스마트 컨트랙트 기반 개인정보 관리권한 연구

백영태[O], 민연아[*]
[O]김포대학교 멀티미디어과,
[*]한양사이버대학교 응용소프트웨어공학과
e-mail: hannae@kimpo.ac.kr[O], yah0612@hycu.ac.kr[*]

Smart contract-based personal information management

Baek YeongTae[O], Min Youn A[*]
[O]Dept. of Multimedia, Kimpo University,
[*]Dept. of Applied Software Engineering, hanyang cyber University

● 요 약 ●

스마트 디바이스 등 디지털 환경의 변화가 가속화되며 온라인을 통한 개인정보 관리에 대한 관심이 높아지고 있다. 개인정보를 다루는 플랫폼마다 다양한 개인정보 접속 가능자가 존재하며 블록체인 기반 스마트 컨트랙트를 이용하여 개인정보의 관리권한에 대한 유연한 관리 및 개인정보 관리 이력을 투명하게 관리할 수 있다. 본 논문을 통하여 블록체인 기술의 스마트 컨트랙트 기반 데이터 사용 및 관리권한에 대한 규칙을 설정하고 유연하게 수정하여 개인정보를 안전하고 투명하게 관리할 수 있다.

키워드: Personal information, smart contract, blockchain, data management rights

I. Introduction

스마트 디바이스의 사용이 증가되며 디지털 환경의 발전에 힘입어 온라인을 통한 개인의 다양한 정보가 쉽게 노출될 수 있다. 쇼핑, 온라인 및 금융 거래 등 다양한 플랫폼에서 쉽게 접근 가능한 개인정보에 대한 분산저장 및 투명한 관리와 선택적 암호화 처리를 위해 본 논문에서는 블록체인 기반 데이터 관리 및 선택적 암호화 처리에 대하여 연구한다.

II. Preliminaries

1. Related works

블록체인은 기록된 데이터의 변경 불가능 및 데이터 조작과 위조 방지를 위해 널리 사용되는 분산원장 기술로써 데이터의 투명한 관리와 데이터 이력의 추적이 용이한 기술이다[1].

암호화 기술을 사용하여 개인정보 등의 민감 데이터에 대한 보안 및 안정성을 높이는데 기여할 수 있으며 블록체인 기술 기반 스마트 컨트랙트를 통해 데이터 사용 및 관리권한에 대한 유연한 규칙을 관리할 수 있다[2].

블록체인 기술을 활용한 기업의 개인정보 보호 사례가 증가하고 있다. 디센트럴라이즈드 파이낸스(DeFi)는 Chainalysis, Circle, Algorand 같은 회사들이 전통 금융과 분산 금융을 연결하고, 암호화폐 거래와 차세대 도구 사용을 안전하게 지원하고 있으며 Santander는 영국에서 최초로 블록체인을 도입하여 국제 결제 서비스 보안 및 유럽과 남미의 Santander 계좌 간 안전한 자불을 보장한다. Barclays는 자금 이체의 보안을 강화하기 위해 블록체인 기술사용. 고객의 개인 식별 정보를 블록체인에 저장하기 위해 Know-Your-Customer 특허를 보유하고 있다. Philips Healthcare는 AI와 블록체인을 함께 사용하여 병원과 협력하여 운영, 관리 및 의료 데이터의 인사이트를 분석한 후, 수집 데이터 보호를 위해 블록체인을 사용한다. MEDICALCHAIN은 환자와 의료 전문가들이 블록체인 기술 기반으로 환자 데이터에 쉽게 접근할 수 있도록 하며 전자 건강 기록의 저장소를 생성하여 환자와 의료 그룹에게 정확한 정보검색을 제공한다. 국방 방위보안업체인 Lockheed Martin은 기술 시스템, 공급망 위험 관리 및 소프트웨어 개발에서 블록체인 사이버보안 프로토콜 조치를 구현한다[3,4].

개인정보 가명화를 위한 다양한 암호화 기법이 존재하며 대표적으로 대칭키 암호화 기법과 비대칭키 기법, 해시함수 기법으로 나눌 수 있다. 본 논문에서는 ms-sql 기반, 개인정보를 관리하는 대다수 기업에서, RSA 암호화 기법을 이용하여 개인정보를 가명화하고 관리자, 사용자(등급별) 개인정보의 노출 정보를 제한하는 스마트 컨트랙트를 작성하여 다양한 위협 환경에서 개인정보의 보안 가능성을 조사하였다.

III. The Proposed Scheme

본 연구에서 다루는 RSA를 이용한 ms-sql의 데이터 가명화 과정을 나타내면 Fig. 1과 같다.

```
# import packages(pyodbc cryptography)
# Generate a pair of RSA keys
private_key = rsa.generate_private_key(
        ...
        backend=default_backend()
)public_key = private_key. public_key()
# Database connection
conn = pyodbc.connect('DRIVER=...)
# Personal information encryption and update
# Update encrypted information
# Commit and exit
```

Fig. 1. RSA-based data pseudonymization process

위의 과정을 통해 전달된 가명 데이터를 연결하여 Ethereum 기반 스마트 컨트랙트를 사용한 접근 제어 과정을 보여주며 이 단계를 통해 관리자와 수준별 사용자를 구분하여 각 사용자별 특정 데이터(개인정보 등)에 대한 접근 권한을 유연하게 관리할 수 있다.

Fig. 2는 스마트 컨트랙트 기반 권한 설정 과정 슈도코드로 나타낸 것이다.

```
#1 :contract settings
contract PersonalInfoAccess {
        address public admin;
        constructor() {
            admin = msg.sender; // Set the person distributing
the contract as administrator
        }
#2 : modifier for administrator settings
modifier T_Admin() {
            require(msg.sender == admin, "Access denied: Only
admin can access.");
            _; }
#3 : modifier for setting weight for each user
//Personal information return logic through administrator
#4 : When changing administrator
function changeAdmin(address newAdmin) public
onlyAdmin {
            admin = newAdmin;       }}
```

Fig. 2. Smart contract-based permission setting process

Fig. 1과 2의 과정을 통해 데이터 암호화 및 유연한 관리자 설정과 사용자별 가중치 설정을 통한 사용자별 개인정보 활용 정도를 제한할 수 있다.

실험을 위해 Apache JMeter를 활용하여, 개인정보로 가정할 수 있는 데이터셋을 기반으로 가명화 단계를 가정하고 권한 설정 이전(A)과 권한 설정시에 대하여 3~5개 그룹의 권한을 가정하여 해당연구 내용을 적용 및 TPS를 측정하였으며 결과 8% 이상 성능이 향상됨을 확인하였다.

Fig. 3. Experimental dataset [5]
(National Health Insurance Corporation_Health checkup information)

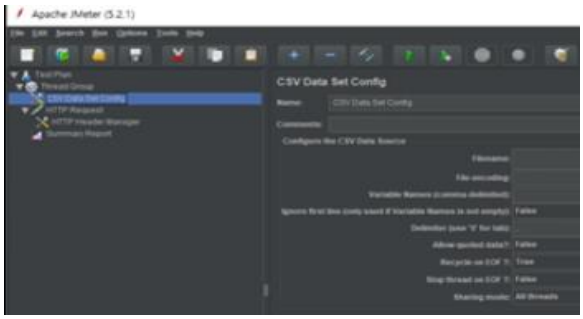

Fig. 3. JMeter data input process

IV. Conclusions

개인정보를 다루는 플랫폼마다 다양한 개인정보 접속 가능자가 존재하기 때문에 개인정보에 대한 보호 측면과 관리 측면의 투명성이 필요하다. 블록체인 기반 스마트 컨트랙트를 이용하여 개인정보의 관리권한에 대한 유연한 관리 및 개인정보 관리 이력을 투명하게 관리할 수 있다. 본 논문을 통하여 블록체인 기술의 스마트 컨트랙트 기반 데이터 사용 및 관리권한에 대한 규칙을 설정하고 유연하게 수정하여 개인정보를 안전하고 투명하고 관리하도록 하였으며 동일 가명화 알고리즘 적용을 전제로 권한설정 전과 후에 대한 성능평가를 실시한 결과 8% 이상 성능이 향상됨을 알 수 있다. 본 연구 과정에서 발생 가능한 데이터 백업의 오류 등은 고려하지 않았으며 데이터셋의 다양성을 고려하지 않았기 때문에 향후 보다 확장성 있는 연구가 필요하다.

REFERENCES

[1] Youn-A Min, “A Study on the Processing Method of pseudonym information considering the scope of data usage”, Journal of The Korea Society of Computer and Information Vol. 26 No. 5, pp.17-22

[2] Hans, Jaqueline, et al., “Blockchain CBDC Security Threats Using STRIDE”, 2023 Fifth International Conference on Blockchain Computing and Applications (BCCA) Blockchain Computing and Applications (BCCA), 2023 Fifth International Conference on. :522-529 Oct, 2023

[3] "How Blockchain Technology Ensures Data Privacy [Guide 2023]" : https://ambcrypto.com/blog/how-blockchain-technology-ensures-data-privacy-guide-2023/

[4] “recent examples of companies using blockchain for personal data protection 2023 : https://bootcamp.berkele

y.edu/blog/blockchain-use-cases/

[5] https://www.data.go.kr/data/15007122/fileData.do?recommendDataYn=Y

[5] https://www.data.go.kr/data/15007122/fileData.do?recommendDataYn=Y