IAM 서비스를 이용한 블록체인에서의 개인정보보호 시스템 설계

강명조[1], 김미희[2]
[1]한경국립대학교 컴퓨터응용수학부
[2]한경국립대학교 컴퓨터응용수학부, 컴퓨터시스템연구소
email:{rkdaudwh13, mhkim}@hknu.ac.kr

Design of Personal Information Protection System in Blockchain using IAM Service

Myung-Joe Kang[1], Mi-Hui Kim[2]
[1]School of Computer Engineering & Applied Mathmatics Hankyong National University
[2]School of Computer Engineering & Applied Mathmatics, Computer System Institute Hankyong National University

요 약

본 논문에서는 인터넷으로 블록체인 플랫폼 및 서비스를 제공하는 BaaS 환경에서 IAM 서비스를 이용한 개인정보 보호 시스템을 설계했다. 서비스 사용자는 API를 통해 클라우드에 데이터를 요청하는데, 사용자와 클라우드 사이에 API 미들웨어를 두어 클라우드 데이터에 직접 접근하지 못하도록 한다. 또한, 미들웨어의 역할을 하는 서버는 IAM(Identity & Access Management) 서비스에서 생성한 역할 및 정책, 권한에 따라 허가된 데이터에만 접근하며 사용자의 데이터 요청 전/후로 인증 절차를 진행해 시스템의 기밀성 및 무결성을 만족할 수 있도록 한다.

1. 서론

유럽연합(EU)은 지역 단체 내의 모든 개인에 대한 데이터 보호를 강화하고 개인정보에 대한 통제권을 개인에게 부여하며, 개인정보를 취급하는 기업의 규제를 위해 개인정보 일반규정 GDPR(General Data Protection Regulation)을 2018년 5월부터 시행중이다. 규정은 사용자의 개인정보 수집부터 처리, 만료 후 삭제 등 모든 과정에서 적용해야 하는 내용을 상세히 서술한다. 세부 내용 중 주요 특징으로, 사용자의 개인정보를 처리하는 기업은 정보 주체가 자신의 개인정보를 관리할 수 있도록 하는 수단을 제공해야 하며, 정보를 받음에 있어 정보 주체가 동의했다는 사실을 증명할 수 있어야 하는 내용이 존재한다. 최근 국내, 국외에서는 이런 GDPR 및 개인정보보호를 만족하기 위해 블록체인을 활용한 연구가 활발히 진행되고 있다. 하지만 블록체인의 특성 중 투명성, 불변성, 분산성 등은 기존의 개인정보보호와는 거리가 있어 별도의 처리가 추가로 필요하다. 그럼에도 블록체인이 제공하는 관리의 편리성, 경제성, 스마트 계약의 강력한 성능, 보안성 등은 개인정보보호에 유용한 주요 속성으로 여겨져 개인정보 보호 시스템의 수단으로써 블록체인을 사용하려는 경우가 늘어나고 있다[1-2].

본 논문에서는 클라우드 사업자가 인터넷으로 블록체인을 제공하는 BaaS 서비스에서 클라우드의 IAM(Identity & Access Management) 서비스를 이용해 개인정보를 보호할 수 있는 시스템을 설계했다.

2. 배경지식

지금까지 제안된 블록체인 기반의 개인정보보호 시스템은 주로 로컬환경에서 구축되어 실제 사용 가능성 및 운영, 유지보수 등의 비용을 고려하지 않았지만, 본 논문에서 제안한 기법은 클라우드의 방대한 자원으로 블록체인과 IAM 서비스를 운영함으로, 개인정보보호 시스템의 기초 인프라부터 구축할 필요 없이 비용 효율적이며 확장성이 높은 시스템을 운영할 수 있는 장점이 있다.

2.1 IAM

IAM 서비스는 클라우드에서 계정 관리, 인증 관리, 역할 설정, 권한 부여 등을 수행하는 보안 서비

스로 클라우드 시장의 발전에 따라 2013년 약 5억 달러의 시장 규모에서 2015년 8억 6천만 달러로 발전했으며 2023년 현재까지도 지속해서 발전하고 있다. 클라우드 서비스를 제공하는 대표적인 회사로 Amazon, Microsoft, IBM 등이 있으며, 이들 중 Amazon IAM 서비스로 IAM의 기능을 설명한다.

Amazon 클라우드 서비스의 정식 명칭은 AWS(Amazon Web Service)로, AWS의 IAM은 사용자가 신청한 서비스와 자원에 대한 접근을 안전하게 통제하는 역할을 한다. 또한, 사용자와 그룹, 역할을 생성하고 접근 권한을 부여하여 정해진 접근제어를 수행할 수 있다. 표 1은 AWS IAM 서비스의 기능을 나타낸다.

<표 1> AWS IAM 기능 목록

Feature	Content
AWS Account Access Sharing	Access control by granting security credentials to user and group, role
Subdivided Authority	Different permission setting for each user and group, role
Multi-Factor Authentication (MFA)	Additional authentication for strengthen access security
ID Federation	Similar to SSO(Single-Sign-On), allowing corporate identities to utilize IAM services
Service Integration	Integrated management of all AWS services in AWS console
Managing Security Credentials	Assign various security credentials including password, key pairs and X.509 certificates, MFA

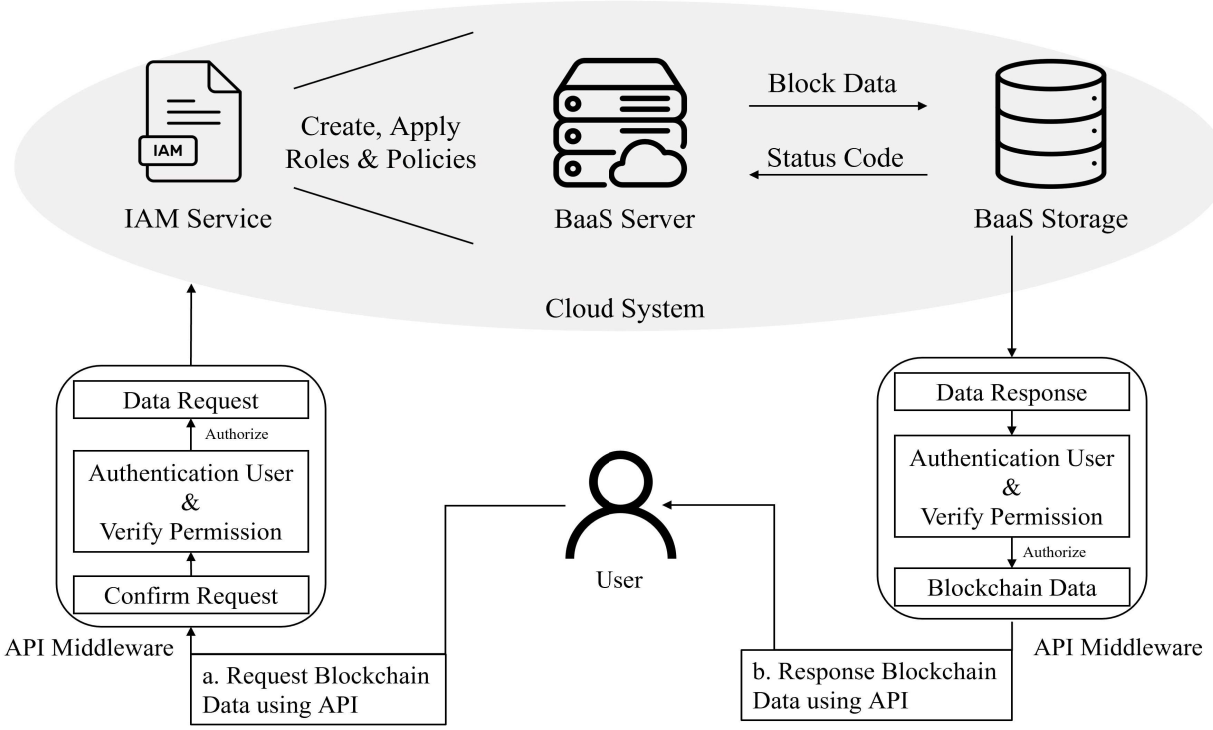
AWS IAM의 기능 중 AWS 계정 접근 공유의 경우 사용자 및 그룹, 역할에 보안 자격 증명을 부여하여 접근할 수 있는 서비스에 제한을 두어 보안을 강화할 수 있다. 또한, 이러한 자격 증명을 부여할 때 사용자, 그룹, 역할에 세분화 된 권한을 부여하여 다양한 수준의 접근제어를 수행할 수 있다. 다단계 인증의 경우 보안 강화를 위해 사용자를 인증할 때 기존 비밀번호 및 암호를 입력받고, 일회용 비밀번호 혹은 개인키 등을 추가로 입력하게끔 하는 방식을 사용하여 보안을 강화할 수 있다. ID 페더레이션(표 1. IP Federation)은 서로 다른 ID 관리 시스템에서, 사용자의 ID를 연결하는 방법으로 SSO와 비슷하게 동작하여 사용자의 편의성을 증대시킨다. 이외에도 IAM을 사용하면 한 번의 권한 설정으로 시스템 내의 모든 서비스에 접근 권한을 설정할 수 있으며, 인증 절차에 있어 비밀번호, 키 쌍, X.509 인증서, MFA 등을 자유롭게 설정할 수 있도록 한다[3-4].

2.2 BaaS

BaaS(Blockchain as a Service)는 클라우드 컴퓨팅을 통해 블록체인을 제공하는 개념으로, 블록체인 플랫폼 및 서비스를 주로 제공한다[5]. 블록체인 네트워크를 직접 구현하여 사용하는 것보다 구조의 변경, 확장, 구조 수정 등이 자유롭고 클라우드의 자원을 사용하여 접근제어, 유연성 제공, 비용 감소 등 다양한 장점을 얻을 수 있다. 또한, 블록체인 환경 구성 및 노드 생성의 일련의 개발 과정을 클라우드 콘솔에서 관리하여 개발 편의성을 확보할 수 있어 많은 기업에서 사용하고 있다. BaaS를 제공하는 기업은 기존 클라우드 서비스를 운영하는 회사로, 국외의 경우 Amazon, Microsoft, IBM, Alibaba 등이 있고 국내의 경우 KT, 두나무, 카카오 등이 있다[6].

3. 제안시스템

그림 1은 제안시스템의 구조를 나타낸다. 이는 사용자(그림 1. User), API 미들웨어(그림 1. API Middleware), 클라우드 환경 속 IAM 서비스(그림 1. IAM Service), BaaS 서버(그림 1. BaaS Server), BaaS 데이터 저장소(그림 1. BaaS Storage)의 엔티티로 구성된다. 사용자는 BaaS 서비스를 이용하는 사람으로, 블록체인에 있는 데이터를 API 미들웨어에게 요청하고, 응답으로 데이터를 전달받는다(그림 1. a). API 미들웨어는 사용자로부터 데이터 요청을 확인하고, 사용자가 해당 데이터에 접근할 수 있는 인물인지 검증한 후 클라우드에 있는 BaaS 구성 요소로부터 데이터를 받아 사용자에게 전달한다(그림 1. b). IAM 서비스는 외부와 통신할 수 있도록 하는 역할을 생성하여 API 미들웨어에 부여하고, BaaS 서비스에 접근을 통제하는 정책을 생성하여 외부 사용자들이 클라우드 내부 데이터에 접근하지 못하도록 구성한다. BaaS 서버는 BaaS 서비스를 제공하는 주체로 IAM이 구성한 정책에 기반하여 데이터 흐름을 관리하고 블록체인 운영, 구성한다. BaaS 데이터 저장소는 BaaS 서비스에서 생성된 블록 및 트랜잭션 데이터를 저장하고 상태 코드를 반환하여 저장상태 및 위치를 알리며, 사용자가 API 미들웨어를 통



(그림 1) 제안시스템 구조도.

해 블록체인 속 데이터를 요청한 경우, 그에 해당하는 데이터만 전달한다.

4. 결론 및 향후 연구

본 논문에서는 BaaS를 활용하는 사용자의 개인정보 및 스마트 계약 내용에 포함된 정보를 외부인의 열람, 수정, 삭제 등으로부터 보호하기 위해 IAM 서비스를 활용한 개인정보보호 시스템을 개념적으로 설계했다. 향후 연구에서는 제안시스템의 구현을 위해 클라우드로 BaaS와 IAM 서비스를 제공하는 Amazon, Microsoft와 같은 공급자를 선택해야 하고 블록체인 네트워크의 유형을 선택해야 하며, 클라우드와 통신할 수 있는 자바스크립트 등으로 구현된 백엔드 시스템 등이 구축되어야 한다. 또한, IAM 서비스의 구체적인 기능을 적용한 BaaS 시스템을 자바스크립트 web3 라이브러리, Solidity 언어 등을 사용해 구성, 구현하여 실제 시스템의 가능성을 보이고 블록체인 환경에서 개인정보 보호를 이루고자 한 관련 연구들과 비교하여 성능을 분석할 것이다.

5. Acknowledgement

이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2018R1A2B6009620), 교신저자 김미희.

참고문헌

[1] GDPR, [internet], https://gdpr-info.eu/ 2023.

[2] J.H. Lee, J.W. Kim, C.S. Kim, et. al, “Research and Implementation of Mutual Trust System for Consent to Use Personal Information Based on Blockchain”, The Jounal of Korean Institute of Communications and Information Science, Vol.45, No.8, pp.1342-1354, 2020.

[3] S.H. Jung, “Cloud-based IAM technology trends”, The Journal of The Korean Institute of Communication Sciences, Vol.32, No.10, pp.58-64, 2015.

[4] Amazon Web Service IAM, [internet], https://docs.aws.amazon.com/ko_kr/IAM/latest/UserGuide/introduction.html, 2023.

[5] J. song, P. Zhang, M. Alkubati,, et. al, “Research advances on blockchain-based-as-a-service: Architecture, applications and challenges”, Digital Communications and Networks, 2021.

[6] M.J. Kang, M.H. Kim, “A Study on Non-Fungible Token Platform for Usability and Privacy Improvement”, Korea Information Processing Society, Vol.11 No.11 pp.403-410, 2022.