Journal of KIIT. Vol. 21, No. 6, pp. 135-142, Jun. 30, 2023. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2023.21.6.135

GNN 환경에서 적용 가능한 블록체인 기반 그래프 학습 데이터 관리 메커니즘

김진수*, 박남제**

Applicable Blockchain-based Graph Learning Data Management Mechanisms in GNN Environments

Jinsu Kim*, Namje Park**

이 논문은 2023학년도 제주대학교 교육·연구 및 학생지도비 지원에 의해서 연구되었음

요 약

데이터 학습은 추가적인 인위적 조작 없이 최적화된 결과를 도출하기 위해 사용되는 머신 러닝의 핵심 요소이다. 특히 데이터의 규모가 과거와 비교할 수 없을 정도로 커짐에 따라 학습에 사용될 수 있는 데이터의 양 또한 방대해지고 있다. 방대한 데이터의 효과적인 학습을 위해 데이터를 그래프로 표현하는 GNN(Graph Neural Network)은 그래프라는 데이터 노드에 대해 관계를 생성함으로써 별도의 테이블 관리 없이 데이터간의 관계성 추가 및 제거에 효과적이다. 하지만 기본적으로 데이터는 무결성 훼손에 따른 위험성을 내포하며, 특히 학습용 데이터로 활용되는 데이터의 경우 데이터 위변조에 따른 학습모델의 잘못된 학습으로 새로운 문제를 야기할 수 있다. 본 논문에서는 무결성을 강화하기 위해 그래프 데이터를 전처리하여 노드 데이터와 노드 데이터간의 관계성을 포함하는 데이터 구조를 생성하고, 학습 데이터를 블록 네트워크에서 관리하는 데이터 관리 메커니즘을 제안한다.

Abstract

Data learning is a key element of machine learning used to derive optimized results without additional artificial manipulation. In particular, as the size of the data becomes incomparable to the past, the amount of data that can be used for learning is also increasing. Graph Neural Network(GNN), which graphically represents data for effective learning of vast amounts of data, is effective in adding and removing relationships between data without separate table management by generating relationships for data nodes called graphs. However, basically, data poses a risk of integrity corruption, especially in the case of data used as learning data, mislearning of learning models due to data forgery can cause new problems. To enhance integrity, this paper proposes a data management mechanism that pretreats graph data to generate data structures containing relationships between node data and node data, and manages learning data in block networks.

Keywords
blockChain, graph neural network, data integrity, machine learning

* 제주대학교 융합정보보안학 협동과정 박사과정
- ORCID: https://orcid.org/0000-0003-1009-3928
** 제주대학교 초등컴퓨터교육학과 교수(교신저자)
- ORCID: https://orcid.org/0000-0003-4434-8933

· Received: Mar. 31, 2023, Revised: Apr. 26, 2023, Accepted: Apr. 29, 2023
· Corresponding Author: Namje Park
Dept. of Computer Education, Teachers College, Jeju National University, 61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 63294, Korea
Tel.: +82-64-754-4914, Email: namjepark@jejunu.ac.kr

Ⅰ. 서 론

데이터는 사회가 발전해감에 따라 기하급수적으로 급증하고 있으며, 급증하고 있는 데이터에 대하여 효과적으로 활용할 수 있는 기술을 빅데이터라 하며, 하나의 분야로서 현재의 융합기술 사회에 필요성이 강조되고 있다. 빅데이터 기술은 노인 가구와 1인 가구가 증가하고 있는 현대 사회에서 개인에 맞춰진 서비스 제공을 위해 다양한 분야에 적용되어 활용되고 있다. 특히 데이터에 기반한 서비스를 효과적으로 제공하기 위해 적용되는 인공지능은 정확성을 높이면서 수반되는 비용을 줄이는 효과적인 방안으로써 적용되고 있다[1][2]. 특히, 디바이스와 디바이스간의 통신을 기반으로 한 IoT(Internet of Things) 기술은 스마트홈과 같이 일상생활에서 데이터를 수집하고, 수집된 데이터를 기반으로 한 사용자 편의성 서비스를 제공 한다는 점에서 수집되는 데이터 간의 관계는 서비스를 사용하는 사용자와도 밀접한 관계를 가진다는 것을 확인할 수 있다. 따라서 데이터 간의 관계성은 학습 과정에서 유효한 지표가 될 수 있으며, GNN에서는 이러한 데이터 간의 관계를 벡터로 활용하여 학습을 수행한다[3]-[5].

통신 기술이 일상과 밀접한 영역에 점차 확장되어 데이터를 수집하는 영역이 다양해진다는 것은 사용자 서비스 제공에 있어 다양한 지표를 활용하여 세밀하게 분류하여 맞춤화된 서비스를 제공할 수 있음을 의미한다. 하지만 동시에 사용자의 개인 성향이나 취미, 나아가 사용자 위치와 같은 민감한 개인정보가 외부에 유출되어 사용자를 추정할 수 있는 정보로 활용될 수 있다는 위험성을 내포한다. 이처럼 사용자의 데이터에 기반한 서비스를 수행하는 경우, 데이터간의 관계성은 개인정보와 밀접한 관계를 가질 수 있다. 따라서 데이터와 관계 벡터를 포함하는 그래프 데이터는 외부 유출에 대한 대비가 요구된다[6][7].

또한, GNN에서의 학습 데이터는 그래프 데이터를 활용하며, 학습 과정에서 학습 데이터는 학습 모델의 신뢰성을 확보하기 위한 중요한 요소이다[8]. 머신 러닝에 대한 대표적 보안 취약점으로 언급되는 적대적 공격(Adversarial attack)의 중독 공격(Poisoning attack)과 회피 공격(Evasion attack)은 악의적인 데이터를 학습 데이터로서 활용하였을 때 발생하는 보안 취약점이다. 따라서 학습 데이터의 무결성을 강화하는 것은 안전한 학습 모델을 구축하기 위해 필수적인 요소가 된다.

본 논문에서는 GNN의 학습 환경에 적용 가능한 블록체인 기반의 데이터 관리 메커니즘을 제안한다. 제안하는 메커니즘은 학습 데이터를 수집하고, 그래프 데이터로 가공한 뒤, 학습 데이터셋을 블록 네트워크에 구축하기 위한 2차 가공을 수행한다. 이후, 블록 네트워크에 기록된 학습 데이터를 이용하여 GNN을 수행하는 과정에서 발생하는 학습 과정을 블록 네트워크에 기록하여 학습의 무결성을 강화하는 방안에 대해 제안한다.

Ⅱ. 관련 연구

2.1 Graph neural network

일반적인 RDB(Relational DataBase)의 경우 데이터의 관리 방식은 row와 column으로 구성된 2차원 구조의 행렬 방식으로 구성된다. RDB는 DB를 구성함에 있어 데이터 자체가 의미를 가지는 경우에 활용이 용이하나, 데이터간의 관계 분석에 활용하기에는 별도의 관계 구축을 위해 추가적인 비용과 자원의 소모가 요구된다[9]-[11]. GDB(Graph DataBase)는 데이터를 노드로 구축하고, 노드간의 연관관계를 설정하기에 데이터간의 연결 관계를 기반으로 한 새로운 연결 패턴이나 높은 연관성을 가지는 연결 패턴을 통해 추측을 수행할 수 있다는 장점을 가진다.

Graph Neural Network는 F. Scarselli, et al[12]에 의해 제안된 개념으로 일반적인 데이터에 대한 정보를 가지고 있는 노드(Node)와 노드간의 관계를 설정하는 벡터 등의 정보를 가지고 있는 엣지(Edge)를 활용하여 구성되는 그래프(Graph) 데이터를 활용하는 딥러닝 기법의 하나이다. GNN에서는 입력 데이터를 그래프 데이터의 노드로서 활용하며, 노드가 주변의 다른 노드와 연결되는 엣지를 이용한다[13]. 엣지는 입력 데이터에 대한 상태 정보로서 활용되어 이웃되는 노드를 갱신하고, 나아가 높은 강도를 가지는 그래프와 엣지를 통해 예측을 수행한다.

2.2 Adversarial attack

적대적 공격을 의미하는 Adversarial Attack은 학습 모델이 학습 과정에서 사람의 시각에서 발견이 불가능한 수준의 학습데이터 위·변조를 통해 최종적인 분류 결과를 달라지게 하는 취약점이다[14]. 적대적 공격은 공격자의 공격 목표에 따라 공격 대상이 되는 분류기에서 출력이 공격자에 의해 의도된 레이블로 변경하려는 표적 공격과 분류기의 출력 레이블에 대한 의도 없이 잘못된 레이블을 선택하도록 하는 비표적 공격으로 분류된다[15]-[17]. 적대적 공격은 학습 모델의 특정 과정에서 발생하는 공격에 대해 중독 공격과 회피 공격으로 분류할 수 있다. 중독 공격은 학습 모델에서 훈련을 수행하는 과정에서 임의의 적대적 사례를 학습함으로써 정상적인 학습의 수행을 방해하는 공격을 의미한다. 회피 공격은 학습이 완료된 학습 모델에 대해 적대적 사례를 입력하여 정상적이지 않은 결과를 도출하도록 하는 공격을 의미한다[18]. 또한 학습 모델의 신경망에 대한 사전 정보를 보유하고 있는 화이트 박스 공격과 공격 대상에 대한 아무런 정보 없이 공격을 수행하는 블랙 박스 공격으로 분류할 수 있다.

2.3 관련 연구 분석

블록체인을 활용한 그래프 데이터의 보안 연구는 다양한 방면에서 수행되어 오고 있다[19]. Yichuan의 연구[20]에서는 지식 그래프 구축 과정에서 프로세스 파일의 위변조에 의한 추론 결과 편향 문제로 인해 블록체인 기반의 프로세스 파일 저장 및 추적 가능성 방안을 제시하였다. Katarzyna의 연구[21]에서는 디지털 이미지를 해시 링크로 연결하는 암호화 구조를 제안하여 이미지에 대한 블록체인 기술을 적용하는 방안을 연구하였다. Gunasekaran의 연구[22]에서는 IoT 스마트 산업 데이터 공유를 위해 블록체인을 활용한 데이터 무결성 및 시퀀스 검증에 대한 연구를 수행하였다.

블록체인의 특성상 데이터 위변조에 대한 검증과 같은 무결성 강화를 목적으로 한 연구, 데이터의 추적과 같은 분야에서 활용되고 있다.

III. 그래프 학습 데이터 변조 방지를 위한 블록체인 기반 무결성 강화 메커니즘 제안

본 논문에서 제안하는 그래프 학습 데이터 변조 방지를 위한 블록체인 기반 무결성 강화 메커니즘은 일반적인 수집 데이터를 그래프 데이터로 가공하고, 그래프 데이터에서 발생하는 관계를 포함하는 모든 데이터를 2차원으로 가공하여 블록 네트워크를 기반으로 데이터 관리를 수행하는 메커니즘이다.

일반적으로 학습에 사용되는 데이터는 입력에 근거하여 결과를 도출할 수 있는 데이터로 특정 영역에서 활용되고 있는 문자나 단어, 그림과 같은 데이터를 활용할 수 있다. 본 논문에서 언급하는 학습 데이터는 하나의 고유한 객체로서 객체에 대해 서술할 수 있는 속성을 가진 데이터셋을 대상으로 한다. 따라서 수집 대상이 되는 데이터는 그래프의 구성 과정에서 각 노드를 정의할 수 있는 명칭과 해당 노드만이 가지는 고유한 개념인 속성을 가지며, 노드 간에 특정한 관계를 형성할 수 있다.

그림 1은 제안하는 메커니즘의 전반적인 개념을 보이는 것이다. 노드와 노드에 대한 속성, 노드간의 연결을 정의하는 엣지에 대한 정보는 1차적으로 GNN에서 활용하기 위한 그래프 데이터로 변환된다. 변환된 데이터는 그래프 데이터로서 노드와 속성의 관계, 노드와 노드의 관계를 기록하는 2개 이상의 관계형 데이터베이스로 구축될 수 있다. 이때, 구축되는 관계형 DB는 블록 네트워크에 기록하여 데이터의 무결성을 확인하기 위한 근거 데이터로 활용한다. 또한 GNN의 수행 과정에서 발생하는 노드 관계 데이터는 지속해서 업데이트되며, 업데이트되는 관계 데이터는 블록 네트워크의 거래 생성 과정에서 해당 내용을 추가한다.

본 논문에서 제안하는 메커니즘은 그림 2와 같이 데이터 수집 모듈, 데이터를 가공하고 보관하는 스토리지 서버 모듈, 학습을 수행하는 학습 모듈, 데이터의 무결성을 강화하기 위한 블록 네트워크 모듈의 4가지로 구성된다.

데이터 수집 모듈은 학습 대상에 맞춰 데이터를 정해진 형태로 수집하고 1차적인 가공을 수행하는 모듈을 의미한다.

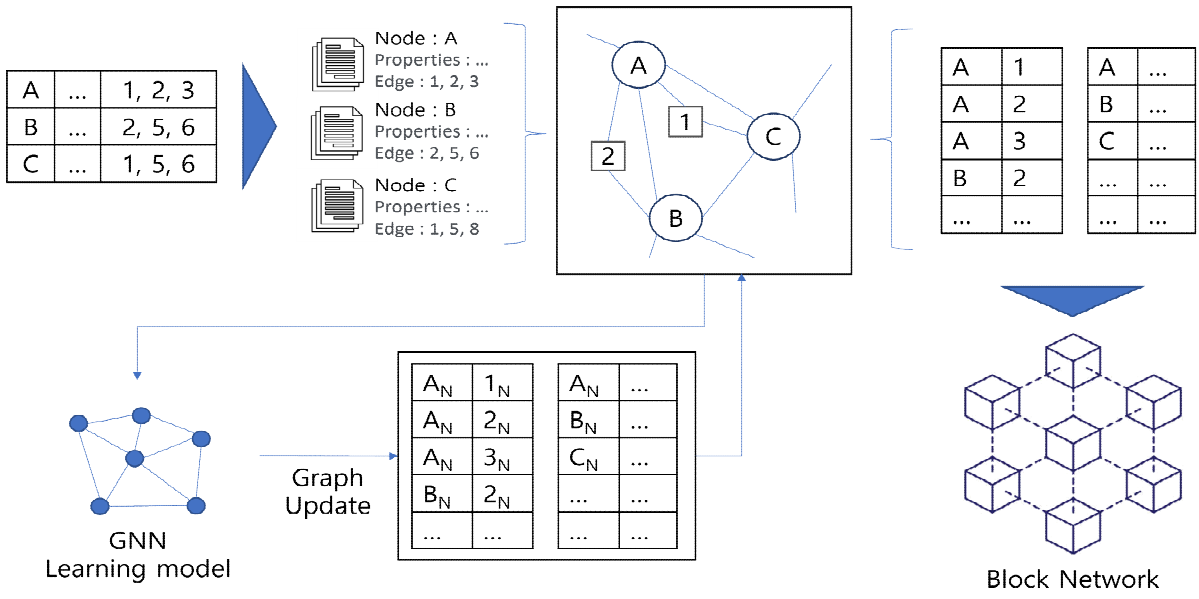


그림 1. 그래프 학습 데이터 변조 방지를 위한 블록체인 기반 무결성 강화 메커니즘 개념도
Fig. 1. Conceptual diagram of proposed blockchain-based integrity enhancement mechanism

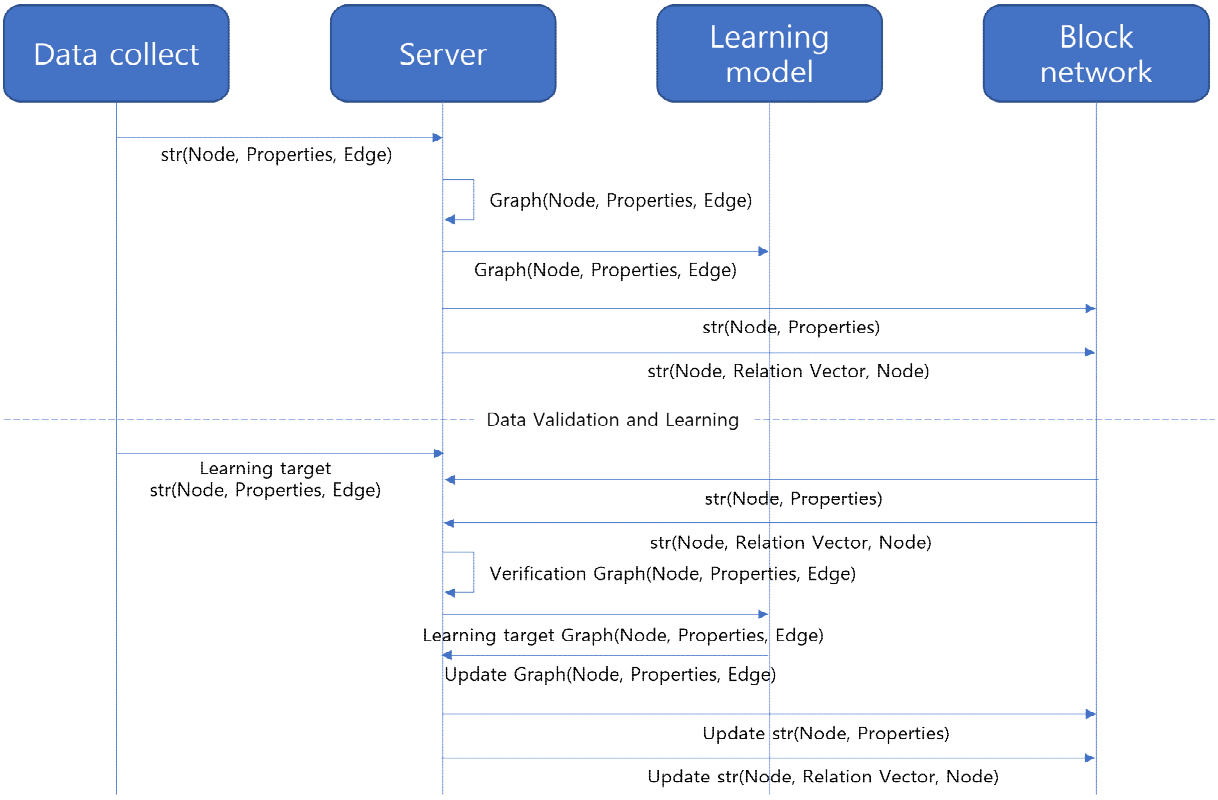


그림 2. 그래프 학습 데이터 변조 방지를 위한 블록체인 기반 무결성 강화 메커니즘 흐름도
Fig. 2. Proposed blockchain-based Integrity enhancement mechanism flowchart

스토리지 서버는 데이터 수집 모듈로부터 수집된 데이터를 학습을 수행하기 위한 그래프의 형태로 2차 가공을 수행하거나 그래프 데이터를 관계형 DB 구조에 맞춰 가공하여 블록 네트워크에 기록하는 역할을 수행한다. 학습 모델은 그래프를 이용한 학습 수행을 위해 GNN 기반의 학습을 수행한다.

이후 스토리지 서버 모듈에서는 1 epoch의 학습이 종료된 데이터를 기록하기 위해 업데이트된 노드의 정보를 관계형 DB 구조의 2차원 데이터로 변환하여 블록 네트워크에 기록한다. 각 학습의 수행하는 경우, 블록 네트워크에 기록되어있는 데이터와 구축된 그래프 데이터에 대한 비교 검증을 수행하여 무결성을 강화한다.

3.1 데이터 수집 모듈

데이터 수집 모듈은 학습 과정에서 사용되는 데이터를 수집하는 과정을 수행하는 모듈을 의미한다. 수집되는 데이터는 그 구조에 따라 다양한 방식으로 구성될 수 있으나 본 논문에서는 그래프 형식으로 구조를 제한하기 위해 하나의 노드를 정의할 수 있는 명칭과 정의된 노드에 속하는 요소, 노드와 노드간의 연결인 엣지를 생성하기 위한 관계 벡터의 3가지 요소로 1차적인 문자열 구성을 가진 데이터 셋 수집을 진행한다.

$$str(node, properties, edge) \tag{1}$$

식 (1)은 이 내용을 간략히 설명하는 것이다. 이처럼 수집된 데이터는 최초의 그래프 구성을 위한 데이터 또는 학습에 사용되는 데이터일 수 있다. 수집된 데이터는 학습의 수행을 위해 그래프 데이터로 변환되어야 하며, 이는 스토리지 서버 모듈에서 2차 가공을 수행한다.

3.2 스토리지 서버 모듈

스토리지 서버 모듈은 데이터 수집 모듈로부터 받은 데이터를 그래프 데이터로 가공하고, 가공된 데이터를 기반으로 학습을 수행하는 물리적 서버 역할과 데이터를 관계형 DB 구조에 맞춰 가공하여 블록 네트워크에 기록하고, 학습 과정에서 데이터의 무결성을 증명하기 위한 검증 역할을 수행하는 모듈을 의미한다. 스토리지 서버 모듈은 초기 학습용 그래프 데이터 구축 과정과 구축된 그래프 데이터에 학습 데이터를 추가하여 학습을 수행하는 과정의 두 가지로 분류할 수 있다. 초기 그래프 데이터 구축 과정은 데이터 수집 모듈로부터 받은 문자열 형태의 node, properties, edge를 그래프 데이터로 변환하는 과정을 수행한다. 그래프 데이터로 변환된 문자열 데이터는 아래의 그림 3과 같이 구성된다.

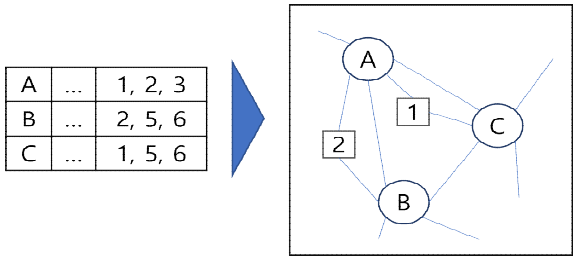


그림 3. 그래프 데이터 처리
Fig. 3. Graph data processing

이후 구축된 그래프는 블록 네트워크에 기록하기 위해 관계형 DB 구조에 맞춰 가공을 수행한다. 가공되는 데이터 구조는 노드의 개체명과 노드에 속하는 속성 정보를 가지는 (Node, Properties)와 각각의 노드와 노드를 연결하는 관계를 설명할 수 있는 (start Node, Relation Vector, end Node) 구조를 사용한다. Relation Vector는 start node와 end node의 연결 edge의 properties에 대한 내용을 포함한다. (Node, Properties)와 (start Node, Relation Vector, end Node)는 각각 별도의 블록 네트워크에 기록하며 학습을 수행하는 과정에서 그래프 데이터의 무결성을 검증하기 위한 검증 데이터로 활용된다. 학습 수행 과정에서 스토리지 서버 모듈은 블록 네트워크에 기록한 데이터를 받아 그래프 데이터 검증을 수행한다.

3.3 학습 모듈

학습 모듈은 GNN을 수행하는 학습 모델을 의미한다. 학습 모듈은 스토리지 서버 모듈에서 구축된 그래프 데이터를 활용하여 학습을 수행한다. 학습 데이터 구축 과정에서 학습 모듈은 학습 대상이 없으므로 별도의 기능을 수행하지 않는다. 학습 수행 과정에서 학습 모듈은 학습을 수행하며 그래프 노드간의 관계 변수값의 변화를 블록 네트워크로 전송하여 학습 수행 과정을 기록할 수 있도록 한다.

학습 수행 과정에서 발생하는 관계 변화는 노드와 노드간의 1차적인 직접 연결 이외에도 n개의 노드를 거쳐 연결되는 관계를 생성할 수 있다. 따라서 학습 수행과정에 대한 데이터는 ($node_n$, learning data, $node_{n-1}$)의 구조로 블록 네트워크에 기록한다.

3.4 블록 네트워크 모듈

블록 네트워크 모듈은 데이터를 기록하고, 요청에 따라 블록 데이터를 전송하는 것에 목적이 있다. 블록 네트워크 모듈은 (node, properties), (start node, relation vector, end node)와 학습 모듈에서 수행한 학습 결과인 ($node_n$, learning data, $node_{n-1}$)의 세 개의 결과에 대한 블록 데이터를 별도로 생성한다.

그림 4는 블록 네트워크 내의 블록 데이터 구조를 보이는 것으로, 별도의 블록 네트워크에 노드와 속성의 관계, 노드와 노드 및 관계 벡터, 노드와 학습 데이터의 변화 데이터의 3가지 데이터를 별도의 블록으로 기록하여 데이터의 무결성을 강화할 수 있다.

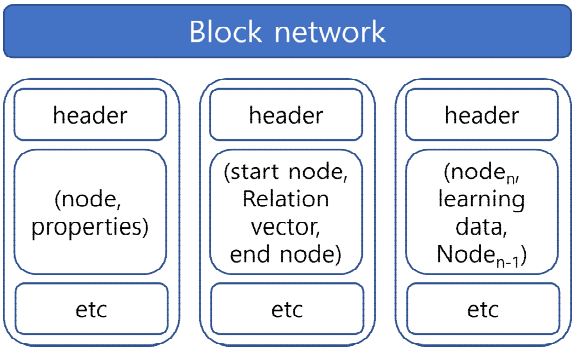


그림 4. 블록 네트워크 데이터 구조
Fig. 4. Block network data structure

IV. 보안성 분석

4.1 무결성 분석

본 논문에서 제안하는 메커니즘은 데이터의 무결성을 검증하기 위해 스토리지 서버 모듈과 블록 네트워크 모듈을 사용하여 2중의 데이터 구조를 가진다. 또한 블록 네트워크의 경우 분산 네트워크 방식으로 구성되므로 데이터에 대한 위변조 가능성을 낮출 수 있다. 학습 수행을 위한 그래프 데이터와 그래프 데이터의 관계 및 학습 수행에 따른 학습 데이터를 블록 네트워크로 기록하고, 학습을 수행하는 경우 먼저 블록 네트워크로부터 데이터를 요청하여 검증을 수행하므로 다중 데이터 기록 방식을 통한 무결성 강화와 동시에 학습 데이터와 블록 네트워크에 기록되어있는 데이터간의 차이가 있을 때 위변조 여부를 판별할 수 있다.

4.2 가용성 분석

본 논문에서 제안하는 메커니즘은 그래프 데이터베이스 구축과정과 데이터 학습 과정의 두가지 과정으로 구분할 수 있다. 그래프 데이터베이스 구축과정은 학습 모델 구축 전 최초의 학습 데이터를 구축하는 과정으로 1차적으로 그래프 데이터를 구축하고 2차적으로 구축된 그래프 데이터를 관계형 구조로 변환하여 블록 네트워크에 기록한다. 이 방식은 데이터 학습 과정에서도 동일한 방식을 유지하며 추가적으로 학습 모듈에서 학습 데이터를 블록 네트워크에 기록하는 방식을 추가한다. 따라서 실제 데이터를 관리하고 학습을 수행하는 물리적 서버 또는 학습 모델에 대한 에러 발생은 전반적인 시스템의 가용성을 훼손할 수 있으나, 블록 네트워크는 분산 네트워크 방식이기에 일부 네트워크에 대한 에러가 전체 네트워크에 대한 문제로 이어지지 않는다.

4.3 기밀성 분석

본 논문에서 제안하는 메커니즘은 데이터의 관리를 스토리지 서버 모듈과 블록 네트워크 모듈의 2개 모듈을 활용하여 수행한다. 일반적으로 물리적 서버는 단독으로 구성하여 외부망과 단절함으로써 제 3자의 접근 가능성을 낮출 수 있으나 제안하는 메커니즘에서는 데이터를 블록 네트워크를 통해 공유하므로 외부망 접근이 요구될 수 밖에 없다. 따라서 제 3자의 접근 가능성이 존재한다. 이와 같은 문제는 관리자에 의해 허가된 참여자만을 허용하는 프라이빗 블록체인 구조를 통해 폐쇄적 네트워크를 구축함으로서 방지할 수 있으나, 데이터의 위변조로부터 안전하지 않을 수 있다.

V. 결 론

데이터의 발생량은 현재에도 빠른 속도로 증가하고 있으며, 발생하는 데이터의 종류도 다양하다. 이처럼 급속히 증가하는 데이터의 효과적 활용을 위한 기술로 많은 분야에서 데이터 학습이 활용되고 있다. 특히 데이터의 학습 과정에서 데이터와 데이터의 관계가 중요한 역할을 하는 경우, 데이터를 하나의 점인 노드로 구성하여 노드와 노드에 관계를 설명하는 선으로 연결되는 그래프 데이터를 활용한다. 하지만 학습 데이터의 경우 학습에 사용되는 데이터 자체를 위변조하여 학습모델에 의도하지 않은 결과를 학습시키거나, 의도적으로 위변조된 데이터를 입력하여 학습 모델에서 의도하지 않은 결과를 도출하도록 하는 등의 학습 모델에 대한 공격이 발생함에 따라 학습 데이터의 무결성을 강화할 수 있는 방안이 요구된다.

본 논문에서는 데이터 학습 과정에서 발생하는 그래프 데이터와 학습 수행 과정에서 발생하는 학습 데이터를 관계형 데이터 구조로 가공하여 블록 네트워크에 기록하여 검증 데이터를 생성함으로써 2중 데이터 관리 구조를 활용한다. 또한 블록 네트워크에 기록된 데이터는 분산 네트워크에 포함되는 다수의 클라이언트에 의해 공유되므로 위변조 가능성을 낮출 수 있다. 향후, 입력된 데이터가 인증된 사용자에 의해 허가된 데이터임을 확인할 수 있는 방안의 연구를 수행하여 데이터의 신뢰성을 증명할 수 있는 연구를 수행할 예정이다.

References

[1] H. Lim, "Big Data Analysis for Strategic Use of Urban Brands: Case Study Seoul city brand ‘I SEOUL U’", Journal of KCA, Vol. 22, No. 1, pp. 197-213, Jan. 2022. https://doi.org/10.5392/JKCA.2022.22.01.197.

[2] Z. K. Lee and H. K. Nam, "A Literature Review Study in the Field of Artificial Intelligence (AI) Aplications, AI-Related Management, and AI Application Risk", Informatization Policy, Vol. 29, No. 2, pp. 3-36, Jun. 2022. https://doi.org/10.22693/NIAIP.2022.29.2.003.

[3] C. Guo, Z. Zhong, Z. Zhang, and J. Song, "NeurstrucEnergy: A bi-directional GNN model for energy prediction of neural networks in IoT", Digital Communications and Networks, Vol. 13, Sep. 2022. https://doi.org/10.1016/j.dcan.2022.09.006.

[4] J. Kim and N. Park, "Blockchain-based data-preserving ai learning environment model for ai cybersecurity systems in iot service environments", Applied Sciences, Vol. 10, No. 14, Jul. 2020. https://doi.org/10.3390/app10144718.

[5] J. Kim, S. Ryu, and N. Park, "Privacy-Enhanced Data Deduplication Computational Intelligence Technique for Secure Healthcare Applications", Computers Materials Continua, Vol. 70, No. 2, pp. 4169-4184, Jan. 2022. http://dx.doi.org/10.32604/cmc.2022.019277.

[6] J. C. Park, "Delegated Provision of Personal Information and Storage of Provided Information on a Blockchain Ensuring Data Confidentiality", Korean Institute of Smart Media, Vol. 11, No. 10, pp. 76-88, Oct. 2022. http://dx.doi.org/10.30693/SMJ.2022.11.10.76.

[7] J. Kim and N. Park, "A face image virtualization mechanism for privacy intrusion prevention in healthcare video surveillance systems", Symmetry, Vol. 12, No. 6, Jun. 2020. https://doi.org/10.3390/sym12060891.

[8] S. Y. Lee , K. Hyun, B. K. Kim, and H. S. Kim, "A Study on the Two-Dimensional Graph Data and Its Effectiveness in Human Behavior Classification Deep Learning", Journal of KIIT, Vol. 19, No. 6, pp. 21-28, Jun. 2021. https://doi.org/10.14801/jkiit.2021.19.6.21.

[9] J. Wu, et al., "CarbonAI, A Non-Docking Deep learning based small molecule virtual screening platform", Theoretical and Computational Chemistry, Vol. 1, Dec. 2022. https://doi.org/10.26434/chemrxiv-2022-gk3n6.

[10] S. Liu, D. Vazquez, J. Tang, and P. A. Noël, "Flaky Performances when Pretraining on

Relational Databases", Computer Science:Machine Learning, Nov. 2022. https://doi.org/10.48550/arXiv.2211.05213.

[11] J. Kim and N. Park, "De-Identification Mechanism of User Data in Video Systems According to Risk Level for Preventing Leakage of Personal Healthcare Information", Sensors, Vol. 22, No. 7, Mar. 2022. https://doi.org/10.3390/s22072589.

[12] F. Scarselli, et al., "The Graph Neural Network Model", IEEE Transactions on Neural Networks, Vol. 20, No. 1, pp. 61-80, Jan. 2009. https://doi.org/10.1109/TNN.2008.2005605.

[13] J.-Y. Kim, J. Seon, and S.-H. Yoon, "Classification Method based on Graph Neural Network Modelfor Diagnosing IoT Device Fault", The Journal of IIBC, Vol. 22, No. 3, pp. 9-14, Jun. 2022. http://doi.org/10.7236/JIIBC.2022.22.3.9.

[14] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. Goodfellow, and R. Fergus, "Intriguing properties of neural networks", Evolutionary Computing, Dec. 2013. https://doi.org/10.48550/arXiv.1312.6199.

[15] H. Kim, D. C. Jung, and B. W. Choi, "Exploiting the Vulnerability of Deep Learning-Based Artificial Intelligence Models in Medical Imaging: Adversarial Attacks", The Korean Society of Radiology, Vol. 80, No. 2, pp. 259-273, 2019. http://doi.org/10.3348/jksr.2019.80.2.259.

[16] J. Kim, D. Lee, and N. Park, "CCTV-RFID enabled multifactor authentication model for secure differential level video access control", Multimedia Tools and Applications, Vol. 79, No. 31, pp. 23461-23481, Jun. 2020. https://doi.org/10.1007/s11042-020-09016-z.

[17] S. Park, S. Kim, H. Yoon, and D. Choi, "Adversarial Example Detection Based on Symbolic Representation of Image", Journal of KIISC, Vol. 32, No. 5, pp. 975-986, Oct. 2022. https://doi.org/10.13089/JKIISC.2022.32.5.975.

[18] H. Oh, "Research Trends in Image-Based Adversarial Case Generation Technology", Journal of KIISC, Vol. 30, No. 6, pp. 107-115, 2020.

[19] T. Kim, et al., "Integrity Support System for Blockchain-based explainableCCTV Video", The Journal of IIBC, Vol. 21, No. 3, pp. 15-21, Jun. 2021. http://doi.org/10.7236/JIIBC.2021.21.3.15.

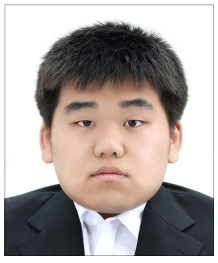
[20] Y. Wang, X. Yin, H. Zhu, and X. Hei, "A Blockchain Based Distributed Storage System for Knowledge Graph Security", Artificial Intelligence and Security, Vol. 12240, pp. 318-327, Sep. 2020. https://doi.org/10.1007/978-3-030-57881-7_29.

[21] B. L. V. V. Kumar and K. R. Kumar, "WITHDRAWN: Image integrity verification using blockchain", materialstoday:proceedings, Dec. 2020. https://doi.org/10.1016/j.matpr.2020.10.864.

[22] G. Manogaranm, et al., "Blockchain Assisted Secure Data Sharing Model for Internet of Things Based Smart Industries", IEEE Transactions on Reliability, Vol. 71, No. 1, pp. 348-358, Mar. 2022. https://doi.org/10.1109/TR.2020.3047833.

저자소개

김 진 수 (Jinsu Kim)



2019년 9월 ~ 현재 : 제주대학교 융합정보보안학협동과정 박사과정
2018년 9월 ~ 현재 : 제주대학교 사이버보안인재교육원 연구원
관심분야 : 클라우드, 지능형 영상감시 시스템, IoT

박 남 제 (Namje Park)

2008년 2월 : 성균관대학교 컴퓨터공학과(공학박사)
2003년 4월 ~ 2008년 12월 : ETRI 정보보호연구단 선임연구원
2009년 1월~ 2010년 8월 : UCLA Post-Doc., ASU Research Scientist
2010년 9월 ~ 현재 : 제주대학교 교육대학 초등컴퓨터교육전공 교수, 대학원 융합정보보안협동과정 교수
관심분야 : 정보교육, STEAM, 정보보호, 암호이론