블록체인	머신러닝	분산 지식

충북대학교 CHUNGBUK NATIONAL UNIVERSITY

블록체인 기반의 데이터 프라이버시를 제공하는 분산 지식 발견 시스템 및 방법

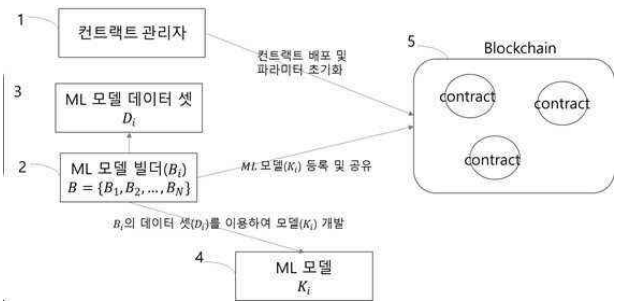
출원인	충북대학교 산학협력단		
연구책임자(소속)	이건명 교수 (충북대학교 소프트웨어학과)	기술완성단계(TRL)	연구개발완료단계 (3단계)
Keyword	블록체인, 데이터 프라이버시, 분산 지식		

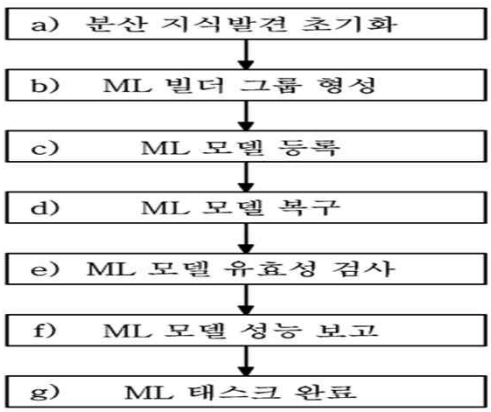
기술 개요

“ 신뢰하지 않는 제 3자간의 모델 공유를 통한 자신의 머신러닝 모델 성능 향상 ”

- 소프트웨어에 의한 정보처리가 하드웨어를 이용하여 구현 가능하도록 된 시스템에 의해 수행되는 블록체인 기반
- 의 데이터 프라이버시를 제공하는 분산 지식 발견 방법
- 등록한 머신러닝 빌더가 자체적으로 개발한 머신러닝 모델을 암호화하여 블록체인에 등록하는 머신러닝 모델 등록 단계
- 머신러닝 성능 보고가 모두 완료되고 해당 절차에 따라 보증금 정산이 완료되는 머신러닝 모델 태스크 완료 단계

시스템 블록 다이어그램 및 개략적 도면





기존 기술의 문제점

- 종래의 기술로 ML 모델을 개발하고자 한다면, 양질의 모델을 개발하기 위해 대량의 데이터가 필요하지만 데이터의 가치로 인한 공유의 어려움이 있음
- 데이터 공유 시에도 동시에 공유하지 않는 경우가 있으며, 공유하더라도 양질의 데이터가 아닌 경우가 있음

✓ 블로체인 기반의 공유 시스템으로 공유전 데이터 유효성 검사로 동일 모델의 판단 여부와 성능검사를 통한 부실모델 분류를 통해 데이터의 안전한 동시 공유가 가능함

기술의 차별성

“ 정직하지 않은 모델 공유자에게 벌금 부과 ”

블록체인 기반의 정직한 공유 유도 시스템

- 성능검사 과정에서 최소성능점수에 도달하지 못한 모델에 대해서 해당 모델 개발자에게 부실모델 벌금을 부여하여 양질의 데이터 공유를 유도함
- 성능이 떨어지는 모델 공유자는 다른 빌더들과 합동하여 검증하게 되므로 해당 과정을 통해 검증된 양질의 머신러닝 모델과의 협업은 모델의 성능 및 가치를 향상시키게 되고 이는 향후 기계학습 발전에 기여할 수 있음