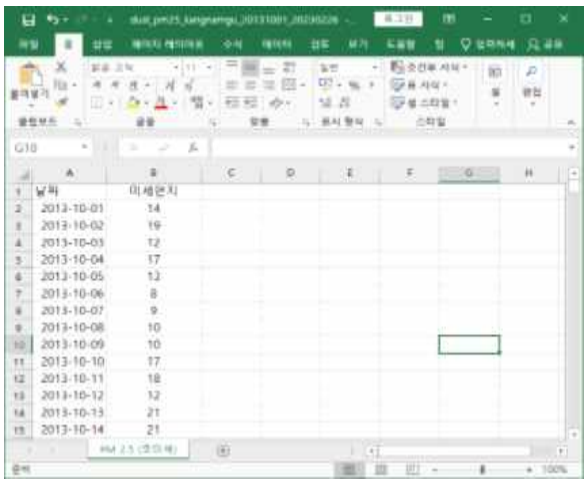


그림 5. 실험에서 사용된 원래의 데이터셋
Figure 5. Original dataset used in the experiment

그림에서 보듯이 한줄에 값 하나씩 순서대로 저장되어 있음을 알 수 있다. [그림 6]은 구현된 도구를 사용하여, 딥러닝 모델 구조에 맞는 데이터 생성기능 실험 결과를 보여 주고 있다.


그림 6. 딥러닝 모델 구조에 맞게 생성된 학습 데이터
Figure 6. Learning dataset fit to a structure of deep learning model

그림에서 보듯이 딥러닝 모델의 구조에 맞도록 한줄에 15개(10개:입력, 5개:정답)의 데이터가 한줄씩 저장되어 있고 값들이 하나씩 밀려서 배치되어 정상적으로 재생성 되었음을 알 수 있다.

다음으로, 개인정보 보호를 위한 데이터 일반화 기능 실험을 진행하였다. [그림 7]은 데이터 일반화를 수행하는 모습을 보여주고 있다.

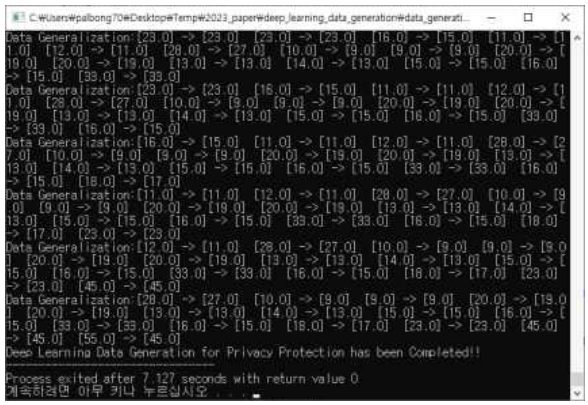


그림 7. 데이터 일반화를 진행하고 있는 화면
Figure 7. Captured screen of data generalization process in the experiment

데이터 일반화 실험 결과는 [표 1]과 같다.

표 1. 데이터 일반화 실험 결과
Table 1. Experiment results of 3-range data generalization

| 원래값 | 일반화된 값(3구간) |
|---|---|
| 14 | 13 |
| 19 | 19 |
| 12 | 11 |
| 17 | 17 |
| 13 | 13 |
| 8 | 7 |
| 9 | 9 |
| 10 | 9 |
| 17 | 17 |
| 18 | 17 |
| 12 | 11 |
| 21 | 21 |
| 21 | 21 |
| 13 | 13 |

일반화된 데이터 파일(CSV파일)로 저장된 데이터셋은 이미 언급된 [그림 6]에 나와 있다. 그림에서 맨 첫 줄에 저장된 15개 데이터가 일반화된 데이터이다. 일반화 이전의 원래의 값은 14, 19, 12, 17, 13, 8, 9, 10, 10, 17, 18, 12, 21, 21, 13이다. 이 값들은 [표 2]과 같은 규칙에 따라, 변경되어야 한다.

표 2. 3구간 데이터 일반화 규칙
Table 2. 3-range data generalization rules

| 원래값(3구간) | 일반화된 후의 대표값 |
|---|---|
| 0,1,2 | 1 |
| 3,4,5 | 4 |
| 6,7,8 | 7 |
| 9,10,11 | 10 |
| 12,13,14 | 13 |
| 15,16,17 | 16 |
| 18,19,20 | 19 |
| 21,22,23 | 22 |
| 24,25,26 | 25 |
| 27,28,29 | 28 |
| 30,31,32 | 31 |
| 33,34,35 | 34 |
| 36,37,38 | 37 |
| 39,40,41 | 40 |
| 42,43,44 | 43 |
| 45,46,47 | 46 |
| 48,49,50 | 49 |
| 51,52,53 | 52 |
| 54,55,56 | 55 |
| 57,58,59 | 58 |
| 60,62,63 | 62 |
| 64,65,66 | 65 |

위 표를 참고하여 첫줄 결과를 살펴보면 정상적으로 일반화되었음을 알 수 있다.

다음으로, 일반화된 데이터가 CSV 파일로 저장이 되는지 실험하였다. [그림 8]은 일반화된 데이터를 저장한 CSV파일 메모장으로 열었을 때의 화면이다. 그림에서, 데이터 사이에 쉼표가 들어가 있으므로, 제대로 CSV 파일로 저장되었음을 알 수 있다.


그림 8. CSV 파일로 저장된 딥러닝 모델 데이터셋
Figure 8. Dataset saved as CSV format for deep learning

## V. 결 론

딥러닝 모델을 학습시키기 위해 수집된 데이터 내에는 다수의 민감정보들이 포함되어 있으며, 개인정보 보호를 위해 이를 적절하게 변경하고 모델의 구조에 맞도록 데이터를 재구성 해주어야 한다. 이러한 과정은 전문가의 경험에 의존하여 수동으로 이루어지기 때문에 많은 시간과 비용이 들어간다. 본 연구에서는 이러한 문제점을 해결하기 위한 기법들을 제시하고 이를 C언어로 구현하고 타당성을 검증하였다. 검증 결과, 딥러닝 모형에 맞는 데이터 재구성과 데이터 일반화가 자동으로 이루어짐을 확인 하였다. 본 연구에서 데이터 일반화의 경우, 3구간 일반화 기능만 구현 하였다. 추후에는 3구간 일반화 뿐만 아니라, 원하는 구간을 사용자로부터 입력받아서, 원하는 구간으로 모두 일반화 할 수 있는 기능을 구현할 필요가 있다.

## References

[1] W. Wei and L. Liu, “Gradient Leakage Attack Resilient Deep Learning,” *IEEE Transactions on Information Forensics and Security*, Vol. 17, pp. 303-316,2022(DOI:10.1109/TIFS.2021.3139777)

[2] N. Bugshan, I. Khalil, M. S. Rahman, M. Atiquzzaman;X. Yi, S. Badsha, “Toward Trustworthy and Privacy-Preserving Federated Deep Learning Service Framework for Industrial Internet of Things,” *IEEE Transactions on Industrial Informatics*, Vol. 19, No.2 pp. 1535-1547,2023(DOI: 10.1109/TII.2022.3209200)

[3] D. Mistry, M. F. Mridha, Me. Safran, S. Alfarhood, A. K. Saha, D. Che, “Privacy-Preserving On-Screen Activity Tracking and Classification in E-Learning Using Federated Learning,” *IEEE Access*, Vol. 11, pp. 79315-79329, 2023(DOI: 10.1109/ACCESS.2023.3299331)

[4] I. Fontana, M. Langheinrich, M. Gjoreski, “GANs for Privacy-Aware Mobility Modeling,” *IEEE Access*, Vol. 11, pp. 29250-29262, 2023(DOI: 10.1109/ACCESS.2023.3260981)

[5] R. Podschwadt, D. Takabi, P. Hu, M. H. Rafiei, Z. Cai, “A Survey of Deep Learning Architectures for Privacy-Preserving Machine Learning With Fully Homomorphic Encryption,” *IEEE Access*, Vol. 10, pp.117477-117500,2022(DOI:10.1109/ACCESS.2022.3219049)

[6] T. Zhang, T. Zhu, K. Gao, W. Zhou, P. S. Yu, “Balancing Learning Model Privacy, Fairness, and Accuracy With Early Stopping Criteria,” *IEEE Transactions on Neural Networks and Learning Systems*, Vol. 34, No.9, pp.5557-5569,2023(DOI: 10.1109/TNNLS.2021.3129592)

[7] V. Stephanie, I. Khalil, M. S. Rahman, M. Atiquzzaman, “Privacy-Preserving Ensemble Infused Enhanced Deep Neural Network Framework for Edge Cloud Convergence,” *IEEE Internet of Things Journal*, Vol. 10, No.5, pp.3763-3773,2023(DOI: 10.1109/JIOT.2022.3151982)

[8] M. Shateri, F. Messina, P. Piantanida, F. Labeau, “Privacy-Cost Management in Smart Meters With Mutual-Information-BasedReinforcement Learning,” *IEEE Internet of Things Journal*, Vol. 9, No.22,pp.22389-22398,2022(DOI:10.1109/JIOT.2021.3128488)

[9] T. Zhu, D. Ye, W. Wang, W. Zhou, P. S. Yu, “More Than Privacy: Applying Differential Privacy in Key Areas of Artificial Intelligence,” *IEEE Transactions on Knowledge and Data Engineering*, Vol. 34, No. 6,pp.2824-2843,2022(DOI:10.1109/TKDE.2020.3014246)

[10] Z. Wu, H. Wang, Z. Wang, H. Jin, Z. Wang, “Privacy-Preserving Deep Action Recognition: An Adversarial Learning Framework and A New Dataset,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 44, No. 4, pp. 2126-2139,2022(DOI: 10.1109/TPAMI.2020.3026709)

[11] L. Xiang, W. Li, J. Yang, X. Wang, B. Li, “Differentially-Private Deep Learning With Directional Noise,” *IEEE Transactions on Mobile Computing*, Vol. 22, No. 5, pp. 2599-2612,2023(DOI: 10.1109/TMC.2021.3130060)

[12] A. E. Ouadrhiri, A. Abdelhadi, “Differential Privacy for Deep and Federated Learning: A Survey,” *IEEE*

*Access*, Vol. 10, pp. 22359-22380,2022(DOI: 10.1109/ACCESS.2022.3151670)

[13] R. Parekh, N. Patel, R. Gupta, N. K. Jadav, S. Tanwar, A. Alharbi, A. Tolba, B.-C. Neagu, M. S. Raboaca, "GeFL: Gradient Encryption-Aided Privacy Preserved Federated Learning for Autonomous Vehicles," *IEEE Access*, Vol. 11, pp. 1825-1839,2023(DOI:10.1109/ACCESS.2023.3233983)

[14] W. Zhang, B. Jiang, M. Li, X. Lin, "Privacy-Preserving Aggregate Mobility Data Release: An Information-Theoretic Deep Reinforcement Learning Approach," *IEEE Transactions on Information Forensics and Security*, Vol. 17, pp. 849-864, 2022(DOI: 10.1109/TIFS.2022.3152361)

[15] X. Ma, Q. Jiang, X. Liu, Q. Pei, J. Ma, W. Lou "Learning in Your "Pocket": Secure Collaborative Deep Learning With Membership Privacy," *IEEE Transactions on Dependable and Secure Computing*, Vol. 20, No.3, pp. 2641-2656, 2023(DOI: 10.1109/TDSC.2022.3192326)

[16] H.-K. Ko, "Privacy Preserving Techniques for Deep Learning in Multi-Party System," *The Journal of the Convergence on Culture Technology (JCCT)*, Vol. 9, No.3, pp. 647-654, 2023(DOI: http://dx.doi.org/10.17703/JCCT.2023.9.3.647)

[17] K. KIM, S.-H. Lee, "Development of CNN-Transformer Hybrid Model for Odor Analysis," *International Journal of Advanced Culture Technology*, Vol. 11, No.3, pp. 297-301, 2023(DOI:https://doi.org/10.17703/IJACT.2023.11.3.297)

※ 이 연구는 금오공과대학교 대학 학술연구비로 지원되었음(2022년)