



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0032412
(43) 공개일자 2020년03월26일

(51) 국제특허분류(Int. Cl.)

H04L 9/08 (2006.01)

(52) CPC특허분류

H04L 9/0825 (2013.01)

H04L 9/0844 (2013.01)

(21) 출원번호 10-2018-0111415

(22) 출원일자 2018년09월18일

심사청구일자 2018년09월18일

(71) 출원인

이화여자대학교 산학협력단

서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)

(72) 발명자

김현정

경상북도 포항시 북구 삼호로 391, 117동 203호 (환호동, 환호해맞이그린빌)

도인실

인천광역시 연수구 센트럴로 194, 201동 2705호 (더샵센트럴파크2단지아파트)

채기준

서울특별시 강남구 강남대로136길 34, 402호 (논현동, 월드노블레스빌)

(74) 대리인

윤귀상

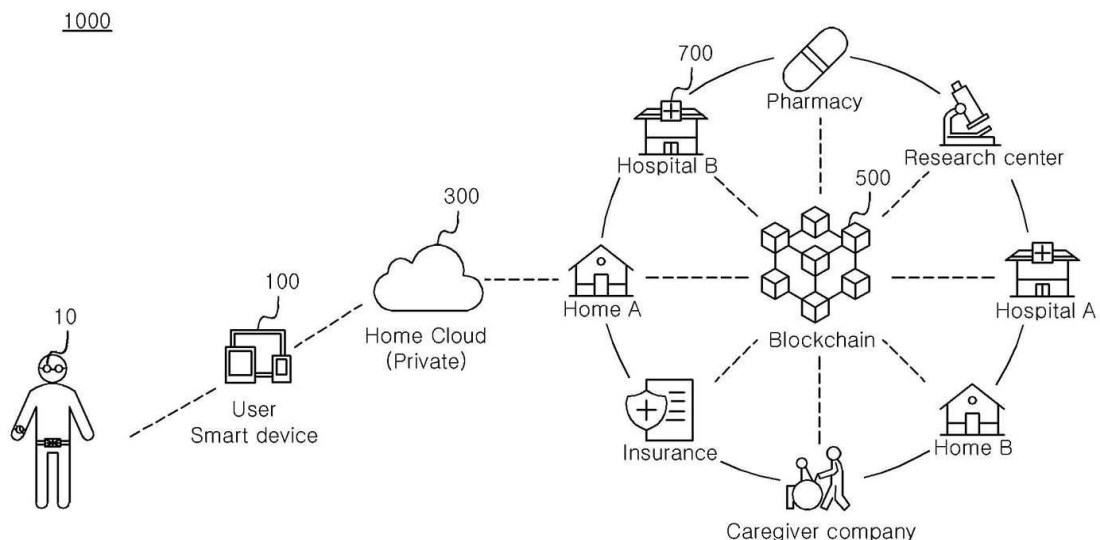
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **블록체인 기반의 데이터 공유 방법, 이를 수행하기 위한 클라우드 서버 및 이를 포함하는 데이터 공유 시스템**

(57) 요약

블록체인 기반의 데이터 공유 방법, 이를 수행하기 위한 클라우드 서버 및 이를 포함하는 블록체인 기반의 데이터 공유 시스템이 개시된다. 블록체인 기반의 데이터 공유 방법은 블록체인에 참여하는 다른 참여자들과 공유하는 암호화키 생성 소스를 이용하여 암호화키를 생성하는 단계, 상기 사용자 단말로부터 상기 사용자 정보를 수신하는 경우, 상기 사용자 정보를 상기 암호화키로 암호화하여 상기 블록체인에 저장하는 단계 및 상기 블록체인에 참여하는 다른 참여자로부터 상기 사용자 정보 열람 요청을 수신하는 경우, 상기 블록체인에 저장된 상기 사용자 정보의 암호문인 상기 암호화키를 상기 다른 참여자가 생성하는 암호화키로 변환시키는 재암호화키를 생성하고, 상기 재암호화키로 상기 블록체인에 저장된 상기 사용자 정보를 재암호화하여 상기 다른 참여자에게 전송하는 단계를 포함한다.

대표도 - 도1



(52) CPC특허분류

H04L 2209/38 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 2016R1A2B4015899

부처명 과학기술정보통신부

연구관리전문기관 한국연구재단

연구사업명 기초연구사업(학술진흥)(2016)-중견연구자지원사업(총연구비1.5억초과~3억이하)

연구과제명 CPS 환경에서의 신뢰성있는 서비스 제공을 위한 보안기법 및 공격 대응 방안

기 여 율 1/1

주관기관 이화여자대학교 산학협력단

연구기간 2018.04.01 ~ 2019.02.28

명세서

청구범위

청구항 1

사용자 정보를 블록체인에 저장하고, 상기 블록체인에 참여하는 다른 참여자들과 상기 블록체인에 저장된 상기 사용자 정보가 공유될 수 있도록 제어하는 클라우드 서버에서의 데이터 공유 방법에 있어서,

상기 블록체인에 참여하는 다른 참여자들과 공유하는 암호화키 생성 소스를 이용하여 암호화키를 생성하는 단계;

상기 사용자 단말로부터 상기 사용자 정보를 수신하는 경우, 상기 사용자 정보를 상기 암호화키로 암호화하여 상기 블록체인에 저장하는 단계; 및

상기 블록체인에 참여하는 다른 참여자로부터 상기 사용자 정보 열람 요청을 수신하는 경우, 상기 블록체인에 저장된 상기 사용자 정보의 암호문인 상기 암호화키를 상기 다른 참여자가 생성하는 암호화키로 변환시키는 재암호화키를 생성하고, 상기 재암호화키로 상기 블록체인에 저장된 상기 사용자 정보를 재암호화하여 상기 다른 참여자에게 전송하는 단계를 포함하는 블록체인 기반의 데이터 공유 방법.

청구항 2

제1항에 있어서,

상기 블록체인에 참여하는 다른 참여자들과 공유하는 암호화키 생성 소스를 이용하여 암호화키를 생성하는 단계는,

엘가말(ElGamal) 암호화 알고리즘을 이용하여 공개키 및 비밀키 쌍의 상기 암호화키를 생성하는 단계를 포함하는 블록체인 기반의 데이터 공유 방법.

청구항 3

제1항에 있어서,

상기 사용자 단말로부터 상기 사용자 정보를 수신하는 경우, 상기 사용자 정보를 상기 암호화키로 암호화하여 상기 블록체인에 저장하는 단계는,

상기 사용자 단말의 인증 여부를 확인하는 단계; 및

상기 사용자 단말이 인증된 단말로 확인되는 경우, 상기 사용자 정보를 상기 암호화키로 암호화하여 상기 블록체인에 저장하는 단계를 포함하는 블록체인 기반의 데이터 공유 방법.

청구항 4

제1항에 있어서,

상기 블록체인에 참여하는 다른 참여자로부터 상기 사용자 정보 열람 요청을 수신하는 경우, 상기 블록체인에 저장된 상기 사용자 정보의 암호문인 상기 암호화키를 상기 다른 참여자가 생성하는 암호화키로 변환시키는 재암호화키를 생성하고, 상기 재암호화키로 상기 블록체인에 저장된 상기 사용자 정보를 재암호화하여 상기 다른 참여자에게 전송하는 단계는,

상기 사용자 단말로 상기 다른 참여자의 상기 사용자 정보 열람 요청 알림을 전송하는 단계; 및

상기 사용자 단말로부터 상기 다른 참여자의 상기 사용자 정보 열람 허가 알림을 수신하는 경우, 상기 재암호화키를 생성하는 단계를 포함하는 블록체인 기반의 데이터 공유 방법.

청구항 5

사용자 정보를 블록체인에 저장하고, 상기 블록체인에 참여하는 다른 참여자들과 상기 블록체인에 저장된 상기 사용자 정보가 공유될 수 있도록 제어하는 클라우드 서버에 있어서,

상기 블록체인에 참여하는 다른 참여자들과 공유하는 암호화키 생성 소스를 이용하여 암호화키를 생성하는 암호화키 생성부;

상기 사용자 단말로부터 상기 사용자 정보를 수신하는 경우, 상기 사용자 정보를 상기 암호화키로 암호화하여 상기 블록체인에 저장하는 암호화부; 및

상기 블록체인에 참여하는 다른 참여자로부터 상기 사용자 정보 열람 요청을 수신하는 경우, 상기 블록체인에 저장된 상기 사용자 정보의 암호문인 상기 암호화키를 상기 다른 참여자가 생성하는 암호화키로 변환시키는 재암호화키를 생성하고, 상기 재암호화키로 상기 블록체인에 저장된 상기 사용자 정보를 재암호화하여 상기 다른 참여자에게 전송하는 재암호화키 생성부를 포함하는 클라우드 서버.

청구항 6

제5항에 있어서,

상기 암호화키 생성부는,

엘가말(ElGamal) 암호화 알고리즘을 이용하여 공개키 및 비밀키 쌍의 상기 암호화키를 생성하는 클라우드 서버.

청구항 7

제5항에 있어서,

상기 암호화부는,

상기 사용자 단말의 인증 여부를 확인하여 상기 사용자 단말이 인증된 단말로 확인되는 경우, 상기 사용자 정보를 상기 암호화키로 암호화하여 상기 블록체인에 저장하는 클라우드 서버.

청구항 8

제5항에 있어서,

상기 재암호화키 생성부는,

상기 사용자 단말로 상기 다른 참여자의 상기 사용자 정보 열람 요청 알림을 전송하고, 상기 사용자 단말로부터 상기 다른 참여자의 상기 사용자 정보 열람 허가 알림을 수신하는 경우, 상기 재암호화키를 생성하는 클라우드 서버.

청구항 9

사용자 정보를 수집하는 사용자 단말;

상기 사용자 정보를 저장하는 블록체인;

상기 블록체인에 참여하며, 상기 블록체인에 저장된 상기 사용자 정보의 열람을 요청하는 적어도 하나의 참여자; 및

상기 사용자 단말로부터 상기 사용자 정보를 수신하는 경우, 상기 사용자 정보를 상기 블록체인에 저장하되, 상기 적어도 하나의 참여자와 공유하는 암호화키 생성 소스를 이용하여 암호화키를 생성하고, 상기 사용자 정보를 상기 암호화키로 암호화하여 상기 블록체인에 저장하며,

상기 적어도 하나의 참여자 중 어느 하나의 참여자로부터 상기 사용자 정보 열람 요청을 수신하는 경우, 상기 블록체인에 저장된 상기 사용자 정보의 암호문인 상기 암호화키를 상기 사용자 정보의 열람을 요청한 참여자가 생성하는 암호화키로 변환시키는 재암호화키를 생성하고, 상기 재암호화키로 상기 블록체인에 저장된 상기 사용자 정보를 재암호화하여 상기 사용자 정보의 열람을 요청한 참여자에게 전송하는 클라우드 서버를 포함하는 블록체인 기반의 데이터 공유 시스템.

청구항 10

제9항에 있어서,

상기 적어도 하나의 참여자는,

각각 상기 암호화키 생성 소스를 이용하여 암호화키를 생성하고,

상기 클라우드 서버로부터 상기 재암호화키에 의해 암호화 된 상기 사용자 정보를 수신하는 경우, 상기 암호화키 생성 소스를 이용하여 생성한 암호화키로 상기 재암호화키에 의해 암호화 된 상기 사용자 정보를 복호화하여 열람하는 블록체인 기반의 데이터 공유 시스템.

발명의 설명

기술 분야

[0001] 본 발명은 블록체인 기반의 데이터 공유 방법, 이를 수행하기 위한 클라우드 서버 및 이를 포함하는 데이터 공유 시스템에 관한 것으로서, 더욱 상세하게는 블록체인에 저장되는 사용자 정보를 블록체인 참여자 간에 안전하게 공유하기 위한 블록체인 기반의 데이터 공유 방법, 이를 수행하기 위한 클라우드 서버 및 이를 포함하는 데이터 공유 시스템에 관한 것이다.

배경 기술

[0002] 최근 스마트 기기를 통해 다양한 건강관리 서비스가 보편화되면서 누구나 시간 및 장소에 구애 받지 않고 자신의 건강상태를 측정하여 기록 및 점검할 수 있다. 나아가 스마트 기기를 통해 수집한 데이터는 전문가에게 정밀한 진단 및 조언을 받을 수 있는 데이터로 활용될 수 있다.

[0003] 이러한 의료 전문가가 아닌 일반 사용자들이 스스로 만들어내는 의료 데이터를 환자 유래의 의료 데이터(PGHD: Patients Generated Health Data)라 하는데, 예를 들면, 건강에 대한 이력, 치료 이력, 생체 데이터, 각종 증상 및 생활 습관 등이 포함될 수 있다.

[0004] 한편, 환자 유래의 의료 데이터는 환자를 진료한 개별 의료기관 중심으로 관리가 되고 있다. 또한, 진료한 의료기관 이외의 다른 의료기관과의 정보교환은 환자 본인이 요청한 경우를 제외하고는 허용되지 않기 때문에, 의료데이터 파편화를 초래함으로써 데이터의 활용이 어렵다.

[0005] 즉, 환자 유래의 의료 데이터의 관리는 전형적인 분절적 중앙 집중형 관리체제로 이루어져 있어 보안과 접근성 및 가용성에 취약한 단일실패점(SPoF: Single Point of Failure)으로 작동하게 될 우려가 증가하고 있다.

[0006] 이에 따라, 블록체인 기반의 의료 데이터 관리 플랫폼이 각광받고 있다. 블록체인은 분산 데이터베이스와 유사한 형태로 데이터를 저장하는 구조체 리스트이며, 네트워크 참여자들이 데이터를 저장 및 검증하므로 임의조작이 어렵도록 설계되어있다. 블록체인은 탈중앙성, 보안성, 신속성, 확장성, 투명성 등을 보장해 줄 수 있는 장점을 가지고 있다.

[0007] 그러나, 블록체인에 악의적인 참여자가 존재하는 경우, 데이터 노출의 가능성이 존재하며, 특히 의료 데이터가 노출되는 경우, 환자에게 치명적인 피해를 입힐 수 있다.

발명의 내용

해결하려는 과제

[0008] 본 발명의 일측면은 블록체인에 저장된 사용자 정보의 열람을 요청하는 경우, 암호화 된 사용자 정보의 암호화키를 변환시켜 제공하는 블록체인 기반의 데이터 공유 방법, 이를 수행하기 위한 클라우드 서버 및 이를 포함하는 블록체인 기반의 데이터 공유 시스템을 제공한다.

과제의 해결 수단

[0009] 상기 과제를 해결하기 위한 본 발명의 블록체인 기반의 데이터 공유 방법은, 사용자 정보를 블록체인에 저장하고, 상기 블록체인에 참여하는 다른 참여자들과 상기 블록체인에 저장된 상기 사용자 정보가 공유될 수 있도록 제어하는 클라우드 서버에서의 데이터 공유 방법에 관한 것으로, 상기 블록체인에 참여하는 다른 참여자들과 공유하는 암호화키 생성 소스를 이용하여 암호화키를 생성하는 단계, 상기 사용자 단말로부터 상기 사용자 정보를 수신하는 경우, 상기 사용자 정보를 상기 암호화키로 암호화하여 상기 블록체인에 저장하는 단계 및 상기 블록체인에 참여하는 다른 참여자로부터 상기 사용자 정보 열람 요청을 수신하는 경우, 상기 블록체인에 저장된 상기 사용자 정보의 암호문인 상기 암호화키를 상기 다른 참여자가 생성하는 암호화키로 변환시키는 재암호화키를 생성하고, 상기 재암호화키로 상기 블록체인에 저장된 상기 사용자 정보를 재암호화하여 상기 다른 참여자에게

전송하는 단계를 포함한다.

- [0010] 또한, 상기 블록체인에 참여하는 다른 참여자들과 공유하는 암호화키 생성 소스를 이용하여 암호화키를 생성하는 단계는, 엘가말(ElGamal) 암호화 알고리즘을 이용하여 공개키 및 비밀키 쌍의 상기 암호화키를 생성하는 단계를 포함할 수 있다.
- [0011] 또한, 상기 사용자 단말로부터 상기 사용자 정보를 수신하는 경우, 상기 사용자 정보를 상기 암호화키로 암호화하여 상기 블록체인에 저장하는 단계는, 상기 사용자 단말의 인증 여부를 확인하는 단계 및 상기 사용자 단말이 인증된 단말로 확인되는 경우, 상기 사용자 정보를 상기 암호화키로 암호화하여 상기 블록체인에 저장하는 단계를 포함할 수 있다.
- [0012] 또한, 상기 블록체인에 참여하는 다른 참여자로부터 상기 사용자 정보 열람 요청을 수신하는 경우, 상기 블록체인에 저장된 상기 사용자 정보의 암호문인 상기 암호화키를 상기 다른 참여자가 생성하는 암호화키로 변환시키는 재암호화키를 생성하고, 상기 재암호화키로 상기 블록체인에 저장된 상기 사용자 정보를 재암호화하여 상기 다른 참여자에게 전송하는 단계는, 상기 사용자 단말로 상기 다른 참여자의 상기 사용자 정보 열람 요청 알림을 전송하는 단계 및 상기 사용자 단말로부터 상기 다른 참여자의 상기 사용자 정보 열람 허가 알림을 수신하는 경우, 상기 재암호화키를 생성하는 단계를 포함할 수 있다.
- [0013] 한편, 본 발명의 클라우드 서버는 사용자 정보를 블록체인에 저장하고, 상기 블록체인에 참여하는 다른 참여자들과 상기 블록체인에 저장된 상기 사용자 정보가 공유될 수 있도록 제어하는 클라우드 서버에 관한 것으로, 상기 블록체인에 참여하는 다른 참여자들과 공유하는 암호화키 생성 소스를 이용하여 암호화키를 생성하는 암호화키 생성부, 상기 사용자 단말로부터 상기 사용자 정보를 수신하는 경우, 상기 사용자 정보를 상기 암호화키로 암호화하여 상기 블록체인에 저장하는 암호화부 및 상기 블록체인에 참여하는 다른 참여자로부터 상기 사용자 정보 열람 요청을 수신하는 경우, 상기 블록체인에 저장된 상기 사용자 정보의 암호문인 상기 암호화키를 상기 다른 참여자가 생성하는 암호화키로 변환시키는 재암호화키를 생성하고, 상기 재암호화키로 상기 블록체인에 저장된 상기 사용자 정보를 재암호화하여 상기 다른 참여자에게 전송하는 재암호화키 생성부를 포함한다.
- [0014] 또한, 상기 암호화키 생성부는, 엘가말(ElGamal) 암호화 알고리즘을 이용하여 공개키 및 비밀키 쌍의 상기 암호화키를 생성할 수 있다.
- [0015] 또한, 상기 암호화부는, 상기 사용자 단말의 인증 여부를 확인하여 상기 사용자 단말이 인증된 단말로 확인되는 경우, 상기 사용자 정보를 상기 암호화키로 암호화하여 상기 블록체인에 저장할 수 있다.
- [0016] 또한, 상기 재암호화키 생성부는, 상기 사용자 단말로 상기 다른 참여자의 상기 사용자 정보 열람 요청 알림을 전송하고, 상기 사용자 단말로부터 상기 다른 참여자의 상기 사용자 정보 열람 허가 알림을 수신하는 경우, 상기 재암호화키를 생성할 수 있다.
- [0017] 한편, 본 발명의 블록체인 기반의 데이터 공유 시스템은 사용자 정보를 수집하는 사용자 단말, 상기 사용자 정보를 저장하는 블록체인, 상기 블록체인에 참여하며, 상기 블록체인에 저장된 상기 사용자 정보의 열람을 요청하는 적어도 하나의 참여자 및 상기 사용자 단말로부터 상기 사용자 정보를 수신하는 경우, 상기 사용자 정보를 상기 블록체인에 저장하되, 상기 적어도 하나의 참여자와 공유하는 암호화키 생성 소스를 이용하여 암호화키를 생성하고, 상기 사용자 정보를 상기 암호화키로 암호화하여 상기 블록체인에 저장하며, 상기 적어도 하나의 참여자 중 어느 하나의 참여자로부터 상기 사용자 정보 열람 요청을 수신하는 경우, 상기 블록체인에 저장된 상기 사용자 정보의 암호문인 상기 암호화키를 상기 사용자 정보의 열람을 요청한 참여자가 생성하는 암호화키로 변환시키는 재암호화키를 생성하고, 상기 재암호화키로 상기 블록체인에 저장된 상기 사용자 정보를 재암호화하여 상기 사용자 정보의 열람을 요청한 참여자에게 전송하는 클라우드 서버를 포함한다.
- [0018] 또한, 상기 적어도 하나의 참여자는, 각각 상기 암호화키 생성 소스를 이용하여 암호화키를 생성하고, 상기 블록체인으로부터 상기 재암호화키에 의해 암호화 된 상기 사용자 정보를 수신하는 경우, 상기 암호화키 생성 소스를 이용하여 생성한 암호화키로 상기 재암호화키에 의해 암호화 된 상기 사용자 정보를 복호화하여 열람할 수 있다.

발명의 효과

- [0019] 본 발명에 따르면, 사용자 정보를 암호화하여 블록체인에 저장함으로써 데이터의 기밀성을 보장할 수 있으며, 변조가 불가능하기 때문에 무결성 또한 보장할 수 있다. 아울러, 사용자 정보 관리의 탈중앙화를 도모하여 보안과 접근성 및 가용성에 취약한 단일실패점점을 방지할 수 있다.

[0020] 또한, 암호화된 사용자 정보를 해당 사용자 정보의 열람 요청자에게 전달하는 경우, 사용자 정보를 복호화한 뒤 요청자의 공개키로 다시 암호화하는 방식 대신 재암호화키를 이용하여 암호화된 사용자 정보의 공개키를 변환시켜 요청자에게 전달하는 방식을 채택함으로써, 사용자 정보의 복호화 단계를 생략할 수 있다. 이에, 악의적인 사용자에 의한 정보 노출을 방지할 수 있다.

[0021] 또한, 사용자가 생성하는 사용자 정보의 공유가 사용자의 관리 하에 이루어지도록 함으로써, 데이터의 통합에 유리하다.

도면의 간단한 설명

[0022] 도 1은 본 발명의 일 실시예에 따른 블록체인 기반의 데이터 공유 시스템의 개념도이다.

도 2는 도 1에 도시된 데이터 공유 시스템에서의 암호문 생성 및 데이터 공유의 흐름도이다.

도 3은 도 1에 도시된 클라우드 서버의 블록도이다.

도 4는 본 발명의 일 실시예에 따른 블록체인 기반의 데이터 공유 방법의 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0023] 후술하는 본 발명에 대한 상세한 설명은, 본 발명이 실시될 수 있는 특정 실시예를 예시로서 도시하는 첨부 도면을 참조한다. 이들 실시예는 당업자가 본 발명을 실시할 수 있기에 충분하도록 상세히 설명된다. 본 발명의 다양한 실시예는 서로 다르지만 상호 배타적일 필요는 없음이 이해되어야 한다. 예를 들어, 여기에 기재되어 있는 특정 형상, 구조 및 특성은 일 실시예와 관련하여 본 발명의 정신 및 범위를 벗어나지 않으면서 다른 실시예로 구현될 수 있다. 또한, 각각의 개시된 실시예 내의 개별 구성요소의 위치 또는 배치는 본 발명의 정신 및 범위를 벗어나지 않으면서 변경될 수 있음이 이해되어야 한다. 따라서, 후술하는 상세한 설명은 한정적인 의미로서 취하려는 것이 아니며, 본 발명의 범위는, 적절하게 설명된다면, 그 청구항들이 주장하는 것과 균등한 모든 범위와 더불어 첨부된 청구항에 의해서만 한정된다. 도면에서 유사한 참조부호는 여러 측면에 걸쳐서 동일하거나 유사한 기능을 지칭한다.

[0024] 이하, 도면들을 참조하여 본 발명의 바람직한 실시예들을 보다 상세하게 설명하기로 한다.

[0025] 도 1은 본 발명의 일 실시예에 따른 블록체인 기반의 데이터 공유 시스템의 개념도이다.

[0026] 본 발명의 일 실시예에 따른 블록체인 기반의 데이터 공유 시스템(1000)은 사용자가 직접 생성하거나 수집하는 사용자 정보가 블록체인(500)에 참여하는 참여자 간에 공유되도록 제어할 수 있다.

[0027] 본 발명의 일 실시예에 따른 블록체인 기반의 데이터 공유 시스템(1000)은 사용자 정보의 공유를 제어하는 주체를 사용자 정보를 생성하는 사용자에게 두어, 사용자 정보를 다른 외부자들과 공유하는 다양한 환경에 적용되기에 적합하다.

[0028] 예를 들면, 본 발명의 일 실시예에 따른 블록체인 기반의 데이터 공유 시스템(1000)은 의료 정보 공유 시스템에 적용될 수 있다. 의료 정보 공유 시스템은 환자가 치료이력, 생체 데이터, 증상 등의 의료 정보를 직접 수집하고, 환자를 진료하는 의료기관뿐만 아니라 다른 의료기관에서도 의료 정보가 공유될 수 있도록 하여 환자의 의료 정보를 통합 관리하는 시스템이다. 종래의 의료 정보 공유 시스템에 따르면 의료 정보는 환자를 진료하는 의료기관을 중심으로 관리되므로, 데이터의 불편화를 초래할 수 있으며, 보안성이 취약하다. 본 발명의 일 실시예에 따른 블록체인 기반의 데이터 공유 시스템(1000)은 의료 정보를 수집하는 환자가 데이터 관리의 중심이 되게 함으로써 데이터 통합이 유리하며, 의료 정보 유출에 따른 피해를 예방할 수 있다.

[0029] 도 1을 참조하면, 본 발명의 일 실시예에 따른 블록체인 기반의 데이터 공유 시스템(1000)은 클라우드 서버(300) 및 적어도 하나의 참여자(700)에 의해 구축되는 블록체인(500), 사용자 정보를 생성하는 센서 장치(10) 및 사용자 정보를 클라우드 서버(300)로 전송하여 블록체인(500)에 저장되게 하는 사용자 단말(100)을 포함할 수 있다.

[0030] 센서 장치(10)는 사용자 정보를 생성 또는 수집할 수 있다. 사용자는 센서 장치(10)를 이용하여 다른 사용자와 공유하고자 하는 데이터를 생성할 수 있다.

[0031] 예를 들면, 센서 장치(10)는 사용자의 신체에 장착되어 생체 데이터, 각종 증상 또는 생활습관 등을 포함하는 사용자 정보를 생성하는 웨어러블 디바이스일 수 있다.

- [0032] 사용자 단말(100)은 센서 장치(10)에서 생성하는 사용자 정보를 수집하여 클라우드 서버(300)로 전송할 수 있다. 즉, 사용자는 사용자 단말(100)을 매개로 하여 센서 장치(10)에서 생성하는 사용자 정보를 클라우드 서버(300)로 전송할 수 있다.
- [0033] 이를 위해, 사용자 단말(100)은 통신이 가능하고 정보의 입출력이 가능한 장치로, 예를 들면, PC, 스마트폰, 태블릿 등으로 구현될 수 있다.
- [0034] 블록체인(500)은 분산 데이터베이스와 유사한 형태로 데이터를 저장하는 구조체 리스트로, 본 실시예에서는 클라우드 서버(300) 및 적어도 하나의 참여자(700)에 의해 구축될 수 있다. 클라우드 서버(300) 및 적어도 하나의 참여자(700)는 블록체인(500)에 정보의 저장 또는 열람이 가능하다.
- [0035] 클라우드 서버(300)는 클라이언트의 접속요청에 응답하여 소정의 정보를 제공하는 일반적인 형태의 서버로, 본 실시예에서 블록체인(500)에 참여하는 네트워크 중 하나일 수 있다.
- [0036] 클라우드 서버(300)는 사용자 단말(100)로부터 수신하는 사용자 정보를 암호화하여 블록체인(500)에 저장할 수 있다. 클라우드 서버(300)는 블록체인(500)에 참여하는 다른 참여자(700)가 사용자 정보의 열람을 요청하는 경우, 이를 사용자 단말(100)을 통해 사용자에게 알리고, 사용자의 통제 하에서 다른 참여자(700)의 사용자 정보 열람을 가능하게 한다.
- [0037] 여기에서, 클라우드 서버(300)는 프록시 재암호화(Proxy Re-Encryption) 기법을 적용할 수 있다. 프록시 재암호화 기법은 프록시 개체(Entity)가 기본 메시지에 대해 아무것도 알지 않고도 하나의 공개키에서 다른 공개키로 암호문을 변환할 수 있게 해주는 일종의 공개키 암호화 기법이다. 이와 관련하여 도 2를 참조하여 구체적으로 설명한다.
- [0038] 도 2는 도 1에 도시된 데이터 공유 시스템에서의 암호문 생성 및 데이터 공유의 흐름도이다.
- [0039] 본 발명의 일 실시예에 따른 블록체인 기반의 데이터 공유 시스템(1000)이 의료 정보 공유 시스템에 적용된 것을 예로 들어 설명하면, 사용자 단말(100)은 환자 또는 보호자와 같이 의료 전문가가 아닌 일반 사용자가 소지하고 있는 단말일 수 있으며, 적어도 하나의 참여자(700)는 병원, 약국, 연구센터, 보험사 등과 같이 의료 전문가들로 구성되는 네트워크 서버일 수 있다.
- [0040] 도 2를 참조하면, 클라우드 서버(300) 및 적어도 하나의 참여자(700)는 블록체인(500)을 구축하는데, 각각 암호화키를 생성하여 저장할 수 있다. 암호화키는 사용자 정보의 암호문인 공개키(pk_A , pk_B) 및 암호화된 사용자 정보를 복호화 하는 데 사용되는 비밀키(sk_A , sk_B)의 쌍으로 구성될 수 있다.
- [0041] 사용자 단말(100)은 사용자 정보(data)를 수집하여 클라우드 서버(300)로 전송할 수 있다.
- [0042] 클라우드 서버(300)는 사용자 단말(100)이 인증된 단말인지를 확인하고, 사용자 단말(100)이 인증된 단말로 확인되는 경우, 사용자 단말(100)로부터 수신하는 사용자 정보(data)를 공개키(pk_A)로 암호화하여 블록체인(500)에 저장할 수 있다.
- [0043] 클라우드 서버(300)는 공개키(pk_A)에 의해 암호화 된 사용자 정보(C_A)를 저장할 수 있다.
- [0044] 클라우드 서버(300)는 참여자(700)로부터 사용자 정보(data) 열람 요청을 수신하는 경우, 사용자 단말(100)로 해당 참여자(700)의 사용자 정보 열람 요청 알림을 전송할 수 있다.
- [0045] 사용자 단말(100)은 참여자(700)의 사용자 정보(data) 열람 요청 알림을 출력하여 사용자로부터 참여자(700)의 사용자 정보(data) 열람 허가 또는 차단을 선택 받고, 그 결과를 클라우드 서버(300)로 전송할 수 있다.
- [0046] 클라우드 서버(300)는 사용자 단말(100)로부터 참여자(700)의 사용자 정보(data) 열람 허가 신호를 수신하는 경우, 재암호화키($rk_{A \rightarrow B}$)를 생성할 수 있다. 재암호화키($rk_{A \rightarrow B}$)는 블록체인(500)에 저장된 사용자 정보(C_A)의 암호문인 클라우드 서버(300)가 생성한 공개키(pk_A)를 참여자(700)가 생성한 공개키(pk_B)로 변환시키는 암호문이다.
- [0047] 클라우드 서버(300)는 재암호화키($rk_{A \rightarrow B}$)를 이용하여 사용자 정보(C_A)를 재암호화하고, 이를 참여자(700)에게 전송할 수 있다.
- [0048] 참여자(700)는 클라우드 서버(300)로부터 재암호화키($rk_{A \rightarrow B}$)에 의해 재암호화 된 사용자 정보(C_B)를 수신하는 경

우, 비밀키(sk_B)로 복호화하여 사용자 정보(data)를 열람할 수 있다.

- [0049] 이와 같이, 본 발명의 일 실시예에 따른 블록체인 기반의 데이터 공유 시스템(1000)은 사용자 정보를 암호화하여 블록체인(500)에 저장함으로써 데이터의 기밀성을 보장할 수 있으며, 변조가 불가능하기 때문에 무결성 또한 보장할 수 있다.
- [0050] 또한, 본 발명의 일 실시예에 따른 블록체인 기반의 데이터 공유 시스템(1000)은 암호화된 사용자 정보를 해당 사용자 정보의 열람 요청자에게 전달하는 경우, 사용자 정보를 복호화한 뒤 요청자의 공개키로 다시 암호화하는 방식 대신 재암호화키를 이용하여 암호화된 사용자 정보의 공개키를 변환시켜 요청자에게 전달하는 방식을 채택함으로써, 사용자 정보의 복호화 단계를 생략할 수 있다. 이에, 악의적인 사용자에 의한 정보 노출을 방지할 수 있다.
- [0051] 또한, 본 발명의 일 실시예에 따른 블록체인 기반의 데이터 공유 시스템(1000)은 사용자가 생성하는 사용자 정보의 공유가 사용자의 관리 하에 이루어지도록 함으로써, 데이터의 통합에 유리하다.
- [0053] 도 3은 도 1에 도시된 클라우드 서버의 블록도이다.
- [0054] 도 3을 참조하면, 클라우드 서버(300)는 암호화키 생성부(310), 암호화부(330) 및 재암호화키 생성부(350)를 포함할 수 있다.
- [0055] 클라우드 서버(300)는 상술한 바와 같이 사용자 단말(100)로부터 사용자 정보를 수집하고, 사용자 정보를 암호화하여 블록체인(500)에 저장할 수 있다.
- [0056] 또한, 클라우드 서버(300)는 블록체인(500)의 다른 참여자(700)로부터 사용자 정보의 열람 요청 신호를 수신하는 경우, 암호화 된 사용자 정보의 암호문을 변환시키는 재암호화키를 생성하고, 재암호화키로 암호화 된 사용자 정보를 재암호화하여 사용자 정보를 요청한 참여자(700)에게 전송할 수 있으며, 참여자(700)는 재암호화 된 사용자 정보를 복호화하여 열람할 수 있다.
- [0057] 이하, 도 3에 도시된 클라우드 서버(300)의 각 구성에 대하여 구체적으로 설명한다.
- [0058] 암호화키 생성부(310)는 사용자 정보를 암호화 또는 복호화 하는 데 사용되는 암호화키를 생성하여 저장할 수 있다.
- [0059] 암호화키는 사용자 단말(100)로부터 수신하는 사용자 정보를 암호화하는 암호문인 공개키 및 공개키에 의해 암호화 된 사용자 정보를 복호화하는 복호문인 비밀키의 쌍으로 이루어질 수 있다.
- [0060] 암호화키 생성부(310)는 블록체인(500)에 참여하는 적어도 하나의 참여자(700)와 공유하는 암호화키 생성 소스를 이용하여 암호화키를 생성할 수 있다.
- [0061] 예를 들면, 암호화키 생성부(310)는 블록체인(500)에 참여하는 적어도 하나의 참여자(700)와 공유하는 암호화키 생성 소스를 엘가말(ElGamal) 암호화 알고리즘에 적용하여 아래 수식식 1과 같이 공개키(pk) 및 비밀키(sk) 쌍의 암호화키를 생성할 수 있다. 이때, 블록체인(500)에 참여하는 적어도 하나의 참여자(700)와 공유하는 암호화키 생성 소스는 그룹 G 의 큰 소수 q 및 생성자 g 를 포함할 수 있다.

수학식 1

- [0062] $\text{KeyGen}(pk_x, sk_x) : pk = g^a \in G, sk = a \in \mathbb{Z}_q$

- [0063] 한편, 도 1에 도시된 적어도 하나의 참여자(700)는 각각 위와 같은 방식으로 블록체인(500)에 참여하는 적어도 하나의 참여자(700)와 공유하는 암호화키 생성 소스를 이용하여 공개키 및 비밀키 쌍의 암호화키를 생성하여 저장할 수 있다.
- [0064] 암호화부(330)는 사용자 단말(100)로부터 수신하는 사용자 정보를 암호화할 수 있다.
- [0065] 암호화부(330)는 사용자 단말(100)로부터 사용자 정보를 수신하는 경우, 사용자 단말(100)의 인증 여부를 확인할 수 있다.

[0066] 예를 들면, 암호화부(330)는 사용자 단말(100)로부터 사용자 정보를 수신하는 경우, 해당 사용자 단말(100)의 식별 정보와 미리 저장된 인증된 사용자 단말 목록을 비교하여 해당 사용자 단말(100)의 인증 여부를 확인할 수 있다.

[0067] 암호화부(330)는 사용자 단말(100)이 인증된 단말로 확인되는 경우, 사용자 정보를 암호화키로 암호화하여 블록체인(500)에 저장할 수 있다.

수학식 2

[0068] $C_A = Enc(pk_A, data)$

[0069] 즉, 블록체인(500)에는 클라우드 서버(300)에서 생성하는 공개키(pk_A)에 의해 암호화 된 상태의 사용자 정보(C_A)가 저장될 수 있다.

[0070] 이처럼, 암호화부(330)는 인증된 사용자 단말(100)로부터 수신하는 사용자 정보에 한하여 블록체인(500)에 저장하며, 아울러, 사용자 정보를 암호화하여 저장함으로써, 데이터의 기밀성을 보장할 수 있다.

[0071] 재암호화키 생성부(350)는 블록체인(500)에 저장된 사용자 정보(C_A)의 암호문인 암호화키(pk_A)를 다른 암호화키로 변환시키는 재암호화키를 생성할 수 있다.

[0072] 재암호화키 생성부(350)는 블록체인(500)에 참여하는 다른 참여자(700)로부터 블록체인(500)에 저장된 사용자 정보의 열람 요청을 수신할 수 있다.

[0073] 재암호화키 생성부(350)는 블록체인(500)에 참여하는 다른 참여자(700)로부터 사용자 정보의 열람 요청을 수신하는 경우, 사용자 단말(100)로 다른 참여자(700)의 사용자 정보 열람 요청 알림을 전송할 수 있다.

[0074] 이와 같은 경우, 사용자 단말(100)은 사용자 정보 열람 요청 알림을 출력하여 참여자(700)의 열람 요청 허가 또는 불허를 사용자로부터 선택 받을 수 있으며, 그 결과를 클라우드 서버(300)로 전송할 수 있다.

[0075] 재암호화키 생성부(350)는 사용자 단말(100)로부터 다른 참여자(700)의 사용자 정보 열람 허가 신호를 수신하는 경우, 재암호화키를 생성할 수 있다.

[0076] 재암호화키는 블록체인(500)에 저장된 사용자 정보(C_A)의 암호문인 암호화키(pk_A)를 해당 사용자 정보(C_A)를 요청한 참여자(700)가 생성하는 암호화키(pk_B)로 변환시킬 수 있는 암호문으로, 아래 수학식 3과 같이 나타낼 수 있다.

수학식 3

[0077] $ReKeyGen(rk_{A \rightarrow B})$

[0078] 재암호화키 생성부(350)는 공지된 Atomic proxy cryptography(BBS98) 기법을 이용하여 재암호화키를 생성할 수 있다. Atomic proxy cryptography(BBS98) 기법은 프록시 재암호화 기법에서 널리 사용되는 프록시 키 생성 기법으로, 구체적인 설명은 "Blaze, M., Bleumer, G., Strauss, M., Divertible protocols and atomic proxy cryptography. Advances in Cryptology. EUROCRYPT'98, pp.127.144, 1998."에 개시되어 있다.

[0079] 재암호화키 생성부(350)는 사용자 정보(C_A)를 재암호화키($rk_{A \rightarrow B}$)로 암호화하여 아래 수학식 4와 같은 사용자 정보(C_B)를 생성할 수 있다. 이처럼 재암호화키($rk_{A \rightarrow B}$)에 의해 암호화 된 사용자 정보(C_B)는 사용자 정보를 요청한 참여자(700)가 생성하는 공개키(pk_B)에 의해 암호화되는 사용자 정보에 해당한다.

수학식 4

[0080] $C_B = ReEnc(rk_{A \rightarrow B}, C_A)$

[0081] 재암호화키 생성부(350)는 재암호화키($rk_{A \rightarrow B}$)에 의해 암호화 된 사용자 정보(C_B)를 사용자 정보를 요청한 참여자(700)에게 전송할 수 있다.

[0082] 참여자(700)는 재암호화키 생성부(350)로부터 수학식 4와 같이 재암호화키($rk_{A \rightarrow B}$)로 재암호화 된 사용자 정보(C_B)를 수신하는 경우, 아래 수학식 5와 같이 자신이 생성한 비밀키(sk_B)로 복호화하여 사용자 정보(data)를 열람할 수 있다.

수학식 5

[0083] $data = Dec(sk_B, C_B)$

[0084] 이처럼, 재암호화키 생성부(350)는 사용자 정보의 암호문을 사용자 정보를 요청한 참여자(700)가 생성한 암호문으로 변환하여 참여자(700)에게 제공될 수 있도록 하는 재암호화키를 생성함으로써, 암호화되어 저장된 사용자 정보의 공유를 위해, 저장된 사용자 정보의 복호화 단계를 생략할 수 있다. 따라서, 악의적인 사용자에게 의한 정보 노출을 방지할 수 있으며, 특히, BBS98 기법을 적용하는 경우 계산 오버헤드를 줄이고, 이산대수 계산에 따른 안전성을 보장할 수 있다.

[0085] 아울러, 재암호화키 생성부(350)는 사용자에게 의해 다른 참여자(700)의 사용자 정보 열람이 허용된 경우에만 재암호화키를 생성함으로써, 사용자 중심의 데이터 공유 서비스를 가능하게 한다.

[0087] 이하에서는, 도 4를 참조하여, 도 3에 도시된 클라우드 서버에서의 데이터 공유 방법에 대하여 설명한다.

[0088] 도 4는 본 발명의 일 실시예에 따른 블록체인 기반의 데이터 공유 방법의 순서도이다.

[0089] 본 발명의 일 실시예에 따른 블록체인 기반의 데이터 공유 방법은 도 1에 도시된 클라우드 서버(300)와 실질적으로 동일한 구성에서 진행될 수 있다. 따라서, 도 1의 데이터 공유 시스템(1000)과 동일한 구성요소는 동일한 도면부호를 부여하고, 반복되는 설명은 생략한다.

[0090] 도 4를 참조하면, 클라우드 서버(300)는 암호화키(pk_A , sk_A)를 생성할 수 있다(S10).

[0091] 암호화키는 사용자 단말(100)로부터 수신하는 사용자 정보를 암호화하는 암호문인 공개키(pk_A) 및 공개키에 의해 암호화 된 사용자 정보를 복호화하는 복호문인 비밀키(sk_A)의 쌍으로 이루어질 수 있다.

[0092] 클라우드 서버(300)는 블록체인(500)의 참여자 중 하나로, 는 블록체인(500)에 참여하는 다른 참여자(700)들과 공유하는 암호화키 생성 소스를 이용하여 암호화키를 생성할 수 있다.

[0093] 예를 들면, 클라우드 서버(300)는 블록체인(500)에 참여하는 적어도 하나의 참여자(700)와 공유하는 암호화키 생성 소스를 엘가말(ElGamal) 암호화 알고리즘에 적용하여 상기 수학식 1과 같이 암호화키를 생성할 수 있다. 이때, 블록체인(500)에 참여하는 적어도 하나의 참여자(700)와 공유하는 암호화키 생성 소스는 그룹 G의 큰 소수 q 및 생성자 g를 포함할 수 있다.

[0094] 한편, 도 1에 도시된 적어도 하나의 참여자(700)는 각각 클라우드 서버(300)와 동일한 방식으로 공개키 및 비밀키 쌍의 암호화키를 생성하여 저장할 수 있다.

[0095] 클라우드 서버(300)는 사용자 단말(100)로부터 사용자 정보를 수신하는 경우(S20), 사용자 단말(100)이 인증된 사용자 단말인지를 확인할 수 있다(S30).

[0096] 사용자 단말(100)은 센서 장치(10)에서 생성하는 사용자 정보를 수집하여 클라우드 서버(300)로 전송할 수 있다. 즉, 사용자는 사용자 단말(100)을 매개로 하여 센서 장치(10)에서 생성하는 사용자 정보를 클라우드 서버

(300)로 전송할 수 있다.

- [0097] 클라우드 서버(300)는 사용자 단말(100)로부터 사용자 정보를 수신하는 경우, 해당 사용자 단말(100)의 식별 정보와 미리 저장된 인증된 사용자 단말 목록을 비교하여 해당 사용자 단말(100)의 인증 여부를 확인할 수 있다.
- [0098] 클라우드 서버(300)는 사용자 단말(100)이 인증된 단말인 것으로 확인되는 경우(S30), 암호화키(pk_A , sk_A)로 사용자 정보를 암호화하여 블록체인(500)에 저장할 수 있다(S40).
- [0099] 클라우드 서버(300)는 상기 수학적식 2와 같이 공개키(pk_A)를 암호문으로 하여 암호화 한 사용자 정보(C_A)를 블록체인(500)에 저장할 수 있다.
- [0100] 클라우드 서버(300)는 블록체인(500)에 참여하는 다른 참여자(700)로부터 사용자 정보 열람을 요청 받는 경우(S50), 사용자 단말(100)로 사용자 정보의 열람 요청 알림을 전달하여(S60), 이에 대한 응답으로 사용자 단말(100)로부터 사용자 정보 열람 허가 알림을 수신할 수 있다(S70).
- [0101] 여기에서, 사용자 단말(100)은 사용자 정보 열람 요청 알림을 출력하여 참여자(700)의 열람 요청 허가 또는 불허를 사용자로부터 선택 받을 수 있으며, 그 결과를 클라우드 서버(300)로 전송할 수 있다.
- [0102] 클라우드 서버(300)는 사용자 단말(100)로부터 다른 참여자(700)의 사용자 정보 열람 허가 신호를 수신하는 경우(S70), 재암호화키($rk_{A \rightarrow B}$)를 생성할 수 있다(S80).
- [0103] 재암호화키는 블록체인(500)에 저장된 사용자 정보(C_A)의 암호문인 암호화키(pk_A)를 해당 사용자 정보(C_A)를 요청한 참여자(700)가 생성하는 암호화키(pk_B)로 변환시킬 수 있는 암호문으로, 상기 수학적식 3과 같이 나타낼 수 있다.
- [0104] 클라우드 서버(300)는 공지된 Atomic proxy cryptography(BBS98) 기법을 이용하여 재암호화키를 생성할 수 있다.
- [0105] 클라우드 서버(300)는 사용자 정보(C_A)를 재암호화키($rk_{A \rightarrow B}$)로 암호화하여 사용자 정보 열람을 요청한 다른 참여자(700)에게 전송할 수 있다(S90).
- [0106] 클라우드 서버(300)는 사용자 정보(C_A)를 재암호화키($rk_{A \rightarrow B}$)로 암호화하여 상기 수학적식 4와 같은 사용자 정보(C_B)를 생성할 수 있다. 이처럼 재암호화키($rk_{A \rightarrow B}$)에 의해 암호화 된 사용자 정보(C_B)는 사용자 정보를 요청한 참여자(700)가 생성하는 공개키(pk_B)에 의해 암호화되는 사용자 정보에 해당한다.
- [0107] 사용자 정보를 요청한 참여자(700)는 클라우드 서버(300)로부터 수학적식 4와 같이 재암호화키($rk_{A \rightarrow B}$)로 재암호화 된 사용자 정보(C_B)를 수신하는 경우, 상기 수학적식 5와 같이 자신이 생성한 비밀키(sk_B)로 복호화하여 사용자 정보(data)를 열람할 수 있다.
- [0108] 이에 따라, 본 발명의 일 실시예에 따른 클라우드 서버에서의 블록체인 기반의 데이터 공유 방법은 사용자 정보를 암호화하여 블록체인(500)에 저장함으로써 데이터의 기밀성을 보장할 수 있으며, 변조가 불가능하기 때문에 무결성 또한 보장할 수 있다.
- [0109] 또한, 암호화된 사용자 정보를 해당 사용자 정보의 열람 요청자에게 전달하는 경우, 사용자 정보를 복호화한 뒤 요청자의 공개키로 다시 암호화하는 방식 대신 재암호화키를 이용하여 암호화된 사용자 정보의 공개키를 변환시켜 요청자에게 전달하는 방식을 채택함으로써, 사용자 정보의 복호화 단계를 생략할 수 있다. 이에, 악의적인 사용자에게 의한 정보 노출을 방지할 수 있다. , 특히, BBS98 기법을 적용하는 경우 계산 오버헤드를 줄이고, 이산대수 계산에 따른 안전성을 보장할 수 있다.
- [0110] 또한, 재암호화키 생성부(350)는 사용자에게 의해 다른 참여자(700)의 사용자 정보 열람이 허용된 경우에만 재암호화키를 생성함으로써, 사용자 중심의 데이터 공유 서비스를 가능하게 한다.
- [0112] 이와 같은, 블록체인 기반의 데이터 공유 방법은 애플리케이션으로 구현되거나 다양한 컴퓨터 구성요소를 통하여 수행될 수 있는 프로그램 명령어의 형태로 구현되어 컴퓨터 판독 가능한 기록 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포

함할 수 있다.

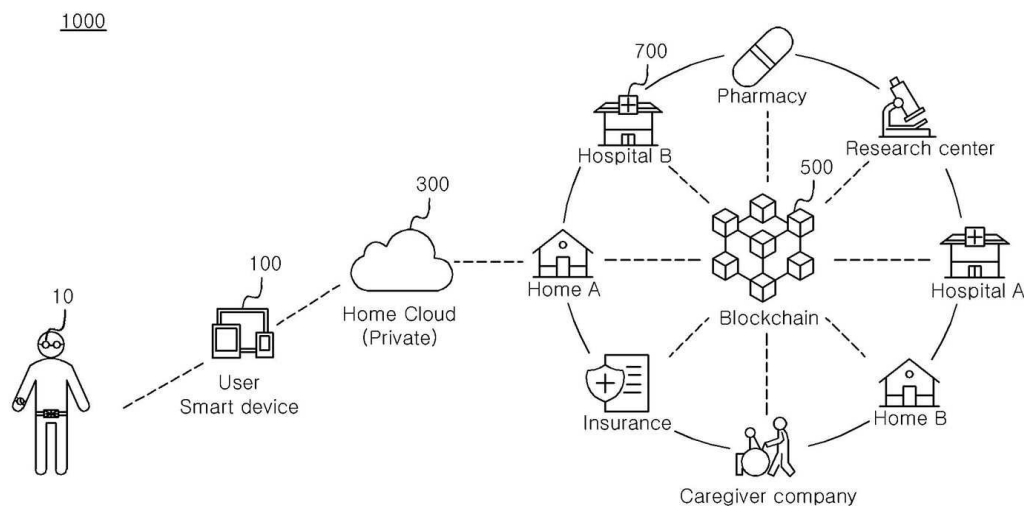
- [0113] 상기 컴퓨터 판독 가능한 기록 매체에 기록되는 프로그램 명령어는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수도 있다.
- [0114] 컴퓨터 판독 가능한 기록 매체의 예에는, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD 와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 ROM, RAM, 플래시 메모리 등과 같은 프로그램 명령어를 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다.
- [0115] 프로그램 명령어의 예에는, 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 상기 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.
- [0116] 이상에서는 실시예들을 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

부호의 설명

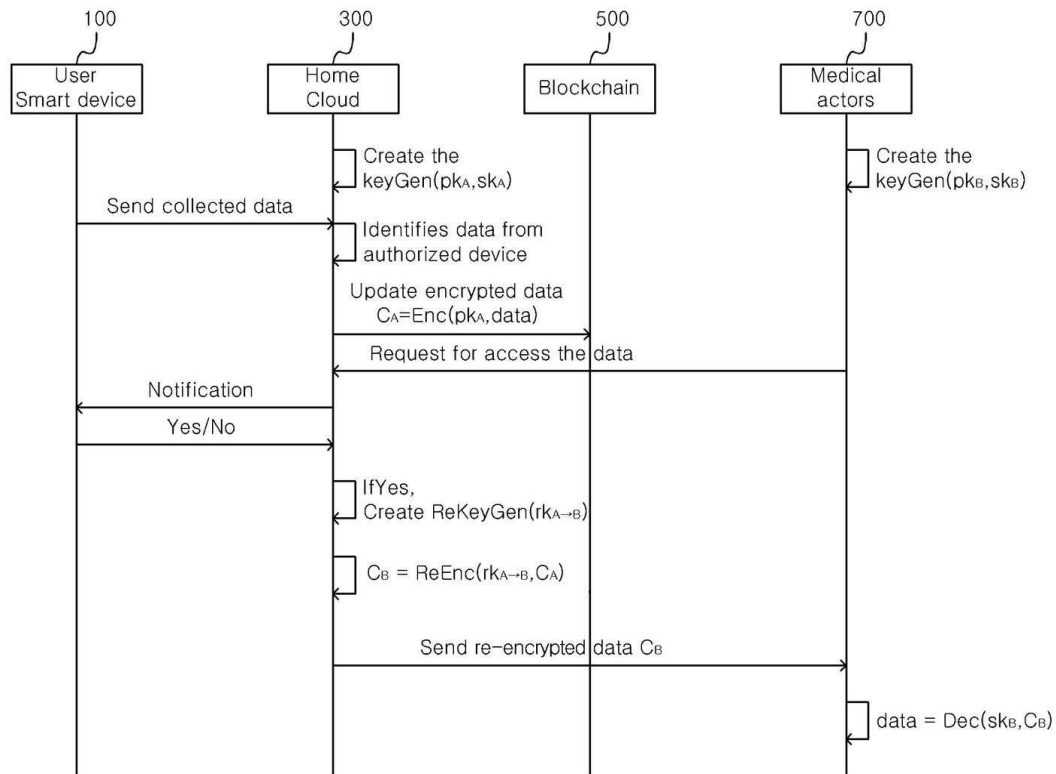
- [0117] 1000: 블록체인 기반의 데이터 공유 시스템
- 10: 센서 장치
- 100: 사용자 단말
- 300: 클라우드 서버
- 500: 블록체인
- 700: 참여자

도면

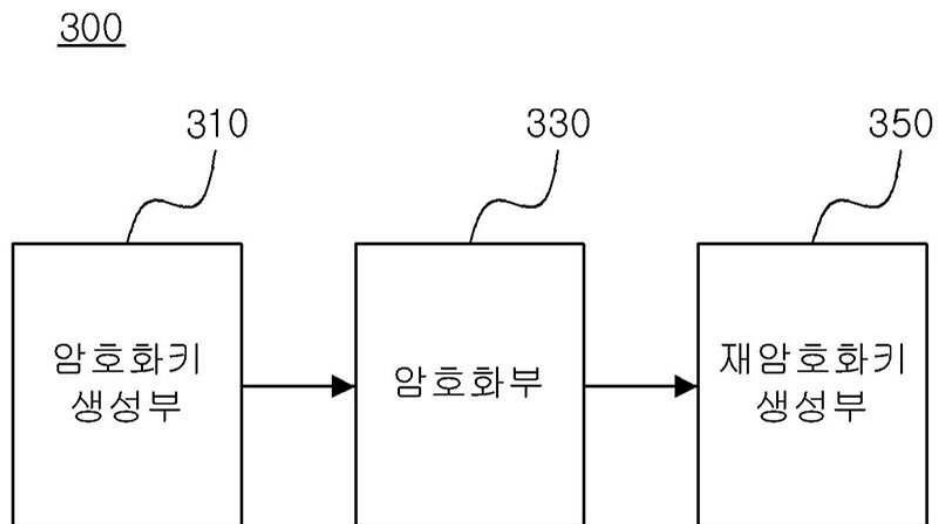
도면1



도면2



도면3



도면4

