원격교육 학습데이터 가중치에 따른 DID 메타데이터 처리방법 연구

민연아O
O한양사이버대학교 응용소프트웨어공학과
e-mail: yah0612@hycu.ac.krO

A study on DID metadata processing method according to distance learning data weight

Youn-A MinO
ODept. of Applied SW Engineering, Hanyang Cyber University

● 요 약 ●

본 논문에서는 블록체인 기반 DID기술을 이용하여 원격교육에서 발생하는 학습데이터를 효율적으로 관리하기 위한 방법으로, 학습데이터 가중치를 고려한 DID 메타데이터관리방법을 제안하였다. 메타데이터의 식별자에 대하여 특정위치로 데이터 가중치를 검색하도록 하고 해당 가중치에 따라 처리방법을 다양화 할 수 있다. 본문에서는 블록체인의 Zero Knowledge Proof 방식 처리에 차별화를 두어 메타데이터를 처리하였으며 데이터 처리속도 및 데이터관리에 효율성높일 수 있다.

키워드: 블록체인, DID, 메타데이터, 원격교육

I. Introduction

다양한 사회적 환경에 의해 원격교육에 대한 관심이 높아짐에 따라 원격교육의 학습환경에 대한 정확성과 인증의 투명성에 대한 관심이 높아지고 있다[1].최근에는 인공지능, 빅데이터뿐 아니라 블록체인 기술 기반 신기술을 원격교육에 적용하여 학습데이터의 인증 및 이력관리에 적용하고 있다[2].블록체인을 이용한 학습이력에 대한 중요성도 증가하고 있다. 블록체인 기술은 네트워크에 포함된 노드 간 원장을 공유하는 분산공유원장 기술을 기반으로 하며 블록에 저장된 데이터에 대한 정확한 관리를 통한 데이터의 투명성과 무결성 및 정확성을 보장한다[2,3]. 블록체인 기술 기반의 DID는 분산 인증이 가능한 기술이며 블록체인 기술을 기반으로 데이터의 정확성과 무결성 및 신뢰성을 보장할 수 있다[3,4].본 논문에서는 블록체인 기반 DID 기술을 이용하는 학습환경에서 데이터를 효율적으로 관리하기 위한 방법으로 학습데이터 가중치를 고려한 메타데이터의 처리방법을 방법을 제안한다.

II. Preliminaries

1. Related works

DID는 블록체인 기반 탈중앙화된 분산 신원인증이 가능한 기술이다. 개인정보를 개인의 단말기에 저장하여 인증이 필요한 경우, 필요한 정보만 골라 제출하는 기술이며 개인이 자신의 데이터를 주도적으로 관리할 수 있다. DID의 투명성과 정확성 및 자기주도성에 대한 장점에 힘입어 최근 운전면허증, 디지털 뱃지 등에 활용되고 있다. Fig.1은 금융결제원에서 제시한 DID모델 기본구조에 대한 이미지이다[5].

Fig. 1. DID 모델 기본 구조

Fig.1에서는 특정 기관이 사용자에게 이력을 요청하였을 때 사용자는 발급기관으로부터 이력을 발급받아 제출하고 특정 기관은 분산ID를 통해 제출된 이력을 검증하는 과정을 거친다.

Table.1은 DID의 사용을 위해 검증하는 DID 문서의 일부를 나타낸다.

Table 1. DID 문서의 일부

```
{
  "@context": "https://w3id.org/did/v1",
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    // used to authenticate as did:...fghi
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "RsaVerificationKey2018",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyPem": "-----BEGIN PUBLIC
KEY...END PUBLIC KEY-----₩r₩n"
  }],
  "service": [{
    ...
  }]
}
```

본 논문에서는 데이터의 가중치를 고려한 DID의 메타데이터를 처리를 통해 데이터 가중치에 따른 데이터 처리의 효율과 데이터 신뢰를 높이는데 주안점을 두어 연구한다.

III. The Proposed Scheme

블록체인기술기반 DID에서 식별자로 메타데이터를 검색하여 주민등록증처럼 식별자의 특정 위치로 데이터의 가중치를 정하고, 가중치에 따라 데이터 암호화 방법을 차별화 한다.

Table.2는 DID에서 메타데이터에 가중치를 부여하는 알고리즘을 슈도코드로 나타낸 것이다.

Table 2. 제안 내용에 대한 알고리즘

```
Set variables to set weights according to data
location (structure)
Map identifiers to metadata as keys
Register metadata
Data encryption (encryption level adjusted according
to data weight)
  if (metadata. weight >= α) {
        return strongEncryption(data);
    } else {
        return weakEncryption(data);
    }
```

Table.2의 알고리즘에 의해 데이터 위치에 따른 가중치 설정을 위한 변수를 구조체로 정의하고 식별자를 키로 메타데이터에 매핑하여 데이터 가중치에 따라 암호화 수준을 조정하는 과정을 거친다.

제안한 논문에 대해 성능평가 하기 위해, 데이터의 크기를 달리하고 각 데이터셋에 대하여 10만개로 제한하여 실험하였다. Hyperledger Indy기반 라이브러리를 사용하여 1개의 channel, 2개의 organization, 2개의 peer(기관당 1개)를 사용하여 Oderer를 구성하여 성능평가를 실시하였다. 거래처리성능에 대하여 Write와 Reponse로 나누어 평가하였으며 결과는 다음과 같다.

Table 3. 성능평가 결과

Data	Write(TPS)	Response(ms)
1~4Kb	270	101
5~10Kb	282	162
10kb이상	300~391	200~498

위의 성능평가에 따라 일반적인 거래처리 대비 성능이 9% 이상 향상됨을 확인하였다.

IV. Conclusions

본 논문은 DID기반 데이터 관리 시 데이터의 가중치에 따라 메타데이터를 처리하였다. 본 논문의 제안에 따라 Write와 Response에 대한 성능을 평가하였으며 일반적 거래상황대비 9~10% 정도의 성능 향상을 확인하였다. 데이터의 특성과 네트워크 환경에 따라 성능평가의 결과에 차이가 있을 수 있으므로 향후 다양한 데이터셋과 환경에 따른 보편적인 성능향상을 위해 연구할 예정이다.

REFERENCES

[1] Wang, Ke, “Analysis of Blockchain Consensus.”, Dissertations Abstracts International, 2021, pp.153=155

[2] Youn-A Min, " Study on Efficient Data De-Identification Method for Blockchain DID", International Journal of Internet, Broadcasting and Communication, Vol. 13, Issue 2, pp. 60-66

[3] Kim, B.G, "A Security Analysis of Blockchain-Based Did Services", IEEE, pp.22894 - 22913, 2021.

[4] Ntefua Saah et al., "Blockchain technology in the AEC industry", Available : https://www.sciencedirect.com/science/article/abs/pii/S235271022300788X?via%3Dihub

[5] Etnews : https://www.etnews.com/20220714000023