안전한 디지털 학습데이터 처리를 위한 DID 연구

백영태*, 민연아O
*김포대학교 멀티미디어과,
O한양사이버대학교 응용소프트웨어공학과
e-mail: hannae@kimpo.ac.kr*, yah0612@hycu.ac.krO

A study on DID for enhanced digital learning data security

Yeong tae Baek*, Min Youn-AO
*Dept. of Multimedia, Kimpo University,
ODepartment of Applied Software Engineering, Hanyang Cyber University

● 요 약 ●

스마트 디바이스 발전과 다양한 환경적 요인에 의해 온라인 학습에 대한 요구가 증가함에 따라 온라인 학습환경에서 발생하는 개인의 학습이력에 대한 투명하고 안전한 관리에 대한 요구가 증가하고 있다. 본 논문에서는 안전한 디지털 학습이력관리를 위한 방법으로 블록체인 DID처리 방법을 연구한다.

키워드: 온라인 학습환경(online learning environment), 블록체인(Blockchain), DID(decentralized identity)

I. Introduction

DID는 기존의 중앙집중적으로 관리되던 신원인증 방식을 탈피하여 탈중앙화된 블록체인 기반 네트워크에서 분산신원확인이 가능한 차세대 인증기술이다[1]. 현재 DID기술은 통신사와 카드사 및 금융업에서 신원인증을 기반으로 한 시범적 서비스가 많이 적용되고 있으나 블록체인기술이 가진 투명성과 무결성 보장이라는 장점을 활용할 수 있는 다양한 영역으로의 확산적용에 대한 관심이 높아지고 있다[1,2].

본 논문에서는 온라인 학습 환경에서 중요한 관리 요소인 개인의 학습 데이터 관리에 대하여, 신뢰성과 효율성을 높이기 위한 방법으로 DID 처리방법을 제안하였다.

II. Preliminaries

1. Related works

1.1 DID

각종 데이터의 DID 처리 시 Fig. 1과 같은 데이터 처리가 진행된다. ISSUER는 소유자의 신원을 검증하고 신원정보를 발급하며 발급내역에 대하여 블록체인을 통하여 분산 저장한다. 사용자는 신원정보 발급을 요청할 수 있다. 서비스 제공자는 사용자로부터 전달받은 신원정보를 블록체인을 통하여 검증 가능하다[3,4,5].

ISSUER (Issuing Authority)	user (individual)	Service Provider (Verifier)
Owner's identity verification Issuance of identity information	Identity information management through e-wallet Request for issuance of identity information	Verification of identity information received from users

Fig. 1. DID process[3]

III. The Proposed Scheme

본 논문에서 제안한 처리방법에 대한 의사코드는 표 2와 같다. 표 2의 내용은 신원정보 인증요청과정을 통해 ID정보를 등록하고, 등록된 ID정보를 통해 DIDs(key)-DID Document를 생성한 후, 요청한 신원정보를 전달하고, DIDs를 통해 DID Document 검증을 통해 요청 내용의 신뢰성을 검증하는 과정을 거친다.

Table 1. System Environment

Handling requests: - Identity information authentication request: Service provider to user - Request for issuance of identity information: User to identity information issuer such as certification authority ID information registration: If ID information registration is possible : -Registration of signed ID information - DIDs (Key) — Create DID Document (Value): The identity information issuer issues identity information to the user Transfer of identity information: If the identity information request is successful : - Delivering identity information selected only in part necessary for authentication to the service provide - Complete identity verification

표 3은 표 2의 과정에서 PKI 생성을 위해 작성한 코드의 일부이며 elliptic.p224, elliptic.P384(), elliptic.P521()를 사용한다.

Table 2. System Environment

```
...
import (
        "crypto/ecdsa"
        "crypto/elliptic"
        "crypto/rand"
        "fmt"
        "log"
)

func main() {
        pvKey,                  err                  :=
ecdsa.GenerateKey(elliptic.P256(), rand.Reader) /

        if err != nil {
                //error message print
        }
        pbKey := &pvKey.PublicKey
        / cpbKey.X.Bytes(), pbKey.Y.Bytes() print
...
}
```

IV. Conclusions

온라인 학습 환경의 확산에 따라 학습 환경에서 발생하는 다양한 학습데이터가 발생한다. 온라인 학습 시 발생하는 데이터의 안전한 관리를 통한 투명한 학습경력관리가 필요하며 본 논문에서는 학습데이터의 안전한 관리를 위한 방법으로 DID 처리를 제안하였다. 본 논문의 제안을 통하여 온라인 학습자의 학습데이터에 대한 신뢰성을 보장하고, 학습플랫폼 기관차원에서는 안전한 정보 관리의 효율성을 높일 수 있다.

REFERENCES

[1] D. Reed et al., “Decentralized Identifiers (DIDs) v1.0, Core Data Model and Syntaxes,” W3C Working Draft 09 December 2019; https://www.w3.org/TR/did-core/.

[2] NISTIR 8053, De-Identification of Personal Information, 2015.

[3] Gabizon, Ariel, Zachary J. Williamson, and Oana Ciobotaru. PLONK: Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge. Cryptology ePrint Archive, Report 2019/953, 2019.

[4] Gabizon, Ariel, Zachary J. Williamson, and Oana Ciobotaru. PLONK: Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge. Cryptology ePrint Archive, Report 2019/953, 2019.

[5] https://byline.network/2022/06/7-139/