논문 2024-4-27 http://dx.doi.org/10.29056/jsav.2024.12.27

Hyperledger Fabric 환경에서 X.509 인증서의 격자 기반 접근제어 적용에 관한 연구

노창현*, 신동명*†

A Study on the Application of LBAC using X.509 Certificates in Hyperledger Fabric Environments

ChangHyun Roh*, Dong-Myung Shin*†

요 약

블록체인 기술의 발전과 함께 엔터프라이즈 환경에서의 보안 및 접근제어의 중요성이 증대되고 있다. Hyperledger Fabric은 허가형 블록체인 플랫폼으로 널리 사용되고 있지만, 접근제어 측면에서 여러 한계점을 보인다. 현재 Fabric의 역할 기반 접근제어 (RBAC)는 기업 환경의 요구사항을 충족시키기에 유연하지 않으며, 정책 관리의 복잡성, 크로스-채널 접근의 어려움 등의 문제점이 존재한다. 또한, 접근제어 결정에 대한 기능이 제한적이며, 기존 기업 신원 관리 시스템과의 통합에도 어려움이 있다.

본 연구는 이러한 문제점들을 해결하기 위해 X.509 인증서를 활용한 격자 기반 접근제어 (Lattice-Based Access Control, LBAC) 모델의 Hyperledger Fabric 적용 가능성과 효과를 탐구한다. 연구 방법으로는 X.509 인증서의 확장 필드를 활용하여 LBAC 모델의 보안 레벨과 카테고리 정보를 인코딩하는 방식을 제안한다. 이를 통해 Hyperledger Fabric의 기존 인증 체계와 통합하면서도 세밀하고 유연한 접근제어 제공이 가능할 것이다. 이를 통해 Hyperledger Fabric의 보안성과 유연성을 크게 향상할 수 있을 것으로 기대한다.

Abstract

The advancement of blockchain technology has increased the importance of security and access control in enterprise environments. Hyperledger Fabric, a widely used permissioned blockchain platform, shows limitations in access control. Its current Role-Based Access Control (RBAC) lacks flexibility for enterprise needs, presenting issues in policy management complexity and cross-channel access difficulties. Moreover, access control decision functionality is limited, and integration with existing enterprise identity systems is challenging. This study explores the application of Lattice-Based Access Control (LBAC) using X.509 certificates in Hyperledger Fabric to address these issues. The research proposes encoding LBAC security levels and category information in X.509 certificate extension fields. This approach enables fine-grained, flexible access control while integrating with Fabric's existing authentication framework. This research aims to significantly enhance Hyperledger Fabric's security and flexibility.

한글키워드 : 블록체인, 하이퍼레저 패브릭, 격자 기반 접근제어, X.509 인증서

keywords : Blockchain, Hyperledger Fabric, Lattice-based Access Control, X.509 Certificate

* 엘에스웨어(주) 소프트웨어연구소 연구개발본부
† 교신저자: 신동명(email: roland@lsware.com)

접수일자: 2024.11.20. 심사완료: 2024.12.13.
게재확정: 2024.12.20.

1. 서 론

블록체인 기술의 발전과 함께 엔터프라이즈 환경에서의 보안 및 접근제어의 중요성이 날로 증대되고 있다. 특히, 허가형 블록체인 플랫폼인 Hyperledger Fabric은 그 확장성과 모듈화된 구조로 인해 많은 기업에 의해 채택되고 있다. 그러나 Fabric의 현재 접근제어 메커니즘은 복잡한 기업 환경의 요구사항을 충족시키는 데 여러 한계점을 보인다.

현재 Hyperledger Fabric에서 주로 사용되는 역할 기반 접근제어(RBAC) 모델은 동적이고 세분화된 접근제어 요구사항을 가진 기업 환경에서 충분한 유연성을 제공하지 못하고 있다[1]. 이는 빠르게 변화하는 비즈니스 환경에서 실시간으로 접근 권한을 조정해야 하는 필요성을 충족시키지 못하는 주요 원인이 되고 있다. 또한, 채널 구성을 통한 정책 관리의 복잡성은 대규모 기업 네트워크에서 일관된 보안 정책을 유지하는 데 어려움을 초래한다.

더불어, 동적 속성 기반 접근제어의 부재로 인해 사용자의 현재 상태나 컨텍스트를 고려한 세밀한 접근제어 결정이 어렵다. 이는 특히 다양한 부서와 역할이 복잡하게 얽혀 있는 대기업 환경에서 큰 제약으로 작용한다. 접근제어 결정에 대한 상세한 감사와 모니터링 기능이 제한적인 점 또한 규제 준수와 보안 사고 대응 측면에서 중요한 문제로 대두되고 있다.

기존 기업 신원 관리 시스템과의 원활한 통합에도 어려움이 있어, 많은 기업이 블록체인 기술 도입 시 기존 시스템과의 호환성 문제로 인한 추가적인 비용과 복잡성을 겪고 있다. 이는 블록체인 기술의 기업 내 광범위한 적용을 저해하는 요인 중 하나로 작용하고 있다.

이러한 다양한 문제점들을 해결하기 위해, 본 연구에서는 X.509 인증서를 활용한 격자 기반 접근제어(LBAC) 모델의 Hyperledger Fabric 적용 가능성과 효과를 탐구한다. LBAC 모델은 그 수학적 기반으로 인해 복잡한 계층 구조와 다차원적인 접근제어 정책을 효과적으로 표현할 수 있어, 기업의 복잡한 조직 구조와 보안 요구사항을 더욱 정확히 반영할 수 있을 것으로 기대된다[2].

본 연구에서 제안하는 접근 방식은 여러 가지 중요한 이점을 제공할 것으로 예상된다. 먼저, 더욱 세밀하고 유연한 접근제어 정책의 구현이 가능해질 것이다. 이는 복잡한 기업 환경에서 요구되는 다양한 접근제어 시나리오를 효과적으로 지원할 수 있게 해준다. 예를 들어, 프로젝트의 진행 단계나 데이터의 민감도에 따라 동적으로 접근 권한을 조정할 수 있게 되어, 정보 보안과 업무 효율성을 동시에 향상시킬 수 있다.

또한, 동적 속성 기반 접근제어를 지원함으로써 실시간으로 변화하는 사용자의 컨텍스트와 속성을 고려한 접근제어 결정이 가능해질 것이다. 이는 사용자의 위치, 시간, 네트워크 상태 등 다양한 컨텍스트 정보를 기반으로 한 정교한 접근제어를 가능하게 하여, 보안성을 크게 향상시킬 수 있다.

더불어, X.509 인증서의 확장 필드를 활용한 LBAC 정보의 인코딩은 기존 Hyperledger Fabric의 인증 체계와의 원활한 통합을 가능하게 한다[3]. 이는 기존 시스템과의 호환성을 유지하면서도 새로운 접근제어 모델을 도입할 수 있게 해주어, 기업의 기술 도입 부담을 크게 줄일 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 Hyperledger Fabric의 기본 구조, 현재의 접근제어 메커니즘, 그리고 LBAC 모델에 대한 배경지식을 소개한다. 3장에서는 제안하는 X.509 인증서 기반 LBAC 모델의 상세한 설계와 구현 방법을 설명한다. 여기에는 인증서 확장 필드의 구조, LBAC 정책의 인코딩 방식, 그리고 Fabric의 체

인코드를 통한 접근제어 로직의 구현 등이 포함된다. 4장에서는 제안된 모델의 성능 평가와 보안 분석 결과를 제시하고, 기존 접근제어 방식과의 비교를 통해 그 효과성을 검증한다. 마지막으로, 연구 결과의 의의와 한계점, 그리고 향후 연구 방향에 대해 심도 있게 논의한다.

본 연구는 Hyperledger Fabric을 활용한 엔터프라이즈 블록체인 시스템의 보안성과 유연성을 크게 향상할 수 있는 새로운 접근제어 모델을 제시함으로써, 블록체인 기술의 기업 적용을 더욱 촉진할 수 있을 것으로 기대한다. 특히, 금융, 의료, 공급망 관리 등 높은 수준의 보안과 규제 준수가 요구되는 산업 분야에서 본 연구의 결과가 유용하게 활용될 수 있을 것이다. 더 나아가, 본 연구는 블록체인 기술과 전통적인 기업 IT 인프라 사이의 간극을 좁히는 데 기여함으로써, 디지털 전환을 가속화하고 기업의 경쟁력 강화에 기여할 수 있을 것으로 전망된다.

2. Backgrounds

2.1 Hyperledger Fabric

Hyperledger Fabric은 엔터프라이즈급 허가형 분산 원장 기술(DLT) 플랫폼으로, 기업 환경에서 사용할 수 있도록 설계되었다[4]. Linux Foundation에서 주관하는 오픈소스 프로젝트인 Hyperledger의 일부로, 다양한 산업 분야의 블록체인 기술 발전을 위한 협력적 노력의 결과물이다. Fabric의 주요 특징으로는 모듈식 아키텍처, 허가형 네트워크, 채널, 스마트컨트랙트(체인코드), 그리고 유연한 합의 메커니즘 등이 있다[5].

모듈식 아키텍처를 통해 조직은 특정 요구사항에 맞춰 구성 요소를 사용자 정의하고 확장할 수 있다. 허가형 네트워크 특성상 참여자가 알려져 있고 인증된 네트워크에서 운영되며, 채널 기능을 통해 메인 블록체인 네트워크 내에서 격리된 프라이빗 서브네트워크를 지원한다. 스마트컨트랙트인 체인코드는 비즈니스 로직을 정의하고 실행하는 데 사용되며, Fabric은 애플리케이션의 요구에 따라 다양한 합의 방식을 선택할 수 있는 유연성을 제공한다.

Hyperledger Fabric의 핵심 구성 요소에는 피어 노드, 오더러 노드, 인증 기관 등이 포함된다. 피어 노드는 트랜잭션을 관리하고 검증하는 역할을 하며, 오더러 노드는 트랜잭션이 올바른 순서로 추가되도록 보장한다. 인증 기관은 네트워크 참여자의 신원을 관리하고 인증하는 중요한 역할을 담당한다.

Hyperledger Fabric의 신원 관리 시스템에서 X.509 인증서는 핵심적인 역할을 한다[6]. X.509 인증서는 공개키 인프라(PKI)를 기반으로 하며, 국제적으로 널리 인정받는 표준이다. 인증 기관(CA)은 네트워크의 각 참여자에게 고유한 X.509 디지털 인증서를 발급한다. 이 인증서에는 버전, 일련번호, 알고리즘 정보, 인증서의 유효기간 등의 정보가 포함되어 있다. Fabric의 멤버십 서비스 제공자(MSP)는 이러한 X.509 인증서를 사용하여 네트워크 참여자의 신원을 관리하고 인증한다.

X.509 인증서는 Fabric 네트워크 내의 모든 엔티티와 구성원을 인증하는 데 사용된다. 이는 기업 환경에 매우 적합한 방식으로, 조직은 기존의 CA 인프라를 사용하여 사용자, 피어 및 애플리케이션에 대한 새로운 인증서를 발급할 수 있다. 네트워크에서 신뢰할 수 있는 CA(즉, 시스템의 유효한 MSP 조직의 CA)에 의해 발급된 인증서를 소지한 사용자는 네트워크와 상호 작용할 수 있는 권한을 갖게 된다.

Hyperledger Fabric의 인증서에는 현재 주로 역할 기반 접근제어(RBAC)와 속성 기반 접근제어(ABAC)를 사용하고 있다. 그러나 이러한 접근

제어 모델들은 복잡하고 동적인 기업 환경에서 여러 한계점을 드러내고 있다[7]. RBAC의 경우, 사용자에게 고정된 역할을 할당하는 방식으로 인해 빠르게 변화하는 비즈니스 요구사항에 유연하게 대응하기 어렵다. 예를 들어, 프로젝트 기반의 업무 환경에서 사용자의 역할이 자주 변경되는 경우, RBAC만으로는 효과적인 접근제어를 구현하기 어렵다. ABAC는 이러한 RBAC의 한계를 일부 해결할 수 있지만, 정책 관리의 복잡성과 성능 저하 문제가 존재한다. 특히 대규모 기업 네트워크에서 수많은 속성을 실시간으로 평가해야 하는 ABAC의 특성은 시스템 성능에 부담을 줄 수 있다. 또한, 두 모델 모두 다차원적이고 계층적인 접근제어 정책을 효과적으로 표현하는 데 한계가 있어, 복잡한 조직 구조와 데이터 민감도를 정확히 반영하기 어렵다.

이러한 문제점들로 인해 Hyperledger Fabric 환경에서 보다 유연하고 효율적인 접근제어 모델의 필요성이 대두되고 있으며, 이러한 배경에서 격자 기반 접근제어가 Hyperledger Fabric 환경에서의 새로운 대안으로 주목받고 있다[8].

2.2 LBAC(Lattice-based Access Control)

Hyperledger Fabric의 접근제어에서 새로운 대안으로 주목받고 있는 LBAC는 수학적 격자 이론을 기반으로 한 접근제어 모델로, 복잡하고 다차원적인 보안 정책을 효과적으로 표현할 수 있는 능력을 갖추고 있다[9]. 이 모델은 1976년 Denning에 의해 처음 제안되었으며, 이후 여러 연구자에 의해 발전됐다. LBAC 모델에서는 보안 레벨과 카테고리를 격자 구조로 표현하며, 이 격자는 부분 순서 집합(partially ordered set)으로, 각 노드는 특정 보안 수준을 나타낸다[10].

LBAC의 핵심 개념에는 정보의 민감도를 나타내는 계층적 구조인 보안 레벨, 정보의 주제나 부서 등을 나타내는 비 계층적 구조인 카테고리, 그리고 두 보안 수준 사이의 관계를 정의하는 최소 상한(Least Upper Bound, LUB)와 최대 하한(Greatest Lower Bound, GLB) 연산이 포함된다[11]. 이러한 개념들을 통해 LBAC는 복잡한 조직 구조와 다양한 보안 요구사항을 정확하게 모델링 할 수 있다.

격자 기반 접근제어는 부분 순서 집합으로 표현되는 보안 수준으로 표현되며, 주체와 객체 간 상호작용에 따라 접근을 선택적으로 제한하는 메커니즘으로 구성된다[12]. 사용되는 핵심 항목은 객체, 주체, 트랜잭션으로 구성되며 자세한 내용은 아래와 같다.

- 객체(O : Object) : 시스템에서 보호해야 할 정보가 포함된 리소스(문서, 파일, DB, 폴더 등)
- 주체(S : Subject) : 객체에 대한 접근을 요청하는 대상(개발자, 사용자 등)
- 트랜잭션(T : Transaction) : 읽기, 쓰기 및 실행

트랜잭션은 Hyperledger Fabric(블록체인)에 저장된 리소스에 대한 접근제어 정책이며, 블록체인에 저장된 데이터는 권한이 있는 주체만이 읽기, 쓰기 및 실행할 수 있다.

정의 1 : 정책(P)

P는 주체(S)를 작업 집합에 매핑하는 함수로 (1)처럼 표현한다.

$$P_o : S \times P_o W(T) \qquad (1)$$

P_o는 객체(O)에 대한 정책 함수를 의미하며, S는 주체에 대한 집합을 의미한다. 그리고 $P_o W(T)$는 리소스에 접근하는 상위 수준과 작업의 집합을 의미한다.

정의 2 : 정책 권한(P_j)

P_j는 주체 S_j와 객체 O_j 간 제한적 접근에 대한 정책작업 T_j를 지정하는 함수이다. S_j는 T_j에 지정된 O_j에서만 해당 정책작업을 수행할 수 있다. 예를 들어, 블록체인에 저장된 문서 D_1의 $alice$라는 데이터 소유자의 접근 정책 권한을 $P_D = < alice, D_1, r, w, x >$와 같이 설정한다면, $alice$의 문서 D_1에 읽기, 쓰기, 실행이 가능한 권한을 확인할 수 있다.

정의 3 : 리소스의 접근 권한(T)

작업 집합 T 는 읽기, 쓰기, 실행 등 작업에 대한 순서로 $T = \{T_1, T_2, T_3, T_4, \cdots, T_n\}$와 같이 표기하며 리소스(객체) O_j에 대한 접근 권한은 R_j이며 $[i_1, i_2, i_3, i_4, \cdots, i_n]$로 표현할 수 있으며, 특정 작업 T_k에 대한 리소스 O_j의 권한을 할당된 경우 i_n의 값은 '1' 반대인 경우 '0'으로 표기한다. 접근 권한의 총개수는 P_j에 따라 표시된다. 예를 들어 문서 D_1에 대한 작업 집합이 $T = \langle r, w, x \rangle$이고, D_1의 접근 권한 R_1은 $R_1 = [110]$의 경우 읽기 및 쓰기 작업이 허용되지만, 실행은 허용되지 않는 것을 보여준다.

정의 4 : 객체의 격자 접근 권한 L을 접근 수준의 집합이라 하며, 부분순서 $\leq$상의 L에 대해 $L \times L$의 관계가 표시되며 이는, 반사 관계, 추이적 관계, 반대칭 관계이다.

- 반사적 관계 : $a \leq a \; \forall \; a \in L$
- 추이적 관계 :
  if $a \leq b$ and $b \leq c$ $then$ $a \leq c \; \forall \; a, b, c \in L$
- 반대칭 관계 :
  if $a \leq b$ and $b \geq a$ $then$ $a = b \; \forall \; a, b \in L$

정의 4에 따라서 접근 권한 $R_j[i_k]$의 I번째 k 요소에 대한 순서 관계는 O_i로 표현되며, R_p와 R_s를 T_n연산에 대한 O_i의 두 접근 권한이라고 할 경우,

$$R_p \geq O_i \geq R_s \;\; \text{if} f \;\; \text{or} \quad R_p[i_k] \geq R_s[i_k] \;\; \forall \;\; k = 1 \tag{2}$$

식(2)처럼 표현할 수 있다.

정의 5 : 최소 상한 연산($\vee$)

최소 상한은 R_p와 R_s로 표시되며, 객체 O_i와 연관된 작업 T의 i번째 k 요소인 i_k에 대해

$$(R_p, R_s)[i_k] = R_p[i_k] \vee R_s[i_k] \tag{3}$$

식(3)처럼 표현할 수 있다. 즉, 두 개의 접근 권한이 동일한 리소스에 접근하려고 하면 하위 접근 권한은 상위 권한에 양보한다.

예를 들어, 문서 D_i에 주체 S_m과 S_n의 접근성과 연관되어 있을 경우, 정책 권한에 따라

$$\langle S_m, S_n \rangle \leq \{alice, D_i, r, w, x\} \tag{4}$$

식(4)처럼 표현된다. 만약 주체 S_m이 문서 D_i에 대한 쓰기 작업의 낮은 접근 권한을 가지고 있어 S_n의 검증이 필요한 상황일 경우 D_i는 S_m에 의해 접근된 후 S_n에게 권한이 넘어가며 아래와 같이 표기된다.

$$(S_m, S_n)D_i = S_m(D_i) \vee S_n(D_i) \tag{5}$$

정의 6 : 최소 하한 연산($\wedge$)

최소 하한은 객체 O_i의 두 접근 권한에 대한

R_p와 R_s로 표시되며 연관된 작업 T의 i번째 k 요소인 i_k에 대해 (6)과같이 표시된다.

$$(R_p, R_s)[i_k] = R_p[i_k] \wedge R_s[i_k] \qquad (6)$$

격자 구조에서 객체에 대한 모든 가능한 접근 권한은 노드로 표현된다. 이는 특정 접근제어 권한을 유지하기 위한 것으로 최하위 경계(Lower Bound)의 경우에는 접근 권한이 전혀 없는 상태, 즉, 사용자가 해당 리소스에 대해 어떠한 작업도 수행할 수 없다는 것을 말한다. 반대로, 최상위 경계(Upper Bound)의 경우 모든 접근 권한을 가진 상태로 해당 리소스에 대해 모든 가능한 작업을 수행할 수 있음을 의미한다[11].

접근 권한의 관련된 모든 작업(트랜잭션)은 반드시 정책 권한에 반영되어야 하며, 동시에 각 리소스의 데이터베이스도 업데이트가 되어야 한다. 이러한 방식으로 시스템은 각 사용자의 접근 권한을 정확하게 추적하고 관리할 수 있으며, 동시에 보안 정책을 엄격하게 적용할 수 있다[12].

LBAC의 주요 장점으로는 복잡한 조직 구조와 다차원적인 보안 정책을 자연스럽게 표현할 수 있는 유연성, 세분화된 접근제어가 가능하여 최소 권한 원칙을 효과적으로 구현할 수 있는 정밀성, 격자 이론을 바탕으로 한 정형적 검증 가능성, 그리고 새로운 보안 레벨이나 카테고리를 쉽게 추가할 수 있는 확장성을 들 수 있다[13].

이러한 LBAC의 특성은 Hyperledger Fabric 환경에서 요구되는 동적이고 세밀한 접근제어 요구사항을 충족시킬 수 있는 잠재력을 가지고 있다. LBAC를 통해 기업들은 더욱 정교하고 유연한 보안 정책을 구현할 수 있으며, 이는 데이터 보안과 프라이버시 보호를 강화하는 동시에 비즈니스 요구사항을 효과적으로 지원할 수 있게 해준다.

2.3 X.509 Extensions

X.509는 공개키 기반구조(PKI)에서 널리 사용되는 디지털 인증서 표준이다. 이 표준은 SSL/TLS 암호화, 서명, 이메일 보안, VPN 인증, 문서 서명 등 다양한 분야에서 활용되며, 안전한 통신과 전자 서명 검증을 가능하게 한다[2].

X.509 인증서의 기본 구조는 표 1과 같이 버전, 일련번호, 서명 알고리즘, 발급자 정보, 유효기간, 공개키 정보 등을 포함한다. 이러한 필드들은 인증서의 핵심 정보를 제공하며, 인증서의 신뢰성과 유효성을 확인하는 데 사용된다[3].

X.509 인증서의 기본 구조와 확장 필드는 본 연구에서 제안하는 LBAC 모델과 관련하여, X.509 인증서의 접근제어 정책이나 보안 레벨 정보를 인코딩하는 데 활용될 수 있어, Hyper-ledger Fabric 환경에서 더욱 세밀하고 유연한 접근제어 메커니즘을 구현하는 데 중요한 역할을 할 수 있다.

표 1. X.509 구성(v3)
Table 1 . X.509 Configuration(v3)

구분	설명
Version	인증서의 버전 명시(v1(0)~v3(2))
Serial Number	CA(인증 기관)가 인증서에 할당한 고유의 양의 정수
Signature Algorithm Identifier	CA가 인증서에 서명하는 데 사용하는 알고리즘 정보
Issuer Name	인증서를 만들고 서명한 CA 고유 이름
Validity Period	인증서의 유효 기간
Subject Name	인증서의 공개 키와 연결된 엔티티
Public Key Information	공개키 및 연결된 알고리즘 정보
Issuer Unique ID (v2)	여러 엔티티에서 재사용될 때 사용할 수 있는 CA의 고유한 값
Subject Unique ID (v2)	여러 엔티티에서 재사용될 때 사용할 수 있는 인증서 소유자의 고유한 값
Extensions (v3)	확장은 키 사용, 인증서 정책 및 제약 조건, 대체 이름, 양식 등에 대한 향상된 정보 등 제공

3. X.509의 격자 기반 접근제어 적용 방안

3.1 격자 기반 접근제어 구현 방안

X.509 인증서의 확장 필드를 활용하여 LBAC에 필요한 속성을 적용하는 방법으로는 Hyperledger Fabric의 인증 기관으로 동작하는 fabric-CA를 사용하여 인증서 발급 시, -id.attrs 명령어로 사용자 속성을 입력할 수 있다.

예를 들어, 특정 수사기관에서 접근 정책을 설정할 때, "접근 레벨 3", "경감 계급", "소속 대한민국"과 같은 조건을 설정할 경우 표 2에서의 'lbac.level=3,lbac.class=seniorInspector,lbac.nation=ROK'와 같이 표현할 수 있다.

이러한 속성들은 X.509 인증서의 확장 필드에 문자열 형식으로 저장되며, Hyperledger Fabric의 스마트컨트랙트인 Chaincode에서 데이터 접근 시 속성을 추출하고 검증할 수 있다.

표 2. 인증서 정보 등록 시 명령어 예시
Table 2. Example of register certificate information

fabic-ca-client 명령어 예시
fabric-ca-client register --id.name investigator ... -id.attrs **'lbac.level=3,lbac.class=seniorInspector, lbac.nation=ROK:ecert'** ...

Hyperledger Fabric의 fabric-contract api에서는 인증서의 인코딩된 속성값을 추출하는 함수인 AssertAttributeValue()를 제공한다. 이를 통해 인증서에 적용된 속성값들을 추출하여 확인하는 개발이 가능하다.

표 3. X.509 인증서 속성 추출 코드 예시
Table 3. Example of extract certificate attributes

Golang 기반 인증서 속성 추출 코드 예시
err := ctx.GetClientIdentity().AssertAttributeValue ("lbac.level", "3") if err != nil {return fmt.Errorf("접근 불가")}

3.2 Hyperledger Fabric LBAC 적용

본 절에서는 Hyperledger Fabric의 Samples에서 제공하는 코드 중 token-erc-721을 기반으로 적용하고자 한다.

3.2.1 블록체인 데이터 접근 레벨 설정

본 절에서는 Hyperledger Fabric에서의 격자 기반 접근 메커니즘을 제공하여 블록체인에 저장된 데이터와 주체 간의 보안성을 확립한다.

erc-721의 데이터는 소유자의 지갑 주소(Fabric에서는 인증서에 저장된 사용자 ID), 해당 Asset에 대한 메타데이터 정보(작품의 이름, 설명, 연계 링크 등)로 구성된다. 블록체인 전체로 보자면 NFT의 거래 금액, 변경 이력, NFT 총발급 수 등을 볼 수 있다. 이러한 내용으로 보안 레벨을 구성하면 아래 내용과 그림 1과 같다.

- 일반 공개(Public) : NFT의 기본적인 메타데이터인 작품 이름, 설명, 썸네일 링크 등
- 대외비(Confidential) : NFT 정보 중 제한하여야 하는 항목인 소유자 ID, 제작자 정보 등
- 기밀(Secret) : NFT의 중요 정보인 거래 금액, 소유자 변경 이력 등
- 최상위 기밀(Top Secret) : 가장 높은 보안 수준으로 블록체인 전체로써 NFT 총 거래 금액, NFT 총발급 개수 등의 통계 정보

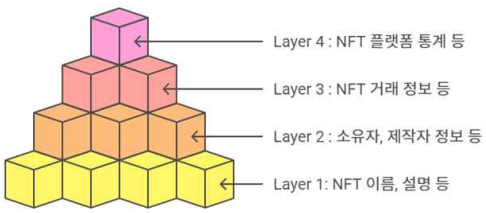

그림 1. NFT 대상 보안 계층 구성
Fig 1. Configuring the NFT Target Security Layer

표 4. 데이터의 민감도 수준 표기법
Table 4. Notations - Sensitivity levels of data

Symbol	Description
S	Subject
S_i	Set of Subject
R	Object(Resources)
R_i	Set of Object(Resources)
Ro	Roles
P_A	Permission Access
Ro_h	Level of roles
P	Permissions
S_A	Subject Access
Se	Sessions
i, j	1 to n entities
r	Read Transaction
α	Mapping

3.2.2 블록체인 데이터의 민감도 레벨 설정

데이터 민감도 레벨(수준)을 처리하는 이유는 주체와 객체 간의 접근제어를 정의하기 위해서이다. 이를 위해 표 4와 같은 표기법을 이용한다.

민감도에는 다음과 같은 요소로 구성된다.

- S, O, Ro, P, Se : 주체, 객체, 역할, 권한 및 세션의 집합
- $P_A \subseteq P \times Ro$: 다대다 권한이 할당됨
- $S_A \subseteq S \times Ro$: 다대다 주체가 할당됨
- $Ro_h \subseteq Ro \times Ro$: 부분적으로 정렬됨
- 주체(S) : $Se \rightarrow S$는 Se_i를 각 주체 S_i에 매핑하는 함수임
- 권한(Ro) : $Se \rightarrow 2^{Ro}$는 각 주체 S_i에 매핑되는 함수임
  $(S_i) \subseteq r / \ni S_i(r) \geq S_j(r) [(S_i, r) \in S_A]$

제약 조건 C_i의 집합은 그림 4와 같이 계층에 정의된 제약 조건의 민감도 수준에 따라 LBAC 모델의 구성 요소를 결정하여 접근 권한을 부여할지를 결정한다.

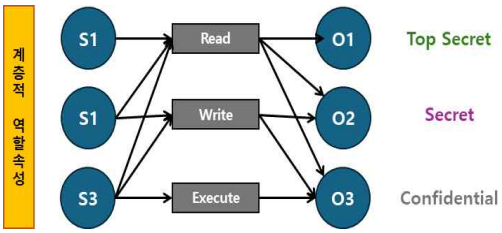

그림 2. 주체와 객체 간 민감도 수준 연결
Fig 2. Sensitivity levels between subject and objects

3.2.3 주체 대 객체의 역할 연결 및 설정

격자 기반의 다중 레벨 보안을 수립하기 위해 NFT 시스템의 주체와 객체 간 접근제어를 식별해야 한다. 주체는 사용자와 관리자로 구성되며, 관리자의 상세 구분으로는 NFT 거래를 검토하는 승인자(Approver), 전체적인 NFT 시장을 관리하는 관리자(Supervisor)로 구성되며, 객체(리소스)의 레벨은 1~4로 구성된다. 이에 해당하는 주체와 객체의 연결은 그림 3과 같다.

이는, 사용자의 보안 레벨을 나타내며 접근할 수 있는 객체를 결정하게 된다.

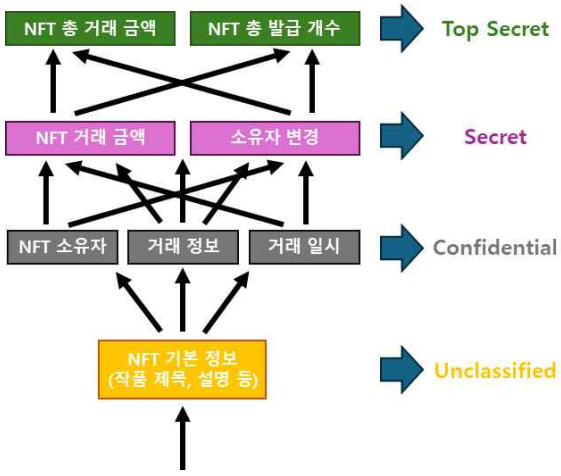

그림 3. 하세 도형을 통한 민감도 분석
Fig 3. Hasse diagram for sensitivity analysis

표 5. Hyperledger Fabric NFT에서의 격자 매트릭스
Table 5. Lattice Matrix in Hyperledger Fabric NFT

Subject \ Object	NFT Info	Transfer Info	Statistical Info
User	r, w, x		
Approver	r, w, x	w, x	r
Supervisor	r, w, x	r, w, x	r, x

그리고 다양한 객체와 주체와의 연계 관계는 다음과 같다.

- R = Set of Object
  = {NFT, Transfer, Statistical}
- S = Set of Subject
  = {User, Approver, Supervisor}
- α - Mapping NFT α {User, Approver, Supervisor} → LV1
  Transferα{Approver, Supervisor} → LV2
  Statistical{Supervisor} → LV3

3.2.4 LBAC 접근 방식 모델링

본 절에서는 Hyperledger Fabric 환경에서 스마트컨트랙트처럼 동작하는 Chaincode를 표 5의 표기법을 사용하여 알고리즘으로 표현한다.

- Procedure 1 : 블록체인 네트워크에서 사용자 자격 증명 검증을 보여준다. 이 절차는 사용자가 정당한 인증서인지, 블록체인 가입자인지 등을 확인할 수 있다.
- Procedure 2 : 블록체인 네트워크에 저장된 데이터의 격자 기반 접근제어 수준을 보여준다. 이는, 권한이 확인될 경우 객체에 접근을 허용하며 객체와 주체는 상위($\vee$)와 하위($\wedge$) 연산과 매핑되며, 표 5의 접근제어 격자를 사용하여 정책으로 사용한다.
- Procedure 3 : 데이터에 접근하기 위한 보안 수준을 사용하여 객체와 주체를 매핑하는 것을 보여준다. 결론적으로 Chaincode에서 수준을 확인하고 데이터에 접근시키고 해당 트랜잭션 작업을 수행한다.

표 6. 데이터의 민감도 수준 표기법
Table 6. Notations - Sensitivity levels of data

Symbol	Description
S_i	Set of subjects
S	Subjects
R_i	Set of object(resources)
R	Object(resources)
S_A	Subject access
i, j	1 to n entities
α	Mapping
T	Transactions
L	Lattice
D	Document
t	Operations(read, write, execute)
d_i	data
r	Read operations
w	Write operations
x	Execute operations
pk	Public key
sk	Private key
cc	Chaincode
id	Identification of User
$Cert$	Certificate
ac	Access control

표 7. LBAC 접근 방식 의사 코드
Table 7. Pseudo code for LBAC

Algorithm 1 : Data accessing using LBAC in Hyperledger Fabric chain-code

Input : $Cert$
Output : Accessing in the blockchain data

Procedure 1: Certificate verification

Input : $Cert$

Output : sk, Authenticated user identity

if $S_i \in Cert$ and $S_i \equiv Cert_{S_i}$

OwnerAccess(S_i, sk)

end if then

End Procedure 1

Procedure 2: Multi-level security using LBAC

Input : (S_i, R_i, sk)

Output : S_i to R_i mapping for different controls based on security level

$S_i \supset$ User(U_i), Approver(Ap_i), Supervisor(Sv_i)

where S_i i=1 to n entites

$R_i \supset \{d_1$:NFT, d_2:Transfer, d_3:Statistical Info$\}$

Let Lattice $L = \{L_i, \wedge, \vee\}$ defined with the level of security as L_i where I =1 to 3

if $S_i == sk$ **then**

Allow(S_i, ac_i) goto Access

else

Reject(S_i)

end if

$L_i = \{R_i \alpha S_i\}$ where i=1 to n

where $\alpha \Rightarrow$mapping

if L_i == allow **then**

for each **do** S_i

for each **do** R_i

if then $S_i \wedge S_j$

end if

if then $S_i \vee S_j$

$R_j \in S_j$

else

$S_i \subseteq ac_i$

end if

end for

for each L_i, i=1 to 3 **do**

for each $S_i \in S$ **do**

such that $S_1 \wedge S_2 \wedge \cdots \wedge S_n$

end for

for each $R_i \in R$

such that $R_1 \wedge R_2 \wedge \cdots \wedge R_n$

end for

end for

for each $R_i \in R$ **do**

such that $R_1 \wedge R_2 \wedge \cdots \wedge R_n$

end for

end for

if $S_i \subseteq ac_i$

$R_j \alpha S_j$ based on the $\vee$ and $\wedge$ *operations*

else

$\{(R_1 \alpha S_1) \in L_1\} \cup \{(R_2 \alpha S_2) \in L_2\} \cup \cdots \cup \{(R_j \alpha S_j) \in L_j\}$

end if

end if then

End Procedure 2

Procedure 3: Transaction executing

Input : S_i, R_i, L_i

Output : Accessing in the blockchain data

Let $D_i \in d_i$ where $D_i \rightarrow$ Document of R_i

if $S_i \subseteq ac_i$ Exists

for each $cc_i \in (R_i \alpha S_i)$ **do**,

$T = \{T_i + (D_i) \in cc_i\}$;

end for

for each owner i **do**

goto remix id

Deploy(T) $\rightarrow S_A$ //accessing the data

end for

end if then

End Procedure 3

4. 적용 방안 분석

4.1 분석 보안 도메인

블록체인 환경에서의 접근제어 체계에 LBAC 적용에 대한 평가를 위해 보안 도메인을 적용하며, 이는 인증, 투명성, 접근제어, 무결성, 기밀성, 다중 계층 보안의 6가지로 구성된다.

- 개인 정보 보호: 개인의 민감한 정보를 무단 접근, 사용, 공개로부터 보호하는 것
- 인증: 시스템에 접근하는 사용자나 엔티티의 신원을 확인하는 프로세스로 무단 접근을 방지하고 데이터의 기밀성과 무결성을 보장하는 데 중요함
- 투명성: 조직이 데이터를 어떻게 수집, 사용, 공유하는지에 대해 명확하고 이해하기 쉬운 정보를 제공하는 것으로 신뢰를 구축하고 규정 준수를 보장함
- 액세스 제어: 권한이 있는 사용자만 특정 데이터나 리소스에 접근할 수 있도록 하는 메커니즘임
- 무결성: 데이터가 정확하고 완전하며 변조되지 않았음을 보장하는 것으로 데이터 신뢰성을 유지하고 부적절한 변경을 방지함
- 다중 계층 보안: 다양한 민감도 수준의 데이터를 처리하여 계층적 데이터 보호를 함

4.2 보안 도메인별 제공 사항

본 논문은 격자 기반 접근제어와 Hyperledger Fabric 기반 Chain-code를 통합하여 블록체인에 저장된 데이터에 다단계 보안을 구현하는 방법을 제안하고 있다. 이 접근 방식은 각 보안 도메인에 대해 다음과 같은 사항들을 제공한다.

- 개인 정보 보호: 표 5의 접근 정책을 사용하여 접근을 제한하고 있으며, 지정된 사용자만이 데이터를 확인할 수 있음
- 인증: X.509에 인코딩된 사용자 ID, 속성 등 정보가 Chain-code 실행 시 확인됨
  (Procedure 1의 첫 시작의 분기문인
  if $S_i \in Cert$ and $S_i \equiv Cert_{S_i}$은 사용자의 인증서 내 정보 안에 Subject 가 포함되는지를 확인하는 절차임)
- 투명성: 블록체인에 저장된 데이터는 변조할 수 없으며 투명한 로그를 제공함
- 액세스 제어: 제안 방식은 개인이 자신의 키를 사용하여 블록체인 내 저장된 데이터의 접근을 제어할 수 있음
  (Procedure 2의 첫 분기문인
  if $S_i == sk$ **then**
  Allow(S_i, ac_i) goto Access
  위 함수는 개인키가 i번째 Subject인 경우 접근을 허락하는 분기문으로 조건 만족 시 Access 허가를 내줌)
- 무결성: 블록체인에 저장되는 데이터는 체인 구조로 앞 데이터와 연계되어 저장되기에 무결성을 보장함
- 다중 레벨 보안: 제안된 모델은 다양한 보안 계층을 통합하였고, 격자 기반의 주체 및 행위를 연계하여 다중으로 보호함
  (Procedure 2에서 goto Access가 끝난 후
  $L_i = \{R_i \, \alpha \, S_i\}$ where i=1 to n
  where $\alpha \Rightarrow$mapping
  부터
  $\{(R_1 \, \alpha \, S_1) \in L_1\} \cup \{(R_2 \, \alpha \, S_2) \in L_2\} \cup \cdots \cup \{(R_j \, \alpha \, S_j) \in L_j\}$
  까지의 실행 부분에서는 주체의 속성(역할)을 기반으로 사용자의 격자 속성에 따른 행위를 할 수 있는 권한을 넘겨주며, 이를 통해 Procedure 3에서는 트랜잭션 생성(행위)을 수행하여 결과를 반환함)

5. 결론

본 연구는 Hyperledger Fabric 환경에서 X.509 인증서를 활용한 격자 기반 접근제어 모델의 적용 가능성과 효과를 탐구하였다. 연구 결과, LBAC 모델은 Hyperledger Fabric의 기존 접근제어 메커니즘의 한계를 극복하고 더욱 세밀하고 유연한 접근제어를 가능하게 했다.

LBAC 모델은 복잡한 조직과 다차원 보안 정책을 자연스럽게 표현할 수 있는 유연성을 제공하며, 최소 권한 원칙을 효과적으로 구현할 수 있는 정밀성을 갖춘다. 또한, 격자 이론을 바탕으로 한 정량적 검증 가능성과 보안 레벨이나 카테고리를 추가할 수 있는 확장성도 제공한다.

X.509 인증서의 확장 필드를 활용하여 LBAC의 보안 레벨과 카테고리 정보를 인코딩하는 방식은 Hyperledger Fabric의 기존 인증 체계와의 원활한 통합을 가능케 한다. 이는 Fabric의 MSP(Membership Service Provider)와 CA(Certi-ficate Authority)를 활용하여 LBAC 정책을 효과적으로 구현하고 관리할 수 있음을 의미한다.

본 연구의 접근 방식은 Hyperledger Fabric 환경에서 요구되는 동적이고 세밀한 접근제어 요구사항을 충족시킬 수 있는 잠재력을 보여주었다. LBAC를 통해 기업들은 더욱 정교하고 유연한 보안 정책을 구현할 수 있으며, 이는 데이터 보안과 프라이버시 보호를 강화할 수 있다.

향후 연구에서는 제안된 모델의 실제 구현과 성능 평가가 필요하며, 다양한 산업 분야에서의 적용 가능성을 탐구해야 할 것이다.

결론적으로, X.509 인증서를 활용한 LBAC 모델은 Hyperledger Fabric 환경에서 더욱 강력하고 유연한 접근제어 메커니즘을 제공할 수 있는 유망한 접근 방식이며, 이는 블록체인 기술의 실적용을 더욱 촉진하고, 보안과 프라이버시 보호의 강화에 기여할 수 있을 것으로 기대된다.

본 연구는 문화체육관광부 및 한국콘텐츠진흥원의 2024년도 문화기술 연구개발 사업으로 수행되었음(과제명 : 한류콘텐츠 보호를 위한 국제공조수사 협력 체계 기술 개발, 과제번호 : RS-2024-00439553, 기여율 : 100%)

참 고 문 헌

[1] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Yellick, J., “Hyperledger fabric: a distributed operating system for permissioned blockchains”, Proceedings of the thirteenth EuroSys conference, pp. 1-15, 2018. DOI: https://doi.org/10.1145/3190508.3190538

[2] Ferraiolo, D. F., Kuhn, D. R., & Sandhu, R., “RBAC standard rationale: comments on ″a critique of the ANSI standard on role-based access control″”, IEEE Security & Privacy, Vol. 5, No. 6, pp. 51-53, 2007. DOI: https://doi.org/10.1109/MSP.2007.173

[3] Maesa, D. D. F., Mori, P., & Ricci, L., “Blockchain based access control”, IFIP international conference on distributed applications and interoperable systems, pp. 206-220, 2017. DOI: https://doi.org/10.1007/978-3-319-59665-5_15

[4] Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T., “FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data”, Computational and Structural Biotechnology Journal, Vol. 16, pp. 267-278, 2018. DOI: https://doi.org/10.1016/j.csbj.2018.07.004

[5] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A., “MedRec: Using Blockchain for Medical Data Access and Permission Management”, 2016 2nd International

Conference on Open and Big Data (OBD), pp. 25-30, 2016.
DOI: https://doi.org/10.1109/OBD.2016.11

[6] Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M., "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain", IEEE Access, Vol. 5, pp. 14757-14767, 2017. DOI: https://doi.org/10.1109/ACCESS.2017.2730843

[7] Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D., "Integrating blockchain for data sharing and collaboration in mobile healthcare applications", 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 1-5, 2017. DOI: https://doi.org/10.1109/PIMRC.2017.8292361

[8] Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W., "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control", Journal of Medical Systems, Vol. 40, No. 10, pp. 218, 2016. DOI: https://doi.org/10.1007/s10916-016-0574-6

[9] T. Haritha and A. Anitha, "Multi-Level Security in Healthcare by Integrating Lattice-Based Access Control and Blockchain-Based Smart Contracts System", IEEE Access, Vol. 6, pp. 464-478, 2017. DOI: https://doi.org/10.1109/ACCESS.2023.3324740

[10] S. Demurjian, T. Agresta, E. Sanzi, and J. DeStefano, "Alternative Approaches for Supporting Lattice-based Access Control (LBAC) in the Fast Healthcare Interoperability Resources (FHIR) Standard", HEALTHINF, pp. 97-108, 2020. DOI: https://doi.org/10.5220/0010150800930104

[11] E. Mohammed and E. S. Hajji, "SWOT Analysis of Access Control Models", International Journal of Security and Its Applications, Vol. 8, No. 3, pp. 407-424, 2014.
DOI: https://doi.org/10.14257/ijsia.2014.8.3.39

[12] C.E. Landwehr, C.L. Heitmeyer, and J. McLean, "A security model for military message systems", ACM Transactions on Computer Systems (TOCS), Vol. 2, No. 3, pp. 198-222, 1984.
DOI: https://doi.org/10.1145/989.991

[13] D.E. Denning, "A lattice model of secure information flow", Communications of the ACM, Vol. 19, No. 5, pp. 236-243, 1976.
DOI: https://doi.org/10.1145/360051.360056

저 자 소 개

노창현(ChangHyun Roh)

2017.08 순천향대학교 소프트웨어공학과 졸업
2020.02 순천향대학교 컴퓨터학과 석사
2020.05-2022.02 에스지에이비엘씨㈜ 컨설팅팀 사원
2022.03-현재 가천대학교 정보보호학과 박사과정
2022.12-현재 엘에스웨어㈜ 소프트웨어연구소 연구개발본부 수석연구원
<주관심분야> 정보보호, CPS 보안, 블록체인, DID, NFT, 저작권 기술, 메타버스, 디지털휴먼

신동명(Dong-Myung Shin)

2003.02 대전대학교 컴퓨터공학과 박사
2001-2006 한국정보보호진흥원 응용기술팀 선임연구원
2006-2014 한국저작권위원회 저작권기술팀 팀장
2014-2016 한국스마트그리드사업단 보안인증팀 팀장
2016-현재 엘에스웨어㈜ 소프트웨어연구소 연구소장/상무이사
<주관심분야> 오픈소스 라이선스, 저작권 기술, 시스템/네트워크보안, SW취약점분석・감정, 블록체인 기술, 메타버스