



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0056866
(43) 공개일자 2021년05월20일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) H04L 9/32 (2006.01)
(52) CPC특허분류
H04L 9/0894 (2013.01)
H04L 9/3263 (2013.01)
(21) 출원번호 10-2019-0143846
(22) 출원일자 2019년11월11일
심사청구일자 2019년11월11일

(71) 출원인
서강대학교산학협력단
서울특별시 마포구 백범로 35 (신수동, 서강대학교)
(72) 발명자
장주욱
서울특별시 마포구 대흥동 백범로 35 서강대학교
피승재
서울특별시 마포구 대흥동 백범로 35 서강대학교
박인환
서울특별시 마포구 대흥동 백범로 35 서강대학교
(74) 대리인
이지연

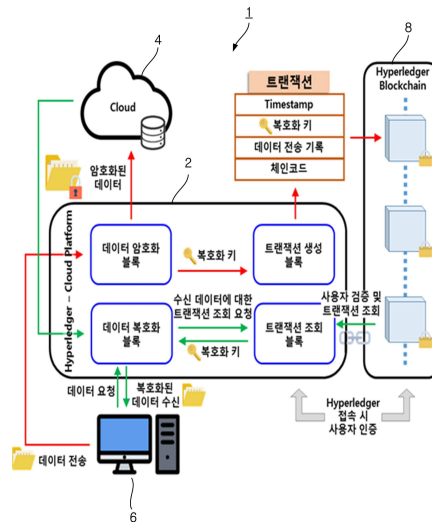
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **블록체인을 기반으로 한 클라우드 데이터 저장 시스템 및 데이터 저장 방법**

(57) 요약

본 발명은 블록체인을 기반으로 한 클라우드 데이터 저장 시스템 및 데이터 저장 방법에 관한 것이다. 상기 클라우드 데이터 저장 시스템은 블록체인 네트워크, 클라우드 저장소 및 클라우드 플랫폼을 구비하며, 상기 클라우드 플랫폼은 프라이빗 블록체인 네트워크인 하이퍼레저 패브릭 네트워크와 연동되어, 데이터는 암호화시켜 클라우드 저장소에 저장하고, 암호화된 데이터에 대한 복호화 키, 타임 스탬프, 사용자 ID와 사용자 인증서를 포함하는 체인 코드 및 데이터 전송 기록을 포함하는 트랜잭션을 생성하여 하이퍼레저 패브릭 네트워크의 블록체인 원장에 기록함으로써, 데이터를 암호화된 형태로 클라우드 저장소에 안전하게 저장시키는 것을 특징으로 한다.

대표도 - 도1



(52) CPC특허분류

H04L 2209/38 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711093140
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	대학ICT연구센터지원사업
연구과제명	적응형 블록체인 플랫폼 기술 개발 및 전문 인력 양성
기 여 율	1/1
과제수행기관명	서강대학교 산학협력단
연구기간	2019.03.01 ~ 2020.12.31

명세서

청구범위

청구항 1

사용자 인증된 노드들이 참여하는 블록체인 네트워크;

데이터를 저장하는 클라우드 저장소;

사용자 노드로부터 입력되는 데이터를 암호화하여 상기 클라우드 저장소에 저장하고, 암호화된 데이터에 대한 복호화 키를 상기 블록체인 네트워크의 블록체인 원장에 저장하며, 사용자 노드로부터의 데이터 요청에 따라 상기 복호화키를 이용하여 상기 암호화된 데이터를 복호화하여 제공하는 클라우드 플랫폼;

을 구비하는 것을 특징으로 하는 블록체인을 기반으로 한 클라우드 데이터 저장 시스템.

청구항 2

제1항에 있어서, 상기 블록체인 네트워크는 사전 설정된 인증 기관에 의해 사용자 인증된 사용자들만이 피어 노드(peer node)로서 참여하는 프라이빗 블록체인 네트워크(Private Blockchain Network)로서, 하이퍼레저 패브릭 네트워크(Hyperledger Fabric Network)인 것을 특징으로 하는 블록체인을 기반으로 한 클라우드 데이터 저장 시스템.

청구항 3

제1항에 있어서, 상기 클라우드 플랫폼은,

사전 설정된 암호화 알고리즘을 이용하여 사용자 노드로부터 입력된 데이터를 암호화하여 상기 클라우드 저장소에 저장하는 데이터 암호화 모듈;

상기 데이터 암호화 모듈로부터 상기 데이터에 대한 복호화 키를 전달받고, 복호화 키를 포함하는 트랜잭션을 생성하여 상기 블록체인 네트워크의 블록체인 원장에 저장하는 트랜잭션 생성 모듈;

데이터 복호화 모듈로부터 특정 데이터에 대한 복호화 키가 요청되면, 상기 요청된 데이터에 대한 트랜잭션을 블록체인 원장으로부터 추출하고, 상기 추출된 트랜잭션에 포함된 복호화 키를 데이터 복호화 모듈로 제공하는 트랜잭션 조회 모듈; 및

사용자 노드로부터의 특정 데이터에 대한 조회 요청에 따라, 클라우드 저장소에서 암호화된 데이터를 수신하고, 상기 트랜잭션 조회 모듈에 상기 특정 데이터에 대한 복호화 키를 요청하고, 상기 요청에 따라 전달받은 복호화 키를 이용하여 상기 암호화된 데이터를 복호화하여 제공하는 데이터 복호화 모듈;

을 구비하는 것을 특징으로 하는 블록체인을 기반으로 한 클라우드 데이터 저장 시스템.

청구항 4

제3항에 있어서, 상기 암호화 알고리즘은 암호화 키와 복호화 키가 동일한 AES 암호화 알고리즘인 것을 특징으로 하는 블록체인을 기반으로 한 클라우드 데이터 저장 시스템.

청구항 5

제3항에 있어서, 상기 트랜잭션 생성 모듈이 생성한 트랜잭션은,

상기 데이터 암호화 모듈로부터 전달받은 데이터에 대한 복호화 키, 타임 스탬프, 데이터 전송 기록 및 체인 코드를 포함하고,

상기 체인 코드는 상기 클라우드 플랫폼의 사용자 ID 및 블록체인 네트워크의 사용자 인증서를 포함하는 것을 특징으로 하는 블록체인을 기반으로 한 클라우드 데이터 저장 시스템.

청구항 6

제1항에 있어서, 상기 클라우드 플랫폼은,

클라우드 서비스 사용자가 상기 클라우드 플랫폼에 등록하고 사용자 ID를 할당받도록 구성된 사용자 등록 모듈;
및

상기 등록된 사용자에게 대하여 상기 블록체인 네트워크에 대한 사용자 인증서를 발급하고 상기 사용자의 단말이
블록체인 네트워크의 피어 노드로서 참가하도록 하는 인증서 발급 모듈;

을 구비하여, 블록체인 네트워크에 대한 MSP(Membership Service Provider)의 역할을 수행하여 사용자에게 대한
등록 및 인증을 수행하는 것을 특징으로 하는 블록체인을 기반으로 한 클라우드 데이터 저장 시스템.

청구항 7

블록체인 네트워크와 연동된 클라우드 플랫폼에서의 데이터 저장 방법은,

(a) 사용자 노드로부터의 데이터 저장 요청에 따라, 사전 설정된 암호화 알고리즘을 이용하여 데이터를 암호화
하고, 상기 암호화된 데이터를 클라우드 저장소에 저장하는 데이터 암호화 단계;

(b) 상기 암호화된 데이터에 대한 복호화 키를 포함하는 트랜잭션을 생성하고 상기 트랜잭션을 블록체인 네트워
크의 블록체인 원장에 기록하는 트랜잭션 생성 단계;

(c) 사용자 노드로부터의 데이터 조회 요청에 따라, 클라우드 저장소로부터 암호화된 데이터를 수신하고, 상기
데이터에 대한 복호화키를 블록체인 네트워크의 블록체인 원장으로부터 조회하여 확인하고, 상기 확인된 복호화
키를 이용하여 상기 암호화된 데이터를 복호화하여 제공하는 데이터 복호화 단계;

를 구비하는 것을 특징으로 하는 블록체인을 기반으로 한 클라우드 플랫폼에서의 데이터 저장 방법.

청구항 8

제7항에 있어서, 상기 (b) 단계에서 생성되는 트랜잭션은,

상기 암호화된 데이터에 대한 복호화 키, 타임 스탬프, 데이터 전송 기록 및 체인 코드를 포함하고,

상기 체인 코드는 상기 클라우드 플랫폼의 사용자 ID 및 블록체인 네트워크의 사용자 인증서를 포함하는 것을
특징으로 하는 블록체인을 기반으로 한 클라우드 플랫폼에서의 데이터 저장 방법.

청구항 9

제7항에 있어서, 상기 클라우드 플랫폼에서의 데이터 저장 방법은,

클라우드 플랫폼에 사용자를 등록하고 사용자 ID를 할당하는 단계; 및

등록된 사용자에게 대하여 인증을 수행하여 블록체인 네트워크에 대한 사용자 인증서를 발급하여 상기 사용자의
단말이 노드로서 상기 블록체인 네트워크에 참여하도록 하는 단계;

를 구비하는 것을 특징으로 하는 블록체인을 기반으로 한 클라우드 플랫폼에서의 데이터 저장 방법.

청구항 10

제7항에 있어서, 상기 블록체인 네트워크는 사전 설정된 인증 기관에 의해 사용자 인증된 사용자들만이 노드로
서 참여하는 프라이빗 블록체인 네트워크(Private Blockchain Network)로서, 하이퍼레저 패브릭 네트워크
(Hyperledger Fabric Network)인 것을 특징으로 하는 블록체인을 기반으로 한 클라우드 플랫폼에서의 데이터 저
장 방법.

발명의 설명

기술 분야

본 발명은 클라우드 데이터 저장 시스템에 관한 것으로서, 더욱 구체적으로는 블록체인을 기반으로 하여, 데이
터는 암호화시켜 클라우드 저장소에 저장하고, 암호화된 데이터에 대한 복호화키는 하이퍼레저 패브릭의 블록체
인 원장에 기록함으로써, 데이터를 클라우드에 안전하게 저장할 수 있도록 한 블록체인을 기반으로 한 클라우드
데이터 저장 시스템 및 데이터 저장 방법에 관한 것이다.

[0001]

배경 기술

- [0002] 최근, 통신 기술 및 모바일 단말에 대한 기술이 급속도로 발전함에 따라, 클라우드 서버에 데이터를 저장하는 다양한 형태의 데이터 저장 시스템들이 개발되어 사용되고 있다. 클라우드 서버의 클라우드 저장소에 저장된 데이터는 클라우드 서비스 사용자가 언제 어디서나 데이터를 다운로드받을 수 있을 뿐만 아니라, 대용량의 데이터도 저장 용량의 우려없이 저장가능하므로, 최근 사용이 증대되고 있는 실정이다.
- [0003] 하지만, 클라우드 데이터 저장 시스템은, 많은 사용자들에게 노출되어 있을 뿐만 아니라, 외부의 공격이나 해킹이 발생하는 경우 클라우드 저장소에 저장된 모든 데이터들이 한꺼번에 노출되어 버리는 문제점이 내재되어 있다.
- [0004] 한편, 블록체인 네트워크는 네트워크에 참여하는 사용자들이 직접 데이터를 검증하고 합의하여 데이터를 분산 저장하는 것으로서, 중앙 관리 기관 없이 사용자들이 직접 거래할 수 있게 된다. 블록체인은 트랜잭션의 위조 및 변조가 어려우므로 데이터의 신뢰성을 보장받을 수 있을 뿐만 아니라 모든 사용자들이 동일한 블록체인 원장을 보유함으로써 누구나 열람할 수 있기 때문에 데이터의 투명성과 무결성을 보장하게 된다.
- [0005] 이러한 블록체인 네트워크는 퍼블릭(Public) 블록체인 네트워크와 프라이빗(Private) 블록체인 네트워크로 나뉘게 된다. 퍼블릭 블록체인 네트워크는 모든 데이터가 공개되며 누구나 네트워크에 참여하여 데이터를 검증하고 블록을 생성할 수 있는 노드가 될 수 있으며, 현재 비트코인 및 이더리움이 퍼블릭 블록체인 네트워크로 이루어진다.
- [0006] 한편, 프라이빗 블록체인 네트워크는 기업을 위하여 개발되었으며, 사적 블록체인, 폐쇄형 블록체인, 허가형 블록체인, 기업형 블록체인 또는 엔터프라이즈 블록체인이라고도 불리우며, 허가된 참여자 외의 거래 내역과 여러 행동(Action)은 공유되지 않고 추적할 수 없다. 그리고, 프라이빗 블록체인 네트워크에 참여하기 위하여, 한 명의 주체로부터 허가된 참여자만이 참여하여 블록을 생성할 수 있으며, 프라이빗 블록체인의 대표적인 사례로는 하이퍼레저 패브릭(Hyperledger Fabric)이 있다. 하이퍼레저 패브릭은 허가된 참여자만 블록체인 네트워크에 참여 가능하며 네트워크내에서 조직(Organization)을 구성하고 논리적 묶음(Channel)으로 서로 다른 원장의 공유가 가능하다.
- [0007] 앞서 설명한 바와 같이, 종래의 클라우드 서비스는 클라우드 서버가 공격당했을 때 클라우드 저장소에 저장된 데이터들이 노출될 위험이 매우 크다. 따라서, 본 발명은 블록체인 네트워크를 이용하여 클라우드 저장소에 저장된 데이터들을 안전하게 관리할 수 있도록 하는 방안을 제안하고자 한다.

선행기술문헌

특허문헌

- [0008] (특허문헌 0001) 한국공개특허공보 제 10-2018-0060044호
(특허문헌 0002) 한국등록특허공보 제 10-1720268호

발명의 내용

해결하려는 과제

- [0009] 전술한 문제점을 해결하기 위한 본 발명의 목적은 프라이빗 블록체인 네트워크인 하이퍼레저 패브릭과 연동되어, 데이터의 노출없이 클라우드에 데이터를 안전하게 저장할 수 있도록 하는 클라우드 데이터 저장 시스템을 제공하는 것이다.
- [0010] 본 발명의 다른 목적은 프라이빗 블록체인 네트워크인 하이퍼레저 패브릭과 연동되어, 클라우드 저장소에 데이터를 안전하게 저장할 수 있도록 하는 클라우드 데이터 저장 방법을 제공하는 것이다.

과제의 해결 수단

- [0011] 전술한 기술적 과제를 달성하기 위한 본 발명의 제1 특징에 따른 블록체인을 기반으로 한 클라우드 데이터 저장 시스템은, 사용자 인증된 노드들이 참여하는 블록체인 네트워크; 데이터를 저장하는 클라우드 저장소; 사용자

노드로부터 입력되는 데이터를 암호화하여 상기 클라우드 저장소에 저장하고, 암호화된 데이터에 대한 복호화 키를 상기 블록체인 네트워크의 블록체인 원장에 저장하며, 사용자 노드로부터의 데이터 요청에 따라 상기 복호화 키를 이용하여 상기 암호화된 데이터를 복호화하여 제공하는 클라우드 플랫폼;을 구비한다.

[0012] 전술한 제1 특징에 따른 블록체인을 기반으로 한 클라우드 데이터 저장 시스템에 있어서, 상기 블록체인 네트워크는 사전 설정된 인증 기관에 의해 사용자 인증된 사용자들만이 노드로서 참여하는 프라이빗 블록체인 네트워크(Private Blockchain Network)로서, 특히 하이퍼레저 패브릭 네트워크(HyperLedger Fabric Network)인 것이 바람직하다.

[0013] 전술한 제1 특징에 따른 블록체인을 기반으로 한 클라우드 데이터 저장 시스템에 있어서, 상기 클라우드 플랫폼은, 사전 설정된 암호화 알고리즘을 이용하여 사용자 노드로부터 입력된 데이터를 암호화하여 상기 클라우드 저장소에 저장하는 데이터 암호화 모듈; 상기 데이터 암호화 모듈로부터 상기 데이터에 대한 복호화 키를 전달받고, 복호화 키를 포함하는 트랜잭션을 생성하여 상기 블록체인 네트워크의 블록체인 원장에 저장하는 트랜잭션 생성 모듈; 사용자 인증을 거친 후 데이터에 대한 트랜잭션의 복호화 키를 제공하는 트랜잭션 조회 모듈; 및 사용자 노드로부터의 데이터 요청에 따라, 클라우드 저장소에서 암호화된 데이터를 수신하고, 상기 트랜잭션 조회 모듈에 데이터에 대한 복호화 키를 요청하고, 상기 요청에 따라 전달받은 복호화 키를 이용하여 상기 암호화된 데이터를 복호화하여 제공하는 데이터 복호화 모듈;을 구비하는 것이 바람직하다.

[0014] 전술한 제1 특징에 따른 블록체인을 기반으로 한 클라우드 데이터 저장 시스템에 있어서, 상기 암호화 알고리즘은 암호화 키와 복호화 키가 동일한 AES 암호화 알고리즘인 것이 바람직하다.

[0015] 전술한 제1 특징에 따른 블록체인을 기반으로 한 클라우드 데이터 저장 시스템에 있어서, 상기 트랜잭션 생성 모듈이 생성한 트랜잭션은, 상기 데이터 암호화 모듈로부터 전달받은 데이터에 대한 복호화 키, 타임 스탬프, 데이터 전송 기록 및 체인 코드를 포함하고, 상기 체인 코드는 상기 클라우드 플랫폼의 사용자 ID 및 블록체인 네트워크의 사용자 인증서를 포함하는 것이 바람직하다.

[0016] 전술한 제1 특징에 따른 블록체인을 기반으로 한 클라우드 데이터 저장 시스템에 있어서, 상기 클라우드 플랫폼은, 클라우드 서비스 사용자가 상기 클라우드 플랫폼에 등록하고 사용자 ID를 할당받도록 구성된 사용자 등록 모듈; 및 상기 등록된 사용자에게 대하여 상기 블록체인 네트워크에 대한 사용자 인증서를 발급하고 상기 사용자의 단말이 블록체인 네트워크의 노드로서 참가하도록 하는 인증서 발급 모듈;을 구비하여, 사용자에게 대한 등록 및 인증을 수행하는 것이 바람직하다.

[0017] 본 발명의 제2 특징에 따른 블록체인을 기반으로 한 클라우드 플랫폼에서의 데이터 저장 방법은, (a) 사용자 노드로부터의 데이터 저장 요청에 따라, 사전 설정된 암호화 알고리즘을 이용하여 데이터를 암호화하고, 상기 암호화된 데이터를 클라우드 저장소에 저장하는 데이터 암호화 단계; (b) 상기 암호화된 데이터에 대한 복호화 키를 포함하는 트랜잭션을 생성하고 상기 트랜잭션을 블록체인 네트워크의 블록체인 원장에 기록하는 트랜잭션 생성 단계; (c) 사용자 노드로부터의 데이터 조회 요청에 따라, 클라우드 저장소로부터 암호화된 데이터를 수신하고, 상기 데이터에 대한 복호화키를 블록체인 네트워크의 블록체인 원장으로부터 조회하여 확인하고, 상기 확인된 복호화키를 이용하여 상기 암호화된 데이터를 복호화하여 제공하는 데이터 복호화 단계; 를 구비한다.

[0018] 전술한 제2 특징에 따른 블록체인을 기반으로 한 클라우드 플랫폼에서의 데이터 저장 방법에 있어서, 상기 (b) 단계에서 생성되는 트랜잭션은, 상기 암호화된 데이터에 대한 복호화 키, 타임 스탬프, 데이터 전송 기록 및 체인 코드를 포함하고, 상기 체인 코드는 상기 클라우드 플랫폼의 사용자 ID 및 블록체인 네트워크의 사용자 인증서를 포함하는 것이 바람직하다.

[0019] 전술한 제2 특징에 따른 블록체인을 기반으로 한 클라우드 플랫폼에서의 데이터 저장 방법은, 클라우드 플랫폼에 사용자를 등록하고 사용자 ID를 할당하는 단계; 및 등록된 사용자에게 대하여 인증을 수행하여 블록체인 네트워크에 대한 사용자 인증서를 발급하여 상기 사용자의 단말이 노드로서 상기 블록체인 네트워크에 참여하도록 하는 단계;를 더 구비하는 것이 바람직하다.

발명의 효과

[0020] 전술한 구성을 갖는 본 발명에 따른 블록체인을 기반으로 한 클라우드 데이터 저장 시스템은, 데이터는 암호화하여 클라우드 저장소에 저장하고, 암호화된 데이터에 대한 복호화 키는 트랜잭션으로 생성하여 프라이빗 블록체인 네트워크인 하이퍼레저 패브릭의 블록체인 원장에 블록의 형태로 저장함으로써, 데이터를 암호화된 형태로 클라우드 저장소에 안전하게 저장할 수 있게 된다.

[0021] 또한, 본 발명에 따른 클라우드 데이터 저장 시스템은, 모든 각각의 데이터들을 개별적으로 암호화하고, 그 기록과 복호화할 수 있는 복호화 키를 하이퍼레저 블록체인에 저장함으로써, 클라우드 저장소에 저장된 데이터들에 대한 보안성을 극대화시킬 수 있게 된다.

[0022] 또한, 본 발명에 따른 클라우드 데이터 저장 시스템은, 클라우드에 저장되는 각각의 데이터가 별도로 암호화되기 때문에, 외부의 공격이나 해킹으로부터 더 안전할 수 있고, 데이터의 입출력 기록이 모두 하이퍼레저 네트워크의 블록체인 원장에 블록의 형태로 저장되기 때문에 신뢰성을 높일 수 있다.

도면의 간단한 설명

[0023] 도 1은 본 발명의 바람직한 실시예에 따른 블록체인을 기반으로 한 클라우드 데이터 저장 시스템을 전체적으로 도시한 구성도이다.

도 2는 본 발명의 바람직한 실시예에 따른 블록체인을 기반으로 한 클라우드 데이터 저장 시스템에 있어서, 클라우드 플랫폼(2)의 구성을 개략적으로 도시한 블록도이다.

도 3은 본 발명의 바람직한 실시예에 따른 블록체인을 기반으로 한 클라우드 데이터 저장 시스템에 있어서, 클라우드 서비스 제공자와 클라우드 서비스 사용자가 맡는 피어의 역할과 각 피어가 구성하는 조직과 채널의 설정 방법을 설명하는 모식도이다.

도 4는 본 발명의 바람직한 실시예에 따른 블록체인을 기반으로 한 클라우드 데이터 저장 시스템에 있어서, 데이터 암호화 모듈과 트랜잭션 생성 모듈에 의해 데이터를 암호화하여 저장하는 과정을 도시한 흐름도이다.

도 5는 본 발명의 바람직한 실시예에 따른 블록체인을 기반으로 한 클라우드 데이터 저장 시스템에 있어서, 데이터 복호화 모듈과 트랜잭션 조회 모듈에 의해 데이터를 복호화하여 제공하는 과정을 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0024] 본 발명에 따른 클라우드 데이터 저장 시스템은 프라이빗 블록체인 네트워크인 하이퍼레저 패브릭 네트워크와 연동되어, 데이터는 암호화시켜 클라우드 저장소에 저장하고, 암호화된 데이터에 대한 복호화 키, 사용자 ID와 사용자 인증서를 포함하는 체인 코드 및 데이터 전송 기록을 포함하는 트랜잭션의 형태로 하이퍼레저 네트워크의 블록체인 원장에 기록함으로써, 데이터를 암호화된 형태로 클라우드 저장소에 안전하게 저장시키는 것을 특징으로 한다.

[0025] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예에 따른 블록체인을 기반으로 한 클라우드 데이터 저장 시스템 및 데이터 저장 방법에 대하여 구체적으로 설명한다.

[0026] 도 1은 본 발명의 바람직한 실시예에 따른 블록체인을 기반으로 한 클라우드 데이터 저장 시스템을 전체적으로 도시한 구성도이다.

[0027] 도 1을 참조하면, 본 발명에 따른 클라우드 데이터 저장 시스템(1)은, 클라우드 플랫폼(2), 클라우드 저장소(4), 사용자 단말들이 노드들(6)로 참여하는 블록체인 네트워크(도시되지 않음)를 포함한다. 상기 블록체인 네트워크는 프라이빗 블록체인 네트워크(Private Blockchain Network)인 하이퍼레저 패브릭 네트워크(HyperLedger Fabric Network)로 구성되는 것이 바람직하다. 따라서, 하이퍼레저 패브릭 네트워크로 구성되는 상기 블록체인 네트워크는 인증기관으로부터 인증되어 사용자 인증서(Ecert)를 발급받은 사용자들이 노드로 참여하게 된다.

[0028] 상기 클라우드 플랫폼(2)은 데이터 저장을 위하여 클라우드 서비스 제공자에 의해 제공되는 플랫폼으로서, 블록체인 네트워크와 연동되어 노드들로부터 제공되는 데이터들을 암호화하여 클라우드 저장소(4)에 저장하고 암호화된 데이터에 대한 복호화키는 트랜잭션으로 하이퍼레저 네트워크의 블록체인 원장(8)에 저장한다.

[0029] 도 2는 본 발명의 바람직한 실시예에 따른 블록체인을 기반으로 한 클라우드 데이터 저장 시스템에 있어서, 클라우드 플랫폼(2)의 구성을 개략적으로 도시한 블록도이다. 도 2를 참조하면, 상기 클라우드 플랫폼(2)은, 인증서 발급 모듈(20), 오더링 서비스 모듈(21), 사용자 등록 모듈(22), 데이터 암호화 모듈(24), 트랜잭션 생성 모듈(25), 데이터 복호화 모듈(26), 트랜잭션 조회 모듈(27)을 구비한다. 클라우드 서비스 제공자는 사용자의 참여를 위하여 본 발명에 따른 클라우드 플랫폼(2)을 제공하고, 하이퍼레저 네트워크를 구성하여 컨소시엄 블록체인의 주체가 된다. 이로써, 클라우드 서비스 제공자는 클라우드 플랫폼(2)을 통해 인증 기관(Certification Authority; 'CA')의 역할을 하며 사용자를 인증하고 인증서를 발급한다. 또한, 클라우드 서비스 제공자는 플랫폼

폼(2)을 통해 오더링 서비스를 제공하는 Orderer의 역할을 맡는다. 또한, 클라우드 서비스 제공자는 플랫폼의 Organization 내부에서 하이퍼레저 패브릭 네트워크의 MSP(Membership Service Provider)의 역할을 맡아, 사용자에 대한 인증 및 검증을 수행하고, 또한 플랫폼 안에서 데이터 암호화 및 복호화기능을 제공한다.

[0030] 클라우드 서비스 제공자에 의해 운영되는 클라우드 플랫폼(2)은 전술한 구성으로 이루어져, 상기 클라우드 저장소(4)와 블록체인 네트워크와 연동된다. 클라우드 플랫폼(2)은 사용자 등록 모듈(22) 및 인증서 발급 모듈(20)을 통해 MSP(Membership Service Provider) 및 블록체인 네트워크의 인증 기관(CA)으로서의 역할을 하여, 클라우드 서비스 사용자에게 대한 등록 및 인증 절차를 수행하게 된다. 상기 사용자 등록 모듈(22)은 클라우드 서비스 사용자에게 대한 사용자 등록을 수행하고 사용자에게 대한 사용자 ID 및 비밀번호를 등록한다. 상기 인증서 발급 모듈(20)은 사용자 등록된 사용자에게 인증 절차를 진행하고 블록체인 네트워크에서 사용하는 사용자 인증서(Ecert)를 발급한다. 상기 인증서 발급 모듈은 하이퍼레저 패브릭 네트워크가 제공하는 인증 기관과 연계하여, 하이퍼레저 패브릭 네트워크에서 사용하는 사용자 인증서의 발급을 수행하게 된다. 상기 인증서 발급 모듈을 통해 인증서를 발급받은 사용자가 클라우드 플랫폼에 접속하여 다른 사용자들과 같은 조직내에서 피어(peer)를 이루게 된다. 즉, 클라우드 서비스 사용자는 플랫폼을 통해 클라우드 서비스에 가입하게 되면 자신에게 할당된 클라우드 저장소에 따라 하이퍼레저 패브릭의 조직에 참가하게 된다.

[0031] 한편, 동일한 사용자의 다른 기기라면, 동일한 사용자 ID로 플랫폼에 접속하여 다른 인증서를 발급받고, 다른 기기의 피어들과 채널을 형성하여 원장을 공유한다.

[0032] 도 3은 본 발명의 바람직한 실시예에 따른 블록체인을 기반으로 한 클라우드 데이터 저장 시스템에 있어서, 클라우드 서비스 제공자와 클라우드 서비스 사용자가 맡는 피어의 역할과 각 피어가 구성하는 조직과 채널의 설정 방법을 설명하는 모식도이다. 도 3을 참조하면, 클라우드 서비스 사용자는 하이퍼레저 네트워크에 참여하며 조직에 참가하게 되는데, 해당 조직은 클라우드 저장소의 분류에 따른다. 도 3의 1번 클라우드 저장소(Cloud 1 : Organization 1)에 할당된 사용자는 1번 조직에, 2번 클라우드 저장소(Cloud 2 : Organization 2)에 할당된 사용자는 2번 조직에 해당된다. 이때 동일한 사용자가 다른 기기로 클라우드 서비스에 참가하기 위해서는 동일한 사용자 ID로 별도의 하이퍼레저의 사용자 인증서를 발급받는데, 다른 기기에서 저장한 데이터의 복호화 키를 확인하기 위하여 같은 사용자의 다른 기기들은 원장을 공유하는 채널을 형성하여 복호화 키를 확인할 수 있다. 피어가 조직에 속한 이후 임의로 선택된 한 피어가 트랜잭션을 보증하는 Endorser 역할을 하며, 다른 피어들은 Committer 역할을 하여 트랜잭션 실행 결과의 타당성을 확인하는 역할을 하게 된다.

[0033] 따라서, 사용자 등록된 클라우드 서비스 사용자는 사용자 ID와 비밀번호를 통해 클라우드 플랫폼에 접속하며, 사용자 인증서(Ecert)를 통해 하이퍼레저 네트워크 참여자인지를 검증받게 된다.

[0034] 상기 오더링 서비스 모듈(21)은 트랜잭션의 결과를 블록체인과 상태 DB에 기록하는 순서를 제어하는 오더링 서비스(Ordering Service)를 제공한다. 상기 클라우드 서비스 제공자는 상기 클라우드 플랫폼의 상기 오더링 서비스 모듈을 통해 Orderer, 즉 Ordering Service Provider의 역할을 맡게 된다.

[0035] 상기 데이터 암호화 모듈(24)은 사전 설정된 암호화 알고리즘을 이용하여 클라우드 서비스 사용자가 제공한 데이터를 암호화하고, 암호화된 데이터는 상기 클라우드 저장소(4)에 저장한다. 상기 트랜잭션 생성 모듈(25)은, 상기 데이터 암호화 모듈에 의해 암호화된 데이터에 대한 복호화키, 타임 스탬프, 데이터 전송 기록 및 체인 코드를 포함하는 트랜잭션을 생성하고, 생성된 트랜잭션은 블록체인 네트워크의 블록체인에 블록의 형태로 저장된다. 한편, 블록체인 네트워크는 상기 트랜잭션이 하이퍼레저 네트워크의 블록체인 원장에 블록 형태로 저장되면, 블록체인과 상태(State) DB가 갱신된다.

[0036] 상기 데이터 복호화 모듈(26)은 클라우드 서비스 사용자로부터 데이터가 요청되면, 클라우드 저장소로부터 암호화된 데이터를 내려 받고, 해당 데이터에 대한 트랜잭션의 조회 요청을 상기 트랜잭션 조회 모듈(37)에 전달한다. 상기 조회 요청에 따라, 상기 트랜잭션 조회 모듈(37)로부터 복호화키를 받고, 복호화키를 이용하여 상기 암호화된 데이터를 복호화하여 사용자에게 전송한다. 상기 트랜잭션 조회 모듈(27)은 상기 데이터 복호화 모듈로부터 트랜잭션 조회 요청이 발생되면, 상기 데이터 복호화 모듈로부터 사용자 ID와 인증서(Ecert)를 제공받고 이를 이용하여 체인코드로 본인 검증하고 해당 트랜잭션의 복호화키를 확인하고, 확인된 복호화키를 데이터 복호화 모듈로 제공한다.

[0037] 한편, 본 발명에 따른 시스템에서의 플랫폼의 일 실시 형태는, 데이터 암호화시에는 암호화키와 복호화키가 동일한 대칭형 AES 암호화 알고리즘을 사용하며, 암호화시 생성된 복호화키는 트랜잭션 생성 모듈을 통해 하이퍼레저 네트워크의 블록체인 원장에 저장된다. 그리고, 데이터를 복호화할 때는 트랜잭션의 체인코드에 포함되어

있는 인증서 정보 및 플랫폼의 사용자 ID를 이용하여 본인 인증 과정을 거친 뒤, 블록체인에 저장되어 있는 트랜잭션을 불러오게 된다.

[0038] 도 4는 본 발명의 바람직한 실시예에 따른 블록체인을 기반으로 한 클라우드 데이터 저장 시스템에 있어서, 데이터 암호화 모듈과 트랜잭션 생성 모듈에 의해 데이터를 암호화하여 저장하는 과정을 도시한 흐름도이다. 도 4를 참조하면, 상기 클라우드 플랫폼의 데이터 암호화 모듈은 사용자로부터 클라우드 저장소에 저장할 데이터를 수신하면(단계 400), AES 암호화 알고리즘을 이용하여 암호화/복호화 키를 생성하고(단계 410), 암호화/복호화 키를 사용하여 데이터를 암호화하여 클라우드 저장소에 저장하고(단계 420), 암호화/복호화 키를 트랜잭션 생성 모듈에 전달한다(단계 430). 상기 암호화/복호화 키를 전달받은 상기 트랜잭션 생성 모듈은 플랫폼에서의 사용자 ID 및 하이퍼레저 네트워크의 사용자 인증서를 포함하는 체인 코드를 작성하고(단계 440), 암호화/복호화 키, 타임 스탬프, 데이터 전송 기록 및 체인 코드를 포함하는 트랜잭션을 생성하고(단계 450), 상기 트랜잭션을 블록의 형태로 하이퍼레저 네트워크의 블록체인 원장에 기록하여 저장한다(단계 460).

[0039] 도 5는 본 발명의 바람직한 실시예에 따른 블록체인을 기반으로 한 클라우드 데이터 저장 시스템에 있어서, 데이터 복호화 모듈과 트랜잭션 조회 모듈에 의해 데이터를 복호화하여 제공하는 과정을 도시한 흐름도이다. 도 5를 참조하면, 데이터 복호화 모듈이 사용자로부터 특정 데이터에 대한 조회를 요청받으면(단계 500), 트랜잭션 조회 모듈에게 트랜잭션 조회를 요청한다(단계 510).

[0040] 상기 트랜잭션 조회 모듈은 체인 코드에 포함된 사용자 ID 및 사용자 인증서로 사용자를 인증하고(단계 520), 트랜잭션 내의 복호화키를 확인하고 복호화키를 데이터 복호화 모듈에게 전송한다(단계 530). 복호화키를 전송받은 데이터 복호화 모듈은 클라우드 저장소에서 암호화된 데이터를 수신하고(단계 540), 상기 수신된 암호화된 데이터를 상기 복호화 키를 이용하여 복호화하여(단계 550) 사용자에게 전송한다(단계 560).

[0041] 전술한 데이터 암호화 모듈 및 데이터 복호화 모듈에 의해 클라우드 저장소에 저장되는 모든 데이터는 AES 암호화 알고리즘을 사용하여 각각 다른 암호화/복호화 키로 암호화되어 클라우드 저장소에 저장된다. 따라서, 클라우드가 공격받더라도 각각의 파일에 대한 복호화 키가 필요하기 때문에 데이터의 복호화가 어렵게 된다. 또한, 복호화 키는 하이퍼레저 블록체인 네트워크의 블록체인 원장에 저장되어 있기 때문에 데이터의 위·변조가 어렵고 트랜잭션의 저장 및 조회 기록이 전부 남기 때문에 보안 사고를 예방할 수 있게 된다. 따라서, 기존의 클라우드 서비스는 서버를 공격당했을 때 클라우드 저장소에 저장된 데이터가 노출될 위험이 매우 크지만, 본 발명에 따른 블록체인을 기반으로 한 클라우드 데이터 저장 시스템은 개별 데이터를 암호화하고 복호화 키를 블록체인 네트워크에 저장하기 때문에 신뢰성이 우수하다.

[0042] 이상에서 본 발명에 대하여 그 바람직한 실시예를 중심으로 설명하였으나, 이는 단지 예시일 뿐 본 발명을 한정하는 것이 아니며, 본 발명이 속하는 분야의 통상의 지식을 가진 자라면 본 발명의 본질적인 특성을 벗어나지 않는 범위에서 이상에 예시되지 않은 여러 가지의 변형과 응용이 가능함을 알 수 있을 것이다. 그리고, 이러한 변형과 응용에 관계된 차이점들은 첨부된 청구 범위에서 규정하는 본 발명의 범위에 포함되는 것으로 해석되어야 할 것이다.

부호의 설명

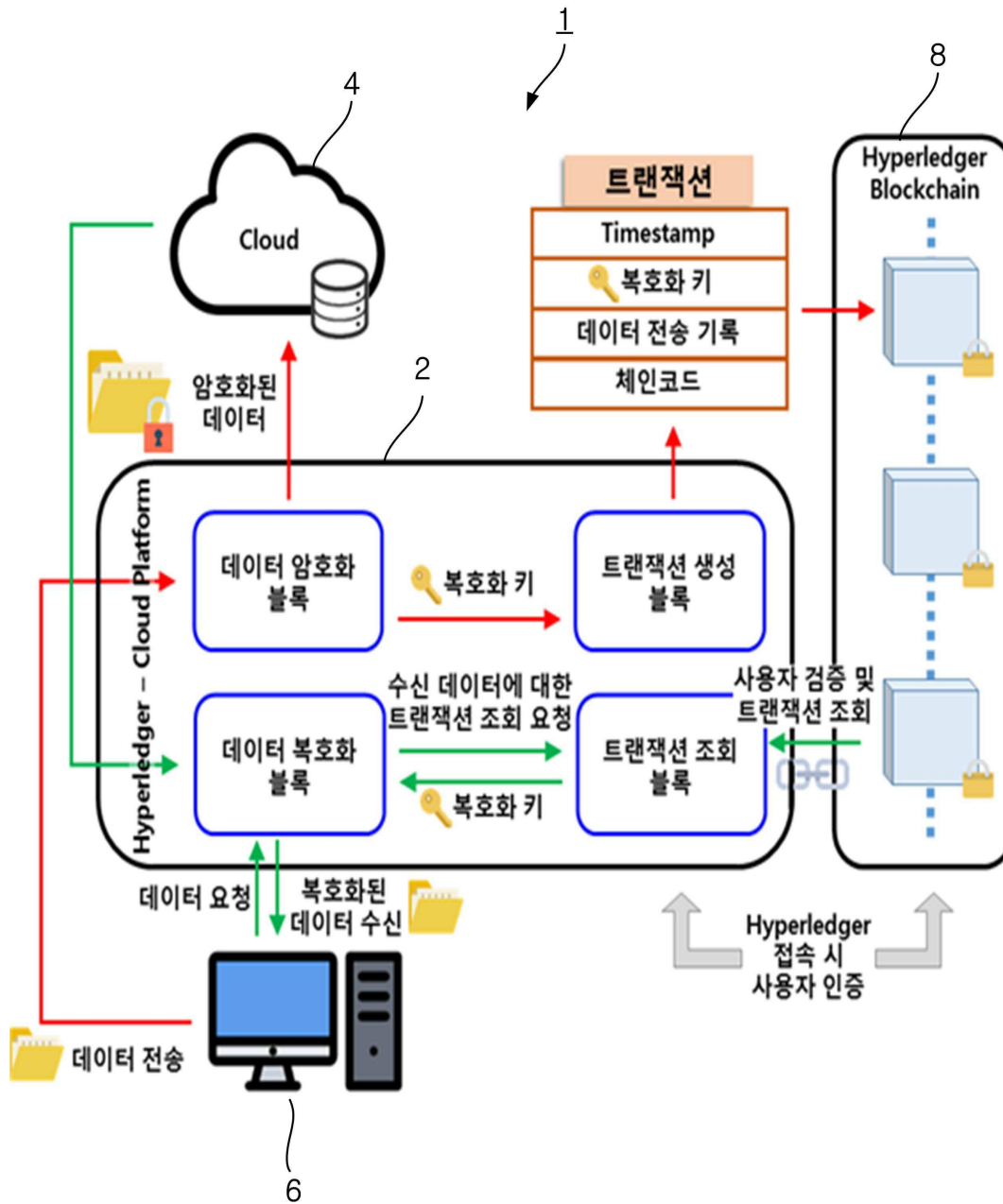
[0043] 1 : 클라우드 데이터 저장 시스템
2 : 클라우드 플랫폼
4 : 클라우드 저장소
6 : 블록체인 네트워크의 피어 노드
8 : 블록체인 네트워크의 블록체인 원장
20 : 인증서 발급 모듈
21 : 오더링 서비스 모듈
22 : 사용자 등록 모듈
24 : 데이터 암호화 모듈
25 : 트랜잭션 생성 모듈

26 : 데이터 복호화 모듈

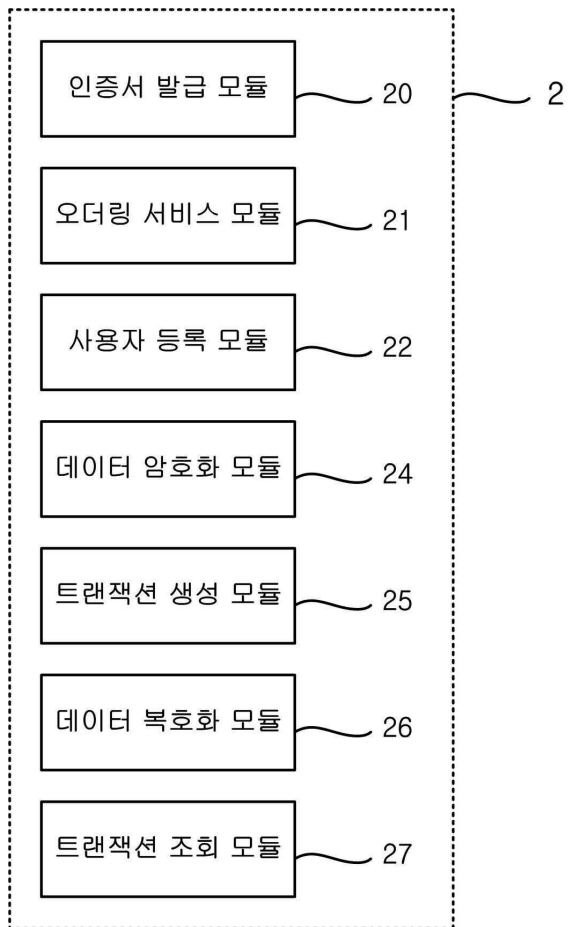
27 : 트랜잭션 조회 모듈

도면

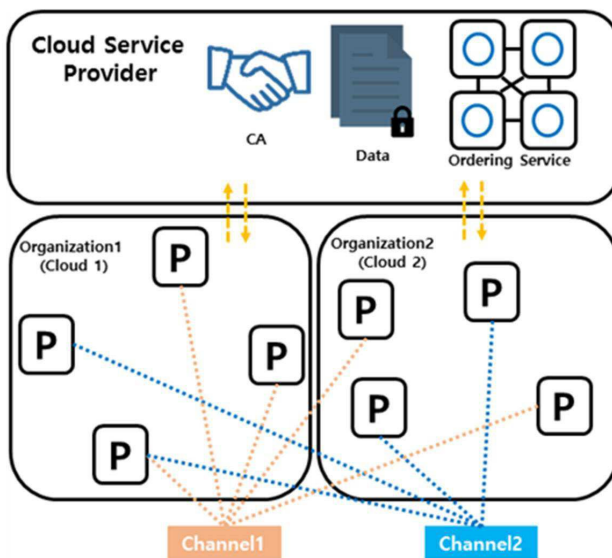
도면1



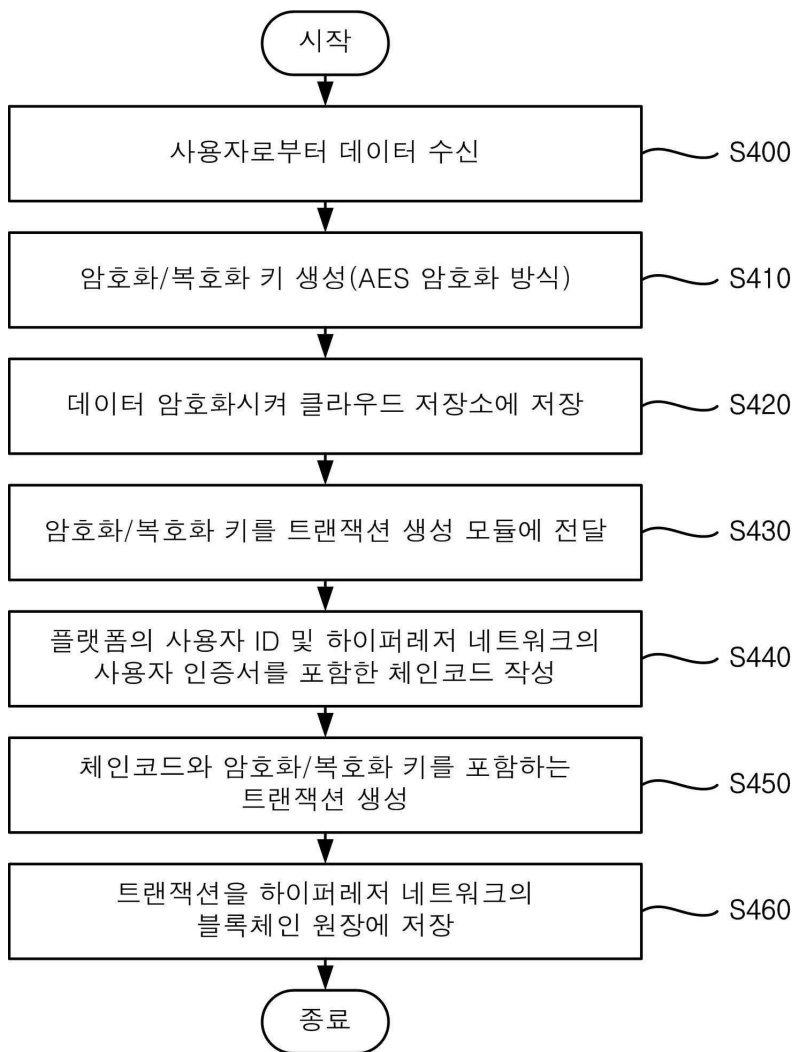
도면2



도면3



도면4



도면5

