(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년11월13일
(11) 등록번호 10-2044396
(24) 등록일자 2019년11월07일

(51) 국제특허분류(Int. Cl.)
G06Q 50/26 (2012.01) *G08B 21/18* (2006.01)
H04L 29/06 (2006.01) *H04L 29/08* (2006.01)
(52) CPC특허분류
G06Q 50/26 (2013.01)
G08B 21/18 (2013.01)
(21) 출원번호 10-2018-0059720
(22) 출원일자 2018년05월25일
심사청구일자 2018년05월25일
(56) 선행기술조사문헌
JP2017204707 A*
(뒷면에 계속)
전체 청구항 수 : 총 7 항

(73) 특허권자
서강대학교산학협력단
서울특별시 마포구 백범로 35 (신수동, 서강대학교)
(72) 발명자
장주욱
서울특별시 서대문구 가재울미래로 2, 206동 202호 (남가좌제1동, DMC파크뷰자이)
강응선
서울특별시 양천구 목동서로 2길 22 106동 807호
(74) 대리인
이지연

심사관 : 김일환

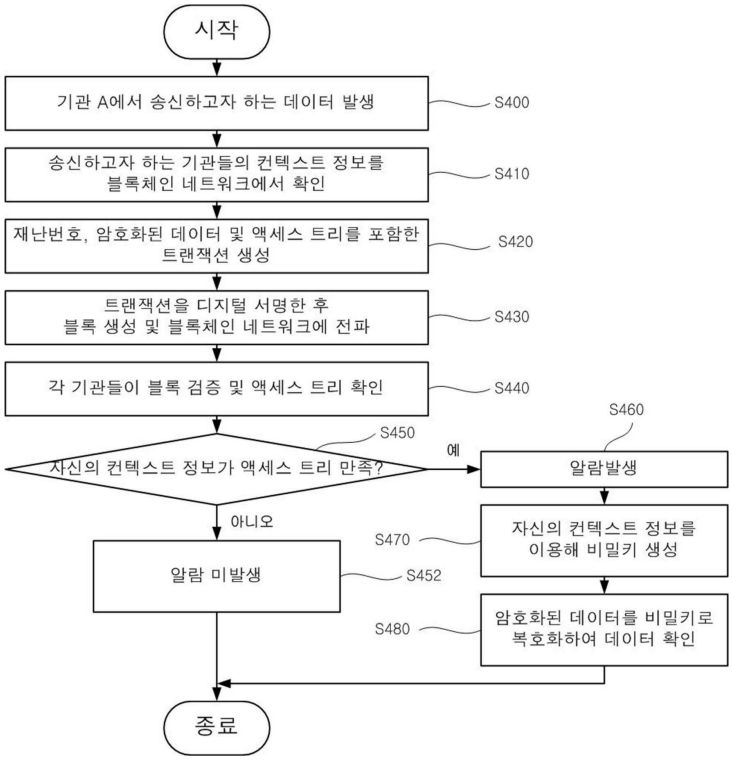
(54) 발명의 명칭 **블록체인을 기반으로 한 국가 재난 관리 시스템 및 방법**

(57) 요 약

본 발명은 블록체인을 기반으로 한 국가 재난 관리 시스템 및 방법에 관한 것이다. 상기 국가 재난 관리 시스템은, 신원이 증명된 다수 개의 노드들을 포함하여 구성된 블록체인 네트워크를 구비하고, 상기 블록체인 네트워크에 참여하는 노드들에 대한 컨텍스트 정보는 블록체인의 블록에 기록된 것을 특징으로 한다. 또한, 본 발명에 따

(뒷면에 계속)

대 표 도 - 도4



라 재난 관련 정보를 제공하고자 하는 노드는 재난 번호, 암호화된 데이터 및 액세스 트리를 포함한 트랜잭션을 생성하고, 상기 생성된 트랜잭션을 자신의 개인키를 이용하여 디지털 서명한 후, 상기 서명된 트랜잭션을 포함하는 블록을 생성하여 블록체인 네트워크로 전파하는 것을 특징으로 한다. 상기 데이터는 재난 관련 데이터이며, 상기 액세스 트리는 해당 트랜잭션을 포함하는 블록에 대한 접근 권한을 갖는 노드들의 컨텍스트 정보들을 이용하여 생성된 것으로서, 해당 트랜잭션에 포함된 암호화된 데이터에 대한 접근 권한 정보를 갖는 것이 바람직하다.

(52) CPC특허분류
H04L 63/102 (2013.01)
H04L 67/1089 (2013.01)
H04L 9/0825 (2013.01)
H04L 2209/38 (2013.01)

(56) 선행기술조사문헌
KR101781583 B1*
JP2017204070 A*
KR101921168 B1*
KR1020180022335 A*
KR1020050062977 A*
*는 심사관에 의하여 인용된 문헌

이 발명을 지원한 국가연구개발사업
과제고유번호 20170016280021001
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술진흥센터
연구사업명 대학 ICT 연구센터 지원
연구과제명 적응형 블록체인 플랫폼 기술 개발 및 전문 인력 양성
기 여 율 1/1
주관기관 서강대학교 산학협력단
연구기간 2017.06.01 ~ 2020.12.31

명 세 서

청구범위

청구항 1

재난에 대응하기 위하여 사전 설정된 정부의 중앙행정기관과 공공기관들의 서버들이 네트워크로 연결되어 이루어진 국가 재난 관리 시스템에 있어서,

신원이 증명된 상기 정부의 중앙 행정 기관과 공공 기관들의 서버들이 노드들로 참여하여 구성된 블록체인 네트워크를 구비하고,

상기 블록체인 네트워크에 참여하는 노드들은 블록체인을 저장 및 관리하고, 상기 블록체인 네트워크에 참여하는 노드들에 대한 컨텍스트 정보는 블록체인의 블록에 기록된 것을 특징으로 하며,

사전 설정된 재난에 대한 재난 관련 정보를 제공하고자 하는 노드는 재난 번호, 암호화된 데이터 및 액세스 트리를 포함한 트랜잭션을 생성하고, 상기 생성된 트랜잭션을 자신의 개인키를 이용하여 디지털 서명한 후, 상기 서명된 트랜잭션을 포함하는 블록을 생성하여 블록체인 네트워크로 전파하는 것을 특징으로 하며,

상기 데이터는 재난 관련 데이터이며,

상기 액세스 트리는 해당 트랜잭션을 포함하는 블록에 대한 접근 권한을 갖는 노드들의 컨텍스트 정보들을 이용하여 생성된 것으로서, 해당 트랜잭션에 포함된 암호화된 데이터에 대한 접근 권한 정보를 갖는 것을 특징으로 하며,

상기 블록체인 네트워크를 구성하는 노드들은 블록체인 네트워크에 새로운 블록이 생성되어 전파되면 자동으로 실행되는 알람용 어플리케이션을 구비하고,

상기 알람용 어플리케이션은,

블록을 전파한 노드에 대한 공개키를 이용하여 해당 블록에 포함된 트랜잭션을 복호화시키고,

상기 블록을 수신한 노드의 컨텍스트 정보가 상기 복호화된 트랜잭션에 포함된 액세스 트리를 만족하는지 여부를 판단하고,

상기 블록을 수신한 노드의 컨텍스트 정보가 상기 액세스 트리를 만족하면 상기 블록을 수신한 노드에게 알람(Alarm)을 발생시켜 재난 정보가 도착되었음을 알리는 것을 특징으로 하며,

상기 블록체인 네트워크를 구성하는 노드는,

재난 종료후, 재난 번호를 기준으로 하여 블록체인에 저장된 데이터를 검색하여, 데이터 발생시간, 데이터 생성기관, 데이터 접근 기관, 데이터 내용을 획득할 수 있는 것을 특징으로 하는 블록체인을 기반으로 한 국가 재난 관리 시스템.

청구항 2

삭제

청구항 3

제1항에 있어서, 상기 알람용 어플리케이션은,

상기 블록을 수신한 노드의 컨텍스트 정보가 상기 액세스 트리를 만족하면 알람(Alarm)을 발생시킨 후, 상기 블록을 수신한 노드의 컨텍스트 정보를 이용하여 비밀키를 생성하고, 상기 생성된 비밀키를 이용하여 상기 트랜잭션에 포함된 암호화된 데이터를 복호화하여 데이터 원문을 획득하는 것을 특징으로 하는 블록체인을 기반으로 한 국가 재난 관리 시스템.

청구항 4

제1항에 있어서, 상기 블록을 전파하는 노드는 재난 관련 데이터를 자신의 컨텍스트 정보를 이용하여 암호화시

키고, 상기 암호화된 데이터를 트랜잭션에 포함시킨 것을 특징으로 하는 블록체인을 기반으로 한 국가 재난 관리 시스템.

청구항 5

제1항에 있어서, 상기 트랜잭션에 포함된 액세스 트리는 재난의 종류에 따라 사전 설정된 대응 기관들에 대한 컨텍스트 정보들을 이용하여 생성된 것을 특징으로 하는 블록체인을 기반으로 한 국가 재난 관리 시스템.

청구항 6

삭제

청구항 7

재난에 대응하기 위하여 신원이 증명된 정부의 중앙행정기관과 공공기관들의 서버들이 노드들로 참여하여 구성된 블록체인 네트워크를 이용한 국가 재난 관리 방법에 있어서,

(a) 상기 블록체인 네트워크에 참여하는 노드들은, 자신들에 대한 컨텍스트 정보를 트랜잭션의 형태로 블록체인의 블록에 기록하는 단계;

(b) 재난 관련 정보를 제공하고자 하는 노드들은, 재난 번호, 암호화된 데이터 및 액세스 트리를 포함하는 트랜잭션을 생성하고, 상기 생성한 트랜잭션을 디지털 서명한 후, 상기 트랜잭션을 포함하는 블록을 생성하여 상기 블록체인 네트워크로 전파하는 단계;

(c) 상기 블록체인 네트워크를 구성하는 노드들은, 블록체인 네트워크에 새로운 블록이 생성되어 전파되면 자동으로 실행되는 알람용 어플리케이션을 설치하여 실행시키는 단계; 및

(d) 상기 블록체인 네트워크를 구성하는 노드는, 재난 종료후, 재난 번호를 기준으로 하여 블록체인에 저장된 데이터를 검색하여, 데이터 발생시간, 데이터 생성 기관, 데이터 접근 기관, 데이터 내용을 획득하는 단계;

를 포함하며,

상기 데이터는 재난 관련 데이터이며,

상기 액세스 트리는 해당 트랜잭션을 포함하는 블록에 대한 접근 권한을 갖는 노드들의 컨텍스트 정보들을 이용하여 생성된 것으로서, 해당 트랜잭션에 포함된 암호화된 데이터에 대한 접근 권한 정보를 갖는 것을 특징으로 하며,

상기 알람용 어플리케이션은,

블록을 전파한 노드에 대한 공개키를 이용하여 해당 블록에 포함된 트랜잭션을 복호화시키고,

상기 블록을 수신한 노드의 컨텍스트 정보가 상기 복호화된 트랜잭션에 포함된 액세스 트리를 만족하는지 여부를 판단하고,

상기 블록을 수신한 노드의 컨텍스트 정보가 상기 액세스 트리를 만족하면 상기 블록을 수신한 노드에게 알람(Alarm)을 발생시켜 재난 정보가 도착되었음을 알리는 것을 특징으로 하는 블록체인을 기반으로 한 국가 재난 관리 방법.

청구항 8

삭제

청구항 9

제7항에 있어서, 상기 알람용 어플리케이션은,

상기 블록을 수신한 노드의 컨텍스트 정보가 상기 액세스 트리를 만족하면 알람(Alarm)을 발생시킨 후, 상기 블록을 수신한 노드의 컨텍스트 정보를 이용하여 비밀키를 생성하고, 상기 생성된 비밀키를 이용하여 상기 트랜잭션에 포함된 암호화된 데이터를 복호화하여 데이터 원문을 획득하는 것을 특징으로 하는 블록체인을 기반으로 한 국가 재난 관리 방법.

청구항 10

제7항에 있어서, 상기 (b) 단계는,

트랜잭션을 생성하는 노드의 컨텍스트 정보를 이용하여 재난 관련 데이터를 암호화시키고, 상기 암호화된 데이터를 트랜잭션에 포함시킨 것을 특징으로 하는 블록체인을 기반으로 한 국가 재난 관리 방법.

청구항 11

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 블록체인을 기반으로 한 국가 재난 관리 시스템 및 방법에 관한 것으로서, 더욱 구체적으로는 신원이 증명된 노드들만 참여하는 프라이빗 블록체인 네트워크를 구성하고, 트랜잭션에 대한 접근 권한 정보를 제공함으로써 트랜잭션에 포함된 암호화된 데이터를 접근 권한있는 노드들만이 접근할 수 있도록 하여, 악의적인 노드가 참여할 수 없고 모든 신원 증명된 기관이 블록을 신속하게 생성할 수 있고, 블록이 전파되더라도 접근 권한이 있는 재난 관련된 대응 기관만이 데이터에 접근할 수 있도록 한 국가 재난 관리 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 기존의 국가재난안전통신망인 PS-LTE(Public Safety LTE)는 정부의 각 부처기관과 공공기관이 합동 대응이 필요한 재난 발생 시 다양한 기관이 협업하여 효과적으로 대응할 수 있도록 구축한 단일 통신망이다. 이러한 종래의 국가재난안전통신망은 전국 규모로 기존 LTE 기술에 재난 안전에 필수적인 기능을 추가한 기술이다.

[0003] 국가재난안전통신망은 음성통신 뿐만 아니라 화상통신과 고화질 이미지 전송 등 고속 데이터 통신 또한 지원하여 재난 현장 상황을 정확하게 파악하고 지휘통제 및 구조에 더욱 신속하게 대응할 수 있다.

[0004] 기존의 국가재난안전통신망을 통해 전송되는 데이터들은 서버 중심 데이터베이스에 저장됨에 따라, 이러한 데이터들은 악의적 해커에 의해 접근될 수 있고 조작, 위조 및 삭제될 수 있어 서버 중심의 보안 문제가 존재하고, 각 기관에서도 데이터 위/변조가 가능해 데이터의 무결성과 신뢰성이 보장되지 않는 문제점이 있다.

[0005] 한편, 블록체인(Blockchain)은 공공 거래 장부라고도 불리우는데, 블록(block)에 데이터를 담아 체인(chain) 형태로 연결한 것으로서, 수많은 노드에 이를 동시에 복제해 저장하는 분산형 데이터 저장 기술이다. 블록체인 기술은 중앙 집중형 서버에 거래 기록을 보관하지 않고 거래에 참여하는 모든 사용자에게 거래 내역을 보내 주며, 거래때마다 모든 거래 참여자들이 정보를 공유하고 이를 대조함으로써 데이터 위조 및 변조를 방지할 수 있게 된다. 또한, 이러한 장점으로 인해 모든 데이터와 정보들을 모든 참여자들이 블록체인의 형태로 공유하게 되어 투명성과 무결정이 보장된다. 전술한 블록체인은 블록체인 네트워크에 참여하는 모든 노드들이 메모리에 저장하고 관리하게 된다.

한편, 블록체인을 저장하는 다수 개의 노드들로 이루어지는 블록체인 네트워크에 있어서, 하나의 노드가 전자서명된 트랜잭션을 브로드캐스팅하면, 이를 수신한 모든 노드들은 작업 증명 과정을 진행하게 되고, 이에 따라 최초로 논스값을 찾은 노드는 블록체인 네트워크의 다른 노드들에 의해 검증된 후 블록 생성 권한을 갖게 된다. 블록 생성 권한을 가진 노드는 트랜잭션을 포함한 블록 생성 정보를 블록체인 네트워크의 모든 노드들로 브로드캐스팅하게 되고, 이를 수신한 모든 노드들은 트랜잭션을 포함하는 블록을 생성하고 자신의 블록체인에 상기 생성된 블록을 연결시켜 저장하게 된다.

기존의 블록체인 기술에서는 이전 블록의 해시 값이 다음 블록에 포함되면서 블록이 연결되어 있다. 블록은 트랜잭션이라는 형태로 구성된 데이터들과 랜덤 변수인 nonce 값으로 이루어져 있다. Nonce란 블록 생성 난이도를 조절하기 위해 블록에 포함된 트랜잭션들의 해싱 값이 기준 값 보다 작도록 만족시키는 랜덤 변수로 nonce를 찾는 과정을 작업 증명(Proof-of-Work)라고 한다. Proof-of-Work를 사용함으로써 블록체인 네트워크에 참여한 노드들 중 어떠한 노드가 nonce를 찾는데 성공하여 블록을 생성할지 모르기 때문에 악의적 노드의 attack을 방지

한다.

[0006] 또한, 작업 증명(Proof-of-Work) 과정에 의해 생성된 블록들은 해시 값으로 연결되어 있기 때문에 악의적 노드가 블록의 데이터를 변경하면 전혀 다른 해시 값이 되기 때문에 블록체인 네트워크 내의 모든 노드들이 이 사실을 인지하게 되기 때문에 악의적 노드의 computing power가 51%를 넘기지 않는 한 데이터 무결성(Data integrity) 특성을 보장한다.

[0007] 전술한 Proof-of-Work 방식의 블록 생성 합의 과정은 네트워크상의 노드에 대한 정보가 없어 신뢰가 분산되어 있는 상황에서 효율적이지만, nonce를 찾기 위해 엄청난 양의 computing power를 사용하여야 하고 그만큼 블록 생성에 시간이 많이 소요되는 문제점이 있다.

[0008] 따라서, 국가 재난 안전 통신망은 신속한 재난 대응을 위하여 데이터 송수신이 신속하게 이루어져야 하므로, 블록 생성을 위하여 많은 시간이 소요되는 작업 증명(Proof-of-Work) 과정이 요구되는 종래의 블록 생성 합의 과정은 국가 재난 안전 통신망에 그대로 적용될 수 없게 된다.

선행기술문헌

특허문헌

[0009] (특허문헌 0001) 한국공개특허공보 제 10-2018-0046269호

발명의 내용

해결하려는 과제

[0010] 전술한 문제점을 해결하기 위한 본 발명의 목적은 신원이 증명된 노드들만 참여하는 프라이빗 블록체인 네트워크를 구성하고, 트랜잭션에 대한 접근 권한 정보를 제공함으로써 트랜잭션에 포함된 암호화된 데이터를 접근 권한있는 노드들만이 접근할 수 있도록 하여, 악의적인 노드가 참여할 수 없고 모든 신원 증명된 기관이 블록을 신속하게 생성할 수 있고, 블록이 전파되더라도 접근 권한이 있는 재난 관련된 대응 기관만이 데이터에 접근할 수 있도록 한 국가 재난 관리 시스템 및 방법을 제공하는 것이다.

과제의 해결 수단

[0011] 전술한 기술적 과제를 달성하기 위한 본 발명의 제1 특징에 따른 국가 재난 관리 시스템은, 신원이 증명된 다수개의 노드들을 포함하여 구성된 블록체인 네트워크를 구비하고, 상기 블록체인 네트워크에 참여하는 노드들에 대한 컨텍스트 정보는 블록체인의 블록에 기록된 것을 특징으로 하며,

[0012] 재난 관련 정보를 제공하고자 하는 노드는 재난 번호, 암호화된 데이터 및 액세스 트리를 포함한 트랜잭션을 생성하고, 상기 생성된 트랜잭션을 자신의 개인키를 이용하여 디지털 서명한 후, 상기 서명된 트랜잭션을 포함하는 블록을 생성하여 블록체인 네트워크로 전파하는 것을 특징으로 하며,

[0013] 상기 데이터는 재난 관련 데이터이며,

[0014] 상기 액세스 트리는 해당 트랜잭션을 포함하는 블록에 대한 접근 권한을 갖는 노드들의 컨텍스트 정보들을 이용하여 생성된 것으로서, 해당 트랜잭션에 포함된 암호화된 데이터에 대한 접근 권한 정보를 갖는 것이 바람직하다.

[0015] 전술한 제1 특징에 따른 블록체인을 기반으로 한 국가 재난 관리 시스템에 있어서, 상기 블록체인 네트워크를 구성하는 노드들은 블록체인 네트워크에 새로운 블록이 생성되어 전파되면 자동으로 실행되는 알람용 어플리케이션을 구비하고,

[0016] 상기 알람용 어플리케이션은, 블록을 전파한 블록 전파 노드에 대한 공개키를 이용하여 해당 블록에 포함된 트랜잭션을 복호화시키고, 상기 블록을 수신한 블록 수신 노드의 컨텍스트 정보가 상기 복호화된 트랜잭션에 포함된 액세스 트리를 만족하는지 여부를 판단하고, 상기 블록 수신 노드의 컨텍스트 정보가 상기 액세스 트리를 만족하면 상기 블록 수신 노드에게 알람(Alarm)을 발생시켜 재난 정보가 도착되었음을 알리는 것이 바람직하며,

[0017] 상기 블록 수신 노드의 컨텍스트 정보가 상기 액세스 트리를 만족하면 알람(Alarm)을 발생시킨 후, 상기 블록

수신 노드의 컨텍스트 정보를 이용하여 비밀키를 생성하고, 상기 생성된 비밀키를 이용하여 상기 트랜잭션에 포함된 암호화된 데이터를 복호화하여 데이터 원문을 획득하는 것이 더욱 바람직하다.

[0018] 전술한 제1 특징에 따른 블록체인을 기반으로 한 국가 재난 관리 시스템에 있어서, 상기 블록 전파 노드는 재난 관련 데이터를 자신의 컨텍스트 정보를 이용하여 암호화시키고, 상기 암호화된 데이터를 트랜잭션에 포함시킨 것이 바람직하며, 상기 트랜잭션에 포함된 액세스 트리는 재난의 종류에 따라 사전 설정된 대응 기관들에 대한 컨텍스트 정보들을 이용하여 생성된 것이 바람직하다.

[0019] 전술한 제1 특징에 따른 블록체인을 기반으로 한 국가 재난 관리 시스템에 있어서, 상기 블록체인 네트워크를 구성하는 노드는, 재난 종료후, 재난 번호를 기준으로 하여 블록체인에 저장된 데이터를 검색하여, 데이터 발생 시간, 데이터 생성 기관, 데이터 접근 기관, 데이터 내용을 획득하는 것이 바람직하다.

[0020] 본 발명의 제2 특징에 따른 국가 재난 관리 방법은, 신원이 증명된 다수 개의 노드들로 구성된 블록체인 네트워크를 이용한 국가 재난 관리 방법에 관한 것으로서, (a) 상기 블록체인 네트워크에 참여하는 노드들에 대한 컨텍스트 정보를 트랜잭션의 형태로 블록체인의 블록에 기록하는 단계; 및 (b) 재난 관련 정보를 제공하고자 하는 노드에 의해, 재난 번호, 암호화된 데이터 및 액세스 트리를 포함하는 트랜잭션이 생성되고, 상기 생성된 트랜잭션을 디지털 서명한 후, 상기 트랜잭션을 포함하는 블록을 생성하여 상기 블록체인 네트워크로 전파하는 단계;를 포함하며,

[0021] 상기 데이터는 재난 관련 데이터이며,

[0022] 상기 액세스 트리는 해당 트랜잭션을 포함하는 블록에 대한 접근 권한을 갖는 노드들의 컨텍스트 정보들을 이용하여 생성된 것으로서, 해당 트랜잭션에 포함된 암호화된 데이터에 대한 접근 권한 정보를 갖는 것이 바람직하다.

[0023] 전술한 제2 특징에 따른 블록체인을 기반으로 한 국가 재난 관리 방법에 있어서, (c) 상기 블록체인 네트워크를 구성하는 노드들에 대해, 블록체인 네트워크에 새로운 블록이 생성되어 전파되면 자동으로 실행되는 알람용 어플리케이션을 설치하여 실행시키는 단계;를 더 구비하고,

[0024] 상기 알람용 어플리케이션은, 블록을 전파한 노드에 대한 공개키를 이용하여 해당 블록에 포함된 트랜잭션을 복호화시키고, 상기 블록을 수신한 블록 수신 노드의 컨텍스트 정보가 상기 복호화된 트랜잭션에 포함된 액세스 트리를 만족하는지 여부를 판단하고, 상기 블록 수신 노드의 컨텍스트 정보가 상기 액세스 트리를 만족하면 상기 블록 수신 노드에게 알람(Alarm)을 발생시켜 재난 정보가 도착되었음을 알리는 것이 바람직하며,

[0025] 상기 블록 수신 노드의 컨텍스트 정보가 상기 액세스 트리를 만족하면 알람(Alarm)을 발생시킨 후, 상기 블록 수신 노드의 컨텍스트 정보를 이용하여 비밀키를 생성하고, 상기 생성된 비밀키를 이용하여 상기 트랜잭션에 포함된 암호화된 데이터를 복호화하여 데이터 원문을 획득하는 것이 더욱 바람직하다.

발명의 효과

[0026] 본 발명은 CP-ABE 알고리즘을 사용하여 데이터에 접근 권한을 부여한 블록체인을 기반으로 한 국가재난안전망에 관한 것으로서, 재난이 발생하였을 때 이루어지는 재난 상황 지휘통제 및 보고와 실시간 의사소통에서 발생하는 모든 데이터가 블록체인의 데이터 무결성과 자기인증 및 부인방지 특성으로 인해 상황 진행과 종료 후 피드백 과정에서 신뢰성을 보장 받는다.

[0027] 본 발명에 따른 블록체인 네트워크는 프라이빗 블록체인 네트워크로 구성되어 허가된 기관만이 노드로서 참여가능하고, 참여할 때 검증을 거치고 해당 기관에 대한 컨텍스트 정보를 블록체인에 기록함에 따라, 각 노드들에 대한 신원이 증명된다. 따라서, 본 발명에 따른 시스템은, 네트워크에 악영향을 줄 수 있는 악의적 노드가 참여할 수 없을 뿐만 아니라, 한번 기록된 데이터는 위/변조가 불가하기 때문에 보안성이 향상된다.

[0028] 또한, 본 발명에 따른 블록체인 네트워크 내에서의 블록 생성 합의 과정은 Proof-of-Authority (PoA) 방식을 응용하여 신원이 증명된 모든 각 기관들이 전파할 데이터 발생시에 블록을 생성하고 다른 기관들이 검증할 수 있게 됨으로써, 작업 증명(Proof-of-Work) 방식에 따른 기존의 블록 생성 합의 과정과는 달리, 블록 생성속도가 빨라 재난 상황에서 실시간으로 즉각적인 지휘 통제 및 보고와 의사소통이 블록체인 네트워크에 전파되어 이루어질 수 있다.

[0029] 또한, 본 발명에 따른 국가 재난 안전 관리 시스템에서 발생하는 모든 데이터는 CP-ABE 알고리즘을 이용하여 접근 권한이 부여된다. 따라서, 블록이 생성되어 전파되더라도, 블록 내 트랜잭션에 대하여 일부 기관들에 대해서

만 접근 권한이 부여된다. 그 결과, 블록체인에 기록된 해당 기관들의 컨텍스트 정보를 바탕으로 생성된 액세스 트리를 트랜잭션에 포함시키고, 상기 트랜잭션에 포함된 액세스 트리를 만족하는 컨텍스트 정보를 가진 기관만이 해당 트랜잭션내에 포함된 암호화된 데이터를 복호화하여 데이터에 접근할 수 있다.

[0030] 기존의 일반적인 블록체인 네트워크에서는 데이터가 트랜잭션 형태로 블록을 통해 전파되면 참여한 모든 노드들이 데이터를 확인할 수 있고 알람을 받게 된다. 하지만, 재난 상황에서는 재난 대응 매뉴얼에 나와 있는 보고체계와 재난 상황에 맞게 지휘 및 통제가 이루어져야 하고 관련된 기관들만이 의사 소통이 가능해야 한다. 따라서, 모든 기관이 데이터를 전파받아 확인할 수 있는 기존의 블록체인 네트워크은 본 발명에 따른 국가재난 관리시스템의 블록체인 네트워크에는 적절치 않게 된다.

[0031] 따라서, 본 발명에 따른 국가재난관리 시스템의 블록체인 네트워크는 액세스 트리를 이용하여 접근 권한을 부여함으로써, 액세스 트리를 만족하는 컨텍스트 정보를 가진 기관만이 알람을 받고 데이터에 접근할 수 있도록 한다.

도면의 간단한 설명

[0032] 도 1은 본 발명의 바람직한 실시예에 따른 국가 재난 관리 시스템에 있어서, 정부의 중앙행정기관과 공공기관이 블록체인 네트워크를 구성하고, 범죄 또는 자연재해와 같은 재난 신고를 통해 이를 인지한 기관이 관련된 데이터에 접근권한을 부여하여 트랜잭션 형태로 블록을 생성하여 블록체인 네트워크에 전파하는 과정을 개념적으로 도시한 모식도이다.

도 2는 본 발명의 바람직한 실시예에 따른 국가 재난 관리 시스템에 있어서, 블록체인 네트워크에 참여하는 기관들의 컨텍스트 정보를 트랜잭션 형태로 블록에 저장하여 블록체인 네트워크에 기록하는 과정을 예시적으로 도시한 모식도이다.

도 3은 본 발명의 바람직한 실시예에 따른 국가 재난 관리 시스템에 있어서, 블록체인 네트워크에서 새로운 블록 생성 시 각 기관이 자신의 컨텍스트 정보가 트랜잭션에 포함된 액세스 트리를 만족할 경우 알람을 발생시키는 어플리케이션의 동작 과정을 순차적으로 도시한 순서도이다.

도 4는 본 발명의 바람직한 실시예에 따른 국가 재난 관리 시스템에 있어서, 재난 상황에서 한 기관이 데이터를 블록체인 네트워크에 송신하고 다른 기관이 수신하여 데이터를 확인하는 과정을 순차적으로 도시한 순서도이다.

도 5는 본 발명의 바람직한 실시예에 따른 국가 재난 관리 시스템에 있어서, 재난 상황 종료 후 피드백을 위해 블록체인 네트워크에 저장되어 있는 데이터들을 검색하는 과정을 순차적으로 도시한 순서도이다.

도 6 및 도 7은 본 발명의 바람직한 실시예에 따른 국가 재난 관리 시스템에 있어서, 액세스 트리를 설명하기 위하여 예시적으로 도시한 것이다.

발명을 실시하기 위한 구체적인 내용

[0033] 본 발명에 따른 국가 재난 관리 시스템은 먼저 재난에 관여하는 정부의 중앙 행정기관과 재난에 대응하는 공공기관들이 블록체인 네트워크에 참여하기 위해 DApps에 의해 검증을 거치고 신원이 증명되면 기관 이름, 부서 이름, 주소, 소속과 같은 컨텍스트 정보를 블록체인에 기록한다.

[0034] 또한, 본 발명에 따른 국가 재난 관리 시스템은, 블록 생성 합의 과정으로 Proof-of-Authority를 응용하여 모든 기관들이 네트워크에 참여할 때 신원이 증명되어 트랜잭션과 블록을 검증하고 생성할 수 있는 validator가 될 뿐만 아니라, 블록을 생성하는데 있어서 각 노드들이 경쟁하지 않기 때문에 computing power의 낭비가 없고 생성속도가 빠르다.

[0035] 또한, 본 발명에 따른 국가 재난 관리 시스템에서의 각 기관은 개인키(Private key)와 공개키(Public key)를 갖고 있고 블록체인 네트워크에 포함된 모든 기관의 공개키를 알고 있으며 디지털서명을 위해 ECDSA알고리즘을 사용한다. 또한, 본 발명에 따른 국가 재난 관리 시스템에서의 각 기관은 재난 번호, 재난 상황에서 송신하고자 하는 CP-ABE 알고리즘을 이용해 암호화된 데이터, 및 접근 권한 정보를 나타내는 액세스 트리를 포함하는 트랜잭션을 생성하고, 상기 트랜잭션을 개인키로 암호화하여 디지털 서명한다. 이렇게 디지털 서명된 트랜잭션들을 모아 블록을 생성하여 전파하면, 블록이 전파된 모든 기관들은 블록을 전파한 기관의 공개키로 트랜잭션을 복호화 해봄으로써 데이터를 전파한 기관이 트랜잭션을 보낸 것임을 증명할 수 있게 되고, 그 결과 자기인증(Authentication)과 부인방지(Non-Repudiation)를 보장하고 암호화된 데이터와 액세스 트리를 확인할 수 있다.

[0036] 또한, 본 발명에 따른 국가 재난 관리 시스템의 블록체인 네트워크에서는, 모든 노드들이 알람용 어플리케이션을 설치 및 실행함으로써, 새로이 생성된 블록이 블록체인 네트워크에 전파되면, 자동으로 블록을 생성한 기관의 공개키로 블록에 포함된 트랜잭션을 복호화하여 액세스 트리를 확인하고 컨텍스트 정보가 액세스 트리를 만족하면 알람을 울려 담당자가 인지할 수 있게 된다. 따라서, 액세스 트리를 만족하는 컨텍스트 정보를 가진 기관 및 부서는 알람을 받고 자신의 컨텍스트 정보를 이용하여 비밀키를 만들어 CP-ABE 알고리즘을 이용해 암호화된 암호문을 복호화하여 데이터의 원문을 얻는다.

[0037] 이러한 방식으로 재난 상황에서 지휘통제, 보고, 기관들 간의 의사소통이 신속하게 블록체인 네트워크에서 이루어지고, 모든 트랜잭션들은 블록으로 이어져 저장되기 때문에 데이터 위/변조가 불가능한 데이터 무결성이 보장되어 재난 상황에서 발생하는 모든 데이터가 어느 시간에 어느 기관이 송신하고 어느 기관이 수신하는지에 대한 신뢰성을 보장한다.

[0038] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예에 따른 블록체인을 기반으로 한 국가 재난 관리 시스템의 구조 및 동작에 대하여 구체적으로 설명한다.

[0039] 도 1은 본 발명의 바람직한 실시예에 따른 국가 재난 관리 시스템에 있어서, 정부의 중앙행정기관과 공공기관의 서버들이 노드들로 참여하는 블록체인 네트워크를 구성하고, 범죄 또는 자연재해와 같은 재난 신고를 통해 이를 인지한 기관이 관련된 데이터에 접근권한을 부여하여 트랜잭션 형태로 블록을 생성하여 블록체인 네트워크에 전파하는 과정을 개념적으로 도시한 모식도이다.

[0040] 도 1을 참조하면, 본 발명에 따른 국가 재난 관리 시스템은, 재난에 대응하는 정부의 중앙행정기관과 산하에 있는 지방자치단체, 경찰, 소방, 군대, 의료 등의 공공기관들의 서버들이 노드로서 참여하여 블록체인 네트워크를 구성하고, 범죄 또는 자연재해와 같은 재난 신고를 통해 이를 인지한 기관에 대응되는 노드가 해당 재난의 보고체계에 대응되는 기관들에 대응되는 노드들에 대해 재난 상황과 관련된 데이터에 접근 권한을 부여하고, 트랜잭션 형태로 블록을 생성하여 블록체인 네트워크에 전파한다. 상기 트랜잭션에는 재난 번호, 암호화된 재난 관련 데이터 및 접근 권한 정보를 갖는 액세스 트리가 포함된다.

[0041] 재난을 인지한 기관은 재난 번호를 부여하고, 재난 대응 매뉴얼의 보고체계에 맞게 액세스 트리를 구성하고, 액세스 트리와 CP-ABE를 이용해 암호화한 데이터를 개인키로 암호화하여 트랜잭션을 생성하여 블록에 포함시켜 블록체인 네트워크에 전파한다. 상기 데이터는 재난 관련 데이터로서, 재난 상황에 관련된 정보와 이미지 및 영상 데이터 등을 포함한다.

[0042] 상기 재난 발생을 감지한 노드는 CP-ABE(Ciphertext-Policy Attribute Based Encryption) 알고리즘에 따라 자신의 컨텍스트 정보를 이용하여 상기 데이터를 암호화시켜 트랜잭션에 포함시키게 된다.

[0043] 기존의 CP-ABE 알고리즘은 제3 인증기관이 비밀키를 발생하는 것을 특징으로 하나, 본 발명에 따른 시스템에서는 각 노드에 대하여 데이터 암호화를 위한 공개키와 마스터키를 생성하여 블록체인에 기록하고, 모든 노드들이 확인할 수 있도록 한다. 따라서, 본 발명에 따른 시스템에서의 노드는 CP-ABE 알고리즘을 이용하여 데이터를 암호화시켜 트랜잭션에 포함시켜 블록체인 네트워크에 전파시키게 되며, 이러한 트랜잭션 수신 노드는 블록체인 네트워크에 기록된 트랜잭션 생성 노드의 마스터키와 트랜잭션 수신 노드의 컨텍스트 정보를 이용하여 비밀키를 생성하고, 상기 생성된 비밀키를 이용하여 상기 암호화된 데이터를 복호화하여 데이터 원문을 획득할 수 있게 된다.

[0044] 한편, 상기 블록의 트랜잭션에 포함된 액세스 트리를 만족하는 컨텍스트 정보를 가진 기관은 알람용 어플리케이션을 통해 알람(Alarm)을 받아 자신에게 데이터가 온 것을 인지하여 접근할 수 있고, 만족하지 못하는 기관은 알람을 받지 않는다.

[0045] 알람을 통해 자신에게 데이터가 수신된 사실을 인지한 기관은, 블록체인 네트워크에 저장되어 있는 트랜잭션 생성 노드의 마스터키와 자신의 컨텍스트 정보를 이용하여 비밀키를 생성하고, 상기 생성된 비밀키를 이용하여 상기 트랜잭션에 포함된 암호화된 데이터를 복호화하여 데이터 원문을 획득하게 된다.

[0046] 이하, 도 2를 참조하여 본 발명에 따른 국가 재난 관리 시스템의 블록체인 네트워크를 구성하는 노드들에 대하여 설명한다.

[0047] 도 2는 본 발명의 바람직한 실시예에 따른 국가 재난 관리 시스템에 있어서, 블록체인 네트워크에 참여하는 기관들의 컨텍스트 정보를 트랜잭션 형태로 블록에 저장하여 블록체인 네트워크에 기록하는 과정을 예시적으로 도시한 모식도이다.

[0048] 도 2를 참조하면, 본 발명에 따른 국가 재난 관리 시스템은 재난에 대응하는 정부의 중앙행정기관과 공공기관들의 서버들을 노드들로서 블록체인 네트워크에 참여시키기 위하여, 각 기관들의 서버에 대해 검증을 거치고 신원을 증명하고 난 후, 각 기관에 대한 컨텍스트 정보를 트랜잭션 형태로 블록체인에 기록한다. 이와 같이 각 노드에 대한 컨텍스트 정보를 블록체인에 기록함으로써, 각 기관들은 블록체인 네트워크에서 신원이 증명된다. 따라서, 신원이 증명된 각 노드들은 PoA(Proof-of-Authority)를 응용하여 블록을 생성하고 검증할 수 있기 때문에, 자신들이 송신하고자 할 데이터가 있을 경우 자체적으로 블록을 생성하여 데이터를 블록체인 네트워크에 전파할 수 있다.

[0049] 본 발명에 따라 블록체인에 기록되는 각 노드에 대한 컨텍스트 정보 항목은, 도 2에 도시된 바와 같이, 기관 이름, 부서 이름, 주소, 소속 등을 포함할 수 있으나, 이러한 항목들에 제한되는 것을 아니며 상황에 따라 컨텍스트 정보의 항목은 달라질 수 있을 것이다. 한편, 블록체인에 기록되는 각 노드에 대한 컨텍스트 정보는 타임스탬프 순으로 최신의 것만을 인정하기 때문에, 컨텍스트 정보를 수정해야 할 경우 수정하여 새로 블록체인에 기록하는 것이 바람직하다.

[0050] 이하, 도 3을 참조하여 각 노드에서 실행되는 알람용 어플리케이션의 동작에 대하여 구체적으로 설명한다.

[0051] 도 3은 본 발명의 바람직한 실시예에 따른 국가 재난 관리 시스템에 있어서, 블록체인 네트워크에서 새로운 블록 생성시 각 기관이 자신의 컨텍스트 정보가 트랜잭션에 포함된 액세스 트리를 만족할 경우 알람을 발생시키는 어플리케이션의 동작 과정을 순차적으로 도시한 순서도이다.

[0052] 본 발명에 따른 알람용 어플리케이션은 각 노드들에 설치되어, 블록체인 네트워크에 새로이 생성된 블록이 전파됨에 따라, 각 노드의 블록체인에 블록이 기록되면 자동으로 실행된다.

[0053] 도 3을 참조하면, 먼저 블록체인 네트워크에 새로운 블록이 생성되어 전파됨에 따라 블록체인에 기록되면(단계 300), 블록 내의 트랜잭션에 포함된 액세스 트리를 확인하기 위해 블록체인 네트워크상에 알려져 있는 트랜잭션을 생성한 기관의 공개키로 디지털 서명을 복호화한다(단계 310). 복호화가 되지 않으면 무효 트랜잭션으로 간주하고 인증을 거부한다(단계 322).

[0054] 상기 트랜잭션이 복호화되면(단계 320), 트랜잭션 내의 액세스 트리를 참조하여 자신의 컨텍스트 정보가 액세스 트리를 만족하는지 여부를 확인하여 해당 트랜잭션에 대한 접근 권한 여부를 확인한다(단계 330).

[0055] 자신의 컨텍스트 정보가 액세스 트리를 만족하는 경우 알람(Alarm)을 발생시켜 각 기관의 담당자가 재난 상황에서 발생한 데이터를 확인할 수 있도록 하고(단계 340), 그렇지 아니한 경우에는 알람을 발생시키지 않고 종료한다.

[0056] 이하, 도 4를 참조하여 본 발명에 따른 국가 재난 관리 시스템에서, 재난 상황에서 각 노드들이 데이터를 송수신하여 데이터를 확인하는 과정을 설명한다.

[0057] 도 4는 본 발명의 바람직한 실시예에 따른 국가 재난 관리 시스템에 있어서, 재난 상황에서 한 기관이 데이터를 블록체인 네트워크에 송신하고 다른 기관이 수신하여 데이터를 확인하는 과정을 순차적으로 도시한 순서도이다.

[0058] 도 4를 참조하면, 재난 상황을 인지하여 데이터를 전파, 상황실에서 내려오는 지휘통제, 각 기관들의 보고 재난에 대응하면서 이루어지는 기관들의 의사소통 등등 한 기관이 송신하고자 하는 데이터가 발생하면(단계 400), 이러한 데이터를 수신해야 될 기관들만이 데이터에 접근할 수 있도록 블록체인 네트워크에서 해당 기관들의 컨텍스트 정보를 확인한다(단계 410). 상기 데이터를 수신해야 될 기관들은 재난 상황에 따라 사전 설정된 재난 대응 매뉴얼에 포함된 기관들로 설정될 수 있으며, 특히 재난 대응 매뉴얼에 따른 보고 체계 및 지휘 통제 체계에 포함되는 기관들을 포함하거나, 그 외에도 재난 상황에 따라 적절하게 추가되거나 제외될 수 있을 것이다.

[0059] 다음, 상기 컨텍스트 정보들을 이용하여 액세스 트리를 구성하고, 데이터를 CP-ABE를 이용해 암호화한다(단계 420). 다음, 처음 재난을 인지한 기관이 부여한 재난 번호와 암호화된 데이터, 액세스 트리를 개인키로 디지털 서명하여 트랜잭션을 생성하고 블록을 구성하여 블록체인 네트워크에 전파한다(단계 430).

[0060] 각 노드에 설치되어 실행되는 알람용 어플리케이션을 통해, 각 기관들은 상기 전파된 블록을 검증하고 액세스 트리를 확인한다(단계 440). 각 노드는 자신의 컨텍스트 정보가 상기 트랜잭션에 포함된 액세스 트리를 만족하는지 여부를 판단한다(단계 450).

[0061] 만약 자신의 컨텍스트 정보가 액세스 트리를 만족하면, 알람(Alarm)을 발생시키고(단계 460), 자신의 컨텍스트 정보를 이용해 비밀키를 생성하고(단계 470), 상기 비밀키를 이용하여 데이터를 복호화하여 데이터 원문을 얻는다(단계 480).

[0062] 만약 자신의 컨텍스트 정보가 액세스 트리를 만족하지 못하면, 알람을 발생시키지 않고 데이터에 접근하지 않고 종료된다(단계 452).

[0063] 이하, 본 발명에 따른 국가 재난 관리 시스템에서 재난 상황이 종료된 후 재난 상황 정보를 피드백(feedback)하기 위하여 데이터를 검색하는 과정을 설명한다.

[0064] 도 5는 본 발명의 바람직한 실시예에 따른 국가 재난 관리 시스템에 있어서, 재난 상황 종료 후 피드백을 위해 블록체인 네트워크에 저장되어 있는 데이터들을 검색하는 과정을 순차적으로 도시한 순서도이다.

[0065] 도 5를 참조하면, 본 발명에 따른 국가 재난 관리 시스템에 있어서, 재난 상황에서 발생하는 모든 트랜잭션들은 해당 재난을 인지한 기관이 전파할 때 부여한 재난 번호를 포함하고 있다. 따라서, 재난 상황이 종료되면(단계 500), 피드백하고자 하는 재난 번호를 확인하고(단계 510), 블록체인 네트워크에서 재난 번호로 검색하여 해당 재난에 대한 블록과 트랜잭션을 찾는다(단계 520). 트랜잭션은 재난 번호, 암호화된 데이터와 액세스 트리를 포함한다.

[0066] 따라서, 트랜잭션에 포함된 재난 번호와 상기 검색하고자 한 재난번호가 일치하면(단계 530), 해당 트랜잭션에 포함된 액세스 트리를 확인하고(단계 540), 액세스 트리에 나타나 있는 기관에서 컨텍스트 정보를 이용하여 비밀키를 생성하고(단계 550), 상기 비밀키를 이용하여 상기 트랜잭션에 포함된 암호화된 데이터를 복호화시켜(단계 560), 데이터 발생시간, 데이터 생성 기관, 데이터 수신 기관, 데이터 내용 등을 확인한다(단계 570).

[0067] 본 발명에 따른 국가 재난 관리 시스템에 저장된 데이터들은 블록체인의 특성으로 인하여 자기인증, 부인방지, 데이터 무결성을 갖기 때문에, 피드백 과정에서 신뢰성을 가지게 된다.

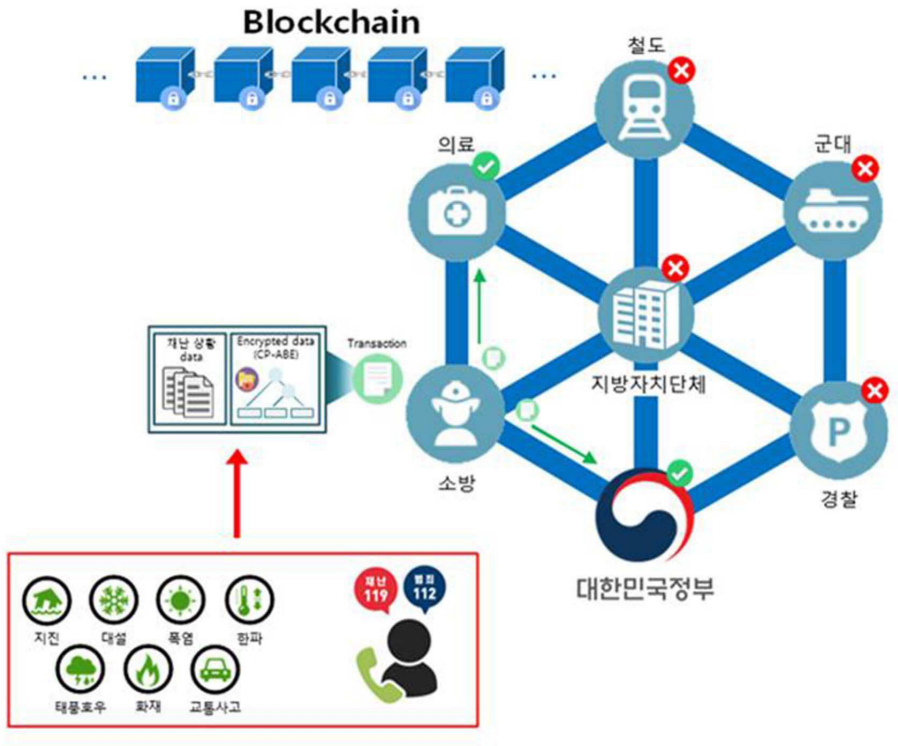
[0068] 도 6 및 도 7은 액세스 트리를 설명하기 위하여 예시적으로 도시한 도면이다. 도 6에 표시된 액세스 트리는 의사가 진료기록이라는 액세스 트리에 접근하여 접근 권한을 획득하는 과정을 나타내고 있다. 도 6을 참조하면, 의사에 대한 컨텍스트는, Job: 의사, Field:흉부외과, 담당환자ID : Kevin_319091 이며, 진료기록이라는 액세스 트리는 진료기록에 대한 접근 허가된 사용자는 담당 의사와 보호자이다. 도 6을 참조하면, 해당 의사는 진료기록이라는 액세스 트리에 접근하여 모든 컨텍스트를 만족하게 되어 접근 권한을 성공적으로 획득하게 된다. 하지만, 도 7을 참조하면, 간호사는 액세스 트리의 "Job:의사" 컨텍스트를 만족시키지 못하므로 접근 권한을 얻지 못하게 된다.

[0069] 이와 같이, 각 사용자별 또는 각 노드별 컨텍스트를 부여하고 데이터에 대한 액세스 트리를 생성함으로써, 많은 사용자 또는 노드의 접근 권한 관리를 할 수 있게 된다.

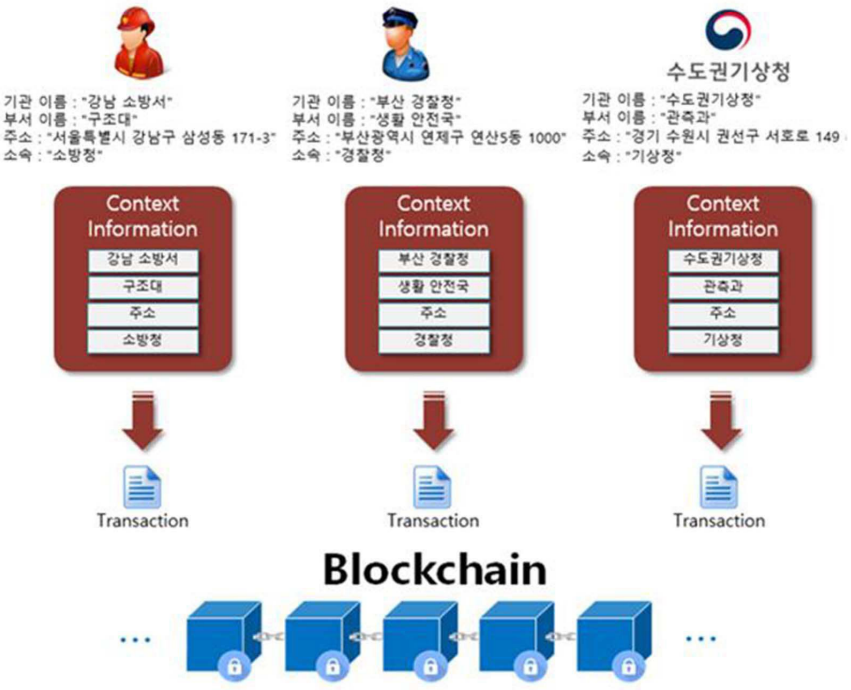
[0070] 이상에서 본 발명에 대하여 그 바람직한 실시예를 중심으로 설명하였으나, 이는 단지 예시일 뿐 본 발명을 한정하는 것이 아니며, 본 발명이 속하는 분야의 통상의 지식을 가진 자라면 본 발명의 본질적인 특성을 벗어나지 않는 범위에서 이상에 예시되지 않은 여러 가지의 변형과 응용이 가능함을 알 수 있을 것이다. 그리고, 이러한 변형과 응용에 관계된 차이점들은 첨부된 청구 범위에서 규정하는 본 발명의 범위에 포함되는 것으로 해석되어야 할 것이다.

도면

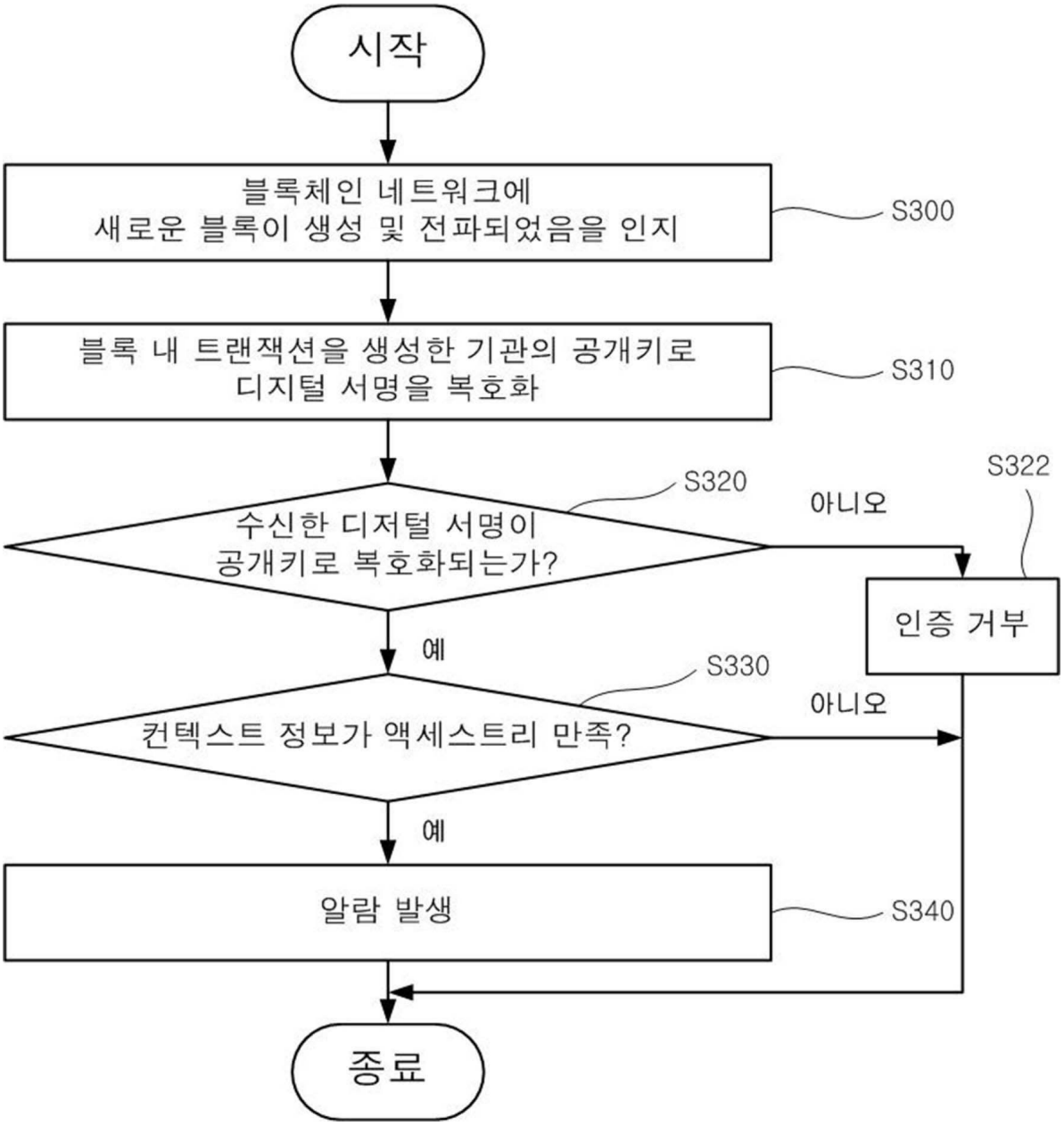
도면1


Blockchain
철도
의료
군대
지방자치단체
소방
경찰
대한민국정부
재난 상황 data
Encrypted data (CP-ABE)
Transaction
지진
대설
폭염
한파
태풍호우
화재
교통사고
재난 119
범죄 112

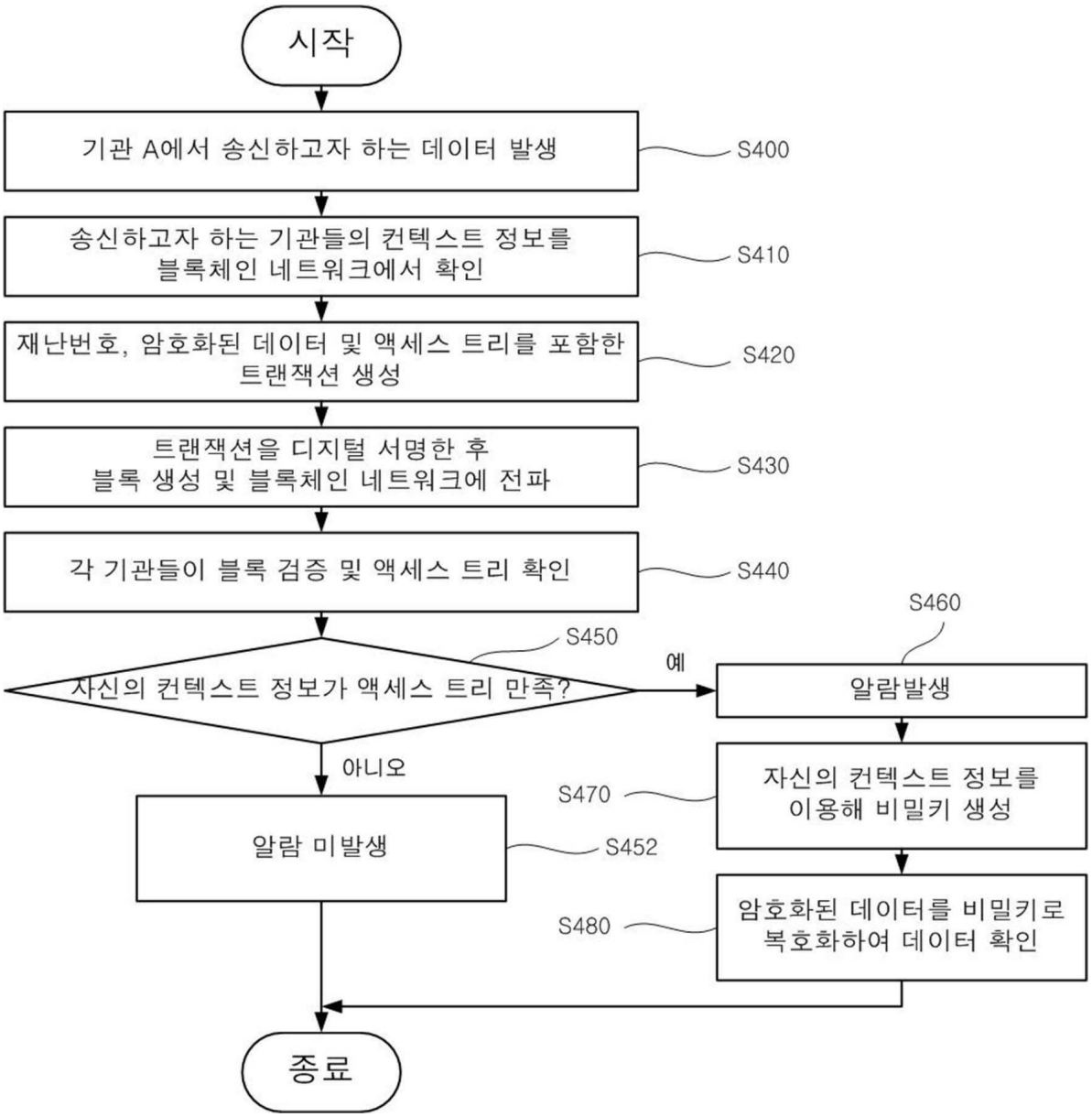
도면2


기관 이름 : "강남 소방서"
부서 이름 : "구조대"
주소 : "서울특별시 강남구 삼성동 171-3"
소속 : "소방청"
기관 이름 : "부산 경찰청"
부서 이름 : "생활 안전국"
주소 : "부산광역시 연제구 연산5동 1000"
소속 : "경찰청"
수도권기상청
기관 이름 : "수도권기상청"
부서 이름 : "관측과"
주소 : "경기 수원시 권선구 서호로 149
소속 : "기상청"
Context Information
강남 소방서
구조대
주소
소방청
Context Information
부산 경찰청
생활 안전국
주소
경찰청
Context Information
수도권기상청
관측과
주소
기상청
Transaction
Transaction
Transaction
Blockchain

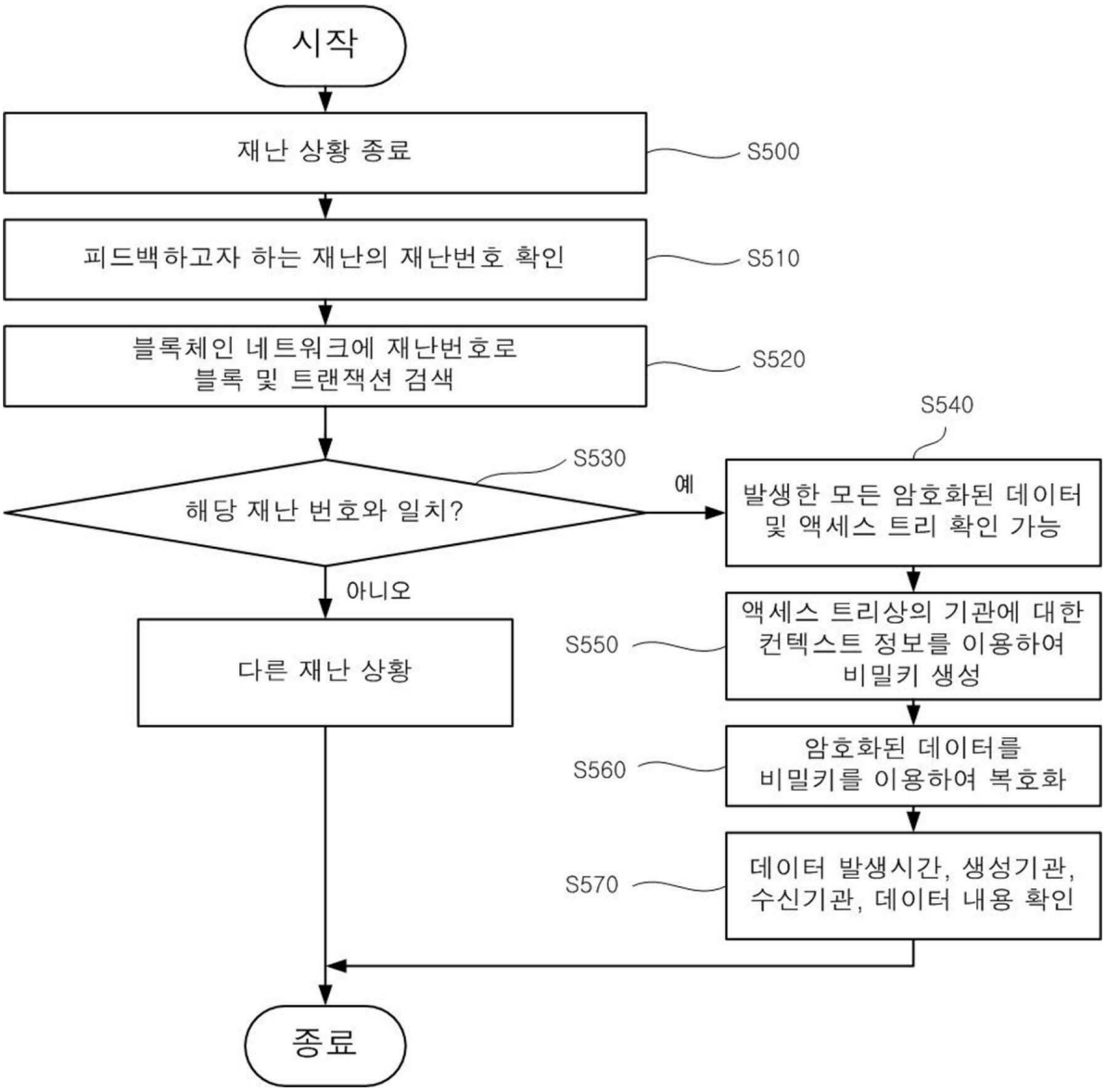
도면3


시작
블록체인 네트워크에
새로운 블록이 생성 및 전파되었음을 인지
S300
블록 내 트랜잭션을 생성한 기관의 공개키로
디지털 서명을 복호화
S310
S320
수신한 디저털 서명이
공개키로 복호화되는가?
아니오
S322
인증 거부
예
S330
컨텍스트 정보가 액세스트리 만족?
아니오
예
알람 발생
S340
종료

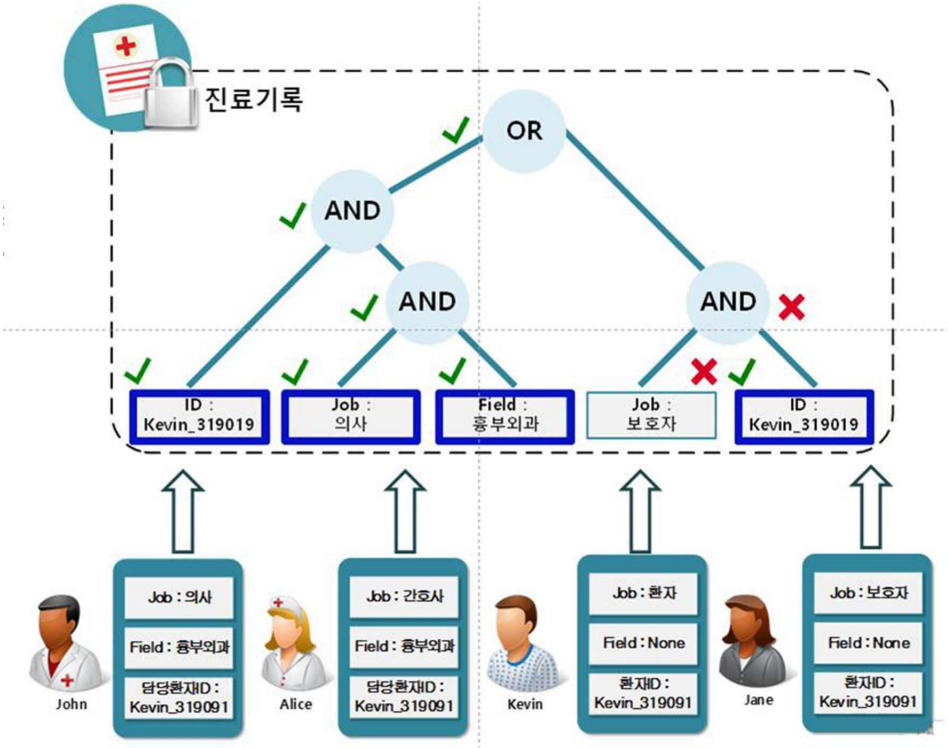
도면4


시작
기관 A에서 송신하고자 하는 데이터 발생
S400
송신하고자 하는 기관들의 컨텍스트 정보를 블록체인 네트워크에서 확인
S410
재난번호, 암호화된 데이터 및 액세스 트리를 포함한 트랜잭션 생성
S420
트랜잭션을 디지털 서명한 후 블록 생성 및 블록체인 네트워크에 전파
S430
각 기관들이 블록 검증 및 액세스 트리 확인
S440
S450
자신의 컨텍스트 정보가 액세스 트리 만족?
예
아니오
S460
알람발생
S470
자신의 컨텍스트 정보를 이용해 비밀키 생성
S480
암호화된 데이터를 비밀키로 복호화하여 데이터 확인
알람 미발생
S452
종료

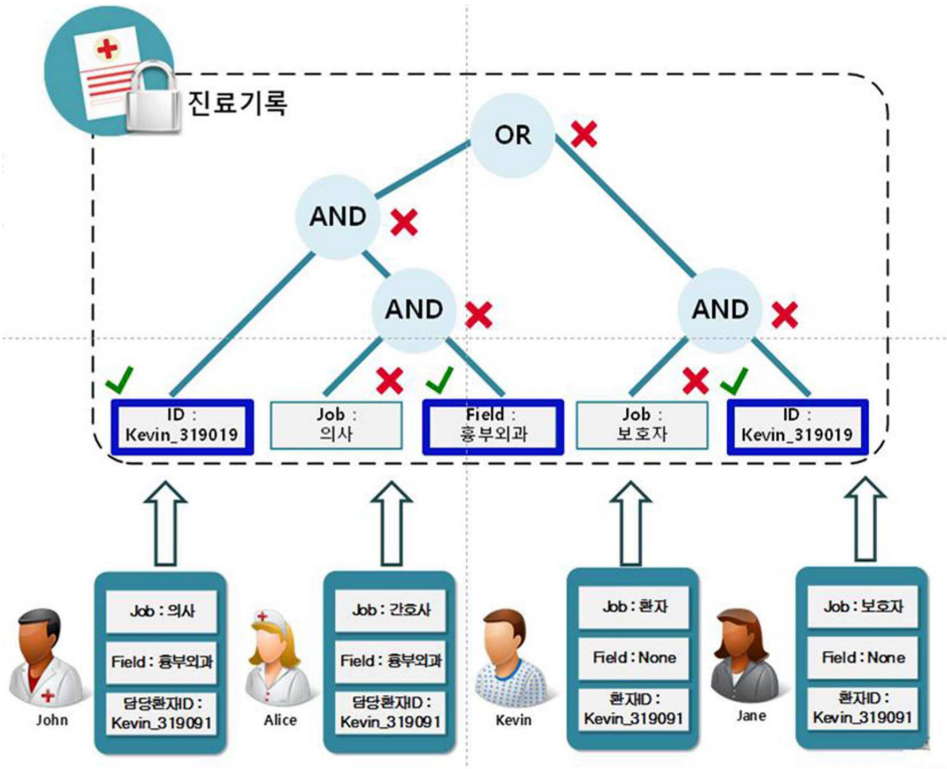
도면5


시작
재난 상황 종료
S500
피드백하고자 하는 재난의 재난번호 확인
S510
블록체인 네트워크에 재난번호로
블록 및 트랜잭션 검색
S520
S530
해당 재난 번호와 일치?
예
아니오
다른 재난 상황
S540
발생한 모든 암호화된 데이터
및 액세스 트리 확인 가능
S550
액세스 트리상의 기관에 대한
컨텍스트 정보를 이용하여
비밀키 생성
S560
암호화된 데이터를
비밀키를 이용하여 복호화
S570
데이터 발생시간, 생성기관,
수신기관, 데이터 내용 확인
종료

도면6


진료기록
OR
AND
AND
AND
ID : Kevin_319019
Job : 의사
Field : 흉부외과
Job : 보호자
ID : Kevin_319019
Job : 의사
Field : 흉부외과
담당환자ID : Kevin_319091
Job : 간호사
Field : 흉부외과
담당환자ID : Kevin_319091
Job : 환자
Field : None
환자ID : Kevin_319091
Job : 보호자
Field : None
환자ID : Kevin_319091
John
Alice
Kevin
Jane

도면7


진료기록
OR
AND
AND
AND
ID : Kevin_319019
Job : 의사
Field : 흉부외과
Job : 보호자
ID : Kevin_319019
Job : 의사
Field : 흉부외과
담당환자ID : Kevin_319091
Job : 간호사
Field : 흉부외과
담당환자ID : Kevin_319091
Job : 환자
Field : None
환자ID : Kevin_319091
Job : 보호자
Field : None
환자ID : Kevin_319091
John
Alice
Kevin
Jane