논문 2023-4-7 http://dx.doi.org/10.29056/jsav.2023.12.07

보안등급 기반 분산신원증명을 활용한 지능형 접근 제어 시스템

김현수*, 최창준*, 박경엽*, 노창현*, 신동명*†

Intelligent access control system using decentralized identity with security level

Hyun-Soo Kim*, Chang-Jun Choi*, Kyung-Yeob Park*, ChangHyun Roh*, Dong-Myung Shin*†

요 약

최근 데이터의 폭증과 시스템의 복잡성 증가로 데이터 유출 문제에 직면하고 있다. 데이터 유출 대응을 위한 평균 비용의 상승으로 기업은 데이터 접근 제어의 중요성을 보다 크게 인식하고 있다. 그러나 기존 데이터 접근 제어 시스템은 사용자의 데이터 접근 및 사용을 제한하고 있으며, 접근하기 위해서는 자격증명을 제출하여 특정 권한을 획득해야 한다. 이러한 경우 개인의 자격증명은 타인에 의해 관리되며, 외부 상황에 신속하게 대처하기 힘든 한계가 존재한다. 이에 본 논문에서는 보안등급 기반 분산신원증명을 활용한 지능형 접근 제어 시스템을 제안한다. 본 시스템을 통해 사용자는 본인이 직접 자격증명을 관리하며, 외부 변화로 인한 새로운 권한 필요 시 강화학습 모델을 통해 필요한 자격증명을 자동으로 선택할 수 있다. 또한 본 시스템은 검증 가능한 자격증명 및 프레젠테이션을 통해 기밀성, 무결성, 부인방지의 보안 요구사항을 충족한다. 향후 강화학습 뿐만 아닌 새로운 인공지능 모델을 적용하여 분산신원증명 기술을 고도화할 수 있다.

Abstract

Facing the recent surge in data volume and increasing complexity of systems, organizations are confronted with data security challenges. The average cost of data breaches has risen, leading businesses to recognize the heightened importance of data access control. However, existing data access control systems restrict users' access and require the submission of credentials to obtain specific permissions. In such cases, individuals' credentials are managed by others, posing limitations in promptly adapting to external changes. In this paper, we propose a intelligent access control system using security level-based decentralized identity (DID). Through this system, users directly manage their credentials, and in the event of new authorization requirements due to external changes, the reinforcement learning model automatically selects the necessary credentials. Furthermore, the proposed system meets security requirements, including confidentiality, integrity, and non-repudiation, through verifiable credentials and presentations. Future advancements can be achieved by applying not only reinforcement learning but also incorporating novel artificial intelligence models to enhance decentralized identity technology.

한글키워드 : 분산신원증명, 데이터 접근 제어, 보안등급, 강화학습, 보안 시스템

keywords : decentralized identity, data access control, security level, reinforcement learning, security system

* 엘에스웨어㈜
† 교신저자: 신동명(roland@lsware.co.kr)

접수일자: 2023.11.30. 심사완료: 2023.12.09.
게재확정: 2023.12.20.

1. 서 론

데이터의 폭증과 관리시스템의 복잡성 증가로 인해 데이터 웨어하우스, 데이터 레이크와 같은 데이터 관리 기술이 등장하고 있다. 하지만 IBM 시큐리티의 2023년 데이터 유출 비용 연구 보고서에 따르면 데이터 유출로 인한 전 세계 평균 비용은 지난 3년간 약 15% 증가한 59억원이며, 한국 역시 19% 증가한 45억 3600만원으로 추산된다. 이에 따라 기업들은 데이터 유출 발생 후 51%의 조직이 보안 지출을 늘린 것으로 조사됐다[1]. 이렇듯 기업의 내부 관리 데이터의 중요도가 증가함에 따라 데이터 접근 제어의 중요성 역시 증가하고 있다.

기존의 데이터 접근 제어는 데이터의 접근 및 사용을 관리하고 제한함으로써 데이터 보안을 유지한다. 이에 사용자는 자신에 대한 자격증명을 시스템에 제출하고 특정 권한을 획득한 뒤, 데이터를 이용한다. 그러나 업무 변경 및 인사이동 등의 외적 요인으로 인해 신규 권한이 필요한 경우 새로운 자격증명을 제출이 필요하고, 이 자격증명을 획득하기 위해 다른 프로세스를 수행해야 한다. 이렇듯 기존의 데이터 접근 제어 관리를 위한 자격증명 발행 및 권한 획득은 본인이 아닌 제 3자에 의해 자격증명이 관리되며, 외부 상황에 신속하게 대처하기 어렵다.

이러한 문제점을 해결하기 위해 본 연구에서는 탈중앙화된 분산 신원증명(DID, Decentralized Indentity)기술과 강화학습(LR, Reinforcement Learning)을 융합한 보안등급 기반 분산신원증명을 활용한 지능형 접근 제어 시스템을 제안한다[2][3]. 제안하는 시스템은 데이터 접근 제어 권한을 얻기위한 자격증명을 사용자가 직접 관리하며, 접근 제어에 필요한 자격증명과 그 요소를 강화학습 모델을 통해 자동으로 선택된다. 이를 통해 사용자의 자격증명을 본인이 직접 관리할 수 있으며, 외부 상황의 변경에 따라 변경되는 필요 권한 획득을 신속하게 대처할 수 있다. 또한 검증된 사용자만 데이터에 접근할 수 있기 때문에 데이터 접근 제어의 신뢰성 역시 확보할 수 있다.

본 논문에서는 2장에서 관련 연구를 설명하고, 3장에서는 제안 시스템에 관해 설명한다. 4장에서는 제안 시스템에 대한 평가를 진행하고, 5장에서 결론 및 향후 연구 방향을 설명하며 마무리한다.

2. 관련연구

2.1 데이터 접근 제어

데이터 접근 제어(DAC, Data Access Control)는 시스템이나 네트워크에 저장된 데이터에 대한 사용자의 접근을 제어하고 관리하는 보안 매커니즘이다[4]. 사용자의 데이터 접근 범위를 판단하기 위해 먼저 기업이 보유하고 있는 데이터를 중요도에 따라 분류하고 등급에 따른 접근 가능 데이터를 판단한다. 데이터 등급은 표 1과 같이 4등급으로 분류할 수 있다[5]. 가장 낮은 등급인 공개 데이터(Public Data)는 기업 내부와 외부에서 모두 접근이 가능한 데이터며, 대외비 데이터(Internal Data)는 내부에서만 접근이 가능한 데이터다. 비밀 데이터(Restricted Data)는 기업 내부에서도 관련 인원만 접근이 가능한 데이터로 같은 부서 인원 또는 협업 중인 부서들 간의 공유할 수 있는 데이터다. 기밀 데이터(Confidential Data)는 기업의 중요 정보로써 기업 내부에서도 관련 임원과 같은 한정된 인원만 접근이 가능한 데이터다. 또한 표 2와 같이 데이터의 보안등급이 낮더라도 접근자의 부서 및 업무 협력정도에 따라 높은 직급의 직원이 접근하지 못하는 상황이 발생할 수 있다.

표 1. 데이터 보안등급 분류
Table 1. Data security levels classification

데이터 등급	기준
기밀 데이터 (Confidential)	내부에서 일부 인원만 접근 가능
비밀 데이터 (Restrict)	내부에서 관련 인원이 접근 가능
대외비 데이터 (Internal)	내부에서 접근 가능
공개 데이터 (Public)	내●외부 모두 접근 가능

표 2. 데이터 보안등급 및 부서별 접근 가능 예시
Table 2. Example of data security level and departmental access

데이터	데이터 보안등급	관련부서	접근가능 직원
A	기밀	경영	임원급
B	대외비	연구	연구팀 전체
C	비밀	연구	연구팀 팀장급● 임원급
D	비밀	인사	인사팀 팀장급● 임원급
E	공개	홍보	제한 없음

2.2 자기주권 신원증명

자기주권 신원증명(SSI, Self-Sovereign Identity)는 사용자가 본인의 디지털 신원을 외부가 아닌 본인 스스로 소유하고 관리하는 개념이다[6]. 이러한 개념을 탈중앙화된 방식인 블록체인 기술을 융합하여 구현한 기술이 분산 신원증명(DID, Decentralized Identify)이다[7][8]. 분산 신원증명의 기술적 구성은 DID 아이디, DID 문서, 검증 가능한 자격증명(VC, Verifiable Credential), 검증 가능한 프레젠테이션(VP, Verifiable Presentation)으로 구분할 수 있다. DID ID는 디지털 신원을 인증하는 고유 식별자이며, DID 문서는 특정 신원증명에 대한 메타데이터 및 관련 정보를 포함하며 이는 공개키, 인증방법 등의 내용이 포함된다. 검증 가능한 자격증명은 신원정보를 포함하는 디지털 자격증으로, 사용자가 제공한 클레임(Claim)을 기반으로 작성한 내용과 함께 사용자의 서명 및 메타데이터 정보로 구성된다. 이렇게 생성된 자격증명들은 개인이 소유하고, 자격증명 자체를 제출하거나 자격증명의 일부 클레임을 제출하여 검증 가능한 프레젠테이션을 생성한다. 검증 가능한 프레젠테이션은 자격증명의 구성과 동일하게, 제출된 자격증명의 내용과 사용자의 서명 및 메타데이터 정보로 구성된다. 분산 신원증명의 컴포넌트는 그림 1과 같이 구성된다. 발행기관(Issuer)는 자격증명을 발행하는 주체로, 사용자(Holder)의 클레임을 기반으로 자격증명을 발행한다. 사용자는 자격증명을 소유하고 관리하는 주체로, 자격증명에서 필요한 정보를 선택하여 프레젠테이션을 생성한다. 검증기관(Verifier)는 프레젠테이션을 검증하는 주체로 사용자의 DID 문서를 사용하여 프레젠테이션을 검증한다. 검증 가능한 데이터 저장소(Verifiable Data Registry)는 DID 아이디, DID 문서를 저장하기 위한 분산 저장소로 블록체인, IPFS(InterPlanetary File System) 등이 활용 가능하다[9].

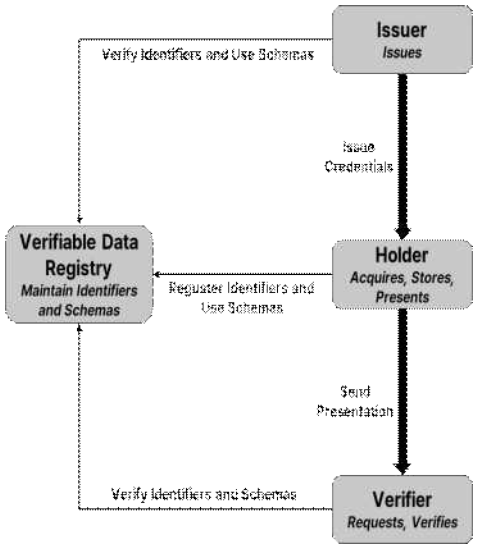

그림 1. 분산 신원증명 구성 및 흐름
Fig 1. DID componet and flow

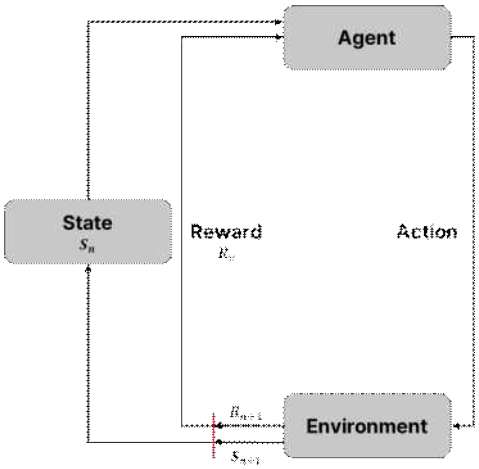

그림 2. 강화학습 구성요소
Fig 2. Reinforcement learning component

2.3 강화학습

강화학습(RL, Reinforcement Learning)은 기계학습의 한 분야로, 에이전트(Agent)가 환경(Environment)과 상호작용하며, 특정 목표를 달성하기 위한 최적의 행동을 스스로 학습하는 알고리즘이다. 이는 스스로 학습하며 시행착오를 통해 경험을 쌓고, 올바른 선택을 했을 때 보상이라는 개념을 통해 편향과 가중치를 학습한다. 강화학습은 그림 2와 같이 4개의 구성요소로 구분할 수 있다. 상태(State)는 에이전트가 환경과 상호작용 할 때 상황을 의미하며, 다양한 파라미터가 포함될 수 있다. 에이전트는 의사를 결정하는 부분으로 현재의 상태를 파악하고 행동(Action)을 선택하기 위한 정책(Policy)을 포함하고 있다. 환경에서는 에이전트의 다음 상태와 보상(Reward)을 결정하고, 다음 보상을 예측하며 학습한다. 보상은 에이전트의 행동에 따라 적합하면 양의 보상, 부적합하면 음의 보상이 주어진다. 이를 통해 에이전트는 최적의 보상을 찾기 위해 지속적으로 학습한다 [10-12].

3. 제안 시스템

사내 파일 관리 시스템의 파일 데이터는 보안을 위해 각 파일별로 보안등급을 분류하여 접근을 제어하고 있다. 이러한 보안등급은 파일의 목적 및 내용에 따라 분류되며, 같은 보안등급의 파일이더라도 부서, 직급, 업무에 따라 접근 가능 여부가 다르다. 본 논문에서는 이러한 파일 데이터 관리가 보안등급에 따라 관리되고 있는 환경에서 자격증명을 생성하고 이를 사용하는 시스템을 그림 3과 같이 제안한다.

3.1 검증 가능한 자격증명

본 시스템에서는 검증 가능한 프레젠테이션(VP, Verifiable Presentation) 생성에 활용하는 검증 가능한 자격증명(VC, Verifiable Credential)은 총 4개로 각 자격증명에 대한 상세한 설명은 다음과 같다.

- **데이터 보안등급(Data Security Level)**
  개인별 데이터 보안등급 자격증명은 데이터 관리자가 개인의 직급, 직책 등을 고려하여

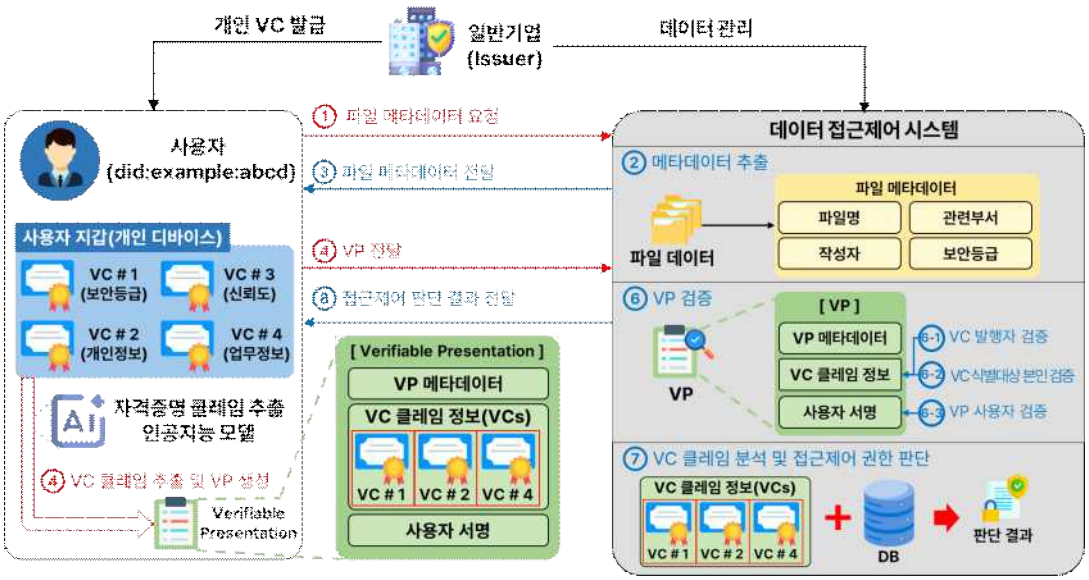

그림 3 제안 시스템 개요도
Fig 3. Proposed system overview

개인에게 부여한다. 발급된 데이터 보안등급 자격증명의 속성은 표 3과 같이 정의한다.

표 3. 데이터 보안등급 자격증명(VC) 속성 정의
Table 3. Data security level VC attribute

속 성		설 명
대분류	중분류	
사원 정보	사원 DID	- VC를 발급받는 사원의 DID 식별자
	사원 번호	- VC를 발급받는 사원의 사원번호
	사원명	- VC를 발급받는 사원의 사원명
	직급	- VC를 발급받는 사원의 직급
	직책	- VC를 발급받는 사원의 직책
발급자 정보	관리자 DID	- 데이터 보안등급 관리자의 DID 식별자
	발급일	- 발급된 VC의 발급일
	발급 보안등급	- 사원에게 허가된 데이터 보안등급
디지털 서명		- 보안 관리자의 디지털 서명

- **개인정보(Private Information)**

개인정보 자격증명은 사내에서 관리하는 인사정보를 기반으로 개인에게 부여한다. 이는 사내에서도 활용할 수 있지만 외부에서도 본인의 신분을 인증하는데에 사용될 수 있으며 속성은 표 4와 같이 정의한다.

표 4. 개인정보 자격증명(VC) 속성 정의
Table 4. Private information VC attribute

속 성		설 명
대분류	중분류	
사원 정보	사원 DID	- VC를 발급받는 사원의 DID 식별자
	사원번호	- VC를 발급받는 사원의 사원번호
	사원명	- VC를 발급받는 사원의 사원명
	주민등록번호	- VC를 발급받는 사원의 주민등록번호
	이메일	- VC를 발급받는 사원의 이메일 주소
	주소	- VC를 발급받는 사원의 자택 주소

	전화번호	- VC를 발급받는 사원의 휴대폰 번호
	학력	- VC를 발급받는 사원의 학력
	경력	- VC를 발급받는 사원의 경력
발급자 정보	관리자 DID	- 사원정보 관리자의 DID 식별자
	발급일	- 발급된 VC의 발급일
디지털 서명		- 인사부의 디지털 서명

- **신뢰도(Reliability)**
  신뢰도 자격증명은 사내에서 개인의 근태현황, 업무평가, 징계여부 등을 기준으로 평가하여 개인에게 부여한다. 발급된 신뢰도 자격증명의 속성은 표 5와 같이 정의한다.

표 5. 신뢰도 자격증명(VC) 속성 정의
Table 5. Reliability VC attribute

속 성		설 명
대분류	중분류	
사원 정보	사원 DID	- VC를 발급받는 사원의 DID 식별자
	사원번호	- VC를 발급받는 사원의 사원번호
	사원명	- VC를 발급받는 사원의 사원명
	근속연수	- VC를 발급받는 사원의 근속 연수
	근태현황	- VC를 발급받는 사원의 근태 현황
	업무평가	- VC를 발급받는 사원의 업무 평가
	징계여부	- VC를 발급받는 사원의 징계 여부
	근무연혁	- VC를 발급받는 사원의 근무 연혁
발급자 정보	관리자 DID	- 신뢰도 평가 관리자의 DID 식별자
	발급일	- 발급된 VC의 발급일
	발급 신뢰도 평가 점수	- 사원 신뢰도 평가 점수
디지털 서명		- 평가 관리자의 디지털 서명

- **업무 정보(Business Information)**
  업무 정보 자격증명은 개인이 담당하고 있는 주요 업무와 협업해서 진행하고 있는 프로젝트 정보 및 특정 부서 정보 고려하여 부여한다. 발급된 업무정보 자격증명의 속성은 표 6과 같이 정의한다.

표 6. 업무 정보 자격증명(VC) 속성 정의
Table 6. Business information VC attribute

속 성		설 명
대분류	중분류	
사원 정보	사원 DID	- VC를 발급받는 사원의 DID 식별자
	사원번호	- VC를 발급받는 사원의 사원번호
	사원명	- VC를 발급받는 사원의 사원명
	부서명	- VC를 발급받는 사원의 근무 부서
	직급	- VC를 발급받는 사원의 직급
	참여 프로젝트	- VC를 발급받는 사원의 참여 프로젝트
	주요 업무	- VC를 발급받는 사원의 프로젝트 내 주요 업무
	관련 부서	- VC를 발급받는 사원이 참여하는 프로젝트 관련 부서
발급자 정보	관리자 DID	- 업무 정보 관리자의 DID 식별자
	발급일	- 발급된 VC의 발급일
	업무 범위	- 사내에서 판단한 사원의 업무 범위
	관계 부서	- 사내에서 판단한 사원의 업무 관련 부서
디지털 서명		- 부서 관리자의 디지털 서명

3.2 검증 가능한 프레젠테이션

3.1 검증 가능한 자격증명을 기반으로한 검증 가능한 프레젠테이션은 여러 자격증명들로부터 추출된 클레임(Claim)과 사용자의 서명, 검증정보 등으로 구성된다. 이렇게 생성된 프레젠테이션을 사내 시스템에서는 검증하고, 사용자가 특정 파일에 대한 접근 권한을 갖고 있는지 판단한다. 본 시스템에서는 자격증명으로부터 적절한 클레임을 추출하는 과정에서 인공지능 모델을 사용하여, 사용자의 목적에 적합한 클레임을 추출한다. 이 과정은 다음과 같은 단계로 진행된다.

- Step 1
  사용자는 시스템에 본인이 접근하고자 하는 파일에 대한 접근 권한 검증을 요청하며 본인의 검증 가능한 자격증명을 전달한다.
- Step 2
  시스템은 파일을 분석하여 파일의 데이터 보안 등급, 작성자, 관련 부서 등의 파라미터 정보를 추출한다.
- Step 3
  인공지능 모델은 추출된 파라미터를 기반으로 검증 가능한 자격증명에서 클레임을 추출하여 검증 가능한 프레젠테이션을 생성하여 사용자에게 전달한다..
- Step 4
  사용자는 전달받은 검증 가능한 프레젠테이션을 이용하여 파일에 대한 접근 권한 유무를 검증한 뒤, 파일에 접근한다.

3.3 자격증명 클레임 추출 모델

본 시스템에서 검증 가능한 프레젠테이션 생성을 위해 자격증명으로부터 최적의 클레임을 추출하는 인공지능 모델은 심층 강화학습(DLP, Deep Reinforcement Learning)으로 학습하고 결과를 추론한다. 파일에서 추출된 파라미터인 데이터 보안 등급, 파일명, 작성자, 작성 부서 등을 기반으로, 주어지는 파라미터에 따라 가장 적합한 자격증명들을 선별하고, 선별된 자격증명으로부터 최적의 클레임을 추출하여 이를 프레젠테이션으로 생성한다. 본 시스템에서는 심층 강화학습 모델 중 정책 최적화 기법의 하나인 PPO(Proximal Policy Optimization), TRPO(Trust Region Policy Optimization) 모델을 검증 가능한 프레젠테이션 생성에 활용한다[13][14].

4. 제안 시스템 평가

본 장에서는 3장에서 제안한 시스템에 대해 4개의 기준을 적용하여 평가하였다.

4.1 시스템 보안 요구사항

본 시스템은 데이터 접근제어에 분산 신원증명과 심층강화학습을 사용한 보안 시스템으로 다음과 같은 보안 요구사항을 충족해야 한다.

- **기밀성**
  본 시스템을 통해 관리되는 데이터는 데이터 보안등급에 따라 분류되고 있으며, 같은 보안등급의 데이터는 파일의 특성에 따라 관리되고 있다. 또한 검증 가능한 자격증명 및 프레젠테이션 기술을 활용하여 인가된 사용자만 파일에 접근할 수 있기 때문에 기밀성을 충족한다.
- **무결성**
  본 시스템은 사용자가 검증 가능한 프레젠테이션을 생성할 경우, 사용자의 보안등급 및 신뢰도, 업무정보와 같은 검증 가능한 자격증명으로부터 클레임을 추출한다. 이에 따라 사용자가 특정 파일에 접근할 때, 해당 파일에 대한 수정 및 삭제 권한을 다르게 부여하

여 관리한다. 이에 따라 본 시스템은 무결성을 충족한다.

- **부인방지**
  본 시스템은 사용자가 파일에 접근할 때, 검증 가능한 자격증명 및 프레젠테이션을 활용한다. 자격증명 및 프레젠테이션에는 이를 사용하는 사용자와 발급자의 서명이 존재한다. 이는 본인의 개인키로 서명이 진행되며, 이를 공개키로 검증이 가능하기 때문에 부인방지를 충족한다.

4.2 검증 가능한 자격증명 발행

본 시스템에서 활용하는 검증 가능한 자격증명은 기본적으로 사내에서 발행되는 자격증명이다. 이에 발행한 자격증명이 유효한지 검증하기 위해서는 사용자와 발급자 DID 아이디의 유효성, 발급자의 서명 여부를 검증한다. DID 아이디의 유효성은 저장소에 저장된 사용자 및 발급자의 DID 문서를 조회하여 적합한 DID 아이디인지 검증이 가능하다. 발급자의 서명 여부는 발급된 검증 가능한 자격증명의 디지털 서명을 발행자의 공개키로 검증할 수 있다.

4.3 검증 가능한 프레젠테이션 검증

본 시스템에서 활용하는 검증 가능한 프레젠테이션을 검증하기 위해서는 검증기관이 필요한데, 이는 시스템 또는 별도의 사내 서버에서 수행한다. 검증기관은 다음의 3가지 항목에 대해서 검증을 수행한다.

- **VP 활용 VC 발행자 검증**
  프레젠테이션에서 활용하는 자격증명의 위●변조 여부 및 발급자가 올바른 발급자인지 검증을 위해, 자격증명 서명의 공개키로 검증할 수 있다.
- **VC 식별대상 본인 검증**
  프레젠테이션에서 자격증명이 가리키는 식별대상이 사용자가 맞는지 검증을 위해, DID Auth라는 사용자가 DID를 관리하고 있음을 증명하는 방법을 통해 사용자를 인증한다.
- **VP 사용자 검증**
  사용자로부터 제출된 프레젠테이션이 위●변조 여부 및 본인 검증을 위해, 프레젠테이션에 서명된 값을 사용자의 공개키로 검증할 수 있다.

4.4 클레임 추출 정확도

본 시스템에서 활용하는 검증 가능한 자격증명으로부터 클레임을 추출하는 인공지능 모델은 사용자가 접근하고자 하는 파일 정보를 기반으로 사용자의 자격증명으로부터 필요한 클레임을 추출해야 한다. 이 과정에서 고려해야 할 부분은 불필요한 클레임을 추출해서, 실제로 접근 가능한 인원이 접근할 수 없거나 접근하지 권한이 없는 인원이 중요 파일에 접근하는 상황이 발생하지 않아야한다. 이에 다수의 테스트케이스를 생성하여 자격증명으로부터 추출한 클레임으로 이루어진 프레젠테이션의 사용 결과를 기반으로 클레임 추출 정확도를 측정한다.

4.5 시스템 검증 방법

본 시스템의 기능을 검증하기 위해서는 시스템이 제공하는 기능들이 일련의 과정을 통해 수행되고 결과를 확인할 수 있어야 한다. 이에 본 시스템의 기능 검증을 위한 시나리오는 아래와 같다.

- Step 1
  시스템에서 관리하는 파일은 보안등급이 평가되어있고, 해당 파일에 접근을 위한 정보인 작성자, 관련 부서 등을 포함하고 있다. 또한 사용자는 분산신원증명을 위한 검증 가능한 자격증명을 발급받아 본인이 소유 및 관리하고 있다.

- Step 2
  사용자는 시스템에서 관리하는 파일에 접근하는 경우, 자동으로 검증 가능한 프레젠테이션을 시스템에 제출하여 본인의 신원 및 자격을 평가받는다. 이 때, 생성되는 검증 가능한 프레젠테이션을 구성하는 클레임은 클레임 추출 인공지능이 사용자가 소유한 자격증명으로부터 추출하여 사용된다.

- Step 3
  시스템은 사용자가 제출한 프레젠테이션을 활용하여, 4.3의 프레젠테이션 검증 과정을 수행한다. 이를 통해 사용자의 신원과 사용자가 제출한 프레젠테이션에 사용된 클레임을 검증할 수 있다.

- Step 4
  사용자가 제출한 프레젠테이션을 사용해 신원에 대한 검증을 수행한 뒤, 시스템은 사용자가 제출한 클레임을 분석한다. 이를 통해 사용자가 특정 파일에 접근 가능한 대상인지 확인하고, 이에 따른 권한을 부여한다. 사용자는 부여받은 권한에 따라 적합한 경우에만 파일에 접근할 수 있다.

5. 결 론

기존의 데이터 접근 제어는 사용자가 데이터 접근 및 사용에 대한 권한을 얻기 위해 본인의 자격증명을 관리자에게 제출해야하는 문제가 있다. 또한 외부 상황의 변화로 필요한 접근제어 권한이 변경될 경우, 권한 부여심사에 필요한 자격증명을 다시 제출해야하고 이에 따라 빠른 대응이 어려운 문제가 있다. 이에 본 연구에서는 탈중앙화된 분산 신원증명과 강화학습 모델을 융합한 보안등급 기반 분산 신원증명을 활용한 지능형 접근 제어 시스템을 제안하였다.

제안 시스템은 검증 가능한 자격증명을 본인이 직접 관리하며, 검증 가능한 프레젠테이션 생성 시 필요한 자격증명을 지능형 강화학습 모델이 선택해서 자동으로 프레젠테이션을 생성한다. 이때, 생성된 프레젠테이션을 사용하여 사용자는 데이터 접근 및 이용이 가능하다. 이 과정에서 사용자는 발급기관으로부터 발급된 자격증명을 본인이 관리하며, 데이터 접근 및 이용에 필요한 정보 역시 외부에 제출하지 않는다. 또한 외부상황이 변화될 경우, 필요한 권한을 신속하게 획득할 수 있다. 이렇듯 제안 시스템은 기존 데이터 접근 제어의 자격증명 관리와 권한 획득 문제를 해결하며, 검증 가능한 자격증명 및 프레젠테이션을 통해 보안 요구사항을 만족한다.

향후에는 데이터 보안 등급 판단과 검증 가능한 자격증명으로부터 클레임을 추출하는 기술에 패턴분석, 데이터 분류, 추천 알고리즘 등 다양한 분야의 인공지능 모델을 적용하여 고도화한다면 보다 높은 수준의 데이터 접근 제어가 가능할 것이다.

이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No. RS-2023-00229451, 이종 플랫폼간 상호호환이 가능한 디지털휴먼(아바타) 연동 기술 개발)

참 고 문 헌

[1] IBM, “2023 Cost of Data Breach Report”
[2] D. Reed et al., “Decentralized Identifiers (DIDs) v1.0, Core Data Model and Syntaxes”, W3C Working Draft 09 December 2019;

https://www.w3.org/TR/did-core/.
[3] Kaelbling, Leslie Pack, Michael L. Littman, and Andrew W. Moore. “Reinforcement learning: A survey”, Journal of artificial intelligence research 4 (1996): 237-285.
[4] Samarati, Pierangela, and Sabrina Capitani de Vimercati. “Access control: Policies, models, and mechanisms”, International school on foundations of security analysis and design. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000. 137-196.
[5] Trade Secret Protection Center, “Trade Secret Classification Guide”, 2021.
[6] Tobin, Andrew, and Drummond Reed. “The inevitable rise of self-sovereign identity”, The Sovrin Foundation 29.2016 (2016): 18.
[7] Avellaneda, Oscar, et al. “Decentralized identity: Where did it come from and where is it going?”, IEEE Communications Standards Magazine 3.4 (2019): 10-13.
[8] Dib, Omar, and Khalifa Toumi. “Decentralized identity systems: Architecture, challenges, solutions and future directions”, Annals of Emerging Technologies in Computing (AETiC), Print ISSN (2020): 2516-0281.
[9] Benet, Juan. “Ipfs-content addressed, versioned, p2p file system”, arXiv preprint arXiv:1407.3561 (2014).
[10] Arulkumaran, Kai, et al. “Deep reinforcement learning: A brief survey”, IEEE Signal Processing Magazine 34.6 (2017): 26-38.
[11] Wiering, Marco A., and Martijn Van Otterlo. “Reinforcement learning”, Adaptation, learning, and optimization 12.3 (2012): 729.
[12] François-Lavet, Vincent, et al. “An introduction to deep reinforcement learning”, Foundations and Trends® in Machine Learning 11.3-4 (2018): 219-354.
[13] Schulman, John, et al. “Proximal policy optimization algorithms”, arXiv preprint arXiv:1707.06347 (2017).
[14] Schulman, John, et al. “Trust region policy optimization”, International conference on machine learning. PMLR, 2015.

저 자 소 개

김현수(Hyun-Soo Kim)

2019.02 단국대학교 소프트웨어학과 학사
2023.08 숭실대학교 AI,SW융합학과 석사
2019.01 - 현재 : 엘에스웨어(주) 선임
<주관심분야>
소프트웨어 공학, 딥러닝, 컴퓨터 비전, 분산신원증명, 빅데이터

최창준(Chang-Jun Choi)

2019.02 상명대학교 컴퓨터공학과 졸업
2021.08 세종대학교 정보보호학과 석사
2021.09-현재 : 엘에스웨어㈜ 소프트웨어연구소 연구개발본부 주임연구원
<주관심분야> 정보보호, 블록체인, 네트워크 보안, 분산신원증명, 저작권 기술

박경엽(Kyung-Yeob Park)

2019.02 서울과학기술대학교 컴퓨터공학과 석사
2019.01-현재 엘에스웨어㈜ 소프트웨어연구소 연구개발본부 선임연구원
<주관심분야> 정보보호, IoT 보안, 블록체인, 빅데이터, 분산신원증명, 저작권 기술

노창현(ChangHyun Roh)

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

신동명(Dong-Myung Shin)

2003.08 대전대학교 컴퓨터공학과 박사
2001-2006 한국정보보호진흥원(KISA) 응용기술팀 선임연구원
2006-2014 한국저작권위원회 저작권기술팀 팀장
2014-2016 한국스마트그리드사업단 보안인증팀 팀장
2016-현재 엘에스웨어㈜ 소프트웨어연구소 연구개발본부 연구소장/상무이사
<주관심분야> 오픈소스 라이선스, 저작권 기술, 시스템/네트워크 보안, SW 취약점 분석·감정, 블록체인 기술