



(19) 대한민국특허청(KR)  
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0070772  
(43) 공개일자 2023년05월23일

|                                                                                                               |                                                               |
|---------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| (51) 국제특허분류(Int. Cl.)<br>G06F 21/62 (2013.01) G06F 21/60 (2013.01)<br>H04L 9/06 (2006.01) H04L 9/08 (2006.01) | (71) 출원인<br>서강대학교산학협력단<br>서울특별시 마포구 백범로 35 (신수동, 서강대학교)       |
| (52) CPC특허분류<br>G06F 21/62 (2013.01)<br>G06F 21/602 (2013.01)                                                 | (72) 발명자<br>장주욱<br>서울특별시 서대문구 가재울미래로 2 DMC파크뷰자<br>이 206동 202호 |
| (21) 출원번호 10-2021-0156700                                                                                     | (74) 대리인<br>이지연                                               |
| (22) 출원일자 2021년11월15일                                                                                         |                                                               |
| 심사청구일자 없음                                                                                                     |                                                               |

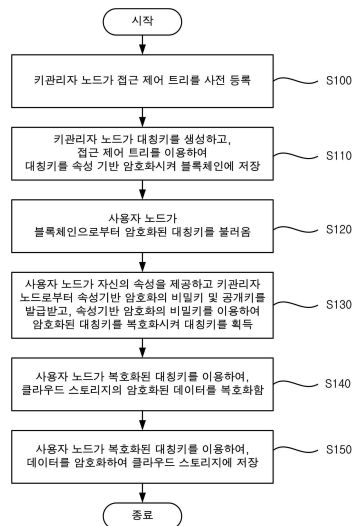
전체 청구항 수 : 총 6 항

(54) 발명의 명칭 블록체인 기반 클라우드 스토리지 시스템 및 상기 시스템에서의 접근 권한 제어 방법

(57) 요약

본 발명은 접근 권한 제어가 가능한 블록체인 기반의 클라우드 스토리지 시스템에 관한 것이다. 상기 블록체인 기반의 클라우드 스토리지 시스템은, 블록체인을 갖는 복수 개의 사용자 노드들을 구비하는 블록체인 네트워크; 데이터에 대한 접근 권한을 갖는 사용자들의 속성들을 포함하는 접근 제어 트리를 구비하고, 대칭키를 생성하고, 상기 접근 제어 트리를 이용하여 상기 대칭키를 속성 기반 암호화하고, 속성 기반 암호화된 대칭키를 상기 블록체인 네트워크의 블록체인에 저장하는 키 관리자 노드; 상기 대칭키를 이용하여 암호화된 데이터를 저장하는 상기 클라우드 스토리지;를 구비하여, 대칭키로 암호화된 데이터는 클라우드 스토리지에 저장되고, 접근 제어 트리를 이용하여 속성 기반 암호화된 대칭키는 블록체인 네트워크의 블록체인에 저장되는 것을 특징으로 한다.

대표도 - 도1



(52) CPC특허분류

*G06F 21/604* (2013.01)

*H04L 9/0618* (2013.01)

*H04L 9/0836* (2013.01)

*H04L 9/0894* (2013.01)

*H04L 9/50* (2022.05)

*G06F 2221/2141* (2013.01)

이 발명을 지원한 국가연구개발사업

|             |                                  |
|-------------|----------------------------------|
| 과제고유번호      | 1711125826                       |
| 과제번호        | 2017-0-01628-005                 |
| 부처명         | 과학기술정보통신부                        |
| 과제관리(전문)기관명 | 정보통신기획평가원                        |
| 연구사업명       | 대학ICT연구센터지원사업 또는 정보통신기술인력양성(R&D) |
| 연구과제명       | 적응형 블록체인 플랫폼 기술 개발 및 전문 인력 양성    |
| 기 여 율       | 1/1                              |
| 과제수행기관명     | 서강대학교산학협력단                       |
| 연구기간        | 2021.01.01 ~ 2022.12.31          |

---

## 명세서

### 청구범위

#### 청구항 1

블록체인을 갖는 복수 개의 사용자 노드들을 구비하는 블록체인 네트워크;

데이터에 대한 접근 권한을 갖는 사용자들의 속성들을 포함하는 접근 제어 트리를 구비하고, 대칭키를 생성하고, 상기 접근 제어 트리를 이용하여 상기 대칭키를 속성 기반 암호화하고, 속성 기반 암호화된 대칭키를 상기 블록체인 네트워크의 블록체인에 저장하는 키 관리자 노드;

상기 대칭키를 이용하여 암호화된 데이터를 저장하는 상기 클라우드 스토리지;

를 구비하여, 대칭키로 암호화된 데이터는 클라우드 스토리지에 저장되고, 접근 제어 트리를 이용하여 속성 기반 암호화된 대칭키는 블록체인 네트워크의 블록체인에 저장된 것을 특징으로 하는 블록체인 기반의 클라우드 스토리지 시스템.

#### 청구항 2

제1항에 있어서, 상기 사용자 노드는

키 관리자 노드에게 자신의 속성을 제공하고, 키 관리자 노드로부터 속성 기반 암호화를 위한 비밀키 및 공개키를 발급받고, 상기 발급된 비밀키를 이용하여 블록체인에 저장된 속성 기반 암호화된 대칭키를 복호화하고,

상기 복호화된 대칭키를 이용하여 데이터를 암호화하고, 암호화된 데이터를 상기 클라우드 스토리지에 저장하는 것을 특징으로 하는 블록체인 기반의 클라우드 스토리지 시스템.

#### 청구항 3

제1항에 있어서, 상기 사용자 노드는

키 관리자 노드에게 자신의 속성을 제공하고, 키 관리자 노드로부터 속성 기반 암호화를 위한 비밀키 및 공개키를 발급받고, 상기 발급된 비밀키를 이용하여 블록체인에 저장된 속성 기반 암호화된 대칭키를 복호화하고,

상기 복호화된 대칭키를 이용하여 상기 클라우드 스토리지에 저장된 암호화된 데이터를 복호화하는 것을 특징으로 하는 블록체인 기반의 클라우드 스토리지 시스템.

#### 청구항 4

(a) 키 관리자 노드가 데이터에 대한 접근 권한을 갖는 사용자들의 속성을 포함하는 접근 제어 트리를 구비하고, 대칭키를 생성하고, 상기 접근 제어 트리를 이용하여 상기 대칭키를 속성 기반 암호화하고, 상기 속성 기반 암호화된 대칭키를 블록체인 네트워크의 블록체인에 저장하는 단계;

(b) 블록체인 네트워크를 구성하는 사용자 노드가 대칭키를 이용하여 암호화된 데이터를 클라우드 스토리지에 저장하는 단계;

를 구비하여, 대칭키로 암호화된 데이터는 클라우드 스토리지에 저장되고, 접근 제어 트리를 이용하여 속성 기반 암호화된 대칭키는 블록체인 네트워크의 블록체인에 저장된 것을 특징으로 하는 블록체인 기반의 클라우드 스토리지 시스템에서의 접근 권한 제어 방법.

#### 청구항 5

제4항에 있어서, 상기 (b) 단계는,

상기 블록체인 네트워크를 구성하는 사용자 노드가,

키 관리자 노드에게 자신의 속성을 제공하고, 키 관리자 노드로부터 속성 기반 암호화를 위한 비밀키 및 공개키를 발급받고, 상기 발급된 비밀키를 이용하여 블록체인에 저장된 속성 기반 암호화된 대칭키를 복호화하고,

상기 복호화된 대칭키를 이용하여 데이터를 암호화하고, 암호화된 데이터를 상기 클라우드 스토리지에 저장하는 것을 특징으로 하는 블록체인 기반의 클라우드 스토리지 시스템에서의 접근 권한 제어 방법.

## 청구항 6

제4항에 있어서, 상기 접근 권한 제어 방법은,

(c) 상기 사용자 노드가,

키 관리자 노드에게 자신의 속성을 제공하고, 키 관리자 노드로부터 속성 기반 암호화를 위한 비밀키 및 공개키를 발급받고, 상기 발급된 비밀키를 이용하여 블록체인에 저장된 속성 기반 암호화된 대칭키를 복호화하고,

상기 복호화된 대칭키를 이용하여 상기 클라우드 스토리지에 저장된 암호화된 데이터를 복호화하는 단계;를 더 구비하는 것을 특징으로 하는 블록체인 기반의 클라우드 스토리지 시스템에서의 접근 권한 제어 방법.

## 발명의 설명

### 기술 분야

[0001] 본 발명은 블록체인 기반 클라우드 스토리지 시스템 및 상기 시스템에서의 효율적인 접근 권한 제어 방법에 관한 것으로서, 더욱 구체적으로는 블록체인을 기반으로 한 클라우드 스토리지에 저장되는 데이터를 속성 기반 암호화(CP-ABE)와 대칭키 알고리즘을 사용하여 암호화하는 방식을 사용함으로써, 속성 기반 암호화의 특징인 동일한 속성을 가진 사용자들과의 암호화된 데이터 공유 특성을 가지면서 암호화 및 복호화에 대한 처리 시간을 감소시켜 효율적으로 데이터를 클라우드 스토리지에 저장할 수 있도록 한 블록체인 기반 클라우드 스토리지 시스템 및 접근 권한 제어 방법에 관한 것이다.

### 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 스토리지에 저장된 데이터는 클라우드 서비스 사용자가 언제 어디서나 데이터를 다운로드받을 수 있을 뿐만 아니라, 대용량의 데이터도 저장 용량의 우려없이 저장 가능하므로, 최근 그 서비스 및 사용이 증대되고 있는 실정이다.

[0003] 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.

[0004] 따라서, 블록체인 네트워크 기술과 클라우드 데이터 저장 시스템을 결합하여 구성된 블록체인 기반 클라우드 스토리지는 데이터를 클라우드 스토리지에 저장하고, 데이터의 해시값을 블록체인 네트워크에 저장시킴으로써, 저장된 데이터의 무결성을 보장하고, 기존의 블록체인 네트워크의 저장 용량의 한계성을 해결하여 대용량의 데이터를 효율적으로 저장할 수 있는 방안을 제시하였다.

[0005] 하지만, 클라우드 데이터 저장 시스템은, 많은 사용자들에게 노출되어 있을 뿐만 아니라, 외부의 공격이나 해킹이 발생하는 경우 클라우드 스토리지에 저장된 모든 데이터들이 한꺼번에 노출되어 버리는 문제점이 내재되어 있다. 이러한 문제점을 해결하기 위하여, 클라우드 스토리지에 저장되는 데이터들을 암호화시키는 방안이 제시되고 있다.

[0006] 한국등록특허공보 제 10-2307574호는 “블록체인을 기반으로 한 클라우드 데이터 저장 시스템 및 데이터 저장 방법”에 관한 것으로서, 데이터는 암호화시켜 클라우드 스토리지에 저장하고, 암호화된 데이터에 대한 복호화키는 하이퍼레저 패브릭의 블록체인 원장에 기록함으로써, 데이터를 클라우드 스토리지에 안전하게 저장할 수 있도록 한 블록체인을 기반으로 한 클라우드 데이터 저장 시스템 및 데이터 저장 방법을 제시하였다.

[0007] 한편, 데이터를 클라우드 스토리지에 안전하게 저장시키기 위하여, 데이터에 대한 다양한 암호화 방법이 제안되고 있다. 특히, 클라우드 스토리지에 저장된 데이터가 의료 정보, 군사 기밀 또는 민감한 개인 정보 등과 같이, 제3자에게 유출되어서는 안되는 민감한 정보들을 포함하는 데이터들인 경우, 해당 데이터들을 클라우드 스토리지에 저장하는 경우 모든 데이터들을 암호화시켜야 할 뿐만 아니라, 수많은 복호화 키가 필요하며, 이러한 키를

공유하였을 때 키의 유출 가능성도 배제할 수 없는 문제가 발생하게 된다.

[0008] 따라서, 클라우드 스토리지에 저장된 데이터가 제3자에게 유출되어서는 안되는 민감 정보인 경우, 데이터에 대한 접근 권한을 제어할 수 있도록 하는 속성 기반 암호화(Ciphertext-Policy Attribute Based Encryption: CP-ABE) 알고리즘을 사용할 수 있다. 속성 기반 암호화 알고리즘은 데이터에 대한 접근 권한을 표현한 접근 제어 트리를 사전에 설정한다. 그리고, 접근 제어 트리를 이용하여 데이터를 암호화시켜 저장하며, 데이터를 복호화하는 경우 자신의 속성을 기반으로 하여 비밀키를 발급받은 후, 그 비밀키를 이용하여 암호화된 데이터의 접근 제어 트리(Access Tree) 구조를 만족하면 복호화가 가능하게 된다. 여기서, 접근 제어 트리 구조란 AND, OR 연산들과 속성들로 이루어진 트리 구조이며, 비밀키에도 그 속성에 대한 정보들이 들어있기 때문에 복호화가 가능하다. 따라서, 이러한 접근 제어 트리 구조를 이용하여 암호화된 데이터들에 대한 접근 제어가 가능하다. 따라서, 데이터를 속성 기반 암호화를 함으로써, 접근 제어 트리를 만족하는 속성을 갖는 사용자만이 데이터를 복호화할 수 있게 되어, 데이터에 대한 접근을 제어할 수 있게 된다.

[0009] 이와 관련하여, 한국공개특허공보 제 10-2021-0030534호는 “블록체인 네트워크를 기반으로 한 의약품 관리 시스템”에 관한 것으로서, 블록체인 네트워크를 구성하는 노드에서 의약품 및 의약품의 거래에 대한 데이터가 발생되면, 해당 노드는 데이터를 자신의 고유한 속성을 이용하여 데이터에 속성 기반의 암호화 알고리즘을 적용하여 암호화시킨 후, 암호화된 데이터를 포함하는 트랜잭션을 생성하여 블록체인 네트워크에 전파하고, 블록체인 네트워크에서 사전 설정된 합의 과정을 통하여 블록을 생성하여 블록체인에 기록하여 공유하는 기술을 제안하였다.

[0010] 전술한 특허에서는, 각 노드에게 고유한 속성을 부여하고, CP-ABE 알고리즘을 적용하여 모든 데이터들을 속성을 이용하여 암호화 및 복호화시킴으로써, 기존 블록체인 특성인 투명성과 데이터의 무결성뿐만 아니라, 동시에 개인정보 보호 및 데이터에 대한 접근 제어까지 할 수 있게 된다.

[0011] 하지만, 이와 같이 속성 기반 암호화를 사용하는 경우, 암호화를 하려는 데이터의 크기가 커지거나 접근 제어 트리의 노드수가 많아질수록 암호화 및 복호화에 걸리는 시간이 증대되는 문제가 발생한다. 속성 기반 암호화 방법은 일반적인 대칭키 알고리즘을 이용한 암호화 방법에 비해 암호화 및 복호화의 시간이 적게는 10배 많게는 100 배 이상 소요될 수 있다. 특히, 대용량 데이터를 저장하는 경우, 속성 기반 암호화를 하는 과정에서 많은 오버헤드(overhead)가 발생하게 된다. 더 나아가, 블록체인을 이용한 클라우드 스토리지에서 데이터를 속성 기반 암호화함으로써 암호화 및 복호화에 걸리는 시간이 증가하게 되고, 이로 인해 클라우드 스토리지의 성능이 저하되는 문제점을 발생하게 된다.

## 선행기술문헌

### 특허문헌

- [0012] (특허문헌 0001) 한국등록특허공보 제 10-2307574호  
(특허문헌 0002) 한국공개특허공보 제 10-2021-0030534호

## 발명의 내용

### 해결하려는 과제

[0013] 전술한 문제점을 해결하기 위한 본 발명의 목적은 대칭키 알고리즘과 속성 기반 암호화 알고리즘을 이용하여 데이터를 암호화하여 블록체인 기반 클라우드 스토리지에 데이터를 안전하게 저장하고 사용자의 접근 제어를 할 수 있도록 함과 동시에 데이터의 암호화 및 복호화의 처리 속도를 향상시킬 수 있도록 함으로써, 블록체인 기반 클라우드 스토리지의 성능을 향상시킬 수 있도록 한 블록체인 기반 클라우드 스토리지 시스템 및 상기 시스템에서의 데이터 접근 권한 제어 방법을 제공하는 것을 목적으로 한다.

### 과제의 해결 수단

[0014] 전술한 기술적 과제를 달성하기 위한 본 발명의 제1 특징에 따른 블록체인 기반의 클라우드 스토리지 시스템은, 블록체인을 갖는 복수 개의 사용자 노드들을 구비하는 블록체인 네트워크; 데이터에 대한 접근 권한을 갖는 사용자들의 속성들을 포함하는 접근 제어 트리를 구비하고, 대칭키를 생성하고, 상기 접근 제어 트리를 이용하여

상기 대칭키를 속성 기반 암호화하고, 속성 기반 암호화된 대칭키를 상기 블록체인 네트워크의 블록체인에 저장하는 키 관리자 노드; 상기 대칭키를 이용하여 암호화된 데이터를 저장하는 상기 클라우드 스토리지;를 구비하여, 대칭키로 암호화된 데이터를 클라우드 스토리지에 저장하고, 접근 제어 트리를 이용하여 속성 기반 암호화된 대칭키는 블록체인 네트워크의 블록체인에 저장한다.

[0015] 전술한 제1 특징에 따른 블록체인 기반의 클라우드 스토리지 시스템에 있어서, 상기 사용자 노드는 키 관리자 노드에게 자신의 속성을 제공하고, 키 관리자 노드로부터 속성 기반 암호화에 필요한 비밀키 및 공개키를 발급받고, 상기 발급된 비밀키를 이용하여 블록체인에 저장된 속성 기반 암호화된 대칭키를 복호화하고, 상기 복호화된 대칭키를 이용하여 데이터를 암호화하고, 암호화된 데이터를 상기 클라우드 스토리지에 저장하거나, 상기 복호화된 대칭키를 이용하여 상기 클라우드 스토리지에 저장된 암호화된 데이터를 복호화하는 것이 바람직하다.

[0016] 본 발명의 제2 특징에 따른 블록체인 기반의 클라우드 스토리지 시스템에서의 접근 권한 제어 방법은, (a) 키 관리자 노드가 데이터에 대한 접근 권한을 갖는 사용자들의 속성을 포함하는 접근 제어 트리를 사전 등록하여 구비하고, 대칭키를 생성하고, 상기 접근 제어 트리를 이용하여 상기 대칭키를 속성 기반 암호화하고, 상기 속성 기반 암호화된 대칭키를 블록체인 네트워크의 블록체인에 저장하는 단계; (b) 블록체인 네트워크를 구성하는 사용자 노드가 대칭키를 이용하여 암호화된 데이터를 클라우드 스토리지에 저장하는 단계; 및 (c) 블록체인 네트워크를 구성하는 사용자 노드가 클라우드 스토리지에 저장된 암호화된 데이터를 대칭키를 이용하여 복호화하는 단계;를 구비하고, 대칭키로 암호화된 데이터를 클라우드 스토리지에 저장하고, 접근 제어 트리를 이용하여 속성 기반 암호화된 대칭키는 블록체인 네트워크의 블록체인에 저장한다.

[0017] 전술한 제2 특징에 따른 블록체인 기반의 클라우드 스토리지 시스템에서의 접근 권한 제어 방법에 있어서, 상기 (b) 단계는, 상기 블록체인 네트워크를 구성하는 사용자 노드가, 키 관리자 노드에게 자신의 속성을 제공하고, 키 관리자 노드로부터 속성 기반 암호화에 필요한 비밀키 및 공개키를 발급받고, 상기 발급된 비밀키를 이용하여 블록체인에 저장된 속성 기반 암호화된 대칭키를 복호화하고, 상기 복호화된 대칭키를 이용하여 데이터를 암호화하고, 암호화된 데이터를 상기 클라우드 스토리지에 저장하는 것이 바람직하다.

[0018] 전술한 제2 특징에 따른 블록체인 기반의 클라우드 스토리지 시스템에서의 접근 권한 제어 방법에 있어서, 상기 (b) 단계는, 상기 사용자 노드가, 키 관리자 노드에게 자신의 속성을 제공하고, 키 관리자 노드로부터 속성 기반 암호화에 필요한 비밀키 및 공개키를 발급받고, 상기 발급된 비밀키를 이용하여 블록체인에 저장된 속성 기반 암호화된 대칭키를 복호화하고, 상기 복호화된 대칭키를 이용하여 상기 클라우드 스토리지에 저장된 암호화된 데이터를 복호화하는 것이 바람직하다.

## 발명의 효과

[0019] 본 발명에 따른 블록체인 기반의 클라우드 스토리지 시스템에서의 데이터 접근 권한 제어 방법은, 대칭키 알고리즘을 이용하여 데이터를 암호화시키고 암호화된 데이터를 클라우드 스토리지에 저장함으로써, 속성 기반 암호화 방법만에 비하여 매우 빠른 속도로 데이터를 암호화 및 복호화시킬 수 있게 되어 클라우드 스토리지의 처리 성능을 월등히 향상시킬 수 있게 된다.

[0020] 또한, 본 발명에 따른 블록체인 기반의 클라우드 스토리지 시스템에서의 데이터 접근 권한 제어 방법은, 접근 제어 트리를 이용하여 대칭키를 속성 기반 암호화시켜 블록체인 네트워크의 블록체인에 저장함으로써, 키 노출을 방지함과 동시에 암호화된 데이터를 클라우드 스토리지에 안전하게 저장 및 관리할 수 있게 된다.

[0021] 또한, 본 발명에 따른 블록체인 기반의 클라우드 스토리지 시스템에서의 데이터 접근 권한 제어 방법은, 데이터를 암호화시킨 대칭키를 접근 제어 트리를 이용하여 속성 기반 암호화시키고, 접근 제어 트리를 만족하는 속성을 가진 사용자 노드에게만 암호화된 대칭키를 복호화시킬 수 있도록 함으로써, 데이터에 대한 사용자의 접근 권한을 제어할 수 있게 된다.

[0022] 이와 같이 본 발명에 따른 접근 권한 제어 방법 및 시스템은, 속성 기반 암호화 알고리즘과 대칭키 알고리즘을 모두 적절하게 사용함으로써, 속성 기반 암호화의 접근 제어 방식에 대한 장점과 대칭키 알고리즘의 시간적인 처리 속도의 장점을 모두 취할 수 있게 된다. 즉, 본 발명에 따른 접근 권한 제어 방법은, 클라우드 스토리지에 저장된 암호화된 데이터를 접근 권한을 갖는 사용자만이 복호화할 수 있도록 제어할 수 있을 뿐만 아니라, 암호화 및 복호화에 소요되는 시간을 감소시켜 처리 속도를 증가시킴으로써 클라우드 스토리지의 처리 성능을 향상시킬 수 있게 된다.

[0023] 한편, 암호화 및 복호화에 걸리는 시간은, 속성 기반 암호화의 경우 데이터의 크기와 접근 제어 트리의 노드 수

에 비례하여 증가하고, 대칭키 알고리즘의 경우 데이터의 크기에만 영향을 받는데, 대칭키 알고리즘을 이용하는 방법이 속성 기반 암호화 방법보다 통상적으로 시간적으로 적게는 10배, 많게는 100배 이상 빠른 처리속도를 갖는다. 따라서, 본 발명에서는 암호화할 데이터는 대칭키로 암호화함으로써 처리 속도면에서 시간적인 이득을 얻게 된다. 또한, 본 발명에서는 대칭키를 속성 기반 암호화하여 블록체인 네트워크에 공유함으로써, 대칭키 자체는 128bits 또는 256bits의 아주 작은 용량으로 속성 기반 암호화의 장점인 접근 제어 특성을 그대로 가질 수 있게 된다. 따라서, 본 발명은 대칭키 알고리즘의 장점인 빠른 처리 속도의 특성과 함께 속성 기반 암호화의 접근 제어의 장점도 함께 취할 수 있게 된다. 이러한 방식을 사용한다면 기존 블록체인 기반 클라우드 스토리지에서 더욱 더 효율적인 방식으로 데이터를 안전하게 관리할 수 있게 된다.

### 도면의 간단한 설명

[0024]

도 1은 본 발명의 바람직한 실시예에 따른 블록체인 기반 클라우드 스토리지 시스템에서의 접근 권한 제어 방법을 순차적으로 도시한 흐름도이다.

도 2는 본 발명의 바람직한 실시예에 따른 블록체인 기반 클라우드 스토리지 시스템에 있어서, 키 관리자 노드가 대칭키를 속성 기반 암호화시켜 블록체인 네트워크에 저장하는 과정을 도시한 모식도이다.

도 3은 본 발명의 바람직한 실시예에 따른 블록체인 기반 클라우드 스토리지 시스템에 있어서, 사용자가 암호화된 대칭키를 복호화하는 과정을 도시한 모식도이다.

도 4는 본 발명의 바람직한 실시예에 따른 블록체인 기반 클라우드 스토리지 시스템에 있어서, 사용자가 대칭키를 이용하여 암호화된 데이터를 복호화하거나 데이터를 암호화하는 과정을 도시한 모식도이다.

도 5는 속성 기반 암호화 알고리즘에서, 데이터를 암호화하는데 걸리는 시간을 도시한 그래프이다.

도 6은 속성 기반 암호화 알고리즘에서, 데이터를 복호화하는데 걸리는 시간을 도시한 그래프이다.

도 7은 속성 기반 암호화 알고리즘에서 도 5의 데이터의 암호화 시간 및 도 6의 복호화 시간을 비교하기 위하여 도시한 그래프이다.

도 8은 대칭키 알고리즘을 이용한 암호화 방식에 있어서, 암호화에 걸리는 시간을 도시한 그래프이다.

도 9는 도 5의 속성 기반 암호화 알고리즘에서 데이터를 암호화시키는 데 걸리는 시간과 도 8의 대칭키 알고리즘에서 데이터를 암호화시키는 데 걸리는 시간을 비교하기 위하여 도시한 그래프이다.

### 발명을 실시하기 위한 구체적인 내용

[0025]

이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예에 따른 블록체인 기반 클라우드 스토리지 시스템 및 상기 시스템에서의 접근 권한 제어 방법을 구체적으로 설명한다.

[0026]

본 발명의 바람직한 실시예에 따른 블록체인 기반 클라우드 스토리지 시스템은, 블록체인을 갖는 복수 개의 사용자 노드들을 구비하는 블록체인 네트워크, 키 관리자 노드 및 클라우드 스토리지를 구비하고, 대칭키로 암호화된 데이터를 클라우드 스토리지에 저장하고, 접근 제어 트리를 이용하여 속성 기반 암호화된 대칭키는 블록체인 네트워크의 블록체인에 저장하는 것을 특징으로 한다.

[0027]

상기 키 관리자 노드는, 데이터에 대한 접근 권한을 갖는 사용자들의 속성들을 포함하는 접근 제어 트리를 사전 등록하여 구비하고, 대칭키를 생성하고, 상기 접근 제어 트리를 이용하여 상기 대칭키를 속성 기반 암호화하고, 속성 기반 암호화된 대칭키를 상기 블록체인 네트워크의 블록체인에 저장한다. 상기 클라우드 스토리지는 상기 대칭키를 이용하여 암호화된 데이터를 저장한다.

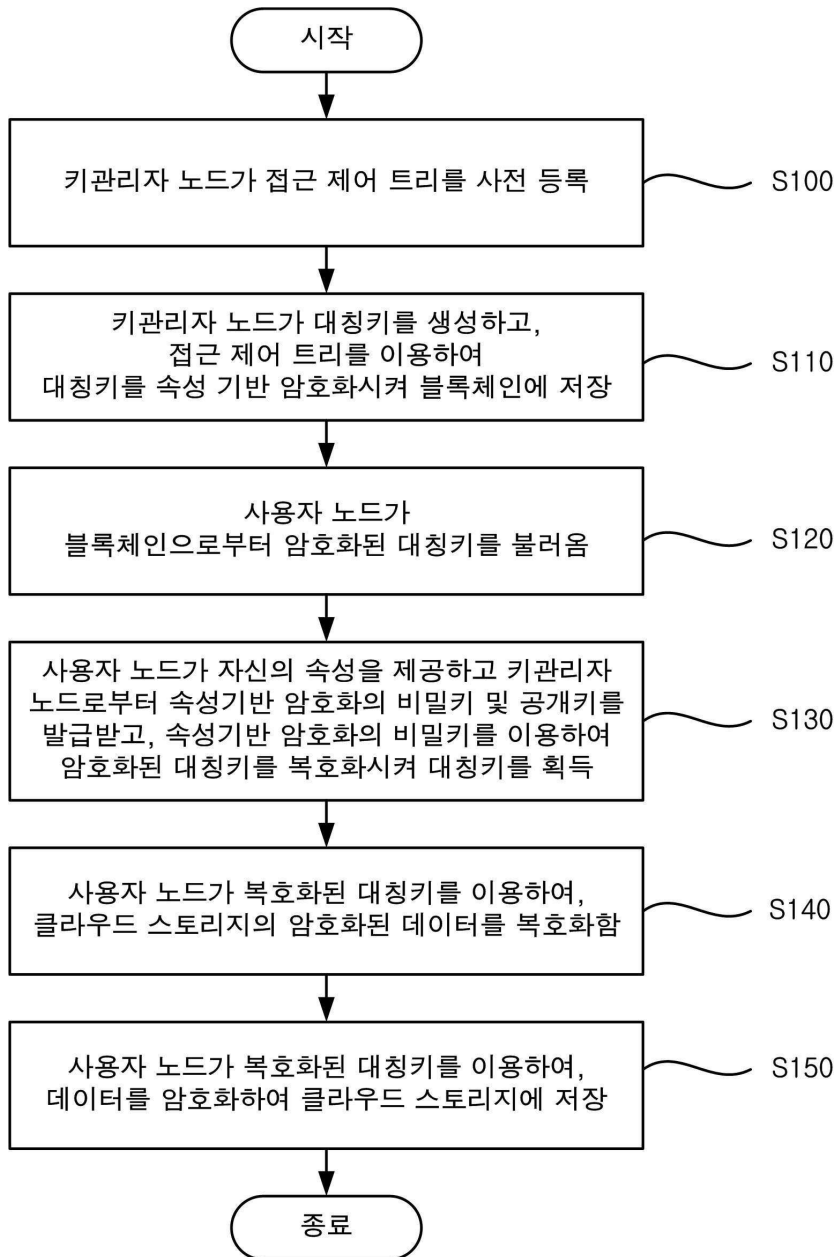
[0028]

도 1은 본 발명의 바람직한 실시예에 따른 블록체인 기반 클라우드 스토리지 시스템에서의 접근 권한 제어 방법을 도시한 흐름도이다. 도 1을 참조하면, 본 발명에 따른 접근 권한 제어 방법은, 먼저 키 관리자 노드가 데이터에 대한 접근 권한을 갖는 사용자들의 속성을 포함하는 접근 제어 트리를 사전 등록하여 구비하고(단계 100), 상기 접근 제어 트리를 이용하여 속성 기반 암호화된 대칭키를 블록체인 네트워크의 블록체인에 저장한다(단계 110). 다음, 사용자 노드는 블록체인 네트워크의 블록체인으로부터 암호화된 대칭키를 불러오고(단계 120), 자신의 속성 정보를 이용하여 상기 암호화된 대칭키를 복호화하여 대칭키를 획득한다(단계 130). 다음, 사용자 노드는 대칭키를 이용하여 데이터를 암호화하여 클라우드 스토리지에 저장하거나(단계 140), 클라우드 스토리지의 암호화된 데이터를 복호화한다(단계 150). 이하, 전술한 각 단계들에 대하여 보다 구체적으로 설명한다.

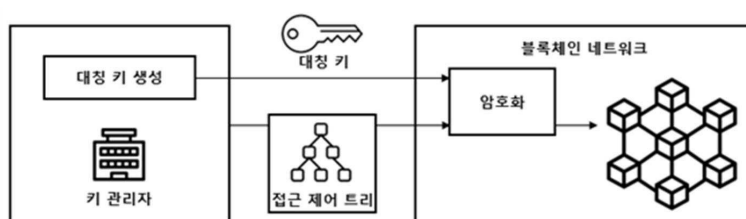
- [0029] 도 2는 본 발명의 바람직한 실시예에 따른 블록체인 기반 클라우드 스토리지 시스템에 있어서, 키 관리자 노드가 속성 기반 암호화된 대칭키를 블록체인 네트워크에 저장하는 과정을 도시한 모식도이다. 이하, 도 2를 참조하여 전술한 단계 100 및 단계 110을 보다 구체적으로 설명한다. 상기 키 관리자 노드는 데이터에 대한 접근 권한을 갖는 사용자들의 속성을 포함하는 접근 제어 트리를 사전 등록하여 구비한다. 상기 키 관리자 노드는 대칭키를 생성하며, 생성된 대칭키를 상기 접근 제어 트리를 이용하여 속성 기반 암호화한다. 다음, 속성 기반 암호화된 대칭키를 블록체인 네트워크의 블록체인에 저장한다. 이와 같이, 본 발명에 따른 접근 권한 제어 방법은 암호화된 대칭키를 블록체인 네트워크에 저장함으로써 모두에게 공유하고, 접근 제어 트리 구조를 만족하는 사용자만이 암호화된 대칭키를 복호화할 수 있도록 한다.
- [0030] 도 3은 본 발명의 바람직한 실시예에 따른 블록체인 기반 클라우드 스토리지 시스템에 있어서, 사용자가 암호화된 대칭키를 복호화하는 과정을 도시한 모식도이다. 이하, 도 3을 참조하여 전술한 단계 120 및 단계 130을 보다 구체적으로 설명한다. 상기 사용자 노드는 키 관리자 노드에게 자신의 속성을 제공하고, 키 관리자 노드로부터 속성 기반 암호화에 필요한 비밀키 및 공개키를 발급받는다. 상기 사용자 노드는 상기 블록체인 네트워크로부터 속성 기반 암호화된 대칭키를 가져온 후, 상기 발급된 자신의 비밀키를 이용하여 상기 속성 기반 암호화된 대칭키를 복호화함으로써, 대칭키를 얻게 된다.
- [0031] 도 4는 본 발명의 바람직한 실시예에 따른 블록체인 기반 클라우드 스토리지 시스템에 있어서, 사용자가 대칭키를 이용하여 암호화된 데이터를 복호화하거나 데이터를 암호화하는 과정을 도시한 모식도이다. 이하, 도 4를 참조하여 단계 140 및 단계 150을 보다 구체적으로 설명한다. 사용자 노드는 상기 복호화된 대칭키를 이용하여 데이터를 암호화하고, 암호화된 데이터를 상기 클라우드 스토리지에 저장함으로써, 대칭키로 암호화된 데이터를 클라우드 스토리지에 저장한다(단계 140). 한편, 사용자 노드는 클라우드 스토리지에 저장된 암호화된 데이터를 읽어와서 상기 복호화된 대칭키를 이용하여 상기 암호화된 데이터를 복호화시킨다(단계 150).
- [0032] 도 5는 속성 기반 암호화 알고리즘에서, 데이터를 암호화하는데 걸리는 시간을 도시한 그래프이다. 도 5를 참조하면, 속성 기반 암호화 알고리즘을 이용하여 데이터를 암호화시키는 시간은, 접근 제어 트리(Access Tree)의 노드 수와 데이터의 크기에 영향을 받기는 하나, Access Tree의 노드 수에는 거의 영향을 받지 않고 데이터의 크기에 많은 영향을 받는다.
- [0033] 도 6은 속성 기반 암호화 알고리즘에서, 데이터를 복호화하는데 걸리는 시간을 도시한 그래프이다. 도 6을 참조하면, 속성 기반 암호화 알고리즘을 이용하여 데이터를 복호화시키는 시간은, 도 5와 마찬가지로 접근 제어 트리의 노드 수와 데이터의 크기에 영향을 받기는 하나, 데이터 크기에는 거의 영향을 받지 않고 접근 제어 트리의 노드 수에는 영향을 많이 받는다.
- [0034] 도 7은 속성 기반 암호화 알고리즘에서 도 5의 데이터의 암호화 시간 및 도 6의 복호화 시간을 비교하기 위하여 도시한 그래프이다. 도 7을 참조하면, 속성 기반 암호화에서 복호화에 걸리는 시간보다 암호화에 걸리는 시간이 훨씬 많음을 확인할 수 있다.
- [0035] 도 8은 대칭키 알고리즘을 이용한 암호화 방식에 있어서, 암호화에 걸리는 시간을 도시한 그래프이다. 도 8을 참조하면, 대칭키 알고리즘을 이용하여 데이터를 암호화하는데 걸리는 시간은 접근 제어 트리를 사용하지 아니하므로 노드 수에는 영향을 전혀 받지 않고 데이터의 크기에만 영향을 받게 된다.
- [0036] 도 9는 도 5의 속성 기반 암호화 알고리즘에서 데이터를 암호화시키는 데 걸리는 시간과 도 8의 대칭키 알고리즘에서 데이터를 암호화시키는 데 걸리는 시간을 비교하기 위하여 도시한 그래프이다. 도 9를 참조하면, 데이터의 크기와 접근 제어 트리의 노드 수와는 관계없이, 대칭키 알고리즘을 이용한 암호화 방식이 속성 기반 암호화 방식에 비해 암호화시키는데 걸리는 시간이 월등히 짧으며 더욱 빠른 속도로 암호화를 시키게 된다.
- [0037] 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.

도면

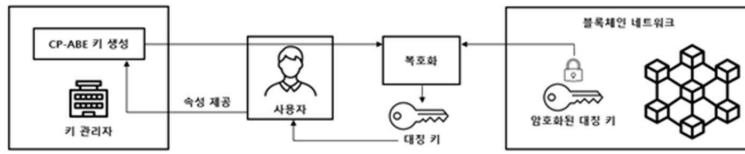
도면1



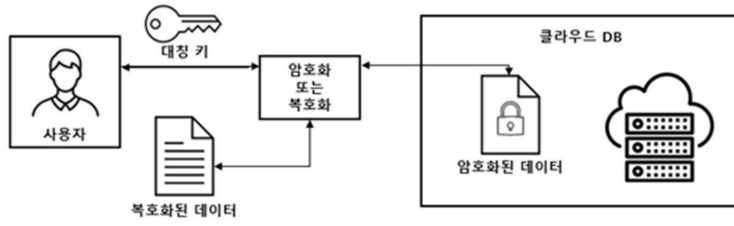
도면2



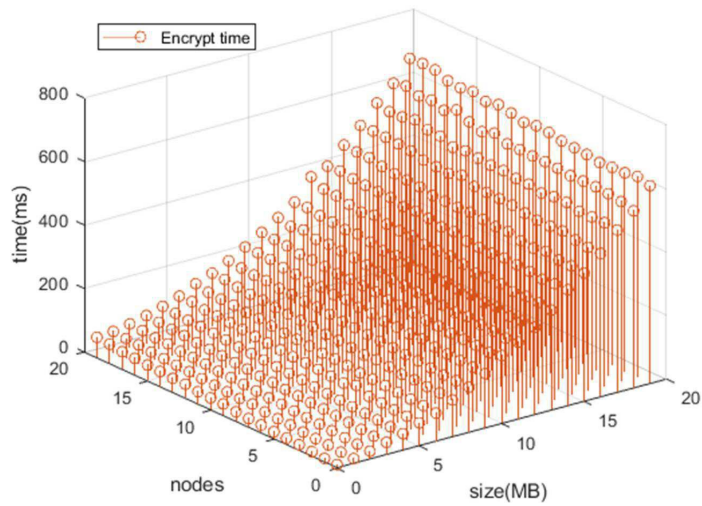
도면3



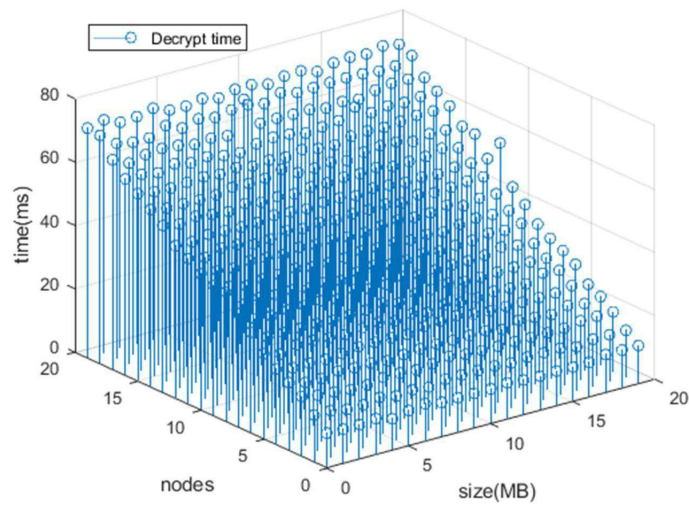
도면4



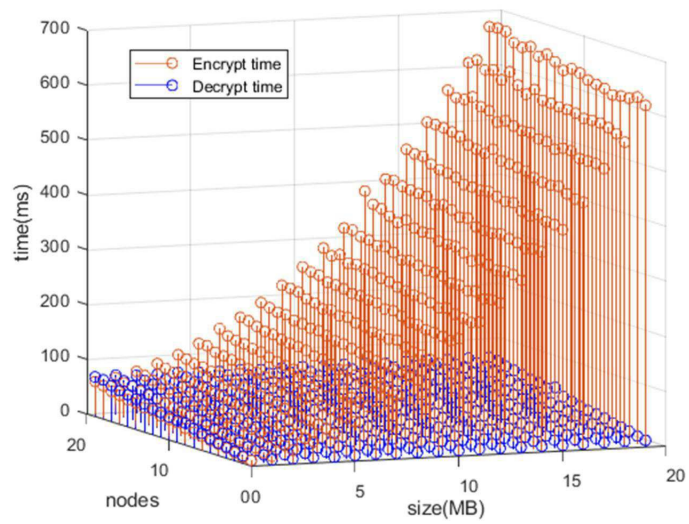
도면5



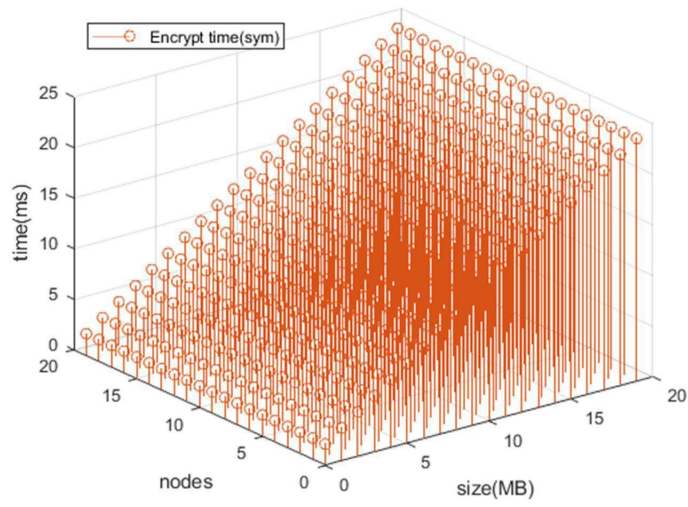
도면6



도면7



도면8



도면9

