블록체인 기반 접근제어 기술 동향

Analysis of Blockchain-based Access Control Technology

김승현 (Seung-Hyun Kim, ayo@etri.re.kr) 신인증·물리보안연구실 선임연구원
김수형 (Soohyung Kim, lifewsky@etri.re.kr) 신인증·물리보안연구실 책임연구원

ABSTRACT

As companies use increasing amounts of data more and more, people are more concerned about protecting their privacy. Many researches studies have been conducted with a to securely view of manage managing and share sharing private information securely using the Bblockchain technology. These studies have suggested a Bblockchain-based approaches to provide efficiency, scalability, data ownership, and systematic data lifecycles that were are the limitations of lacking in traditional access controls. More Sspecifically, these studies have introduced a new access control models, distributed hash tables, trusted execution environments, and hierarchical ID-based cryptographic mechanisms to provide reliable access control even in complex environments such as IoT Internet of Things. In this paperstudy, we present the criteria to for classifying the functional characteristics of the Bblockchain-based access control methods and derive the differentiateion between of each the several methods.

KEYWORDS 블록체인, Blockchain, 접근제어, GDPR

Ⅰ. 서론

정보통신 기술의 급속한 발전으로 인해 도래한 데이터 중심 사회에서 사용자와 기업은 이전에 누리지 못했던 이점을 가지게 되었다. 사용자는 자신의 데이터와 활동 내역, 그리고 심지어 자신의 관심사항을 기업에 제공하여 무료에 가까운 비용으로 서비스를 제공받는다. 기업은 사용자의 데이터를 기반으로 맞춤화된 광고, 서비스를 제공하여 막대한 수익을 창출한다. 기업들이 보유하고 있는 데이터 용량은 2018년 9.7페타바이트(1페타바이트 = 1,000테라바이트)로, 2016년 평균 1.45페타바이트에 비해 7배나 증가하였다. 특히 업계의 리더들은 평균 21.4페타바이트의 데이터를 보유하여, 후발주자의 평균인 1.18페타바이트에 비해 18배나 많다[1].

* DOI: https://doi.org/10.22648/ETRI.2019.J.340412
* 이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No.2018-0-01369, O2O 서비스를 위한 무자각 증강인증 및 프라이버시가 보장되는 블록체인 ID 관리 기술 개발).

데이터 활용이 늘어남에 따라 개인정보 보호에 대한 관심도 증가하고 있다. IoT, AI 기술의 발전으로 인해 데이터의 축적 범위와 규모가 확장되고 더욱 정확하게 사용자를 분석할 수 있게 되었다. 그러나 사용자에 관한 더 많은 데이터가 수집, 공유 및 분석될수록 개인정보가 침해될지도 모른다는 우려가 커지고 있다. 실제로 기업들은 사용자가 의식하지 못한 상태에도 개인정보를 수집하고 제3자에게 공유한다. 사용자은 자신의 어떤 정보가 어떻게 활용되고 공유되는지 알 수 없고, 이로 인해 데이터 프라이버시가 침해될 수 있다. 일례로, 페이스북은 사용자에게 고지하지 않고 대규모의 인간대상 실험을 추진하였고[2], 타 업체에 사용자의 개인정보를 무단으로 제공하였다[3].

이러한 문제를 해결하기 위해, 기업이 보유한 데이터를 대상으로 개인정보를 보호하는 연구가 다수 수행되었다. 권한이 부여된 기업만 사용자 데이터에 접근할 수 있는 데이터 접근제어 기술[4], 개인 식별 정보를 데이터에서 제거하고 게시된 데이터와 개별 사용자 간의 연결 가능성을 방지하는 데이터 익명화 기술[5]이 대표적이다. 최근에는 의도된 목적을 달성하기 위해서만 데이터를 사용할 수 있게 하는 연구가 수행되었다[6]. 하지만 사용자가 동의하지 않은 목적으로 데이터를 사용하는 경우, 현재는 법적 조치가 취해질 수 있지만 기술적 접근법은 부족한 실정이다.

최근에는 블록체인(Blockchain)이라고 하는 공개적으로 검증 가능한 공개 원장을 사용하여, 사용자가 중앙 권한을 필요로 하지 않고 암호화된 데이터(예, 비트코인에서의 거래내역)를 안전하게 전송할 수 있게 해 주는 시스템이 등장했다. 블록체인은 시간순으로 연결된 블록을 기록하고 저장하는 공개 원장으로, 암호화, 디지털 서명 및 P2P 네크워킹 기술에 기반을 둔다[7]. 블록체인 기술은 변조 방지라는 속성으로 인해 데이터 회계 및 감사 기능에 널리 채택되고 있다.

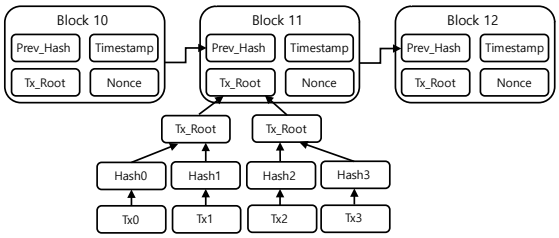
블록체인의 특성을 활용하여 개인정보를 안전하게 관리하고 공유하는 연구가 다수 진행되고 있다. 이들 연구는 전통적인 접근제어 방식의 문제였던 효율성, 확장성, 데이터 소유권 및 체계적인 데이터 수명주기 접근을 블록체인으로 해소하는 방안을 제시한다. 새로운 접근제어 모델, 분산된 해시 테이블, 신뢰할 수 있는 실행 환경, 계층적 ID 기반의 암호화 메커니즘 등을 도입하여 IoT 환경과 같은 복잡한 조건에서도 신뢰된 접근제어를 제공한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서 블록체인과 접근제어 기술, 데이터 보호규정(GDPR: General Data Protection Regulation)과 데이터 프라이버시 서비스에 대한 배경설명을 한다. Ⅲ장에서는 블록체인 기반의 개인정보 접근제어 기술을 간략히 살펴본다. 그리고 Ⅳ장에서는 블록체인 접근제어 기술의 기능 특성 별로 분류하기 위한 기준을 정의한다. 마지막으로 Ⅴ장에서 결론 및 향후 연구를 제시한다.

Ⅱ. 기반 기술

1. 블록체인

블록체인 데이터베이스는 레코드를 블록으로 유지·관리하는 공유된 분산 데이터베이스이다. 블록은 모든 블록체인 사용자가 접근할 수 있지만 삭제하거나 변경할 수는 없고 추가만 가능하다. 각 블록은 이전 블록의 해시 값을 가지므로 블록은 체인으로 서로 연결된다. 각 블록은 여러 개의 검증된 트랜잭션, 해당 블록의 생성 시간을 나타내는 타임 스탬프, 암호화 작업을 위한 난수(Nonce)를 포함한다. 블록체인 네트워크는 P2P 방식으로



출처 Reprinted from Matthäus Wander [CC BY-SA 3.0 (https://creativecommons.org/licenses/by-sa/3.0)].

그림 1 **블록체인 시스템**

블록체인을 유지·관리하는 노드로 구성된다. 모든 노드는 블록에 접근할 수 있지만 완전히 제어할 수는 없다.

블록체인 기술을 통해, 사용자들은 신뢰할 수 있는 제3자가 없어도 상호작용할 수 있다. 사용자가 원하는 수준의 보안 요구 사항을 제공하는 블록체인 데이터베이스에 사용자들 간의 상호작용 이력이 기록된다. 구체적으로, 블록체인 사용자가 다른 사용자와 상호작용해야 할 때 블록체인 네트워크에 트랜잭션을 브로드캐스트한다. 블록체인 네트워크의 여러 노드는 트랜잭션이 유효한지 확인하고, 유효한 트랜잭션을 결합하는 마이닝 과정을 거치면서 트랜잭션 블록을 생성한다. 새 블록이 유효하면 블록체인 데이터베이스에 연결되며 나중에 삭제하거나 변경할 수 없다. 만약 새 블록이 유효하지 않으면 블록이 삭제된다. 트랜잭션과 블록 모두 서명되기 때문에 되돌리거나 부정될 수 없다. 그림 1은 블록체인의 각 구성 요소를 보인다.

블록체인 기술은 적용 범위에 따라 자금 거래, 자산, 스마트 컨트랙트를 각각 지원하는 3가지 세대로 구분될 수 있다[8]. 블록체인 1세대는 2009년 사토시 나카모토에 의해 등장한 비트코인이 대표적이다[9]. 1세대의 애플리케이션은 자금 거래에만 국한되어 가상화폐로 구현되었으며, 블록체인 개념을 처음으로 사용했다. 블록체인 2세대는 화폐가 아니라 자산을 교환하는 광범위한 사용 사례를 가진다. 2세대에서 사용자는 주식 또는 자산을 소유하며, 상품, 부동산 및 심지어 투표를 포함한 다양한 유형의 자산을 교환할 수 있다. 블록체인 3세대에서는 스마트 컨트랙트가 도입되었다. 스마트 컨트랙트(Smart contract)는 블록체인 네트워크의 모든 사람이 확인할 수 있는 프로그래밍 가능한 계약으로, 두 통신 당사자가 계약을 엄격히 준수하도록 동작한다. 블록체인의 기능은 3세대에서 크게 향상되어 세계적인 인기를 얻었고, 몇 가지 다른 중요한 서비스에 대한 응용 분야에 대한 관심이 증가했다.

블록체인은 활용 목적과 데이터 관리 방식, 참여자의 범위에 따라 퍼블릭(public) 블록체인, 프라이빗(private) 블록체인, 컨소시엄(consortium) 블록체인으로 구분할 수 있다. 퍼블릭 블록체인은 누구나 접근 가능한 개방형 블록체인으로 채굴 등 알고리즘을 통해 거래를 증명하여 거래 신뢰도를 높이고 익명성을 보장한다는 장점이 있어 비트코인 등 암호화폐 시장의 기반 플랫폼으로 활용되고 있다. 하지만 익명화된 상태에서 거래를 증명하는 알고리즘이 많은 계산량을 요구하기 때문에 거래시간이 느리다. 프라이빗 블록체인은 승인된 사용자만 접근이 가능하도록 협의하여 통제하는 형태로 기업들의 요구에 맞게 적용 가능한 기업형 블록체인이라고 할 수 있다. 중앙 기관에서 트랜잭션을 증명하기 때문에 빠르고 효율적인 거래처리가 가능하다. 하지만 중앙기관에 의존하기 때문에 퍼블릭 블록체인보다는 덜 안전하다. 컨소시엄 블록체인은 프라이빗 블록체인처럼 승인된 사용자만 접근 가능하지만, 조직 간의 협조적인 참여를 허용하는 특징이 있다. 사전 합의된 규칙으로 빠르게 거래를 증명하며 사용자 권한을 관리하여 민감한 정보를 제어할 수 있는 장점이 있다. 초기에는 확장성

이 낮다는 문제가 보고되었으나[10], 최근에는 문제를 해결하여 대규모 서비스에 적용되고 있다.

2. 접근제어

컴퓨터 보안에서, 접근제어란 시스템이 인증된 주체(subject)의 객체(object)에 대한 접근 요청을 승인 또는 거절하는 절차를 의미한다. 시스템은 사용자에게 주어진 접근 권한에 따라 접근제어를 수행한다. 기존의 접근제어 기술은 다음과 같이 분류할 수 있다.

- 강제적 접근제어(Mandatory access control): 객체와 주체에게 주어진 권한에 따라 접근을 제어하는 방법이다. 시스템 관리자는 객체에게 서비스나 정보의 민감도에 따라 보안 수준을 할당하고, 각 주체에게 권한을 부여한다. 주체가 객체에 접근할 때, 객체의 보안수준과 주체에게 주어진 권한을 비교하여 접근 여부를 결정한다. 객체와 주체를 모두 관리하는 시스템 관리자만이 객체의 보안레벨 또는 사용자 보안등급을 수정할 수 있기 때문에 엄격한 접근제어가 가능하지만 유연성은 떨어진다.
- 임의적 접근제어(Discretionary access control): 주체 또는 주체의 그룹이 자신들이 소유한 객체에 대해 임의로 접근 권한을 설정하는 방법이다. 다른 주체나 그룹에게 자유롭게 접근 권한을 부여할 수 있으며, 주체의 판단에 의해 설정되기 때문에 유연한 접근제어가 가능하다. 접근 권한을 가지고 있는 주체는 임의의 다른 주체에게 자신의 권한을 위임할 수 있다. 하지만 주체의 실수로 인해 의도하지 않은 접근을 허용하거나 거부하여 문제가 발생할 수 있다.
- 역할 기반 접근제어(Role based access control): 주체와 객체 간의 접근제어가 아니라 주체의 역할과 객체들의 관계를 설정하여, 주체의 역할에 따라 객체의 접근을 제어하는 방법이다. 조직 내의 몇 가지 역할로 주체를 구분할 수 있는 대규모 시스템에서 접근제어를 관리하는 데 효율적이다.
- 속성기반 접근제어(Attribute based access control): 주체의 권한이 아닌 속성에 따라 접근제어를 수행하는 방법이다. 각 개체별로 접근 가능한 주체의 특정 속성에 대한 실제 값 또는 정보를 명시하고, 이 정보와 객체에 접근하는 주체의 속성값을 비교하여 접근 여부를 결정한다. 접근 권한이 필요한 주체의 속성을 추가함으로써 쉽게 접근제어 정책을 생성할 수 있다. 수행 속도 관점에서는 효율적이나 저장 공간 관점에서는 비효율적이기 때문에 속성의 복잡성을 효과적으로 줄이려는 연구 개발이 활발히 이루어지고 있다.
- 자격기반 접근제어(Capability based access control): 최소 권한 원칙과 권한 위임 기능을 주체에게 부여하여, 주체가 자신의 서비스 및 정보에 대한 접근제어를 관리하는 방법이다. 자격기반 접근제어는 최소한의 권한만을 체크하여 객체의 접근제어를 허가함으로써 접근제어의 복잡성을 줄인다. 또한 다른 주체에게 권한을 조절할 수 있는 역할을 부여하여 IoT 환경과 같은 다수의 디바이스 관리 어려움을 줄였다.
- 상황인식 기반 접근제어(Context-aware access control): 상황을 표현하는 규칙에 따라서 접근제어를 수행하는 방법이다. 주체의 주변 환경에서 발생하는 데이터를 분석하여 해당 상황을 식별한 뒤, 기존 규칙을 적용하여 객

체의 접근 여부를 결정한다. 상황인식 기반 접근제어는 즉각적이며 시시각각 변화하는 상황에 맞는 서비스 제공 시스템에 매우 효과적이다[11]. 주변의 많은 디바이스에 존재하는 센서들을 이용하여 자연스럽고 즉각적인 상황의 값을 활용한 접근제어가 가능하다. 또한 누적인 메타 데이터를 이용하여 기존의 규칙을 갱신할 수 있다.[11].

접근제어 정책은 환경의 특성에 따라 다른 방식을 고려할 수 있다. 예를 들어 IoT 환경에서 접근제어는 기존 인터넷 환경과 다르게 짧은 시간 동안 상호작용이 일어나고, 동일한 요청이 빈번하게 수행될 수 있다. 또한 매번 같은 요청에 대해서도 접근제어 결과는 고정적이지 않고 주변의 상황에 따라서 바뀔 수 있으며, 확장성 문제나 권한 위임과 같은 요구사항이 발생할 수 있다. 접근제어 기법은 새로운 요구사항을 반영하기 위한 연구가 활발히 진행되고 있으며, 주어진 환경의 문제를 고려하여 적절한 접근제어 기법을 선택하고 개선하는 작업이 필요하다[12].

3. GDPR과 데이터 프라이버시 서비스

2016년 EU는 기업에 대한 새로운 의무를 강요하는 일반 데이터 보호 규정(GDPR: General Data Protection Regulation)을 채택하여 개인정보 보호를 강화했다. 이 규정에 따르면 조직에 대한 책임 및 책임 요구 사항을 확대하고, 데이터 소유자의 동의가 필요한 경우 등 몇 가지 핵심 의무가 고려되어야 한다. GDPR과 같은 규정을 기술적으로 준수하기 위해서는 다음의 요소를 제공할 수 있어야 한다.

- 사용자 데이터에 대한 기밀 보호: 사용자에 의해 생성된 데이터는 기업의 클라우드 저장소에 저장된다. 민감한 개인정보는 적절한 수준의 보호가 필요하며, 기업에게도 노출되어서는 안 된다. 따라서 기업이 주관하는 암호화/복호화보다는 사용자가 직접 데이터 제어에 관여할 수 있어야 한다.
- 검증 가능하고 사용자가 주도하는 세밀한 접근제어: 데이터가 기업의 클라우드로 업로드되면 서비스 계약에 따라 기업의 소유물에 속하게 된다. 사용자는 자신의 데이터에 대한 접근 권한을 다른 사용자에게 부여할 수 있지만, 자신의 개인정보에 실제로 접근한 사람을 알아낼 수 있는 방법은 없으며 어떤 목적을 위해서 접근한 것인지도 모른다. 따라서 사용자의 개인정보를 보호할 뿐만 아니라 커뮤니티에서 데이터 공유를 촉진하기 위해서는, 사용자 데이터 사용 내역을 추적하고 사용자가 확인 가능할 수 있어야 한다.
- 사용자 데이터 사용에 대한 법적 근거: 현재 상황에서 사용자 데이터의 수집, 저장, 공유를 통제하는 유일한 방안은, 서비스 수준 계약 및 법적 계약이다. 기업은 수집된 데이터를 기반으로 양질의 서비스를 제공하지만, 이를 오용하여 사용자에게 불이익이 발생할 수 있다. 따라서 사용자 개인 데이터 사용에 대해 유연하게 대응할 수 있으면서, 입증 가능한 법적 구속력과 연결할 수 있는 기능이 필요하다.

여러 연구가 존재하지만, 효율적인 데이터 프라이버시 서비스를 제공하는 것은 여전히 어려운 과제다. 특히, 효율성, 확장성, 데이터 소유권 및 체계적인 데이터 수명주기 접근 방법이 부족하다[13].

- 효율성 및 확장성: 대부분의 데이터 프라이버시 기술은 복잡한 암호화 알고리즘에 의존한다. 따라서 대규모 응용 프로그램에 적용하기에는 비효율적이고 확장하기 어렵다. 최근의 연구는 암호화 기법의 복잡성을 줄이고 효율성을 향상시키는 방안을 시도한다. 그러나 제안된 접근법의 대부분은 실용성이 부족하고, 방대한 양의 데이터 처리가 어렵다.
- 데이터 소유권 및 통제: 일반적으로 데이터 소유자는 데이터를 저장하고, 이에 대한 접근제어 규칙을 결정하는 당사자이다. 하지만 기존의 중앙집중화된 시스템이 아닌 경우, 데이터의 저장 위치와 제어 주체는 다양하게 정의될 수 있다. 이 경우에 발생하는 소유권 문제를 전통적인 접근제어 기술로는 명확하게 해소하지 못한다.
- 체계적인 데이터 수명주기 접근법: 데이터의 라이프사이클을 체계적으로 정의하기 위해 데이터 프라이버시를 위한 프레임워크를 구축해야 한다. 이 프레임워크는 각 개인정보 관리 단계를 식별하고 개인정보 보호 요구 사항을 정의하며 라이프사이클 변경을 유연하게 허용할 수 있어야 한다. 개인정보 관리 단계에는 데이터 및 자원의 획득, 공유 및 삭제가 포함될 수 있다. 그러나 지금까지 제안된 프라이버시 기술의 대부분에서는 체계적인 접근법이 빠져 있다.

III. 블록체인 기반 접근제어 기술 동향

블록체인 기술은 앞서 설명한 기존 접근제어 문제를 해결할 수 있는 방안을 제시한다. 특히 데이터 소유권 솔루션을 제공하고, 필요할 때 동적으로 접근권한을 변경할 수 있다[14].

- 효율성: 블록체인에 최적화된 접근제어 솔루션은 없다. 기존 암호화 기법이 사용되고 있어서 효율성 문제가 여전히 존재한다.
- 확장성: 일반적으로 블록체인의 확장성이 기존 방안보다 더 좋으나 완벽히 해결되지는 않았다.
- 데이터 소유권과 제어: 블록체인은 데이터 소유권과 데이터 변경 내역을 기록함으로써 문제를 해결한다. 사용자는 ACL(Access Control List) 정의를 완벽히 제어할 수 있다.
- 체계적인 라이프사이클: 블록체인 사용자는 자신의 스마트 컨트랙트를 쉽게 만들고 업데이트하기 때문에 변화에 유연하다. 프로그래밍 가능한 ACL을 블록체인상에서 작성하여, 라이프사이클을 체계적으로 구성할 수 있다.

이상적인 블록체인 기반 데이터 프라이버시의 기본 개념은 데이터 저장소 계층 위에 블록체인 계층을 구축하는 것이다. 소유자는 스마트 컨트랙트를 통해 원하는 ACL을 정의하고, ACL 및 데이터를 암호화한 뒤에 블록체인 트랜잭션에 게시한다. 기존 방식과 달리, 조직은 데이터를 직접 소유하지 않는다. 대신 이들은 블록체인 네트워크의 일부가 되며 ACL이 허용하는 경우에만 데이터를 처리할 수 있다. 데이터 접근을 정의하는 정책은 스마트 컨트랙트 또는 데이터 관리 메시지를 기반으로 한다. 또한 블록체인 메모리가 제한되어 대량의 데이터를 저장할 수 없기 때문에 오프체인 데이터베이스를 사용하여 암호화된 데이터를 저장할 수 있다.

다음에서는 프라이버시 서비스를 제공하기 위해 블록체인 기술을 이용하는 몇 가지 최신 연구들을 분석한다.

1. FairAccess

IoT 분야는 제한된 환경에 대한 보안 및 접근 제어 메커니즘의 적용과 관련하여 여전히 어려운 문제에 직면하고 있다. FairAccess는 IoT 보안 및 개인정보 보호 요구 사항을 충족하는 블록체인 기반의 분산된 접근제어 프레임워크이다[15]. 사용자가 네트워크 또는 클라우드에서 공유한 데이터에 대해 완전하고 세밀한 접근제어 권한을 가진다.

FairAccess 프레임워크는 IoT의 접근제어 정책을 관리하기 위한 중앙 집중식 및 분산된 방식을 제안한다. 이 방식은 OrBAC(Organization Based Access Control)이라고 불리며, 기존 RBAC를 확장하여 조직이라는 개념을 제시하고 추상적/구체적인 수준으로 접근제어 정책을 나누어 접근한다. 첫째, 추상적 수준의 분산된 접근 방식은 협력 조직 간의 상호작용에 관한 것으로, 각 조직이 자체 보안 정책을 정의하고 구현할 책임이 있는 P2P 방식(완전히 분산된 방식)을 선택한다. 둘째, 구체적 수준에서는 IoT 환경의 제한적인 리소스 성능을 감안하여, AMP(Authorization Manager Point)라는 중앙 객체가 정의하는 중앙 집중식 접근 방식을 선택한다. 이 AMP는 자원에 대한 인증 및 권한 부여 데이터를 관리하고 승인한다.

FairAccess 아키텍처에 따르면, FairAccess의 모든 사용자는 자신의 자격 증명, 주소 및 관련 트랜잭션을 저장하는 지갑을 가진다. 이 지갑에는 자원을 등록하고 식별하고, 거래를 서명하고, 접근을 요청하는 데 필요한 모든 키가 들어 있다. FairAccess 프레임워크에서 지갑은 AMP로 간주된다. 사용자는 개인정보를 등록하거나 접근제어 정책을 정의할 수 있다. 지갑은 키와 주소를 생성하고, 접근제어 정책을 트랜잭션으로 변환하고 네트워크로 브로드캐스트한 뒤, 네트워크로부터 수신된 트랜잭션의 유효성을 검사한다.

개념 증명 차원에서 FairAccess는 라즈베이파이 장치와 로컬 블록체인을 사용하여 초기 구현 및 실행을 검증했다. 프레임워크의 유용성을 입증하고 사용자 경험을 설명하기 위해, 원격 제어 기능이 있는 스마트 보안 카메라 시나리오를 고려했다. 그러나 FairAccess는 실시간 서비스(1시간 이상 대기 시간 초래), 확장성(비금융 데이터를 블록체인에 저장하는 것에 대한 비트코인 커뮤니티 내부 논쟁), 세밀한 접근제어(스크립트 언어 사용 안 됨)가 어려운 단점이 도출되었다.

2. Zyskind의 제안 기법

Zyskind는 사용자가 자신의 데이터를 제어하고 블록체인 블록을 사용하여 데이터와 ACL을 저장하는 분산형 데이터 프라이버시 접근법을 제안했다[6]. 제안 시스템은 사용자, 공급자 및 블록체인 네트워크의 세 가지 주요 구성 요소로 이루어진다. 사용자는 응용 프로그램을 다운로드하거나 서비스를 사용하는 노드이다. 공급자는 서비스나 응용 프로그램을 보유한 제공 업체로, 운영 및 비즈니스 목적으로 사용자의 개인 데이터를 처리한다. 블록체인 노드는 블록체인 네트워크를 구성하고 오프체인 데이터 저장소가 있는 신뢰할 수 없는 객체이다. 데이터는 개인정보 보호 및 고가용성 서비스를 보장하기 위해 분산 데이터 저장소에 암호화된 상태로 복제된다.

블록체인 네트워크는 Taccess와 Tdata의 두 가지 유형의 트랜잭션을 수용한다. Taccess는 ACL 정의 및 접근권한 수정과 같이 데이터에 대한 제어 및 관리 작업에 사용된다. Tdata는 데이터 저장 및 검

색에 사용된다.

소유자는 Taccess 트랜잭션에서 정책 집합을 전송하여 허용 및 접근제어를 변경할 수 있다. 이 정책 집합을 통해 블록체인 노드의 정확성을 검사할 수 있다. 마찬가지로 사용자 또는 서비스 공급자는 앞서 지정한 정책이 충족될 경우, 블록체인 노드가 승인할 Tdata 트랜잭션을 전송하여 데이터에 접근할 수 있다. 반환된 응답(접근 정보 또는 거부 메시지)은 암호화되기 때문에 권한이 없는 사용자는 데이터에 접근할 수 없다.

오프 블록체인 키 값 저장소는 분산된 해시테이블(DHT: Distributed Hash Tables)의 하나인 Kademilia로 구현하고, LevelDB2라는 경량 데이터베이스를 사용하여 지속성 있는 블록체인 인터페이스를 제공한다. DHT는 승인된 읽기/쓰기 트랜잭션을 수행하는 노드 네트워크(블록체인 네트워크와 분리되어있을 수 있음)에 의해 유지·관리된다. 데이터는 노드 전체에서 충분히 무작위화 되고 고가용성을 보장하기 위해 복제된다.

Zyskind의 제안 기법에 따르면 사용자만 데이터를 제어할 수 있다. 공용 장부에는 해시 포인터만 저장되므로 공격자는 아무 것도 얻을 수 없다. 노드가 가지고 있지 않은 키로 암호화되기 때문에, 하나 이상의 DHT 노드를 제어하는 공격자들은 사용자 데이터에 대해 아무것도 얻을 수 없다. 마지막으로 각 사용자–서비스 쌍에 대해 새로운 복합 신원을 생성하면, 공격자가 서명자와 암호화 키를 모두 얻더라도 데이터의 일부분만 손상시킬 수 있다. 공격자가 키 중 하나만 얻을 경우, 데이터는 여전히 안전하다.

Zyskind의 접근법은 이론적으로 검증되었다. 그러나 제안된 접근법의 오픈 소스 구현은 아직 완료되지 못했으므로, 실용성과 적합성을 검증할 필요가 있다.

3. PrivacyGuard

IoT 생태계에서 서비스 제공 업체는 수집된 사용자 데이터를 완벽하게 제어하지만, 데이터는 종종 사용자가 명시적으로 동의하지 않은 다른 목적으로 사용된다. 사용자가 본인의 개인정보를 완벽하게 제어할 수 있도록, PrivacyGuard 프레임워크는 블록체인과 신뢰할 수 있는 실행 환경(TEE: Trusted Execution Environmnet)을 결합했다[16]. PrivacyGuard는 데이터 접근 정책 및 사용을 스마트 컨트랙트로 인코딩함으로써, 데이터 소유자가 자신의 데이터에 접근할 수 있는 사람을 제어할 수 있다. 또한 데이터 사용에 대한 신뢰할 수 있는 기록을 유지할 수 있다. 원격 인증 및 TEE를 통해, 개인 데이터는 데이터 소유자가 승인한 용도로만 사용된다.

PrivacyGuard이 적용된 IoT 시스템은 제공하는 기술 지원을 기준으로 4개의 계층으로 나눌 수 있다. 가장 낮은 계층은 디바이스 계층으로, 물리적 세계에 대한 IoT 시스템의 인터페이스가 되며, 물리적 환경과 상호작용하여 실시간 정보를 수집하고 처리한다. 두 번째 계층은 다양한 무선 접근 기술의 상호 연결성을 제공하고 라우팅 기능을 지원하는 네트워크 계층이다. 가장 높은 계층은 백엔드 서비스/응용 프로그램이 상주하는 클라우드 계층으로, 집중된 데이터를 분석한다.

클라우드 계층과 네트워크 계층 사이를 서비스 지원 계층이라고 부른다. 이 계층은 더 많은 계산 및 저장 기능을 갖추고 있으며, 데이터 분석을 통해 가능한 정보 처리 작업을 수행할 수 있다. 보안 및 개인정보 보호 측면에서 보안 제어 및 장치 관리, 프로세스 모델링 및 데이터 흐름 필터링과 같은 정보 흐름 제어는 이 계층에서 모두 처리될 수 있다.

PrivacyGuard 아키텍처에는 세 가지 주요 구성

요소가 존재한다.

- 블록체인: 외부 블록체인(예, Ethereum)을 사용하여 접근 정책 게시 및 데이터 사용 기록을 작성한다. 데이터 접근제어의 경우 데이터 소유자는 자신의 접근제어 약관을 스마트 컨트랙트로 인코딩할 수 있다.
- iDataAgent: 신뢰할 수 있는 객체이며 TEE에서 실행되는 프로그램의 인스턴스이다. 사용자 데이터의 브로커 역할을 하며, 사용자 데이터 저장소에서 들어오고 나가는 모든 데이터는 iDataAgent를 통과한다. iDataAgent는 데이터 소유자의 키와 해당 사용자의 데이터 암호화/복호화를 관리한다.
- 암호화된 저장소: 사용자 데이터는 클라우드에 있을 때 항상 암호화되어, 클라우드 서비스 제공 업체에 대한 데이터 기밀 유지가 보장된다.

PrivacyGuard에서 사용자의 개인정보 보호 정책은 블록체인 플랫폼의 스마트 컨트랙트로 인코딩된다. PrivacyGuard에서 스마트 컨트랙트는 프로토콜 수준에서 원하는 개인정보 보호를 보장하는 메커니즘을 제공하기 때문에, 개인정보 사용 거래를 촉진하고 접근제어 및 변조 방지 기록을 남기는 데 사용될 수 있다. 그러나 프로그램이 데이터 소유자가 완전히 신뢰할 수 없는 제3자 컴퓨터(예, 클라우드)에서 실행된다면, 사용자 데이터의 기밀성은 더 이상 보장될 수 없다. 하드웨어로 구현된 보안 실행영역 내에서 데이터를 처리함으로써 데이터 기밀성을 보장하고 데이터 사용을 제어할 수 있다.

4. Kaaniche의 제안 기법

대량으로 사용자의 데이터를 수집, 처리 및 관리하는 제3자가 사용자의 개인정보를 침해하는 문제를 해결하기 위해, Kaaniche는 계층적 ID 기반의 암호화 메커니즘을 블록체인 인프라와 결합한 블록체인 기반의 데이터 사용 감사 아키텍처를 제안했다[17]. 개인정보를 보존하는 방식으로 가용성과 책임성을 보장하는데, 이 접근 방식은 블록체인 인프라에 구축된 감사 가능한 계약의 사용에 의존한다. 따라서 투명하고 제어된 개인정보 접근, 공유 및 처리 기능을 제공하므로, 권한이 없는 사용자 또는 신뢰할 수 없는 서버는 클라이언트의 승인 없이 데이터를 처리할 수 없다. 이 솔루션은 암호화 메커니즘을 기반으로 데이터 소유자의 프라이버시를 보호하고, 여러 서비스 제공 업체와 공유되는 데이터의 기밀 유지를 보장한다. 또한, 감사 기관에 데이터 사용 적합성에 대한 변조되지 않은 증거자료를 제공한다.

신뢰할 수 있는 루트 PKG(Public Key Generator, 공개키 생성기) 객체는 ID 기반 서명 및 암호화 체계로 ID 기반 공용 요소(공개키와 개인키)를 생성하고 게시한다. 이를 활용하여 스마트 컨트랙트용 ID 및 해당 공개키와 개인키 쌍을 계층적으로 파생시킬 수 있다. 데이터 사용 요청을 승인한 사용자는 스마트 컨트랙트의 데이터 섹션을 작성한다. 개인정보를 게시하는 것을 피하기 위해 공개 해시 기능을 사용하여 데이터 값을 난독화한다. 프라이버시를 강화하고 연결 가능성 공격을 방지하기 위해, 데이터 값은 해시 함수를 적용하기 전에 스마트 컨트랙트의 개인키와 연결된다. 그런 다음 사용자는 스마트 컨트랙트 생성 트랜잭션을 수행하고, 생성된 스마트 컨트랙트를 블록체인에 등록한다.

스마트 컨트랙트 생성 요청 통지를 수신한 뒤, 서비스 제공자는 자신의 개인키에서 파생된 암호화된 개인키의 복호화를 시작한다. 그다음 공개키를 사용하여 해당 데이터 소유자 서명을 확인한다.

두 작업이 모두 성공하면 서비스 제공자는 개인키로 스마트 컨트랙트 생성과 관련된 트랜잭션을 승인한다. 승인 후에 사용자는 스마트 컨트랙트에 명시된 해시 값과 매치되는 자신의 개인 데이터를 보안 채널을 통해 서비스 제공자로 전송하여 동의를 확인한다. 해독된 개인키 및 수신된 데이터 값을 사용하여, 서비스 제공자는 데이터의 무결성을 검사할 수 있다. 서비스 제공자에 의한 스마트 컨트랙트의 승인에 추가하여, 사용자가 자신의 스마트 컨트랙트를 블록체인에서 삭제하는 내용도 스마트 컨트랙트에 포함된다.

Kaaniche의 아키텍처는 계층적 ID 기반 암호화(HIBE: Hierarchical Identity Based Encryption) 및 서명 기법[18]을 사용하기 때문에 몇 가지 이점을 제공한다. 첫째, 블록체인 객체로 간주되는 각 사용자는 위임된 개인키 생성기 역할을 할 수 있다. 둘째, 계층적 ID 기반 방식으로 루트 PKG 객체(즉, 신뢰된 중앙 객체) 역할을 할 수 있다. 셋째, 스마트 컨트랙트마다 ID 기반 키를 사용하여 사용자에 대한 재식별 공격을 방지한다.

또한 컨소시엄 블록체인 인프라에 기반한 Kaaniche의 아키텍처는 법률을 적절히 집행하는 규제 프레임워크를 제공한다. 위임된 PKG 역할을 하는 각 사용자는 스마트 컨트랙트로 개인정보 사용에 대한 동의를 제공하고 수집 및 처리 활동을 제어한다. 또한 서비스 제공자는 개인정보를 처리하기 전에 사용자의 동의를 받았다는 증거를 확보할 수 있다.

IV. 블록체인 접근제어 분류기준

관련 연구들을 분석한 결과, 이들 연구들을 비교하기 위한 기준을 다음과 같이 도출할 수 있다.

- 자동화된 접근제어: 사용자가 미리 설정한 정책에 따라서 자동으로 접근제어를 처리할 수 있다.
- 사용자 실시간 접근제어: 사용자가 고려하지 못한 상황이나 사용자의 의도가 변경되었을 때 사용자가 직접 접근제어 요청에 대해 응답할 수 있다.
- 세밀한 접근제어 정책: 사용자의 개인정보 제어 의도를 정책에 충분히 표현할 수 있다.
- 데이터 저장 위치: 사용자의 데이터가 저장되는 위치를 의미한다. 해당 위치는 데이터 노출이나 변조, 서비스 거부 공격과 같은 보안 위협에 대비한다.
- 정책 저장 위치: 사용자의 프라이버시 정책이 저장되는 위치를 의미한다. 해당 위치는 데이터 노출이나 변조, 서비스 거부 공격과

표 1 블록체인 접근제어 분류 기준에 따른 기존 연구의 분석 결과

	FairAccess	Zyskind의 제안기법	PrivacyGuard	Kaaniche의 제안기법
자동화된 접근제어	×	○	○	○
사용자 실시간 접근제어	○	×	×	×
세밀한 접근제어 정책	×	×	○	○
데이터 저장위치	IoT	DHT	클라우드	사용자
정책 저장위치	사용자	블록체인	스마트 컨트랙트	스마트 컨트랙트
블록체인 타입	퍼블릭	퍼블릭	퍼블릭	컨소시엄
스마트 컨트랙트 사용	×	×	○	○
구현	○	×	×	×
특징적인 보안요소	OrBAC	DHT	TEE	HIBE

같은 보안 위협에 대비한다.

- 블록체인 타입: 제안 기법이 적용될 수 있는 블록체인의 종류를 명시한다.
- 스마트 컨트랙트 사용: 정교한 접근제어나 보안 작업을 위해 스마트 컨트랙트를 사용하는지 여부를 의미한다.
- 구현: 제안 기법이 실제로 검증 가능한 수준으로 구현되었는지를 명시한다.
- 특징적인 보안요소: 제안 기법이 채택한 특징적인 보안 요소를 명시한다.

표 1은 본 논문에서 분석한 관련 연구에 대해 위의 기준을 대입한 결과를 보인다.

V. 결론 및 향후 연구

본 논문은 블록체인 기반의 개인정보 접근제어 기술을 분석했다. 이들 연구는 전통적인 접근제어 방식의 문제였던 효율성, 확장성, 데이터 소유권 및 체계적인 데이터 수명주기 접근을 블록체인으로 해소하는 방안을 제시한다. 새로운 접근제어 모델, 분산된 해시테이블, 신뢰할 수 있는 실행 환경, 계층적 ID 기반의 암호화 메커니즘 등을 도입하여 IoT 환경과 같은 복잡한 조건에서도 신뢰된 접근제어를 제공했다. 또한 본 논문은 블록체인 접근제어 기술의 기능 특성을 분류하기 위한 기준을 제시했다. 이 기준을 통해 각 기술의 차별성을 도출하고, 기존 기술의 한계를 극복하기 위한 새로운 접근제어 기술을 연구할 예정이다.

용어해설

블록체인(Blockchain) 공개적으로 검증 가능한 공개 원장을 사용하여 사용자가 중앙 권한을 필요로 하지 않고 암호화된 데이터를 안전하게 공유할 수 있게 해 주는 시스템

약어 정리

ACL	Access Control List
DHT	Distributed Hash Tables
GDPR	General Data Protection Regulation
HIBE	Hierarchical Identity Based Encryption
OrBAC	Organization Based Access Control
PKG	Public Key Generator
TEE	Trusted Execution Environment

참고문헌

[1] DELL EMC, "New Dell EMC Research: Most Businesses Worldwide Now Recognize Value of Data Yet Struggle with Adequate Data Protection," 2019, https://www.emc.com/about/news/press/2019/20190321-01.htm

[2] D. Rushe, "Facebook Sorry - Almost - for Secret Psychological Experiment on Users," The Guardian, Oct. 2, 2014.

[3] C. Cadwalladr, E Mraham-Harrison, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach," The Guardian, Mar. 17, 2018.

[4] S. de Capitani di Vimercati et al., "Encryption Policies for Regulating Access to Outsourced Data," ACM Trans. Database Syst. *(TODS)*, vol. 35, no. 2, Apr. 2010, pp. 12:1-46.

[5] C. Dwork, "Differential privacy," in *Encyclopedia of Cryptography and Security*, Springer: New York, USA, 2011, pp. 338-340.

[6] G. Zyskind, O. Nathan, A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in *IEEE Security Privacy Workshops*, San jose, CA, USA, May 2015, pp. 180-184.

[7] M. Crosby et al., "Blockchain Technology: Beyond Bitcoin," *Appl. Innovation Rev.*, vol. 2, 2016, pp. 7-19.

[8] K. Christidis, M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, 2016, pp. 2292-2303.

[9] M. Pilkington, "11 Blockchain technology: principles and applications," in *Research Handbook on Digital Transformations*, Sept. 2016, pp. 225-253.

[10] M. Vukolić, "The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication," in *International Workshop on Open Problems in Network Security*, Springer: New York, USA, 2015, pp. 112-125.

[11] J. Zheng et al., "Dynamic Role-Based Access control model," *J. Softw.*, vol. 6, no. 6, 2011, pp. 1096-1102.

[12] J.L. Hernández-Ramos et al., "Distributed Capability-Based Access Control for the Internet of Things," *J. Internet Services Inf. Security (JISIS)*, vol. 3, no. 3/4, 2013, pp. 1-16.

[13] E. Bertino, "Big Data-Security and Privacy," in *IEEE Int. Congress Big Data*, New York, USA, 2015, pp. 757-761.

[14] T. Salman et al., "Security Services Using Blockchains: A State of the Art Survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, 2018, pp. 858-880.

[15] A. Ouaddah et al., "FairAccess: A New Blockchain-Based Access Control Framework for the Internet of Things," *Security Commun. Netw.*, vol. 9, no. 18, 2016, pp. 5943-5964.

[16] N. Zhang et al., "PrivacyGuard: Enforcing Private Data Usage with Blockchain and Attested Execution," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, Springer: New York, USA, 2018. pp. 345-353.

[17] N. Kaaniche, M. Laurent, "A Blockchain-Based Data Usage Auditing Architecture with Enhanced Privacy and Availability," in *IEEE 16th Int. Symp. Netw. Comput. Applicat (NCA)*, Cambridge, MA, USA, 2017, pp. 1-5.

[18] C. Gentry, S. Halevi, "Hierarchical Identity Based Encryption with Polynomially Many Levels," in *Theory of Cryptography Conference*, Springer, New York, USA, 2009. pp. 437-456.