(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0063619
(43) 공개일자 2021년06월02일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 29/06* (2006.01)
(52) CPC특허분류
H04L 9/3213 (2013.01)
H04L 63/062 (2013.01)
(21) 출원번호 10-2019-0151960
(22) 출원일자 2019년11월25일
심사청구일자 2019년11월25일

(71) 출원인
서강대학교산학협력단
서울특별시 마포구 백범로 35 (신수동, 서강대학교)
주식회사 엠블럭
서울특별시 마포구 와우산로5길 17, 1층(상수동)
(72) 발명자
박수용
서울특별시 마포구 독막로 18 길 5, 101동 1001호 (상수동, 상수두산위브아파트)
이선재
서울특별시 성동구 마장로 137 텐즈힐 201동 1303호
(뒷면에 계속)
(74) 대리인
이지연

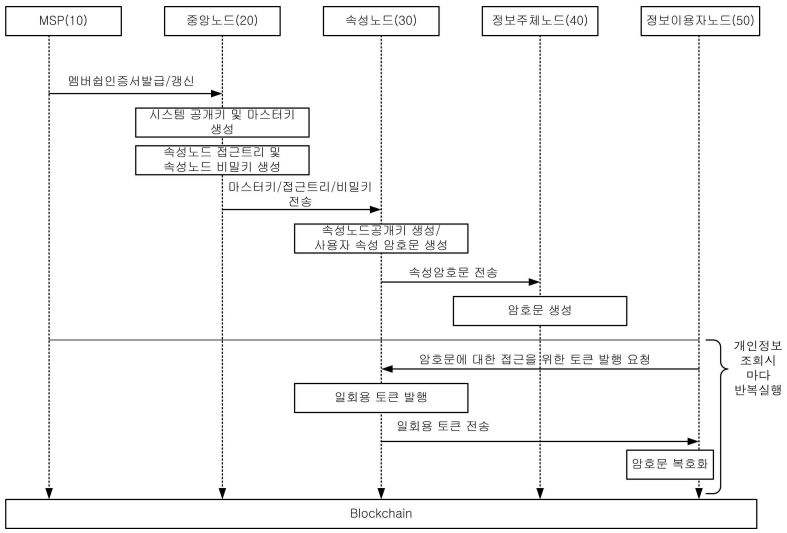
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 **속성을 기반으로 한 블록체인 네트워크에서의 접근 권한 제어 시스템 및 접근 권한 제어 방법**

(57) 요 약

본 발명은 복수 개의 노드들을 포함하는 블록체인 네트워크에서의 접근 권한 제어 시스템에 관한 것이다. 상기 접근 권한 제어 시스템은, 공개키와 비밀키를 생성하는 중앙 노드; 사용자 속성을 검증하고, 검증에 성공한 사용자에게는 일회용 토큰을 발급하는 속성 노드; 정보 주체가 배포하는 스마트 컨트랙트로서, 개인 정보를 속성 노드가 관리하는 접근 정책과 중앙 노드가 배포한 공개키로 암호화하여 암호문을 생성하여 블록체인에 기록하는 제1 스마트 컨트랙트; 정보 이용자가 배포하는 스마트 컨트랙트로서, 블록체인의 암호문에 대한 접근을 요청하고, 상기 접근 요청에 따라 속성 노드로부터 일회용 토큰을 제공받고, 일회용 토큰을 이용하여 중앙노드로부터 비밀키를 제공받고, 상기 비밀키를 이용하여 암호문을 복호화하는 제2 스마트 컨트랙트;를 구비하여, 속성을 기반으로 하여 개인 정보를 암호화하여 분산 원장에 저장하고 암호화된 정보를 복호화하는 것을 특징으로 한다.

대 표 도 - 도3



(52) CPC특허분류
H04L 63/067 (2013.01)
H04L 63/0823 (2013.01)
H04L 63/0838 (2013.01)
H04L 63/102 (2013.01)
H04L 9/3263 (2013.01)
H04L 9/3297 (2013.01)
H04L 2209/38 (2013.01)
(72) 발명자
이도현
서울특별시 관악구 대학길 119 대진하우스 102호

한세진
경기도 군포시 고산로539번길 24 동성백두아파트

이 발명을 지원한 국가연구개발사업

과제고유번호	1711093140
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보통신기술인력양성(R&D)
연구과제명	적응형 블록체인 플랫폼 기술 개발 및 전문 인력 양성
기 여 율	100/100
과제수행기관명	서강대학교산학협력단
연구기간	2019.01.01 ~ 2019.12.31

명 세 서

청구범위

청구항 1

복수 개의 노드들을 포함하는 블록체인 네트워크에서의 접근 권한 제어 시스템에 있어서,

상기 노드들 중 단일의 중앙 노드와 속성 노드를 선정하는 MSP;

공개키와 비밀키를 생성하는 중앙 노드;

사용자 속성을 검증하고, 검증에 성공한 사용자에게는 일회용 토큰을 발급하는 속성 노드;

정보 주체가 배포하는 스마트 컨트랙트로서, 개인 정보를 속성 노드가 관리하는 접근 정책과 중앙 노드가 배포한 공개키로 암호화하여 암호문을 생성하여 블록체인에 기록하는 제1 스마트 컨트랙트;

정보 이용자가 배포하는 스마트 컨트랙트로서, 블록체인의 암호문에 대한 접근을 요청하고, 상기 접근 요청에 따라 속성 노드로부터 속성을 검증받고, 검증 성공시 속성 노드로부터 일회용 토큰을 제공받고, 일회용 토큰을 이용하여 중앙노드로부터 비밀키를 제공받고, 상기 비밀키를 이용하여 암호문을 복호화하는 제2 스마트 컨트랙트;

를 구비하여, 속성을 기반으로 하여 개인 정보를 암호화하여 분산 원장에 저장하고 암호화된 정보를 복호화하는 것을 특징으로 하는 블록체인 네트워크에서의 접근 권한 제어 시스템.

청구항 2

제1항에 있어서, 상기 접근 정책은 접근 트리로 표현되며,

상기 접근 트리는 정보 이용자의 자격 속성을 나타내는 부분 트리와 상기 개인 정보에 대한 보유 기간을 나타내는 부분 트리의 AND 게이트로 표현된 것을 특징으로 하는 블록체인 네트워크에서의 접근 권한 제어 시스템.

청구항 3

제1항에 있어서, 상기 속성 노드는 정보 이용자로부터의 암호문 접근 요청에 따라, 자격 속성과 타임 스탬프를 포함한 정보 이용자의 속성을 이용하여, 정보 이용자에 대한 일회용 토큰을 생성하고, 생성된 일회용 토큰을 정보 이용자 노드에게 전송하는 것을 특징으로 하는 블록체인 네트워크에서의 접근 권한 제어 시스템.

청구항 4

복수 개의 노드들을 포함하는 블록체인 네트워크에서의 접근 권한 제어 시스템에 있어서,

사용자의 속성을 검증하여 검증에 성공하면 일회용 토큰을 발행하여 정보 주체에게 전송하는 속성 노드;

정보 주체에 의해 배포되는 스마트 컨트랙트로서, 사용자의 속성을 기반으로 한 접근 정책으로 데이터를 암호화하여 암호문을 생성하여 블록체인에 기록하는 제1 스마트 컨트랙트;

정보 이용자가 배포하는 스마트 컨트랙트로서, 블록체인의 암호문에 대한 접근을 요청하고, 상기 접근 요청에 따라 속성 노드로부터 일회용 토큰을 제공받고, 일회용 토큰을 이용하여 중앙노드로부터 비밀키를 제공받고, 상기 비밀키를 이용하여 암호문을 복호화하는 제2 스마트 컨트랙트;

을 구비하여, 속성을 기반으로 하여 개인 정보를 암호화하여 분산 원장에 저장하고 분산 원장의 암호문을 복호화하는 것을 특징으로 하는 블록체인 네트워크에서의 접근 권한 제어 시스템.

청구항 5

제4항에 있어서, 상기 접근 정책은 접근 트리로 표현되며,

상기 접근 트리는 정보 이용자의 자격 속성을 나타내는 부분 트리와 상기 개인 정보에 대한 보유 기간을 나타내는 부분 트리의 AND 게이트로 표현된 것을 특징으로 하는 블록체인 네트워크에서의 접근 권한 제어 시스템.

청구항 6

제4항에 있어서, 상기 속성 노드는,

정보 이용자 노드로부터의 암호문 접근 요청에 따라, 자격 속성과 타임 스탬프를 포함한 정보 이용자의 속성을 이용하여, 정보 이용자에 대한 일회용 토큰을 생성하고, 생성된 일회용 토큰을 정보 이용자 노드에게 전송하는 것을 특징으로 하는 블록체인 네트워크에서의 접근 권한 제어 시스템.

청구항 7

제4항에 있어서, 상기 접근 권한 제어 시스템은,

블록체인 네트워크를 구성하는 노드들 중 단일의 중앙 노드와 K개의 속성 노드들이 설정되며,

K개의 속성 노드들은 해당 속성 노드들에 포함된 사용자의 정보 요청에 따라 속성 검증을 수행하고 검증에 성공한 사용자에게는 일회용 토큰을 발행하는 것을 특징으로 하는 블록체인 네트워크에서의 접근 권한 제어 시스템.

청구항 8

제7항에 있어서, 상기 중앙 노드는

1개의 시스템 공개키와 K개의 마스터키를 생성하고 이를 이용하여 K개의 속성 노드 비밀키들을 생성하며, 시스템 공개키를 이용하여 K개의 속성 노드 접근 트리들을 생성하고,

상기 중앙 노드는 상기 마스터키, 속성 노드 접근 트리, 속성 노드 비밀키를 상기 속성 노드에게 전달하는 것을 특징으로 하는 블록체인 네트워크에서의 접근 권한 제어 시스템.

청구항 9

중앙 노드, 속성 노드, 정보 주체에 의해 배포된 제1 스마트 컨트랙트 및 정보 이용자에 의해 배포된 제2 스마트 컨트랙트를 포함하는 블록체인 네트워크에서의 접근 권한 제어 방법에 있어서,

(a) 상기 중앙 노드가 공개키와 비밀키를 생성하는 단계;

(b) 속성 노드가 속성 노드 공개키를 생성하고, 속성 노드 접근 트리를 이용하여 사용자 속성에 대한 속성 암호문을 생성하여 제1 스마트 컨트랙트에게 전송하는 단계;

(c) 정보 주체가 제1 스마트 컨트랙트를 통해, 개인 정보를 속성 노드가 관리하는 접근 정책과 중앙 노드가 배포한 공개키로 암호화하여 블록체인에 기록하는 단계;

를 구비하여, 속성 기반으로 하여 개인 정보를 암호화하여 분산 원장에 저장하는 것을 특징으로 하는 블록체인 네트워크에서의 접근 권한 제어 방법.

청구항 10

제9항에 있어서, 상기 접근 정책은 접근 트리로 표현되며,

상기 접근 트리는 정보 이용자의 자격 속성을 나타내는 부분 트리와 상기 개인 정보에 대한 보유 기간을 나타내는 부분 트리의 AND 게이트로 표현된 것을 특징으로 하는 블록체인 네트워크에서의 접근 권한 제어 방법.

청구항 11

제9항에 있어서, 상기 접근 권한 제어 방법은,

(d) 정보 이용자가 제2 스마트 컨트랙트를 통해, 블록체인의 암호문에 대한 접근을 속성 노드에게 요청하고, 상기 접근 요청에 따라 속성 노드로부터 일회용 토큰을 제공받고, 일회용 토큰을 이용하여 중앙노드로부터 비밀키를 제공받고, 상기 비밀키를 이용하여 암호문을 복호화하는 단계;

를 더 구비하는 것을 특징으로 하는 블록체인 네트워크에서의 접근 권한 제어 방법.

청구항 12

제11항에 있어서, 상기 속성 노드는,

정보 이용자에 의해 배포된 제2 스마트 컨트랙트를 통한 암호문 접근 요청에 따라, 자격 속성과 타임 스탬프를 포함한 정보 이용자의 속성을 이용하여, 정보 이용자에 대한 일회용 토큰을 생성하고, 생성된 일회용 토큰을 제2 스마트 컨트랙트에게 전송하는 것을 특징으로 하는 블록체인 네트워크에서의 접근 권한 제어 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 블록체인 네트워크에서의 접근 권한 제어 시스템 및 접근 권한 제어 방법에 관한 것으로서, 더욱 구체적으로는 블록체인 네트워크에 있어서, 이용자의 자격 속성 및 데이터의 보유 기간에 대한 속성을 기반으로 하여 데이터를 암호화 및 복호화하도록 함으로써, 데이터에 대한 접근 권한을 제어할 수 있도록 하는 블록체인 네트워크에서의 접근 권한 제어 시스템 및 접근 권한 제어 방법에 관한 것이다.

배 경 기 술

[0002] 블록체인은 암호화폐인 비트코인을 구현하는 기반 기술로서 2008년에 처음으로 소개되었다. 블록체인은 별도의 중앙기관이 존재하지 않는 피어-투-피어(Peer-to-peer)구조에서 가명의 계정을 사용하여 거래를 주고 받을 수 있는 혁신적 기술로 평가된다. 중앙기관이 존재하지 않아도 거래가 정상적으로 수행될 수 있는 것은 모든 데이터 기록이 각 노드에 동일하게 복제된 분산원장을 사용하기 때문이다. 분산원장은 블록체인의 핵심적인 기술로서, 일정 시간 동안 모아진 거래의 집합인 블록들을 시간 순으로 나열한 것이며, 각 블록은 전후 블록의 해쉬값을 참조하는 형식으로 서로가 연결된다. 블록은 작업증명(Proof of work, POW)등과 같은 합의 알고리즘에 따라 선발된 하나의 노드에 의하여 승인되어 블록체인에 추가된다.

[0003] 블록체인은 데이터의 위변조가 어려운 불변성, 중앙기관이 필요 없는 탈중앙화, 거래 기록의 타당성을 모든 참가자가 검증하는 투명성의 특징을 지닌다. 블록체인은 이러한 특징으로 인하여 다양한 응용분야에 활용되고 있다. 블록체인은 참여 범위에 따라 참여 제한이 없는 공개형과 참여 제한이 있는 허가형으로 나뉜다. 공개형은 블록체인이 태생부터 추구해온 목표인 완전한 분산화와 가장 가까운 형태이지만 현실적으로는 다양한 곳에 적용되기 힘들다는 문제점이 있다. 반면, 허가형은 블록체인의 참여나 정보 열람 자격 등을 제한하기 때문에 공개형보다는 개인정보보호 측면에서는 좀더 현실적인 대안이 될 수 있다.

[0004] 한편, 접근통제 시스템은 조직이 보유한 자원을 보호하기 위하여 누가, 어디서, 어떠한 자원에 대하여 어떠한 동작을 하는지에 대한 허용 또는 거부를 결정하는 시스템이다. 즉, 접근 통제는 접근 정책을 기반으로 이용자 신원을 승인한 이후 부여된 접근권한을 확인하며, 해당 접근권한을 기준으로 할당된 자원에 대한 접근을 허용 또는 거부를 하는 절차를 거친다. 조직에서 사용되는 접근통제시스템은 이용자의 개인정보, 민감정보, 직위 등을 포함한 다양한 정보를 바탕으로 하기에 지속적이고 무결한 모니터링이 필요하다.

[0005] 전술한 접근 통제는 통상적으로 3가지의 원칙이 충족되어야 한다. 첫 번째는 '필요성의 원칙'으로 이용자 별로 해당 업무 및 관련 업무에 대해서만 접근 권한을 부여해야 함을 의미한다. 두 번째는 '최소권한의 원칙'으로 허가 받은 일을 수행하기 위한 최소한의 권한만을 부여하여, 권한 남용으로 인한 피해를 최소화하는 원칙을 의미한다. 세 번째는 '직무분리의 원칙'으로 업무의 발생으로부터 승인, 수정, 확인, 완료 등이 처음부터 끝까지 한 사람에 의해 처리될 수 없도록 하는 보안 정책을 의미한다.

[0006] 접근 통제 프로세스에서 접근 및 관리되는 다양한 부류의 정보 및 데이터 중에는 기밀 정보, 영업 정보, 개인정보, 민감정보 등 다양하게 다뤄질 수 있다. 이에 따라 다양한 분류의 정보 및 데이터를 활용하는 블록체인의 경우 접근 통제 측면에서 다양한 요구사항들이 도출될 수 있다. 그 중 가장 엄격하게 다뤄지는 정보의 대표적 부류가 개인정보이다.

[0007] 개인정보란 개인정보보호법에 의하면 살아있는 개인을 알아볼 수 있는 정보 및 다른 정보와 쉽게 결합하여 개인을 알아볼 수 있는 정보이다. 대한민국을 포함한 세계 주요 국가는 개인정보 보호법을 시행하고 있으며 특히 EU(유럽연합)는 2018년 5월 25일부터 유럽시민의 개인정보를 취급하는 사업자 등을 대상으로 일반 정보보호 규정(General Data Protection Regulation, GDPR)을 시행하고 있다. 그러나 블록체인의 탈중앙화 및 분산원장의 특성은 개인정보 보호 의무를 준수하고 책임을 부담하는 중앙기관에 기반한 현행의 GDPR규범 체계가 상충된다. 즉, 블록체인 기술은, 개인정보 목적에 부합한 수집 또는 최소수집 원칙 등 전술한 접근통제 3가지 원칙과 관련한 성질을 충족하기 어려운 설계구조를 가지고 있고, 정보주체의 정보통제권(잊혀질 권리 등)을 어렵게 하며,

탈중앙화의 특성상 정보유출에 대한 과실 책임에 대한 소지도 불분명하기 때문에 특히 공개형 블록체인이 현재의 GDPR체계와 정합될 것인지에는 많은 논란의 여지가 존재한다.

[0008] 한편, 블록체인 상에서 데이터 보호를 위하여 다양한 기술들이 제안되고 있다. 먼저, 속성기반 암호화 기술은 시스템에 저장된 데이터에 일정한 접근정책을 부여하고 이를 암호화한 다음, 데이터 이용자가 동 접근정책을 충족하는 속성을 지닐 경우에 복호화를 허용하는 암호 스킴이다. 속성기반 암호화는 제3의 신뢰기관을 중심으로 운영된다. 신뢰기관은 정보주체가 정보의 접근정책을 정의하여 암호화할 수 있도록 접근정책과 공개키를 관리한다. 또한 정보이용자의 자격 속성을 검증하고 비밀키를 발급하는 역할을 수행한다. 속성기반 암호화에서 신뢰기관은 가장 핵심적인 역할을 담당하는 부분이 된다. 탈중앙 구조의 블록체인에서 속성기반 암호화를 사용하기 위해서는 키와 속성을 관리할 새로운 메커니즘이 필요하다.

[0009] 개인정보를 암호화 기술로 은닉하여 정보를 노출하지 않고도 주어진 업무를 처리할 수 있다. 이는 영지식증명 기술로 구현 가능하다. 영지식증명(zero-knowledge proof)이란 거래 상대방에게 어떠한 정보도 제공하지 않은 채, 자신이 해당 정보를 가지고 있거나 알고 있다는 사실을 증명하는 것을 말한다. 영지식증명을 이용한 개인정보 보호의 대표적인 사례는, ZCash라고 하는 암호화폐이다. ZCash는 거래상대방에게 자신이 보유한 잔액이 거래금액보다 같거나 크다는 것을 영지식증명을 이용하여 증명함으로써 거래상대방에게 잔액을 노출하지 않고도 거래를 할 수 있다. 이와 같은 영지식증명 방식은 블록체인과 같은 다자간의 비대면 통신 프로토콜에서 개인정보 보호 기능을 제공하기 위한 고급 암호 기술로 분류된다.

[0010] 한편, 프라이빗 블록체인 기술 중 하나인 하이퍼레저 패브릭은 채널(channel)을 이용하여 접근 통제를 수행한다. 하이퍼레저 패브릭은 이해관계가 맞는 조직들로 분리되어 채널을 형성하며 해당 채널간에만 원장을 공유함으로써, 타 채널에서 유지되는 원장은 열람할 수 없고 접근이 차단된다. 하지만, 많은 채널이 생성될 경우, 각 노드는 다수의 원장을 관리하여야 하므로 매우 비효율적인 측면이 있기 때문에, 개인 사용자를 대상으로 하는 접근 제어 방식이 필요하다. 하이퍼래저 패브릭은 채널 내에서도 정보의 접근을 제한하기 위하여 'visibility setting'과 같은 기능을 제공하기도 하며, 체인코드를 이용하여 역할에 따른 접근제어 로직을 구현할 수도 있다. 그러나 이 경우 반드시 복호키의 발행 및 배포 방식을 사용자가 구현할 수 있어야 한다.

[0011] 전술한 바와 같이, 블록체인 상에서 데이터 보호를 위하여 제안되고 있는 기술들은 비효율성이 발생되고, 다양한 문제점들이 내포되어 있는 실정이다.

선행기술문헌

특허문헌

[0012] (특허문헌 0001) 한국공개특허공보 제 10-2018-0101870호

(특허문헌 0002) 한국등록특허공보 제 10-0989605호

(특허문헌 0003) 한국등록특허공보 제 10-2025409호

발명의 내용

해결하려는 과제

[0013] 전술한 문제점을 해결하기 위한 본 발명의 목적은 블록체인 네트워크 상에서의 개인정보, 민감 정보 등의 데이터를 효율적이면서도 안전하게 보호할 수 있는 블록체인 네트워크에서의 접근 권한 제어 시스템을 제공하는 것이다.

[0014] 본 발명의 다른 목적은 블록체인 네트워크 상에서의 개인정보, 민감 정보 등의 데이터를 효율적이면서도 안전하게 보호할 수 있는 블록체인 네트워크에서의 접근 권한 제어 방법을 제공하는 것이다.

과제의 해결 수단

[0015] 전술한 기술적 과제를 달성하기 위한 본 발명의 제1 특징에 따른 복수 개의 노드들을 포함하는 블록체인 네트워크에서의 접근 권한 제어 시스템은, 상기 노드들 중 단일의 중앙 노드와 K개(블록체인에 참여하는 조직의 개수)의 속성 노드들을 선정하는 MSP; 공개키와 비밀키를 생성하는 중앙 노드; 사용자 속성을 검증하고 검증에 성

공한 사용자에게는 일회용 토큰을 발급하는 속성 노드; 개인정보를 속성 노드가 관리하는 접근정책과 중앙노드가 배포한 공개키로 암호화하여 블록체인에 기록하는 정보주체가 배포한 제1 스마트 컨트랙트; 암호문에 대한 접근을 요청하면, 상기 속성 노드로부터 속성을 검증받은 후, 검증 성공시 일회용 토큰을 제공받고, 상기 일회용 토큰을 중앙 노드에게 제시하여 중앙 노드로부터 비밀키를 제공받고, 해당 비밀키를 이용하여 암호문을 복호화하는 정보 이용자가 배포한 제2 스마트 컨트랙트;를 구비하여, 속성을 기반으로 하여 분산 원장의 데이터를 암호화 및 복호화한다.

[0016] 전술한 제1 특징에 따른 블록체인 네트워크에서의 접근 권한 제어 시스템에 있어서, 상기 접근 정책은 접근 트리로 표현되며, 상기 접근 트리는 이용자의 자격 속성들을 나타내는 부분 트리와 개인정보의 보유기간을 나타내는 부분 트리의 AND 게이트로 표현되는 것이 바람직히다.

[0017] 전술한 제1 특징에 따른 블록체인 네트워크에서의 접근 권한 제어 시스템에 있어서, 상기 속성 노드는 정보 이용자 노드로부터의 암호문 접근 요청에 따라, 자격 속성과 타임 스탬프를 포함한 정보 이용자의 속성을 이용하여 일회용 토큰을 생성하고, 생성된 일회용 토큰을 정보 이용자 노드에게 전송하는 것이 바람직하다.

[0018] 본 발명의 제2 특징에 따른 블록체인 네트워크에서의 접근 권한 제어 시스템은, 사용자의 속성을 검증하여 검증에 성공할 경우 일회용 코튼을 발생하여 정보주체에게 전송하는 속성 노드; 사용자의 속성을 기반으로 한 접근정책으로 데이터를 암호화하여 암호문을 생성하고 이를 블록체인에 기록하는 정보 주체의 제1 스마트 컨트랙트; 암호문에 대한 접근을 요청하면, 상기 속성 노드로부터 일회용 토큰을 제공받고, 상기 일회용 토큰을 이용하여 중앙 노드로부터 비밀키를 제공받고, 상기 비밀키를 이용하여 상기 암호문을 복호화하는 정보 이용자의 제2 스마트 컨트랙트;을 구비하여, 속성을 기반으로 하여 분산 원장의 데이터를 암호화 및 복호화한다.

[0019] 전술한 제2 특징에 따른 블록체인 네트워크에서의 접근 권한 제어 시스템에 있어서, 상기 접근 정책은 접근 트리로 표현되며, 자격 속성 트리와 보유 기간 속성 트리를 포함하는 것이 바람직하다.

[0020] 전술한 제2 특징에 따른 블록체인 네트워크에서의 접근 권한 제어 시스템에 있어서, 상기 속성 노드는 정보 이용자 노드로부터의 암호문 접근 요청에 따라, 자격 속성과 타임 스탬프를 포함한 정보 이용자의 속성을 이용하여 일회용 토큰을 생성하고, 생성된 일회용 토큰을 정보 이용자 노드에게 전송하는 것이 바람직하다.

[0021] 전술한 제2 특징에 따른 블록체인 네트워크에서의 접근 권한 제어 시스템은, 블록체인 네트워크의 노드들 중 단일의 중앙 노드와 K개의 속성 노드들이 설정되고, K개의 분산된 속성 노드들은 각 조직을 대표하는 노드로서, 해당 조직원인 사용자의 정보 요청에 대하여 속성 검증을 수행하고 검증에 성공한 사용자에게는 일회용 토큰을 발행한다. 일회용 토큰을 제공받은 사용자는 이를 중앙 노드에게 제시하여 자신이 적법한 자격을 가진 자임을 증명하고, 이로부터 비밀키를 발급받는다.

발명의 효과

[0022] 본 발명에 따른 블록체인 네트워크를 기반으로 한 접근 권한 제어 시스템은, 블록체인 내의 개인 정보를 포함한 다양한 정보에 대하여 사용자 단위별 권한에 따른 접근 통제를 할 수 있게 된다. 또한, 도 4는 본 발명과 종래의 유사 연구들에 대하여, 개인 정보에 대하여 GDPR 에서 요구하는 법적 준수 사항을 충족하는 정도를 비교한 도표이다. 도 4를 통해, 개인 정보의 경우, GDPR에서 요구하는 법적 준수 사항을 충족하며, 유사 연구에 비해 많은 장점이 있음을 알 수 잇다.

[0023] 또한, 본 발명에 따른 블록체인 네트워크를 기반으로 한 접근 권한 제어 시스템은, 별도의 신뢰 기관이 없으며 K개의 속성 노드들과 같이 다중 노드를 선정함으로써, 전체 네트워크의 정보 이용의 연속성과 데이터의 기밀성을 보장할 수 있다. 또한, 본 발명에 따른 시스템은 단일 노드와 복수개의 속성 노드로 구성되는 특징으로 인하여 블록체인 네트워크의 병목 현상을 해결할 수 있다. 즉, 기존의 속성기반 암호화 스킴에서 단일한 신뢰기관이 수행하는 역할인 사용자 속성 검증과 키 발급 기능을 분리하고 이를 각각 K개의 속성노드와 단일한 중앙 노드에게 부여하여 블록체인 네트워크의 부하를 분산시킬 수 있기 때문에 전체 시스템이 안정화 될 수 있다.

[0024] 또한, 본 발명에 따른 블록체인 네트워크를 기반으로 한 접근 권한 제어 시스템은, 영구적인 복호화키를 제공하는 것이 아니라 일회용 토큰을 이용하여 복호화키를 생성하게 됨으로써, 기존의 다른 속성 기반 암호화에 비하여, 키 관리에 대한 효율성과 보안성을 가진다. 따라서 속성 노드로부터 속성 검증에 실패한 정보 이용자는 키를 제공받을 수 있는 권한인 일회용 토큰을 획득할 수 없다. 이 경우 이용자는 정보를 복호화하지 못한다. 속성 노드로부터 검증에 실패한 경우란, 어떠한 사유로 이용자의 속성이 변동되어 기존의 접근정책과 속성이 일치하지 않는 경우 또는 개인정보의 보유기간 속성이 현재의 타임스탬프보다 과거일 경우에 해당된다. 이와 같이 속

성 검증과 키 발급 기능이 분리되면 정보 이용자의 속성 변동에 유연하게 대응할 수 있게 되며 변동된 속성을 위해 발급받았던 키를 갱신하거나 폐기할 필요가 없어진다. 또한 개인정보의 보유기간 만료시 자동으로 정보 접근을 차단할 수 있는 장점도 있다. 도 5는 본 발명과 종래의 유사 연구들에 대하여, 개인 정보에 대한 보안성을 평가하여 비교한 도표이다. 도 5를 통해, 본 발명에 따른 방법은 모든 분야에서 보안성이 향상되고 있음을 알 수 있다.

도면의 간단한 설명

[0025] 도 1은 본 발명의 바람직한 실시예에 따른 접근 권한 제어 시스템에 있어서, 각 노드에 대한 구성을 개략적으로 도시한 블록도이다.

도 2는 본 발명의 바람직한 실시예에 따른 접근 권한 제어 시스템에 있어서, 개인정보의 접근정책을 접근트리로 도시한 것으로서, 접근트리는 사용자의 속성을 나타내는 부분 트리(a)와 개인정보의 보유기간을 나타내는 부분 트리(b)로 구성된다.

도 3은 본 발명의 바람직한 실시예에 따른 블록체인 네트워크에서의 접근 권한 제어 시스템의 각 노드들의 동작을 전체적으로 도시한 흐름도이다.

도 4는 본 발명과 종래의 유사 연구들에 대하여, 개인 정보에 대하여 GDPR 에서 요구하는 법적 준수 사항을 충족하는 정도를 비교한 도표이다.

도 5는 본 발명과 종래의 유사 연구들에 대하여, 개인 정보에 대한 보안성을 평가하여 비교한 도표이다.

도 6은 본 발명의 바람직한 실시예에 따른 접근 권한 제어 시스템에 있어서, 중앙 노드와 K개의 속성 노드의 동작을 설명하기 위한 모식도이다.

도 7은 본 발명의 바람직한 실시예에 따른 접근 권한 제어 시스템에 있어서, 정보 주체 노드와 정보 이용자 노드의 동작을 설명하기 위한 모식도이다.

발명을 실시하기 위한 구체적인 내용

[0026] 본 발명은 블록체인의 블록에 포함된 기밀 정보, 개인 정보, 민감 정보 등을 포함한 다양한 데이터에 대하여 이용자의 권한, 접근 정책 및 보유 기간 등에 따른 차등적 접근 통제를 적용하는 블록체인을 기반으로 한 접근 권한 제어 시스템이다. 본 발명에 따른 접근 권한 제어 시스템은, 블록체인 거래에 포함된 정보에 따라 속성 기반 암호화를 활용하여 데이터의 속성에 따른 접근 정책으로 암호화하고 해당 접근 정책을 만족하는 정보 이용자만 해당 정보를 복호화하여 조회할 수 있도록 한다. 이에 따라, 블록체인인 분산 원장이 갱신되거나 조회될 때마다 스마트 컨트랙트를 통해 속성기반 암호화 및 복호화를 실행하게 된다. 본 발명에 따른 접근 권한 제어 시스템에 있어서, 속성은 접근정책을 기준으로 속성 노드에 의해 검증되고, 검증된 이용자에게는 일회용 토큰이 발행된다. 중앙 노드는 이용자의 일회용 토큰을 통해 비밀키를 생성하며, 이러한 비밀키는 암호문을 복호화하기 위한 키에 해당된다. 접근트리는 사용자의 속성을 나타내는 부분 트리와 개인정보의 보유기간을 나타내는 부분 트리로 구성된다. 상기 두개의 부분 트리는 AND게이트로 연결된다. 부분 트리 a는 사용자의 속성을 표현하는 리프노드(Leaf node)와 이들간의 논리적 관계를 나타내는 AND, OR게이트로 구성된다. 정보 이용자의 속성을 검증하기 위해서는 트리의 리프노드와 속성값을 비교하여 일치할 경우 해당 트리 노드 값이 참이 된다. 이와 같은 동작을 리프노드로부터 루트노드까지 반복 실행하여 전체 트리 노드가 참이 될 경우 속성 검증에 성공한다.

[0027] 본 발명에 따른 접근 권한 제어 시스템은 정보 주체가 거래 정보를 생성할 때 정보에 접근할 수 있는 속성 구조(access structure)를 기반으로 한 접근정책으로 암호화하여 이를 블록체인에 기록한다. 한편, 정보 이용자가 암호화된 데이터에 대한 접근을 요청하면, 속성 노드는 정보 이용자에 대한 자격 속성과 타임 스탬프를 이용하여 일회용 토큰(tu)을 생성한다. 정보 이용자는 속성 노드가 제공한 일회용 토큰을 이용하여 중앙 노드로부터 비밀키를 제공받아 이를 통해 데이터에 접근할 수 있다. 정보는 접근 정책과 보유 기간으로 암호화되고, 속성 노드는 정보 이용자의 속성 정보와 접근 요청 시간 정보를 이용하여, 정보 이용자에 대한 일회용 토큰을 생성하여 발행한다. 이때, 정보 이용자의 속성과 해당 정보에 대한 접근 정책이 일치해야 일회용 토큰을 제공받을 수 있다.

[0028] 속성 기반 암호화는 접근 정책에 기반하여 동작한다. 접근 정책이란 각 정보 주체가 접근할 수 있는 객체에 대한 정보를 기술해 놓은 정책으로서, 정보 주체의 경우 직책과 직무 등을 포함한 주체를 표현하는 다양한 정보가 속성으로 부여되고, 객체는 보유 기간이 부여된다. 접근 정책은 조직의 정책에 따라 언제든지 추가, 수정, 삭제

될 수 있다.

[0029] 속성 기반 암호화에서는 접근 정책을 접근 트리 형태로 표현한다. 접근 트리는 모든 주체의 속성을 리프 노드로 구성하고 각 속성간의 관계를 내부 노드로 구성한다. 이어, 트리 탐색 알고리즘을 통해 임의의 정보 이용자의 속성이 접근 정책과 일치하는지 판단할 수 있다.

[0030] 암호화와 복호화는 단일 중앙 노드와 K개의 속성 노드로 동작한다. 접근트리는 사용자의 자격 속성을 나타내는 부분 트리와 개인정보의 보유기간을 나타내는 부분 트리로 구성된다. 상기 두개의 부분 트리는 AND게이트로 연결된다. 자격 속성을 나타내는 부분 트리는 사용자의 속성을 표현하는 리프노드(Leaf node)와 이들간의 논리적 관계를 나타내는 AND, OR게이트로 구성된다. 보유기간 속성을 나타내는 부분 트리는 개인정보가 블록체인에 기록된 시점의 날짜에 해당 개인정보의 법적 최대 보유기간(10년 등)을 기산하여 트리로 표현한다. 즉, 보유기간 속성 트리는 문자가 아닌 숫자에 대한 대소 비교를 하여야 하므로, 보유기간 속성 트리는 별도의 비트열로 구성된 트리(n-bit integer)로 구성한 다음, 정보 이용자가 정보를 요청한 타임 스탬프보다 같거나 큰지를 비교한다.

[0031] 이하, 도 1을 참조하여 본 발명의 바람직한 실시예에 따른 접근 권한 제어 시스템의 각 노드에 대한 구조를 구체적으로 설명한다. 도 1은 본 발명의 바람직한 실시예에 따른 접근 권한 제어 시스템에 있어서, 각 노드에 대한 구성을 개략적으로 도시한 블록도이다.

[0032] 도 1을 참조하면, 본 발명에 따른 블록체인을 기반으로 한 접근 권한 제어 시스템의 각 노드는, 블록체인 모듈(100), 감시 모듈(110), 접근 제어 모듈(120), 암호 모듈(130), 및 접근 정책 모듈(140)을 구비한다.

[0033] 상기 블록체인 모듈(Blockchain Module; 100)은, 거래를 생성하고 유효성을 검증한 후 블록에 추가하여 조회한다. 상기 감시 모듈(Auditing Module; 110)은, 누가 언제 어떤 개인 정보를 암호화하여 블록에 저장하였고 복호화하여 조회하였는지를 감시하고 기록한다. 상기 접근 제어 모듈(Access control Module; 120)은, 블록체인 개인 정보에 누가 어떤 정보를 언제까지 조회할 수 있는가에 대한 규칙을 정의하며, 필요시 접근 정책은 수정, 삭제 및 추가될 수 있다.

[0034] 상기 암호 모듈(Cryptography Module; 130)은, 블록체인상의 정보를 접근 정책을 참조하여 암호화하고, 정보 이용자의 속성에 따라 복호화한다. 상기 접근 정책 모듈(Access Control Policy Module; 140)은 블록체인의 개인 정보에 대하여 누가 어떤 정보를 언제까지 조회할 수 있는가에 대한 규칙인 접근 정책을 정의하며, 필요시에는 접근 정책은 수정, 삭제, 추가될 수 있다. 접근 정책은 모두 주체와 객체의 속성에 논리연산(AND, OR)을 결합한 트리 구조로 구현된다.

[0035] 도 2는 본 발명의 바람직한 실시예에 따른 접근 권한 제어 시스템에 있어서, 자격 속성 부분 트리(a)와 보유기간 속성 부분 트리로 구성된 접근트리(b)를 예시적으로 도시한 것이다. 접근 트리는, 도 2에 도시된 바와 같이, K개의 부분 트리로 나누어 처리되며, shamir의 비밀분산법에 의하여 각 부분 트리의 값이 모두 만족될 때 일회용 토큰이 발행될 수 있다.

[0036] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예에 따른 블록체인 네트워크에서의 접근 권한 제어 시스템의 동작에 대하여 구체적으로 설명한다.

[0037] 도 3은 본 발명의 바람직한 실시예에 따른 블록체인 네트워크에서의 접근 권한 제어 시스템의 각 노드들의 동작을 전체적으로 도시한 흐름도이다.

[0038] 도 3을 참조하면, 본 발명에 따른 블록체인 네트워크에서의 접근 권한 제어 시스템은, 멤버쉽 서비스 프로바이더(10: Membership Service Provider; MSP), 중앙 노드(20), K개의 속성 노드들(30), 정보 정보 주체가 배포한 제1 스마트 컨트랙트(40), 정보 이용자가 배포한 제2 스마트 컨트랙트(50)를 포함한다.

[0039] 상기 MSP는 블록체인 네트워크를 구성하는 노드들 중 1개의 중앙 노드와 K개의 분산된 속성 노드들을 설정한다. K개의 분산된 속성 노드들은 각 조직을 대표하는 노드로서, 제2 스마트 컨트랙트를 통해 해당 조직의 구성원인 사용자의 정보 요청이 발생되면, 속성 검증을 수행하고, 검증에 성공한 사용자에게는 일회용 토큰을 발행한다. 일회용 토큰을 제공받은 사용자는 이를 중앙 노드에게 제시하고 자신이 적법한 자격을 가진 자임을 증명하고, 이로부터 비밀키를 발급하게 된다. 이에 따라, 사용자는 중앙 노드로부터 발급된 비밀키를 이용하여 암호문을 복호화할 수 있게 된다.

[0040] 도 6은 본 발명의 바람직한 실시예에 따른 접근 권한 제어 시스템에 있어서, 중앙 노드와 K개의 속성 노드의 동작을 설명하기 위한 모식도이다. 도 6을 참조하면, 상기 중앙 노드는 MSP에 의해 선정되며, 암호화에 사용될 시

스템 공개키와, 비밀키, 그리고 비밀키 생성에 사용되는 마스터키를 생성한다. 메시지 암호화 및 사용자에게 분배할 수 있는 모든 속성값들의 집합을 정의하며 암호화에 사용되는 공개키 PK와 개인키 발급에 사용되는 마스터키 MK를 생성한다.

[0041] 도 7은 본 발명의 바람직한 실시예에 따른 접근 권한 제어 시스템에 있어서, 정보 주체 노드와 정보 이용자 노드의 동작을 설명하기 위한 모식도이다. 도 7을 참조하면, 정보 이용자 노드는 정보 이용자의 속성을 접근정책 기준으로 검증하여 검증에 성공할 경우 정보 이용자에 대한 일회용 토큰을 생성한다. 상기 정보 이용자 노드는 상기 속성 노드로부터 제공받은 일회용 토큰을 이용하여 중앙 노드에게 비밀키를 요청하고 중앙노드는 일회용 토큰 값이 적정할 경우 비밀키를 발급한다. 정보 이용자는 상기 비밀키를 이용하여 암호문을 복호화하여 원문을 얻게 된다

[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] 10 : 멤버쉽 서비스 프로바이더(Membership Service Provider; MSP)

20 : 중앙 노드

30 : K개의 속성 노드들

40 : 정보 주체 노드가 배포하는 제1 스마트 컨트랙트

50 : 정보 이용자 노드가 배포하는 제2 스마트 컨트랙트

100 : 블록체인 모듈

110 : 감시 모듈

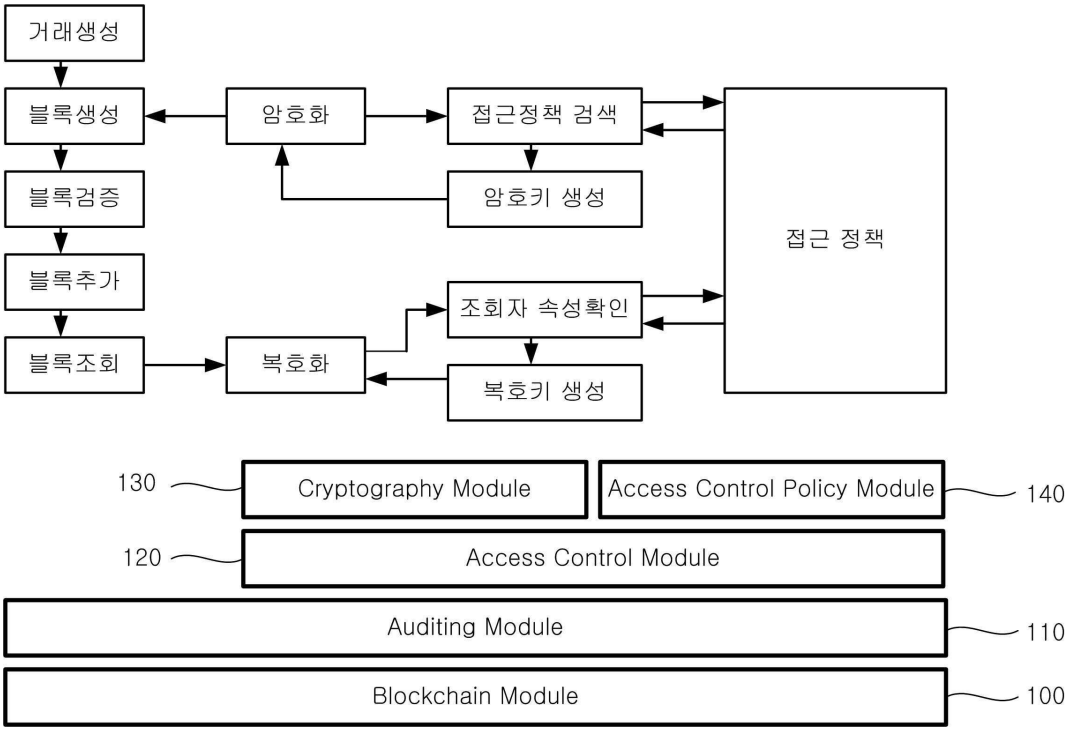
120 : 접근 제어 모듈

130 : 암호 모듈

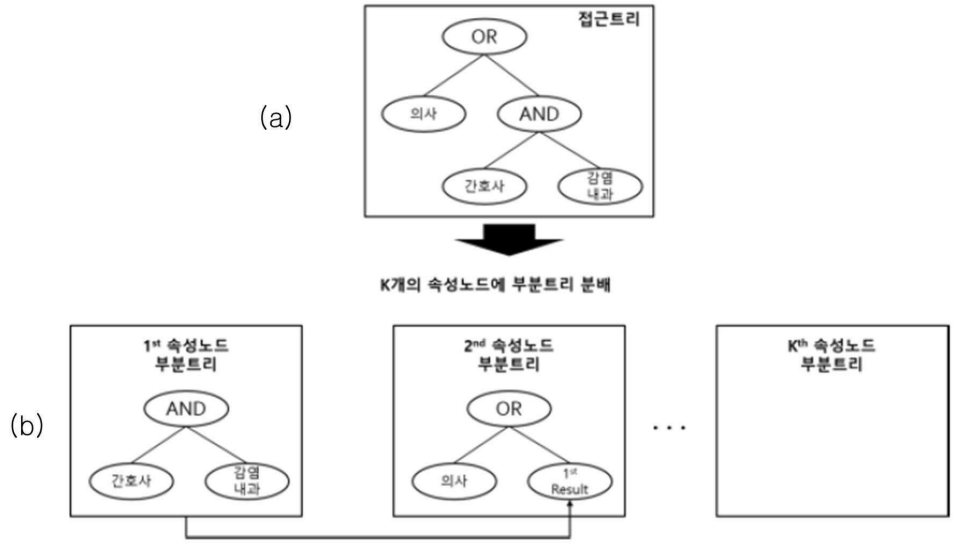
140 : 접근 정책 모듈

도면

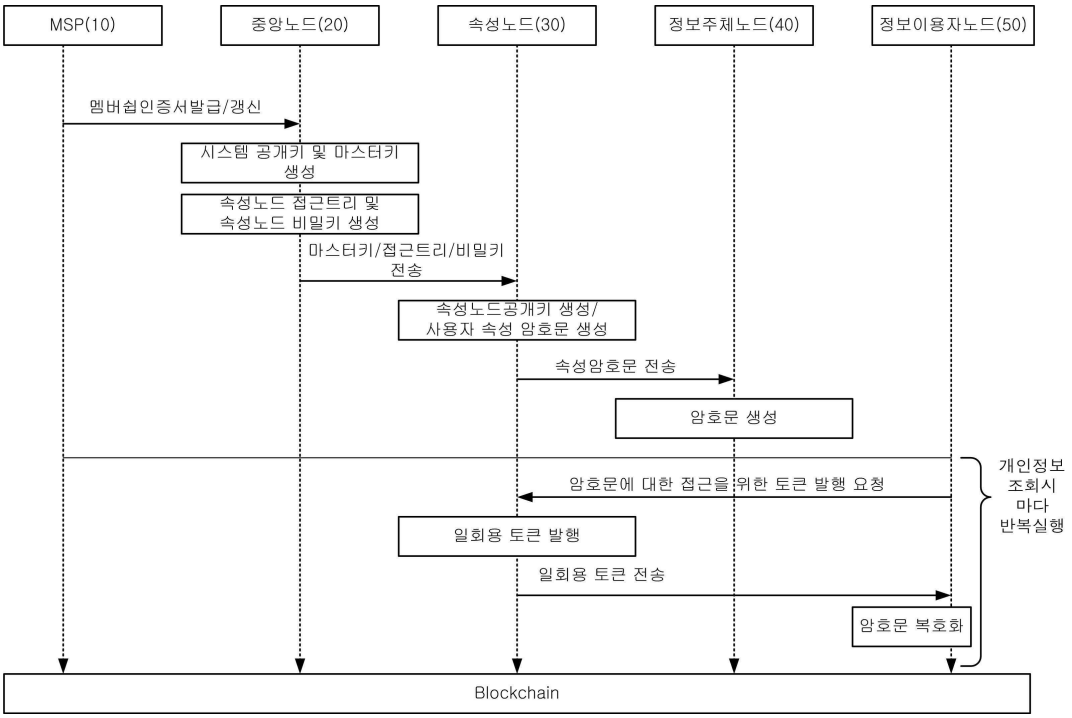
도면1


거래생성
블록생성
암호화
접근정책 검색
블록검증
암호키 생성
접근 정책
블록추가
조회자 속성확인
블록조회
복호화
복호키 생성
130
Cryptography Module
Access Control Policy Module
140
120
Access Control Module
Auditing Module
110
Blockchain Module
100

도면2


(a)
접근트리
OR
의사
AND
간호사
감염내과
K개의 속성노드에 부분트리 분배
(b)
1st 속성노드 부분트리
AND
간호사
감염내과
2nd 속성노드 부분트리
OR
의사
1st Result
...
Kth 속성노드 부분트리

도면3



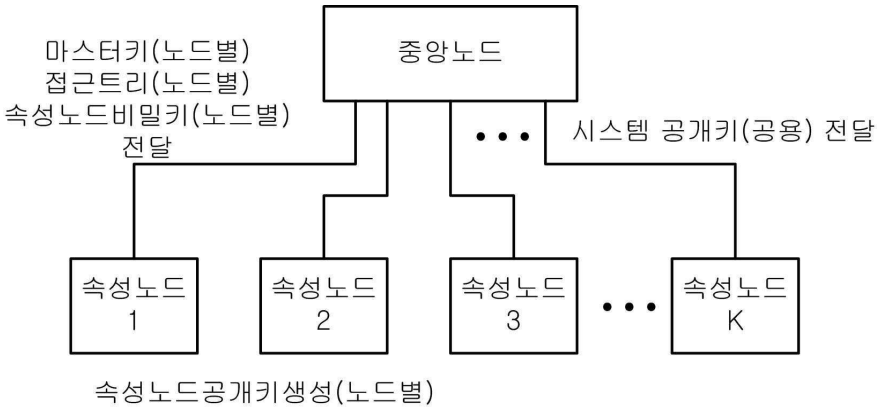
도면4

구분	Ours	ZKP	MPC	동형암호	주소은폐
적법성	O	X	X	X	X
삭제 및 정정	O	X	X	X	X
처리제한	O	O	O	O	X
정확성	O	X	X	X	X
보유기간 제한	O	X	X	X	X
민감정보 처리	O	O	O	O	X

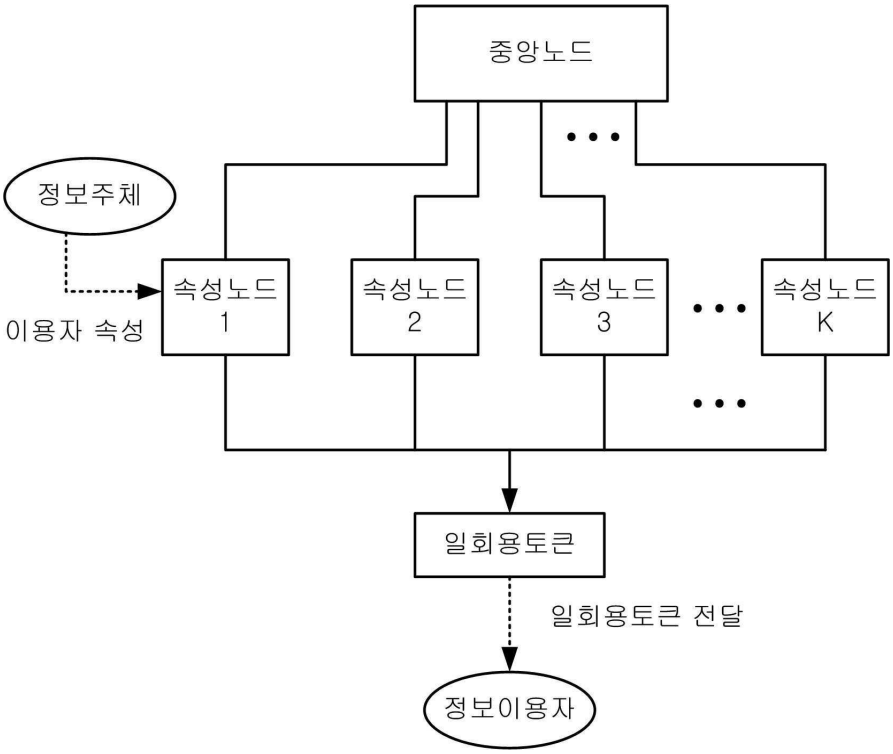
도면5

구분	Ours	Bethencourt	JEMEL	Chase	S&W
속성변경 유연성	O	X	O	X	X
오라클 방지	O	X	O	O	X
책임추적성	O	X	O	X	X
보유기간 통제	O	O	X	X	X
키분실위험관리	O	X	O	X	X
단일점장애감내	O	X	O	O	X
계산량	$O(C^n)$	$O(C^n)$	$O(C^n)$	$O(C^n)$	$O(C^n)$

도면6


마스터키(노드별)
접근트리(노드별)
속성노드비밀키(노드별)
전달
중앙노드
시스템 공개키(공용) 전달
속성노드 1
속성노드 2
속성노드 3
속성노드 K
속성노드공개키생성(노드별)

도면7


중앙노드
정보주체
이용자 속성
속성노드 1
속성노드 2
속성노드 3
속성노드 K
일회용토큰
일회용토큰 전달
정보이용자