블록체인 환경에서 스마트 컨트랙트를 활용한 사용자 동적 접근제어 메커니즘

[1*]조도은

User Dynamic Access Control Mechanism Using Smart Contracts in Blockchain Environment

[1*]Do-Eun Cho

요 약

최근 블록체인 기술을 다양한 분야에 활용하기 위한 연구가 활발히 진행되고 있다. 특히 블록체인 기반의 스마트 컨트랙트는 분산 원장 환경에서 데이터를 기록하여 데이터의 무결성과 유효성이 검증되며, 미리 작성되어 등록된 코드에 의하여 설정된 조건이 충족되면 자동으로 이행되는 특징을 가지고 있어서 신뢰성을 요구하는 다양한 자동화 시스템에 적용되고 있다. 그러나 블록 체인에서는 네트워크 참여자들에게 데이터가 공유되기 때문에 데이터 접근 제어와 정보의 보안이 이루어지지 못하고 있다. 본 논문에서는 블록체인 환경에서 스마트 컨트랙트를 활용한 사용자 동적 접근 제어 메커니즘을 제안한다. 제안된 메커니즘은 사용자가 데이터 접근시 사용자의 상황정보를 판별하여 사용자의 역할을 할당하고 데이터 접근 범위를 동적으로 제어한다. 이는 네트워크 시스템의 사용자 그룹별로 할당된 역할로 동일한 서비스를 제공하기 보다는, 사용자 인증 시점에 동적으로 데이터 접근 권한을 부여함으로써 시스템의 보안성과 데이터 관리의 효율성을 증가시킬 수 있다. 제안된 메커니즘은 블록체인 네트워크 내에 저장된 데이터의 보안성을 강화하기 위해 사용자의 동적인 데이터 접근 제어를 통해 유연한 인증 기능을 제공할 수 있을 것으로 기대된다.

Abstract

Recently, research has been actively conducted to utilize blockchain technology in various fields. In particular, blockchain-based smart contracts are applied to various automation systems that require reliability as they have the characteristics of recording data in a distributed ledger environment to verify the integrity and validity of data. However, blockchain does not provide data access control and information security because data is shared among network participants. In this paper, we propose a user dynamic access control mechanism utilizing smart contracts in blockchain environments. The proposed mechanism identifies the user's contextual information when accessing data, allocating the user's role and dynamically controlling the data access range. This can increase the security of the system and the efficiency of data management by granting data access dynamically at the time of user authentication, rather than providing the same services in roles assigned to each user group of the network system. The proposed mechanism is expected to provide flexible authentication capabilities through dynamic data access control by users to enhance the security of data stored within blockchain networks.

Keywords: *IoT Security, Blockchain, Access Control, Security Policy, Smart Contracts*

[1*] *목원대학교 SW 교양학부 교수 (decho@mokwon.ac.kr)*

Received: Feb. 27, 2021, Revised: Mar.10, 2021, Accepted: Mar.18, 2021

I. 서론

사물인터넷(IoT, Internet of Things)을 이용한 기술이 발전함에 따라 IoT 환경에서 개인정보를 수집 및 수집된 데이터의 활용 사례가 급증하고 있다. 이에 따라 IoT 환경에서 보안성을 높일 수 있는 방안으로 블록체인을 적용한 연구가 진행되고 있다. 가트너(Gartner)는 블록체인(Blockchain) 기술을 미래의 유망한 기술로 발표하였다[1]. 블록체인은 P2P(Peer-to-peer)환경에서 안전하게 데이터를 저장할 수 있는 기술이다. 블록체인에 등록된 데이터는 수정이 불가능하므로 저장된 데이터의 신뢰성과 무결성이 보장된다[2]. IoT 환경에서도 블록체인을 활용하면 디바이스들 간의 서비스와 리소스 공유를 촉진할 수 있고, 암호화 방식으로 검증 가능하도록 자동화함으로써 보안 취약점을 보완할 수 있다는 연구가 활발히 진행되고 있다[3-4]. 하지만 IoT 환경에서는 작은 데이터들이 빈번하게 생성되고 저장되는 특성을 가지고 있으므로 블록체인 기술을 적용하기 위해서는 빠른 속도로 블록을 생성하고 트랜잭션을 처리할 수 있는 환경의 필요성이 제기되고 있다.

최근에는 블록체인 기술 기반에 스마트 컨트랙트(Smart Contract) 기능을 구현하기 위한 분산 컴퓨팅 플랫폼인 이더리움(Ethereum)을 다양한 분야에 활용하기 위한 연구가 진행되고 있다. 특히 스마트 컨트랙트는 분산 원장 환경에서 데이터를 기록하여 데이터의 무결성과 유효성이 검증되며, 미리 작성되어 등록된 코드에 의하여 설정된 조건이 충족되면 자동으로 이행되는 특징을 가지고 있어서 신뢰성을 요구하는 다양한 자동화 시스템에 적용되고 있다. 오늘날 스마트 컨트랙트는 보안성과 신뢰성을 필요로 하는 분야로 일정한 형식의 반복적인 계약이나, 원격자 간 계약 체결, 제품의 유통 추적 등의 분야에서 우선적으로 도입되고 있으며, 그 외에도 스마트 컨트랙트를 통하여 디바이스들 간의 제어, 데이터 접근을 용이하게 하는 의료시스템 등 보안성과 자료 접근 문제를 해결하려는 다양한 분야의 적용이 시도되고 있다[5-7]. 하지만 블록체인이 가진 분산 원장 환경의 특성상 거래되는 데이터가 모든 네트워크 참여자들에게 공유되기 때문에 기밀성이 요구되는 데이터는 저장하지 못한다는 문제가 있다.

본 논문에서는 블록체인 네트워크 내에 저장된 데이터의 보안성을 강화하기 위해 사용자의 데이터 접근 제어를 통해 유연한 인증 기능을 제공하고자 한다. 유연한 인증 기능이란 네트워크 시스템의 모든 서비스에 동일한 수준의 인증을 요구하기 보다는, 사용자 인증 시점에 동적으로 데이터 접근 권한을 부여함으로써 데이터의 보안성과 시스템 관리의 효율성을 증가시키고자 한다. 따라서 최근 연구가 활발한 블록체인 환경에 스마트 컨트랙트를 활용한 사용자 동적 접근 제어 방법에 대해 제안한다.

본 논문의 구성은 다음과 같다. 2 장에서는 블록체인과 스마트 컨트랙트, 사용자 접근제어 기법에 대해 살펴본다. 3 장에서는 스마트 컨트랙트를 활용한 사용자 동적 접근 제어 메커니즘에 대해 기술한다. 4 장에서는 제안한 메커니즘의 적용 예와 수행과정을 설명하고, 5 장에서 결론을 맺는다.

II. 관련 연구

2.1 블록체인(Blockchain)

블록체인은 P2P(Peer-to-Peer)환경에서 클라이언트들에게 데이터 사본을 공유하여 신뢰성 있게 자료를 관리하는 분산원장 네트워크 기술이다. 블록체인은 블록이 사슬처럼 연결되어 있으며, 각 블록은 해시 값((Hash Value)으로 식별되어 이전 블록의 해시를 참조함으로써 연결된다. 블록체인에서 블록이 연결되는 구조는 그림 1 과 같다.

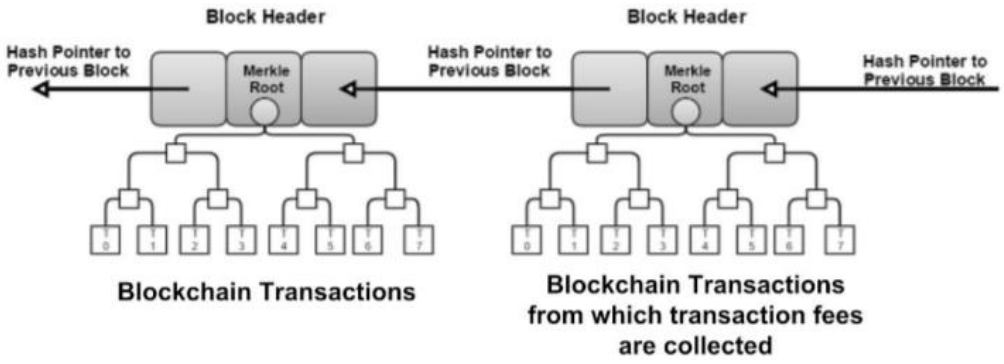

Figure 1. Blockchain Connection Structure[8]
그림 1. 블록체인 연결 구조

전통적 클라이언트-서버 구조에서는 서버 컴퓨터가 클라이언트 요청을 받아 요구 사항을 처리하는 연산을 수행한다. 이러한 구조에서 서버의 연산 과정이 클러이언트에게 투명하게 공개되지 않으며, 프로그램 오류가 발생하거나 자료의 연산이 조작될 가능성이 있다. 그러나 블록체인은 합의 과정을 통해서 신뢰성 있게 자료 연산을 수행한다. 합의 과정은 일반적으로 특정 기관 또는 여러 기관들이 운영하는 다수의 컴퓨터상에서 수행된다. 합의 과정을 수행하는 컴퓨터들은 사용자의 요청 사항에 따라 자료 연산을 수행하고, 수행 결과를 합의 알고리즘을 통해 상호 검증하여 연산의 신뢰성을 높인다. 또 블록체인의 합의 결과는 사용자에게 배포함으로써 자료 연산 과정을 투명하게 공개하여 사용자 요청 내용, 요청의 처리 결과를 확인할 수 있다. 따라서 블록체인은 사용자들이 자료를 공유함으로써 자료를 임의로 변경하는 것은 매우 어렵다[9-10].

블록체인은 은행 등 제 3 의 중개기관이 없더라도 블록체인 기술을 통해 신회성 있는 안전한 거래를 할 수 있다. 블록체인은 암호화폐뿐 아니라, 온라인 거래와 이력 관리 서비스에 활용될 수 있으며, 계약 및 물류관리, 문서관리, 의료정보관리, 저작권 관리 등 다양한 활용이 가능하다.

블록체인은 활용의 목적과 데이터 관리 방식, 참여자의 범위에 따라 퍼블릭(public) 블록체인, 프라이빗(private) 블록체인, 하이브리드(hybrid) 블록체인으로 구분된다. 퍼블릭 블록체인은 누구나 접근 가능한 개방형 블록체인으로 채굴 등 알고리즘을 통해 거래를 증명하여 거래 신뢰도를 높이고 익명성을 보장하는 장점이 있어 비트코인 등 암호화폐 시장의 기반 플랫폼으로 활용되고 있다. 하지만 익명화된 상태에서 거래를 증명하는 알고리즘이 많은 계산량을 요구한다. 프라이빗 블록체인은 승인된 사용자만 접근이 가능하도록 통제하는 형태로 기업들의 요구에 맞게 적용 가능한 기업형 블록체인이라 할 수 있다. 중앙 기관에서 트랜잭션을 증명하기 때문에 빠르고 효율적인 거래처리가 가능하지만 중앙기관에 의존하기 때문에 퍼블릭 블록체인보다는 안전성이 부족하다. 하이브리드 블록체인은 프라이빗 블록체인처럼 승인된 사용자만 접근 가능하지만 조직 간의 협조적인 참여를 허용한다. 사전 합의된 규칙으로 빠르게 거래를 증명하며 사용자 권한을 관리하여 민감한 정보를 제어할 수 있다[11].

2.2 스마트 컨트랙트(Smart Contract)

1994 년 암호학자인 Nick Sazbo 는 신뢰할 수 없는 컴퓨터 네트워크 환경에서 고도로 발달된 자동계약 이행 방법을 제시하는 스마트 컨트랙트를 고안하였다[12]. 스마트 컨트랙트는 블록체인 안에 컴퓨터 코드로 프로그램된 분산된 합의로 정의되며, 계약의 성립과 이행이라는 블록체인의 두 과정을 하나로 합친것이라 할 수 있다.

스마트 컨트랙트는 프로그램 형태로 작성된 스마트 계약서로, 계약 이행 요청 시 미리 프로그램된 계약 조건에 따라 계약 내용을 수행한다. 대부분의 블록체인 시스템은 스마트

컨트랙트의 등록, 삭제 기능을 제공하고 있으며, 블록체인에 등록된 스마트 컨트랙트를 호출함으로써 계약 이행을 요청할 수 있다.

블록체인 서비스의 수행 과정은 스마트 컨트랙트의 호출과 이에 대한 수행 결과로 볼 수 있다. 블록 체인은 사용자 요청을 트랜잭션 형태로 받아서, 합의 과정을 통하여 트랜잭션 수행 순서 및 수행 결과를 결정하고, 합의 결과를 블록에 저장하여 모든 사용자에게 배포한다. 블록체인의 사용자 요청은 스마트 컨트랙트 호출에 해당하며, 이에 대한 수행 결과는 블록에 저장되어 사용자에게 배포된다[10, 13].

그림 2 는 스마트 컨트랙트 실행과정을 나타낸 것이다. 스마트 컨트랙트를 구현하기 위한 컨트랙트 코드(contract code)는 이더리움 가상머신(EVM; Ethereum Virtual Machine)이라는 독립된 실행 환경에서 실행된다. 이더리움에서 스마트 컨트랙트는 Solidity 언어로 프로그래밍된다. 프로그래밍된 스마트 컨트랙트는 컴파일러(solc)에 의해 바이트코드(bytecode)로 컴파일되고, 컴파일된 바이트코드는 블록에 포함되어, 이더리움 가상머신(EVM)에 의해 실행된다. 이더리움 가상머신(EVM)은 이더리움 스마트 컨트랙트의 바이트코드를 실행하는 32 바이트 스택 기반의 실행환경이다[10].

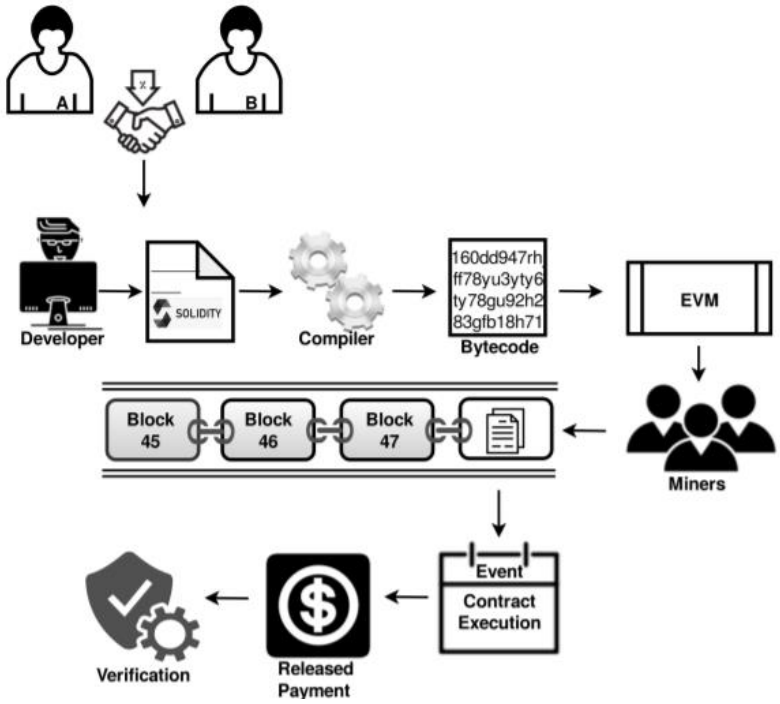

Figure 2. Total cycle of smart contract execution over Ethereum blockchain[14]
그림 2. 이더리움 블록체인을 통한 스마트 컨트랙트 실행 사이클

블록체인 기반 스마트 컨트랙트는 기본적으로 모든 트랜잭션 로그가 저장된 블록체인 데이터베이스와 스마트 컨트랙트의 상태를 저장하는 데이터베이스가 존재한다. 스마트 컨트랙트는 상태를 변경할 수 있는 어플리케이션이라고 할 수 있고, 스마트 컨트랙트의 상태는 해당 어플리케이션에서 사용하는 변수라고 할 수 있다. 스마트 컨트랙트는 트랜잭션(transaction)과 쿼리(query)라는 두 가지 인터페이스를 공개하고 있다. 트랜잭션을 통한 인터페이스는 트랜잭션 데이터베이스에 저장되고, 스마트 컨트랙트의 상태를 변경시키는 접근방법이다. 쿼리는 트랜잭션 데이터베이스에 기록이 남지 않으면서 스마트 컨트랙트의 상태를 읽는 작업이다. 트랜잭션은 쓰기, 삭제, 수정을 실행하고, 쿼리는 읽기를 통한 조회만을 실행한다. 예를 들어 '상품 거래' 과정에서 스마트 컨트랙트는 다음과 같이 작동한다[15].

• **기록 저장** : 판매자가 상품을 등록의 트랜잭션을 만든 후 블록체인에 전송한다. 상품 등록 트랜잭션 발생 시, 네트워크의 모든 노드는 상품 등록 트랜잭션을 공유하고 블록을 생성한 후 블록을 브로드캐스팅한다. 블록을 전달받은 각 노드는 해당 블록을 자신의 블록체인 맨 마지막에 추가하고, 해당 블록에 저장되어 있는 트랜잭션을 적용시켜 자신의 스마트 컨트랙트 데이터베이스를 동기화한다. 이러한 과정을 통해 모든 블록체인의 노드들이 스마트 컨트랙트 상태 데이터베이스를 공유하게 된다.

• **상품 조회** : 구매자는 블록체인 네트워크에서 상품을 조회한다. 스마트 컨트랙트에 "쓰기"는 트랜잭션을 발생시키지만, 이미 저장되어 있던 값을 읽어 오는 것은 트랙잭션을 발생시키지 않는다. 블록체인의 스마트 컨트랙트 데이터베이스 내 저장된 상태 값만 조회하면 되기 때문에 쿼리 정보는 블록체인에 동기화할 필요 없고, 블록 동기화 타이밍에 상관없이 바로 응답할 수 있다.

• **계약 이행** : 구매자가 상품 구매 트랜잭션을 보내면 트랜잭션을 공유하고 블록체인 네트워크에 동기화한다. 모든 노드의 스마트 컨트랙트 데이터베이스에 상품 구매자를 등록하고 돈을 판매자에게 전송한다. 그러면 등록된 콘텐츠의 소유권이 구매자에게로 이동한다.

오늘날 스마트 컨트랙트는 보안성과 신뢰성을 보장하는 특성상 다음과 같이 활용될 수 있다.

보험업에서 특정 조건을 만족시키면 계약 보상금이 지급되도록 스마트 컨트랙트를 작성함으로써, 조건 충족 시 보험금이 자동으로 지불되도록 할 수 있으며, 보험 업무를 신속하고 정확하며 투명하게 처리할 수 있다. 은행에서는 고객이 한 은행에서 공동 인증서를 발급 받으면 다른 은행에서도 간단한 인증만으로 거래 은행의 모바일 뱅킹 서비스를 편리하게 이용할 수 있다. 또한 저작권 관리로 저작물의 소유권을 관리하고, 저작물 구입 관련 거래 정보를 투명하게 공유하며, 지적재산권을 보호할 수 있다. 뿐만 아니라 공유경제로 집 또는 자동차를 공유하기 위해 계약 조건을 정하고 이에 따라 금전 지급 및 서비스 제공이 이루어지도록 스마트 계약을 실행하면, 중개업체를 거치지 않는 사용자 간 직접 거래가 실현될 수 있다. 물류 유통에서는 제품의 유통 추적이 필요한 분야인 전 세계 식품 유통에 관여하는 생산자, 공급자, 운영자, 배급업체, 유통업체, 규제당국, 소비자 등이 모두 블록체인 상에서 식품 오염 이력을 확인하고, 이에 따른 대금 지불이 가능하다.

2.3 접근 제어(Access Control)

접근제어란 시스템이 인증된 주체(subject)가 객체(object)에 접근하는 것을 승인 또는 거절하는 것을 의미한다. 시스템은 일반적으로 주체에게 할당된 접근 권한에 따라 접근제어를 수행한다.

역할 기반 접근제어(RBAC : Role Based Access Control)는 주체에 해당하는 사용자(user)의 역할과 객체들의 관계로 접근 권한을 제어하는 방법이다. 조직 내의 그룹화된 역할로 주체를 구분할 수 있는 대규모 시스템에서 접근제어를 관리하는 데 효율적이다.

역할기반 접근제어 모델은 데이터에 접근하고 연산을 수행할 수 있는 권한이 역할(Role)에 할당되고, 역할이 사용자(user)에게 할당됨으로써 사용자가 접근권한(Permission)을 획득한다. RBAC는 역할과 객체간의 관계로 접근 권한을 관리함으로써 사용자와 객체의 수가 많고, 그 구성이 수시로 변할 수 있는 분산 컴퓨팅 환경에서 효율적이다. 또한, 역할 간 계층구조를 통해 하위 역할에 할당된 권한이 상위 역할에 의해 사용될 수 있는 권한 상속을 제공한다. 권한상속을 이용하여 계층구조를 가진 역할들에 대한 권한 부여를 보다 효과적으로 수행할 수 있다. 이러한 방식은 권한 관리를 단순화 시킬 뿐만 아니라, 접근 보안정책을 구현하는데 있어서 유연성을 제공하는 장점이 있다[16].

Sandhu 는 역할기반 접근제어 기술에 대해 다음과 같은 네 가지 모델로 구분하였다. 역할기반 접근제어의 기본 모델인 $RBAC_0$ 과 기본 모델에 역할의 상속 개념인 역할 계층을 추가한 $RBAC_1$, 기본 모델에 제약 조건을 추가한 $RBAC_2$, $RBAC_0$ 에 역할 계층과 제약 조건을 추가한 $RBAC_3$으로 구분하였다[17]. 그림 3 은 역할 기반 접근제어 모델을 나타낸 것이다.

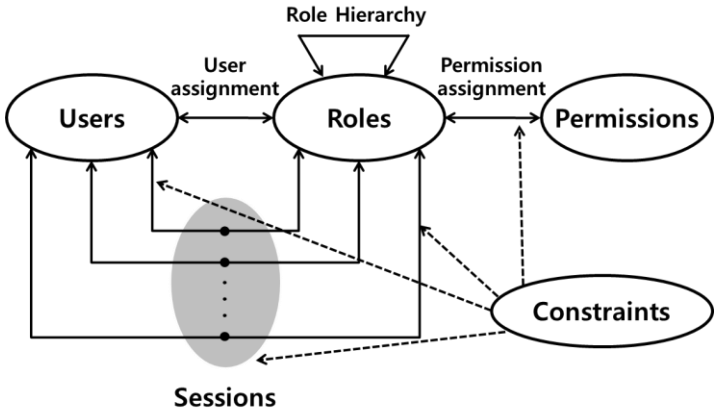

Figure 3. Role base access control model[16]
그림 3. 역할 기반 접근 제어 모델

역할기반 접근제어 모델은 접근 권한을 역할에 따라 그룹화하고, 사용자 개개인의 책임과 권한을 역할에 부여하여 자원에 대한 접근 제어를 통해 보안 서비스를 제공함으로써 자원의 보안 관리에 효율성을 극대화시켰다. 그러나 사용자의 접근 시간과 접근 위치와 같은 상황에 따른 접근 제어는 수행 할 수 없다.

Gustarf Neumann 과 Mark Strembeck 는 상황정보를 접근 제어 결정에 이용하기 위하여 역할기반 접근제어에 제한사항을 사용하는 xoRBAC 모델을 제안하였다[18]. 상황 제한 사항(context constraint)은 상황을 표현하는 규칙에 따라서 접근 제어를 수행하는 방법이다. 상황 제한 사항은 상황정보 속성을 미리 정의된 조건과 비교하는 역할 기반 접근제어 제한사항으로 사용자가 특정 연산을 수행하기 위한 요청의 허용여부를 결정하기 위해 상황정보 속성이 충족되어야 할 조건을 기술한다. 상황 제한 사항은 속성(context attribute), 함수(context function), 조건(context condition)의 튜플(tuple)을 갖는다. 속성은 시간이나 위치 등 변화하는 속성을 나타내거나 소유 관계와 같은 객체의 인스턴스에 따라 변화하는 속성을 나타낸다. 권한 결정은 특정 주체 또는 역할이 상황 제한 요소에 따라 결정된다. 권한은 여러 개의 상황 제한과 관련되고, 모든 상황 제한 사항이 참값을 가질 때 접근이 허용된다. 주체의 주변 환경에서 발생하는 데이터를 분석하여 해당 상황을 식별한 뒤, 접근 규칙을 적용하여 객체의 접근 여부를 결정한다. 상황인식 기반 접근 제어는 상황 변화가 많은 서비스 제공 시스템에 매우 효과적이다. 주변의 많은 디바이스에 존재하는 센서들을 이용하여 즉각적인 상황의 정보를 활용한 접근제어가 가능하다. 또한 누적인 메타 데이터를 이용하여 기존의 규칙을 갱신할 수 있다[16]. 그림 4 는 xoRBAC 모델을 나타낸 것이다.

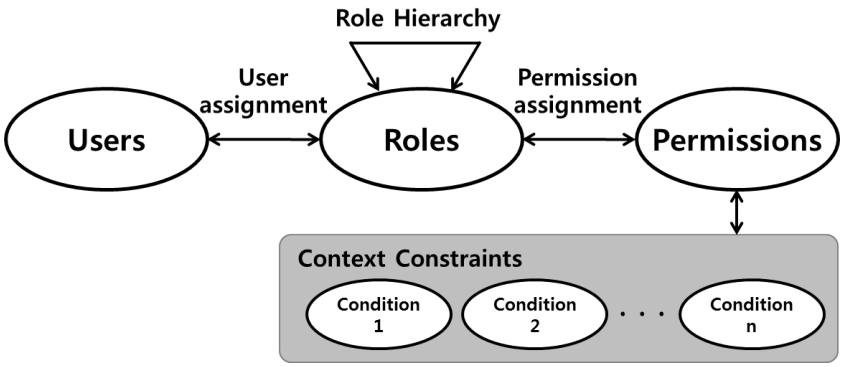

Figure 4. xoRBAC model[16]
그림 4. xoRBAC 모델

접근제어 정책은 환경의 특성에 따라 다양한 방식을 고려할 수 있다. 예를 들어 IoT 환경은 기존 인터넷 환경과 다르게 짧은 시간 동안 상호 작용이 일어나고, 동일한 요청이 빈번하게 일어난다. 또한 요청에 대한 접근제어 결과도 고정적이지 않고 주변의 상황에 따라서 바뀔 수 있고, 네트워크의 확장성이나 권한 위임과 같은 요구 사항이 있을 수도 있다. 따라서 접근제어 기법은 새로운 환경이나 요구 사항을 반영하기 위한 연구가 활발히 진행되고 있으며, 주어진 환경의 문제를 고려하여 적절한 접근제어 기법을 선택하고 개선이 필요하다. 최근 연구에서는 IoT 환경에 적합한 접근 제어를 제공하기 위해서 블록체인(Blockchain)을 적용하는 연구도 있다. 그러나, 블록체인을 사용할 경우 토큰 기반 권한과 자원 소유자만이 접근을 해야만 하는 조건이 있기 때문에 안전성 측면에서 접근 제어 보장이 완벽하지 않은 문제점이 있다[11].

III. 스마트 컨트랙트를 활용한 사용자 동적 접근 제어 메커니즘

본 장에서는 블록체인 환경에서 스마트 컨트랙트를 활용하여 역할에 상황정보를 더한 동적 접근 제어 모델을 제안한다. 객체는 동적 접근제어 모델으로 보안 서비스를 제공하며, 접근제어 메커니즘에 있어서 접근제어 규칙을 생성하고 접근제어 결정을 위한 기준으로 상황정보를 사용한다.

3.1 동적 접근 제어 모델

제안하는 동적 접근 제어 모델은 역할 기반 접근제어 모델 기반에 접근하는 사용자의 상황정보를 고려하여 접근을 제어한다. 본 모델은 프라이빗 블록체인 네트워크내의 사용자들, 모바일 기기 및 컴퓨터를 포함하는 장치, 그리고 블록체인 서비스의 특성을 고려하여 구성하였다. 그림 5 는 본 논문에서 제안하는 동적 접근제어의 기본 모델로 구성요소에는 주체(Subject), 역할(Role), 객체(Object), 상황 정보(Context)가 있다.

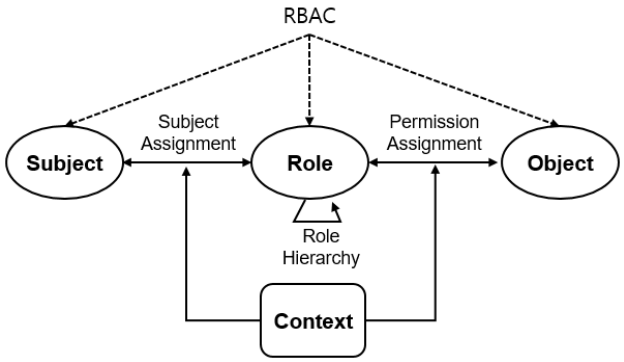

Figure 5. Proposed Dynamic Access Control Model
그림 5. 제안하는 동적 접근 제어 모델

주체(Subject)는 프라이빗 네트워크내의 시스템 자원을 사용하기 위해 능동적으로 접근 권한을 요청하는 요소이며, 사용자 그룹별로 접근 권한이 부여되어 있는 하나 이상의 기본 역할이 배정 된다. 주체는 프라이빗 네트워크 환경의 관리자에 의해 등록되고 관리된다. 역할(Role)은 주체가 소속된 그룹의 객체(Object)에 대한 접근 권한이 부여되는 구성 요소이다. 역할은 그 역할에 소속된 모든 주체에게 기본 역할이 적용되며, 주체가 접근 요청시 상황정보를 고려하여 보안 정책에 따라 주체의 역할이 동적으로 변경 된다. 역할 간 계층구조를 통해 하위 역할 요소에 할당된 권한이 상위 역할 요소에 의해 사용될 수 있도록 권한 상속을 제공한다. 객체(Object)는 주체가 접근 권한을 요청하는 대상으로 특정한 기능을 수행하는 수동적 개체인 자원의 집합이다. 블록체인 네트워크에서 접근 권한을 요청하는 시점에 주체와 객체로 나뉘어

접근제어가 이루어진다. 상황정보(Context)는 제안하는 보안 모델에 동적인 특성을 부여하는 요소로 보안 정책에 부합하는 접근제어 결정에 이용하는 입력 값이다. 이는 주체가 객체에 접근 요청시 접속 기기 또는 네트워크 환경 정보를 사용할 수 있으며, 동적 접근제어 규칙을 생성하기 위해 사용된다.

3.2 스마트 컨트랙트를 적용한 사용자 동적 접근 제어 시스템

제안하는 동적 접근제어 모델은 블록체인 네트워크 기반의 프라이빗 네트워크 환경에서 구현된다. 관리자에 의해 구현된 접근 정책을 블록체인에 기록하고, 네트워크의 사용자 모두가 블록체인을 공유함으로써 데이터의 무결성을 보장할 수 있다. 또한 저장된 데이터의 보안성을 위해 사용자 접근시 상황에 따라 동적인 접근 권한을 부여하여, 권한 관리와 서비스 제공여부를 판단하게 함으로써 동일 사용자라 할지라도 상황 정보에 따라 접속 보안 정책을 다르게 적용한다. 그림 6 은 제안된 접근 제어 메커니즘의 시스템 구조를 표현한 것이다. 사용자에 의한 자료 접근 요청이 발생하는 경우 서비스 에이전트에서 사용자 권한을 블록체인 네트워크에 요청하고, 스마트 컨트랙트에 의해 허가된 사용자로 확인되는 경우 자료에 접근이 가능하다.

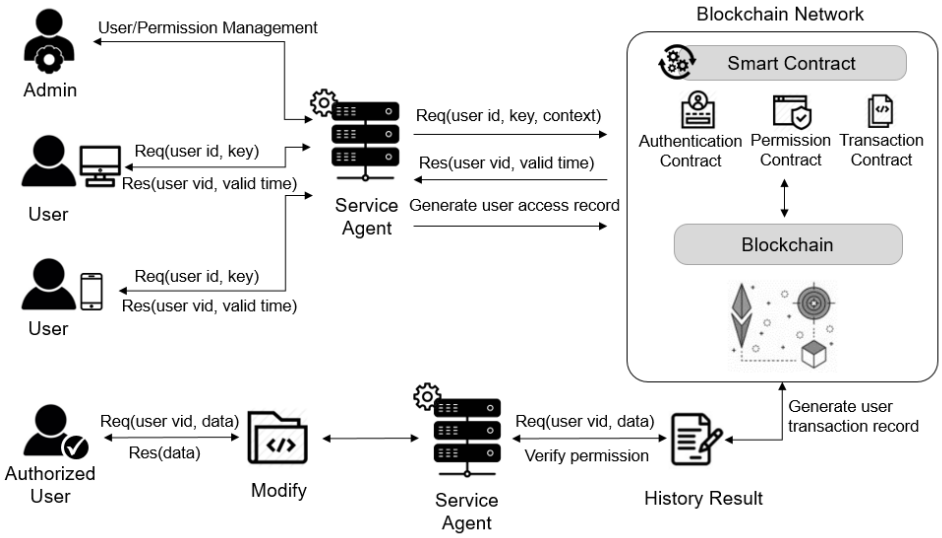

Figure 6. Proposed User Dynamic Access Control System Structure Using Smart Contracts
그림 6. 스마트 컨트랙트를 활용한 사용자 동적 접근제어 시스템 구조

관리자(admin)는 사용자의 데이터 접근 권한에 대한 정책 생성 및 수정을 수행한다. 사용자 접근 권한 변경이 필요한 경우, 서비스 에이전트(Service Agent)에 변경 요청을 한다. 관리자 인증이 완료되면 서비스 에이전트는 블록체인 네트워크에 기록된 접근 권한 목록을 요청하고, 해당 목록을 관리자에게 반환한다. 관리자는 이후 변경 내용을 서비스 에이전트에 전달하고, 서비스 에이전트는 관리자의 정보와 관리자가 요청한 변경 기록을 블록 데이터로 생성하여 블록 체인 네트워크에 기록하며, 블록 네트워크는 생성된 블록의 결과를 서비스 에이전트에 전달한다. 사용자(User)는 데이터 접근 요청을 할 수 있다. 사용자는 데이터 요청을 위해 서비스 에이전트에 자신의 ID 와 인증키를 전송하고, 동적인 접근 권한을 할당 받는다. 서비스 에이전트(Service Agent)는 사용자의 요청을 받으면 사용자의 권한을 확인하기위해 사용자 식별정보와 상황 정보(Context)를 확인한다. 이는 접근 가능한 사용자가 접근 요청을 하는 경우에 상황에 따라 데이터 접근을 제한하기 위해서이다. 블록체인 네트워크(Blockchain Network)에서는 사용자의 권한 기록 대조 요청을 받으면 스마트 컨트랙트에 의해 사용자 권한 블록에 기록되어 있는 사용자의 권한 기록을 서비스 에이전트에 제공하고, 사용자의 접근 기록에 대해 공개키 기반의 암호화된 블록 데이터를 생성한다. 암호화된 블록 데이터는 블록

네트워크에 기록된다. 상황 정보(Context)는 사용자의 동적 접근 권한을 부여하기 위한 요소로, 사용자의 접근 요청시 접속 기기, 네트워크 타입, 요청 작업, 네트워크 접속시간 등을 사용할 수 있다. 접근 정책(Policy)은 관리자에 의해 생성 및 관리되며 사용자의 ID 에 할당된 기본 역할이 부여되어 있다. 사용자가 정보를 요청하면, 서비스 에트전트에 의해 사용자의 상황정보가 확인되고, 상황 정보는 상황인식 정책의 제약 규칙에 따른다.

Define of user's context constraint :
- *Access Device = Switch(case 1(use PC), case 2(use Mobile device), etc)*
- *Network Type = Switch (case 1(in LAN), case 2(in WAN), case 3(in WiFi), case 4(in LTE), etc)*
- *Operation = Switch (case 1(use READ), case 2(use WRITE), case 3(use UPDATE), etc)*

Assign of user's Dynamic Role :
- *User ID$_{Role}$: Case User Base Role,*

if Access Device = use PC and Network Type = in LAN then Assign Base Role
else if Network Type = in WAN and Operation = WRITE then Assign Lower Role
else Access Device = use Mobile device then Assign Lower Role

IV. 블록체인 환경의 스마트 컨트랙트를 활용한 사용자 동적 접근 제어 서비스

본 장은 제안한 사용자 동적 접근 제어 모델을 블록체인 환경에서 적용하였을 때의 서비스 과정을 구체적으로 기술하였다.

4.1 사용자 접근 권한 등록 및 수정

그림 7 은 관리자에 의해 사용자의 접근 권한을 변경하는 과정을 표현한 것이다. 관리자가 사용자의 접근 권한 변경을 요청하기 위해서는 우선 관리자 인증 과정이 수행되어야 한다. 작업 요청시 관리자는 관리자를 식별할 수 있는 관리자 ID 와 인증키 $E(Key_{Admin})$를 서비스 에이전트에 전송한다. 인증키는 암호화하여 $Req(Admin\ ID, E(Key_{Admin}))$ 요청 메시지를 전송한다. 스마트 컨트랙트는 관리자 인증과정을 수행하고, 인증이 완료되면 접근 권한 목록을 전송한다. 또한 사용자의 접근 권한 변경 트랜잭션이 발생하는 경우 관리자 접근 기록과 사용자 접근 권한 변경 기록을 블록 데이터로 생성하여 블록체인 네트워크에 기록하고, 생성된 블록 결과를 응답한다.

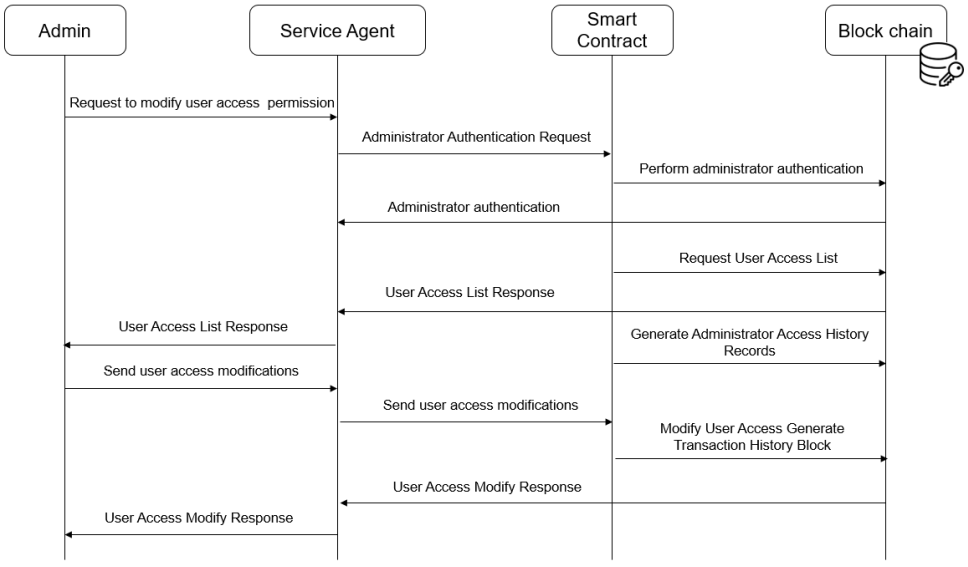

Figure 7. Process for modifying user access policies for administrators
그림 7. 관리자의 사용자 액세스 정책 수정 프로세스

4.2 사용자 데이터 접근 및 수정

사용자가 데이터 접근을 요청하기 위해서는 사용자 인증 과정이 우선적으로 수행되어야 한다. 데이터 접근 요청시 사용자는 사용자 ID 와 인증키 $E(Key_{user})$를 서비스 에이전트에 전송한다. $Req(User\ ID, E(Key_{user}))$ 요청 메시지를 전송하면, 서비스 에이전트는 사용자의 상황 정보를 추가하여 사용자 인증과 권한을 확인하기 위해 $Req(User\ ID, E(Key_{user}), Context)$ 요청 메시지를 블록체인 네트워크에 전송한다. 블록체인 네트워크에서는 사용자 인증 요청메시지를 받으면 스마트 컨트랙트가 사용자 인증 과정을 수행하고, 사용자 권한을 확인한다.

블록체인에 기록된 권한에서 사용자의 기본 역할(Base Role)을 확인하고, 상황 인식 제한 요소와 접근 정책 리스트에 따라 동적 역할(Dynamic Role)을 할당한다. 사용자의 동적 역할은 사용자 가상 ID(VID)로 매칭되고 유효시간(Valid Time)을 $Res(User\ VID, Valid\ Time)$ 메시지로 전송한다. 이후 사용자가 요청하는 데이터의 접근 수준이 접근 권한과 비교하여 트랜잭션의 허가 또는 거부를 나타내는 승인 정보를 접근 정책으로 저장한다. 그림 8 은 사용자가 데이터에 접근하기 위해 요청하는 과정을 표현한 것이다.

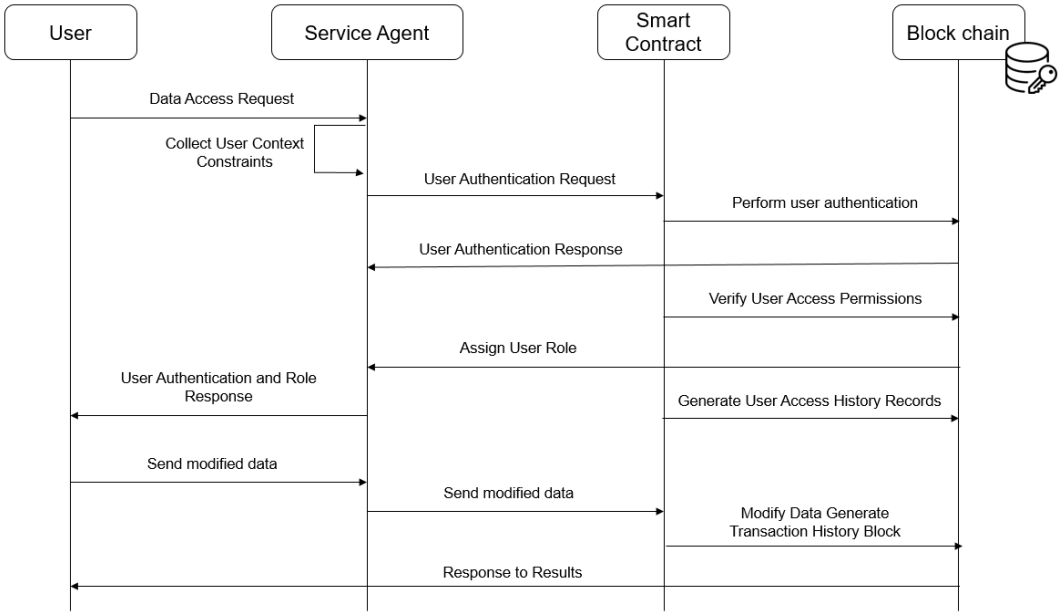

Figure 8. The process by which users access data
그림 8. 사용자 데이터 액세스 프로세스

본 메커니즘에서의 보안성과 효율성을 분석하면 다음과 같다. 사용자 동적 접근 제어는 블록체인 네트워크에서 데이터의 저장과 접근 기록 및 변경 내용을 암호화된 블록으로 생성하여 기록함으로써 데이터의 무결성과 신뢰성은 보장된다. 또한 블록체인의 특성상 모든 네트워크 참여자에게 데이터가 공유되므로 기밀성이 보장되지 않는 단점을 보완하기 위해 사용자 인증시 사용자 ID 와 인증키를 사용함으로써 허가 되지 않은 사용자의 데이터 접근을 방지하고, 허가된 사용자 일지라도 데이터 접근 시 상황정보를 활용하여 기본 할당된 접근 권한(Base Role)을 유지할지 또는 접근 제어 정책에 따라 축소된 접근 권한(Dynamin Role)을 새로이 할당할지를 결정함으로써 데이터의 보안성을 높였다.

사용자에게 축소된 새로운 권한을 할당하는 경우 사용자의 ID 에 가상 ID(VID)를 매칭함으로써 변경된 접근 권한을 사용하도록 하고, VID 할당시 유효시간(Valid Time)을 부여하여 일정 시간 이후 해당 권한은 자동 폐기되도록 하여 시스템 내에서 사용자 권한 관리의 효율성을 높일 수 있다. 또한 블록체인 네트워크에 스마트 컨트랙트를 활용함으로써

사용자의 인증과 접근 권한 부여를 조건을 확인하여 자동 실행되도록 함으로써 시스템의 효율성과 신뢰성을 확보할 수 있다.

V. 결론

최근 블록체인 기술을 다양한 분야에 활용하기 위한 연구가 활발히 진행되고 있다. 특히 블록체인 기반의 스마트 컨트랙트는 분산 원장 환경에서 데이터를 기록하여 데이터의 무결성과 유효성이 검증되며, 미리 작성되어 등록된 코드에 의하여 설정된 조건이 충족되면 자동으로 이행되는 특징을 가지고 있어서 신뢰성을 요구하는 다양한 자동화 시스템에 적용되고 있다.

정보통신기술의 발달로 방대한 데이터 생성과 데이터 활용이 늘어남에 따라 데이터에 대한 정보 보호에 대한 관심도 증가하고 있다. 기업의 잘못된 데이터 접근 권한 관리나 접근 권한의 조작 등에 의하여 데이터가 허가 되지 않은 사용자에게 유출될 위험성이 존재한다. 특히 유출된 대상이 악의적인 의도를 가진 내부자인 경우에는 데이터가 외부로 유출될 가능성이 더욱 높다. 데이터 보안을 위해서는 데이터에 대한 철저한 접근 관리와 외부의 불적적인 접근자에 의해 접근 권한이 위변조되지 않았음을 증명할 수 있어야 한다.

본 논문에서는 블록체인 기반의 스마트 컨트랙트를 활용한 동적 접근 제어 메커니즘을 제안하였다. 제안한 메커니즘은 블록체인 네트워크 환경에서 사용자의 데이터 접근 요청시 상황 정보를 고려하여 접근 권한을 동적으로 부여함으로써 데이터의 보안성과 신뢰성을 보장하고, 스마트 컨트랙를 활용하여 사용자 인증 및 동적인 사용자 접근 권한을 부여함으로써 시스템의 효율성도 확보하였다. 또한 사용자의 동적 접근 권한 부여시 사용자 가상 ID(VID)를 통해 변경된 접근 권한을 사용하고, 유효시간(Valid Time)을 부여하여 일정 시간 이후 해당 권한은 자동 폐기되도록 하여 시스템 내에서 사용자 권한 관리의 효율성을 높일 수 있다.

더불어 제안된 메커니즘은 사용자 접근 제어에 필요한 상황 정보를 통해 역할을 부여하므로 능동적인 권한 부여가 가능하다. 데이터의 동적 접근 제어는 사용자 그룹이 동일한 역할로 데이터에 접근하는 것이 아니라 사용자가 해당 역할에 배정되어 접근 권한을 가지고 있더라도 현재 상황이 보안 정책을 만족하고 있는지 확인하여 가지고 있는 권한의 유효성을 판단하고, 접근 권한을 동적으로 부여하게 함으로써 네트워크의 보안성을 높이는 효과를 얻을 수 있다.

VI. 참고문헌

[1] Gartner Identifies the Top 10 Strategic Technology Trends for 2018. https://www.gartner.com/newsroom/id/3812063

[2] Andres Guadamuz & Chris Marsden, Blockchanins and Bitcoin: Regulatory Responses to Cryptocurrencies, First Monday-Peer Reviewed Journal on The Internet, 20(12), 2015. https://firstmonday.org/article/view/6198/5163

[3] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the internet of things,” IEEE Access, vol. 4, pp. 2292-2303, 2016.

[4] G. Sagirlar, B. Carminati, E. Ferrari, J. D. Sheehan, and E. Ragnoli, “Hybrid-iot: Hybrid blockchain architecture for internet of things-pow subblockchains,” arXiv preprint arXiv:1804.03903, 2018.

[5] Y. J. Huh, “A IoT control system that provides Authentication, Non-repudiation and Integrity Using a blockchain,” Graduate School of Electronic Engineering, Master dissertation. Sogang University, Seoul, 2017.

[6] S. H. Yang, “Proposal for Smart Contract method for domestic medical system based on the colored coin,” Department of Convergence Service Security Engineering, Master dissertation. Soonchunhyang University, Asan, 2017.

[7] Financial Services Commission, Study on the introduction of the block chain technology financial sector. Corda platform. https://www.r3.com, 2016.

[8] YOSEMITE Public Blockchain, Technical White Paper (KOR version), 2018. 02
[9] Z. Zheng, S. Xie, H. N. Dai, and H. Wang, “Blockchain challenges and opportunities: A survey,” Work Pap, 2016.
[10] Ik-Soon Kim, "Survey on Smart Contract Programming Languages," [ETRI] Electronics and Telecommunications Trends, 35(5), pp. 134-138, 2020.
[11] Seung-Hyun Kim, Soohyung Kim. "Analysis of Blockchain-based Access Control Technology," [ETRI] Electronics and Telecommunications Trends, pp. 117-128, 2019.
[12] Szabo, Nick, The idea of smart contracts. Nick Szabo's Papers and Concise Tutorials, 1997.
[13] Young-Hun Kim. (2019). "A Study on Smart Contract for Personal Information Protection," Journal of Digital Convergence, Vol. 17. No. 3, pp. 215-220, 2019.
[14] Sayeed, Sarwar & Marco-Gisbert, Hector & Caira, Tom. Smart Contract: Attacks and Protections. IEEE Access. pp. 1-1, 2020.
[15] http://wiki.hash.kr/index.php/%EC%8A%A4%EB%A7%88%ED%8A%B8_%EA%B3%84%EC%95%BD
[16] Sang-Soo Yeo, Si-Jung Kim, Do-Eun Cho, "Dynamic Access Control Model for Security Client Services in Smart Grid," International Journal of Distributed Sensor Networks, June 2014.
[17] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, “Computer role-based access control models,” Computer, vol. 29, no. 2, pp. 38–47, 1996.
[18] G. Neumann and M. Strembeck, “An approach to engineer and enforce context constraints in an RBAC environment,” in Proceedings of 8th ACM Symposium on Access Control Models and Technologies (SACMAT ’03), pp. 65–79, Como, Italy, June, 2003.

저자 소개

조도은(Do-Eun Cho)

2001 년 8 월 세명대학교 대학원 전자계산교육학과 석사
2007 년 2 월 충북대학교 대학원 컴퓨터공학과 박사
2008 년 3 월~현재 목원대학교 SW 교양학부 조교수

관심분야 : 정보보안, 센서네트워크, 공학교육