JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 27 No. 11, pp. 1-11, November 2022
https://doi.org/10.9708/jksci.2022.27.11.001

Contract-based Access Control Method for NFT Use Rights

Yoonsung Jeong*, Deokyoon Ko**, Jungwon Seo*, Sooyong Park*,
Seong-Jin Kim***, Bum-Soo Kim***, Do-Young Kim***

*M.S Student, Dept. of Computer Science, Sogang University, Seoul, Korea
**CEO, Noncelab Inc., Seoul, Korea
*Ph.D. Candidate, Dept. of Computer Science, Sogang University, Seoul, Korea
*Professor, Dept. of Computer Science, Sogang University, Seoul, Korea
***Senior Researcher, Dept. of Future & Smart Construction Research, Korea Institute of Civil Engineering and Building Technology(KICT), Goyang-Si, Korea
***Senior Researcher, Dept. of Future & Smart Construction Research, Korea Institute of Civil Engineering and Building Technology(KICT), Goyang-Si, Korea
***Postdoctoral Researcher, Dept. of Future & Smart Construction Research, Korea Institute of Civil Engineering and Building Technology(KICT), Goyang-Si, Korea

[Abstract]

In this paper, we propose an NFT(Non-Fungible Token)-based access control method for safely sharing data between users in blockchain environment. Since all data stored in the blockchain can be accessed by anyone due to the nature of the technology, it is necessary to control access except for authorized users when sharing sensitive data. For that, we generate each data as NFT and controls access to the data through the smart contract. In addition, in order to overcome the limitations of single ownership of the existing NFT, we separated the NFT into ownership and use rights, so that data can be safely shared between users. Ownership is represented as an original NFT, use rights is represented as a copied NFT, and all data generated as NFT is encrypted and uploaded, so data can be shared only through the smart contract with access control. To verify this approach, we set up a hypothetical scenario called Building Information Modeling (BIM) data trade, and deployed a smart contract that satisfies 32 function call scenarios that require access control. Also, we evaluated the stability in consideration of the possibility of decryption through brute-force attack. Through our approach, we confirmed that the data can be safely shared between users in blockchain environment.

▸ **Key words**: Blockchain, Data Access Control, Smart Contract, NFT, IPFS, Data Share

• First Author: Yoonsung Jeong, Corresponding Author: Seong-Jin Kim
*Yoonsung Jeong (yuon1233@gmail.com), Dept. of Computer Science, Sogang University
**Deokyoon Ko (dykoh@noncelab.com), Noncelab Inc.
*Jungwon Seo (jungwonrs@gmail.com), Dept. of Computer Science, Sogang University
*Sooyong Park (sypark@sogang.ac.kr), Dept. of Computer Science, Sogang University
***Seong-Jin Kim (sjkim72@kict.re.kr), Dept. of Future & Smart Construction Research, Korea Institute of Civil Engineering and Building Technology(KICT)
***Bum-Soo Kim (bsk@kict.re.kr),Dept. of Future & Smart Construction Research, Korea Institute of Civil Engineering and Building Technology(KICT)
***Do-Young Kim (doyoungkim0123@kict.re.kr), Dept. of Future & Smart Construction Research, Korea Institute of Civil Engineering and Building Technology(KICT)
• Received: 2022. 10. 12, Revised: 2022. 10. 28, Accepted: 2022. 11. 02.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

[요 약]

본 논문에서는 블록체인 환경에서 상호간 데이터를 안전하게 공유하기 위한 NFT 기반의 접근 제어 방안을 제안한다. 기존의 블록체인에 기록되는 모든 데이터는 기술 특성상 누구나 접근할 수 있기 때문에 민감한 데이터를 공유하는 경우에는 인가받은 사람 외에는 접근을 제어할 필요가 있다. 이를 위해서 제안하는 방안에서는 각 데이터를 NFT로 발행하고, 컨트랙트를 통해 데이터에 대한 접근을 제어한다. 또, 기존의 NFT가 가지는 단일 소유권의 한계를 극복하기 위해 소유권과 사용권으로 개념을 분리하여 사용자간 데이터를 안전하게 공유할 수 있도록 한다. 소유권은 원본 NFT로 발행하고, 사용권은 사본 NFT로 발행하여 관리하며, NFT로 발행되는 모든 데이터는 암호화된 후 업로드가 진행되기 때문에 반드시 접근 제어가 이루어지는 스마트 컨트랙트를 통해서만 데이터의 공유가 가능하다. 이러한 접근 방안을 검증하기 위해 BIM(Building Information Modeling) 데이터 거래라는 가상의 시나리오를 설정하고, 접근 제어가 필요한 32가지 함수 호출 시나리오를 만족하는 스마트 컨트랙트를 구성하였다. 또한, 무차별 대입을 통한 복호화 공격 가능성을 고려하여 이에 대한 안정성을 평가하였다. 이를 통해 블록체인 환경에서 안전하게 개인 간 데이터를 공유할 수 있음을 확인하였다.

▸ **주제어**: 블록체인, 데이터 접근 제어, 스마트 컨트랙트, NFT, IPFS, 데이터 공유

I. Introduction

블록체인은 P2P(Peer-to-Peer) 네트워크, 공개키-개인키 구조, 해시 알고리즘 및 합의 알고리즘과 같은 요소 기술에 의해 데이터의 무결성 및 신뢰성을 보장하는 기술이다. 블록체인의 대표적인 플랫폼으로는 비트코인[1], 이더리움[2]이 있다. 또한, 이더리움 기반의 DeFi(Decen- tralized Finance), NFT(Non-Fungible Token)와 같은 서비스가 활성화됨에 따라 다양한 비즈니스[3, 4]가 창출되고 있다.

블록체인을 활용한 다양한 비즈니스가 창출되고 있는 가운데, 블록체인을 이용한 데이터 접근 제어 기반의 비즈니스도 함께 주목받고 있다. 예를 들어, BIM(Building Information Modeling) 분야에서는 설계 도면 데이터의 보존 및 지적 재산권 보장을 기반으로 거래 환경을 조성하기 위해 블록체인을 활용하고 있다. 또한, BIM 분야와 블록체인을 활용한 다양한 연구들[5-9]도 계속해서 진행되고 있다.

블록체인 기술의 가장 큰 장점은 데이터의 투명성이다. 블록체인은 관리자 없이도 알고리즘에 의해 데이터의 투명성을 보장하고, 데이터의 공개를 통해 블록체인 네트워크 참여자들간의 신뢰를 추구한다. 하지만, 블록체인이 가진 데이터의 투명성으로 인해 개인정보와 같이 보호되어야 할 데이터, 혹은 관리자 권한 부여가 필요한 데이터를 블록체인에 직접 저장하기에는 적합하지 않다. 하지만 반대로, 데이터에 대한 출처 표기가 투명하게 공개되어야 하는 경우, 블록체인을 활용했을 때 그 효과가 두드러질 수 있다. 이와 같은 비즈니스를 위해서는 민감한 데이터에 대한 접근 제어 방안이 반드시 필요하다.

블록체인에 민감한 데이터를 저장하기 위해 블록체인 기반의 데이터 접근 제어를 위한 연구들이 진행되고 있다. RBAC-SC(Role-based Access Control-Smart Contract)를 제안한 연구[10]는 챌린지-응답 프로토콜을 이용하여 역할 소유권 인증 및 사용자 역할 할당 확인 과정을 통한 데이터 접근 제어 방안을 제안하였다. 하지만 해당 연구에서는 권한을 관리하는 중앙화된 관리자가 필요하다는 한계가 존재한다. 또 다른 연구들[11, 12]은 여러 속성을 기반으로 데이터의 접근을 통제하는 연구를 제안하였다. 하지만 속성 기반의 접근 제어 연구들은 특정 사용자에게 권한이 계속하여 증가할 수 있기 때문에 접근 통제 관리가 어려울 수 있다는 한계를 가지고 있다. 분산형 연합 스마트 컨트랙트 기반의 접근 제어를 제안한 연구[13]는 코디네이터(Coordinator)를 두어 데이터의 접근을 제어하는 방안을 제안하였다. 해당 연구는 코디네이터에 의해 데이터 접근 제어가 중앙화 될 수 있다는 한계가 존재한다. 마지막으로, 스마트 컨트랙트 및 오프체인 저장소를 활용한 접근 제어 방식을 제안한 연구[14]는 Hydra, ECFChecker 모듈을 통해 스마트 컨트랙트를 사전 검증하였다. 또, 별도로 정의한 접근 제어 규칙 및 토큰 발행 규칙을 활용한 데이터 접근 제어 방안을 제안하였다. 해당 연구는 스마트 컨트랙트 사전 검증을 위해 오프체인에 다소 의존적이라는 한계점을 가지고 있다.

본 논문에서는 기존의 연구들이 가진 한계점인 데이터 접근 제어를 위한 관리자가 존재한다는 점과 오프체인을 통한 접근 제어로 발생할 수 있는 외부 의존성의 한계를 극복하는 접근 방안을 제안하고자 한다.

제안하는 접근 방안은 NFT를 활용한 데이터 접근 제어 방법을 제안한다. 본 논문에서 제안하는 접근 방안은 데이터를 암호화하여 오프체인상에 저장한다. 암호화된 데이터는 스마트 컨트랙트에 의해 접근 제어가 가능하다. 또한, NFT를 통해 소유권과 사용권을 분리하여 데이터를 안전하게 공유할 수 있다. 본 논문의 접근 방안 검증을 위해 가상 시나리오를 통한 접근 방안의 구현 및 안정성 평가 실험을 진행하였다.

본 연구에서 제안하는 NFT 기반의 접근 제어 기법은 다음과 같은 기여를 가진다.

1) 외부 혹은 내부의 관리자가 존재하지 않더라도 데이터의 접근 제어가 가능
2) 데이터를 암호화하여 공유되는 원본 데이터를 보호
3) 소유권과 사용권 분리 및 데이터 접근 권한 부여

본 논문의 구성은 1장 서론에 이어 2장은 배경지식 및 관련 연구를 서술한다. 또한, 3장에서는 접근 방안을 설명하며, 4장에서는 실험에 관한 내용을 서술한다. 마지막 5장에서는 결론 및 향후 연구를 서술한다.

II. Preliminaries

본 장에서는 본 논문의 접근 방안을 이해하기 위한 배경지식 및 블록체인 기반의 데이터 접근 제어 방안을 적용하고 있는 기존 연구에 대해 서술한다.

2.1. Background

2.1.1. Blockchain

블록체인은 여러 가지 요소 기술에 의해 데이터의 무결성 및 신뢰성을 보장하는 기술이다. 대표적인 요소 기술은 P2P 네트워크, 공개키-개인키 구조, 해시 알고리즘, 그리고 합의 알고리즘이 있다. P2P 네트워크를 사용하여 기존의 중앙화된 환경으로부터 벗어나 개인 간 거래를 지원함으로써 사용자는 중개 수수료 비용 절감 및 실시간 정산과 같은 효과를 누릴 수 있다. 네트워크에 참여한 각 사용자는 공개키와 개인키 쌍을 통해 만들어진 주소에 의해 구별되며, 데이터를 기록하는데 있어 개인키를 이용한 서명이 이루어지므로 이에 대한 출처는 누구든지 확인할 수 있다. 또한, 블록에 들어가는 데이터는 해시 알고리즘과 합의 알고리즘에 의해 기록되며, 모든 사용자들이 동일한 데이터를 분산 저장하고 있기 때문에 한 번 만들어진 데이터를 수정, 삭제하는 것은 불가능에 가깝다. 이를 통해 데이터의 무결성과 신뢰성을 보장받을 수 있다.

2.1.2. NFT (Non-Fungible Token)

NFT(Non-Fungible Token)는 소유권 보장을 통해 디지털 자산에 가치를 부여할 수 있는 토큰을 의미하며, 최근까지도 계속해서 많은 주목을 받고 있다[15]. 논문에서 중점을 두고 있는 이더리움 기반의 NFT는 주로 ERC-721(Ethereum Request for Comments-721)[16]과 ERC-1155[17] 표준을 통해 생성된다. 또한, 각 NFT 토큰에는 토큰 ID가 존재하며, 각 토큰 ID는 하나의 소유권자에게 종속되기 때문에 고유성이 인정된다. 이러한 특성 덕분에 NFT는 여러 방면에서 활용될 가능성이 있다. 현재 NFT는 주로 수집품(Collectible), 미술품(Art), 가상부동산(Virtual World) 등에 활용되고 있으며, NFT와 관련된 다양한 연구들도 진행되었다[18, 19].

2.1.3. IPFS (InterPlanetary File System)

IPFS(InterPlanetary File System)는 수많은 디바이스들을 동일한 파일 시스템처럼 관리하는 P2P 기반의 분산 파일 시스템이다[20]. IPFS는 기존 중앙형 스토리지와 달리 분산된 형태로 데이터를 저장하기 때문에 데이터에 대한 검열 문제, 혹은 단일점 공격(Single Point of Failure)과 같은 문제에 대비할 수 있다. 또한, 하나의 데이터에 대해 연결된 모든 노드들이 데이터를 삭제하지 않는 한, 계속해서 같은 데이터에 접근할 수 있다. 이러한 특징 덕분에 IPFS에 저장하는 데이터는 중앙화 스토리지 대비 다소 안전하다고 할 수 있으며, 블록체인에 저장되는 데이터도 IPFS와 같은 분산형 오프체인 저장소에 병행하여 저장한다.

2.1.4. Symmetric Key and Asymmetric Key

대칭키(Symmetric Key) 암호화 방식은 평문을 암, 복호화하기 위해 동일한 키를 사용하는 방식을 말한다[21]. 대표적으로 DES(Data Encryption Standard)[22], AES(Advanced Encryption Standard)[23], 아리아(ARIA, Academy Research Institute Agency)[24] 등이 있다. 대칭키는 송신자와 수신자가 동일한 키를 사용하기 때문에 알고리즘이 비교적 간단하여 속도가 빠르다는 장점이 있다. 하지만, 여러 개의 암호화된 데이터를 주고받는 경우, 이를 위해 여러 개의 키를 저장해야 한다는 단점이 있다.

비대칭키(Asymmetric Key) 암호화 방식은 평문을 암, 복호화 하기 위해 서로 다른 키를 사용하는 방식을 말한다[25]. 대표적으로 RSA(Rivest, Shamir, and Adleman)[26], Diffie-Hellman[27] 등이 있다. 비대칭키는 공개키와 개인키 쌍을 이용해 암호화를 진행하기 때문에 알고리즘이 복잡하고, 대칭키에 비해 속도가 느리다는 단점이 있다. 하지만, 송신자와 수신자간 키를 공유하지 않더라도 자신의 개인키를 통해서만 복호화가 가능하기 때문에 비교적 안전하다는 장점이 있다.

2.2. Related Works

관련 연구는 2.2.1절부터 2.2.3절까지 다루며, 연구에 대한 요약 및 본 논문에서 제안하는 방안과의 비교는 <Table 1>에 나타내었다.

2.2.1. Role-based Access Control (RBAC)

역할 기반의 접근 제어(RBAC, Role-based Access Control)는 권한을 역할로 구분하여 부여하는 접근 제어 방식이다[28]. Cruz가 제안한 연구[10]에서는 서로 다른 기관 사이에 RBAC-SC라는 모델을 적용한 데이터 접근 제어 방안을 제안하였다. 저자는 RBAC-SC 모델의 챌린지-응답 프로토콜을 적용해 역할 소유권 인증 및 사용자 역할 할당 확인 과정을 구현하였다. 이를 통해 저자는 안전성, 유저 친화성, 검증 가능성, 확장 가능성, 그리고 관리 가능성을 보장하도록 했다. 하지만 해당 연구에서 제안하는 접근 방안에서는 권한을 관리하는 관리자가 필요하다는 한계가 존재한다.

2.2.2. Attribute-based Access Control (ABAC)

속성 기반의 접근 제어(ABAC, Attribute-based Access Control)는 사용자 특성, 객체 유형, 행위 유형, 기타로 나누어 접근을 제어하는 방식이다[29].

Guo가 제안한 연구[11]에서는 전통적인 속성 기반의 접근 제어 메커니즘에 특성 집합과 접근 정책을 대표할 토큰 규칙을 추가하여 데이터 접근을 제어하는 방안을 제안하였다. 하지만 탈중앙화 환경에서는 다수의 관리자가 결정을 내려야 하는 경우가 생기기 때문에 이 또한 관리자가 필요하다는 한계가 존재한다.

Zhang이 제안한 연구[12]에서는 접근 제어가 다양한 방식으로 적용될 수 있기 때문에 여러 가지 타입의 데이터를 보유할 수 있도록 동적으로 관리될 필요성을 언급하였다. 저자는 기존의 속성 기반 접근 제어 방식이 가지는 사용자 특성, 객체 유형, 행위 유형, 기타에 맞는 스마트 컨트랙트를 작성하여 데이터 접근을 제어하는 방안을 제안하였다. 해당 연구는 대규모 서비스에서 각 단위 서비스의 권한을 세분화하여 탈중앙성을 높이는데 기여하고 있지만, 각 서비스에 대한 접근 제어를 관리하기 위해 중앙 관리자가 필요하다는 한계점은 여전히 존재한다.

2.2.3. Smart Contract-based Access Control

Xu가 제안한 연구[13]에서는 BlendCAC(Blockchain-enabled Decentralized Capability-based Access Control)이라는 접근 제어 모델을 제안하였다. BlendCAC 모델은 도메인별로 코디네이터가 존재하며, 각 코디네이터는 중앙 클라우드로부터 권한을 위임받아 유저의 요청을

Table 1. Research Comparison and Our Approach

Research	Access Control Method	Opinion on Threshold	Admin Non-Existence	Data Encryption	On-Chain Access Control
[10]	Relation-based Access Control (RBAC)	The approach in this paper has a limitation that needs a manager who manages authority.	X	X	O
[11]	Attribute-based Access Control (ABAC)	In decentralized environment, there is a limitation in that managers are necessary because there are some cases where a large number of managers have to make decisions together.	X	O	O
[12]	Attribute-based Access Control (ABAC)	There is still a limitation that a central manager is needed to manage access control for each device.	X	X	O
[13]	Distributed Federated Smart Contract	There is a limitation in that there is a coordinator who is a manager, and it is somewhat dependent on the coordinator existing on off-chain.	X	X	X
[14]	Common Smart Contract	The centralized access control mechanism may increase dependence on the institution, operating the mechanism.	X	X	X
Our Approach	**NFT-based Access Control (NBAC)**	-	**O**	**O**	**O**

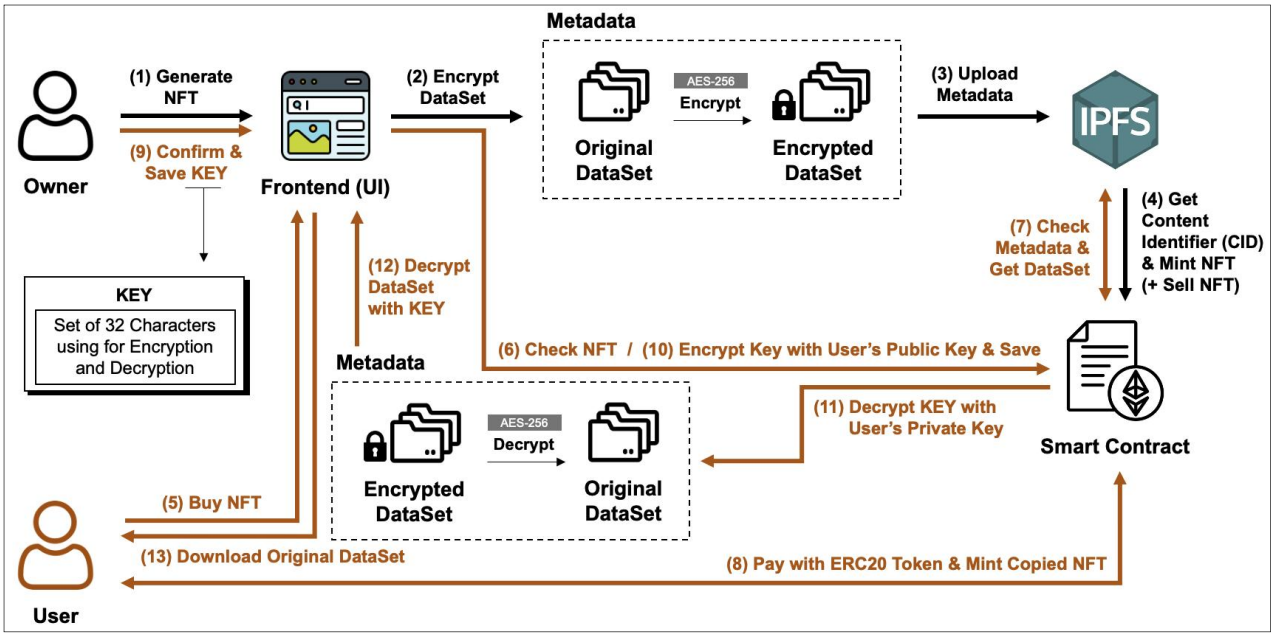


Fig. 1. Overview of Contract-based Access Control for NFT Use Rights

처리한다. 이를 활용하여 탈중앙성과 확장성을 동시에 보장하고, 시스템 데이터를 보호하고자 하였다. 하지만 이 방식 또한 관리자인 코디네이터가 존재하고, 동시에 오프체인상에 존재하는 코디네이터에 다소 의존적이라는 한계가 있다.

Liu가 제안한 연구[14]에서는 SMACS(Smart Contract Access Control Service)라는 모델을 통해 스마트 컨트랙트를 생성 및 검증하는 방안을 제안하였다. 해당 연구는 오프체인의 Hydra, ECF- Checker 모듈을 통해 접근을 제어하는 특징이 있다. 하지만, 해당 연구는 오프체인상에 존재하는 모듈에 의존적이라는 한계가 있다.

III. The Proposed Scheme

본 장에서는 앞서 언급한 기존 연구들이 가진 한계점인 접근 제어를 위한 관리자가 존재한다는 점과, 데이터 검증을 위해 오프체인에 의존적이라는 한계를 극복할 수 있는 접근 방안을 제안하고자 한다. 이를 통해 데이터의 프라이버시 보호와 스마트 컨트랙트를 활용한 데이터 접근 제어를 할 수 있다.

Table 2. Abbreviated Name for Access Type

Type	Abbreviation
Data Owner (NFT Minter)	DON
Data Ownership	DOS
Data User (NFT Buyer)	DU
Data Use Rights	DUR

제안하는 접근 방안에서는 모든 데이터를 암호화하여 IPFS에 업로드하고, 해당 링크를 참조하여 데이터 소유권을 나타내는 NFT(DOS)를 생성한다. NFT를 생성한 사용자(DON)는 해당 데이터에 대한 DOS를 얻게 된다. 또한, 동일한 데이터에 접근하고자 하는 사용자(DU)가 있을 경우, DON은 자신의 DOS와 똑같은 데이터를 가지는 사본 NFT (DUR)를 발행하여 DU에게 제공할 수 있다. DU에게 DUR을 제공함으로써, DON은 자신의 소유권은 지키면서 동시에 DU에게 자신의 데이터를 제한적으로 사용할 수 있는 권리를 제공한다.

제안하는 접근 방안의 흐름은 (Fig. 1)과 같으며, 제안하는 접근 방안에서 사용하는 약어는 <Table 2>와 같이 정리하였다. (Fig. 1)의 1~4까지의 과정은 DON이 DOS를 만들기 위한 과정이며, 이 과정에서 암호화 및 컨트랙트를 통한 DOS 발행이 이루어진다. (Fig. 1)의 5~13까지의 과정은 DU가 DUR을 얻기 위한 과정이며, 이 과정에서 컨트랙트를 통한 DUR 발행 및 복호화 과정이 이루어진다.

제안하는 접근 방안의 구성은 1) 원본 데이터 암호화, 2) NFT 발행, 3) NFT 스마트 컨트랙트 설계, 4) 접근 방안 구현 과정으로 분류할 수 있으며, 해당 과정에 대한 자세한 설명은 3.1절에서부터 서술한다.

3.1. Encryption for Original Data

본 논문에서는 원본 데이터의 프라이버시를 보호하기 위해 대칭키와 비대칭키를 사용하여 암호화를 진행한다. 대칭키는 DON이 원본 파일을 암호화하기위해 사용하며, 비대칭

키는 DON이 대칭키를 DU에게 전달하기 위해 사용한다.

대칭키는 랜덤으로 생성된 256자리의 문자열 중 32자리를 추출하여 만들어진다. 256자리의 문자열은 문자로 표현할 수 있는 ASCII 코드 95개 중 공백, 큰따옴표(“”), 역슬래시(＼)를 제외한 92개로 랜덤하게 생성한다. DON은 추출된 32개의 문자열을 시드(Seed)로 사용하여 AES-256(Advanced Encryption Standard) 알고리즘을 통해 원본 데이터를 암호화한다. 또한, 데이터에 접근하고자 하는 사용자에게 32자리의 문자열을 전달한다.

비대칭키는 32자리의 문자열로 만들어진 대칭키를 DU에게 전달하기 위해 사용한다. DON은 DU의 공개키를 사용하여 생성된 대칭키를 다시 암호화하고, 이를 스마트 컨트랙트에 저장한다. DU는 데이터에 접근하기 위해 스마트 컨트랙트에서 해당 값을 불러와 자신의 개인키로 복호화하여 암호화된 데이터에 접근할 수 있다.

3.2. Generate NFT

제안하는 접근 방안에서는 데이터 공유를 위해 데이터의 소유권과 사용권을 분리한다. 소유권은 데이터에 대한 통제권을 갖는 것을 의미하며, 사용권은 데이터에 대한 통제 권리를 부여받는 것을 의미한다[30]. 제안하는 접근 방안에서 소유권 양도는 DON이 DU에게 NFT를 전송함으로써 이루어질 수 있다. 소유권 양도와 달리, 데이터에 대한 사용권 제공은 사본 NFT를 발행한 후 DU에게 제공함으로써 데이터에 접근할 수 있는 권한을 부여할 수 있다.

원본 NFT는 데이터에 대한 소유권을 가지고 있다는 것을 의미한다. 원본 NFT는 DON이 공유하고자 하는 데이터를 NFT로 발행함으로써 만들 수 있다. DON은 대칭키를 활용해 원본 데이터를 암호화하고, 해당 데이터를 IPFS에 저장한다. 이후, 데이터가 저장된 IPFS에 접근할 수 있는 URL(Uniform Resource Locator)을 NFT의 token URI (데이터 저장 주소) 값으로 설정한 후, NFT를 발행한다.

사본 NFT 발행은 원본 NFT를 활용하여 생성할 수 있다. DON은 컨트랙트에 기록했던 원본 NFT의 IPFS URL을 사본 NFT의 tokenURI 값으로 동일하게 설정한다. 추가적으로, 사용권의 유효 기간, 사용 가능 횟수를 나타내는 옵션을 적용하여 사본 NFT 발행 정보를 지정한다. 사용권 옵션은 스마트 컨트랙트에 의해 자동으로 관리되며, 옵션이 만료될 경우, 소각 기능에 의해 사본 NFT를 폐기할 수 있다.

3.3. Design NFT Smart Contract

제안하는 접근 방안을 활용하기 위한 스마트 컨트랙트는 총 32가지의 시나리오에 위배되지 않도록 설계되어야 하며, 각각의 시나리오는 <Table 3>을 통해 정리하였다.

Table 3. 32 Function Call Scenarios

Num	Function Call Scenario Name
1	**[Possible]** Deploy contract
2	**[Possible]** Mint NFT
3	**[Impossible]** Sell not owned NFT
4	**[Possible]** Sell NFT (Owner)
5	**[Impossible]** Sell copied NFT
6	**[Impossible]** Sell burned NFT
7	**[Impossible]** Cancel selling for not owned NFT
8	**[Possible]** Cancel selling for own NFT
9	**[Impossible]** Buy not selling NFT
10	**[Possible]** Buy NFT
11	**[Possible]** Buy copied NFT
12	**[Impossible]** Buy own NFT
13	**[Impossible]** Buy NFT with insufficient token
14	**[Impossible]** Burn not owned NFT
15	**[Possible]** Burn own NFT
16	**[Impossible]** Confirm for not owned NFT
17	**[Possible]** Confirm for copied NFT
18	**[Impossible]** Confirm for own NFT
19	**[Impossible]** Download data of not owned NFT
20	**[Possible]** Download data of own NFT
21	**[Possible]** Download data of copied NFT
22	**[Impossible]** Download data of burned NFT
23	**[Impossible]** Download data after out of time
24	**[Impossible]** Download data after out of number
25	**[Impossible]** Transfer not owned NFT
26	**[Possible]** Transfer own NFT
27	**[Impossible]** Transfer copied NFT
28	**[Impossible]** Decrypt file through IPFS directly
29	**[Impossible]** Decrypt file with wrong key
30	**[Possible]** Decrypt key with findKey value
31	**[Impossible]** Call ownerList update function
32	**[Impossible]** Call saleList update function

<Table 3>에 나타낸 번호 2~13, 17, 18, 31, 32에 해당하는 기능들은 소유권과 사용권을 이용한 접근 제어 방안을 구현하기 위해 원본 NFT 및 사본 NFT 생성 및 공유에 필요한 기능이다.

또한, 14, 15, 19~27에 해당하는 기능들은 사용자가 직접 데이터에 접근하거나, 자신의 데이터를 다른 곳으로 전송하기 위해 필요한 기능들이다.

28~30에 해당하는 기능들은 IPFS에 직접 접근하여 파일을 처리하는 데 필요한 기능이다.

IV. Experiments

본 장에서는 제안하는 접근 방안의 실현 가능성을 알아보기 위해 1) 접근 방안 구현 및 2) 접근 방안의 안정성을 평가하기 위한 두 가지 실험을 진행하였다. 실험은 macOS 환경에서 진행하였으며, 자세한 장비 스펙은 <Table 4>와 같다.

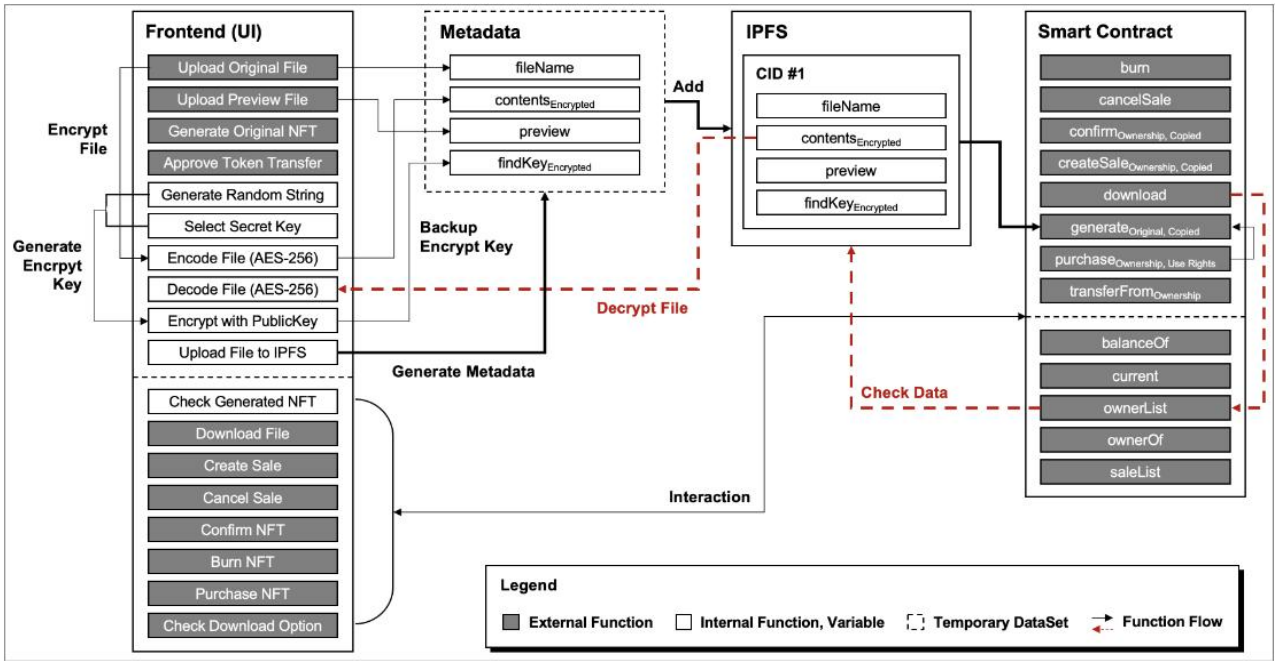


Fig. 2. Entire Process and Data Structure

Table 4. Equipment Specification

Category	Specification
Operating System	macOS Monterey
Processor	2.6 GHz 6-Core Intel Core i7
Memory	16 GB 2667 MHz DDR4
Graphics	AMD Radeon Pro 5300M 4 GB Intel UHD Graphics 630 1536 MB

4.1. Implementation

본 장에서는 BIM 데이터를 판매 및 구매한다는 가상의 시나리오를 설정하여 제안하는 접근 방안의 구현 방법에 대해 서술한다. 구현을 위한 시스템의 전체적인 구조는 (Fig. 2)와 같다.

NFT 컨트랙트는 총 13개의 함수로 동작한다. 각 함수는 소각(burn), 판매 취소(cancelSale), 구매 승인(confirm), 판매 등록(createSale), 원본 파일 다운로드(download), NFT 발행(generate), 구매(purchase), 소유권 이전(transferFrom), NFT 보유 개수 확인(balanceOf), 생성된 토큰 ID 수 확인(current), 소유자 정보 확인(ownerList), 특정 NFT 소유자 정보 확인(ownerOf), 판매 정보 확인(saleList)을 의미한다. 또한, 3.3장에 서술한 것과 같이 시나리오에 위배되지 않고, 모든 기능을 사용할 수 있는 컨트랙트를 배포하였다.

데이터 소유자의 NFT 발행은 generate 함수를 이용하여 NFT를 발행함으로써 시작된다. generate 함수가 호출되면 ownerList가 자동으로 업데이트 된다. 이후, 소유자는 createSale 함수를 통해 자신의 NFT를 판매하거나, cancelSale 함수를 통해 판매를 취소할 수 있다. createSale과 cancelSale 함수가 호출되면 판매 정보인 saleList 값은 자동으로 업데이트 된다.

만약 판매되고 있는 NFT를 구매하고자 하는 사용자가 있는 경우, purchase 함수를 통해 NFT를 구매할 수 있다. 또, NFT를 구매한 경우, 소유자 정보인 ownerList가 자동으로 업데이트 된다. 구매한 사용자는 암호키를 받지 않은 대기 상태로 사본 NFT를 수령하게 되며, 소유자가 confirm 하는 경우, ownerList 상에 사용자를 위한 새로운 암호키 값을 저장한다.

이후, 사용자는 download 함수를 호출하여 원본 데이터를 확인할 수 있게 된다. 만약 사용자가 구매한 NFT의 다운로드 가능 옵션이 모두 소진되어 필요하지 않게 된 경우에는 burn 함수 호출을 통해 NFT를 소각시킬 수 있다. 또, 소유자의 경우, 판매가 아닌 단순히 소유권을 이전하고 싶을 때, transferFrom 함수를 통해 자신의 NFT 소유권을 다른 주소로 이전할 수 있다.

프론트엔드(Frontend)에는 스마트 컨트랙트를 호출하기 전 필요한 과정들을 먼저 구현하였다. 대표적으로는 파일 업로드 및 암호화 기능이 있다. 스마트 컨트랙트상에서 직접 암호화를 진행하는 경우 외부에 암호키가 노출될 가능성이 있고, 난수를 추출하는 과정에서 많은 연산으로 인해 과도한 가스비가 발생할 가능성이 있다. 이를 위해서는 프론트엔드에서 암호화를 수행하며, 대칭키 방식은 crypto-js 모듈, 비대칭키 방식은 eth-crypto 모듈을 사용하였다.

데이터를 업로드하는 과정은 다음과 같다. 프론트엔드에서 원본 파일 업로드(Upload Original File), 미리보기 파일 업로드(Upload Preview File)를 통해 파일을 업로드하며, 암호키 복구를 위해 소유자의 개인키를 추가로 입력해야 한다. 이후, 256자리의 난수 문자열을 생성한 후 그 중에서 임의의 32자리 문자열을 추가로 추출한다. 추출된 32자리의 문자열은 원본 파일 암호화(Encode File)를 통해 대칭키 방식으로 파일을 암호화하는데 사용된다. 또, 암호키 백업을 위한 암호키 재암호화(Encrypt with PublicKey)를 통해 비대칭키 방식으로 암호키를 추가로 암호화한다.

두 번의 암호화 과정이 끝나면, 프론트엔드는 IPFS에 업로드할 메타데이터를 생성한다. 메타데이터는 파일 이름(fileName), 암호화된 원본 파일(contents_Encrypted), 미리보기 파일(preview), 암호키 복구를 위한 재암호화된 암호키(findKey_Encrypted)가 포함되어 있다. 이 메타데이터를 IPFS에 업로드하면 하나의 CID(Content Identifier)가 반환되며, 이 주소를 tokenURI로 하는 NFT를 생성하게 된다. 또한, NFT가 생성되면, 해당 NFT의 소유 정보 및 특성을 ownerList에 기록한다. 사용자가 프론트엔드에서 데이터를 올리는 과정부터 스마트 컨트랙트를 통해 NFT를 발행하는 과정은 (Fig. 3)과 같이 표현할 수 있다. 소유자는 이후에 판매 등록(CreateSale)을 통해 자신의 NFT를 판매할 수 있고, 사용 가능 시간과 횟수 측면에서 옵션을 제한할 수도 있다.

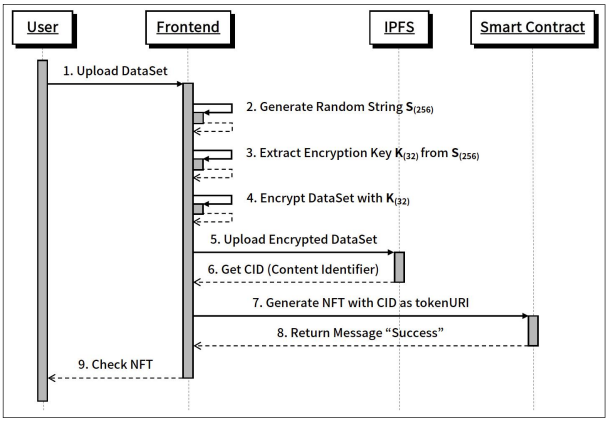


Fig. 3. Process of NFT Generation

다른 사용자가 NFT를 구매 및 다운로드하는 과정은 다음과 같다. 사용자는 프론트엔드에서 구매(Purchase NFT)를 통해 스마트 컨트랙트로부터 해당 NFT에 대한 정보를 불러온다. 만약 사용자가 판매중인 NFT 가격 이상의 ERC-20 토큰[31]을 보유하고 있다면 구매가 가능하며, 구매 즉시 사본 NFT가 발행되어 구매한 사용자에게 전달된다.

하지만 사용자는 암호화된 데이터에 대한 암호키를 가지고 있지 않기 때문에 소유자의 별도 승인이 필요하다. 소유자는 구매한 기록이 스마트 컨트랙트에 남으면 구매 승인(Confirm NFT)을 통해 승인을 요청한다. 이후, 원본 데이터가 있는 IPFS로부터 메타데이터를 다운로드 받은 후, findKey 값으로부터 기존의 암호키를 복원하게 된다. 이 과정에서는 소유자의 개인키가 있어야 복호화가 가능하다.

프론트엔드는 복원된 암호키를 얻는 즉시 구매자의 공개키로 암호키를 재암호화하여 스마트 컨트랙트상에 저장한다. 그렇게 되면 사용자는 스마트 컨트랙트에 저장된 재암호화된 암호키를 복호화해 원본 데이터를 복원할 수 있다. 이 과정에서는 구매자의 개인키가 사용된다.

많은 과정들이 복잡하게 이루어지고 있지만, 실질적으로 구매 승인 기능을 제외한 나머지 기능은 모두 자동화되어 실시간으로 동작하므로 사용자의 입장에서 크게 고려할 요소가 없다. 사용자가 프론트엔드에서 NFT를 구매하고, 원본 데이터를 복원하기까지의 과정은 (Fig. 4)와 같이 표현할 수 있다.

본 장에서는 대칭키 생성에 필요한 32자리 문자열을 추출하는 과정에서의 안전성 분석을 진행한다. Formula (1)은 92가지 문자열을 기반으로 32개의 문자열을 추출한다고 했을 때, 나올 수 있는 경우의 수를 계산하기 위한 수식이다.

$$P(92,32) = \frac{92!}{(92-32)!} = 1.4948E+60 \qquad (1)$$

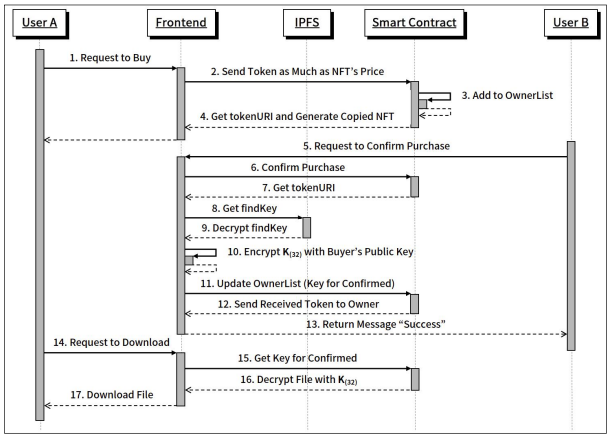


Fig. 4. Process of NFT Purchase and Download

해당 수식에 의하면 92P32는 '1.4948 * 10^60'이라는 수가 나온다. 해당 수는 우리 은하에 존재하는 별의 대략적인 개수인 '6 * 10^11' 보다 큰 수이다. 얼마나 큰 수인지 파악하기 위해, 해당 경우의 수를 계산하는 데 걸리는 시간을 측정하는 실험을 진행하였다. 실험은 추출될 수 있

는 92개의 문자를 사전 정의한 후, 그 안에서 32개의 문자를 무작위 공격(Brute-Force Attack) 방식으로 순차적으로 대입하였다.

<Table 4>에 명시한 장비로 실험을 진행한 결과, 10억 번의 연산을 하는데 약 112분이 소요되었고, 이는 초당 약 14만 9천 번 정도의 연산이 가능하다는 것을 의미한다. 이를 토대로 볼 때, 1년을 계산하더라도 최대 약 '4.698 * 10^12' 정도의 연산량에 그친다. 만약, 초당 10억 번의 연산을 할 수 있는 컴퓨터를 가정한다고 했을 때, 변수 없이 1년을 계산하면 최대 약 '3.1536 * 10^16'이라는 수치가 나오는데, 이 또한 수천 년을 계산하더라도 암호키에 도달하기에는 턱없이 부족한 수치이다. 이를 통해, 일반적인 컴퓨터로 암호키 값을 일일이 찾아내기에는 어려움이 있음을 확인하였으며, 본 논문에서 제안하는 방안이 다소 안전하다고 평가할 수 있다.

V. Conclusions

본 연구에서는 블록체인 기반의 데이터 공유를 위한 접근 제어 방안을 제안하였다. 제안하는 접근 방안은 외부 혹은 내부의 관리자가 존재하지 않더라도 데이터의 접근 제어가 가능하며, 데이터를 암호화하여 공유할 원본 데이터를 보호하였다. 또, 소유권과 사용권을 분리하여 데이터에 대한 접근 권한을 부여하였다.

본 논문은 NFT를 활용한 데이터 접근 제어 방안을 제안하였으며, 제안하는 접근 방안의 검증을 위해 가상 시나리오를 만족하는 스마트 컨트랙트를 구현하였다. 또한, 접근 방안에 대한 안정성 평가도 진행하였다. 실험을 통해 32가지 시나리오에 대해 컨트랙트가 정상적으로 동작함을 확인하였으며, 안전성 실험을 통해 복호화에 대한 무차별 대입 공격의 실현 가능성이 상당히 낮음을 확인할 수 있었다.

본 논문에서 제안하는 방법은 현재 구매 승인 과정이 완전 자동화되지 못하는 문제를 가지고 있기 때문에 향후 이러한 문제를 해결하기 위한 연구를 추가로 진행할 예정이다.

ACKNOWLEDGEMENT

This work is supported by the Korea Agency for Infrastructure Technology Advancement(KAIA) grant funded by the Ministry of Land, Infrastructure and Transport(Grant 22CTAP-C164356-02).

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Decentralized Business Review, 21260, October 2008. https://www.debr.io/article/21260.pdf.

[2] B. Vitalik, "A Next-Generation Smart Contract and Decentralized Application Platform", White Paper, 3(37), 2-1, December 2014. https://nft2x.com/wp-content/uploads/20 21/03/EthereumWP.pdf.

[3] E. Lee, "The Bored Ape Business Model: Decentralized Collaboration via Blockchain and NFTs", Available at SSRN 3963881, November 2021. http://dx.doi.org/10.2139/ ssrn.3963881.

[4] T. A. Xu and J. Xu, "A Short Survey on Business Models of Decentralized Finance (DeFi) Protocols", arXiv Preprint arXiv:2202.07742, February 2022. https://doi.org/10.48550/arXiv.2202.07742.

[5] J. Seo, D. Ko, S. Park, S. Kim, B. Kim, and D. Kim, "Design and Implementation of a Blockchain System for Storing BIM Files in a Distributed Network Environment", Journal of the Korea Society of Computer and Information, vol.26, no.12, pp.159-168, December 2021. https://doi.org/ 10.9708/jksci.2021.26.12.159.

[6] N. O. Nawari and S. Ravindran, "Blockchain and Building Information Modeling (BIM): Review and Applications in Post-Disaster Recovery", Buildings, 9(6), 149, June 2019. https://doi.org/10.3390/buildings9060149.

[7] A. S. E. Pradeep, T. W. Yiu, and R. Amor, "Leveraging Blockchain Technology in a BIM Workflow: A Literature Review", International Conference on Smart Infrastructure and Construction 2019 (ICSIC) Driving Data-informed Decision-making, ICE Publishing, pp.371-380, July 2019. https://doi.org/10.1680/icsic.64669.371.

[8] N. O. Nawari and S. Ravindran, "Blockchain Technology and BIM Process: Review and Potential Applications", J. Inf. Technol. Constr, 24(12), pp.209-238, May 2019. https://www.academia.edu/40578593/Blockchain_technology_and_BIM_process_Review_and_potential_applications.

[9] D. Mohammad and M. Joo, "Protecting BIM Design Intellectual Property with Blockchain: Review and Framework", Proc. of the Conference CIB W78, vol.2021, pp.11-15, October 2021. https://www.researchgate.net/ publication/355195615_Protecting_BIM_Design_Intellectual_Property_with_Blockchain_Review_and_Framework.

[10] J. P. Cruz, Y. Kaji, and N. Yanai, "RBAC-SC: Role-based Access Control using Smart Contract", IEEE Access, 6, 12240-12251, March 2018. https://doi.org/10.1109/ACCESS. 2018.2812844.

[11] H. Guo, E. Meamari, and C. C. Shen, "Multi-Authority Attribute-based Access Control with Smart Contract", Proceedings of the 2019 International Conference on Blockchain Technology, pp.6-11, March 2019. https://doi. org/10.1145/3320154.3320164.

[12] Y. Zhang, M. Yutaka, M. Sasabe, and S. Kasahara,

"Attribute-based Access Control for Smart Cities: A Smart-Contract-Driven Framework", IEEE Internet of Things Journal, 8(8), 6372-6384, October 2020. https://doi.org/10.1109/JIOT.2020.3033434.

[13] R. Xu, Y. Chen, E. Blasch, and G. Chen, "BlendCAC: A Smart Contract-enabled Decentralized Capability-based Access Control Mechanism for the IoT", Computers, 7(3), 39, July 2018. https://doi.org/10.3390/computers7030039.

[14] B. Liu, S. Sun, and P. Szalachowski, "SMACS: Smart Contract Access Control Service", 2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp.221-232, July 2020. https://doi.org/10.1109/DSN48063.2020.00039.

[15] M. Nadini, L. Alessandretti, F. D. Giacinto, M. Martino, L. M. Aiello, and A. Baronchelli, "Mapping the NFT Revolution: Market Trends, Trade Networks, and Visual Features", Scientific Reports, 11(1), 1-11, October 2021. https://doi.org/10.1038/s41598-021-00053-8.

[16] EIP-721: Non-Fungible Token Standard [Internet], https://eips.ethereum.org/EIPS/eip-721 (Checked on 20th September 2022).

[17] EIP-1155: Multi Token Standard [Internet], https://eips.ethereum.org/EIPS/eip-1155 (Checked on 26th September 2022).

[18] S. W. Choi, S. M. Lee, J. E. Koh, H. J. Kim, and J. S. Kim, "A Study on the Elements of Business Model Innovation of Non-Fungible Token Blockchain Game: Based on 'PlayDapp' Case, An in-game Digital Asset Distribution Platform", Journal of Korea Game Society, 21(2), 123-137, April 2021. https://doi.org/10.7583/JKGS.2021.21.2.123.

[19] D. Avrilionis and T. Hardjono, "From Trade-only to Zero-Value NFTs: The Asset Proxy NFT Paradigm in Web3", arXiv Preprint arXiv:2205.04899, May 2022. https://doi.org/10.48550/arXiv.2205.04899.

[20] Q. Zheng, Y. Li, and P. Chen, "An Innovative IPFS-Based Storage Model for Blockchain", 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI). IEEE, pp.704-708, December 2018. https://doi.org/10.1109/WI.2018. 000-8.

[21] M. B. Yassein, S. Aljawarneh, and E. Qawasmeh, "Comprehensive Study of Symmetric Key and Asymmetric Key Encryption Algorithms", 2017 International Conference on Engineering and Technology (ICET). IEEE, pp.1-7, August 2017. https://doi.org/10.1109/ICEngTechnol.2017. 8308215.

[22] N. M. M. Alhag and Y. A. Mohamed, "An Enhancement of Data Encryption Standards Algorithm (DES)", 2018 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE). IEEE, pp.1-6, August 2018. https://doi.org/10.1109/ICCCEEE.2018.8515843.

[23] A. Menezes and D. Stebila, "The Advanced Encryption Standard: 20 Years Later", IEEE Security & Privacy, 19(6), 98-102, October 2021. https://doi.org/10.1109/MSEC.2021. 3107078.

[24] ARIA (Academy Research Institute Agency) [Internet], https://seed.kisa.or.kr/kisa/algorithm/EgovAriaInfo.do (Checked on 29th September 2022).

[25] M. A. Al-Shabi, "A Survey on Symmetric and Asymmetric Cryptography Algorithms in Information Security", International Journal of Scientific and Research Publications (IJSRP), 9(3), 576-589, March 2019. https://doi.org/10. 29322/IJSRP.9.03.2019.p8779.

[26] F. Mallouli, A. Hellal, N. S. Saeed, F. A. Alzahrani, "A Survey on Cryptography: Comparative Study between RSA vs ECC Algorithms, and RSA vs El-Gamal Algorithms", 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom). IEEE, pp.173-176, June 2019. https://doi.org/10.1109/CSCloud/EdgeCom.2019.00022.

[27] Y. Yusfrizal, A. Meizar, H. Kurniawan, and F. Agustin, "Key Management using Combination of Diffie-Hellman Key Exchange with AES Encryption", 2018 6th International Conference on Cyber and IT Service Management (CITSM). IEEE, pp.1-6, August 2018. https://doi.org/10.1109/CITSM.2018.8674278.

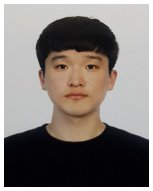
[28] M. U. Aftab, Z. Qin, Zakria, S. Ali, Pirah, and J. Khan, "The Evaluation and Comparative Analysis of Role based Access Control and Attribute based Access Control Model", 2018 15th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP). IEEE, December 2018. https://doi.org/ 10.1109/ICCWAMTIP.2018.8632578.

[29] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A Novel Attribute-based Access Control Scheme using Blockchain for IoT", IEEE Access 7, 38431-38441, March 2019. https://doi.org/10.1109/ACCESS.2019.2905846.

[30] F. Thouvenin and A. Tamo-Larrieux, "Data Ownership and Data Access Rights: Meaningful Tools for Promoting the European Digital Single Market?", Big Data and Global Trade Law, M. Burri, Ed. Cambridge: Cambridge University Press, pp.316-339, July 2021. http://dx.doi.org/ 10.1017/9781108919234.020.

[31] EIP 20: Token Standard [Internet], https://eips.ethereum.org/EIPS/eip-20 (Checked on 20th September 2022).

Authors



Yoonsung Jeong is currently M.S degree student in Computer Science and Engineering from Sogang University. Yoonsung Jeong's research interests are in blockchain, especially for NFT and massive amount of data management.

Deokyoon Ko holds Ph.D in Computer Science from Sogang University, M.S. in Software Engineering from Sogang University, and B.S. at Myungji University. Dr. Deokyoon Ko is CEO of Noncelab Inc. He is interested in Blockchain Key Recovery and Blockchain business.

Jungwon Seo received M.S degree in Computer Science and Engineering from Sogang University, Korea in March 2020, and is currently pursuing Ph.D degree. Jungwon Seo's research interests are in blockchain and Consensus Algorithm.

Professor Sooyong Park holds Ph.D in Information Technology from George Mason University, M.S. in Computer Science from the Florida State University, and B.S. at Sogang University.
Dr. Sooyong Park is currently Director of Blockchain Research Center at Sogang University sponsored by Korean Government and was a President & CEO of National IT Industry Promotion Agency (NIPA) from September, 2012 until November 14, 2014. Before joining NIPA, he was a computer science professor (March, 1998-September, 2012) and dean of Graduate School of Information and Technology (March, 2011-September, 2012) at Sogang University.

Seong-Jin Kim received his B.S., M.S. degree in Industrial Engineering from Keimyung University, Korea in 1995 and 2001, respectively. He has been working in KICT since 2001. He is currently a Senior researcher at KICT. He is in charge of development of Construction CALS Project. He is interested in Electronic Document, Blockchain and Construction Information System.

Bum-Soo Kim received his Ph. D. (2013) degrees in computer science from Kangwon National University. From 2013 to 2017, he was a postdoctoral researcher in KAIST (2013 and 2015), Kangwon National University (2014), Korea University (2016-2017), and KICT (2017-2020). He is currently a senior researcher in Department of Future & Smart Construction Research from KICT. His research interests include time-series data mining, construction bigdata analysis, blockchain and AI.

Do-Young Kim received the Ph.D. degrees in architectural planning from Sungkyunkwan University, Korea, in 2018. Research areas include BIM, generative design, and smart construction -based regulatory improvement.
Kim joined the Department of Architectural Planning at Sungkyunkwan University, Suwon, Korea, in 2010. She is currently a postdoctoral researcher in the Department of Future & Smart Construction Research, Korea Institute of Civil Engineering (KICT). She is interested in 3D scanning, AI, and IoT.