Journal of KIIT. Vol. 22, No. 5, pp. 33-42, May 31, 2024. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2024.22.5.33

AI 네트워킹 기반의 블록체인 기술을 이용한 트랜잭션의 합법적인 검증 모델

정윤수*, 김용태**

Legal Verification Technique for Transactions using AI Networking-based Blockchain Model

Yoon-Su Jeong*, Yong-Tae Kim**

요 약

최근 인공지능(AI)과 블록체인 기술이 널리 사용되면서 트랜잭션의 정상적인 처리 유·무에 많은 관심이 있다. 그러나, 트랜잭션의 합법적인 검증이 이루어지기 위해서는 각 블록체인 네트워크 노드가 거래 데이터의 무결성을 유지해야만 한다. 본 논문에서는 AI 블록체인을 이용하여 트랜잭션의 무결성 손상으로 인한 클라우드에 저장된 데이터의 손실을 예방할 수 있는 트랜잭션의 합법적인 검증 모델을 제안한다. 제안 모델은 AI 네트워크 환경에서 AI 블록체인의 불량률을 줄이기 위해서 가상화 자원 할당한 후 동적으로 서버 또는 장치를 이중화하여 안정성과 가용성을 향상시켰다. 성능평가 결과, 블록체인을 사용하는 AI 네트워크인 경우 왜곡된 IoT 장치의 트랜잭션 그룹을 6개로 파티셔닝할 경우 정확도는 95.805%, F1 점수는 96.847로 가장 높다.

Abstract

Recently, with the widespread use of artificial intelligence(AI) and blockchain technology, there is a lot of interest in the normal processing of transactions. However, in order for a transaction to be legally verified, each blockchain network node must maintain the integrity of the transaction data. In this paper, we propose a legal verification model of transactions that can prevent the loss of data stored in the cloud due to the damage to the integrity of transactions using AI blockchain. The proposed model improved stability and availability by dynamically duplexing servers or devices after allocating virtualization resources to reduce the defect rate of AI blockchain in an AI network environment. As a result of the performance evaluation, in the case of an AI network using a blockchain, when the transaction group of the distorted IoT device is partitioned into six, the accuracy is the highest at 95.805%, and the F1 score is the highest at 96.847.

Keywords

AI, network, IoT, verification, resource accuracy, blockchain

* 목원대학교 게임소프트웨어공학과 교수
- ORCID: https://orcid.org/0000-0003-3455-5947
** 한남대학교 멀티미디어공학과 교수(교신저자)
- ORCID: https://orcid.org/0000-0002-1554-1040

· Received: Feb. 02, 2024, Revised: Feb. 23, 2024, Accepted: Feb. 26, 2024

· Corresponding Author: Yong-Tae Kim
Dept. of Multimedia Engineering, Hannam Korea
Tel.: +82-42-829-7678, Email: ky7762@hnu.kr

Ⅰ. 서 론

최근 네트워크 및 통신 기술의 급속한 성장으로 인해 인공지능(AI) 및 블록체인 기술이 널리 사용되고 있다[1]. 인공지능과 블록체인 기술은 네트워크 공급망 추적성을 향상시키는 데 있어서 핵심 구성 요소이다. 네트워크 공급망은 추적성에 크게 의존하며, 블록체인 및 인공지능은 전체 공급망에서 서비스 추적성을 향상시키는 효과적인 솔루션을 제공한다.

공급망 추적성을 위한 블록체인과 인공지능 기술의 적용은 아직 초기 단계이지만, 둘 다 공급망 가시성과 효율성을 높일 수 있는 많은 잠재력을 가지고 있다[2][3]. 인공지능을 사용하면 재료 추적 및 제품 및 서비스 모니터링을 포함한 특정 공급망 작업을 자동화할 수 있으며, 블록체인 기술은 공급망 전반에 걸쳐 상품 및 서비스를 추적하고 모니터링할 수 있는 안전하고 신뢰할 수 있으며 투명한 플랫폼을 제공할 수 있다.

오늘날 블록체인 기술은 분산된 환경을 만들고 분산된 데이터베이스 솔루션을 제공할 수 있다. 모든 트랜잭션은 블록체인에 의해 기록되므로 데이터가 일단 네트워크에 있으면 위조, 추적 또는 변조하기 어렵고 변경할 수 있는 사람이 거의 없다. 연구자들은 블록체인 기술을 기반으로 최근 데이터 무결성 검증을 위한 몇 가지 데이터 감사 체계를 만들었다[4][5]. 이 때문에 연구자들은 신뢰할 수 있는 감사를 제공하기 위해 TPA를 블록체인 기술로 대체하고 있다[6].

J. Xu et al.[7]은 부정직한 TPA와 스토리지 서비스 제공업체가 데이터 무결성 인증서를 결합하고 조작하는 것을 방지하기 위해 무작위 챌린지 메시지를 개발하고 블록체인 기술을 통해 신원 기반 공공 감사 메커니즘을 구축했다. C. Zhang et al.[8]은 블록체인 기반 멀티 클라우드 스토리지에 대해 데이터 감사 방법을 제시했지만 검증 효율성은 낮다. 따라서 기존 블록체인 기술은 무결성 검증의 효율성에 큰 영향을 미치며 효율성이 떨어지는 문제가 발생할 수 있다.

본 논문에서는 AI 네트워킹 기반의 블록체인 기술을 이용하여 트랜잭션의 합법적인 검증 기법을 제안한다. 제안 모델은 AI 블록체인을 활용하여 클라우드 스토리지의 데이터 손실을 방지하기 위해 트랜잭션 무결성을 활용할 수 있다. 제안 모델은 AI 네트워크에서 가상화 자원 할당을 사용하여 AI 블록체인의 실패율을 낮추었다. 제안 모델은 서버 또는 장치의 이중화를 사용하고 가상화를 통해 필요한 AI 블록체인을 동적으로 수정함으로써 안정성과 가용성을 높였다.

AI 네트워크 환경에서 AI 블록체인 자원의 무결성을 보장하기 위한 제안 모델의 목적은 다음과 같다. 첫째, 제안 모델은 가용 스토리지와 모든 IoT 디바이스 컴퓨팅 기능을 극대화하기 위해 먼저 저비용 에지 디바이스를 통합한 다음 데이터 처리 및 공유 퍼블릭 블록체인을 AI 알고리즘에 적용하고 처리한다. 둘째, AI 블록체인 자원의 무결성을 보장하기 위해 에지와 IoT 기기를 AI 관련 데이터로 통합 처리한다. 셋째, AI를 수행하여 IoT 데이터의 유지 보수, 문제 해결 및 사고 관리를 자동화하고 최적화하는 것이다.

이 논문의 구성은 다음과 같다. 2장에서는 IoT 블록체인 관련 기존 연구를 분석한다. 3장에서는 블록체인 기반 트랜잭션의 합법적인 검증 기법을 제안하고, 4장에서는 성과 평가를 수행한다. 마지막으로 5장은 결론을 맺는다.

Ⅱ. 관련 연구

2.1 AI 네트워킹

인공지능 네트워킹은 기존의 IT 운영을 변화시키면서 네트워크의 지능, 자기 적응, 효율성, 그리고 신뢰성을 향상시킨다. 그 기술은 기계 학습 (ML), 딥 러닝, 자연어 처리 (NLP), 생성 인공지능 (genAI), 그리고 다른 기술들을 사용하여 네트워크를 감시하고, 문제를 해결하고, 보호한다.

AI 네트워킹은 AI와 네트워킹 인프라를 통합함으로써 유지 보수, 문제 해결 및 사고 관리를 자동화하고 IT 운영을 최적화할 수 있다. 이는 혁신적인 네트워크 관리로 이어질 수 있다. AI 네트워킹은 디지털 트윈, 패턴 인식, 예측 및 추세 분석, genAI 등 많은 기술을 통합하기 때문에 운영 관리 비용의 최대 25%를 차지할 수 있다.

AI 네트워킹의 특징은 다음과 같다. 첫째, 초기에 CPU나 플래시 드라이브 결함을 포함한 하드웨어 결함의 가능성을 인식하고 필요에 따라 수정한다. 둘째, 여러 데이터 세트를 연결하여 지연 시간이나 기타 문제의 근본 원인을 파악한다. 셋째, 수요 증가에 대응하여 노이즈, 간섭 또는 혼잡 시 추가 대역폭을 요청하거나 트래픽을 다른 채널로 전환할 수 있다. 넷째, 서버 응답 시간이 길어지는 원인을 확인한다. 다섯째, IT 직원이 모든 공급업체의 기술 세부 사항이나 플랫폼별 언어를 이해하지 않아도 되도록 공급자 중립적인 이슈 솔루션이나 프로비저닝을 제공한다.

2.2 블록체인 기반 트랜잭션 검증

블록체인 검증은 블록체인 네트워크 내부에서 거래와 데이터의 진위와 유효성을 검증하는 과정이다. 블록체인은 원장의 현재 상태에 대한 여러 참여자, 즉 노드의 합의를 도출하기 위해 합의 방식에 의존하는 탈중앙화된 시스템이다. 모든 거래가 새로운 블록에 포함되기 전에 검증을 통해 합법적이고 미리 정해진 지침을 준수하는지 확인한다.

O. S. Saleh et al.[9]은 자격증 검증 솔루션 마지막에는 하이퍼레저 패브릭 프레임워크를 활용하여 인증, 권한, 기밀성, 프라이버시, 소유권 등의 주제를 중심으로 교육 자격증을 검증하는 블록체인 기반 프레임워크를 제안하였다.

J. Zhang et al.[10]은 송신 노드의 평판(Reputation)을 고려하여 트랜잭션 처리 효율성을 높이기 위한 기반 메커니즘을 제안하였다. 이 메커니즘은 트랜잭션을 평판이 높은 수신자에게 우선 순위를 지정하여 전파 지연을 줄이기 위해 트랜잭션 포워딩 프로토콜을 최적화하였다.

Y. Xu et al.[11]은 IoT 애플리케이션의 거래 수요를 충족시키기 위해 공간 구조화된 원장을 기반으로 하는 통합 블록체인 및 MEC(IBM) 프레임워크를 제안하였다. 이 프레임워크는 마이닝 효율성을 촉진하기 위해 MD의 명성에 따라 차별화된 마이닝 대상이 할당되는 평판 기반 작업 증명(Re-PoW)이라는 고성능 합의 메커니즘을 추가로 개발하였다.

Y. Liang et al.[12]은 스펙트럼 공유를 촉진하면서 거래 효율성을 개선하고 시스템 오버헤드를 줄이기 위해 사용할 수 있는 간섭 기반 합의 메커니즘을 제안하였다. 이 메커니즘은 스펙트럼 거래자로 인한 유해한 간섭을 피하기 위해 블록에 저장된 스펙트럼 거래를 검증하기 위해 간섭 기반 거래 검증 메커니즘이 설계되었다.

2.3 기존 연구

이전 연구에서는 아웃소싱 데이터의 무결성을 보호하기 위해 데이터 감사를 사용하여 데이터의 MAC 값을 검증하는 방법을 검토했지만, 높은 오버헤드와 짧은 검증 시간의 문제가 있다[13]. 사용자는 전체 파일을 다운로드하지 않고도 RSA 기반 PDP 모델에서 CSP에 저장된 데이터의 하위 집합을 무작위로 검증함으로써 챌린지 응답을 통해 데이터 무결성에 대한 확률적 확인을 얻을 수 있다. 이후 더 많은 PDP 시스템이 제안되었다[14].

C. Zhang et al.[8]은 멀티 클라우드 시나리오에서 공개 배치 데이터의 무결성 감사를 수행하기 위해 블록체인 기반 멀티 클라우드 스토리지의 데이터 감사 기법을 제안했다. 이 기법은 블록체인 기술을 도입했는데, 검증 효율성이 낮다는 점이 이 기법의 한 가지 문제점이다. 이 기법은 기존 방식의 중앙 집중화 문제를 해결하지만, 여러 서버를 보유한 CSP 시스템은 블록체인 기술 사용으로 인한 효율성 저하 문제를 간과하고 있으며, 데이터 무결성 검증 절차가 길고 부진하여 데이터 활용에 영향을 미친다.

III. IoT 블록체인을 이용한 트랜잭션의 합법적인 검증 기법

3.1 개요

최근 다양한 분야에서 클라우드 컴퓨팅 기술은 네트워크 및 통신 기술의 급속한 발전으로 널리 사용되고 있다. 클라우드 컴퓨팅이 제공하는 한 가지 특징은 클라우드 스토리지인데, 스토리지 리소스는 네트워크를 통해 액세스할 수 있기 때문에 사용자가 아무리 크든 작든 정보를 쉽게 교환할 수 있다.

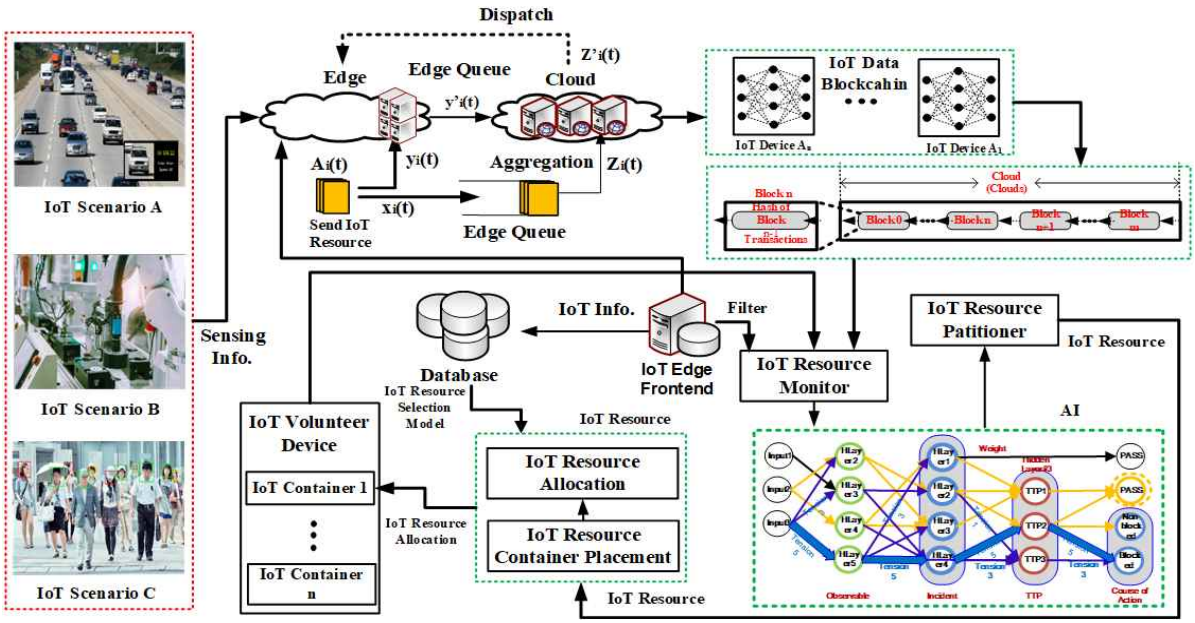

그림 1. 제안 기법의 AI 네트워킹 환경

Fig. 1. AI Network environment of the proposed technique

공공 클라우드 서비스는 초기 비용을 최소화하기 때문에 활용하기에 매우 효율적이다. 하지만 에지에서 생성된 방대한 양의 데이터가 수집되어 클라우드 서비스로 전송되면 네트워크 비용에 큰 영향을 받는다. 그 이유는 네트워크 통신 기반 퍼블릭 클라우드 과금 체계 때문에 과다한 사용 비용이 발생하기 때문이다. AI 블록체인 기반의 인프라는 민감한 내부 데이터가 퍼블릭 클라우드에 노출되면 안 되며, 정밀한 분석을 통해 데이터를 안전하게 저장하고 처리해야 한다.

본 논문에서는 인공지능 네트워킹에 기반한 블록체인 기술을 활용하여 트랜잭션의 합법적인 검증 모델을 제안한다. 제안 모델은 막대한 양의 계층적 AI 블록체인 데이터를 안전하게 수집, 분석 및 추출하기 위해 비용 절감을 유지하면서 AI 네트워킹을 활용한 네트워크를 지속적으로 관리, 유지 및 최적화한다. 그림 1은 AI 네트워킹 기반의 블록체인 기술을 이용하여 트랜잭션의 합법적인 검증이 이루어지는 전체 과정을 보여주고 있다. 그림 1은 IoT 센싱 데이터를 수집한 후 데이터 처리 및 공유 퍼블릭 블록체인을 AI 알고리즘에 적용한 후 처리한다. 그 이유는 저비용 에지 장치의 통합을 기반으로 사용 가능한 스토리지와 모든 IoT 장치 계산 능력을 최대한 활용하기 위해서이다.

그림 1은 AI 네트워크 환경에서 IoT 센싱 데이터를 수집, 처리, 분석 및 도출하기 위해서 지능형 모델(예: DNN 등)을 사용하여 지속적인 피드백과 기술 발전에 기반한 고유 요구사항을 포함한다. 그림 1은 고급 분석, 기계 학습 및 인공지능을 활용하여 지능적인 의사결정을 지원하고 운영을 최적화하여 효율성을 향상시킨다.

제안 모델은 적절한 에지와 IoT 디바이스를 통합하여 AI 관련 데이터를 AI 블록체인과 통합하고 처리하므로 AI 블록체인 리소스의 무결성을 보장한다. IoT 센싱 데이터는 먼저 다양한 특성 데이터를 수집하기 위해 에지 계층에서 AI 블록체인을 전처리하고 필터링하는 중앙 플랫폼으로 전송한다. 데이터베이스는 처리된 데이터와 원시 데이터를 모두 사용하여 추가 평가를 수행한다. 제안 모델은 머신러닝에 대한 고급 분석과 기술 분석을 통해 통계 알고리즘과 머신러닝 모델을 사용하여 트랜잭션 오작동을 예측하여 프로세스를 개선한다.

3.2 AI 블록체인 기반의 트랜잭션 처리 과정

제안 모델은 그림 2와 같이 계층적 AI 데이터 처리 과정에서 생성되는 대용량 데이터에 대한 수집, 처리, 추출 및 서비스를 제공한다.

그림 2은 제안 모델이 제공하는 데이터 수집, 처리 및 분석 시스템과 노드 간에 공유할 수 있는 일반적인 처리 절차를 보여준다. 제안 모델의 계층적 AI 데이터 처리는 크게 4단계로 구성된다.

첫 번째 단계는 모니터링 및 수집하는 단계이다. 이 단계는 사물인터넷 시스템의 상황을 주시하면서 가장 낮은 계층의 센서를 사용하여 환경을 수집하거나 데이터를 변경한다. 두 번째 단계는 네트워크를 P2P 처리하는 단계이다. 이 과정은 에지 노드와 같이 게이트웨이 역할을 하는 노드들이 수집한 데이터를 활용하여 분석 및 예측을 제공한다. 세 번째 단계는 에지 디바이스에서 생성된 결과물에 무제한으로 액세스할 수 있도록 하는 단계이다. 이 단계는 에지 디바이스에서 생성된 결과물을 퍼블릭 블록체인 네트워크의 모든 참여 노드가 자유롭게 공유한다. 마지막 단계는 퍼블릭 블록체인을 사용하여 분석한 데이터를 제공하는 단계이다. 이 단계는 인공지능 기술을 통해 모든 데이터를 공개적으로 사용할 수 있다.

3.2.1 센싱 계층

이 계층은 아키텍처에서 가장 낮은 계층이며 가장 중요한 계층이다. 이 계층은 공통 플랫폼에 데이터를 제공하며, 광범위한 저비용, 저전력 및 소형 센서 장치가 모니터링 및 데이터 수집에 사용된다. 센서 데이터는 수집되어 게이트웨이로 전송되는데, 게이트웨이는 처리, 준비 및 수정을 위해 다음 계층으로 전송되는 저비용 장치(예: 아두이노 ESP-32)이다. 이는 아키텍처의 초기 모니터링 및 수집 단계를 완료하는 데 도움이 된다.

3.2.2 네트워크 계층

게이트웨이에 의해 제출된 데이터는 다음 계층으로 전송된다. 이 계층은 서로 다른 통신 링크(예: Wi-Fi, 5G 또는 유선 연결)가 사용될 수 있다.

3.2.3 블록체인 계층

이 계층은 아키텍처, 분석 및 예측의 두 번째 단계를 완료하는 역할을 담당한다. 이 계층은 필요한 분석을 수행하는 데 필요한 AI 엔진이 제공된다.

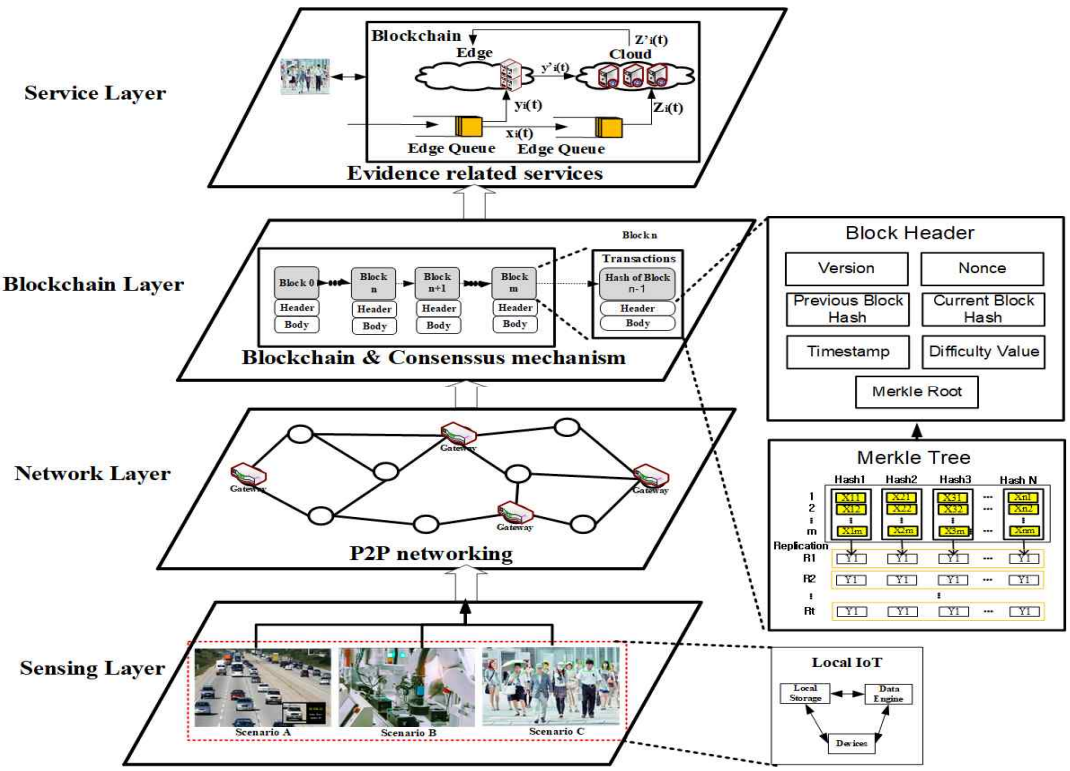

그림 2. 계층별 AI 블록체인 기반의 트랜잭션 처리 과정

Fig. 2. AI blockchain-based transaction processing by hierarchy layer

이 계층에 배치된 장치는 비용과 전력 모두에서 저렴할 수 있으며, 이러한 장치의 한 예로 라즈베리 파이가 있다. 이 계층에 위치한 모든 노드는 블록체인 플랫폼의 완전한 클라이언트여야 한다. 플랫폼은 지속적인 데이터 스트림(센서 및 AI 결과 수집)을 가질 수 있어 시스템 성능이 향상된다. 이 노드가 수집한 데이터와 AI 결과는 즉시 다른 블록체인 클라이언트와 공유할 수 있다.

3.2.4 서비스 계층

이 계층은 자유롭게 접근할 수 있는 퍼블릭 블록체인 플랫폼이며 공유 내용을 보관하는 역할을 한다. 서비스 계층 내부의 모든 장치는 공개 블록체인에 통합된다. 이를 통해 모든 기업이나 개인 또는 관련 당사자가 이러한 플랫폼에 참여하고 모든 처리된 AI 및 수집된 데이터에 제한 없이 액세스할 수 있다.

3.3 AI 블록체인 데이터 다이어그램

블록체인 프로세스 단계가 성공적으로 완료되면 관리자를 통해 서비스를 제공한다. 이에 따라 관리자는 모든 트랜잭션의 AI 데이터 검증 프로세스를 완료하기 위한 기능 요청을 수행한다. 그림 3은 블록체인 검증 과정을 포함한 자원 공유 시스템을 보여준다. IoT 장치가 제공하는 자원 수요 데이터를 병합하여 거래 정보를 생성한다. 주기적으로 블록체인 코드를 인가하는 IoT 자원 관리자는 이를 네트워크 개체에 전송한다.

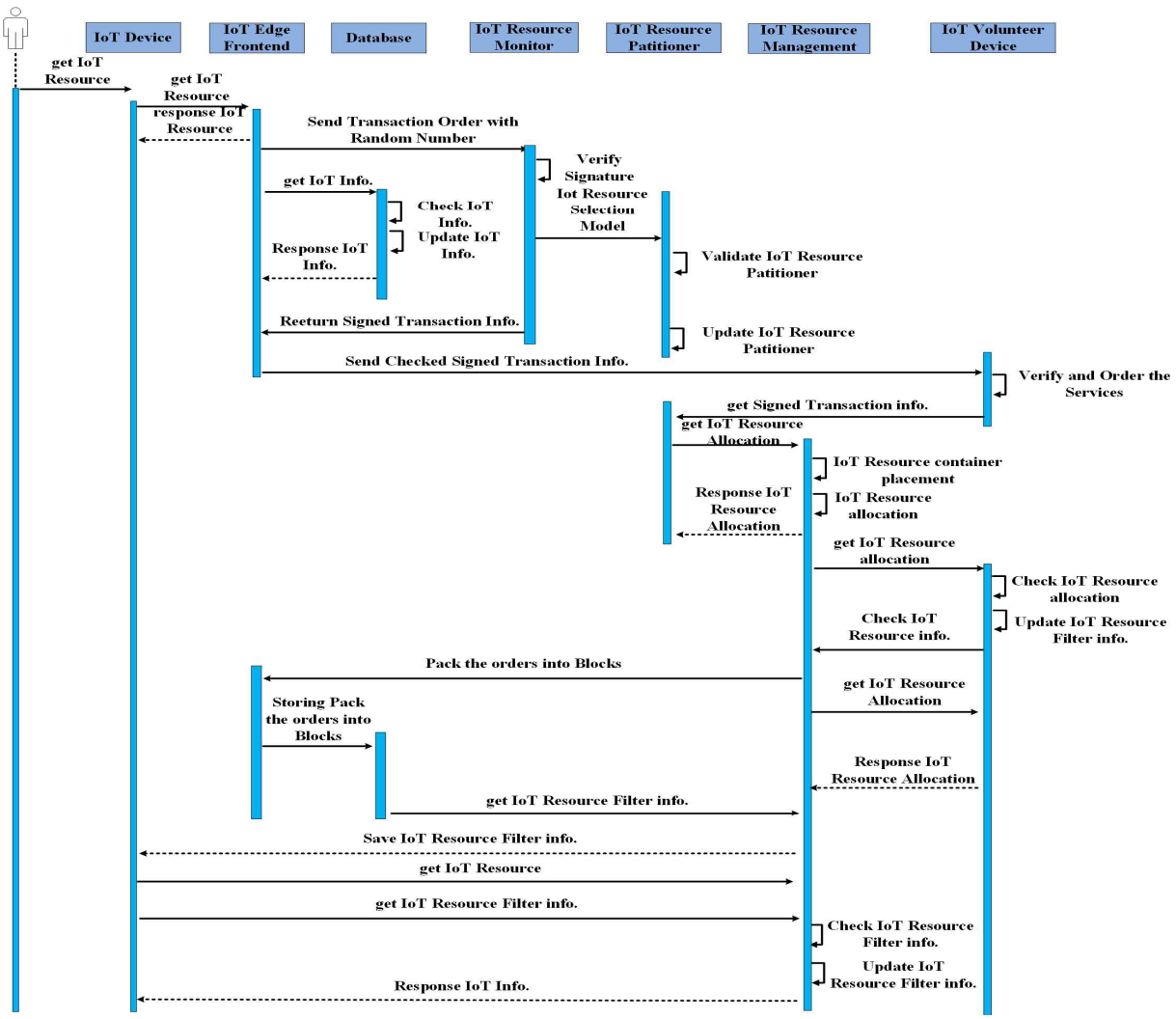

그림 3. 제안 기법의 계층별 AI 블록체인 트랜잭션 처리 다이어그램
Fig. 3. Hierarchical transaction processing process of proposed techniques

네트워크 임계값을 달성할 때까지 거래기록 패키지는 요청된 주문, 즉 블록 형태로 수집된다. 실행 결과가 확인된 블록은 임계값 레벨이 충족되면 트랜잭션 서비스에 의해 각 피어에게 정기적으로 제공된다. IoT 장치의 데이터는 블록체인 네트워크, 클라우드 네트워크, 물리적 자원, 보안 설정, 사물인터넷 기기 등의 실시간 객체에 의해 접근되어 기기의 정보를 찾는다.

그림 3은 각 블록이 블록 헤더와 블록 바디의 두 부분으로 나뉘며, 블록 바디는 검증된 트랜잭션 데이터를 저장하고, 블록 헤더에는 버전, 이전 블록의 해시 값, 현재 블록의 해시 값, 타임스탬프, 난이도 값, 난수값, 머클 루트가 포함된다.

그림 3에서 블록체인의 트랜잭션 실행 과정은 다음과 같다. 초기에 노드들은 자신의 공개 키와 개인 키를 무작위로 생성하고 스크립팅 도구나 지갑을 사용하여 트랜잭션을 구축한 다음 개인 키로 트랜잭션에 서명한 다음 P2P 네트워크를 통해 서명된 트랜잭션을 배포한다. 이를 받은 노드는 트랜잭션이 합법적인지 확인한 후 합의 절차를 통해 새로운 블록을 생성한다. 노드들은 새로운 블록의 유효성을 확인하여 새로운 블록을 P2P 네트워크를 통해 다른 노드로 브로드캐스트한 후 로컬 체인에 추가할지 아니면 삭제할지 결정한다. 이는 새로운 트랜잭션이 빈 블록을 준수한 후 블록체인의 노드 간에 성공적으로 전송되었음을 보여준다.

Ⅳ. 평 가

이 절에서는 AI 네트워크 환경에서 블록체인 거래의 법적 검증 과정의 효율성을 평가하기 위해 IoT 기기 수에 따른 거래 정확도와 블록체인 유무에 따른 블록 검증을 비교 평가한다.

4.1 환경설정

제안 모델은 클러스터의 수를 {1, 2, 5, 10}을 구성하고, 트랜잭션의 수는 {300, 600, 900}으로 설정한다. 제안 모델은 블록 크기를 {1, 3, 5}MB 로 하고, 잡음(noise)은 2^{10}KHz로 설정한다. 제안 모델은 12GB의 RAM을 가진 GeForce RTX 2080 Ti가 장착된 서버를 사용하고, 수집된 샘플 데이터의 70%는 훈련에 사용된다. 훈련 샘플은 고유성을 기반으로 네트워크의 각 클라이언트로 다시 분할한다. 클라이언트와 중앙 서버 간의 통신 주기마다 5번의 에포크 동안 클라이언트 모델은 32개의 배치 크기로 학습한다. 제안하는 모델은 훈련 중에 80개의 통신 주기를 수행한다. 모든 실험의 구현과 평가에는 PyTorch가 사용되었다.

4.2 성능평가

4.2.1 IoT 수에 따른 트랜잭션 정확도

제안 모델은 IoT 트랜잭션의 이상 탐지를 통한 성능 결과는 표 1과 같다. 제안 모델은 p 값이 0.001인 카이제곱 통계량을 이용하여 이상 탐지 모듈의 실제 측정값을 측정하였다. 표 1은 n개의 IoT 장치로 트랜잭션을 무작위로 분할했으며, 트랜잭션이 서로 다른 수의 IoT 장치로 그룹화한 결과이다.

표 1은 AI 네트워크와 일반 네트워크 모두 정확도와 F1 점수가 IoT 장치 수가 증가함에 따라 변동하는 것을 모두 관찰하였으며, 패턴 변화에 따라 트랜잭션의 파티셔닝은 다른 결과가 도출되었다. 또한, IoT 악성 트랜잭션의 변화는 트랜잭션 검증을 저하시키는 결과를 야기하였다. 제안 모델은 블록체인을 사용하지 않고 AI 네트워크에서 모든 트랜잭션의 검증 정확도가 평균 89.795%와 F1 점수는 91.679가 나타났지만, 블록체인을 사용하는 AI 네트워크인 경우 왜곡된 IoT 장치의 트랜잭션 분포인 경우는 트랜잭션의 그룹을 6개로 파티셔닝하였을 때가 정확도는 95.805%, F1 점수는 96.847로 가장 높게 나타났다.

표 1. IoT 수에 따른 트랜잭션 정확도 성능 결과
Table 1. Transaction accuracy performance results based on the number of IoTs

Network	Not using blockchain		Using blockchain	
	Accuracy (%)	F1 Score	Accuracy (%)	F1 Score
Public network	85.681	87.247	92.387	93.384
AI network	89.795	91.679	95.805	96.847

4.2.2 블록체인 유·무에 따른 블록 검증 비교

표 2은 블록체인 유·무에 따른 우회 기간 제어(Bypass period control)와 부정 거래 탐지(Fraud transaction detection) 블록의 검증 방법을 평가한 결과이다. 표 2처럼, 부정 거래 탐지는 필터링 성능으로 인해 매우 높은 트랜잭션 데이터 무결성을 제공하지만, 검증을 위해 더 많은 컴퓨팅 리소스가 필요하였다. 그러나, 블록체인을 사용하는 부정거래 탐지는 작업의 안전성을 보장할 수 있는 결과를 얻었다.

표 2. 블록 검증 방법에 따른 성능 결과
Table 2. Performance results by block validation method

	Not using blockchain		Using blockchain	
	Fraud transaction filtering rate(%)	Validatino rate(%)	Fraud transaction filtering rate(%)	Validatino rate(%)
Bypass period control	88.87	78.74	91.62	86.42
Fraud transaction detection	90.92	82.08	96.54	94.32

4.2.3 블록 크기에 따른 트랙잭션의 처리량 분석

트랜잭션 크기와 블록 크기를 사용한 처리량 분석은 그림 4 및 그림 5와 같다. 그림 4 처럼 트랜잭션의 수(No. of transactions) 또는 블록 크기가 증가하면 각 트랜잭션에 대해 시스템 처리량이 확장된다. 따라서 제안 모델은 사용자에게 효율적이고 신뢰할 수 있는 사용자 인증을 제공하고 인공 지능을 갖춘 데이터 인증을 제공한다. 이를 위해서, 제안 모델에서는 인공지능 관련 데이터 학습 방법을 3가지 기반의 방법(과거 데이터 정보 학습 HDIL, 인간 인식 학습 HPL, 현재 신뢰 점수 학습 CCSL)으로 처리한다.

그림 5에서 트랜잭션의 수가 적을 때보다 높을수록 처리량을 많아졌으며, 트랜잭션의 수가 300일 경우는 트랜잭션의 수가 600과 900보다 처리량은 최대 18.75% 차이가 났다.

그림 5 처럼 트랜잭션의 블록 크기가 증가하면 각 트랜잭션에 대해 시스템 처리량이 확장된다. 제안 모델에서 사용되는 데이터는 분산 해시 테이블(DHT)과 분산 해시 테이블과 함께 분산 클라우드 계층에 저장된다. 그림 5에서 블록의 수가 적을 때보다 높을수록 처리량을 많아졌으며, 트랜잭션의 수가 300일 경우는 트랜잭션의 수가 600과 900보다 처리량은 최대 10.8% 차이가 났다.

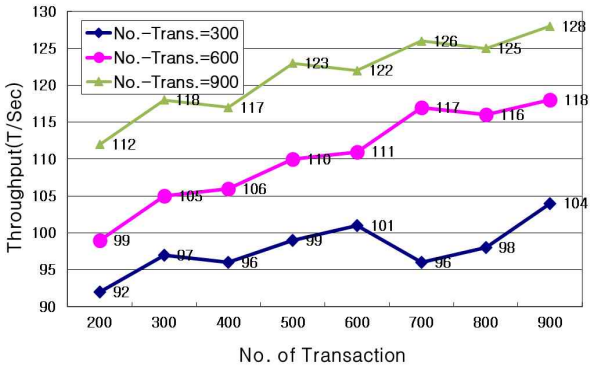

그림 4. 트랜잭션 수에 따른 처리량
Fig. 4. Throughput based on the number of transactions

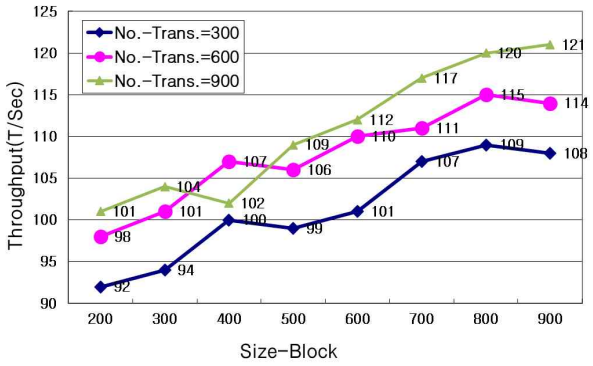

그림 5. 블록 크기에 따른 따른 처리량
Fig. 5. Throughput according to block size

V. 결론 및 향후 과제

블록체인 기반 거래의 무결성을 보장하기 위해 최근 AI 네트워크에서는 다양한 연구가 진행되고 있다. 본 논문에서는 AI 블록체인을 이용하여 트랜잭션의 무결성 손상으로 인한 클라우드에 저장된 데이터의 손실을 예방할 수 있는 트랜잭션의 합법적인 검증 기법을 제안하였다. AI 네트워크에서 블록체인 유·무에 따라 트랜잭션의 무결성이 다르게 나타났다. 제안 모델은 AI 네트워크의 가상화 리소스를 이용하여 서버나 디바이스를 이중화함으로써 안정성과 가용성을 높였다.

성능 평가 결과, 블록체인을 사용하는 AI 네트워크인 경우 왜곡된 IoT 장치의 트랜잭션 그룹을 6개로 파티셔닝하였을 때가 정확도는 95.805%, F1 점수는 96.847로 가장 높게 나타났다. 본 연구의 결과를 바탕으로 향후 연구에서는 제안 모델을 다양한 네트워크 환경에 적용하여 그 효과를 평가할 것이다.

References

[1] T. X. Tran and D. Pompili, "Joint task offloading and resource allocation for multi-server mobile-edge computing networks", IEEE Trans. Veh. Technol., Vol. 68, No. 1, pp. 856-868, Jan. 2019. https://doi.org/10.1109/TVT.2018.2881191.

[2] D. Yaga, P. Mell, and N. Roby, "Blockchain technology overview", NIST, pp. 1-68, Oct. 2019. https://doi.org/10.6028/NIST.IR.8202.

[3] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges", IEEE Communications Surveys & Tutorials, Vol. 21, No. 2, pp. 1508-1532, Feb. 2019. https://doi.org/10.1109/COMST.2019.2894727.

[4] Y. Xu, C. Zhang, G. Wang, Z. Qin, and Q. Zeng, "A blockchainenabled deduplicatable data auditing mechanism for network storage services", IEEE Transactions on Emerging Topics in Computing, Vol. 9, No. 3, pp. 1421-1432, Jul. 2020. https://doi.org/10.1109/TETC.2020.3005610.

[5] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for IoT data", Proc. of the 2017 IEEE International Conference on Web Services (ICWS), Honolulu, HI, USA, pp. 468-475, Jun. 2017. https://doi.org/10.1109/ICWS.2017.54.

[6] Y. Xu, J. Ren, Y. Zhang, C. Zhang, B. Shen, and Y. Zhang, "Blockchain empowered arbitrable data auditing scheme for network storage as a service", IEEE Transactions on Services Computing, Vol. 13, No. 2, pp. 289-300, Mar. 2019. https://doi.org/10.1109/TSC.2019.2953033.

[7] J. Xue, C. Xu, J. Zhao, and J. Ma, "Identity-based public auditing for cloud storage systems against malicious auditors via blockchain", Science China Information Sciences, Vol. 62, No. 3, pp. 1-16, Mar. 2019. https://doi.org/10.1007/s11432-018-9462-0

[8] C. Zhang, Y. Xu, Y. Hu, J. Wu, J. Ren, and Y. Zhang, "A blockchainbased multi-cloud storage data auditing scheme to locate faults", IEEE Transactions on Cloud Computing, Vol. 10, No. 4, pp. 2252-2263, Feb. 2021. https://doi.org/10.1109/TCC.2021.3057771.

[9] O. S. Saleh, O. Ghazali, and M. E. Rana, "Blockchain based framework for educational certificates verification", Journal of Critical Reviews, Vol. 7, No. 3, pp. 79-84, Mar. 2020. https://doi.org/10.1109/ICESC51422.2021.9532968.

[10] J. Zhang, Y. Cheng, X. Deng, B. Wang, J. Xie, Y. Yang, and M. Zhang "A Reputation-Based Mechanism for Transaction Processing in Blockchain Systems", IEEE Transactions on Computers, Vol. 71, No. 10, pp. 2423-2434, Oct. 2022. https://doi.org/10.1109/TC.2021.3129934.

[11] Y. Xu, H. Zhang, H. Ji, L. Yang, X. Li, and C. M. Leung, "Transaction Throughput Optimization for Integrated Blockchain and MEC System in IoT", IEEE Transactions on Wireless Communications, Vol. 21, No. 2, pp. 1022-1036, Aug. 2022. https://doi.org/10.1109/TWC.2021.3100985.

[12] Y. Liang, C. Lu, Y. Zhao, and C. Sun, "Interference-based consensus and transaction validation mechanisms for blockchain-based spectrum management", IEEE Access, Vol. 9, pp. 90757-90766, Jun. 2021. https://doi.org/10.1109/ACCESS.2021.3091802.

[13] Y. Deswarte, J. J. Quisquater, and A. Saïdane, "Remote integrity checking", Proceedings of the Sixth Working Conference on Integrity and Internal Control in Information Systems (IICIS), Lausanne, Switzerland, pp. 1-11, Nov. 2003. https://doi.org/10.1007/1-4020-7901-X_1.

[14] S. Shin and T. Kwon, "A survey of public provable data possession schemes with batch verification in cloud storage", Journal of Internet Services and Information Security, Vol. 5, No. 3, pp. 37-47, Aug. 2015. https://doi.org/10.22667/JISIS.2015.08.31.037.

저자소개

정 윤 수 (Yoon-Su Jeong)

1998년 2월 : 청주대학교 전자계산학과(공학사)
2000년 2월 : 충북대학교 전자계산학과(이학석사)
2008년 2월 : 충북대학교 전자계산학과(이학박사)
2012년 2월 ~ 현재 : 목원대학교 게임소프트웨어공학과 교수
관심분야 : IoT/IIoT, 네트워크, 정보보안, 빅데이터, 암호학, 스마트팜

김 용 태(Yong-Tae Kim)

1984년 2월 : 한남대학교 계산통계학과(공학학사)
1988년 2월 : 숭실대학교 전자계산학과(공학석사)
2002년 2월 : 충북대학교 전자계산학과(이학박사)
2010년 10월 ~ 현재 : 한남대학교 멀티미디어학부 교수
관심분야 : 모바일 웹서비스, 정보 보호, 센서 웹, 모바일 통 신보안