ISSN : 1226-7244 (Print)
ISSN : 2288-243X (Online)
논문번호 23-04-25
j.inst.Korean.electr.electron.eng.Vol.27,No.4,548~555,December 2023
https : //doi.org/10.7471/ikeee.2023.27.4.548

BaaS에서 IAM을 이용한 개인정보 보호 기법에 관한 연구

A Study on IAM-Based Personal Data Protection Techniques in BaaS

김 미 희[1)★], 강 명 조[*]

Mi-Hui Kim[*★], Myung-Joe Kang[*]

Abstract

With the advancement of the internet, the use of personal information in online interactions has increased, underscoring the significance of data protection. Breaches of personal data due to unauthorized access can result in psychological and financial damage to individuals, and may even enable wide-ranging societal attacks aimed at those associated with the victims. In response to such threats, there is active research into security measures using blockchain to safeguard personal information. This study proposes a system that uses middleware and IAM (Identity and Access Management) services to protect personal information in a BaaS (Blockchain as a Service) environment where blockchain is provided via the Internet. The middleware operates on servers where IAM roles and policies are applied, authenticates users, and performs access control to allow only legitimate users to access blockchain data existing in the cloud. Additionally, to understand the impact of the proposed personal information protection method on the system, we measure the response time according to the time taken and the number of users under three assumed scenarios, and compare the proposed method and research related to personal information protection using blockchain in terms of security characteristics such as idea, type of blockchain, authentication, and confidentiality.

요 약

인터넷의 발전에 따라 개인정보를 활용한 온라인 상호작용이 활발해지며 개인정보를 보호하는 것이 중요해졌다. 허가되지 않은 접근으로부터 발생한 개인정보 침해는 개인에게 정신적, 재산적 피해를 불러올 수 있으며, 침해 피해자의 주변인을 대상으로 한 사회적 공격도 가능하다. 이러한 공격으로부터 개인정보를 보호하기 위해 블록체인을 활용한 보안 기법이 활발히 연구되고 있다. 본 논문에서는 블록체인을 인터넷으로 제공하는 BaaS(Blockchain as a Service) 환경에서 개인정보 보호를 위해 미들웨어와 IAM(Identity and Access Management) 서비스를 활용한 시스템을 제안했다. 미들웨어는 IAM 역할 및 정책이 적용된 서버에서 운영되며 사용자를 인증하고, 접근 권한을 파악하여 정상 사용자인 경우에만 클라우드에 존재하는 블록체인 데이터에 접근할 수 있도록 접근 제어를 수행한다. 또한, 제안한 개인정보 보호 기법이 시스템에 주는 영향을 파악하기 위해 세 가지 시나리오를 가정하여 소요 시간과 사용자 수별 응답 시간을 측정하고, 제안 기법과 블록체인을 활용한 개인정보 보호 관련 연구를 아이디어, 블록체인 유형, 인증, 기밀성 등과 같은 보안 특성 기준으로 비교한다.

Key words : BaaS, IAM, Privacy, Personal Information Protection, Middleware

1) School. of Computer Engineering & Applied Mathematics, Computer System Institute, Hankyong National University
★ Corresponding author
Email : mhkim@hknu.ac.kr, Tel : +82 31-670-5167
Manuscript received Oct. 18, 2023; revised Nov. 16, 2023; accepted Dec. 26, 2023,

Ⅰ. 서론

인터넷의 발전으로 디지털 세계에서 다양한 정보를 주고받는 것이 일상화되었으며, 이에 따라 전 세계적으로 개인정보 보호를 위한 다양한 정책과 법규가 도입되고 있다. 이러한 정책과 법규를 준수하지 않을 경우, 벌금 부과나 손해배상 책임을 질 수 있으며, 이러한 사례는 점점 증가하는 추세다[1]. 유럽의 경우 GDPR(General Data Protection Regulation)을 제정하여 EU 시민의 개인정보 처리와 보호를 조율하고 강화하며, 캐나다는

PIPEDA(Personal Information Protection and Electronic Documents Act)를 제정하여 기업과 정부 기관이 개인정보 처리에 있어 일련의 원칙을 준수하도록 규제한다. 국내에서는 정보통신망 이용촉진 및 정보보호 등에 관한 법률 등을 통해 개인정보 주체의 권리를 보장하고 기업이나 단체가 준수해야 할 의무를 명시하여 개인정보 처리에 대해 매우 엄격한 규칙을 준수하도록 하고 있다[2].

최근 블록체인은 불변성, 분산성, 투명성 등의 특징으로 인해 금융 및 보건, 정보 저장 등 다양한 분야에서 활용되며 개인정보 보호 분야에서 활용하는 연구가 진행되고 있다. 개인정보 보호에 블록체인을 활용하는 경우 데이터를 한 번 기록하면 변경이나 삭제가 불가해 데이터 무결성을 보장할 수 있으며 스마트 계약 기반의 데이터 접근 권한 관리를 자동화할 수 있다. 또한, 사용자의 디지털 신원 관리를 본인이 직접 제어할 수 있어 어떤 정보를 어떤 방식으로 공유할지 선택함으로써 프라이버시를 보장할 수 있다[3].

인터넷을 통해 인프라, 플랫폼, 소프트웨어를 제공하는 클라우드 서비스의 개념을 확장해 블록체인을 손쉽게 사용할 수 있도록 도와주는 BaaS(Blockchain as a Service)는 클라우드 상에서 운영되며 다양한 보안 위협에 노출되어 있다. 그중 하나가 네트워크를 통한 공격이나 부적절한 접근으로, 서비스 제공을 위해 사용하는 HTTP Endpoint나 API가 노출되는 경우, 접근 제어 절차 없이 노출된 API를 활용해 서비스에 접근하는 인증 우회 공격, 노출된 HTTP Endpoint를 이용해 서버에서 공격 코드를 실행하여 제어권을 탈취하는 원격 코드 실행 공격 등과 같은 비정상적인 행위로 인해 BaaS 환경에서 블록체인 데이터를 저장하는 데이터베이스에 저장된 정보가 노출될 수 있다. 이는 개인정보 침해와 블록체인 네트워크 생태계의 불안정을 일으킬 수 있으며, 정보를 조작하여 시스템의 무결성을 해칠 수 있다. 또한, 인증된 계정을 탈취하여 클라우드에 존재하는 기타 서비스 등을 불법적으로 사용할 수 있고, 블록체인의 신뢰성을 해칠 수 있다. 이를 예방하고 방어하기 위해 인증 절차의 강화 및 적절한 접근 제어가 수행되어야 한다[4].

본 논문에서는 BaaS 환경에서 개인정보 및 데이터 보호를 위해 IAM(Identity and Access Management) 서비스를 활용한 보안 기법을 제안한다. IAM 서비스가 생성한 역할 및 정책은 외부 접근을 차단하고 허용된 사용자만 접근할 수 있도록 통제하여 보안성을 강화한다. 시스템을 구성하고 있는 서버와 스토리지, 미들웨어는 IAM 서비스가 생성한 역할 및 정책에 의해 관리되며, 클라우드와 외부의 소통은 미들웨어가 중개한다.

본 논문의 구성은 다음과 같다. 2장 연구 배경에서는 BaaS와 IAM 서비스 및 개인정보 보호에 블록체인을 활용한 관련 연구를 소개한다. 3장 제안시스템에서는 본 논문에서 설계한 시스템과 구성요소를 자세히 서술한다. 4장 비교에서는 2장에서 소개한 관련 연구와 제안시스템을 몇 가지 기준에 따라 비교하고 분석하며, 5장 결론에서는 제안시스템의 기능을 환기하고 연구의 의의를 보인다.

II. 연구 배경

1. BaaS

BaaS는 서비스 사용자가 블록체인 개발 및 운영의 간편화를 위해 프로세스를 단순화하여 구축해 놓은 클라우드 서비스다. 블록체인 네트워크의 설치, 설정, 관리 등 복잡한 작업 없이 플랫폼이나 소프트웨어를 제공받아 사용하는 형태로, 연산 수에 해당하는 비용을 지불한다. BaaS를 사용하면 초기 인프라 구축 및 설정에 비용과 시간을 절약할 수 있으며, 클라우드 내 대시보드 형태로 제공되는 모니터링 시스템을 통해 유지보수 및 관리가 용이하다. 또한, IAM 서비스와 같은 보안 서비스를 이용해 네트워크 전체 보안을 강화할 수 있으며, 클라우드에 존재하는 방대한 자원을 활용하기에 블록체인 네트워크의 형태에 따라 규모 확장이나 네트워크 구조 변경 등이 간편하다. BaaS를 제공하는 기업은 해외의 경우 Microsoft, Amazon, IBM 등이 있으며 국내의 경우 SK, LG, KT, 두나무, 카카오 등이 있다. 주로 퍼블릭 네트워크로는 이더리움을 사용하고, 프라이빗 네트워크로는 하이퍼레저 패브릭을 사용하며, 기업에 따라 폴리곤, 멀티체인 등도 지원한다[5].

2. IAM 서비스

IAM 서비스는 클라우드 내 다양한 구성 요소들의 보안성을 강화하기 위한 서비스로, 구성요소 별 역할을 설정하고 접근 제어를 위한 정책을 수립한다. 주요한 기능으로는 사용자 계정 인증 관리, MFA(Multi-Factor Authentication), 접근 제어, 서비스 통합, SSO(Single-Sign-On), 인증서 관리 등이 있다. 사용자 계정 인증 관리는 클라우드 서비스를 사용하는 사용자의 신원을 확인하는 과정으로, MFA나 2FA(2-Factor Authentication)와 함께 진행된다. 접근 제어로는 인증된 사용자가 클라

우드 내 어떤 자원에 접근할 수 있는지 결정하는 내용으로, 역할 기반 접근 제어나 속성 기반 접근 제어 방식을 사용한다. 서비스 통합의 경우 클라우드에서 제공하는 다양한 서비스를 특정 콘솔에서 확인할 수 있도록 통합하고 관리할 수 있는 기능을 의미한다. ID Federation이라고도 불리는 SSO는 한 가지 서비스에서 사용자를 인증했을 때, 다른 서비스에도 같은 계정 정보를 연동하여 활용할 수 있도록 하는 기능을 의미한다. 인증서 관리는 X.509 인증서나 MFA에 사용하는 인자들, 키 쌍 등을 보관하고 관리한다. 이러한 다양한 기능들은 클라우드 내 데이터 보호와 법률 준수, 효율성 및 생산성 향상에 기여한다. 또한, 클라우드 서비스에 직접 적용할 수 있어 설정이나 유지보수 등이 간편하며, 관련된 모니터링 및 로그 서비스를 활용해 접근 제어 현황을 쉽게 파악할 수 있는 장점이 있다.

3. 블록체인을 활용한 개인정보 보호 관련 연구

연구[7]은 2020년 전자상거래 과정에 블록체인을 적용했을 때 공개될 수 있는 개인정보를 보호하고, 특정 당사자에게만 열람 권한을 부여하기 위해 AES(Advanced Encryption Standard) CBC(Cipher Block Chaining) 대칭 키 암호화 알고리즘을 활용한 멀티유저 암호키 방법을 제안했다. AES 암호화 알고리즘에 사용된 대칭키는 구매자 ID, 판매자 ID, 서버 ID로 구성된 멀티유저 암호키를 사용하며, 이런 방법을 적용했을 때 각 트랜잭션이 다른 대칭키가 사용되어 타인이 복호화할 수 없도록 한다.

연구[8]은 학생의 학업 및 학점 증명서의 내용을 외부로부터 보호하기 위해 다중 서명을 사용하는 블록체인 기반 아키텍처를 제안했다. 사용한 블록체인은 오픈소스이며 퍼블릭 블록체인인 Ark 네트워크를 사용했다. 하지만, 데이터나 사용자가 증가할수록 비용이 증가하며 확장성 문제가 발생할 수 있는 온 체인 저장소를 사용하면서 제안시스템의 구체적인 구현 내용이나 실험 결과가 존재하지 않는 문제점이 있다.

연구[9]는 의료 서비스 제공을 위해 환자의 의료정보를 전달하는 과정에서 정보를 외부 공격이나 개인정보 침해 위험으로부터 보호하기 위해 인공지능과 블록체인을 활용한 프레임워크를 제안했다. 블록체인 네트워크로 하이퍼레저 프로젝트의 소우투스 네트워크를 2개 활용했으며, REST API를 사용해 통신한다. 또한, 원활한 데이터 저장을 위해 오프 체인 저장소로 MySQL을 사용했으며, 환자 1000의 정보를 활용해 구성한 시스템의 구체적인 구현 내용은 서술했다. 하지만, 성능 측정 및 비교를 위한 실험을 진행하지 않아 아쉬운 점이 존재한다.

Ⅲ. 제안시스템

1. 사용자 인증 및 권한 확인

Case	Block Number for Request Data	User ID
Wallet Address	90	0x7C2BEBf17D0665aF7b4bE365eAFcFe3c92B1db4C
IP Address	34	192.168.xxx.xxx
E-Mail Address	61	rkdaudwh13@hknu.ac.kr
UUID	13	f47ac10b-58cc-4372-a592-0e02b2c7d419

UUID: Universally Unique Identifier

Fig. 1. Example of block number and user ID.
그림 1. 블록 번호와 유저 ID 예시

제안시스템은 클라우드에 대한 부적절한 접근을 차단하기 위해 API 미들웨어에서 사용자를 인증하고, 해당 사용자의 권한을 확인한다. 사용자는 API 미들웨어에 [블록 번호, 사용자 ID]의 형태로 정보를 전달한다. 그림 1은 사용자가 API 미들웨어에 전달하는 [블록 번호, 사용자 ID]의 형태의 예를 보인다. 예는 지갑 주소, IP 주소, 이메일 주소, UUID(Universally Unique Identifier)의 4가지 경우를 나타낸다.

사용자는 원하는 블록 순번과 자신을 식별할 수 있는 ID를 함께 전달하여 데이터를 요청한다. 사용자로부터 데이터 요청을 확인한 API 미들웨어는 사용자가 전달한 사용자 ID와 IP 정보 등을 통해 사용자를 인증하고, 해당 사용자의 권한을 확인하여 접근할 수 있는 데이터인 경우에만 API를 통해 클라우드에 데이터 요청을 전달한다.

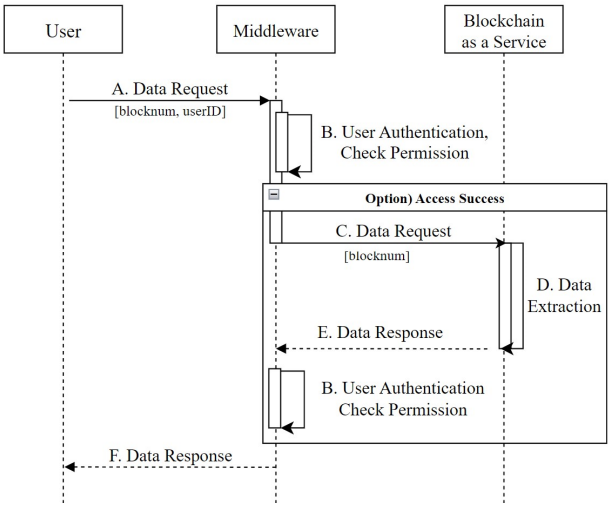


Fig. 2. Sequence diagram of data request process.
그림 2. 데이터 요청 과정 시퀀스 다이어그램

그림 2는 제안시스템의 데이터 요청 흐름을 나타낸다. 가장 먼저 사용자가 미들웨어에 원하는 데이터가 담긴 블록 번호와 유저 ID를 전달하며 데이터를 요청한다(그림 2. A. Data Request). 요청을 확인한 미들웨어는 사용자 정보를 기반으로 인증 절차 및 권한 확인 과정을 수행하고(그림 2. B. User Authentication, Check Permission), 문제가 없는 경우에 블록 번호에 해당하는 데이터를 요청한다(그림 2. C. Data Request). 만약 부적절한 접근인 경우, 해당 요청은 무시한다. 미들웨어로부터 데이터를 요청받은 BaaS 서버는 사용자가 넘겨준 BaaS 스토리지에서 블록 번호에 해당하는 데이터를 추출한 후(그림 2. D. Data Extraction) 미들웨어에 전달한다(그림 2. E. Data Response). 미들웨어는 잘못된 데이터 전달을 방지하기 위해 사용자를 다시 인증하고(그림 2. B. User Authentication, Check Permission) 데이터를 전달한다(그림 2. F. Data Response).

그림 3은 제안시스템의 구조도를 나타낸다. 시스템을 구성하는 엔티티에는 사용자, API 미들웨어, IAM 서비스, BaaS 서버, BaaS 스토리지가 존재한다. 사용자(그림 3. User)는 서비스 사용자를 의미하며 자신의 개인정보를 활용해 신원을 인증받고, 원하는 블록체인 데이터를 요청한다(그림 3. A. Request Blockchain Data). API 미들웨어(그림 3. API Middleware)는 사용자의 개인정보를 활용해 신원을 인증하고, 권한을 검사하여 사용자가 데이터를 요청할 수 있는지 확인한다(그림 3. B. Authentication User & Check Permission). 이후 사용자 인증 및 권한 확인에 문제가 없으면 사용자가 요청한 데이터가 담긴 블록 번호와 유저 ID를 활용한 API 요청을 통해 데이터에 접근한다(그림 3. C. Get /chaindata?block={blocknum}&id={userid}). 미들웨어는 IAM 서비스에서 생성한 역할 및 정책에 기반하여 클라우드와 외부를 연결하는 게이트 역할만 수행하며 클라우드를 향한 접근을 제어한다. 또한, 사용자 인증 및 권한 확인을 위해 블록체인 데이터에 접근할 수 있는 사용자 목록과 권한 내용을 별도 데이터베이스에서 관리한다. IAM 서비스(그림 3. IAM Services)는 클라우드 내 서비스에 적용될 역할 및 정책을 생성하고 이를 적용한다. 예를 들어 특정 IP 대역에서 오는 요청만 받도록 하는 정책, 내부 서비스와 외부 서비스 간 통신을 중개하도록 하는 역할 등을 설정한다. BaaS 서버(그림 3. BaaS Server)는 블록체인을 생성 및 운영하고, BaaS 스토리지에 데이터를 저장한다. IAM 서비스가 부여한 역할 및 정책에 따라 BaaS를 운영하며 통신을 관리한다. BaaS 스토리지(그림 3. BaaS Storage)는 블록체인에서 생성된 데이터를 저장하고, 저장 결과에 대한 상태 코드를 서버에게 전달한다. 또한, 데이터 요청이 들어왔을 경우 사용자가 요청한 블록 번호에 담겨있는 데이터를 추출하고(그림 3. D. Data Extraction) 미들웨어로 전달한다(그림 3. E. Response Blockchain Data). BaaS 스토리지로부터 데이터를 전달받은 미들웨어는 사용자 재인증 절차를 거친 뒤, 문제가 없는 경우 데이터를 전달한다(그림 3. F. Response Blockchain Data).

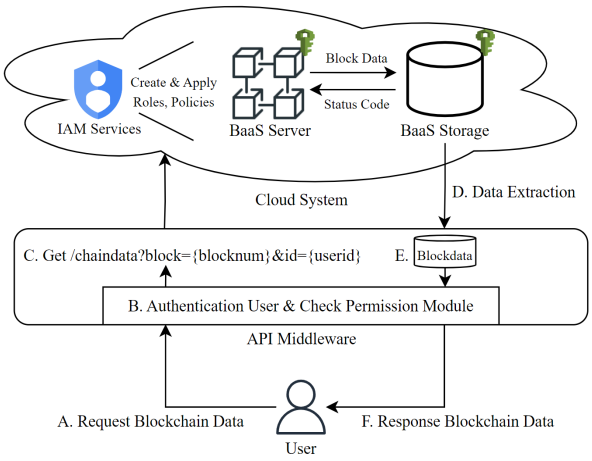


Fig. 3. Structure of proposed system.
그림 3. 제안시스템 구조도

2. IAM 역할 및 정책

IAM 역할은 서비스나 사용자, 어플리케이션 등이 안전하게 클라우드에 접근할 수 있도록 하는 개체다. IAM 정책은 JSON(Javascript Object Notation, JSON)의 형식의 문서로, 클라우드 내 자원에 대한 접근 권한을 부여하거나 거부하는 규칙을 정의하며 사용자나 그룹, 역할에 연결한다. 적절한 접근 제어를 수행하려면, 역할을 생성하고 정책을 연결하여 역할을 가진 개체가 정책에 정의된 권한을 가진다.

클라우드 내외부 통신 관리와 구성요소의 접근 제어를 위해 역할 및 정책을 생성하고, 이를 적용한다. 안전한 데이터 이동을 위해 외부와의 통신은 API 미들웨어만 수행할 수 있도록 하며, BaaS 서버나 BaaS 스토리지도 외부와의 통신을 차단하고 API 미들웨어하고만 통신하도록 정책을 설정한다. API 미들웨어는 통신 및 데이터 전달만 수행할 수 있도록 설정하여 권한을 제어한다.

표 1은 IAM 서비스를 활용하여 특정 IP주소로부터의 접근만 허용하고, 그 외의 모든 접근을 차단하는 정책을 나타낸다. 먼저 모든 접근을 거부하는 설정을 작성하고

Table 1. Example of IAM Policy.
표 1. IAM 정책 예시

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      A). "Effect": "Deny",
      "NotAction": "*",
      "Resource": "*",
      "Condition": {
        B) "NotIpAddress": {
          "aws:SourceIp": "IP Address"
        }
      }
    },
    {
      B). "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    }
  ]
}
```

(표 1. A), IAM 특성 중 Condition 요소를 사용하여 IP 주소에 해당하는 접근만 제외하도록 한다(표 2. B). 필요에 따라 클라우드에서 특정 작업을 의미하는 Action과 클라우드 자원을 나타내는 Resource를 조정하여 어떤 작업이 어떤 자원에 대해 허용되거나 거부될지를 정의할 수 있다. 제안시스템은 미들웨어와 BaaS 서버 통신 과정에 있어 IAM 서비스를 활용하여 외부 접근을 모두 거부하고, 두 서비스만 통신할 수 있도록 정책을 생성하여 적용한다. 이를 통해 HTTP Endpoint 및 API의 노출을 방지하고, 구체적인 접근 제어를 활용해 인증 우회 공격이나 코드 실행 공격을 예방한다.

3. BaaS 운영 및 데이터 저장

BaaS는 제공하는 서비스의 특성에 따라 공개적인 퍼블릭 블록체인, 비공개적인 프라이빗 블록체인, 공개/비공개 모두 수행할 수 있는 하이브리드 블록체인으로 운영할 수 있다. 운영 방식은 서비스의 주체가 설정할 수 있으며, 퍼블릭이나 하이브리드 블록체인과 같이 외부와의 통신이 필요한 경우 IAM 서비스의 정책을 수정하여 외부와의 접점을 만들어 사용할 수 있다. 클라우드 서비스로 제공하는 BaaS의 경우 실제 블록체인 연산이 수행되는 서버와 서버에서 발생하는 데이터를 저장하는 스토리지를 별개로 운영하기 때문에, BaaS 스토리지는 외부와의 통신을 수행하지 않는다.

Ⅳ. 실험 및 분석

1. 실험 계획 및 환경

본 논문에서는 제안 기법 적용 유무에 따른 시스템 성능 차이를 확인하고 실현 가능성을 보이기 위해, 구현된 시스템에서 사용자가 데이터를 요청하는 전체 프로세스 중 IAM 서비스 기반의 접근 제어와 사용자 인증 및 권한 확인 연산을 적용했을 때와 적용하지 않았을 때의 수행 시간을 측정하고, 동시 데이터 요청 수가 10개, 100개, 1,000개일 때의 데이터 응답 시간을 비교한다. 실험 결과는 네트워크 상태 및 지연 시간을 고려하기 위해 10회 측정하여 나온 결과의 평균값을 사용한다.

실험 환경은 클라우드 서비스를 제공하는 대표적인 기업인 Amazon의 AWS를 활용했으며, 미들웨어는 EC2를 활용해 구현했다. 클라우드에 존재하는 블록체인과의 통신은 미들웨어만 접근할 수 있도록 IAM을 정책을 설정했으며, 사용자 인증이 완료된 경우만 데이터를 요청할 수 있도록 한다.

2. 사용자 인증 및 권한 확인 과정 소요 시간 비교

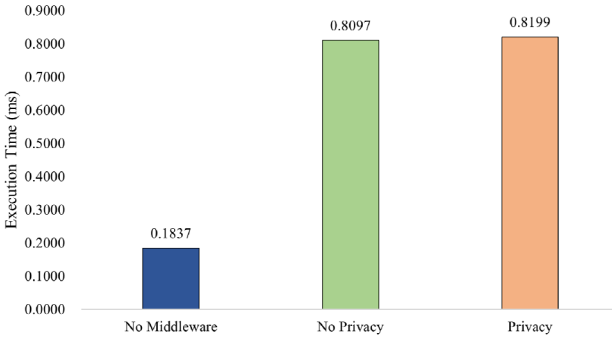


Fig. 4. Comparison of execution time on user authentication and authority check process.
그림 4. 사용자 인증 및 권한 확인 과정 소요 시간 비교

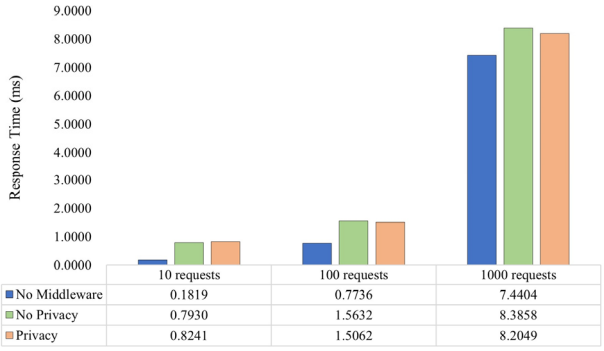
그림 4는 사용자를 인증하고, 권한을 확인하는 과정에서 소요된 시간을 나타낸다. X축에 존재하는 No Middleware, No Privacy, Privacy는 각각 미들웨어를 거치지 않고 바로 클라우드에 접근한 경우(그림 2. A-B-F), 미들웨어를 거치지만 사용자 인증 및 권한 확인 프로세스를 진행하지 않은 경우(그림 2. A-C-D-E-F), 미들웨어를 거쳐 사용자 인증 및 권한 확인 프로세스를 진행한 경우(그림 2. A-B-C-D-E-F)이다. 가장 빠른 속

도로 요청을 처리한 시나리오는 No Middleware이며, Privacy와 No Privacy의 경우 0.102ms 차이로 큰 차이가 존재하지 않음을 확인할 수 있으며, 실험 과정 중 두 시나리오의 속도 차이는 네트워크 상태 및 지연으로부터 도출됨을 확인했다.

3. 데이터 요청 수에 따른 소요 시간 비교

그림 5는 많은 사용자가 동시다발적으로 데이터를 요청하는 경우의 수행 시간 속도 차이를 나타낸다. 10개, 100개, 1,000개 요청 수의 시나리오에 대해 실험을 진행했으며, 네트워크 지연에 따른 영향을 최소화하기 위해 모든 실험은 10회 측정하여 평균값을 산출했다.

No Privacy와 Privacy의 경우 10개, 100개, 1,000개 부분에서 0.1~0.2 사이의 차이가 존재하지만, 비슷한 정도의 시간이 소요됨을 확인했다.



	10 requests	100 requests	1000 requests
No Middleware	0.1819	0.7736	7.4404
No Privacy	0.7930	1.5632	8.3858
Privacy	0.8241	1.5062	8.2049

Fig. 5. Comparison of response time based on number of data requests.

그림 5. 데이터 요청 수에 따른 응답 시간 비교

미들웨어를 거치지 않는 No Middleware의 경우 미들웨어를 거치는 두 시나리오와 비교해 10개 요청에서는 약 3.4배, 100개의 요청에서는 2.1배 빠른 짧은 응답속도를 보여줬지만, 1,000개의 요청에서는 약 11.5% 짧은 응답을 수행했다.

사용자 인증 및 권한 확인 과정 소요 시간 비교와 데이터 요청 수에 따른 소요 시간 비교 실험을 통해 클라우드에 접속하는 개인에 대한 사용자 인증 및 권한 확인 과정 도입은 시스템에 악영향을 주지 않을 것으로 판단할 수 있다.

4. 관련 연구 비교

본 장에서는 각각 다른 분야에서 개인정보 보호를 위해 블록체인을 활용한 관련 연구들과 제안시스템을 주요 아이디어, 블록체인 유형, 사용자 인증 여부, 기밀성, 확장성, 실험 여부, 클라우드 활용 가능성의 기준으로 비교한다. 관련 연구와 소요 시간이나 응답 시간과 같이 정량적 비교가 아닌 정성적 비교를 수행하는 이유로는, 각 시스템의 구성 방법에 따라 성능 차이가 크게 발생할 수 있으며, 각 연구 분야가 모두 다르기 때문이다. 표 2는 2장 관련 연구 부분에 작성한 개인정보 보호를 위한 논문과 제안시스템을 비교한다.

연구[7]은 블록체인 환경에서 AES 기반의 다중 사용자 암호화를 주요 주제로 하는 기법을 제안했으며, 블록체인 네트워크 유형이나 구현에 대한 설명이 존재하지 않았다. 외부로부터 사용자의 개인정보가 노출되지 않도록 AES 기반의 다중 사용자 암호키와 전자서명을 활용해 사용자 인증 및 기밀성을 만족한다. 하지만 블록체인의 유형이나 이름, 구현 방식 등이 서술되어 있지 않아 확장성과 관련된 부분은 판단하기 어렵다. 또한, 시스템의 성능을 나타내기 위해 대칭 키 암호화 알고리즘의 파일 크기별 암호화 및 복호화 처리시간 비교 실험을 진행했지만, 클라우드에서의 활용 가능성 등은 언급되지 않았다.

연구[8]은 학업 정보와 같은 학생의 민감 정보를 외부로부터 보호하기 위해 블록체인 기반의 다중 서명 아키텍처를 제안했다. 블록체인은 공개적으로 누구나 참여할 수 있는 Ark Blockchain을 활용했으며 전자서명을 통해 사용자를 인증할 수 있지만, 공개 블록체인을 사용하며 암호화 등의 작업을 수행하지 않아 기밀성을 유지하지 못하는 단점이 있다. 또한, 블록체인 자체에 데이터를 저장하는 온 체인 스토리지 기법을 사용하기 때문에, 블록체인 용량의 한계와 비용 문제로 인해 확장성을 만족하기 어렵다. 시스템 구현 내용 및 결과를 구체적으로 서술했지만, 연산에 걸리는 시간 등을 측정하는 실험을 진행하지 않았고, 클라우드에 대한 언급은 존재하지 않았다.

연구[9]는 환자의 의료정보를 공유하고 전달하는 과정에서 외부로 유출 및 침해 위협을 예방하기 위해 블록체인과 인공지능을 활용한 프레임워크를 제안했다. 비공개 블록체인 프로젝트인 하이퍼레저의 소우투스 네트워크를 활용하여 기밀성을 확보했고, 네트워크에 참여하기 위해 환자 본인 인증을 진행한다. 또한, 오프 체인 저장소를 활용해 데이터가 증가하더라도 처리할 수 있어 확장성을 만족했으며, 클라우드와 기존 시스템, 제안시스템의 통합을 향후 연구로서 서술했다. 시스템 구현에 대한 구체적인 내용을 서술했지만, 성능 측정을 위한 별도의 실험은 진행하지 않았다.

제안시스템은 클라우드 서비스 중 하나인 BaaS 환경에서 API 미들웨어와 IAM 서비스를 활용한 구조를 제안

Table 2. Comparison of proposed system with other works.
표 2. 제안시스템과 관련 연구 비교

	Main Idea	Network Type	Authenticity	Confidentiality	Scalability	Test of Execution Time	Cloud Operation
[7]	Multi-User Encryption in Blockchain	-	✓	✓	-	✓	X
[8]	Blockchain based Multi-Signature Architecture	Public	✓	✓	X	X	X
[9]	Integration AI and Blockchain for Privacy	Private	✓	✓	✓	X	✓
Proposed	API Middleware + IAM in BaaS	Hybrid	✓	✓	✓	✓	✓

✓ : provided
X : unprovided
- : unknown

했다. 제안 기법은 연구 [7, 8, 9]와 달리 BaaS 환경에서 운영되기 때문에 데이터 유통 및 저장에 공개/비공개, 하이브리드 블록체인을 상황에 맞게 구성할 수 있어, 정보 공개 범위의 조정이 자유로우며, API 미들웨어에서 사용자 인증 및 권한 확인 과정을 수행하고 정상 접근인 경우에만 미리 정의된 스마트 계약을 통해 블록체인 데이터에 접근할 수 있어 기밀성을 만족한다. 또한, 데이터 크기가 커질수록 시스템의 확장이 어려운 연구 [7, 8]과 다르게 블록체인에 저장할 데이터를 오프 체인 저장소나 클라우드 내 저장소를 활용하여 데이터 크기가 커지더라도 확장성을 확보할 수 있다. 끝으로 연구 [8, 9]에서는 수행하지 않았지만, 제안 기법으로부터 발생하는 추가 연산으로 인한 시스템 영향을 파악하기 위해 미들웨어를 사용하지 않은 경우, 프라이버시 기법을 적용하지 않은 경우, 모두 적용한 경우의 세 가지 시나리오에 대해 응답 시간 및 요청 수별 응답 시간 실험을 진행해 시스템 가용성을 해치지 않음을 확인했고, 이는 제안 기법의 실현 가능성을 나타낸다.

V. 결론

본 논문에서는 BaaS 환경에서 개인정보 보호 및 프라이버시 보장을 위해 블록체인에 접근하기 전 IAM 서비스 기반의 미들웨어를 통과하도록 설계한 시스템을 제안한다. 클라우드에서 운영되는 블록체인 또한 IAM 서비스의 역할 및 정책에 기반하여 미들웨어로부터 발생한 데이터 요청만 수용할 수 있으며, 미들웨어는 요청을 확인하고 사용자 인증, 권한 확인을 마친 후에 데이터를 요청할 수 있도록 한다. 개인정보 보호를 위해 미들웨어에서 사용자 인증 및 권한 확인 연산이 추가되었을 때, 그렇지 않은 경우와 비교하기 위해 설계한 시스템을 구현하여 실험을 진행했다. 실험 결과 사용자 인증 및 권한 확인 과정 연산이 큰 시간 지연을 발생하지 않는 것으로 나타났으며, 네트워크 상태에 따른 지연이 존재했다. 또한, 개인정보 보호에 블록체인을 활용한 관련 연구들과 제안 시스템을 특정 기준에 따라 비교, 분석하며 기존에 존재한 연구와 제안시스템의 차별점 및 장점을 나타낸다.

References

[1] B. S. R, A. Enes, L. Yang and L. Shujun, “A systematic literature review on the tension between the GDPR and public blockchain systems,” *Blockchain: Research and Applications*, vol.4, no.2, 2023. DOI: 10.1016/j.bcra.2023.100129

[2] J. H. Lee, J. W. Kim, C. S. Kim and J. H. Yang, “Research and Implementation of Mutual Trust System for Consent to User Personal Information Based on Blockchain,” *The Journal of Korean Institute of Communications and Information Sciences*, vol.45, no.8 pp.1342-1354, 2020. DOI: 10.7840/kics.2020.45.8.1342

[3] M. M. H. Onik, C. S. Kim, N. Y. Lee and J. H. Yang, “Privacy-aware blockchain for personal data

sharing and tracking," *Open Computer Science*, vol.9, no.1, pp.80-91, Apr. 2019.
DOI: 10.1515/comp-2019-0005
[4] H. K. Bella and S. Vasundra, "A study of Security Threats and Attacks in Cloud Computing," *2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 2022, pp.658-666. DOI: 10.1109/ICSSIT53264.2022.9716317
[5] M. J. Kang and M. H. Kim, "A study on non-fungible token platform for usability and privacy improvement," *KIPS Transactions on Computer and Communication Systems*, vol.11, no.11, pp.403-410, 2022. DOI: 10.3745/KTCCS.2022.11.11.403
[6] Amazon aws-documentation, "AWS Identity and Access Management," https://docs.aws.amazon.com/ko_kr/IAM/latest/UserGuide/introduction.html/
[7] H. B. Kang, H. C. Jang and C. S. Jang, "A Study on the Application Method of Multi-User Encryption Keys for Personal Information Protection in Blockchain," *Jounal of KIIT*, vol.18, no.1, pp. 135-141, Jan. 2020.
[8] A. Srivastava, P. Bhattacharya, A. Singh, A. Mathur, O. Prakash and R. Pradhan, "A Distributed Credit Transfer Educational Framework based on Blockchain," *2018 Second International Conference on Advances in Computing, Control and Communication Technology (IAC3T)*, 2018, pp.54-59. DOI: 10.1109/IAC3T.2018.8674023
[9] H. S. Jennath, S. Anoop and S. Asharaf, "Blockchain for Healthcare: Securing Patient Data and Enabling Trusted Artificial Intelligence", *International Journal of Interactive Multimedia and Artificial Intelligence*, In Press, Sep. 2020.
DOI: 10.9781/ijimai.2020.07.002,

BIOGRAPHY

Myung-Joe Kang (Member)

2022 : BS degree in Computer Science and Engineering, Hankyong National University
2022~present : MS student in School of Computer Engineering & Applied Mathematics, Hankyong National University

Mi-Hui Kim (Member)

1997 : BS degree in Computer Science and Engineering, Ewha Womans University.
1999 : MS degree in Computer Science and Engineering, Ewha Womans University.
1999~2003 : Researchers at Switching & Transmission Technology Lab.(ETRI)
2007 : Ph.D. degree in Computer Science and Engineering, Ewha Womans University
2009~2010 : postdoctoral researcher of the department of computer science, North Carolina State University
2011~present : School of Computer Engineering & Applied Mathematics, Hankyong National University