https://doi.org/10.7840/kics.2025.50.3.395

데이터 분포 불균형 문제 해결을 위한 다중 기기 연합학습 기반 운전자 이상 행동 탐지

권 병 근◆, 김 수 현°

Driver Behavior Anomaly Detection Based on Federated Learning Considering Data Distribution Imbalance

Byeongkeun Kwon◆, Suhyeon Kim°

요 약

본 연구는 자동차 모빌리티 환경에서의 이상 행동 탐지를 위한 연합학습 기반 프레임워크를 제안하고, 이를 다양한 시나리오 실험을 통해 검증한다. 제안한 프레임워크는 데이터를 로컬 차량 클라이언트에 안전하게 보존하면서 다중 기기 연합 학습 기법을 적용하여, 데이터 프라이버시 보호와 높은 예측 성능 간의 균형을 달성한다. 특히 자동차 모빌리티 환경 특유의 데이터 분포 불균형 문제를 반영하고, MobileNet과 같은 경량 딥러닝 모델을 활용하여 실시간 이상 행동 감지에 적합한 계산 효율성을 확보하였다. 그 결과, 중앙집중형 모델과 유사한 수준의 연합 학습 모델 정확도를 달성하여 민감한 운전자 데이터의 직접적인 공유 없이 학습을 진행할 수 있음을 확인하였다. 이는 스마트 모빌리티 플랫폼과 같은 빅데이터 환경에서 개인정보 보호 규제를 준수하면서도 고성능 인공지능 모델 개발이 가능함을 의미한다. 본 연구는 모빌리티 분야에서 연합학습 적용의 실용성을 입증하고, 향후 다양한 응용 영역에서 데이터 프라이버시와 기술적 성능을 동시 달성할 수 있는 새로운 가능성을 제시한다.

키워드 : 모빌리티 데이터 분석, 프라이버시 보호 인공지능, 연합 학습, 이상탐지
Key Words : Mobility Data Analysis, Privacy-preserving AI, Federated Learning, Anomaly Detection

ABSTRACT

This study presents a cross-device federated learning framework for detecting anomalous behavior in automotive mobility and evaluates its performance across various experimental scenarios. The proposed framework retains data locally on vehicle clients, ensuring data privacy while achieving high predictive performance through cross-device federated learning settings. It addresses challenges specific to automotive mobility, such as data distribution imbalance, and employs the lightweight deep learning model like MobileNet for computational efficiency, enabling real-time anomaly detection. Experimental results can demonstrate that the federated learning model achieves accuracy comparable to centralized models without requiring the direct sharing of sensitive driver data. This highlights the framework's ability to balance data privacy and

※ This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No. RS-2023-00245529). Also, this work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (Ministry of Science and ICT) (No. RS-2023-00242528) and by the IITP (Institute for Information & Communications Technology Planning & Evaluation)-ITRC (Information Technology Research Center) grant funded by the Korea government (MSIT) (No. IITP-2025-RS-2024-00437756).
◆ First Author : Kyungpook National University, Graduate School of Data Science, house9895@knu.ac.kr, 학생회원
° Corresponding Author : Kyungpook National University, Graduate School of Data Science, suhyeonkim@knu.ac.kr, 정회원
논문번호 : 202412-318-A-RU, Received December 12, 2024; Revised January 23, 2025; Accepted February 5, 2025

performance, making it suitable for privacy-sensitive environments such as smart mobility platforms. We believe that the practicality of our framework in mobility applications and its broader potential for developing smart intelligent systems to comply with stringent privacy regulations can offer a valuable solution for integrating artificial intelligence into data-driven industries.

Ⅰ. 서 론

자동차 모빌리티 데이터 분석은 차량 주변 환경을 이해하고 운전자의 안전을 보장하기 위해 현대 모빌리티 산업분야에서 중요한 연구 주제로 떠오르고 있다. 데이터 분석 기술력이 점점 발전하면서 자동차 모빌리티 데이터를 활용한 분석 연구가 운전자의 안전 확보와 차량 주변 환경 보완에 기여하고 있다. 특히, 졸음, 휴대폰 사용, 흡연, 뒤돌아보기 등 운전자의 부주의 행동을 탐지해 이를 경고하는 시스템은 사고를 예방하는 데 중요한 역할을 한다. 이를 위해 국내외의 다양한 연구에서 영상 및 이미지 데이터를 활용해 딥러닝 기반의 모델을 학습하여 이상 행동을 탐지하는 것을 제안하고 있다.

딥러닝 기반 접근법은 운전자의 부주의 및 공격적 운전 행동을 탐지하기 위한 효과적인 도구로 부상하고 있다. 예를 들어, 운전자의 복잡한 시간적 행동 패턴을 학습하는 연구에서는 이러한 딥러닝 접근법이 전통적인 방법의 한계를 보완할 수 있음을 입증했다[1,2]. 또한, Inception v3와 Long Short Term Memory 등의 딥러닝 모델을 활용하여 흡연, 뒤돌아보기, 하품 등 다양한 부주의 행동을 탐지하며 높은 정확도를 달성한 사례도 있다[3,4]. 영상데이터 기반 탐지 기술도 중요한 연구 방향으로 제시되고 있다. 운전자의 이상 행동을 실시간으로 탐지한 연구[5]와 운전 이미지 데이터에 Convolutional Neural Network (CNN)을 활용한 연구[6]는 이러한 접근법의 가능성을 잘 보여준다. 또한 비지도 학습과 노이즈 제거 기법을 결합하여 비정상 운전을 탐지하는 오토인코더 기반 모델[7]과 경량화 된 딥러닝 프레임워크를 통해 실시간으로 이상 행동을 탐지하는 접근법은 모바일 환경에서도 실효성 높은 적용 가능성을 보여준다[8,9].

그러나 이상행동 탐지 모델의 학습을 위한 데이터는 운전자의 사진, 운전 패턴 등 프라이버시와 직결된 민감한 문제이다. 따라서 프라이버시 보호에 대한 고려 없이 데이터를 수집하고 분석하는 과정은 많은 윤리적, 법적 문제점을 불러올 수 있다[10]. 모든 데이터를 한군데 모아 학습하고 해당 모델을 배포하면, 운전자의 프라이버시를 보호하지 못할 가능성이 있다. 따라서 해당 문제를 해결하기 위해 노이즈 추가 또는 암호화 기술을 적용하여 프라이버시를 보호하려는 연구들이 진행되었다[11]. 하지만 노이즈 추가에 따른 모델의 성능 저하와 암호화에 따른 컴퓨팅 비용 증가라는 새로운 문제를 야기하는 한계가 있다[12].

이에 따라 본 연구에서는 데이터를 한군데 모으지 않고 직접적인 공유 없이 운전자 이상 행동 탐지 모델을 학습하기 위해 연합학습을 활용한 모델을 고안하였다. 연합학습은 분산된 환경에서 데이터를 직접 공유하지 않고, 각 로컬 클라이언트에서 개별적으로 학습된 딥러닝 모델의 파라미터만 교환해 모델을 훈련하는 방식이다. 중앙 서버와 클라이언트 간 파라미터 정보만 서로 교환되기 때문에 데이터가 한곳에 모이지 않아 정보의 유출을 효과적으로 방지할 수 있다는 장점이 있다[13].

이처럼 연합학습이 데이터 프라이버시 보호에 특화된 강점을 가짐에도, 이를 모빌리티 분야 데이터 분석에 단순히 적용하기에는 도메인 특성에서 기반하는 어려움이 있다. 대부분의 딥러닝 기반 중앙집중형 운전자 이상 행동 탐지 연구들은 전체적인 모델 성능 향상에는 기여할 수 있으나, 개별 차량의 고유성 및 상황별 특성 등을 반영하지 못하는 문제점이 존재한다. 특히, 다중 기기(e.g., 차량) 환경에서 발생하는 데이터 분포의 비균형성 문제가 극심하다. 운전 환경, 도로 조건 등의 다양한 요인에 따라 수집되는 데이터의 샘플 수와 라벨 분포 형태의 변동성이 매우 크다는 한계를 가진다.

기존에도 연합 학습을 운전자 이상 행동 탐지에 적용한 시도가 없었던 것은 아니다. 예를 들어, 자동차 산업 내 데이터 사일로(cross-silo) 문제를 해결하기 위해 졸음 운전 탐지 모델에 연합학습을 적용한 연구나[14], 교통 분야에서 분산된 센서 데이터를 활용하는 프레임워크[15] 등이 보고된 바 있다. 그러나 이러한 연구 대부분은 데이터가 independent and identically distributed (IID)에 가깝다는 가정 하에 실험을 설계하거나, 일부 제한된 시나리오에서만 연합학습 기법의 가능성을 제시한 경우가 많다. 또한 극단적인 데이터 불균형이나 차량 단말(클라이언트) 간 분포 편차가 심한 non- independent and identically distributed (Non-IID) 환경에서 연합학습 모델이 어떤 성능 변화를 보이는지 체계적으로 분석한 사례는 상대적으로 드물다[16]. 본 연구는 이와 같은 제한점을 극복하고, 실제 모빌리티 환경에서 발생할 수 있는 다양한 분포 시나리오를 설계해 모델의

성능을 정량적으로 평가한다. 특히, MobileNet과 같은 경량화 CNN 모델을 활용해 프라이버시 보호와 현실적 적용 가능성을 함께 추구한 점이 기존 연구들과의 차별화 요소라 할 수 있다. 시나리오별 실험 결과를 통해, 분산된 환경에서의 데이터 편향이 모델 성능에 어떠한 영향을 미치는지 구체적으로 제시하고, 연합 학습이 중앙집중형 학습에 비해 어느 정도 성능을 유지하는지 검증함으로써 모빌리티 데이터 활용의 새로운 가능성을 제시하고자 한다.

따라서, 본 연구는 자동차 모빌리티 환경에서의 실질적인 활용 가능성을 높이기 위한 시나리오 기반 다중 기기 연합학습 모델을 설계하고 실증적 검증을 진행하고자 한다. 본 연구에서는 모빌리티 데이터의 차량별 고유한 특성을 반영하면서도 개인정보 보호와 학습 성능 간의 균형을 유지할 수 있는 맞춤형 연합학습 프레임워크를 제안한다. 이를 통해 연합학습의 실효성을 검증하는 것을 주요 목표로 삼고 있으며, 다양한 시나리오 환경을 설정 후 실험을 진행하여 제안 기법의 효과와 실용성을 체계적으로 평가하고자 한다. 본 연구는 연합학습의 잠재력을 극대화하고 모빌리티 데이터 활용에 새로운 가능성을 제시하는 데 기여할 것이다.

Ⅱ. 데이터

본 연구에서는 한국지능정보사회진흥원에서 운영하는 AI Hub 플랫폼에서 제공한 졸음 운전 예방을 위한 운전자 상태 정보 영상데이터를 활용하였다. 이 데이터는 운전자의 이상 행동(졸음, 부주의, 휴대폰 사용, 흡연 등)을 분류하기 위한 인공지능 모델 개발을 목적으로 한국교통안전공단, ㈜테스트웍스, ㈜이즈테크놀리지가 공동으로 구축한 것이다. 실제 도로 주행 상황에서 졸음 상태를 수집하기에는 안전상의 제약이 따르므로, 실험실 시뮬레이터 환경에서 운전자의 졸음 및 부주의 연기를 수행하여 약 125시간 분량의 동영상을 확보하였다. 이후 해당 영상을 분석하여 주요 순간을 추출하고, 이를 112,500장의 이미지로 가공하여 학습용 데이터셋을 구성하였다.

촬영 과정에서는 근적외선 카메라와 녹화 장비를 사용하여 운전자의 얼굴 표정, 시선, 눈 깜빡임 등 상태 변화를 정교하게 포착할 수 있도록 하였으며, 이 과정에서 250명의 개인 운전자가 참여하였다. 가공 단계에서는 동영상을 프레임 단위로 분할하고, 해당 프레임을 이미지 형태로 변환한 뒤, 운전자의 얼굴 영역을 비롯해 눈, 입, 담배, 휴대폰 등 중요한 객체를 bounding box로 표시하였다. 또, 눈, 코, 입과 같은 주요 얼굴 특징점을

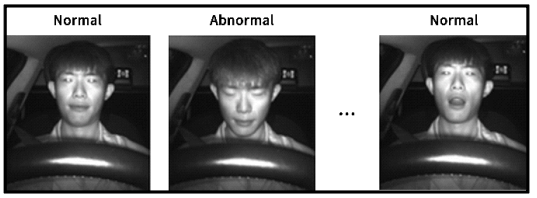


Fig. 1. Examples of driver anomalous behavior data in vehicle mobility. The left and right images indicate that the driver's eyes are open, representing a "Normal" state, meaning no drowsiness. The central image represents an "Abnormal" state, indicating that the driver is currently drowsy.

자동 추출하고, 전문가의 수동 검수를 거쳐 정확도를 높였다. 최종적으로 다단계 리뷰 과정을 통해 잘못된 라벨링이나 누락된 데이터가 없는지 검수함으로써 데이터 품질을 보장하였다.

데이터 내에서 가장 중요한 이상 행동은 졸음 운전이며, 본 연구에서는 운전자의 눈 감음 상태를 졸음으로 정의하여 분류를 진행하였다. 졸음 운전은 사고 발생과 피해 규모에 큰 영향을 미치기 때문에 본 연구의 주된 분석 대상이 되었으며, 실제로 데이터셋에서 졸음 상태(label 1)은 전체의 약 25%를 차지하고, 나머지 75%는 정상 상태(label 0)로 구성되어 있다. 본 연구에서 실제로 사용한 데이터셋은 위에 언급된 전체 데이터 중 243명의 운전자로부터 수집된 112,866장의 이미지로, 데이터상의 누락 등으로 인한 일부 데이터를 제외한 결과이다. 모든 이미지는 운전자의 얼굴과 그 표정, 눈, 입 등 특정 특징점이 명확히 보이도록 정제되었으며, 졸음 상태 여부를 판단하는 데 필요한 정보를 최대한 확보할 수 있도록 가공되었다. 분석에 사용된 데이터의 예시는 Figure 1에서 확인할 수 있다.

Ⅲ. 분석 방법

3.1 연합학습

연합학습(Federated Learning)은 데이터를 중앙 서버로 직접 공유하지 않고, 분산된 환경에서 각 로컬 클라이언트에서 개별적으로 학습된 모델의 파라미터만을 교환하여 모델을 훈련시키는 접근 방식이다. 이 과정에서 데이터는 로컬 환경에 그대로 보관되며, 서버와 클라이언트 간에는 오직 모델의 가중치 즉 weights 정보만 교환된다. 이러한 방식은 데이터가 한곳에 집중되지 않기 때문에 정보 유출 위험을 효과적으로 차단할 수 있다는 점에서 큰 장점을 제공한다.

연합학습은 크게 Cross-Silo Federated Learning과 Cross-Device Federated Learning 두 가지 주요 유형으

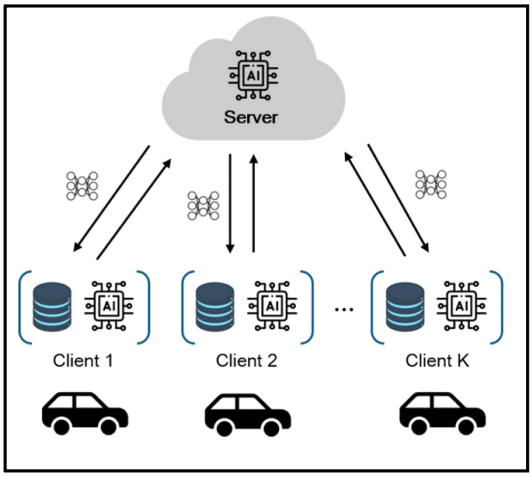


Fig. 2. Federated learning process with multiple devices in vehicle mobility. Each vehicle is treated as an individual device, and only the model parameters are exchanged with the central server for model updates.

로 구분된다. Cross-Silo Federated Learning은 조직 간 협력 또는 지리적으로 분산된 데이터 센터에서 주로 활용되며, 일반적으로 2~100개 클라이언트의 제한된 규모를 대상으로 한다. 반면에 Cross-Device Federated Learning은 수많은 IoT 디바이스를 클라이언트로 삼아 최대, 10^{10}개 이상의 클라이언트로 확장 가능하다. 이 유형은 주로 방대한 규모의 디바이스로부터 데이터가 분산된 상태로 유지되도록 설계되어 있다. 두 유형 모두 데이터가 로컬에서 생성되고 중상 서버는 학습 과정을 조율하지만, 원시 데이터는 공유되지 않으므로 개인 정보 보호 측면에서 강력한 보안을 제공한다.

본 연구에서는 차량을 개별 디바이스로 간주하여 Cross-Device Federated Learning을 기반으로 분석을 진행하였다. 이를 통해 각 차량에서 생성된 로컬 환경에 유지하면서도 모델 훈련을 효과적으로 수행하여, 개인 정보의 보호와 동시에 학습 효율성을 확보하였다 (Figure 2).

3.2 Federated Averaging

연합학습에는 다양한 학습 방법이 존재하지만, 본 연구에서는 연합학습의 대표적인 알고리즘인 Federated Averaging (FedAVG)[17] 방식을 적용하였다. FedAVG는 각 로컬 클라이언트에서 독립적으로 모델 파라미터를 업데이트한 후, 중앙 서버에서 이를 평균 내어 글로벌 모델을 최적화하는 방식으로 동작한다. 이러한 접근법은 분산 환경에서도 모델 학습의 일관성을 유지하면서 데이터 프라이버시를 보호할 수 있다는 장점을 가진다.

기존의 머신 러닝 또는 딥러닝 모델의 손실함수는 수식 (1)과 같이 정의된다.

$$\min_{\omega \in R^d} f(\omega) = \frac{1}{n}\sum_{i=1}^{n} f_i(\omega) \quad where\ f_i(\omega) = l(x_i, y_i; \omega) \tag{1}$$

반면, FedAVG는 각 클라이언트에서 계산된 로컬

손실 함수 값을 중앙 서버로 전송하여 이를 평균화함으로써 글로벌 손실 함수를 업데이트한다. 이 과정에서 FedAVG는 분산된 데이터를 기반으로 중앙 집중화된 학습 환경과 동일한 수준의 최적화를 달성하며 모델의 일관성과 성능을 유지한다. 이와 같은 FedAVG의 글로벌 손실함수는 수식 (2)로 나타낼 수 있다.

$$f(\omega) = \sum_{k=1}^{K} \frac{n_k}{n} F_k(\omega) \quad where\ F_k(\omega) = \frac{1}{n_k}\sum_{i \in P_k} f_i(\omega) \tag{2}$$

3.3 MobileNet

FedAVG는 각 클라이언트, 즉 본 연구에서는 각 디바이스에서 개별적으로 계산된 모델 파라미터를 집계하여 글로벌 모델의 파라미터를 업데이트 하는 방식으로 학습이 진행된다. 이 과정에서 사용할 모델은 연구 목적에 따라 별도로 정의해야 한다. 본 연구는 운전자 이상 행동 탐지를 목표로 하고 있으며, 라벨이 부착된 이미지 데이터를 분석하기 때문에 이미지 분류 모델을 각 클라이언트의 모델로 채택하였다.

특히 본 연구에서는 대표적인 CNN 모델 중 하나인 MobileNet[18]을 사용하였다. Cross-Device Federated Learning 환경에서는 각 디바이스에서 효율적인 학습이 필수적이며, MobileNet은 가볍고 계산 효율이 뛰어나 이러한 요구를 충족시킬 수 있는 적합한 모델로 판단되었다.

실제 구현 단계에서는 MobileNetv3 Large 모델의 사전 학습된 가중치를 활용하였으며, 전이 학습을 통해 운전자 이상 행동 감지에 적합하도록 최종 분류기 구성을 재설계하였다. 구체적으로는 원본 MobileNet의 특성 추출 부분은 그대로 유지하되, 최종에 위치한 분류기 단을 이진 분류 작업에 맞춰 1024차원의 완전 연결층 레이어, ReLU 활성화 함수, 0.4의 드롭아웃, 그리고 2개 클래스를 출력하는 Linear 레이어로 구성하였다.

모델 학습 과정에서는 AdamW 옵티마이저와 0.0001의 학습률, Cross Entropy Loss를 적용하였습니다. 이처럼 경량화 모델로서의 효율성과 이미지 분류

성능을 동시에 고려할 수 있는 MobileNetv3 Large를 적용함으로써, 실제 자동차 모빌리티 환경에 쉽게 배치할 수 있는 모델 구조를 지향하였다. 이러한 전이학습 기반 접근은 사전 학습된 풍부한 특성 정보를 최대한 활용하면서도, 이진 분류 태스크(이상 행동 vs. 정상 상태)에 맞춘 모델의 성능을 확보하는 데 큰 도움이 되었다.

3.4 시나리오 기반 다중 기기 모빌리티 연합학습 모델 프레임워크

본 연구에서 개발한 모델의 프레임워크의 전체적인 개요는 Figure 3과 같이 도식화될 수 있다. 본 연구는 각 차량을 독립적인 디바이스로 간주하며, 각 디바이스는 독립적으로 동작하는 분류기를 보유하고 있다. 이 분류기는 앞서 3.3절에서 언급한바와 같이 MobileNet으로 구성된다.

학습 프로세스는 각 디바이스 자체 데이터를 활용하여 독립적으로 분류기를 훈련하는 단계에서 시작된다. 이후 훈련된 모델의 파라미터만 글로벌 서버로 전송되며, 글로벌 서버는 수집된 파라미터를 평균화하여 갱신된 글로벌 모델의 파라미터를 생성한다. 이 갱신된 파라미터는 다시 각 디바이스로 전송되어 업데이트된다. 파라미터를 디바이스와 글로벌 서버간 1번 주고받는 과정을 통신 라운드가 1회 진행되었다고 정의한다.

통신 라운드가 완료될 때 마다, 각 디바이스는 글로벌 서버로부터 받은 갱신된 파라미터를 기반으로 자신의 데이터를 활용해 다시 학습을 수행한다. 이러한 반복적인 학습-전송-갱신 과정을 통해, 분산된 환경에서도 높은 성능의 글로벌 모델을 효율적으로 학습할 수 있다. 특히 이 과정에서 원시 데이터는 디바이스 내부에 유지되며, 중앙 서버로는 모델의 파라미터만 전송되기 때문에 개인 정보 보호와 데이터 프라이버시가 효과적으로 보장된다.

Ⅳ. 실험 시나리오 설계

본 연구에서는 차량별로 수집되는 데이터의 양과 운전자의 행동 습관이 서로 다르기 때문에 발생할 수 있는 각 차량 디바이스의 데이터의 분포가 서로 다른 특징을 고려하는 다양한 시나리오들을 구성하고자 하였다. 이는 특히, 모빌리티 환경에서의 연합학습에서 각 클라이언트 또는 기기마다 데이터의 분포가 달라지는 Non-IID 이슈를 함께 고려하는 실험 설계이다. 본 연구에서는 Non-IID 원인 종류 중, 클라이언트별 데이터 개수가 크게 차이나는 수량 왜곡(Quantity Skew) 문제를 다양하게 고려할 수 있는 다음의 7가지 연합학습용 차량 운전자 데이터 수집 시나리오를 구성 후 다중 기기 연합학습 실험을 진행하고자 한다. 특히, 데이터 비대칭 시나리오들의 경우, 클라이언트 간 데이터 불균형과 극단적 분포 상황을 시뮬레이션하기 위해 설계되었다.

- *Experiment Scenario 1.* 원본 데이터 활용 시나리오
- *Experiment Scenario 2.* 균등 분포 유사 시나리오: 데이터를 모든 클라이언트에 균등하게 분포한 시나리오
- *Experiment Scenario 3.* 클라이언트별 데이터 샘플

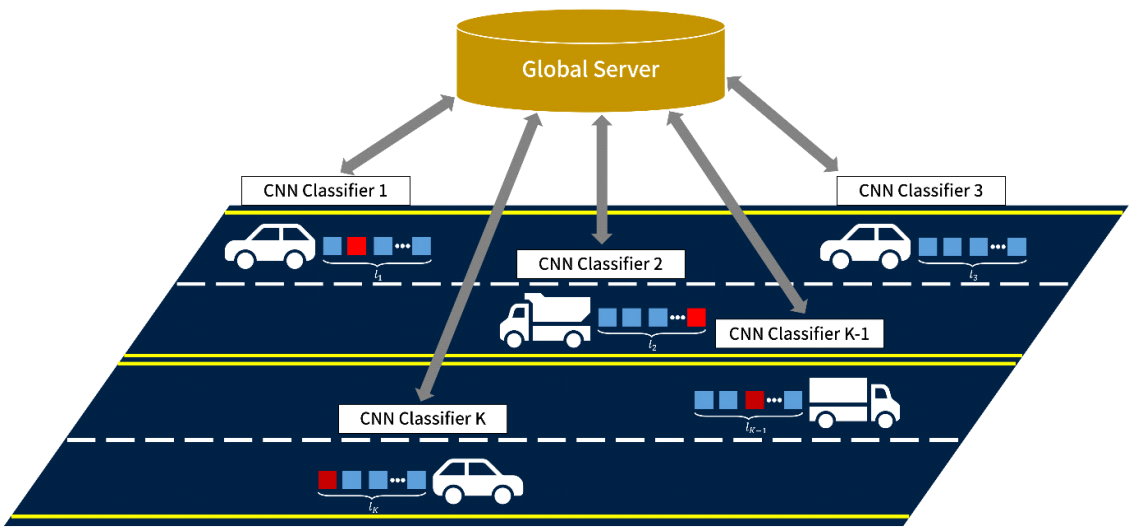


Fig. 3. Proposed framework based on cross-device federated learning

수 분포를 정규분포화: 중심 극한 정리를 기반으로 표본 평균의 분포가 정규 분포에 가까워진다는 가정 하에 설계

- *Experiment Scenario 4.* 클라이언트별 데이터 샘플 수 분포를 정규분포화 (small variance 가정)
- *Experiment Scenario 5.* Left skewness 데이터 비대칭 시나리오: 데이터 샘플 수가 적은 클라이언트가 많은 경우
- *Experiment Scenario 6.* Right Skewness 데이터 비대칭 시나리오: 데이터 샘플 수가 많은 클라이언트가 많은 경우
- *Experiment Scenario 7.* 데이터 양극화 비대칭 시나리오: 데이터 샘플 수가 많은 클라이언트와 적은 클라이언트가 다수, 그 외는 정규분포 가정

각 시나리오별 실험 설계 구성의 특징 요약은 Table 1에 나타나 있다.

Table 1을 살펴보면, Scenario 1과 2는 특징, 레이블, 개수 측면에서 분포가 고르게 유지되도록 설계했기 때문에 IID, Scenario 3, 4는 클라이언트별 샘플 수 차이 분포를 정규 분포로 고려하여 부분적으로 Non-IID 성격을 가진다. Scenario 5, 6, 7은 강한 수량 왜곡을 가지는 Non-IID 상황으로 간주한다. Scenario 5, 6에서는 데이터의 양이 한쪽으로 치우는 왜곡(Skewness)가 존재하여 수량 왜곡을 고려하였으며, Scenario 7의 경우 실제 모빌리티 환경에서 운전을 많이 하는 운전자들과 운전을 거의 하지 않는 운전자 들이 존재하며, 나머지 운전자들은 중심 극한 정리에 의하여 정규분포에 가까워 질것이라는 가정을 반영하여 시나리오를 설계하였다. Figure 4에서는 7가지 시나리오의 실제 데이터 분포 형태를 시각적으로 확인할 수 있다.

Table 1. Experimental description by each scenario

Experiment Scenario	Quantity Skew	IID / Non-IID
1	No	IID
2	No	IID
3	Yes	Partial Non-IID
4	Yes	Partial Non-IID
5	Yes	Non-IID
6	Yes	Non-IID
7	Yes	Non-IID

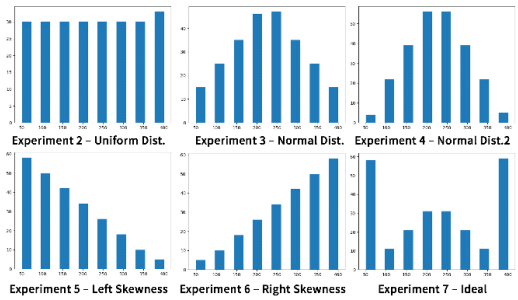


Fig. 4. Histogram of data distribution across seven experiment scenarios. The x-axis represents the number of datasets held by each client, while the y-axis indicates the number of clients with a given number of datasets.

V. 실험 결과

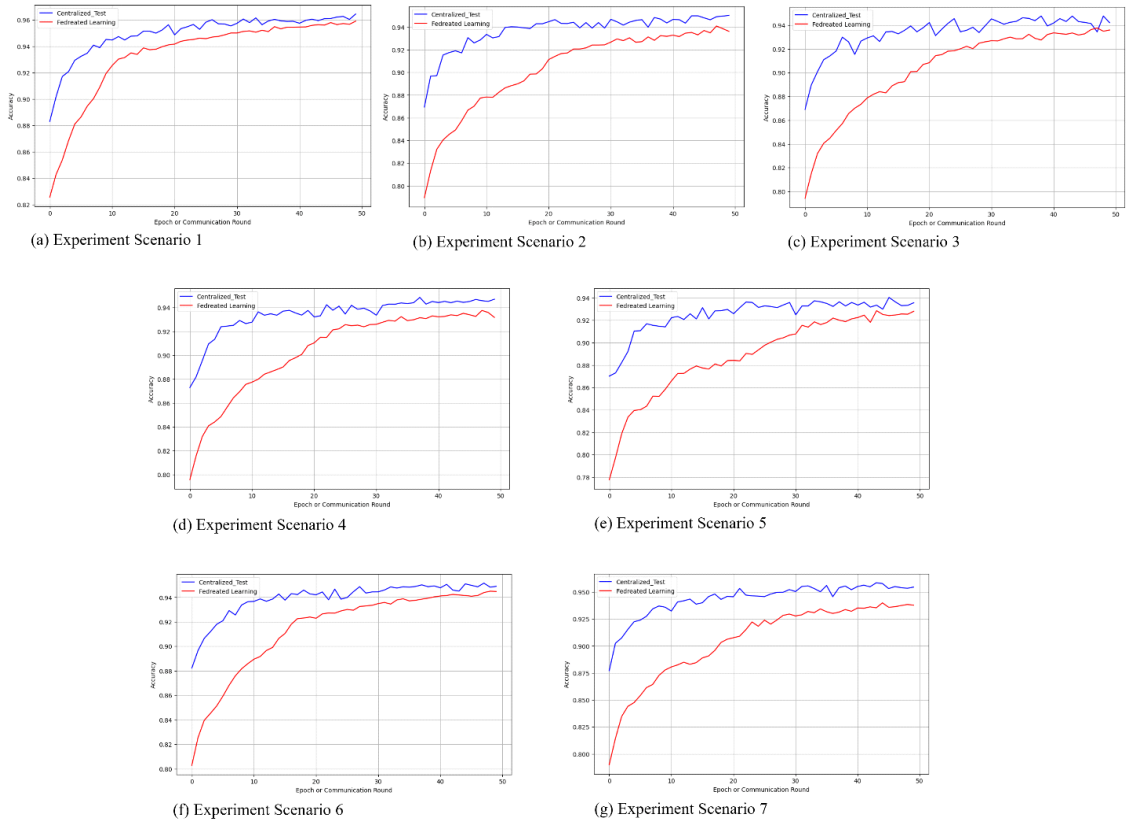
본 연구에서는 기 구성한 7가지 실험 시나리오에 대해 운전자 이상 행동 탐지 모델 학습을 수행하였다. 모든 실험에서는 Centralized 모델과 FedAVG 모델을 비교 대상으로 설정했으며, 모델 성능 평가는 정확도와 F1-Score를 측정 후 비교하였다. 각 실험에서 동일한 비교 조건을 유지하기 위해, Centralized 모델은 총 50회의 에포크를 FedAVG모델은 총 50회의 통신 라운드를 수행하도록 설정하였다. 두 모델 간의 성능 차이가 작을수록, FedAVG의 성능이 Centralized 모델에 비해 성능이 많이 떨어지지 않는다는 것을 의미하며, 제안한 모델이 프라이버시를 효과적으로 보호하면서도 우수한 성능을 제공한다는 점을 입증할 수 있다. 본 연구에서 수행한 모든 실험은 동일한 하드웨어 및 소프트웨어 환경에서 진행되었다. 하드웨어는 Intel Core i9-14900K CPU, GIGABYTE RTX 4090 GPU(24GB) × 2, 128GB DDR5 메모리, 2TB SSD, 12TB HDD 등을 사용하였다. 모델 학습은 Python 3.10.14와 PyTorch 2.5.1(CUDA 12.4 지원)를 이용하여 진행하였다. 또한, 실험 재현성을 보장하기 위해 base 모델에 해당하는 MobileNet의 학습률, 에포크, 옵티마이저 설정을 고정시켜 모든 실험에서 일관되게 적용하였다. 실험 결과는 Table 2에 정리되어 있다.

실험 결과, FedAVG는 Centralized 모델에 비해 정확도는 평균 1.01%p, F1 점수는 0.96%p 낮은 극소량의 성능 차이를 보였다. 이러한 결과는 FedAVG 모델이 프라이버시를 효과적으로 보호하는 동시에, Centralized 모델에 근접한 성능을 유지할 수 있음을 입증한다.

추가적으로, 각 실험에서 Centralized 모델과 FedAVG 모델의 성능을 Epoch 및 통신 라운드 변화에

Table 2. Performance evaluation results by scenario

Experiment Scenario	Accuracy			F1-Score		
	Centralized	FedAVG	△(Centralized - FedAVG)	Centralized	FedAVG	△(Centralized - FedAVG)
1	0.9660	0.9591	**-0.0069**	0.9659	0.9590	**-0.0069**
2	0.9508	0.9362	**-0.0146**	0.9505	0.9360	**-0.0145**
3	0.9421	0.9359	**-0.0062**	0.9422	0.9354	**-0.0068**
4	0.9469	0.9317	**-0.0152**	0.9466	0.9306	**-0.0160**
5	0.9357	0.9281	**-0.0076**	0.9356	0.9272	**-0.0084**
6	0.9490	0.9448	**-0.0042**	0.9488	0.9444	**-0.0044**
7	0.9545	0.9378	**-0.0167**	0.9543	0.9378	**-0.0165**



(a) Experiment Scenario 1 (b) Experiment Scenario 2 (c) Experiment Scenario 3

(d) Experiment Scenario 4 (e) Experiment Scenario 5

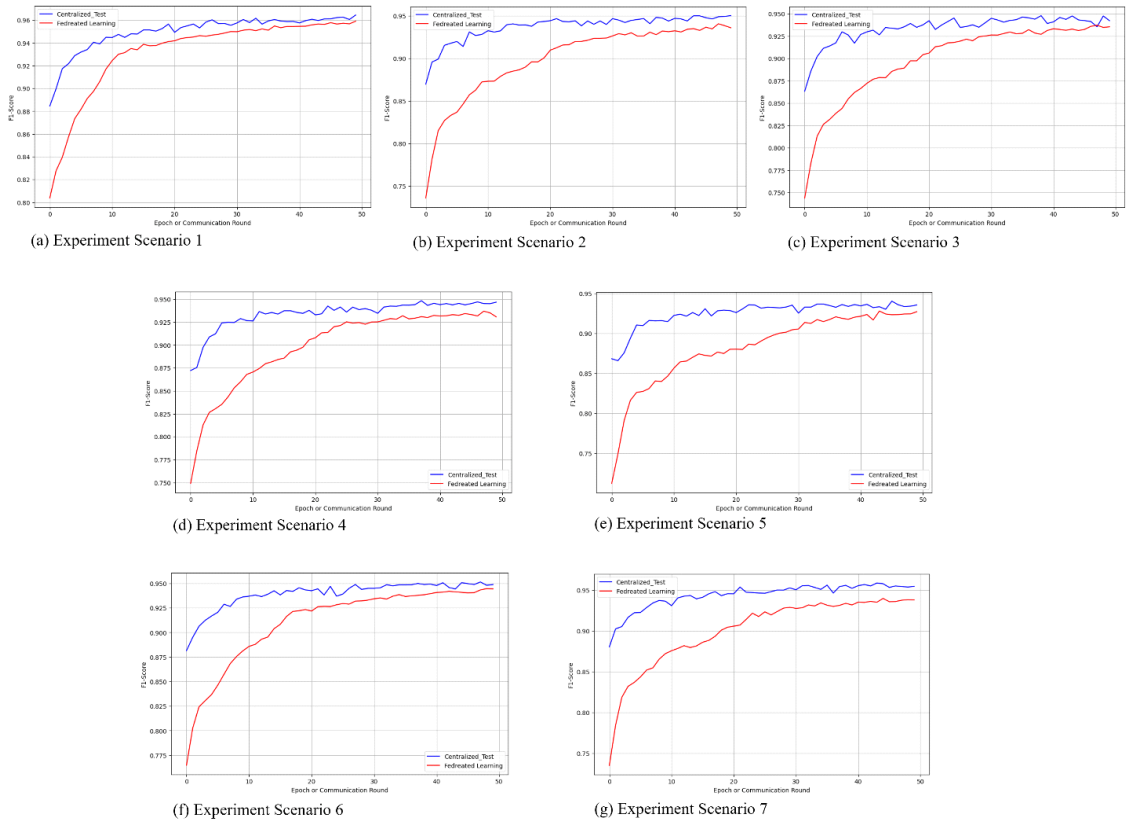
(f) Experiment Scenario 6 (g) Experiment Scenario 7

Fig. 5. Comparison of accuracy changes across communication rounds by scenario. The blue line represents the accuracy changes of the centralized model, while the red line represents those of FedAVG.

따라 비교하여 Figure 5와 6에 나타내었다. 각 그래프에서 X축은 Centralized 모델의 Epoch 수와 동시에 FedAVG 모델의 통신 라운드를 나타낸다. Figure 5와 6을 통해, 통신 라운드가 진행됨에 따라 FedAVG 모델의 성능이 점진적으로 Centralized 모델의 성능에 근접하고, 두 모델 간의 성능 격차가 줄어드는 경향을 보인다. 이는 연합학습 환경에서도 지속적인 통신과 학습을 통해 중앙집중식 학습에 가까운 성능을 달성할 수 있음을 시사하며, 실제 다양한 실험 시나리오 세팅에서 실증 접목이 가능하다고 판단할 수 있다.

Ⅵ. 결 론

본 연구는 모빌리티 데이터의 특성과 요구를 반영한 연합학습 환경을 설계하여, 분산된 데이터 환경에서도 고성능의 글로벌 모델 학습이 가능함을 입증하였다. 특



(a) Experiment Scenario 1 (b) Experiment Scenario 2 (c) Experiment Scenario 3

(d) Experiment Scenario 4 (e) Experiment Scenario 5

(f) Experiment Scenario 6 (g) Experiment Scenario 7

Fig. 6. Comparison of F1-score changes across communication rounds by scenario. The blue line represents the F1-score changes of the centralized model, while the red line represents those of FedAVG.

히, Cross-Device Federated Learning의 프레임워크를 기반으로 데이터를 중앙 서버로 직접 전송하지 않고 클라이언트 로컬에 안전하게 유지하면서도 Centralized 모델과 유사한 수준의 학습 성능을 달성하였다. 이러한 결과는 데이터 프라이버시를 보호하면서도 고성능 학습을 가능하게 하는 연합학습의 모빌리티 분야 특화 실용적 가능성을 보여준다.

제안된 프레임워크는 각 차량을 독립적인 디바이스로 간주함으로써 자동차 모빌리티 환경의 고유한 특성을 충실히 반영하였다. 클라이언트 간 데이터 크기 편향을 고려한 학습 프로세스를 구축하였으며, MobileNet과 같은 경량 모델을 활용하여 계산 효율성을 극대화하였다. 이를 통해, 중앙 데이터 수집 없이도 개별 디바이스의 데이터를 활용하여 실시간 이상 행동 탐지와 같은 응용 사례에 적합한 솔루션을 제시하였다.

본 연구는 다음 두 가지 측면에서 중요한 기여를 한다. 첫째, 데이터를 클라이언트 로컬에 보존하면서 글로벌 학습을 수행할 수 있는 Cross-Device Federated Learning의 효과를 입증함으로써, 데이터 프라이버시 규제를 충족할 수 있는 실질적 접근법을 제시하였다. 이를 통해, 스마트 모빌리티 플랫폼과 같은 민감한 데이터 환경에서도 안전하고 효과적으로 AI 기술을 도입할 수 있는 가능성을 열었다. 둘째, 다양한 시나리오 실험 설정을 통해 자동차 모빌리티 환경에서 데이터의 실제 특성을 반영한 연합학습 성능을 검증함으로써, 프레임워크의 실용성과 신뢰성을 동시에 확보하였다.

특히, Cross-Device Federated Learning의 강점은 대규모 디바이스 환경에서도 데이터 프라이버시를 보호하며, 클라이언트 간 데이터의 비균일성과 분산 특성을 효과적으로 처리할 수 있다는 점이다. 본 연구는 이러한 Cross-Device Federated Learning의 장점을 모빌리티 데이터에 구체적으로 적용함으로써, 차량 관리, 운전자 모니터링, 졸음 운전 탐지와 같은 스마트 모빌리티 플랫폼의 다양한 응용 사례에 활용할 수 있는 가능성을 확인하였다.

결론적으로, 본 연구는 데이터 프라이버시와 고성능 학습이라는 두 가지 상충되는 요구를 균형 있게 충족시키는 연합학습의 잠재력을 재조명하였다. 이를 통해,

Cross-Device Federated Learning이 스마트 모빌리티 뿐만 아니라 대규모 IoT 환경에서도 효과적으로 활용될 수 있는 기반을 마련하였으며, 향후 개인정보 보호와 기술 발전을 동시에 달성할 수 있는 연구 방향을 제시하였다.

Ⅶ. 한계점 및 향후 연구 방향

본 연구는 연합학습의 효율성과 잠재력을 입증했지만, 몇 가지 한계점을 안고 있다. 먼저, 연합학습 환경에서 발생할 수 있는 다른 종류의 Non-IID 상황을 충분히 반영하지 못했다는 점이다. 본 연구에서 고려한 수량 왜곡으로 인한 데이터 분포 불균형 이외에도 Non-IID는 다음의 세가지 원인들을 추가적으로 고려할 필요가 있다[19]. 특정 클라이언트에 특정 속성값이 편향되어 나타나는 특정 분포 왜곡(Feature Distribution Skew), 일부 클라이언트에 특정 클래스 레이블이 과도하게 몰리는 레이블 편향, 간과 경과나 환경 차이로 인해 데이터 분포가 달라지는 개념 변화(Concept Drift) 등 또한 모빌리티 환경에서 도전적인 Non-IID 이슈이다. 하지만 본 연구에서는 다양한 실질적인 조건에서의 모델 성능을 완전히 입증하지 못한 한계가 있다. 또한, FedAVG는 단순하고 효과적인 알고리즘으로 널리 사용되지만, 복잡한 데이터 환경에서 클라이언트 간의 데이터 다양성과 편향 문제를 완벽히 해결하지는 못한다. FedAVG는 클라이언트별 모델 업데이트를 단순 평균화하여 글로벌 모델을 학습하기 때문에, 데이터 불균형이 심한 상황에서는 추가적인 성능 개선이 필요하다. 특히, 다중 기기 환경과 같은 대규모 클라이언트 환경에서는 이러한 한계가 더욱 두드러질 가능성이 있다.

향후 연구에서는 이러한 한계점을 보완하기 위해 추가적인 Non-IID 데이터 분포를 고려한 새로운 연합학습 설정을 설계하고, 다양한 환경에서 성능 검증을 진행할 계획이다. 클라이언트 간 데이터 레이블 편향이 심한 환경에서도 안정적으로 작동할 수 있는 모델 학습 방식을 개발함으로써, 더욱 현실적인 조건에서 연합학습의 적용 가능성을 확장하고자 한다. 특히, 모빌리티 데이터의 특성을 반영한 시나리오를 다수 설계하여, 실제 응용 가능성을 검증하는 데 주력할 예정이다. 아울러, 연합학습의 통신 효율성을 향상시키는 방법도 탐구할 계획이다. 대규모 클라이언트 환경에서는 통신 비용이 학습의 주요 제약으로 작용하므로, 통신 라운드 수를 줄이거나 모델 업데이트를 최적화하는 기술이 필수적이다. 이를 위해, 양자화와 희소화와 같은 기술을 연합학습에 접목하여 통신 비용을 최소화하면서도 높은 성능을 유지하는 방법을 모색할 것이다. 본 연구는 연합학습이 모빌리티 환경에서 효과적인 솔루션이 될 수 있음을 보여주었으며, 향후 연구를 통해 이를 더욱 정교하고 실용적으로 발전시켜 스마트 모빌리티 플랫폼의 안전성과 효율성을 크게 향상시키는 데 기여하고자 한다. 데이터 프라이버시와 성능 간의 균형을 유지하며, 연합학습의 잠재력을 극대화할 수 있는 기반을 마련하는 데 초점을 맞출 것이다.

References

[1] M. H. Alkinani, W. Z. Khan, and Q. Arshad, “Detecting human driver inattentive and aggressive driving behavior using deep learning: recent advances, requirements, and open challenges,” *IEEE Access*, vol. 8, pp. 105008-105028, Aug. 2020. (https://doi.org/10.1109/ACCESS.2020.2999829)

[2] L. Jiang, W. Xie, D. Zhang, and T. Gu, “Smart diagnosis: Deep learning boosted driver inattention detection and abnormal driving prediction,” *IEEE Internet of Things J.*, vol. 9, no. 6, pp. 4076-4088, Mar. 2022. (https://doi.org/10.1109/JIOT.2021.3103852)

[3] W. Huang, X. Liu, M. Luo, P. Zhang, W. Wang, and J. Wang, “Video-based abnormal driving behavior detection via deep learning fusions,” *IEEE Access*, vol. 7, pp. 64571-64582, Jun. 2019. (https://doi.org/10.1109/ACCESS.2019.2917213)

[4] M. Shahverdy, M. Fathy, R. Berangi, and M. Sabokrou, “Driver behavior detection and classification using deep convolutional neural networks,” *Expert Syst. with Appl.*, vol. 149, art. no. 113240, Feb. 2020. (https://doi.org/10.1016/j.eswa.2020.113240)

[5] J. Hu, X. Zhang, and S. Maybank, “Abnormal driving detection with normalized driving behavior data: A deep learning approach,” *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 6943-6954, Jul. 2020. (https://doi.org/10.1109/TVT.2020.2993247)

[6] M. Hou, M. Wang, W. Zhao, Q. Ni, Z. Cai, and X. Kong, “A lightweight framework for abnormal driving behavior detection,”

Computer Commun., Sep. 2021.
(https://doi.org/10.1016/j.comcom.2021.12.007)

[7] S. Yong, J. Chang, S. Jo, S. Park, J. Kim, and S. Kim, "Development of driver abnormal behavior detection system using contrastive learning," in *Proc. 2022 Korean Institute of Inf. Technol. Conf.*, pp. 480-481, Dec. 2022.

[8] H. A. Abosaq, M. Ramzan, F. Althobiani, A. Abid, K. M. Aamir, H. Abdushkour, M. Irfan, M. E. Gommosani, S. M. Ghonaim, V. R. Shamji, and S. Rahman, "Unusual driver behavior detection in videos using deep learning models," *Sensors*, vol. 23, art. no. 311, Jan. 2023.
(https://doi.org/10.3390/s23010311)

[9] Y. Fan, F. Gu, J. Wang, J. Wang, K. Lu, and J. Niu, "SafeDriving: An effective abnormal driving behavior detection system based on EMG signals," *IEEE Internet of Things J.*, vol. 9, no. 14, pp. 12338–12349, Jul. 2022.
(https://doi.org/10.1109/JIOT.2021.3135512)

[10] L. Zhu, Z. Liu, and S. Han, "Deep leakage from gradients," in *Proc. 33rd Conf. Neural Inf. Process. Syst. (NeurIPS 2019)*, Dec. 2019.
(https://doi.org/10.48550/arXiv.1906.08935)

[11] H. Bae, J. Jang, D. Jung, H. Jang, H. Ha, H. Lee, and S. Yoon, "Security and privacy issues in deep learning," *IEEE Trans. Artificial Intell.*, Jun. 2020.
(https://doi.org/10.48550/arXiv.1807.11655)

[12] F. Mireshghallah, M. Taram, P. Ramrakhyani, A. Jalali, D. Tullsen, and H. Esmaeilzadeh, "Shredder: Learning noise distributions to protect inference privacy," in *Proc. 25th Int. Conf. Architectural Support for Programming Languages and Operating Syst. (ASPLOS '20)*, Lausanne, Switzerland, Mar. 2020.
(https://doi.org/10.1145/3373376.3378522)

[13] P. Kairouz et al., "Advances and open problems in federated learning," *arXiv preprint* arXiv:1912.04977, Dec. 2021.
(https://doi.org/10.48550/arXiv.1912.04977)

[14] W. Lindskog, V. Spannagl, and C. Prehofer, "Federated learning for drowsiness detection in connected vehicles," *arXiv preprint* arXiv:2405.03311, May 2024.
(https://doi.org/10.48550/arXiv.2405.03311)

[15] X. Huang, T. Huang, S. Gu, S. Zhao, and G. Zhang, "Responsible federated learning in smart transportation: outlooks and challenges," *arXiv preprint* arXiv:2404.06777, Apr. 2024.
(https://doi.org/10.48550/arXiv.2404.06777)

[16] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE Signal Process. Mag.*, vol. 37, no. 3, pp. 50-60, May 2020.
(https://doi.org/10.1109/MSP.2020.2975749)

[17] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. Agüera y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proc. 20th Int. Conf. Artificial Intell. and Statistics (AISTATS 2017)*, Fort Lauderdale, FL, USA, Apr. 2017.
(https://doi.org/10.48550/arXiv.1602.05629)

[18] A. G. Howard, M. Zhu, B. Chen, D. Kalenichenko, W. Wang, T. Weyand, M. Andreetto, and H. Adam, "MobileNets: Efficient convolutional neural networks for mobile vision applications," *arXiv preprint* arXiv:1704.04861, Apr. 2017.
(https://doi.org/10.48550/arXiv.1704.04861)

[19] M. F. Criado, F. E. Casado, R. Iglesias, C. V. Regueiro, and S. Barro, "Non-IID data and continual learning processes in federated learning: a long road ahead," *Inf. Fusion*, vol. 88, pp. 263-280, Jan. 2022.
(https://doi.org/10.1016/j.inffus.2022.07.024)

권 병 근 (Byeongkeun Kwon)

2024년 2월 : 부산대학교 수학과 졸업
2024년 3월~현재 : 경북대학교 데이터사이언스대학원 석사과정
<관심분야> 인공 지능 응용, 프라이버시 보호, 연합학습
[ORCID:0009-0009-1632-4249]

김 수 현 (Suhyeon Kim)

2018년 2월 : 부산대학교 대기환경과학과/통계학과 이학사
2020년 2월 : 울산과학기술원 융합경영대학원 비즈니스분석 이학석사
2023년 2월 : 울산과학기술원 산업공학과 공학박사
2023년~현재 : 경북대학교 데이터사이언스대학원 교수
<관심분야> 데이터 마이닝, 인공지능 응용, 모빌리티 데이터 분석, 연합학습
[ORCID:0000-0001-6475-2461]