(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0082444
(43) 공개일자 2024년06월11일

(51) 국제특허분류(Int. Cl.)
H04L 9/06 (2006.01) *H04L 67/1097* (2022.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
H04L 9/0631 (2013.01)
H04L 67/1097 (2022.05)
(21) 출원번호 10-2022-0165756
(22) 출원일자 2022년12월01일
심사청구일자 2022년12월01일

(71) 출원인
서강대학교산학협력단
서울특별시 마포구 백범로 35 (신수동, 서강대학교)
(72) 발명자
박수용
서울특별시 마포구 독막로 18 길 5, 101동 1001호 (상수동, 상수두산위브아파트)
서중원
서울특별시 서대문구 수색로8가길 11 한양빌라 201호
(74) 대리인
이지연

전체 청구항 수 : 총 15 항

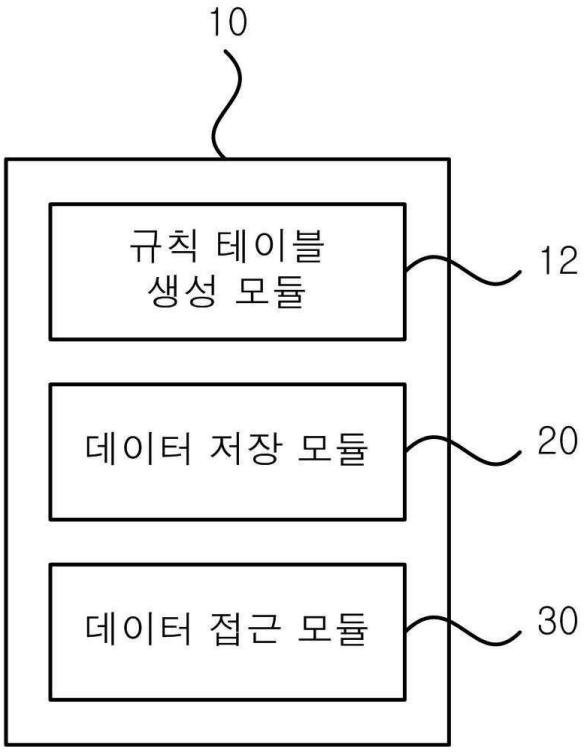
(54) 발명의 명칭 **블록체인을 기반으로 한 치환 암호화를 이용한 데이터 접근 제어 시스템, 장치 및 그 방법**

(57) 요 약

본 발명은 스마트 컨트랙트를 이용하여 블록체인 네트워크에 데이터를 저장하거나 블록체인 네트워크에 저장된 데이터에 접근하도록 구성된 데이터 접근 제어 장치 및 그 방법에 관한 것이다. 상기 데이터 접근 제어 장치는, 사전 설정된 3개의 요소들(3F)을 이용하여 치환 암호화 및 복호화에 사용될 규칙 테이블을 생성하는 규칙 테이블

(뒷면에 계속)

대 표 도 - 도3



생성 모듈; 데이터 제공자로부터 블록체인 네트워크에 저장할 데이터 및 3F값들을 제공받고, 3F 값들을 이용하여 생성된 규칙 테이블을 이용하여 데이터를 치환 암호화시키고, 상기 치환 암호화 데이터를 블록체인 네트워크에 저장하는 데이터 저장 모듈; 및 데이터 사용자로부터 데이터가 저장된 스마트 컨트랙트 주소 및 3F 값들을 제공받고, 블록체인 네트워크의 상기 스마트 컨트랙트 주소의 치환 암호화 데이터를 호출하고, 3F 값들을 이용하여 생성된 규칙 테이블을 이용하여 상기 호출된 치환 암호화 데이터를 역치환하여 복호화하는 데이터 접근 모듈;을 구비한다.

(52) CPC특허분류
H04L 9/0643 (2013.01)
H04L 9/32 (2022.08)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711152712
과제번호	2017-0-01628-006
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보통신방송혁신인재양성
연구과제명	적응형 블록체인 플랫폼 기술 개발 및 전문 인력 양성
기 여 율	1/1
과제수행기관명	서강대학교산학협력단
연구기간	2022.01.01 ~ 2022.12.31

명 세 서

청구범위

청구항 1

스마트 컨트랙트를 이용하여 블록체인 네트워크에 데이터를 저장하거나 블록체인 네트워크에 저장된 데이터에 접근하도록 구성된 데이터 접근 제어 장치에 있어서,

사전 설정된 3개의 요소들을 이용하여 치환 암호화 및 복호화에 사용될 규칙 테이블을 생성하는 규칙 테이블 생성 모듈;

데이터 제공자로부터 블록체인 네트워크에 저장할 데이터 및 상기 설정된 3개의 요소들에 대한 값들을 제공받고, 상기 3개의 요소들의 값들을 이용하여 생성된 규칙 테이블을 이용하여 데이터를 치환 암호화시키고, 상기 치환 암호화된 데이터를 블록체인 네트워크에 저장하는 데이터 저장 모듈; 및

데이터 사용자로부터 데이터가 저장된 스마트 컨트랙트 주소 및 상기 설정된 3개의 요소들에 대한 값들을 제공받고, 스마트 컨트랙트를 통해 블록체인 네트워크의 상기 스마트 컨트랙트 주소의 치환 암호화 데이터를 호출하고, 상기 3개의 요소에 대한 값들을 이용하여 생성된 규칙 테이블을 이용하여 상기 호출된 치환 암호화 데이터를 역치환하여 복호화하는 데이터 접근 모듈;

을 구비하는 것을 특징으로 하는 블록체인을 기반으로 한 치환 암호화를 이용한 데이터 접근 제어 장치.

청구항 2

제1항에 있어서, 상기 사전 설정된 3개의 요소는,

데이터 제공자의 블록체인 개인키를 해시 알고리즘을 적용하여 얻은 데이터 제공자의 개인키의 해시값(HRoot);

데이터 사용자에 의해 임의로 생성되고, 사전 설정된 개수(n) 이상의 요소로 구성된 값(Salt); 및

데이터 제공자와 데이터 사용자의 합의에 의해 생성되고, 사전 설정된 개수(n)의 숫자들로 구성된 집합(NKey);

인 것을 특징으로 하는 블록체인을 기반으로 한 치환 암호화를 이용한 데이터 접근 제어 장치.

청구항 3

제1항에 있어서, 상기 규칙 테이블 생성 모듈이 생성한 규칙 테이블은,

사전 설정된 자리수로 표현된 비트값들(Bit Value);

데이터 제공자의 HRoot를 NKey값을 이용하여 해시하여 상기 비트값들에 대응되도록 설정된 제1 치환 설정값들; 및

데이터 사용자의 Salt값과 NKey값을 매칭시킨 뒤 재정렬시킨 후, 상기 비트값들에 대응되도록 설정된 제2 치환 설정값들;

을 구비하는 것을 특징으로 하는 블록체인을 기반으로 한 치환 암호화를 이용한 데이터 접근 제어 장치.

청구항 4

제1항에 있어서, 상기 데이터 저장 모듈은,

데이터 제공자로부터 입력된 데이터를 비트 형태로 변환시키고, 비트값을 사전 설정된 자리수로 분할하여 복수개의 단위 비트(SB)들을 생성하는 분할 유닛;

규칙 테이블을 이용하여 상기 복수 개의 단위 비트(SB)들을 치환시켜 치환 암호화 데이터(Xst)를 생성하는 데이터 치환 유닛; 및

치환 암호화 데이터를 특정 크기로 분할하고, 분할된 데이터 유닛들을 스마트 컨트랙트를 통해 블록체인 네트워크에 배포하는 배포 유닛;

을 구비하는 것을 특징으로 하는 블록체인을 기반으로 한 치환 암호화를 이용한 데이터 접근 제어 장치.

청구항 5

제1항에 있어서, 상기 데이터 접근 모듈은,

데이터 사용자로부터 입력된 스마트 컨트랙트 주소를 이용하여 블록체인 네트워크로부터 치환 암호화 데이터를 호출하는 호출 유닛;

HRoot 값과 Salt를 사용하여 데이터 사용자의 접근 권한을 확인하는 검증 유닛; 및

규칙 테이블을 이용하여, 상기 호출된 치환 암호화 데이터를 역치환하여 복호화하는 복원 유닛;

을 구비하는 것을 특징으로 하는 블록체인을 기반으로 한 치환 암호화를 이용한 데이터 접근 제어 장치.

청구항 6

컴퓨팅 시스템에서 실행되는 프로그램에 의해 구현된 데이터 접근 제어 방법에 있어서,

사전 설정된 3개의 요소를 이용하여 치환 암호화 및 복호화에 사용될 규칙 테이블을 생성하는 규칙 테이블 생성 단계; 및

데이터 제공자로부터 블록체인 네트워크에 저장할 데이터 및 상기 설정된 3개의 요소에 대한 값들을 제공받고, 상기 3개의 요소에 대한 값들을 이용하여 생성된 규칙 테이블을 이용하여 데이터를 치환 암호화시키고, 상기 치환 암호화된 데이터를 블록체인 네트워크에 저장하는 데이터 저장 단계;

를 구비하는 것을 특징으로 하는 블록체인을 기반으로 한 치환 암호화를 이용한 데이터 접근 제어 방법.

청구항 7

제6항에 있어서, 상기 사전 설정된 3개의 요소는,

데이터 제공자의 블록체인 개인키를 해시 알고리즘을 적용하여 얻은 데이터 제공자의 개인키의 해시값(HRoot);

데이터 사용자에 의해 임의로 생성되고, 사전 설정된 개수(n) 이상의 요소로 구성된 값(Salt); 및

데이터 제공자와 데이터 사용자의 합의에 의해 생성되고, 사전 설정된 개수(n)의 숫자들로 구성된 집합(NKey);

인 것을 특징으로 하는 블록체인을 기반으로 한 치환 암호화를 이용한 데이터 접근 제어 방법.

청구항 8

제6항에 있어서, 상기 데이터 저장 단계는,

데이터 제공자로부터 입력된 데이터를 비트 형태로 변환시키고, 비트값을 사전 설정된 자리수로 분할하여 복수 개의 단위 비트(SB)들을 생성하는 단계;

규칙 테이블을 이용하여 상기 복수 개의 단위 비트(SB)들을 치환시켜 치환 암호화 데이터(Xst)를 생성하는 단계; 및

치환 암호화 데이터를 특정 크기로 분할하고, 분할된 데이터 유닛들을 스마트 컨트랙트를 통해 블록체인 네트워크에 배포하는 단계;

을 구비하는 것을 특징으로 하는 블록체인을 기반으로 한 치환 암호화를 이용한 데이터 접근 제어 방법.

청구항 9

제6항에 있어서, 상기 데이터 접근 제어 방법은,

데이터 사용자로부터 데이터가 저장된 스마트 컨트랙트 주소 및 상기 설정된 3개의 요소에 대한 값들을 제공받고, 스마트 컨트랙트를 통해 블록체인 네트워크의 상기 스마트 컨트랙트 주소의 치환 암호화된 데이터를 획득하고, 상기 3개의 요소에 대한 값들을 이용하여 생성된 규칙 테이블을 이용하여 상기 치환 암호화된 데이터를 복원하는 데이터 접근 단계;

를 더 구비하는 것을 특징으로 하는 블록체인을 기반으로 한 치환 암호화를 이용한 데이터 접근 제어 방법.

청구항 10

제9항에 있어서, 상기 데이터 접근 단계는,

데이터 사용자로부터 입력된 스마트 컨트랙트 주소를 통해 블록체인 네트워크로부터 치환 암호화 데이터를 호출하는 단계;

HRoot 값과 Salt를 사용하여 데이터 사용자의 접근 권한을 검증하는 단계; 및

규칙 테이블을 이용하여, 상기 호출된 치환 암호화 데이터를 역치환시켜 복원하는 단계;

를 구비하는 것을 특징으로 하는 블록체인을 기반으로 한 치환 암호화를 이용한 데이터 접근 제어 방법.

청구항 11

데이터 제공자의 요청에 따라 데이터를 치환 암호화시켜 블록체인 네트워크에 저장하거나, 데이터 사용자의 요청에 따라 블록체인 네트워크에 저장된 치환 암호화된 데이터를 복호화하여 제공하는 데이터 접근 제어 장치; 및

상기 데이터 접근 제어 장치로부터의 요청에 따라, 스마트 컨트랙트를 통해 블록체인에 데이터를 저장하거나, 블록체인에 저장된 데이터를 호출하여 제공하는 블록체인 네트워크;를 구비하고,

상기 데이터 접근 제어 장치는,

사전 설정된 3개의 요소를 이용하여 암호화 및 복호화에 사용될 규칙 테이블을 생성하는 규칙 테이블 생성 모듈;

데이터 제공자로부터 블록체인 네트워크에 저장할 데이터 및 상기 설정된 3개의 요소에 대한 값들을 제공받고, 상기 3개의 요소에 대한 값들을 이용하여 생성된 규칙 테이블을 이용하여 데이터를 치환 암호화시키고, 상기 치환 암호화된 데이터를 상기 스마트 컨트랙트를 통해 블록체인 네트워크에 저장하는 데이터 저장 모듈; 및

데이터 사용자로부터 데이터가 저장된 스마트 컨트랙트 주소 및 상기 설정된 3개의 요소에 대한 값들을 제공받고, 스마트 컨트랙트를 통해 블록체인 네트워크의 상기 스마트 컨트랙트 주소의 치환 암호화된 데이터를 획득하고, 상기 3개의 요소에 대한 값들을 이용하여 생성된 규칙 테이블을 이용하여 상기 치환 암호화된 데이터를 복원하는 데이터 접근 모듈;

을 구비하는 것을 특징으로 하는 블록체인을 기반으로 한 치환 암호화를 이용한 데이터 접근 제어 시스템.

청구항 12

제11항에 있어서, 상기 사전 설정된 3개의 요소는,

데이터 제공자의 블록체인 개인키를 해시 알고리즘을 적용하여 얻은 데이터 제공자의 개인키의 해시값(HRoot);

데이터 사용자가 임의로 생성되고, 사전 설정된 개수(n) 이상의 요소로 구성된 값(Salt); 및

데이터 제공자와 데이터 사용자의 합의에 의해 생성되고, 사전 설정된 개수(n)의 숫자들로 구성된 집합(NKey);

인 것을 특징으로 하는 블록체인을 기반으로 한 치환 암호화를 이용한 데이터 접근 제어 시스템.

청구항 13

제11항에 있어서, 상기 데이터 저장 모듈은,

데이터 제공자로부터 입력된 데이터를 비트 형태로 변환시키고, 비트값을 사전 설정된 자리수로 분할하여 복수개의 단위 비트(SB)들을 생성하는 분할 유닛;

규칙 테이블을 이용하여 상기 복수 개의 단위 비트(SB)들을 치환시켜 치환 암호화 데이터(Xst)를 생성하는 데이터 치환 유닛; 및

치환 암호화 데이터를 특정 크기로 분할하고, 분할된 데이터 유닛들을 스마트 컨트랙트를 통해 블록체인 네트워크에 배포하는 배포 유닛;

을 구비하는 것을 특징으로 하는 블록체인을 기반으로 한 치환 암호화를 이용한 데이터 접근 제어 시스템.

청구항 14

제11항에 있어서, 상기 데이터 접근 모듈은,

데이터 사용자로부터 입력된 스마트 컨트랙트 주소를 통해 블록체인 네트워크로부터 치환 암호화 데이터를 호출하는 호출 유닛;

HRoot 값과 Salt를 사용하여 데이터 사용자의 접근 권한을 확인하는 검증 유닛; 및

규칙 테이블을 이용하여, 상기 호출된 치환 암호화 데이터를 역치환시켜 복원하는 복원 유닛;

을 구비하는 것을 특징으로 하는 블록체인을 기반으로 한 치환 암호화를 이용한 데이터 접근 제어 시스템.

청구항 15

제11항에 있어서, 상기 블록체인 네트워크의 스마트 컨트랙트는,

Mother 컨트랙트와 Child 컨트랙트로 구성된 이중 구조의 스마트 컨트랙트이며,

상기 Mother 컨트랙트는 사용자와 직접 상호 작용하고, Child 컨트랙드의 주소를 관리하는 스마트 컨트랙트이며,

상기 Child 컨트랙트는 데이터를 저장하고, 저장하고 있는 데이터를 반환하는 컨트랙트인 것을 특징으로 하는 블록체인을 기반으로 한 치환 암호화를 이용한 데이터 접근 제어 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 블록체인을 기반으로 한 치환 암호화를 이용한 데이터 접근 제어 시스템에 관한 것으로서, 더욱 구체적으로는 메타버스상의 사용자에 대한 개인 정보 보호를 위하여, 규칙 테이블을 이용하여 사용자에 대한 개인정보를 치환 암호화를 한 후 스마트 컨트랙트를 통해 블록체인에 저장함으로써, 관리자의 개입없이 개인 정보를 암호화 및 복호화할 뿐만 아니라, RSA 암호화 방식에 비하여 암호화 및 복호화의 속도를 향상시킬 수 있도록 구성된 데이터 접근 제어 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 코로나로 인한 전 세계적인 판데믹 사태는 사람들의 생활을 변화시켰다. 사람들은 인터넷을 활용하여 회의를 하는것이 어색하지 않으며, 다양한 온라인 플랫폼들을 활용하여 생활하는 것에 익숙해졌다. 온라인과 오프라인의 경계가 점점 허물어져 가는 시대속에서 메타버스에 대한 사람들의 관심은 필연적인 현상이다. 메타버스에 대한 사람들의 관심은 다양한 연구들을 촉진시켰다.

[0003] 메타버스가 사람들의 관심을 받고 있지만, 진정으로 메타버스가 활성화되기 위해서는 AR/VR, AI, 블록체인 등과 같은 메타버스를 구성하는 다양한 요소 기술들의 발전이 필요하다. 특히, 가상 세계와 현실 세계가 연결된 메타버스 특성상 메타버스 사용자 개인정보를 보호하기 위한 연구들도 필요하다. 아바타의 정보가 현실 세계의 사용자 개인 정보와 직접적으로 연결될 수 있는 환경인 메타버스에서는 사용자 아바타 정보를 통해서 사용자의 사는 위치, 나이, 인종 등이 쉽게 노출될 수 있다.

[0004] 접근 통제 기법은 메타버스 사용자 개인정보를 보호하기 위한 하나의 방법이 될 수 있다. 접근 통제는 데이터에 접근하지 못하도록 제한하면서 감시하는 기술로서, IBAC (Identification Based Access Control), RBAC (Role Based Access Control), ABAC (Attribute Based Access Control) 등의 다양한 모델들이 존재한다. 하지만, 기존의 접근 제어 모델들은 접근 제어를 위해 관리자가 필요하며, 이는 단일 장애점 (Single Point of Failure) 한계를 가지고 있다. 메타버스는 불특정 다수의 사람들이 접근할 수 있는 환경이기 때문에 특정 관리자에 의한 단일 장애 문제는 중요한 문제가 될 수 있다.

[0005] 블록체인 기반 접근통제는 기존 접근제어 모델들이 가진 단일 장애점 문제를 해결하면서, 메타버스에서 새롭게 사용할 수 있는 개인정보 보호 기술이 될 수 있다. 하지만, 블록체인 네트워크에 저장된 데이터는 변경이 불가능하도록 설계되었기 때문에, 개인 정보 보호에 필요한 잊혀질 권리(Right to be forgotten)와 같은 요구 조건

을 만족시키지 못한다. 잊혀질 권리 등 개인 정보 보호 요구조건을 만족하기 위해서는 블록체인 네트워크에 저장되는 데이터를 최소화해야 한다. 이로 인하여, 개인정보 보호를 위한 블록체인 기반 접근 통제는 온체인과 오프체인을 분리하여 데이터를 저장해야 한다.

[0006] 개인 정보 보호를 위한 블록체인 기반 접근 통제에서는 지문, 신원정보 같이 직접적인 사용자 개인정보는 블록체인 네트워크 외부에 따로 관리하여, 개인 정보보호에 필요한 요구 조건을 만족시킬 수 있다. 또한, 블록체인에는 개인 정보가 담긴 저장소 위치 정보와 같은 데이터들을 기록하는 형태로 개인정보 보호를 위한 블록체인 기반 접근 통제를 할 수 있다. 블록체인은 개인 정보가 담긴 저장소에 위치 데이터를 암호화하여 블록체인 네트워크에 기록함으로써, 개인 정보 저장소 접근을 제한하면서, 오프체인 저장소에 관련된 정보를 무결하고 투명하게 관리할 수 있다.

[0007] 개인정보 보호를 위한 블록체인 기반의 접근 통제를 수행하기 위해서는 외부 저장소 위치와 같은 개인 정보와 직접적으로 관련이 없는 데이터만을 암호화하여 블록체인 네트워크에 저장하는 방안이 필요하다. 데이터를 암호화하는 방법은 대표적으로 대칭키를 활용한 방법과 비대칭키를 활용한 방법이 존재한다.

[0008] 대칭키는 하나의 키로 데이터를 암호화하는 것이며, 대표적으로는 AES가 존재한다. AES는 키 분배 및 관리가 관리자의 개입에 의해서 이루어진다는 한계가 있으며, 이는 관리자로 인해 암호화된 데이터가 노출될 수 있다는 위험이 존재한다. 이는 결국 관리자의 신뢰도에 따라서 접근 통제의 안전성이 위협받을 수 있다는 것을 의미한다.

[0009] 비대칭 키로 데이터를 암호화하는 방식은 개인키와 공개키를 사용하여 데이터 암호화 및 복호화를 하는 것으로, 대표적으로 RSA가 존재한다. RSA은 관리자의 존재없이 개인키와 공개키를 활용하여 데이터를 안전하게 암호화할 수 있다는 장점이 있다. 하지만, RSA은 암호화 및 복호화 속도가 느리다는 단점이 존재한다.

[0010] 기존의 블록체인 기반 접근 통제 연구들은 데이터 공유를 위한 접근통제, 개인정보 보호를 위한 접근통제 연구들로 분류할 수 있다. 각각의 연구들은 블록체인에 저장되는 데이터들을 각기 다른 방식으로 암호화하여 접근 제어하는 방안을 제안하였다. 하지만, 기존 연구들은 외부 관리자 혹은 특정 블록체인 노드에 의해서 접근 통제의 안전성이 위협받을 수 있다는 한계가 존재한다.

[0011] 한편, 몇몇 기본적인 학술 연구들로 시작된 블록체인은 비트코인의 탄생으로 사람들의 주목을 받게 되었다. 블록체인은 P2P 네트워크 (Peer-to-Peer Network) 기반의 분산형 저장소이다. 블록체인 네트워크에서 발생하는 데이터는 합의 알고리즘에 의해 '블록'이라고 불리는 형태로 저장되며, 생성된 블록들은 사슬 형태로 연결된다. 블록체인 참여자들은 동일한 블록을 가지고 있기 때문에 사용자들은 데이터에 대한 투명성 및 무결성을 보장받을 수 있다.

[0012] 또한, 블록체인 네트워크 기준으로 하여, 온체인과 오프체인으로 범위를 구분할 수 있다. 블록체인 네트워크를 '온체인'이라고 부르며, 블록체인 네트워크 외부를 '오프체인'이라 부른다. 오프체인에서는 블록체인과 상호 작용할 수 있는 관리자, 외부 저장소 등이 존재할 수 있다. 온체인에 저장되는 데이터들은 해시 알고리즘과 같은 블록체인의 기술적 특징에 의해서 무결성과 투명성을 보장받는다. 오프체인 요소들은 블록체인과 상호 작용이 가능하지만, 독립적으로 운영된다.

[0013] 해시 알고리즘(Hash Algorithm)은 임의의 데이터를 고정된 길이를 가진 데이터로 변환해주는 알고리즘을 의미한다. 해시 알고리즘은 특정 데이터의 무결성을 확인하기 위해서 확인할 수 있다. 해시 알고리즘은 비암호학적 해시 알고리즘(non-cryptographic hash algorithm)과 암호학적 해시 알고리즘으로 구분할 수 있다.

[0014] 비암호학적 해시 알고리즘은 암호학적 해시 알고리즘과 비교했을 때 안전성이 떨어질 수 있으나, 속도가 뛰어나서 블룸 필터 (bloom filters), 해시 테이블 등에서 사용된다. 대표적인 비암호학적 해시 알고리즘은 lookup3, superFashHash, DJBX33A, BuzHash가 존재한다. 암호학적 해시 알고리즘은 비암호학적 해시 알고리즘보다 안전성이 뛰어난 장점이 있으나 속도가 느리다. 암호학적 해시 알고리즘은 충돌 저항성 (Collision Resistance)와 역상 저항성 (Preimage Resistance)의 특징을 가지고 있다. 대표적인 암호학적 해시 알고리즘은 SHA2, SHA3, MD5가 존재한다.

[0015] 치환 암호(Substitution Cipher)는 특정 규칙에 기반하여 평문을 다른 글자로 치환하여 암호문을 만드는 것을 의미한다. 도 1은 기존 기술에 따른 치환 암호를 예시적으로 설명하기 위하여 도시한 도표이다. 치환 암호는, 도 1에 도시된 바와 같이, 규칙에 의해서 특정 평문이 암호문으로 치환된다. 예를 들어, 'Hello'를 암호화 한다고 하면, 49BBD의 암호문을 만들 수 있다. 치환 암호는 크게 단일 치환 암호와 다중 치환 암호로 구분될 수 있다. 대표적인 단일 치환 암호는 시저 암호 (Caesar Cipher)가 존재하며, 대표적인 다중 치환 암호는 비즈네르

암호 (Vigenere Cipher)가 존재한다. 치환 암호는 무작위 공격에 취약하다는 단점이 존재한다.

[0016] 이하, 데이터 공유(Data sharing)을 위한 블록체인 기반의 접근 제어 방법(Blockchain based Access Control)에 대하여 살펴본다.

[0017] Wenti Yang은 오프체인 Key Generation Group (KGG)와 블록체인의 검증 노드를 활용한 블록체인 기반의 접근 제어를 제안하였다. 해당 논문에서 사용자는 파일을 암호화할 수 있는 키를 KGG로부터 받고, 해당 키를 통해서 데이터를 암호화하여 오프체인 저장소에 저장한다. 사용자는 KGG와 블록체인 검증 노드로부터 접근 권한을 검증받아서 암호화된 데이터에 접근할 수 있다.

[0018] Xin Wei는 Attribute-based encryption 기법을 활용한 데이터 접근 제어 연구를 진행한 바 있다. 해당 연구에서는 Attribute-based encryption을 위해서 오프체인 서버에게 데이터 암호화를 아웃소싱(Outsourcing)한다. 암호화된 데이터는 오프체인 저장소에 저장되며, 암호화된 데이터에 접근하기 위해서는 블록체인의 특정 노드들로부터 접근 권한을 부여받아서 접근할 수 있다.

[0019] Xin Wei이 제안한 연구처럼 Xiaofeing Lu는 Attribute-based Encryption을 사용한 블록체인 기반의 접근제어를 연구한 바 있다. 해당 연구에서 데이터 제공자는 대칭 키를 사용하여 데이터를 암호화하여 오프체인 분산 저장소에 저장한다. 또 다른 오프체인 서버는 데이터 제공자가 사용한 대칭키에 속성값을 부여하여 새로운 키를 생성한다. 이후, 새롭게 생성된 키를 가진 사용자만 오프체인 서버의 추가적인 검증을 받아서 저장된 데이터에 접근할 수 있다.

[0020] V.Ezhil Arsasi 또한 auditable attribute-based encryption을 활용한 블록체인 기반의 접근 제어 연구를 제안한 바 있다. 해당 연구에서는 오프체인 서버가 데이터를 직접 암호화하여 저장한다. 또한, 해당 서버에 접근하기 위한 권한은 스마트 컨트랙트와 오프체인에 존재하는 데이터 매니저에 의해서 이루어진다. 사용자가 데이터 접근을 원할 경우 스마트 컨트랙트와 데이터 매니저에 의해 검증을 받고, 오프체인 서버를 통해 복호화된 파일을 제공받을 수 있다.

[0021] 기존 데이터 공유를 위한 블록체인 기반 접근통제 연구들은 데이터 암호화를 통한 접근 제어 연구들을 진행하였다. 하지만, 기존 연구들은 접근 통제의 안전성을 확보하기 위해 블록체인 노드에게 추가적인 권한을 부여하는 한계를 가지고 있다. 또한, 데이터 암호화 과정에서 오프체인 서버 혹은 오프체인 사용자가 참여한다는 한계를 가지고 있다. 이는 블록체인 노드 혹은 외부 요소의 신뢰도에 따라서 접근 통제의 안전성이 위협받을 수 있다.

[0022] 이하, 개인 정보 보호(Privacy Protection)을 위한 블록체인 기반의 접근 제어 방법(Blockchain based Access Control)에 대하여 살펴 본다.

[0023] Wei Liang은 Ciphertext policy attribute-based encryption 와 Paillier Encryption을 활용한 블록체인 기반 접근 제어 연구를 제안하였다. 해당 연구에서는 사용자가 블록체인 특정 노드로부터 키를 발급받은 후, Paillier Encryption를 데이터에 적용시킨다. 이후, Paillier Encryption된 데이터를 오프체인 서버인 Distributed Private Cluster에 저장하면서, Distributed Private Cluster가 데이터에 ciphertext policy attribute-based encryption을 진행하여 추가적인 데이터 암호화를 진행한다. 사용자가 암호화된 데이터에 접근하기 위해서는 특정 블록체인 노드에게 본인이 가진 키 검증을 받은 후에 데이터에 접근할 수 있다.

[0024] Xinyin Xiang은 사용자가 블록체인 특정 노드로부터 데이터 searchable attribute-base encryption 할 수 있는 키를 발급받고, 해당 키를 통해서 데이터를 암호화하는 연구를 제안한 바 있다. 사용자가 데이터 접근이 필요할 때는 오프체인 서버가 사용자의 데이터에 접근 권한을 확인하여 데이터에 접근할 수 있도록 하는 연구를 진행하였다.

[0025] Hanan E. Alhazmi가 제안한 연구에서는 데이터 제공자가 데이터를 분할하여 분할된 데이터와 해당 데이터에 접근 할 수 있는 인증 리스트를 생성한다. 이후, 오프체인 BCSM (Blockchain Based Security Manager)가 분할된 데이터를 암호화하여 각 분할된 데이터들의 메타 데이터 값만 블록체인에 저장한다. 원본 데이터는 외부 저장소에 저장이 되며 데이터 사용자는 오프체인 저장소에 접근할 수 있는 권한을 BCSM의 검증을 통해서 부여받는다.

[0026] Xiaodong Yang의 연구는 데이터 제공자가 데이터를 attribute-based encryption 하여 오프체인 저장소인 클라우드에 저장한다. 또한, 해당 데이터를 해독할 수 있는 키를 다른 오프체인 저장소인 Outsource sever에게 제공한다. Outsource server는 데이터 접근 요청이 들어오면, 사용자의 권한을 확인 후 클라우드에 저장된 데이터를 해독하여 제공한다.

[0027] Keping Yu의 연구는 데이터 제공자의 키를 분할해 주는 오프체인 서버가 따로 존재하며, 해당 분할된 키에 접근

할 수 있는 권한을 부여하는 오프체인 그룹이 존재한다. 데이터 제공자는 오프체인 저장소에 데이터를 암호화하여 저장한다. 이후, 해당 데이터를 암호화할 때 사용한 키를 분할하여 블록체인에 배포한다. 데이터 사용자는 데이터에 접근하기 위해 오프체인 그룹으로부터 권한을 부여받고, 해당 권한을 활용해 분할 된 키를 다시 조합하여 암호화된 데이터에 접근할 수 있다.

[0028] 기존 개인 정보 보호를 위한 블록체인 기반 접근통제 연구들도, 기존 데이터 공유를 위한 블록체인 기반 접근통제 연구들과 마찬가지로, 데이터 암호화를 통한 접근제어 연구를 진행하였으며, 동일한 한계점을 가진다. 위에서 언급한 것과 같이 블록체인 노드에게 추가적인 권한을 부여하는 한계를 가지고 있으며, 데이터 암호화 과정 및 접근제어 과정에 오프체인 서버 혹은 오프체인 사용자가 참여한다는 한계를 가지고 있다.

선행기술문헌

특허문헌

[0029] (특허문헌 0001) 한국등록특허공보 제 10-2418443호

(특허문헌 0002) 한국공개특허공보 제 10-2022-0130494호

(특허문헌 0003) 한국등록특허공보 제 10-2415260호

발명의 내용

해결하려는 과제

[0030] 전술한 문제점을 해결하기 위하여 본 발명은 메타버스 상의 개인 정보를 보호하기 위하여 관리자없이 생성할 수 있는 규칙 테이블을 이용하여 개인 정보를 치환 암호화 및 복호화를 할 수 있으며, 또한 기존의 RSA 방식보다 빠른 속도를 갖는 암호화 및 복호화를 수행할 수 있는 블록체인 기반의 치환 암호화 접근 제어 시스템 및 방법을 제공하는 것을 목적으로 한다.

과제의 해결 수단

[0031] 전술한 기술적 과제를 달성하기 위한 본 발명의 제1 특징에 따른 데이터 접근 제어 장치는, 스마트 컨트랙트를 이용하여 블록체인 네트워크에 데이터를 저장하거나 블록체인 네트워크에 저장된 데이터에 접근하도록 구성된 데이터 접근 제어 장치에 관한 것으로서, 사전 설정된 3개의 요소들을 이용하여 치환 암호화 및 복호화에 사용될 규칙 테이블을 생성하는 규칙 테이블 생성 모듈; 데이터 제공자로부터 블록체인 네트워크에 저장할 데이터 및 상기 설정된 3개의 요소들에 대한 값들을 제공받고, 상기 3개의 요소들의 값들을 이용하여 생성된 규칙 테이블을 이용하여 데이터를 치환 암호화시키고, 상기 치환 암호화된 데이터를 블록체인 네트워크에 저장하는 데이터 저장 모듈; 및 데이터 사용자로부터 데이터가 저장된 스마트 컨트랙트 주소 및 상기 설정된 3개의 요소들에 대한 값들을 제공받고, 스마트 컨트랙트를 통해 블록체인 네트워크의 상기 스마트 컨트랙트 주소의 치환 암호화 데이터를 호출하고, 상기 3개의 요소에 대한 값들을 이용하여 생성된 규칙 테이블을 이용하여 상기 호출된 치환 암호화 데이터를 역치환하여 복호화하는 데이터 접근 모듈;을 구비한다.

[0032] 전술한 제1 특징에 따른 블록체인을 기반으로 한 치환 암호화를 이용한 데이터 접근 제어 장치에 있어서, 상기 사전 설정된 3개의 요소는, 데이터 제공자의 블록체인 개인키를 해시 알고리즘을 적용하여 얻은 데이터 제공자의 개인키의 해시값(HRoot); 데이터 사용자에 의해 임의로 생성되고, 사전 설정된 개수(n) 이상의 요소로 구성된 값(Salt); 및 데이터 제공자와 데이터 사용자의 합의에 의해 생성되고, 사전 설정된 개수(n)의 숫자들로 구성된 집합(NKey);인 것이 바람직하다.

[0033] 전술한 제1 특징에 따른 블록체인을 기반으로 한 치환 암호화를 이용한 데이터 접근 제어 장치에 있어서, 상기 규칙 테이블 생성 모듈이 생성한 규칙 테이블은, 사전 설정된 자리수로 표현된 비트값들(Bit Value); 데이터 제공자의 HRoot를 NKey값을 이용하여 해시하여 상기 비트값들에 대응되도록 설정된 제1 치환 설정값들; 및 데이터 사용자의 Salt값과 NKey값을 매칭시킨 뒤 재정렬시킨 후, 상기 비트값들에 대응되도록 설정된 제2 치환 설정값들;을 구비하는 것이 바람직하다.

[0034] 전술한 제1 특징에 따른 블록체인을 기반으로 한 치환 암호화를 이용한 데이터 접근 제어 장치에 있어서, 상기 데이터 저장 모듈은, 데이터 제공자로부터 입력된 데이터를 비트 형태로 변환시키고, 비트값을 사전 설정된 자

리수로 분할하여 복수 개의 단위 비트(SB)들을 생성하는 분할 유닛; 규칙 테이블을 이용하여 상기 복수 개의 단위 비트(SB)들을 치환시켜 치환 암호화 데이터(Xst)를 생성하는 데이터 치환 유닛; 및 치환 암호화 데이터를 특정 크기로 분할하고, 분할된 데이터 유닛들을 스마트 컨트랙트를 통해 블록체인 네트워크에 배포하는 배포 유닛;을 구비하는 것이 바람직하다.

[0035] 전술한 제1 특징에 따른 블록체인을 기반으로 한 치환 암호화를 이용한 데이터 접근 제어 장치에 있어서, 상기 데이터 접근 모듈은, 데이터 사용자로부터 입력된 스마트 컨트랙트 주소를 이용하여 블록체인 네트워크로부터 치환 암호화 데이터를 호출하는 호출 유닛; HRoot 값과 Salt를 사용하여 데이터 사용자의 접근 권한을 확인하는 검증 유닛; 및 규칙 테이블을 이용하여, 상기 호출된 치환 암호화 데이터를 역치환하여 복호화하는 복원 유닛;을 구비하는 것이 바람직하다.

[0036] 본 발명의 제2 특징에 따른 치환 암호화를 이용한 데이터 접근 제어 방법은, 컴퓨팅 시스템에서 실행되는 프로그램에 의해 구현된 데이터 접근 제어 방법에 관한 것으로서, 사전 설정된 3개의 요소를 이용하여 치환 암호화 및 복호화에 사용될 규칙 테이블을 생성하는 규칙 테이블 생성 단계; 및 데이터 제공자로부터 블록체인 네트워크에 저장할 데이터 및 상기 설정된 3개의 요소에 대한 값들을 제공받고, 상기 3개의 요소에 대한 값들을 이용하여 생성된 규칙 테이블을 이용하여 데이터를 치환 암호화시키고, 상기 치환 암호화된 데이터를 블록체인 네트워크에 저장하는 데이터 저장 단계; 를 구비한다.

[0037] 전술한 제2 특징에 따른 블록체인을 기반으로 한 치환 암호화를 이용한 데이터 접근 제어 방법에 있어서, 상기 사전 설정된 3개의 요소는, 데이터 제공자의 블록체인 개인키를 해시 알고리즘을 적용하여 얻은 데이터 제공자의 개인키의 해시값(HRoot); 데이터 사용자에 의해 임의로 생성되고, 사전 설정된 개수(n) 이상의 요소로 구성된 값(Salt); 및 데이터 제공자와 데이터 사용자의 합의에 의해 생성되고, 사전 설정된 개수(n)의 숫자들로 구성된 집합(NKey);인 것이 바람직하다.

[0038] 전술한 제2 특징에 따른 블록체인을 기반으로 한 치환 암호화를 이용한 데이터 접근 제어 방법에 있어서, 상기 데이터 저장 단계는, 데이터 제공자로부터 입력된 데이터를 비트 형태로 변환시키고, 비트값을 사전 설정된 자리수로 분할하여 복수 개의 단위 비트(SB)들을 생성하는 단계; 규칙 테이블을 이용하여 상기 복수 개의 단위 비트(SB)들을 치환시켜 치환 암호화 데이터(Xst)를 생성하는 단계; 및 치환 암호화 데이터를 특정 크기로 분할하고, 분할된 데이터 유닛들을 스마트 컨트랙트를 통해 블록체인 네트워크에 배포하는 단계;을 구비하는 것이 바람직하다.

[0039] 전술한 제2 특징에 따른 블록체인을 기반으로 한 치환 암호화를 이용한 데이터 접근 제어 방법은, 데이터 사용자로부터 데이터가 저장된 스마트 컨트랙트 주소 및 상기 설정된 3개의 요소에 대한 값들을 제공받고, 스마트 컨트랙트를 통해 블록체인 네트워크의 상기 스마트 컨트랙트 주소의 치환 암호화된 데이터를 획득하고, 상기 3개의 요소에 대한 값들을 이용하여 생성된 규칙 테이블을 이용하여 상기 치환 암호화된 데이터를 복원하는 데이터 접근 단계;를 더 구비하고,

[0040] 상기 데이터 접근 단계는, 데이터 사용자로부터 입력된 스마트 컨트랙트 주소를 통해 블록체인 네트워크로부터 치환 암호화 데이터를 호출하는 단계; HRoot 값과 Salt를 사용하여 데이터 사용자의 접근 권한을 검증하는 단계; 및 규칙 테이블을 이용하여, 상기 호출된 치환 암호화 데이터를 역치환시켜 복원하는 단계; 를 구비하는 것이 바람직하다.

[0041] 본 발명의 제3 특징에 따른 블록체인을 기반으로 한 치환 암호화를 이용한 데이터 접근 제어 시스템은, 데이터 제공자의 요청에 따라 데이터를 치환 암호화시켜 블록체인 네트워크에 저장하거나, 데이터 사용자의 요청에 따라 블록체인 네트워크에 저장된 치환 암호화된 데이터를 복호화하여 제공하는 데이터 접근 제어 장치; 및 상기 데이터 접근 제어 장치로부터의 요청에 따라, 스마트 컨트랙트를 통해 블록체인에 데이터를 저장하거나, 블록체인에 저장된 데이터를 호출하여 제공하는 블록체인 네트워크;를 구비한다.

[0042] 전술한 제3 특징에 따른 블록체인을 기반으로 한 치환 암호화를 이용한 데이터 접근 제어 시스템에 있어서, 상기 블록체인 네트워크의 스마트 컨트랙트는, Mother 컨트랙트와 Child 컨트랙트로 구성된 이중 구조의 스마트 컨트랙트이며, 상기 Mother 컨트랙트는 사용자와 직접 상호 작용하고, Child 컨트랙드의 주소를 관리하는 스마트 컨트랙트이며, 상기 Child 컨트랙트는 데이터를 저장하고, 저장하고 있는 데이터를 반환하는 컨트랙트인 것이 바람직하다.

발명의 효과

[0043] 본 발명에서는 메타버스 개인정보 보호를 위해 블록체인 기반 치환암호화를 사용한 접근 통제 기법을 제안한다. 본 발명에서 제안하는 접근 방안은 암호화 및 복호화를 위해서 관리자가 존재하지 않으며, RSA 보다 암호화 및 복호화의 속도가 빠르다. 본 발명에 따른 블록체인 기반의 치환 암호화를 활용한 접근 통제 기법은 데이터 제공자와, 데이터 사용자간에 사전에 공유된 3 가지 요소 값들로 생성되는 규칙 테이블에 의해서 데이터가 암호화되어 접근 통제가 진행된다. 본 발명에 따른 방법은 접근 통제에 직접적으로 관여하는 참여자들에 의해 규칙 테이블을 생성하기 때문에 추가적인 관리자가 필요없다. 또한, 규칙 테이블에 의해 데이터를 치환하여 암호화하기 때문에 수학적 어려움에 기반하고 있는 RSA 보다 암호화 및 복호화 속도가 빠르다.

[0044] 또한, 본 발명에 따른 규칙 테이블의 두번째 열인 DiB는 DP 의 개인키를 기반으로 암호학적 해시 알고리즘을 사용하여 생성된 HRoot에 의해서 만들어진다. 암호학적 해시 알고리즘은 결과값의 충돌 저항성(Collision Resistance)과 입력값의 역상 저항성(Preimage Resistance)를 가지고 있기 때문에, DiB를 생성하는 초기값인 HRoot를 만드는 DP 의 개인키 값이 중복되지 않으면 규칙 테이블의 DiB 값들이 중복될 일이 없다.

[0045] 또한, 블록체인 사용자 개인키 생성은 2048개의 단어 리스트로 구성되어 있는 BIP-0039를 활용하여 생성되며, 사용자는 12개 ~ 24개의 단어들을 조합하여 개인키를 생성할 수 있다. 따라서, 서로 다른 사용자가 우연하게 동일한 개인키를 가지고 동일한 HRoot를 가질 확률은 불가능하다고 할 수 있다.

[0046] 또한, DiB 값이 중복 발생하여 인가받지 않은 사람이 우연하게 접근하거나 무작위 공격으로 규칙 테이블의 DiB 내용을 유추하는 것도 불가능하다고 할 수 있다.

[0047] 이러한 내용을 토대로 하여, 특별한 해킹 기법, 사회적 공학 기법, 3F에 대한 사용자의 관리 부실이 아닌 이상, 본 발명에 따른 방법의 규칙 테이블은 충돌성 및 무작위 공격으로부터 안전하다고 할 수 있다.

도면의 간단한 설명

[0048] 도 1은 기존 기술에 따른 치환 암호를 예시적으로 설명하기 위하여 도시한 도표이다.

도 2는 본 발명에서 사용되는 용어들에 대한 설명을 정리한 테이블(Notations Table)이다.

도 3은 본 발명의 바람직한 실시예에 따른 블록체인 기반의 치환 암호화를 이용한 데이터 접근 제어 시스템에 있어서, 데이터 접근 제어 장치의 구성을 개략적으로 도시한 블록도이다.

도 4는 본 발명의 바람직한 실시예에 따른 블록체인 기반의 치환 암호화를 이용한 데이터 접근 제어 시스템에 있어서, 데이터 제공자가 데이터 접근 제어 장치의 데이터 저장 모듈을 이용하여 데이터를 저장하는 과정을 순차적으로 도시한 시퀀스 다이어그램이다.

도 5는 본 발명의 바람직한 실시예에 따른 블록체인 기반의 치환 암호화를 이용한 데이터 접근 제어 시스템에 있어서, 데이터 사용자가 데이터 접근 제어 장치의 데이터 접근 모듈을 이용하여 데이터에 접근하는 과정을 순차적으로 도시한 시퀀스 다이어그램이다.

도 6은 본 발명에 따른 블록체인 기반의 치환 암호화를 이용한 접근 통제 시스템에 있어서, 데이터 접근 제어 장치의 데이터 저장 모듈에 의한 데이터 저장 과정을 개략적으로 도시한 흐름도이다.

도 7은 본 발명에 따른 블록체인 기반의 치환 암호화를 이용한 접근 통제 시스템에 있어서, 데이터 접근 제어 장치의 데이터 저장 모듈에 의한 데이터 저장 과정을 구현한 알고리즘에 대한 수도 코드이다.

도 8은 본 발명에 따른 블록체인 기반의 치환 암호화를 이용한 접근 통제 시스템에 있어서, 블록체인 네트워크에 데이터를 저장하기 위한 스마트 컨트랙트를 구현한 수도 코드이다.

도 9는 본 발명에 따른 블록체인 기반의 치환 암호화를 이용한 접근 통제 시스템에 있어서, 데이터 접근 제어 장치의 데이터 접근 모듈의 데이터 접근 과정을 개략적으로 도시한 흐름도이다.

도 10은 본 발명에 따른 블록체인 기반의 치환 암호화를 이용한 접근 통제 시스템에 있어서, 데이터 접근 제어 장치의 데이터 접근 모듈의 데이터 저장 과정을 구현한 알고리즘에 대한 수도 코드이다.

발명을 실시하기 위한 구체적인 내용

[0049] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예에 따른 블록체인 기반의 치환 암호화를 이용한 데이터 접근 제어 시스템의 구성 및 동작에 대하여 구체적으로 설명한다.

[0050] 본 발명에 따른 데이터 접근 제어 시스템은 데이터 사용자 또는 데이터 제공자가 접속하도록 구성된 데이터 접근 제어 장치 및 데이터를 저장하는 블록체인 네트워크를 구비한다. 상기 데이터 접근 제어 장치는 데이터 제공자의 요청에 따라 데이터를 치환 암호화시켜 블록체인 네트워크에 저장하거나, 데이터 사용자의 요청에 따라 블록체인 네트워크에 저장된 치환 암호화된 데이터를 호출하고 복호화하여 제공한다. 상기 블록체인 네트워크는, 상기 데이터 접근 제어 장치로부터의 요청에 따라, 스마트 컨트랙트를 통해 블록체인에 데이터를 저장하거나, 블록체인에 저장된 데이터를 호출하여 제공한다. 한편, 본 발명에 따른 데이터 접근 제어 장치는 데이터 사용자 또는 데이터 제공자의 단말기에 설치되어 실행되는 소프트웨어로 구현될 수도 있다.

[0051] 이하, 도 3을 참조하여, 본 발명에 따른 데이터 접근 제어 시스템의 데이터 접근 제어 장치의 구성 및 동작에 대하여 구체적으로 설명한다.

[0052] 도 3은 본 발명의 바람직한 실시예에 따른 블록체인 기반의 치환 암호화를 이용한 데이터 접근 제어 시스템에 있어서, 데이터 접근 제어 장치의 구성을 개략적으로 도시한 블록도이다. 도 3을 참조하면, 상기 데이터 접근 제어 장치(10)는, 규칙 테이블 생성 모듈(12), 데이터 저장 모듈(20) 및 데이터 접근 모듈(30)을 구비한다. 상기 규칙 테이블 생성 모듈(12)은 사전 설정된 3개의 요소를 이용하여 암호화 및 복호화에 사용될 규칙 테이블을 생성한다. 상기 데이터 저장 모듈(20)은, 데이터 제공자로부터 블록체인 네트워크에 저장할 데이터 및 상기 설정된 3개의 요소에 대한 값들을 제공받고, 상기 3개의 요소에 대한 값들을 이용하여 생성된 규칙 테이블을 이용하여 데이터를 치환 암호화시키고, 상기 치환 암호화된 데이터를 상기 스마트 컨트랙트를 통해 블록체인 네트워크에 저장한다. 상기 데이터 접근 모듈(30)은, 데이터 사용자로부터 데이터가 저장된 스마트 컨트랙트 주소 및 상기 설정된 3개의 요소에 대한 값들을 제공받고, 스마트 컨트랙트를 통해 블록체인 네트워크의 상기 스마트 컨트랙트 주소의 치환 암호화된 데이터를 획득하고, 상기 3개의 요소에 대한 값들을 이용하여 생성된 규칙 테이블을 이용하여 상기 치환 암호화된 데이터를 복원한다.

[0053] 본 발명에 따른 블록체인 기반의 치환 암호화를 이용한 접근 통제 방법은 1) 규칙 테이블을 생성하는 방법, 2) 데이터를 암호화하여 저장하는 방법과, 3) 암호화된 데이터에 접근하는 방법으로 구성된다. 본 명세서에서 사용되는 기호는 도 2에 정리되어 있다. 도 2는 본 발명에서 사용되는 용어들에 대한 설명을 정리한 테이블(Notations Table)이다.

[0054] 본 발명에 따른 블록체인 기반의 치환 암호화를 이용한 접근 통제 방법은 데이터 제공자(Data Provider; 이하 'DP'라 함)와 데이터 사용자(Data User; 이하 'DU'라 함)가 3가지 요소값(3F)을 사전에 공유하며, 3F를 이용하여 규칙테이블을 생성한다. 3F는 HRoot, Salt, NKey이다. 3F의 구성요소 중 하나인 HRoot는 DP의 블록체인 개인키를 해시 알고리즘에 적용시켜 나온 결과 값이다. Salt 값은 DU가 임의로 생성하는 값으로 16개 이상의 요소로 구성된 집합이다. NKey는 DP와 DU가 합의하여 만든 임의의 16개 숫자로 구성된 집합이다. 도 2에 표기된 H_n은 HRoot를 기반으로 해시 함수를 n번 만큼 누적 반복해서 출력되는 값으로써, H_3은 Hash(Hash(Hash(HRoot)))를 의미한다. 또한 $Salt_n$은 Salt 집합의 n 번째 값을 의미한다. 예를 들어 Salt = {H, e, L, l, o} 인 경우 $Salt_1$ = H, $Salt_2$ = e 이다.

[0055] 도 4는 본 발명의 바람직한 실시예에 따른 블록체인 기반의 치환 암호화를 이용한 데이터 접근 제어 시스템에 있어서, 데이터 제공자가 데이터 접근 제어 장치의 데이터 저장 모듈을 이용하여 데이터를 저장하는 과정을 순차적으로 도시한 시퀀스 다이어그램이다. 도 4를 참조하면, DP는 off-chain 저장소에 개인 정보를 저장하고, Off-Chain 저장소로부터 접근 정보(access information)를 제공받는다. 이후, DP는 본 발명에 따른 데이터 접근 제어 장치의 데이터 저장 모듈을 이용하여, 상기 접근 정보인 데이터를 치환 암호화하여 스마트 컨트랙트를 활용하여 블록체인 네트워크에 배포한다. Off-chain 저장소와 Data Provider 간의 상호작용은 다양한 방법으로 이루어질 수 있기 때문에 본 발명에서는 오른쪽 박스로 표기된 (Red Box) 부분에 대해서만 설명하며, 이에 대한 자세한 설명은 후술한다.

[0056] 도 5는 본 발명의 바람직한 실시예에 따른 블록체인 기반의 치환 암호화를 이용한 데이터 접근 제어 시스템에 있어서, 데이터 사용자가 데이터 접근 제어 장치의 데이터 접근 모듈을 이용하여 데이터에 접근하는 과정을 순차적으로 도시한 시퀀스 다이어그램이다. 도 5를 참조하면, DU는, 블록체인을 활용하여 스마트 컨트랙트 데이터를 호출하고, 해당 호출된 데이터는 데이터 접근 제어 장치의 데이터 접근 모듈을 통해서 복호화되어 사용자에게 전달된다. 사용자는 전달된 복호화 데이터를 통해서 Off-chain 저장소에 접근할 수 있다. 본 발명에서는 데이터 접근 프로세스의 테두리로 표현된 부분(Red Box)만을 서술하며, 이에 대한 자세한 설명은 후술한다.

[0057] 먼저, 본 발명에 따른 블록체인 기반의 치환 암호화를 이용한 접근 통제 시스템에 있어서, DP와 DU에 의해 실행

되는 데이터 접근 제어 장치의 규칙 테이블 생성 모듈이 사전에 공유한 3F를 활용하여 규칙 테이블을 생성하는 과정에 대해서 서술한다. 규칙 테이블은 치환 암호화를 하기 위해서 사용되는 테이블로서, DP 혹은 DU가 저장하는 형태가 아니다. 규칙 테이블은 데이터 저장, 혹은 접근 과정에서 매번 3F에 의해서 생성되고 지워지는 형태이다. 표 1은 규칙 테이블의 형태를 도시한 도표이다.

표 1

[0058]

Bit Value	0110	0111	0000	0001	0011	0010	0101	0100	1111	1110	1100	1101	1010	1011	1001	1000
Hash	Ht_1	Ht_2	Ht_3	Ht_4	Ht_5	Ht_6	Ht_7	Ht_8	Ht_9	Ht_10	Ht_11	Ht_12	Ht_13	Ht_14	Ht_15	Ht_16
Salt	St_1	St_2	St_3	St_4	St_5	St_6	St_7	St_8	St_9	St_10	St_11	St_12	St_13	St_14	St_15	St_16

[0059] 표 1에 표현된 첫번째 Row는 Bit Value를 의미하며, 각각의 Column은 4비트씩 표현되어 있다. 해당 Row 값들의 순서는 알고리즘 설계시 변경이 가능하다. 두 번째 Row는 H_n이 입력될 위치로서 각각의 위치는 Ht_1, Ht_2, ..., Ht_16 과 같이 표현하였다. 세번째 Row는 $Salt_n$ 이 입력될 위치로서 두 번째 Row와 동일하게 각각의 위치를 St_1, St_2, ..., St_16과 같이 표현하였다.

[0060] 규칙 테이블의 두번째 Row는 NKey 값을 적용하고 해당 수치만큼 HRoot를 해시화하여 완성할 수 있다. 또한, 세번째 Row 에는 Salt 값을 넣고, NKey 값을 매칭 시킨 뒤 오름차순으로 정렬하여 완성시킬 수 있다.

[0061] 규칙 테이블 생성 예시를 위해서 Salt = {t,e,s,y,1,2,3,4,5,6,7,8,9,0,@,#}, NKey = {1, 2, 3, 8, 9, 10, 15, 4, 5, 6, 11, 13, 44, 52, 12, 19} 이라고 가정한다. 두번째 row를 채우기 위해서는 NKey 값들을 두번째 row의 각각의 column에 적용시킨다. 즉, Ht_1 = 1, Ht_7 = 15, Ht_16 = 19이 된다. 이후, 각각의 column에 입력된 수만큼 HRoot를 해시한 값들을 저장한다. 결국 최종적으로 Ht_1 = H_1, Ht_7 = H_{15}, Ht_16 = H_{19} 가 된다. 세번째 row를 채우기 위해서는 Salt 값과 NKey 값을 먼저 각각의 Column에 적용시킨다. 즉, St_1 = (1, t), St_7 = (15, 3), St_16 = (19, #)이 된다. 이후, NKey 값을 기준으로 오름차순으로 정렬하고, 각 Column에 저장되어 있는 NKey 값들을 삭제한다. 최종적으로 Salt 값들은 섞이기 때문에 St_1 = t, St_7 = y, St_16 = 0 이 된다. 언급한 Salt, HRoot, NKey를 활용하여 생성된 규칙 테이블 예시의 최종적인 모습은 표 2와 같이 완성될 수 있다. 표 2는 규칙 테이블의 예시를 도시한 도표이다.

표 2

[0062]

Bit Value	0110	0111	0000	0001	0011	0010	0101	0100	1111	1110	1100	1101	1010	1011	1001	1000
Hash	H1	H2	H3	H8	H9	H10	H15	H4	H5	H6	H11	H13	H44	H52	H12	H19
Salt	t	e	s	4	5	6	y	1	2	7	@	8	3	#	12	0

[0063] 이하, 도 6 및 도 7을 참조하여, 본 발명에 따른 블록체인 기반의 치환 암호화를 이용한 접근 통제 시스템에 있어서, 데이터 접근 제어 장치의 데이터 저장 모듈이 규칙 테이블을 이용하여 데이터를 블록체인 네트워크에 저장하는 과정을 설명한다.

[0064] 도 6는 본 발명에 따른 블록체인 기반의 치환 암호화를 이용한 접근 통제 시스템에 있어서, 데이터 접근 제어 장치의 데이터 저장 모듈에 의한 데이터 저장 과정을 개략적으로 도시한 흐름도이다.

[0065] 도 6를 참조하면, 본 발명에 따른 데이터 접근 제어 장치의 데이터 저장 모듈에 의한 데이터 저장 과정은 총 4단계로 구성되어 있으며, 요약하자면 다음과 같다. (1) 사용자로부터 받은 비트 값을 4 비트씩 분할한다. (2) 분할된 비트 값들을 규칙 테이블을 사용하여 치환한다. (3) 이전 단계에서 치환된 값을 다시 한번 규칙 테이블

을 사용하여 치환한다. (4) 치환이 완료된 값을 XOR 연산을 통해 한번 더 숨기고 스마트 컨트랙트를 활용하여 블록체인에 저장한다.

[0066] 도 7은 본 발명에 따른 블록체인 기반의 치환 암호화를 이용한 접근 통제 시스템에 있어서, 데이터 접근 제어 장치의 데이터 저장 모듈에 의한 데이터 저장 과정을 구현한 알고리즘에 대한 수도 코드이다. 도 6 및 도 7을 참조하면, 접근 제어 장치의 데이터 저장 모듈은 DP로부터 저장하고자 하는 데이터를 비트 값으로 표현한 값(BO)과 3F를 입력받는다. BO 값을 생성하는 방법은 데이터의 종류 혹은 사용하는 프로그래밍 언어에 따라서 방법이 각기 다를 수 있기 때문에 본 발명에서는 BO 값을 만드는 과정에 대해서는 언급하지 않는다.

[0067] 다음, DP로부터 받은 BO를 4비트씩 분할하여 n개의 SB를 생성한다. 이 과정을 Division 프로세스라 한다. 예를 들어, BO = 01101000 이라면, SB_1 = 0110, SB_2 = 1000 으로 표현될 수 있다.

[0068] 다음, 생성된 각각의 SB_n을 규칙 테이블 두번째 Row (Hash) 값으로 치환시키고 DiB 값을 얻는다. 이 과정을 Diffusion 프로세스라 한다. 예를 들어, 표 2를 기준으로 하였을 때 $SB_1 = H_1$, $SB_2 = H_{19}$ 로 치환된다. Diffusion 프로세스는 원본 데이터의 값을 확산시켜 데이터의 직접적인 노출을 피하기 위해서 사용되는 과정이다. Diffusion 과정으로 나타나는 H_n 값의 크기 및 표현은 암호학적 해시 알고리즘에 따라 변화할 수 있다.

[0069] 다음, Diffusion 프로세스 이후에 다시 한번 규칙 테이블을 활용하여 DiB 값을 규칙 테이블 세번째 Row 값으로 치환하여 SuB값을 얻는다. 이 과정을 Replacement 프로세스라 한다. 예를 들어, 표 2를 기준으로 $H_n = t$, $H_{19} = 0$ 이 된다 Replacement 프로세스는 BO 값을 DiB 값으로 치환하면서 늘어난 데이터의 양을 블록체인에 저장을 용이하게 하기 위해서 데이터의 크기를 축소하는 과정이다.

[0070] 다음, Replacement 과정을 통해 생성된 SuB값과 Du가 제공한 Salt 값을 합쳐서 St를 생성한다. 생성된 St와 HRoot를 활용해 XOR 연산을 진행하여 XSt 값을 만든다. 이 과정을 XOR 프로세스라 한다. XOR 프로세스는 SuB 값의 직접적인 노출을 방지하며 데이터 접근 과정에서 DU 검증을 위해서 진행하는 과정이다.

[0071] 다음, XSt를 저장을 위해서 특정 크기로 분할하여 XStp를 생성하고, $XStp_n$ 을 스마트 컨트랙트를 활용해서 블록체인 네트워크에 순차적으로 배포한다.

[0072] 이하, 도 8을 참조하여, 본 발명에 따른 블록체인 기반의 치환 암호화를 이용한 접근 통제 시스템에 있어서, 블록체인 네트워크에 데이터를 저장하기 위한 스마트 컨트랙트에 대하여 구체적으로 설명한다. 블록체인 네트워크에 데이터를 저장하기 위해서는 스마트 컨트랙트 사용이 필수적이다. 본 발명에서는 스마트 컨트랙트에 저장되기 전에 암호화가 진행되기 때문에, 스마트 컨트랙트는 데이터의 저장 및 호출 기능만 포함하도록 설계된다.

[0073] 도 8은 본 발명에 따른 블록체인 기반의 치환 암호화를 이용한 접근 통제 시스템에 있어서, 블록체인 네트워크에 데이터를 저장하기 위한 스마트 컨트랙트를 구현한 수도 코드이다. 도 8을 참조하면, 본 발명에 따른 블록체인 네트워크의 스마트 컨트랙트는 이중 구조로 되어 있는 스마트 컨트랙트로서, Mother contract와 Child contract로 구성된다. Mother contract는 사용자와 직접 상호작용하는 스마트 컨트랙트임과 동시에 Child contract의 주소를 관리하는 스마트 컨트랙트이다. 사용자는 Mother contract 주소 하나만 알고 있더라도 Child contract의 주소를 알 수 있다. Child Contract는 실질적으로 데이터를 저장하고 있는 스마트 컨트랙트로써 가지고 있는 데이터를 반환하는 역할만을 담당한다.

[0074] 본 발명에 따른 시스템에서는 데이터를 저장하고자 하는 경우 1개의 Mother Contract와 1개 이상의 Child Contract를 배포하게 된다. DP는 Mother Contract를 통해서 Child Contract를 배포하면서 데이터를 저장하며, 스마트 컨트랙트는 도 8에 도시된 알고리즘으로 표현된다. 또한, DU가 데이터를 호출하고자 할 때는 Mother Contract로부터 Child Contract 주소를 받아 Child Contract에 저장되어 있는 데이터들을 하나씩 호출한다.

[0075] 이하, 도 9 및 도 10를 참조하여, 본 발명에 따른 블록체인 기반의 치환 암호화를 이용한 접근 통제 시스템에 있어서, 데이터 접근 제어 장치의 데이터 접근 모듈이 규칙 테이블을 이용하여 블록체인 네트워크으로부터 데이터에 접근하는 과정을 설명한다.

[0076] 도 9은 본 발명에 따른 블록체인 기반의 치환 암호화를 이용한 접근 통제 시스템에 있어서, 데이터 접근 제어 장치의 데이터 접근 모듈의 데이터 접근 과정을 개략적으로 도시한 흐름도이다.

[0077] 도 9을 참조하면, 본 발명에 따른 데이터 접근 제어 장치의 데이터 접근 제어 모듈에 의한 데이터 접근 프로세스는 총 5단계에 걸쳐서 이루어진다. 본 발명에 따른 데이터 접근 프로세스의 각 단계에 대해서 간략하게 요약

하자면 다음과 같다. (1) DU는 3F와 스마트 컨트랙트 주소를 활용하여 데이터를 호출한다. (2) HRoot와 Salt를 사용하여 DU가 접근 권한이 있는지 확인한다. (3) HRoot와 Salt가 맞는 경우, 규칙 테이블 기반으로 SuB을 DiB 값으로 복원한다. (4) 이전 과정과 동일하게 DiB을 SB 값으로 복원한다. (5) SB 값을 BO 값으로 복원한다.

[0078] 도 10는 본 발명에 따른 블록체인 기반의 치환 암호화를 이용한 접근 통제 시스템에 있어서, 데이터 접근 제어 장치의 데이터 접근 모듈의 데이터 저장 과정을 구현한 알고리즘에 대한 수도 코드이다. 도 9 및 도 10를 참조하면, 먼저, 접근 제어 장치의 데이터 접근 모듈은 DU로부터 스마트 컨트랙트 주소 및 3F를 입력받는다. 다음, DU로부터 받은 3F 값으로 규칙 테이블을 생성한다. 다음, DU로부터 받은 Smart Contract 주소를 활용하여 블록체인 네트워크에서 스마트 컨트랙트를 호출한다. 이후, 순차적으로 호출된 스마트 컨트랙트에 의해 제공되는 데이터들을 연결하여 XSt값을 생성한다 (Call Smart Contract).

[0079] 다음, XSt 값과 HRoot를 활용하여 St 값을 복원한다. A XOR B = C, 이며 A XOR C = B 인 특징을 가진 XOR 연산은 DU가 제대로 된 HRoot 값을 가지고 있다면 정상적인 St 값을 가질 수 있다. St 는 SuB 와 Salt 값으로 구성되어 있기 때문에 DU가 제공한 Salt 값과 XoR 연산을 통해서 나타난 Salt 값이 맞는지 확인한다. 만약 두 Salt 값이 틀릴 경우 알고리즘은 프로세스를 종료한다. 이 공정이 Verification 프로세스이다.

[0080] 다음, St 안에 속해 있는 Salt 값이 DU가 제공한 Salt 값과 동일할 경우 올바른 접근으로 간주하고, 규칙테이블 기반으로 SuB 값을 DiB 값으로 복원한다. 이 공정이 Reverse Replacement 프로세스이다. 또한, 이전 과정과 동일하게 규칙 테이블을 활용하여 DiB를 다시한번 SB로 복원한다. 이 공정이 Reverse Diffusion 프로세스이다.

[0081] 이후, 복원된 SB 값들을 합쳐서 BO 값을 완전하게 생성한다. 다음, BO값으로부터 파일을 복원한다.

[0082] 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

[0083] 10 : 데이터 접근 제어 장치

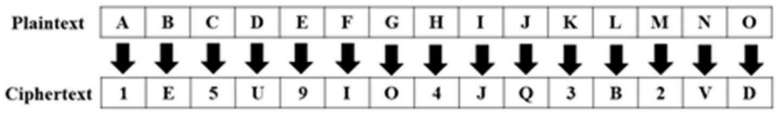
12 : 규칙 테이블 생성 모듈

20 : 데이터 저장 모듈

30 : 데이터 접근 모듈

도면

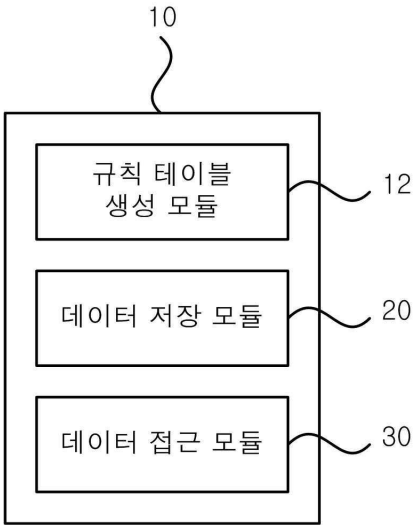
도면1



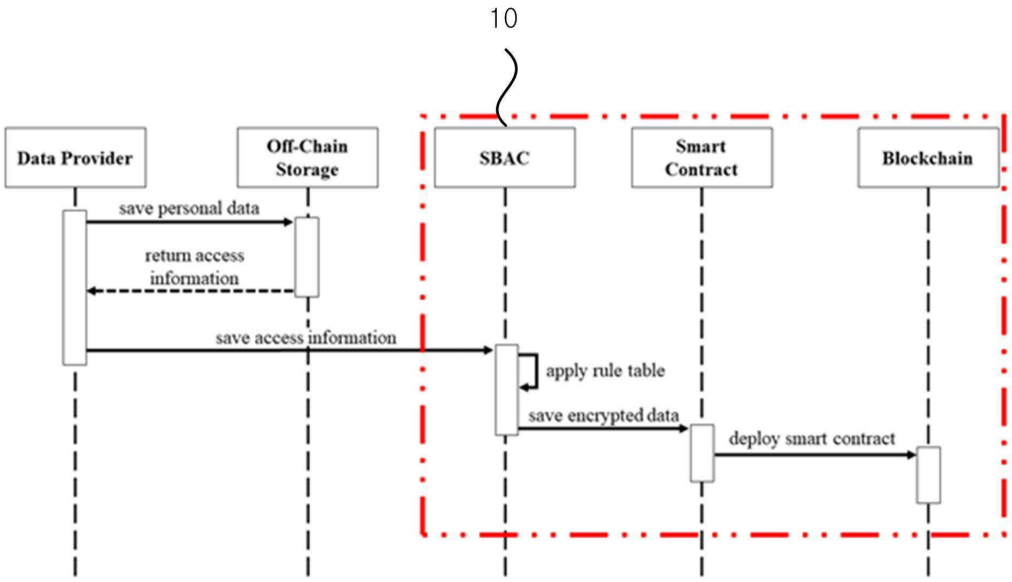
도면2

Symbol	Description
DP	A data Provider
DU	A data User
3F	Three factors (HRoot, Salt, NKey)
HRoot	A hashed value of DP's private key
Salt	A set of created values by DU
NKey	A set of numbers agreed upon between the DP and DU
H_n	N^{th} hash value
$Salt_n$	N^{th} word in the Salt set
BO	Bit values from original Data
SB	Result values of divided Step
DiB	Result values of Diffusion Step
SuB	Result values of Replacement Step
St	Values with SuB and Salt values
XSt	St value after XOR operation is completed
XStp	Split Values from XSt

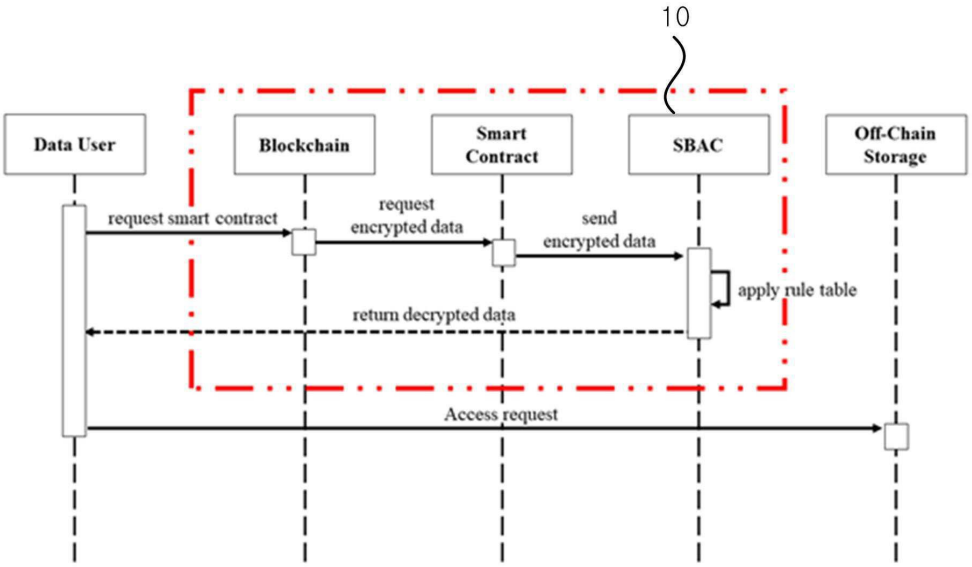
도면3


10
규칙 테이블
생성 모듈
12
데이터 저장 모듈
20
데이터 접근 모듈
30

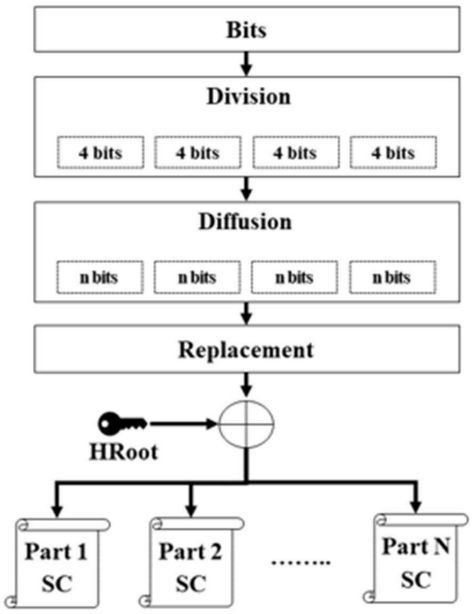
도면4


10
Data Provider
Off-Chain Storage
SBAC
Smart Contract
Blockchain
save personal data
return access information
save access information
apply rule table
save encrypted data
deploy smart contract

도면5


10
Data User
Blockchain
Smart Contract
SBAC
Off-Chain Storage
request smart contract
request encrypted data
send encrypted data
apply rule table
return decrypted data
Access request

도면6


Bits
Division
4 bits
4 bits
4 bits
4 bits
Diffusion
n bits
n bits
n bits
n bits
Replacement
HRoot
Part 1 SC
Part 2 SC
.....
Part N SC

도면7

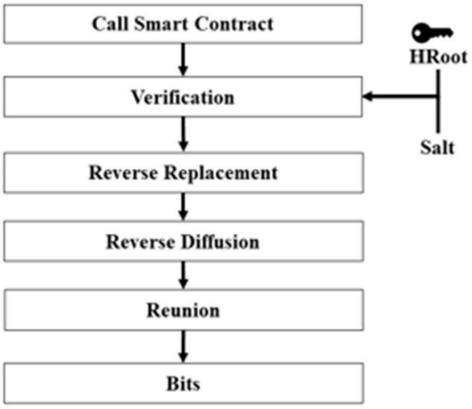
Input: BO, HRoot, Salt, NKey
1. Create Rule Table (HRoot, Salt, NKey)
Division Part
2. SB = divide BO into 4bits
Diffusion Part
3. DiB = [ ]
4. for j in range len(SB):
5. DiB_raw[j]= Rule Table (SB[j])
6. DiB.appened (DiB_raw[j])
7. end for
Replacement Part
8. SuB = [ ]
9. for z in range len (DiB):
10. SuB_raw[z]= Rule Table (DiB[z])
11. SuB.appened(SuB_raw[z])
12. end for
XOR part
13. XStp = [ ]
14. St = {SuB, Salt}
15. XSt = st ⊕ HRoot
16. XStp.append (divide XSt into Smart Contract Size)
Deploy Smart Contract
17. for q in range len (XStp):
18. sc_address = deploy smart contract (XStp[q])
19. end for
20. return sc_address

도면8

Mother Contract
input: XStp
1. child contract address = [ ]
2. create child contract = new child contract (XStp)
3. child contract address.appended(create child contract.address)
4. return mother contract.address

Child Contract
input: XStp
5. data = XStp

도면9


Call Smart Contract
HRoot
Verification
Salt
Reverse Replacement
Reverse Diffusion
Reunion
Bits

도면10

Input: Contract Address, HRoot, Salt, NKey
1. Create Rule Table (HRoot, Salt, NKey)
Call Smart Contract
2. XStp = Contract Call (Contract Address)
3. XSt = concatenate XStp together
Verification
4. St = XSt ⊕ HRoot
5. Salt' = St[Salt]
6. if salt' is not equal to *Salt* then
7. throw
8. end if
Reverse Replacement
9. SuB = St[SuB]
11. DiB = [ ]
10. for j in range len (SuB):
11. DiB_raw[j] = Rule Table (SuB[j])
12. DiB. appended(DiB_raw[j])
13. end for
Reverse Diffusion
14. SB = [ ]
15. for z in range len (DiB)
16. SB_raw[z] = Rule Table (SB[z])
17. SB.appended(SB_raw[z])
18. end for
Reunion
19. BO = concatenate SB together