# 블록체인 기반의 실시간 모니터링을 통한 SplitNN 트레이닝 신뢰성 강화기법 연구

윤여국, 조연정, 심채린, 이명준, 윤태현

{durnffl, jeong7323, chaelin0520}@gmail.com, mjlee@cicweb.ulsan.ac.kr, thyoon0820@etri.re.kr

# Enhancing Training Reliability of SplitNN through Blockchain-Based Real-Time Monitoring

Yoon Yeo Guk, Jo Yeon Jeong, Sim Chae Lin, Lee Myung Joon, Yoon Tae Hyun

요 약

스플릿 뉴럴 네트워크(SplitNN) 기법은 데이터를 노출하지 않고 딥러닝 모델을 훈련할 수 있는 중요한 기술로, 제조업, 금융업 등 데이터 보안이 중요한 분야에서 널리 주목받고 있다. 기존의 스플릿 러닝 방식은 데이터 소유자가 원본 데이터를 보호할 수 있는 장점을 제공하지만, 트레이닝 과정의 투명성과 신뢰성을 실시간으로 확인할 수 없는 한계가 있었다.

본 연구는 기존의 Train4U 시스템을 확장하여, SplitNN 트레이닝 과정에서 실시간 모니터링 및 데이터 무결성 검증을 제공하는 블록체인 기반 모니터링 기법을 제안한다. 확장된 Train4U는 트레이닝의 세부 과정에 대한 웹 기반의 모니터링 도구를 제공하여 사용자 신뢰성을 제고한다. 모니터링 도구는 트레이닝 단계별 과정에 대한 블록체인 상의 위/변조가 불가능한 정보를 데이터 소유자와 AI 서비스사에게 동일하게 시각화하여 제공한다. 이를 통해 데이터 소유자와 AI 서비스사는 트레이닝 과정이 올바르게 수행되고 있는지, 결과 데이터의 무결성이 유지되고 있는지를 동시에 확인할 수 있다. 확장된 Train4U는 데이터 유출에 대한 우려 없이 민감한 데이터를 다루는 산업 분야에 AI 기술을 안전하게 도입할 수 있는 환경을 제공한다.

## Ⅰ. 서론

AI 기술의 빠른 발전 및 적용 분야 다각화로 인하여, 여러 산업 분야에서 AI를 활용한 혁신이 활발히 이루어지고 있다. 특히, 제조업과 금융업과 같은 민감한 데이터를 다루는 분야에서는 AI 기술을 도입하는 과정에서 데이터 보안에 대한 우려가 중요하게 대두되고 있다.[1] 일반적으로 AI 기술을 도입하려면 대규모의 데이터를 확보해야 하지만, 데이터 제공자는 원본 데이터를 외부에 공개하지 않기를 원하며, 이러한 요구사항은 AI 서비스 제공자와의 충돌을 일으킨다. 따라서, 데이터 제공자의 기밀성을 유지하면서도 AI 트레이닝을 원활하게 진행할 수 있는 방법이 절실히 필요하다.[2]

스플릿 뉴럴 네트워크(SplitNN)[3] 기법은 이러한 문제를 해결하기 위한 중요한 기술로 주목받고 있다. SplitNN은 데이터를 노출하지 않고도 트레이닝을 진행할 수 있으며, 데이터 제공자와 AI 서비스사가 물리적으로 분리된 환경에서 각각의 모델을 학습할 수 있도록 지원한다. 그러나 SplitNN 기법에도 한계가 존재한다. 분산된 환경에서 데이터가 외부 노드와 통신되는 과정에서, 해당 데이터가 악의적으로 접근되거나 변조될 가능성을 배제할 수 없으며, 트레이닝 과정에서 데이터 무결성을 실시간으로 확인할 수 있는 방법이 부족하다. 또한, 데이터 제공자와 AI 서비스 기업 간의 직접적인 통신이 이루어질 경우 데이터 소유자가 원본 데이터를 독점적으로 관리하는 장점이 희석될 수 있다.

이를 해결하기 위해 본 연구에서는 기존의 Train4U[4] 시스템을 확장하여, SplitNN 기법의 트레이닝 과정에 대한 신뢰성, 투명성, 보안성을 보완하는 블록체인 기반의 실시간 모니터링 기법을 제시한다. 확장된 Train4U 시스템은 데이터 제공자와 AI 서비스사가 직접적으로 데이터를 주고받지 않고, 블록체인 트랜잭션 및 이벤트를 통해 데이터를 교환하며, 실시간으로 트레이닝 과정의 정확도와 무결성을 모니터링할 수 있는 환경을 제공한다.

## Ⅱ. 본론

SplitNN(스플릿 뉴럴 네트워크)은 데이터 제공자와 AI 서비스사가 서로 다른 환경에서 딥러닝 모델을 학습할 수 있도록 지원하는 기법이다. 이 기법은 데이터를 노출하지 않고도 트레이닝을 진행할 수 있는 장점을 가지고 있지만, 트레이닝 과정의 투명성과 신뢰성을 실시간으로 확인할 수 있는 방법이 부족하다는 문제를 안고 있다. 이러한 한계를 해결하기 위해, 본 논문에서는 블록체인 기반의 실시간 모니터링 기법을 활용하여 확장한 Train4U 시스템을 제안한다.

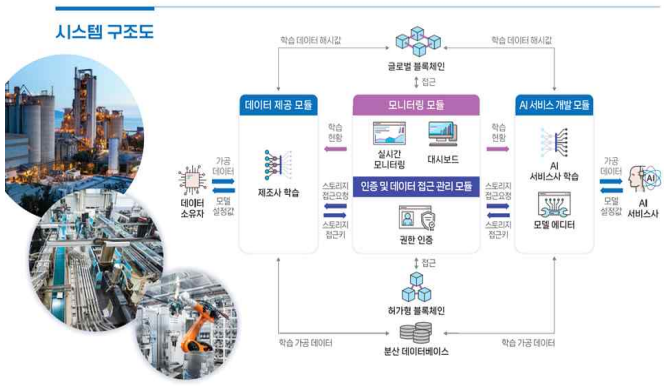


그림 1. Train4U 시스템 구조도

SplitNN 기법의 신뢰성, 투명성, 보안성 한계를 해결하기 위하여 Train4U는 퍼블릭 블록체인인 Klaytn과[5] 프라이빗 블록체인인

Hyperledger Fabric을[6] 함께 사용한다. SplitNN 구동의 두 주체인 데이터 소유자와 AI 서비스사가 딥러닝 과정에 참여하고, 순차적인 과정에 맞게 접근하기 위한 key 값 관리에는 프라이빗 블록체인이 사용되며, 실제로 딥러닝이 수행되고 있음에 대한 검증을 위한 값(intermediate, target, gradient 등에 대한 해시값)을 투명하고 신뢰성있게 확인하기 위하여 퍼블릭 블록체인을 사용한다. 검증을 위하여 퍼블릭 블록체인에 저장되는 값들은 데이터 소유자와 AI 서비스사가 SplitNN 구동 과정에서 동일한 트레이닝 중간값을 주고받으며 딥러닝이 수행되었음을 확인하기 위하여 필수적으로 교차 검증이 되어야 하는 값이다. 트레이닝 전 과정에서 해당 검증을 위한 값들을 양측에서 실시간으로 모니터링하는것은 Train4U의 신뢰성 보장을 위하여 필수적이다.

확장된 Train4U 시스템은 트레이닝 과정에서 발생하는 데이터에 대한 해시값을 퍼블릭 블록체인에 저장하고, 이를 Train4U 구동 주체인 데이터 소유자와 AI 서비스사가 실시간으로 모니터링할 수 있는 기능을 제공한다. 이를 통해 트레이닝 과정 중 데이터 변조 여부를 실시간으로 감지할 수 있다. 데이터 소유자와 AI 서비스사는 직접적인 통신을 하지 않고 각각의 데이터 해시값을 퍼블릭 블록체인에 저장하는 트랜잭션 처리 시 블록체인 이벤트를 발생하고 이를 수집하는 방식으로, 별도의 p2p 연결 없이 실시간으로 해당 데이터를 모니터링한다.

또한 Train4U 시스템은 딥러닝 트레이닝 과정에서 발생하는 트레이닝 데이터 외에도, 각 에포크, 배치별 정확도와 같이 트레이닝 상태를 직관적으로 확인할 수 있는 값에 대한 모니터링도 함께 제공한다. 데이터 소유자와 AI 서비스사는 이러한 데이터를 기반으로 트레이닝 진행 상태를 확인할 수 있다. 특히, 각 에포크별로 트레이닝 성능(정확도)을 막대 그래프 형태로 시각화하여 제공하며, 트레이닝 진행도와 현재 정확도를 원형 그래프 형태로 보여줌으로써 직관적으로 트레이닝 성과를 파악할 수 있도록 지원한다. 이를 통해 데이터 소유자와 AI 서비스사는 트레이닝이 예상대로 진행되고 있는지, 결과 데이터의 무결성이 유지되고 있는지를 실시간으로 확인할 수 있다.

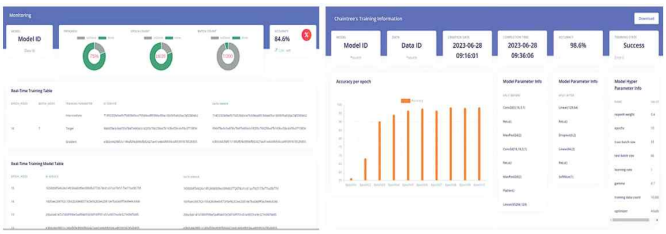


그림 2 Train4U 실시간 모니터링 화면

## Ⅲ. 결론

본 연구에서는 기존의 Train4U 시스템을 확장하여, SplitNN 트레이닝 과정에서 실시간 모니터링 및 데이터 무결성 검증을 제공하는 블록체인 기반 모니터링 기법을 제안하였다. 기존의 SplitNN 기법이 데이터를 노출하지 않고 딥러닝 트레이닝을 가능하게 했음에도 불구하고, 트레이닝 과정과 데이터 무결성을 실시간으로 확인하기 어려웠던 문제를 해결하고자 블록체인 기반 모니터링 기법을 도입하였다.

확장된 Train4U 시스템은 퍼블릭 블록체인과 프라이빗 블록체인을 함께 사용하여 트레이닝 과정에서 발생하는 데이터와 권한을 안전하게 관리하며, 데이터 소유자와 AI 서비스사가 직접 통신하지 않고도 블록체인을 통해 데이터를 교환할 수 있도록 구성되었다. 이를 통해 데이터 소유자는 원본 데이터를 독점적으로 유지하면서도, 트레이닝 과정의 신뢰성과 무결성을 실시간으로 검증할 수 있다.

또한, 확장된 Train4U 시스템은 트레이닝 과정에서 발생하는 데이터를 각 요소별 필요에 맞게 그래프 형태로 시각화하여, 트레이닝 성능과 진행 상태를 직관적으로 모니터링할 수 있는 기능을 제공한다. 이를 통해 데이터 소유자와 AI 서비스사는 트레이닝이 예상대로 진행되고 있는지, 그리고 데이터 무결성이 유지되고 있는지를 실시간으로 확인할 수 있다.

이러한 Train4U 시스템은 민감한 데이터를 다루는 제조업, 금융업 등에서 AI 도입을 주저했던 문제를 해결할 수 있는 중요한 방법을 제공하며, AI 기술의 산업 전반적인 확산을 촉진하는 데 기여할 것이다. 향후 연구에서는 Train4U 시스템의 성능을 더욱 강화하고, 다양한 산업 분야에서의 실용적인 적용 가능성을 검토할 예정이다.

## ACKNOWLEDGMENT

(한글)본 논문은 울산시-ETRI 2차 공동협력사업의 일환으로 수행되었음. [23AS1600, 제조 혁신을 위한 주력산업 지능화 기술 개발 및 산업현장에서의 사람-이동체-공간 자율협업지능 기술 개발]

## 참 고 문 헌

[1] Balthazar, P., Harri, P., Prater, A., & Safdar, N. M. (2018). Protecting your patients' interests in the era of big data, artificial intelligence, and predictive analytics. Journal of the American College of Radiology, 15(3), 580-586.

[2] Jack Lawto, "Can you use AI for good where sensitive data is concerned?", AIIMI, Available: https://www.aiimi.com/insights/can-you-use-ai-for-good-where-sensitive-data-is-concerned, accessed on October 14, 2022.

[3] MIT Media Lab, "MIT Media Lab's Split Learning: Distributed and collaborative learning," Available: http://splitlearning.mit.edu, accessed on November 10, 2021.

[4] J. Y. Jeong, C. L. Sim, Y. G. Yoon, T. H. Yoon, and M. J. Lee, "A study on the trustworthy split learning execution methodology based on blockchain systems," Proceedings of the Korean Institute of Communications and Information Sciences Conference, Gyeongbuk, Korea, Nov. 2023

[5] Klaytn, https://ko.docs.klaytn.foundation/

[6] Hyperledger Fabric, https://hyperledger-fabric.readthedocs.io/ko/latest/whatis.html