블록체인을 활용한 데이터 위변조 검증 시스템 개발 방법

임대근, 김양중*

한국공학대학교

{putnagy, zeroplus*}@tukorea.ac.kr

Implementation on the Data Forgery and Modulation Verification System Using Blockchain Technology

DaeGeun Lim, Yangjung Kim*
Tech University of Korea

요 약

블록체인 기술을 활용한 다양한 위변조 검증 시스템들이 개발되어 적용되는 가운데, 전산시스템들의 정보들이 데이터베이스를 기반으로 저장, 검색, 가공되기 때문에, 여전히 데이터검증의 중심이 될 수밖에 없다. 이에, 본 논문에서는 데이터베이스 테이블의 컬럼 기준으로 위변조 검증이 필요한 시스템의 개발 메커니즘 및 방법론을 제시한다. 제안하는 시스템은 위변조 검증이 필요한 원본 테이블과 블록체인 분산원장의 TX-ID 를 가지고 있는 검증 로그 데이터베이스, 클라이언트와 서버의 데이터 전송 규칙 및 데이터 저장, 조회 모듈의 구성하며, 이 블록체인 기술을 이용한 데이터 위변조 검증 시스템을 이용할 시, 보안적 측면의 효과 및 데이터 무결성을 보장할 수 있다.

Ⅰ. 서 론

DLT(Distributed Ledger Technology) 기술은 중앙 관리자 또는 저장소가 없이 분산 네트워크 내의 참여자가 알고리즘을 통해 정보를 복제해 공유하는 기술로, 이 기술의 대표적인 사례인, '블록체인'을 이용해 이미지 및 문서 등을 해싱함으로써 위변조 검증시스템을 구현하게 된다. 기업에서 이용하는 주요 데이터를 비롯해 입찰 시스템 및 인사평가 시스템들은 일반적으로 데이터베이스 기반의 시스템이 구축됨으로 이러한 데이터들은 데이터 무결성의 대상이자, 또 위변조 진위 검증의 대상이기도 하다. 데이터 위변조는 외부적으로는 해킹과 악성 프로그램, 내부적으로 권한을 갖고 있는 악의적인 내부자의 소행일 수 있어서, 사전방지를 한다고 해도 막을 수 없는 상황이 될 수 있다. 하지만 위변조 검증을 위해서 블록 체인 기술을 이용한 관리시스템을 도입한다면 이러한 우려 상황은 극복할 수 있을 것이다.

따라서, 본 논문에서는 데이터베이스 테이블의 컬럼 기준으로 블록체인 기술을 통한 위변조 방지 및 검증 메커니즘을 제안하고 이에 개발방법을 제시한다.

Ⅱ. 본론

1. 블록체인을 이용한 위변조 검증 대상 저장

위변조 검증을 위해서는 검증을 위한 대상 설정 이 먼저 선행되어야 하며, 테이블 컬럼을 기준으로 검증 기준을 설정하도록 한다. 이를 위해서 요구된 컬럼은 관리자가 특정할 수 있으며, 클라이언트에서 설정된 컬럼값이 서버로 전송되면 서버에서는 해당 데이 터가 위변조 검증이 필요한 여부를 판단하고 기본적으로 데이터베이스와 분산원장에 해당 데이터를 저장하도록 한다. 위변조 검증을 위해서 서버는 로깅대상 정보와 Timestamp 를 기준으로 'sha256' 해시값을 생성한다. 이 해시값은 로그데이터로 증적정보를 갖는 로그 테이블에 저장된다[1]. 또한 해시값은 블록체인에 저장되고 반환되는 TX-ID 를 생성해, 해당 로그 테이블의 키값 기준으로 저장된다. 이 키값은 원테이블과 로그 증적정보 테이블이 동일하게 보관되고 관리되도록 하며, 결국 키값을 기준으로 TX-ID 를 검색하게 된다. 블록체인 시스템들은 기본적으로 데이터가 실시간으로 저장되는 구조가 아니기 때문에, 종류에 따라 해시값이 저장되면서 시간적 차이가 발생한다. 위변조 시스템은 이러한 실시간성이 우선시 하지 않기에 본 논문에서는 논의되지 않는다.

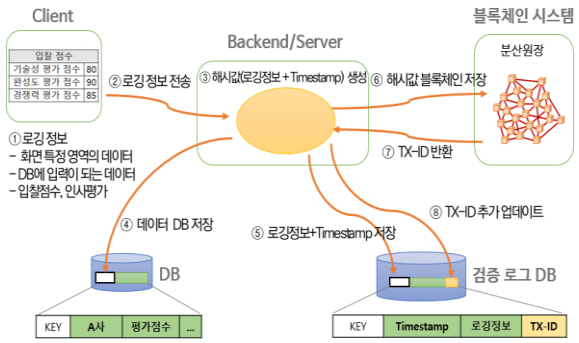

그림 1. 위변조 검증 대상 저장 프로세스

2. 블록체인을 이용한 위변조 검증 대상 조회

그림 2 에서 볼 수 있듯이, 위변조 검증 대상을 조회하기 위해서는, 검증이 요구되는 대상의 키값을 기준으로 데이터베이스의 블록체인 TX-ID 를 추출한다. 이에, 서버는 검증로그 데이터베이스에서 추출된, TX-ID 를 이용해 블록체인에 저장된 해시값을 획득한다. 획득된 해시값은 검증로그 데이터베이스에 저장된

Timestamp 와 로깅 정보를 해시한 값과 기존 데이터베이스 테이블에 저장된 로깅 정보와 검증로그 데이터베이스의 Timestamp 해시값과 비교하여 위변조 검증을 한다. 세 파트의 해시값이 모두 같다면 해당 데이터 정보는 위변조가 없다고 판별할 수 있으며, 이는 데이터무결성을 신뢰할 수 있다고 볼 수 있다.

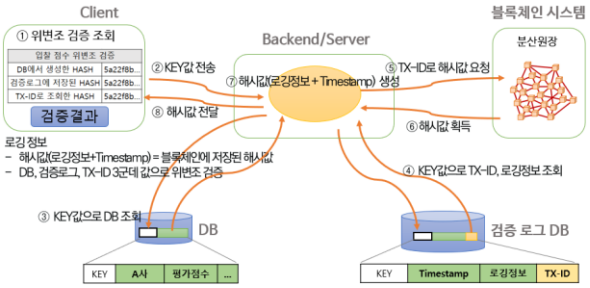

그림 2. 위변조 대상 검증 프로세스

3. 위변조 검증 시스템의 구성

위변조 검증시스템의 구성에는 크게 위변조 검증 대상이 만들어지는 Front-End 데이터 입력부, 입력부에서 데이터를 받아서 Timestamp 와 로깅정보로 해시값을 만들고 키값과 함께 검증로그 DB 와 블록체인에 저장을 담당하는 서버측 저장모듈, 생성된 키를 기준으로 검정대상의 Timestamp 와 로깅정보를 통해 해시값을 만들고 TX-ID 를 통해 블록체인의 해시값을 검색해 비교하는 서버측 조회모듈로 나눌 수 있다. 부가적으로, 블록 체인 시스템과의 트랜잭션에 필요한 데이터 쓰기, 읽기 버퍼 모듈 및 전자지갑 관리모듈 등이 요구되며, 최근에는 블록체인 시스템을 위해 하이퍼렛저를 사용한 프라이 빗 블록체인의 활용해 추가될 수 있다[2].

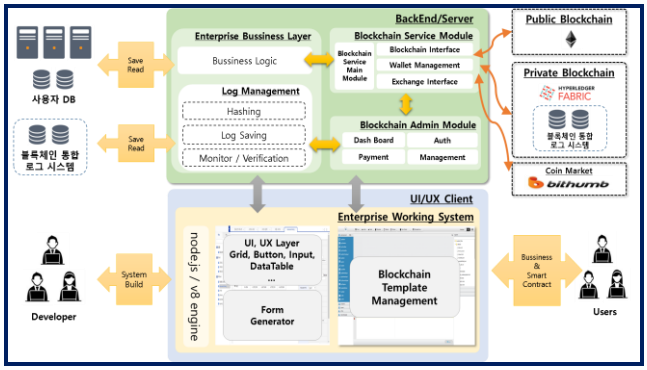

그림 3. 위변조 검증 시스템 구성도

그림 3 에서 볼 수 있듯이, 제안된 검증 시스템 구성도를 활용해 신규 시스템을 구축할 때는 물론이고, 기존 시스템의 위변조 검증 프로세스를 도입하고자 할 시, 검증로그 데이터베이스와 블록체인 서버 모듈만 추가하고 기존 데이터베이스와 검증로그 데이터베이스 간의 연관성 매핑으로도 어느 수준의 위변조 검증시스템을 구축하도록 설정이 가능하며, 기존의 주요 멀티미디어 자료를 블록체인으로 관리하는 방안에서 전체적으로 많은 데이터를 관리하는 방식에 비효율적인 요소를 제거하고 필요한 부분 블록체인으로 관리하도록 하는 메커니즘을 갖는 바, 이에 효율성을 극대화한다고 볼 수 있다[3].

위변조 검증의 대상이 되는 기준 데이터들은 Front-End 입력부에서 설정할 수 있도록 하여, 전체 시스템에서 위변조 검증을 원하는 데이터들만 선택적으로 사용할 수 있도록 할 수 있으며, 위변조 검증이 필요하지 않은 데이터들은 기존과 같이 데이터베이스에 저장되고 위변조 검증이 필요한 데이터인 경우는 Front-End 에서 서버로 전송되도록 추가 속성값을 갖게 한다. 이 추가 속성값은 데이터가 생성되는 Front-End 화면에서 설정할 수 있어, 서버측 모듈의 의존없이 쉽게 처리되도록 구성할 수 있는 것이다. 서버측 모듈에서는 블록체인 속성값이 'TRUE'인 경우, 해당 데이터의 값을 통해 해시값을 만들고 검증로그 데이터베이스와 블록체인의 위변조 검증을 위한 데이터를 동시에 저장하도록 하였다.

```
<grid>
    <header>
        <column ID="name">입찰 참가 회사명</column>
        <column ID="tech" blockchain="true">기술 평가 점수</column>
        <column ID="perfection" blockchain="true">완성도 평가 점수</column>
        <column ID="competitive" blockchain="true">경쟁력 평가 점수</column>
    </header>
    <body>
        <row>
            <cell>A사</cell>
            <cell>80</cell>
            <cell>90</cell>
            <cell>85</cell>
        </row>
        <row>
            <cell>B사</cell>
            <cell>75</cell>
            <cell>85</cell>
            <cell>80</cell>
        </row>
    </body>
</grid>
```

그림 4. Front-End 데이터 입력부 설정

Ⅲ. 결론

여전히 데이터베이스의 이용도가 폭넓고 더욱 디지털 정보가 방대해지는 가운데, 데이터 무결성을 위한 방지책이 필요하며, 이러한 요구에 분산원장 기술인 블록체인의 도입은 절실한 상황이다. 모든 데이터를 블록체인의 대상으로 하기 보다는 데이터베이스의 특정 칼럼만을 부분적으로 해싱해 데이터 무결성을 확인하는 방법을 제안하였으며, 이를 통해 효율성 높은 위변조 검증 시스템을 구축할 수 있을 것으로, 검증 프로세스와 시스템 구성을 제안하였다. 향후, DBMS 상의 여러 컬럼구조와 데이터 형태에 따른 보다 정확한 위변조 검증을 통해 데이터 무결성을 확보하는 연구를 이어나갈 예정이다.

ACKNOWLEDGMENT

본 연구는 고용노동부 및 한국산업인력공단의 '2024 년 고숙련 마이스터 사업'의 지원을 받음.

참 고 문 헌

[1] 김진주, 한영근, 변재영, LGCNS 정보기술연구소(블록체인 기술팀)(2019). 블록체인을 활용한 위·변조가 불가능한 로그관리시스템

[2] 김태환, 조창희, 최형광(2021).오픈소스 블록체인을 활용한 전자문서 위·변조 방지 시스템 설계 및 구현 연구 - 하이퍼레저를 중심으로

[3] 차중혁, 이재민, 김동성(2023).국방시험평가서의 위변조 방지를 위한 하이브리드 블록체인 설계 및 구현