Journal of KIIT. Vol. 17, No. 9, pp. 113-121, Sep. 30, 2019. pISSN 1598-8619, eISSN 2093-7571 113
http://dx.doi.org/10.14801/jkiit.2019.17.9.113

스마트 컨트랙트를 적용한 역할 기반 접근 제어 기반 파일 접근제어 메커니즘

김진수*, 박남제**

Role Based Access Control based File Access Control Mechanism with Smart Contract

Jinsu Kim*, Namje Park**

이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임[2019-0-00203,선제적 위험대응을 위한 예측적 영상보안 핵심기술 개발]. 그리고 2019년도 정부(교육부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(과제번호:NRF-2019R1I1A3A01062789)

요 약

최근 내부자에 의한 정보 유출이 큰 화제가 됨에 따라 접근권한을 벗어나는 정보에 대한 접근을 제어할 수 있는 방안이 요구되고 있다. 하지만 악의적인 내부자에 의한 보안 위협의 경우 고의적으로 정보를 유출하며, 데이터를 복사해도 외부적으로 보이는 특징이 없는 디지털 데이터의 특성상 명확히 구분할 수 있는 방안은 전무하다는 문제가 존재한다. 본 논문에서는 데이터에 접근을 요청하는 데이터에 대한 접근 권한과 사용자의 정보를 블록데이터에 기록함으로서 무결성이 보장되는 사용자의 접근 권한 정보와, 접근 기록을 저장하는 메커니즘을 제안한다. 제안된 메커니즘은 역할에 따라 접근을 제어하는 RBAC(Role Based Access Control)를 적용하여 블록데이터에 기록되어있는 사용자의 역할을 이용하여 데이터에 대한 접근을 제어하고, 사용자의 접근 데이터를 기록하는 메커니즘으로 스마트 컨트랙트를 활용하는 하나의 방안을 제안한다.

Abstract

Recently, information leakage by insiders has become a hot topic, and there is a need to control access to information beyond access rights. However, in the case of security threats caused by malicious insiders, there is a problem that information is leaked intentionally and there is no way to distinguish clearly by the characteristics of digital data that do not have external features when data is copied. In this paper, we propose a mechanism to store user 's access right information and access record which are guaranteed integrity by recording access right to data requesting user and user' s information in block data. The proposed mechanism applies RBAC(Role Based Access Control) to control access according to role. Then, Access to the data is controlled using the role of the user recorded in the block data. Then, we propose a way to utilize smart contract as a mechanism for recording the access data of the user.

Keywords
role based access control, block data, smart contract, access authority, insider threat

* 제주대학교 대학원 컴퓨터교육학과 박사과정
- ORCID: https://orcid.org/0000-0003-1009-3928
** 제주대학교 초등컴퓨터교육전공, 융합정보보안학과 교수(교신저자)
- ORCID: https://orcid.org/0000-0003-4434-8933

· Received: Jul. 22, 2019, Revised: Sep. 18, 2019, Accepted: Sep. 21, 2019
· 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

인터넷의 급격한 발전에 따라 점차 디지털화 되어가는 사회상에 의해 기존의 아날로그 방식에서 디지털 방식을 적용함에 따라 물리적 보안만이 요구되었던 과거와 달리 디지털 자료에 대한 보안성이 강조되고 있으며, 특히 디지털 자료에 대한 권리가 없는 사용자에 의해 침해되는 것이 큰 문제가 되고 있다[1]-[3]. 여기서 사용 권한이 없는 사용자는 자료와 관계가 없는 외부자일 수도 있으나 자료와 밀접한 관계를 가지고 있는 내부자일 가능성 또한 존재한다[4]-[6]. 내부자에 의한 정보 유출은 보안의 난이도가 급격히 상승하며, 일반적으로 장기적 진행이 요구되는 프로젝트의 특성상 내용의 유출은 기업에 대해 큰 피해를 가져올 수 있다[6][7].

본 논문에서는 파일에 대한 접근 권한을 블록에 기록하고, 사용자에 의해 자료에 접근 요청이 발생할 경우에 블록에 기록된 사용자의 역할에 기반한 접근 허가를 진행하며, 일정 기간 내에 요청한 기록을 블록에 추가함으로서 자료에 대한 접근 기록을 관리함으로서 자료가 외부에 유출될 경우, 유출 경로를 추적할 수 있는 하나의 방안이 될 수 있는 메커니즘을 제안한다.

Ⅱ. 관련 연구

2.1 스마트 컨트랙트

스마트 컨트랙트의 개념은 1996년 Nick Szabo에 의해 제안되었으며, 작성되어 있는 디지털상의 계약조건이 만족되면 자동적으로 계약을 실행하는 방법을 의미한다[8][9]. 하지만 계약에 대한 신뢰성을 보장하기 어려웠으며, 계약조건의 무결성을 보장하기 어렵다는 단점으로 인해 실현에 어려움이 존재하였다[10]-[12].

이와 같은 문제를 데이터에 대한 무결성을 보장하는 블록체인 기술이 제안됨에 따라 계약 조건과 계약에 대한 신뢰성을 확보할 수 있게 되었으며, 정해진 조건에 의해 계약을 수행하기 때문에 계약에 요구되는 중계 과정이 간략화 되었다[13][14]. 또한, 실시간에 가까운 거래가 가능하게 되었으며, 중계 과정의 간략화에 따라 수수료를 절감할 수 있게 되었다[15][16].

2.2 RBAC

RBAC(Role-Based Access Control)은 사용자의 접근을 제어하기 위한 접근제어 기법으로, 사용자의 역할에 기반하여 접근을 제어한다[17][18]. 다수의 접근 권한자가 존재할 경우 많이 채택되는 방식으로 사전에 역할을 정의하고, 접근 권한자에 해당하는 역할을 부여함으로서 역할에 허가된 접근만을 허가함으로서 권한을 벗어나는 자료에 대한 접근을 제어하여 불필요한 자료의 유출을 방지할 수 있도록 한다[19][20].

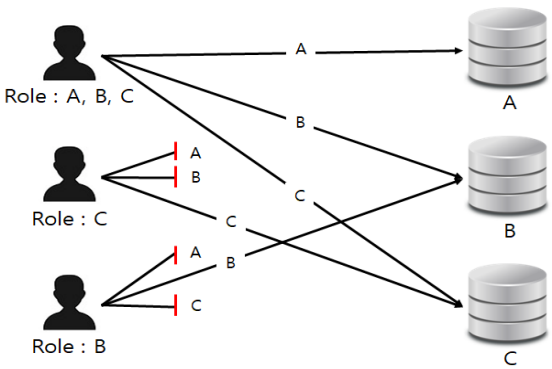


그림 1. Role Based Access Control 개념
Fig. 1. Role based access control concept

2.3 관련 연구 동향

데이터에 대한 무결성을 보장하는 블록체인을 적용한 접근제어 기법은 IoT, 의료기록과 같은 분야에서 많은 연구가 진행되고 있으며, 본 절에서는 블록체인에 접근제어를 접목한 연구사례를 소개한다.

Oscar(2018)의 연구사례는 지리적으로 분산된 센서네트워크에 적용 가능한 접근제어 시스템을 제안하였으며[21], Aafaf(2017)의 연구사례는 IoT에 접목하여 접근 권한의 부여, 획득, 위임, 취소에 사용되는 트랜잭션을 블록체인에 적용하였다[22]. Asaph(2016)의 연구사례는 의료 연구를 목적으로 블록체인을 기반으로 하는 데이터 공유 메커니즘을 제안하였다[23].

스마트 컨트랙트를 적용한 RBAC 연구사례로는

사용자의 역할 소유를 확인하는 인증 프로토콜을 연구한 Jason(2018)의 연구사례[24]와 블록체인에 기록되는 역할 관리가 관리자에 의해 진행할 수 있도록 하는 Yongjoo(2018)의 연구사례[25]가 있다.

III. 제안하는 메커니즘

본 논문에서 제안하는 스마트 컨트랙트를 적용한 RBAC는 프라이빗 블록체인 환경에서 구현되어 다수의 기업에서 접근권한 관리자에 의해 구현된 접근 정책을 블록체인으로 기록하고 기업의 사용자 모두가 블록체인을 공유함으로서 데이터의 무결성을 보장할 수 있다. 사용자에 의한 자료 접근 요청이 발생할 경우, 암호화된 자료를 보관하고 있는 관리 시스템에서 사용자 권한 확인을 블록 네트워크에 요청하고, 스마트 컨트렉트에 의해 허가된 사용자로 확인된 경우, 자료를 복호화하여 사용자에게 전송하도록 함으로서 접근 제어를 구현하였다. 각 관리자에 의해 구현된 접근정책은 생성자의 공개키를 이용하여 암호화되어 블록 네트워크에 기록하고, 기록된 블록 데이터는 관리자의 비밀키로 복호화할 수 있는 데이터를 구하기 위한 식별키로서 공개키를 사용하여 찾을 수 있으며, 관리자는 자신의 블록을 찾아 접근정책을 확인할 수 있다[26][27].

그림 2는 제안하는 메커니즘에서 생성되는 블록 데이터를 보이는 것이다. 관리자의 접근 정책 수정 과성에서 발생되는 관리자 접근 정책 블록, 사용자의 접근 요청에 의해 생성되는 사용자 접근 관리 블록, 역할 기반 접근제어를 수행하기 위해 사용자와 사용자의 역할을 저장하는 접근 권한 블록의 3가지 블록으로 구성된다. 각 블록에 대한 식별 방법은 블록체인의 기타데이터에 식별키를 적용하는 방식을 적용하여 식별할 수 있다.

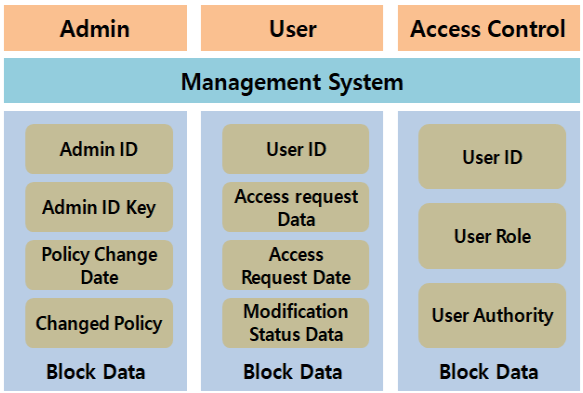


그림 2. 제안된 블록 구성
Fig. 2. Proposed block configuration

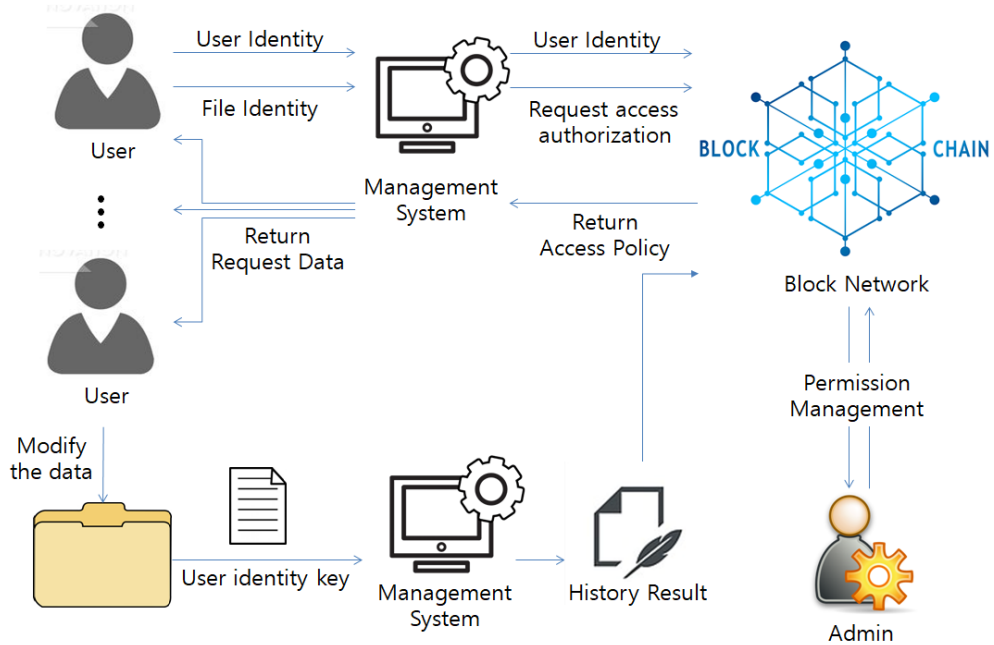


그림 3. 제안된 메커니즘 구상도
Fig. 3. Proposed mechanism schematic

3.1 용어

표 1. 용어
Table 1. Term

Content	Abbreviation
Encrypted Admin Identity Key	E_{IDK}
Decrypt Admin Identity Key	D_{IDK}
Encrypted User Data	E_{UD}
RSA Public Key	RSA_{PubK}
RSA Private Key	RSA_{PriK}

3.2 사용자 접근 권한 변경

사용자의 접근 권한에 대한 생성/변경/삭제와 같은 권한 수정은 관리자에 의해서만 진행될 수 있다. 사용자의 접근 권한 변경이 요구되는 경우, 관리자는 관리 시스템에 권한 변경을 요청하고 관리자에 대한 인증 절차를 진행한다. 관리자의 인증키는 대칭키 암호 알고리즘은 AES(Advanced Encryption Standard)를 이용하여 관리자와 관리 시스템이 공유하는 비밀키를 이용하여 전송된다. 식 (1)은 관리자 인증 키 암호화 과정을 보이는 것이다.

$$E_{IDK} = AES(Identity\,Key) \tag{1}$$

암호화된 관리자 인증키를 받은 관리 시스템은 인증키를 복호화하고, 관리자 인증키에 대해 블록에 기록되어 있는 데이터를 요청하여 기록되어있는 인증키와 대조하여 정당한 관리자임을 확인한다. 식 (2)는 관리자 인증키를 복원하는 과정을 보이는 것이다.

$$D_{IDK} = Decryption(E_{IDK}) \tag{2}$$

관리자임이 인증되면 관리 시스템은 블록 네트워크에 기록된 접근 권한 목록을 요청하고, 해당 기록을 관리자에게 반환한다. 관리자는 접근 권한 목록에서 변경하고자 하는 사용자의 역할을 관리 시스템에 전달하고, 관리 시스템은 관리자의 정보와 관리자가 요청한 사용자의 역할을 변경한 기록을 블록데이터로 생성하여 블록 네트워크에 기록하고 블록 네트워크는 생성된 블록의 내용을 관리 시스템에 전달한다.

그림 4는 관리자에 의해 사용자의 접근 권한을 변경하는 과정을 보이는 순서도이다. 접근 권한의 생성/변경/삭제의 3가지 접근 권한 수정에 대해 아래의 그림과 같은 과정을 통해 수행된다.

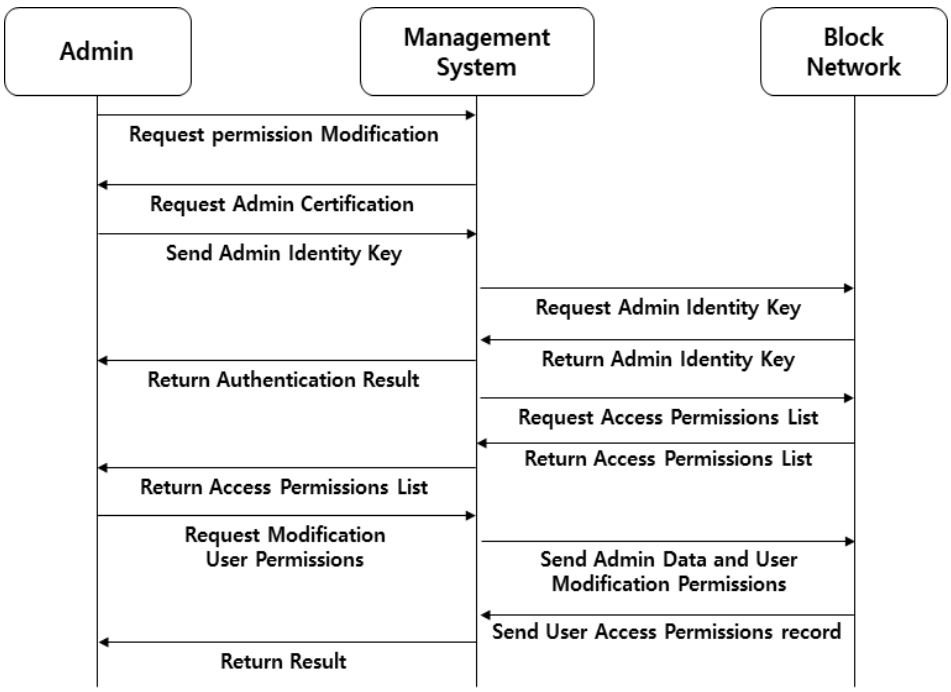


그림 4. 관리자의 사용자 접근 권한 변경 과정
Fig. 4. Process for changing the administrator's user access permission

3.3 사용자 데이터 접근 요청

사용자는 데이터에 접근을 요청할 수 있고, 이를 수정할 수 있다. 사용자는 데이터를 요청하기 위해 관리 시스템에 자신의 식별키와 요청하고자하는 데이터를 관리 시스템으로 전송한다. 여기서 암호화키는 공개키 알고리즘인 RSA를 적용하며, 사용자는 비밀키를 사용하여 자신의 식별키와 요청 데이터를 암호화한다. 식 (3)은 사용자의 요청 데이터에 대한 암호문을 생성하는 것을 보이는 것이다.

$$E_{UD} = RSA_{PubK}(User\,Data) \tag{3}$$

관리 시스템은 다수의 사용자로부터 공개키로 암호화된 암호문을 받아 비밀키로 복원하며, 복원된 사용자의 식별키를 통해 사용자의 권한을 확인한다. 식 (4)는 사용자의 정보를 복호화하는 과정을 보이는 것이다.

$$User\,Data = RSA_{PriK}(E_{UD}) \tag{4}$$

블록체인에서는 사용자의 권한 기록 대조 요청을 받으면 스마트 컨트렉트에 의해 사용자 권한 블록에 기록되어 있는 사용자의 권한 기록을 관리 시스템에 제공하고, 사용자의 접근 기록에 대해 공개키 기반의 암호화가 진행된 블록데이터를 생성한다. 암호화된 블록데이터는 블록 네트워크에 기록되고, 공개키에 의해 암호화된 블록은 이후 해당 블록을 찾기 위해 공개키를 같이 저장함으로서 저장된 공개키는 이후 하나의 식별키로 작용하여 계약 기록을 찾기위한 역할을 수행할 수 있다. 또한 프라이빗 블록체인에 연결되어 있는 다른 접근권한 관리자와는 서로 다른 암호키를 적용하여 시스템 내에서 다른 관리자의 정보를 확인할 수 없도록 한다.

그림 5는 사용자가 데이터를 요청하거나, 추가 또는 수정하는 과정을 보이는 것이다.

Ⅳ. 기존 방법론과의 비교분석

본 논문에서 제안하는 메커니즘은 데이터베이스에 암호화되어 있는 데이터에 대한 접근 제어를 프라이빗 블록체인을 이용하여 진행하였으며, 관리자의 접근 권한 관리, 사용자의 데이터 접근 관리, 사용자의 접근 권한 관리의 작업이 진행될 때, 각각의 블록을 생성하여 관리하는 것을 특징으로 한다. 본 절에서는 기존의 방법론을 분석하고 제안된 메커니즘과의 비교분석을 진행하였다[24]-[30].

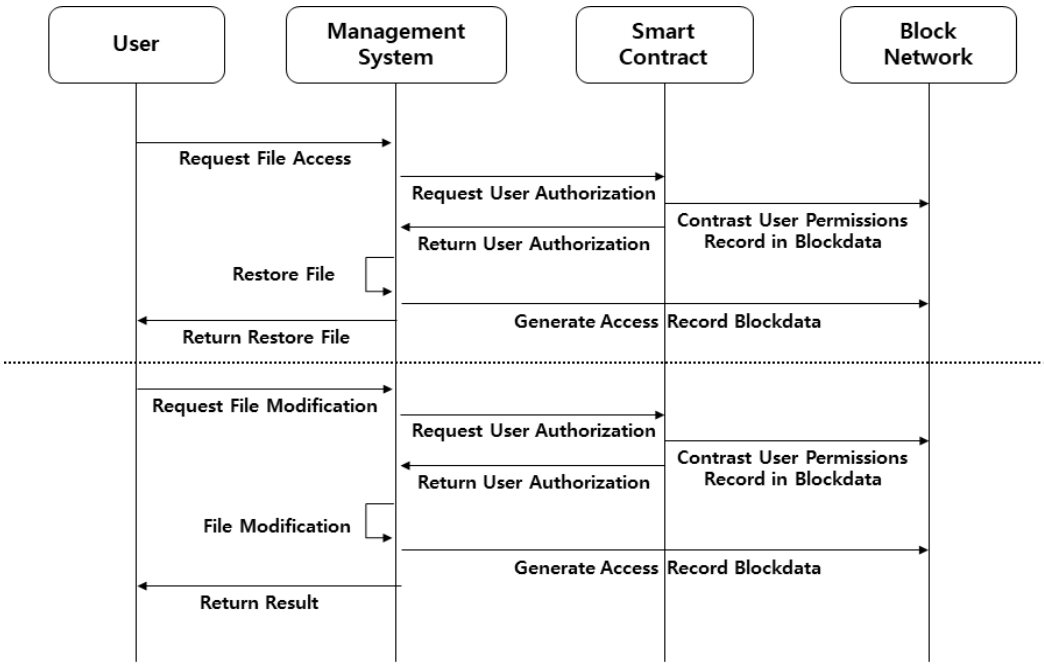


그림 5. 사용자 데이터 요청 과정
Fig. 5. User data request course

4.1 RBAC-SC

RBAC-SC(Smart Contract)는 2018년 Jason에 의해 제안된 방식으로 스마트 컨트랙트를 이용하여 RBAC을 구현하는 방법을 소개하였다[24]. RBAC-SC는 전자결제 시스템에 적용하기 위한 방법으로 사용자의 역할을 인증하는 Role Issuer, 역할에 따른 서비스를 제공받고자 하는 User, 역할에 따른 서비스를 제공하는 Service Provider의 3가지로 구성된다. 먼저 Role Issuer이 User에 대한 역할을 할당하고 블록체인에 기록하면, User는 할당된 역할을 이용하여 Service Provider에게 역할에 맞는 서비스를 요청한다. Service Provider는 Role Issuer에 의해 생성된 블록 데이터에 User의 역할 검증을 요청한다. 역할 검증은 Smart Contract에 의해 진행되며, 역할이 검증되면 Service Provider는 User에게 역할에 맞는 서비스를 제공하는 방식이다.

4.2 RBAC-PAC

RBAC-PAC(Permission Attribute Certificate)는 2018년 이용주에 의해 제안된 방식으로 스마트 팩토리의 물류관리를 위한 방법을 소개하였다[25]. RBAC-PAC는 PAC가 할당되는 주체가 역할에 있다. ACI(AC Issuer)라는 인증기관에서 PAC를 발급을 위한 공개키를 블록체인을 이용하여 배포하고, 관리자가 특정한 규칙에 따른 PAC에 대한 발급이나 갱신을 요청하면 ACI에서는 PAC을 발급하고 비밀키로 서명하며, 관리자는 발급된 트랜잭션을 블록체인에 등록한다. 등록된 트랜잭션은 노드에 브로드캐스팅을 사용하여 블록을 생성하고, AC Verifier는 역할에 대한 PAC를 찾아 공개되어있는 공개키로 복호화하여 접근제어를 적용하는 방식이다.

4.3 기존 연구와의 비교분석

본 논문에서 제안하는 내용은 접근권한을 블록체인에서 관리함으로서 접근권한의 무결성을 강화하는 것을 목적으로 하며, Admin에 의해 블록체인에 접근 권한을 기록하고, 사용자가 데이터에 접근을 요청하는 경우, 블록체인의 접근권한 기록을 공개키로 암호화하여 DB로 전송한다. DB에서는 저장되어 있는 비밀키를 이용하여 받은 접근권한 기록을 복원하고, 사용자에게 할당된 권한이 정당할 경우, 사용자가 가진 비밀키에 대응하는 공개키를 이용하여 데이터를 전송하는 방법으로 그림 6과 같은 차별성을 가진다.

Ⅴ. 구현 결과

그림 7은 구현된 내용 중 사용자의 접근권한을 가진 블록을 임의적으로 생성한 결과를 보이는 것이다. 문자열로 기록된 사용자 블록은 hex로 변환되어 블록에 기록되며, 사용자의 요청에 따라 DB는 사용자 블록을 요청하고, 접근권한 블록의 hex코드를 문자열로 변환하여 사용자의 권한을 인증한다[31]-[39].

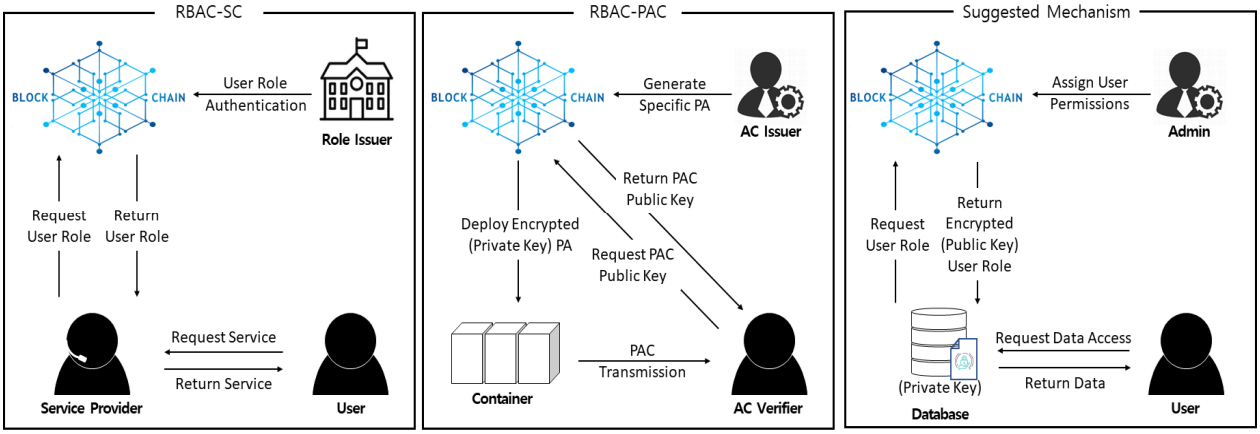


그림 6. 기존 연구와의 비교분석
Fig. 6. Comparative analysis with existing research

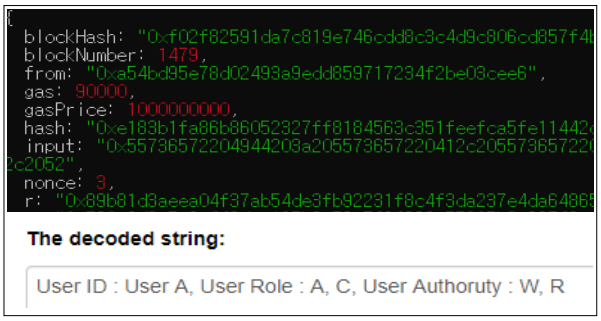


그림 7. 접근권한 블록 구현 결과
Fig. 7. Access control block implementation results

Ⅵ. 결론 및 향후 과제

잘못된 접근 권한 관리나, 접근 권한의 조작 등에 의하여 데이터가 허가되지 않은 사용자에게 유출될 수 있다. 특히, 유출된 대상이 악의적인 의도를 가진 내부자인 경우에는 데이터가 외부로 유출될 가능성이 존재한다. 데이터의 관리가 아날로그 방식에서 디지털화됨에 따라 데이터의 유출은 유출 당사자에게 있어 큰 문제가 될 수 있으며, 데이터 유출을 방지하기 위한 철저한 접근 관리와, 외부의 악의적인 공격자에 의해 접근 권한이 위·변조되지 않았음을 증명할 수 있어야 한다.

위와 같은 문제를 보완하기 위해 본 논문에서는 블록체인을 이용하여 접근권한을 기록하고, 사용자가 데이터를 요청할 경우, 공개키에 의해 암호화된 접근권한을 비밀키를 가지고 있는 시스템으로 전송하여, 인가된 시스템에서만 사용자의 접근권한을 확인하고, 데이터를 제공하는 메커니즘을 제안하였다. 향후, 블록 데이터는 항시 공개되어있으므로 악의적인 공격자에 의해 비밀키를 유추할 수 있다는 점에서 보다 복잡하고 유추할 수 없는 암호화가 연구되어야 할 것이다.

References

[1] Jungjae Kim, Jaepyo Park, and Moonseog Jun, "A Digital Right Management System based on Shared Key Pool for Video Data Protection", Journal of KIPS, Vol. 12, No. 2, pp. 183-190, Apr. 2005.

[2] Sung-Hwa Han, Joong-Soo Bang, Sang-Oh Yoo, and Gwang-Yong Gim, "Medical Information Sharing Service Architecture based on Blockchain", Journal of AJMAHS, Vol. 9, No. 1, pp. 339-348, Jan. 2019.

[3] Jinsu Kim, Namje Park, Geonwoo Kim, and Seunghun Jin, "CCTV Video Processing Metadata Security Scheme Using Character Order Preserving -Transformation in the Emerging Multimedia", ELECTRONICS, Vol. 8, No. 4, Apr. 2019. https://doi.org/10.3390/electronics8040412.

[5] Donghyeok Lee, Namje Park, Geonwoo Kim, and Seunghun Jin, "De-identification of metering data for smart grid personal security in intelligent CCTV-based P2P cloud computing environment", Journal of Peer-to-Peer Networking and Applications, Vol. 11, No. 6, pp. 1299-1308, Nov. 2018.

[6] Seunghyeon Nam and Taeha Kim, "Risks and Network Effect upon Cloud ERP Investments:Real Options Approach", Journal of ISR, Vol. 20, No. 4, pp. 43-57, Dec. 2018.

[7] Donghyeok Lee and Namje Park, "Electronic identity information hiding methods using a secret sharing scheme in multimedia-centric internet of things environment", Journal of Personal And Ubiquitous Computing, Vol. 22, No. 1, pp. 3-10, Feb. 2018.

[8] Chul-Jin Kim, "A Static and Dynamic Design Technique of Smart Contract based on Block Chain", Journal of KAIS, Vol. 19, No. 6, pp. 110-119, Jun. 2018.

[9] Jun-hyeok Yun and Mihui Kim, "Private Blockchain and Smart Contract Based High Trustiness Crowdsensing Incentive Mechanism", Journal of KIISC, Vol. 28, No. 4, pp. 999-1007, Aug. 2018.

[10] Donghyeok Lee and Namje Park, "Geocasting-based synchronization of Almanac on the maritime cloud for distributed smart surveillance", Supercomputing, Vol. 73, No. 3, pp. 1103-1118, Mar. 2017.

[11] Namje Park and Hyochan Bang, "Mobile middleware platform for secure vessel traffic system in IoT service environment", Journal of

Security And Communication Networks, Vol. 9, No. 6, pp. 500-512, 2016.

[12] Heejung Kang, Hye Ri Kim, and Seng-phil Hong, "A Study on the Design of Smart Contracts mechanism based on the Blockchain for anti-money laundering" Journal of KSII, Vol. 19, No. 5, pp. 1-11, Oct. 2018.

[13] Song In-Bang and Yang Young-Sik, "A Study on the Availability of Blockchain Smart Contract in Real Estate Transaction", Journal of JLS, Vol. 18, No. 4, pp. 1-26, Dec. 2018

[14] Namje Park and Namhi Kang, "Mutual Authentication Scheme in Secure Internet of Things Technology for Comfortable Lifestyle", Journal of Sensors (Basel), Vol. 16, No. 1, pp. 1-16, Dec. 2015.

[15] Jae-Hyun Se, "Business Value of Blockchain and Applications of Artificial Intelligence", Journal of AJMAHS, Vol. 8, No. 7, pp. 779-789, Jul. 2018.

[16] Jung-Jae Lee, "A Study on Music Copyright Management Model Using Block Chain Technology", Journal of KSAF, Vol. 35, pp. 341-351, Sep. 2018.

[17] Namje Park, Jin Kwak, Seungjoo Kim, Dongho Won and Howon Kim, "WIPI Mobile Platform with Secure Service for Mobile RFID Network Environment", Journal of AWNTA, pp. 741-748, Jan. 2006.

[18] Namje Park, Hongxin Hu, and Qun Jin, "Security and Privacy Mechanisms for Sensor Middleware and Application in Internet of Things (IoT)", Journal of Distributed Sensor Networks, Vol. 2016, No. 1, Jan. 2016. https://doi.org/10.1155/2016/2965438.

[19] You-Ri Lee and Dong-Gue Park, "Implementation of Role Based Access Control Model for U-healthcare", Journal of KAIS, Vol. 10, No. 6, pp. 1256-1264, Jun. 2019.

[20] Se Jong Oh, "Information Security : Permission-Based Separation of Duty Model on Role-Based Access Control", Journal of KIPS, Vol. 11, No. 7, pp. 725-730, Dec. 2004.

[21] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT", Journal of Internet of Things, Vol. 5, No. 2, pp. 1184-1195, Apr. 2018.

[22] A. Aoaddah, A. A. Elkalam, and A. A Ouahman, "Fair Access: a new Blockchain-based access control framework for the Internet of Things", Journal of Security and Communication Networks, Vol. 9, No. 18, pp. 5943-5964, Feb. 2017.

[23] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management", Conference of Open and Big Data, Aug. 2016.

[24] J. P. Cruz, Y. Kaji, and N. Yanai, "RBAC-SC: Role-Based Access Control Using Smart Contract", IEEE Access, Vol. 6, pp. 12240-12251, Mar. 2018.

[25] Y. Lee and S. Lee, "Efficient RBAC based on Block Chain for Entities in Smart Factory", Journal of Korea Convergence Society, Vol. 9, No. 7, pp. 69-75, Jul. 2018.

[26] Namje Park, Byung-Gyu Kim, and Jinsu Kim, "A Mechanism of Masking Identification Information regarding Moving Objects Recorded on Visual Surveillance Systems by Differentially Implementing Access Permission", ELECTRONICS, Vol. 8, No. 7, pp. 735, Jul. 2019.

[27] Namje Park, Younghoon Sung, Youngsik Jeong, Soo-Bum Shin, and Chul Kim, "The Analysis of the Appropriateness of Information Education Curriculum Standard Model for Elementary School in Korea", International Conference on Computer and Information Science, Springer, pp. 1-15, Jun. 2018.

[28] Jae-Young Chang, Sung-Mun Hong, Damy Son, Hojin Yoo, and Hyoung-Woo Ahn, "Development of Real-time Video Surveillance System Using the Intelligent Behavior Recognition Technique", Journal of IIIBC, Vol. 19, No. 2, pp. 161-168, 2018.

[29] Namje Park, Jungsoo Park, and Hyoungjun Kim, "Inter-Authentication and Session Key Sharing Procedure for Secure M2M/IoT Environment", International Information Institute(Tokyo) Information, Vol. 18, No. 1, pp. 261-266, Jan. 2015.

[30] Donghyeok Lee and Namje Park, "A Secure Almanac Synchronization Method for Open IoT Maritime Cloud Environment", Journal of KIIT, Vol. 15, No. 2, pp. 79-90, Feb. 2017.

[31] Namje Park, "Implementation of Terminal Middleware Platform for Mobile RFID Computing", International Journal of Ad Hoc and Ubiquitous Computing, Vol. 8, No. 4, pp. 205-219, Nov. 2011.

[32] Donghyeok Lee and Namje Park, "A Proposal of SH-Tree Based Data Synchronization Method for Secure Maritime Cloud", Journal of the Korea Institute of Information Security & Cryptology, Vol. 26, No. 4, pp. 929-940, Aug. 2016.

[33] Namje Park and Marie Kim, "Implementation of load management application system using smart grid privacy policy in energy management service environment", Cluster Computing, Vol. 17, No. 3, pp. 653-664, Sep. 2014.

[34] Seung-Gag Lim, "A Performance Comparison of CCA and RMMA Algorithm for Blind Adaptive Equalization", Journal of IIBC, Vol. 19, No. 1, pp. 51-56, Feb. 2019.

[35] Park N., "Implementation of inter-VTS data exchange format protocol based on mobile platform for next-generation vessel traffic service system", INFORMATION-An International Interdisciplinary Journal, Vol. 17, No. 10A, pp. 4847-4856, Oct. 2014.

[36] Young-Do Joo, "A Study on the Construction of Near-Real Time Drone Image Preprocessing System to use Drone Data in Disaster Monitoring", Journal of IIBC, Vol. 18, No. 3, pp. 143-149, Jun. 2019.

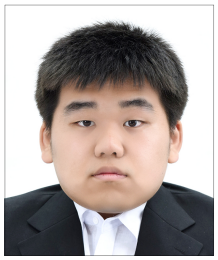
[37] Donghyeok Lee and Namje Park, "ROI-based efficient video data processing for large-scale cloud storage in intelligent CCTV environment", Journal of IJET, Vol. 7, No. 2.33, pp. 151-154, Mar. 2018.

[38] Jinsu Kim, Sangchoon Kim, and Namje Park, "Face Information Conversion Mechanism to Prevent Privacy Infringement", Journal of KIIT, Vol. 17, No. 6, pp. 115-112, Jun. 2019.

[39] Jinsu Kim and Namje Park, "Inteligent Video Surveilance Incubating Security Mechanism in Open Cloud Environments", Journal of KIIT, Vol. 17, No. 5, pp. 105-116, May 2019.

저자소개

김 진 수 (Jinsu Kim)



2017년 2월 : 강원대학교 정보통신공학전공 학사
2019년 8월 : 강원대학교 전자정보통신공학전공 석사
2019년 9월 : 제주대학교 대학원 컴퓨터교육전공 박사과정
2018년 9월 ~ 현재 : 제주대학교 사이버보안인재교육원 연구원
관심분야 : 클라우드, 지능형 영상감시 시스템, IoT 등

박 남 제 (Namje Park)

2008년 2월 : 성균관대학교 컴퓨터공학과 박사
2003년 4월 ~ 2008년 12월 : 한국전자통신연구원 정보보호연구단 선임연구원
2009년 1월 ~ 2009년 12월 : 미국 UCLA대학교 공과대학 Post-Doc, WINMEC 연구센터 Staff Researcher
2010년 1월 ~ 2010년 8월 : 미국 아리조나 주립대학교 컴퓨터공학과 연구원
2010년 9월 ~ 현재 : 제주대학교 초등컴퓨터교육전공, 대학원 융합정보보안학과 교수
2011년 9월 ~ 현재 : 창의교육거점센터장, 과학기술사회(STS)연구센터 부센터장, 정보영재 주임교수, 사이버보안인재교육원장
관심분야 : 융합기술보안, 컴퓨터교육, 스마트그리드, IoT, 해사클라우드 등