제목: AI 사이버보안 체계를 위한 블록체인 기반의 Data-Preserving AI 학습환경 모델

1.연구 배경:

현대의 AI 기술은 데이터에 의존하여 학습하므로, 데이터의 품질과 무결성은 매우 중요

그러나 원시 데이터를 가공하거나 검수하는 과정에서 인적 오류나 악의적인 조작이 발생할 수 있음.

특히 사이버보안 분야에서는 데이터의 무결성이 보장되어야 하기 때문에 AI가 학습하는 데이터의 정확성과 무결성을 보장하기 위한 방법이 필요해 연구함.

2.연구 내용:

1)방법 제안

사이버보안 관점에서 AI 학습 데이터의 부정확한 사례와 사이버 공격 방법을 분석하고 데이터 무결성 검증을 위해 블록체인 기술을 활용한 Data-preserving 인공지능 시스템을 제안

2)방법 설명

이 시스템은 학습 데이터가 블록체인에 저장되어 변조되지 않은 상태로 유지되며, 데이터를 제공하고 활용하는 과정에서 발생할 수 있는 사이버 공격과 데이터 변질 등의 위협을 사전에 방지할 수 있음.

3.향후 방향

이 연구를 통해 제안된 Data-preserving AI 학습환경 모델은 AI 기반 사이버보안 체계를 더 안전하고 신뢰할 수 있도록 도와줄 것으로 예상됨.