



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0137251
(43) 공개일자 2018년12월27일

(51) 국제특허분류(Int. Cl.)
G06F 21/50 (2013.01) G06F 21/62 (2013.01)
H04L 9/06 (2006.01) H04L 9/08 (2006.01)
(52) CPC특허분류
G06F 21/50 (2013.01)
G06F 21/62 (2013.01)
(21) 출원번호 10-2017-0076678
(22) 출원일자 2017년06월16일
심사청구일자 2017년06월16일

(71) 출원인
서강대학교산학협력단
서울특별시 마포구 백범로 35 (신수동, 서강대학교)
(72) 발명자
장주욱
서울특별시 서대문구 가재울미래로 2, 206동 202호 (남가좌제1동, DMC파크뷰자이)
정준우
서울특별시 금천구 금하로 9길 4-22
(74) 대리인
이지연

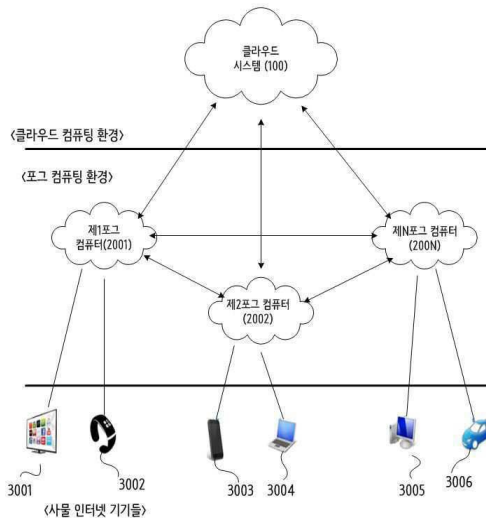
전체 청구항 수 : 총 6 항

(54) 발명의 명칭 **블록체인 기술을 활용한 포그 컴퓨터의 보안 및 디바이스 제어 방법**

(57) 요약

본 발명에 따르는 블록체인 기술을 활용한 포그 컴퓨터의 보안 및 디바이스 제어 방법은, 각기 다른 하나 이상의 디바이스와 연결된 다수의 포그 컴퓨터 각각이, 어느 한 디바이스와의 데이터 송수신 또는 제어가 발생되는지를 체크하는 단계; 상기 디바이스와의 데이터 송수신 또는 제어가 발생되면, 데이터 송수신 또는 제어 내역정보에 이전 내역정보를 나타내는 연결정보를 포함하는 트랜잭션 정보를 생성하여 브로드캐스팅하는 단계; 및 외부로부터 브로드캐스팅되어 트랜잭션 정보가 수신되면 블록체인방식의 저장소에 저장하는 단계;를 포함하는 것을 특징으로 한다.

대표도 - 도1



(52) CPC특허분류

H04L 9/06 (2013.01)

H04L 9/0844 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 20150001830031001

부처명 미래창조과학부

연구관리전문기관 정보통신기술진흥센터(IITP)

연구사업명 정보통신·방송 연구개발사업

연구과제명 초연결 자율형 IoT 서비스 지향 네트워크 인프라 기술 연구

기 여 율 1/1

주관기관 서강대학교 산학협력단

연구기간 2015.03.01 ~ 2018.02.28

명세서

청구범위

청구항 1

블록체인 기술을 활용한 포그 컴퓨터의 보안 및 디바이스 제어 방법에 있어서,

각기 다른 하나 이상의 디바이스와 연결된 다수의 포그 컴퓨터 각각이, 어느 한 디바이스와의 데이터 송수신 또는 제어가 발생되는지를 체크하는 단계;

상기 디바이스와의 데이터 송수신 또는 제어가 발생되면, 데이터 송수신 또는 제어 내역정보에 이전 내역정보를 나타내는 연결정보를 포함하는 트랜잭션 정보를 생성하여 브로드캐스팅하는 단계;

외부로부터 브로드캐스팅되어 트랜잭션 정보가 수신되면 블록체인방식의 저장소에 저장하는 단계;를 포함하는 것을 특징으로 하는 블록체인 기술을 활용한 포그 컴퓨터의 보안 및 디바이스 제어 방법.

청구항 2

제1항에 있어서,

상기 데이터 송수신 또는 제어 내역정보에 이전 내역정보를 나타내는 연결정보는 개인키로 암호화됨을 특징으로 하는 블록체인 기술을 활용한 포그 컴퓨터의 보안 및 디바이스 제어 방법.

청구항 3

제1항에 있어서,

상기 이전 내역정보를 나타내는 연결정보는 이전에 생성된 트랜잭션 정보에 포함된 내역정보를 해쉬 함수 처리하여 획득됨을 특징으로 하는 블록체인 기술을 활용한 포그 컴퓨터의 보안 및 디바이스 제어 방법.

청구항 4

제1항에 있어서,

상기 트랜잭션 정보에는 공용키가 부가되며,

상기 포그 컴퓨터는 외부로부터 브로드캐스팅되어 트랜잭션 정보가 수신되면 상기 공용키로 인증을 이행하고, 인증에 성공할 때에만 상기 트랜잭션 정보를 상기 블록체인방식의 저장소에 저장함을 특징으로 하는 블록체인 기술을 활용한 포그 컴퓨터의 보안 및 디바이스 제어 방법.

청구항 5

제1항에 있어서,

상기 다수의 포그 컴퓨터 중 어느 하나가 다운되면, 다운을 상기 다수의 포그 컴퓨터 중 나머지인 주변 포그 컴퓨터들로 통지하는 단계; 및

상기 주변 포그 단말기들 각각이 상기 블록체인방식의 저장소에 저장된 트랜잭션 정보와 클라우드 시스템으로 요청하여 제공받은 필요 데이터를 토대로 인접 포그 단말기 여부를 결정하고,

인접 포그 단말기로 결정된 포그 단말기가 상기 블록체인방식의 저장소에 저장된 트랜잭션 정보에 따라 상기 다운된 포그 컴퓨터에 연결된 디바이스를 검출하고, 검출된 디바이스에 연결하여 상기 디바이스와의 데이터 송수신 또는 제어를 이행하는 단계;를 더 구비함을 특징으로 하는 블록체인 기술을 활용한 포그 컴퓨터의 보안 및 디바이스 제어 방법.

청구항 6

제5항에 있어서,

상기 다운된 포그 단말기가 복구 기능을 브로드캐스팅하여 주변 포그 단말기들로 통지하는 단계;

상기 주변 포그 단말기들이 상기 다운된 포그 단말기의 복구 기능이 통지되면 복구 기능을 통지한 포그 컴퓨터에 연결되었던 디바이스에 대한 제어 및 데이터 송수신 내역을 기록한 트랜잭션 정보를 독출하여 전송하는 단계; 및

상기 복구 기능을 통지한 포그 컴퓨터가 상기 트랜잭션 정보와 클라우드 시스템으로 필요 데이터를 요청하여 제공받은 필요 데이터를 토대로 상기 디바이스에 연결하여 상기 디바이스와의 데이터 송수신 또는 제어를 이행하는 단계;를 더 구비함을 특징으로 하는 블록체인 기술을 활용한 포그 컴퓨터의 보안 및 디바이스 제어 방법.

발명의 설명

기술 분야

[0001] 본 발명은 포그 컴퓨팅 기술에 관한 것으로, 더욱 상세하게는 포그 컴퓨터들이 디바이스를 제어한 내역정보를 블록체인방식으로 가공하여 생성한 트랜잭션 정보들을 공유하여 사물 인터넷 네트워크 시스템의 안정성을 높일 수 있게 하는 블록체인 기술을 활용한 포그 컴퓨터의 보안 및 디바이스 제어 방법에 관한 것이다.

배경 기술

[0002] 최근 제안되고 있는 포그 컴퓨팅은 사물 인터넷의 수가 매우 많아짐에 따라 모든 데이터들을 클라우드 시스템에 저장하기가 곤란해지는 문제가 대두됨에 따라 등장하였다. 이러한 포그 컴퓨팅은 사물 인터넷으로부터 생성된 방대한 양의 데이터를 원격지에 위치하는 클라우드 시스템으로 전송하여 저장하지 않고, 인근에 위치하는 센서 또는 공유기와 같은 포그 컴퓨터에서 처리하여 필요한 것만 선별하여 클라우드 시스템으로 전송한다.

[0003] 그러나 상기한 포그 컴퓨터는 악의적 사용자에게 의한 공격에 의해 다운되는 것을 사전에 차단하거나, 포그 컴퓨터의 다운 또는 복구시의 처리 방식에 대해서는 논의가 이루어지지 않고 있다.

[0004] 종래 클라우드 시스템은 기본적으로 어니스트 벳 큐리어스 모델(honest but curious model)을 따른다. 이는 서비스 제공 및 데이터 관리, 연산 등의 업무는 정직하게 수행하지만, 필요한 경우에는 암호화된 데이터를 복호화하려는 시도가 있을 수 있는 반신뢰 모델(Semi-trust model) 모델이다. 다만 서비스 제공자가 제3의 기관에 클라우드 서비스를 위탁했을 때에는, 클라우드를 비신뢰모델(untrust model)로 정의할 수 있다.

[0005] 그리고 종래의 포그 컴퓨터의 경우에는 특정 사물 인터넷 기기를 고립시키거나 사물 인터넷 기기의 위치 정보를 활용하여 다양한 공격을 시도하기도 하였다. 이에 안전한 인증 기법으로 공격자가 악의적인 포그 컴퓨터를 사용할 수 없게 하는 것이 최선이지만, 인증에 성공하거나 포그 컴퓨터와 공격자가 공모한 경우에는 악의적인 공격을 피할 수 없는 문제가 있었다.

[0006] 이에 종래에는 포그 컴퓨터들이 관리하는 디바이스에 대한 제어정보의 보안을 제공함은 물론이며, 상기 포그 컴퓨터의 다운 또는 복구시에도 시스템 및 데이터가 안정적으로 동작할 수 있게 하는 기술의 개발이 절실하게 요망되었다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) 대한민국 특허등록 제1015740260000호
(특허문헌 0002) 대한민국 특허공개 제1020170004493호
(특허문헌 0003) 대한한국 특허등록 제10-1714306호

발명의 내용

해결하려는 과제

[0008] 본 발명은 포그 컴퓨터들이 디바이스를 제어한 내역정보를 블록체인방식으로 가공하여 생성한 트랜잭션 정보들을 공유 및 기록하여 사물 인터넷 네트워크 시스템의 안정성을 높일 수 있게 하는 블록체인 기술을 활용한 포그

컴퓨터의 보안 및 디바이스 제어 방법을 제공하는 것을 그 목적으로 한다.

[0009] 또한 본 발명의 다른 목적은 어느 한 포그 컴퓨터가 다운되면 다른 포그 컴퓨터가 공유 및 기록된 트랜잭션 정보들을 이용하여 다운된 포그 컴퓨터가 제어하던 디바이스들을 인근의 주변 포그 컴퓨터가 제어하게 하여 사물 인터넷 네트워크 시스템의 안정성을 높일 수 있게 하는 블록체인 기술을 활용한 포그 컴퓨터의 보안 및 디바이스 제어 방법을 제공하는 것이다.

[0010] 또한 본 발명의 또 다른 목적은 어느 한 포그 컴퓨터가 다운되었다가 복구되면, 복구된 포그 컴퓨터가 제어하던 디바이스에 대한 제어 내역정보를 인근의 주변 포그 컴퓨터로부터 제공받아 디바이스의 제어를 다시 개시할 수 있게 하여 사물 인터넷 네트워크 시스템의 안정성을 높일 수 있게 하는 블록체인 기술을 활용한 포그 컴퓨터의 보안 및 디바이스 제어 방법을 제공하는 것이다.

과제의 해결 수단

[0011] 상기한 목적을 달성하기 위한 본 발명에 따르는 블록체인 기술을 활용한 포그 컴퓨터의 보안 및 디바이스 제어 방법은, 각기 다른 하나 이상의 디바이스와 연결된 다수의 포그 컴퓨터 각각이, 어느 한 디바이스와의 데이터 송수신 또는 제어가 발생하는지를 체크하는 단계; 상기 디바이스와의 데이터 송수신 또는 제어가 발생되면, 데이터 송수신 또는 제어 내역정보에 이전 내역정보를 나타내는 연결정보를 포함하는 트랜잭션 정보를 생성하여 브로드캐스팅하는 단계; 및 외부로부터 브로드캐스팅되어 트랜잭션 정보가 수신되면 블록체인방식의 저장소에 저장하는 단계;를 포함하는 것을 특징으로 한다.

발명의 효과

[0012] 본 발명은 포그 컴퓨터들이 디바이스를 제어한 내역정보를 블록체인방식으로 가공하여 생성한 트랜잭션 정보들을 공유 및 기록하여 사물 인터넷 네트워크 시스템의 안정성을 높일 수 있는 효과를 야기한다.

[0013] 또한 본 발명은 어느 한 포그 컴퓨터가 다운되면 다른 포그 컴퓨터가 공유 및 기록된 트랜잭션 정보들을 이용하여 다운된 포그 컴퓨터가 제어하던 디바이스들을 인근의 주변 포그 컴퓨터가 제어하게 하여 사물 인터넷 네트워크 시스템의 안정성을 높일 수 있는 효과를 야기한다.

[0014] 또한 본 발명은 어느 한 포그 컴퓨터가 다운되었다가 복구되면, 복구된 포그 컴퓨터가 제어하던 디바이스에 대한 제어 내역정보를 인근의 주변 포그 컴퓨터로부터 제공받아 디바이스의 제어를 다시 개시할 수 있게 하여 사물 인터넷 네트워크 시스템의 안정성을 높일 수 있는 효과를 야기한다.

[0015]

도면의 간단한 설명

[0016] 도 1은 본 발명의 바람직한 실시예에 따르는 사물 인터넷 네트워크 시스템의 구성도.

도 2 내지 도 4는 본 발명의 바람직한 실시예에 따르는 블록체인 기술을 활용한 포그 컴퓨터의 보안 및 디바이스 제어 방법의 절차도.

도 5는 본 발명의 바람직한 실시예에 따르는 트랜잭션 정보의 구조를 도시한 도면.

발명을 실시하기 위한 구체적인 내용

[0017] 본 발명은 포그 컴퓨터들이 디바이스를 제어한 내역정보를 블록체인방식으로 가공하여 생성한 트랜잭션 정보들을 공유 및 기록하여 사물 인터넷 네트워크 시스템의 안정성을 높일 수 있다.

[0018] 좀더 설명하면, 본 발명은 하나의 클라우드 시스템과 연결된 여러 개의 포그 컴퓨터 사이의 인증 절차 또는 포그 노드에 연결된 다양한 사물 인터넷 기기에 대한 인증 절차를 블록체인기술에서 사용하는 해쉬(HASH) 함수 및 PKI(Public Key Infrastructure) 인증 방법을 사용하여, 자기인증(Authentication), 자기부인방지(non-repudiation), 무결성(integrity)을 보장하여, 악의적 사용자의 침입을 효율적으로 제한할 수 있다. 또한 포그 컴퓨터들 각각이 다른 포그 컴퓨터들의 공용키(Public key)를 가지고, 암호화되어 보내진 각 포그 컴퓨터들의 제어 내역정보를 트랜잭션 정보로 가공하여 공유 및 기록함으로써, 상기 포그 컴퓨터들의 트랜잭션 정보의 변조를 불가하게 하여 모든 포그 컴퓨터들이 서로를 신뢰할 수 있게 한다.

[0019] 또한 본 발명은 어느 한 포그 컴퓨터가 다운되면 다른 포그 컴퓨터가 공유 및 기록된 트랜잭션 정보들을 이용하여

여 다운된 포그 컴퓨터가 제어하던 디바이스들을 인근의 주변 포그 컴퓨터가 제어하게 하여 사물 인터넷 네트워크 시스템의 안정성을 높일 수 있다.

[0020] 또한 본 발명은 어느 한 포그 컴퓨터가 다운되었다가 복구되면, 복구된 포그 컴퓨터가 제어하던 디바이스에 대한 제어 내역정보를 인근의 주변 포그 컴퓨터로부터 제공받아 디바이스의 제어를 다시 개시할 수 있게 하므로, 보다 쉽고 빠르게 정상 상태로 복구될 수 있게 한다.

[0021] 이러한 본 발명의 바람직한 실시예에 따르는 블록체인 기술을 활용한 포그 컴퓨터의 보안 및 디바이스 제어 방법을 도면을 참조하여 상세히 설명한다.

[0022] <사물 인터넷 시스템>

[0023] 도 1은 본 발명의 바람직한 실시예에 따르는 사물 인터넷 시스템의 구성을 도시한 것이다.

[0024] 상기 사물 인터넷 시스템은 크게 클라우드 컴퓨팅 환경과 포그 컴퓨팅 환경과 사물 인터넷 기기들로 나눌 수 있다.

[0025] 상기 클라우드 컴퓨팅 환경에는 클라우드 시스템(100)이 위치하고, 상기 포그 컴퓨팅 환경에는 제1 내지 제N포그 컴퓨터(2001~200N)가 위치하고, 상기 사물 인터넷 기기들로는 다수의 디바이스(3001~3006)가 위치한다.

[0026] 상기 제1 내지 제N포그 컴퓨터(2001~200N) 각각은 자신과 연결된 다수의 디바이스(3001~3006)로부터 각종 데이터를 제공받아 저장하였다가 클라우드 시스템(100)으로 업로드할 데이터를 선별하고, 선택된 데이터만을 상기 클라우드 시스템(100)으로 업로드한다. 또한 상기 제1 내지 제N포그 컴퓨터(2001~200N)는 상기 클라우드 시스템(100)으로부터 다수의 디바이스(3001~3006) 중 선택된 디바이스로 다운로드할 데이터를 제공받아 해당 기기로 제공하거나 상기 클라우드 시스템(100)으로부터의 제어명령을 선택된 디바이스로 제공하여 디바이스를 제어할 수도 있다.

[0027] 또한 제1 내지 제N포그 컴퓨터(2001~200N) 각각은 자신과 연결되어 있는 사물 인터넷 기기들(3001~3006)로부터 데이터를 제공받거나 사물 인터넷 기기들(3001~3006)로 제공한 데이터, 제어명령에 대한 내역정보들(이하, 내역정보라 칭함)을 트랜잭션 정보로 가공하여 주변 포그 컴퓨터(2001~200N)와 브로드캐스팅하여 전송하여 공유함과 아울러 기록한다.

[0028] 여기서, 상기 트랜잭션 정보는 도 5에 도시한 바와 같이 트랜잭션 정보가 연쇄적으로 순차 저장된다. 상기 트랜잭션 정보는 트랜잭션과 공용키 정보로 구성되며, 상기 트랜잭션은 내역정보와 이전 내역정보를 해쉬함수 처리하여 생성한 연결정보를 개별키로 암호화한 것이다.

[0029] 또한 제1 내지 제N포그 컴퓨터(2001~200N) 각각은 다른 포그 컴퓨터로부터 트랜잭션 정보가 제공되면, 공용키를 통해 상기 트랜잭션 정보를 검증하고, 상기 검증에 성공하면 상기 트랜잭션 정보에 포함되어 있는 정보인, 해쉬함수를 통해 암호화된 이전 트랜잭션의 일부가 자신이 저장하고 있는 이전 트랜잭션의 일부와 동일한지 여부를 통해 해당 트랜잭션이 유효한지를 판별한다. 상기 트랜잭션이 유효하면 블록체인형태의 트랜잭션 정보 저장소에 상기 트랜잭션 정보를 부가하여 저장한다.

[0030] 또한 제1 내지 제N포그 컴퓨터(2001~200N) 각각은 상기 블록체인형태의 트랜잭션 정보 저장소에 저장된 트랜잭션 정보들을 이용하여, 어느 한 포그 컴퓨터가 다운되면 인접한 포그 컴퓨터가 다운된 포그 컴퓨터에 연결되었던 디바이스에 연결하여 데이터 송수신 및 제어를 대행한다.

[0031] 또한 제1 내지 제N포그 컴퓨터(2001~200N) 각각은 상기 블록체인정보에 저장된 트랜잭션들을 이용하여, 다운되었던 어느 한 포그 컴퓨터가 복구하면 인근 포그 컴퓨터들이 자신의 블록체인형태의 트랜잭션 정보 저장소에 저장된 트랜잭션 정보들을 독출하여 해당 포그 컴퓨터에 제공함으로써 해당 포그 컴퓨터의 데이터 복구를 빠르고 정확하게 이행할 수 있게 한다.

[0032] <블록체인 기술을 이용한 포그 컴퓨터 제어 방법>

[0033] 이러한 본 발명에 따르는 사물 인터넷 시스템에 적용 가능한 블록체인 기술을 이용한 포그 컴퓨터 제어 방법을 도면을 참조하여 설명한다.

[0034] <포그 컴퓨터 사이의 데이터 공유 과정>

[0035] 도 2는 본 발명의 바람직한 실시예에 따라 포그 컴퓨터 사이의 데이터 공유 과정을 도시한 것이다.

[0036] 상기 도 2를 참조하면, 상기 제1 내지 제N포그 컴퓨터(2001~200N) 각각은 자신과 연결되어 있는 디바이스에 대

해 제어 또는 데이터 송수신이 발생하는지를 체크한다(400단계).

- [0037] 상기 자신과 연결되어 있는 디바이스에 대한 제어 또는 데이터 송수신이 발생하면, 제1 내지 제N포그 컴퓨터(2001~200N) 각각은 다른 포그 컴퓨터로부터 브로드캐스팅되어 제공된 트랜잭션 정보가 존재하는지를 체크한다(402단계).
- [0038] 상기 트랜잭션 정보가 존재하면, 상기 제1 내지 제N포그 컴퓨터(2001~200N) 각각은 수신된 트랜잭션 정보에 포함된 공용키로 해당 트랜잭션 정보를 인증하고(404단계), 상기 트랜잭션 정보의 인증이 성공하면(406단계), 상기 제1 내지 제N포그 컴퓨터(2001~200N) 각각은 상기 수신된 트랜잭션 정보를 블록체인형태의 트랜잭션 정보 저장소에 부가하여 저장한다(408단계).
- [0039] 상기한 트랜잭션 정보가 공용키를 이용한 인증에 성공하지 않으면(406단계), 상기 제1 내지 제N포그 컴퓨터(2001~200N) 각각은 상기 수신된 트랜잭션 정보를 파기한다(414단계).
- [0040] 상기 수신된 트랜잭션 정보에 대한 처리가 완료되었거나(404~408, 414단계), 수신된 트랜잭션 정보가 없다면(402단계), 상기 제1 내지 제N포그 컴퓨터(2001~200N) 각각은 최신의 디바이스 제어 또는 데이터 송수신 내역정보와 트랜잭션 정보에 기록된 이전 내역정보를 해쉬 함수 처리하여 생성한 연결정보를 개인키로 암호화하여 트랜잭션을 생성하고, 상기 트랜잭션에 공용키정보를 부가하여 새로운 트랜잭션 정보를 생성한다(410단계). 여기서, 이전내역정보를 해쉬(HASH) 함수로 묶은 이유는 HASH 함수는 단방향 함수(one-way function)으로써 역연산이 불가능하기 때문에 이전내역정보의 조작 또는 변조를 불가능하게 할 수 있기 때문이다.
- [0041] 상기 새로운 트랜잭션 정보가 생성되면, 상기 제1 내지 제N포그 컴퓨터(2001~200N) 각각은 상기 새로운 트랜잭션 정보를 다른 포그 컴퓨터들로 브로드캐스팅하여 공유하고 기록하게 한다(412단계).
- [0042] <다운된 포그 컴퓨터에 대한 처리 과정>
- [0043] 그리고 본 발명의 바람직한 실시예에 따라 다운된 포그 컴퓨터에 대한 처리 과정을 도 3을 참조하여 설명한다.
- [0044] 상기 제1 내지 제N포그 컴퓨터(2001~200N) 중 어느 하나는 외부의 공격 또는 장치의 고장 등 다양한 이유로 다운될 수 있다. 이와 같이 어느 한 포그 컴퓨터가 다운되면, 그 다운된 포그 컴퓨터는 주변의 포그 컴퓨터들로 자신의 다운상태를 통지한다(500, 502단계). 좀 더 설명하면, 다운되는 포그 컴퓨터는 자신에게 문제가 생기면 연결되어 있는 디바이스들과의 연결을 끊고, 주변의 포그 컴퓨터들에게 다운 통지 메시지를 브로드캐스팅한다. 상기 다운 통지 메시지에는 포그 컴퓨터 자신의 식별정보 및 다운 요인 식별정보를 포함한다.
- [0045] 상기 주변의 포그 컴퓨터들은 어느 한 포그 컴퓨터로부터 다운이 통지되면, 상기 다운 통지된 포그 컴퓨터에 대한 다운 요인을 분석하여, 데이터가 모두 삭제된 상태인 것인지, 혹은 데이터는 모두 살아 있지만 통신간에 문제가 있어서 일정 기간만의 데이터 복구가 필요한 것인지, 혹은 해킹으로부터의 다운이 되어서 추가적인 보완이 필요한 상태인 것인지를 체크한다(506단계). 이는 다운되는 포그 컴퓨터가 제공하는 다운 통지 메시지에 포함된 다운 요인 식별정보에 기록된다. 이는 해당 포그 컴퓨터가 복구될 때에 신속하게 대응하기 위함이다.
- [0046] 상기 주변 포그 컴퓨터들 각각은 다운된 포그 컴퓨터에 연결된 디바이스가 하나 이상 존재하고 자신이 가장 인접한 포그 컴퓨터인지를 체크한다(508단계). 여기서 상기 인접한 포그 컴퓨터 여부는 포그 컴퓨터들 사이의 메시지 응답 및 속도에 관한 레이턴시(latency) 혹은 IP 주소의 비교를 통해 같은 서브넷 마스크 네트워크(subnet mask network)안에 있는지 여부를 통해 판별될 수 있다.
- [0047] 상기 다운된 포그 컴퓨터에 연결된 디바이스 하나이상 존재하고, 자신이 가장 인접한 포그 컴퓨터이면, 해당 포그 컴퓨터는 다운 통지된 포그 컴퓨터로부터 제공받아 저장해둔 트랜잭션 정보들을 독출하고(510단계), 다운 통지된 포그 컴퓨터의 역할 대행을 위한 필요정보를 클라우드 시스템(100)으로 요청하여 제공받는다(512, 514단계). 여기서 상기 필요정보는 데이터, 타임 스탬프, 데이터 전송 및 저장 기록 등으로 구성될 수 있다.
- [0048] 이후 상기 포그 컴퓨터는 다운 통지된 포그 컴퓨터에 연결된 디바이스와 연결을 허용하고, 상기 필요정보를 토대로 상기 디바이스에 대한 제어 및 데이터 송수신을 이행한다(516단계).
- [0049] 상기 디바이스에 대한 제어 및 데이터 송수신이 이행되면, 상기 포그 컴퓨터는 상기 디바이스에 대한 제어 및 데이터 송수신 내역정보와 이전 내역정보를 해쉬 함수로 처리하여 생성한 연결정보를 개인키로 암호화하여 트랜잭션으로 가공하고, 상기 트랜잭션에 공용키를 부가하여 트랜잭션 정보를 생성하고, 상기 트랜잭션 정보를 주변 포그 컴퓨터들로 브로드캐스팅하여 전달한다(518단계).

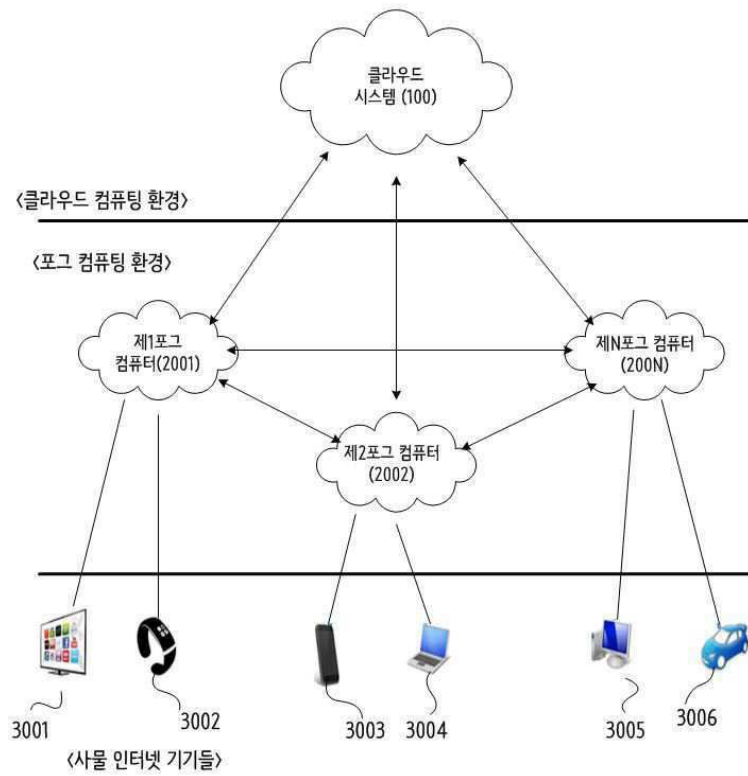
- [0050] 상기한 바와 달리 상기 주변의 포그 컴퓨터들은 상기 다운된 포그 컴퓨터에 연결된 디바이스가 없거나, 자신이 가장 인접한 포그 컴퓨터가 아니면, 상기의 프로세스를 종료한다.
- [0051] <다운되었다가 복구된 포그 컴퓨터에 대한 처리 과정>
- [0052] 그리고 본 발명의 바람직한 실시예에 따라 다운되었다가 복구된 포그 컴퓨터에 대한 처리 과정을 도 4를 참조하여 설명한다.
- [0053] 상기 제1 내지 제N포그 컴퓨터(2001~200N) 중 다운되었다가 복구된 어느 한 포그 컴퓨터는 리부팅 등을 이유로 복구 가능 상태가 도래할 수 있다.
- [0054] 상기 다운되었다가 복구된 어느 한 포그 컴퓨터는 복구 가능 상태가 도래하면(600단계), 복구가능 통지 메시지를 주변 포그 컴퓨터들로 브로드캐스팅하여 전달한다(602단계).
- [0055] 상기 주변 포그 컴퓨터들은 복구가능 통지 메시지를 송신한 포그 컴퓨터에 연결되었던 디바이스에 대한 제어 및 데이터 송수신 내역을 기록한 트랜잭션 정보를 복구가능 통지한 포그 컴퓨터로 전송한다(606,608단계).
- [0056] 상기 복구가능 통지 메시지를 송신한 포그 컴퓨터에 연결되었던 디바이스에 대한 제어 및 데이터 송수신 내역을 기록한 트랜잭션 정보가 제공되면, 해당 포그 컴퓨터는 상기 트랜잭션 정보를 저장함과 아울러 그 트랜잭션 정보를 분석하여 이전에 연결되었던 디바이스가 존재하였는지를 판단한다(610,612단계).
- [0057] 상기 이전에 연결되었던 디바이스가 존재하였다면, 상기 포그 컴퓨터는 클라우드 시스템으로 디바이스 제어를 위한 필요 데이터를 요청하는 필요 데이터 요청 메시지를 전송한다(614단계). 여기서, 상기 필요 데이터 요청 메시지에는 포그 컴퓨터 식별정보, 디바이스 식별정보, 필요 정보 식별정보를 포함한다.
- [0058] 이후 상기 클라우드 시스템(100)이 포그 컴퓨터가 제공한 필요 데이터 요청 메시지에 따라 해당 디바이스 제어를 위한 필요 데이터를 해당 포그 컴퓨터로 다운로드한다(616단계).
- [0059] 상기 포그 컴퓨터는 해당 디바이스 제어를 위한 필요 데이터가 클라우드 시스템(100)으로부터 제공되면, 해당 디바이스와 연결하여 제어를 개시한다(618단계). 이후 상기 포그 컴퓨터는 해당 디바이스에 대한 제어 내역정보를 트랜잭션으로 가공하여 주변 포그 컴퓨터들로 브로드캐스팅하여 공유한다(620단계).
- [0060] 이러한 본 발명의 동작을 예로 들어 설명한다.
- [0061] 사물 인터넷 디바이스인 신호등 장치로부터 센싱정보를 제공받음과 아울러 상기 센싱정보에 따라 상기 신호등 장치를 제어하는 포그 컴퓨터가 존재하고, 그 포그 컴퓨터의 인근에 사물 인터넷 디바이스인 차량 장치로부터 센싱정보를 제공받음과 아울러 상기 센싱정보에 따라 상기 차량 장치를 제어하는 포그 컴퓨터가 존재할 때에, 상기 두 포그 컴퓨터는 상기 사물 인터넷 시스템과 제어 및 데이터 송수신 내역을 블록체인방식으로 공유하여 기록함과 아울러, 일부 정보는 추출하여 클라우드 시스템에 업로드하여 기록한다.
- [0062] 이러한 상태에서 차량 장치를 제어하는 포그 컴퓨터가 다운되면, 상기 신호등 장치를 제어하는 포그 컴퓨터가 블록체인방식으로 기록해둔 제어 및 데이터 송수신 내역과 클라우드 시스템에 기록된 정보를 토대로, 상기 차량 장치와 연결하여 상기 차량 장치의 제어 및 데이터 송수신을 대행한다.
- [0063] 또한 상기 다운되었던 포그 컴퓨터가 복구하면, 상기 신호등 장치를 제어하는 포그 컴퓨터가 상기 차량 장치의 제어 및 데이터 송수신 내역을 상기 복구한 포그 컴퓨터로 제공하여, 상기 복구한 포그 컴퓨터를 신속하고 안전하게 복구할 수 있게 한다.

부호의 설명

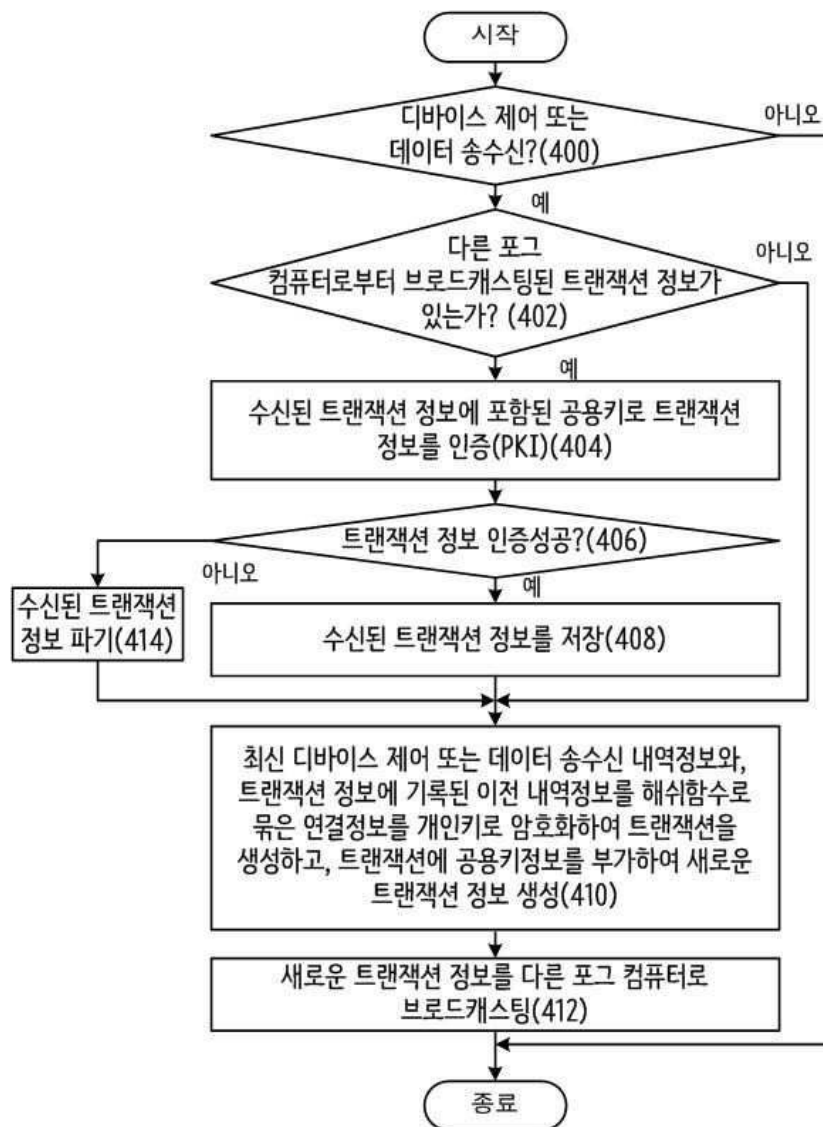
- [0064] 100 : 클라우드 시스템
- 2001~200N : 제1 내지 제N포그 컴퓨터
- 3001~3006 : 사물 인터넷 디바이스들

도면

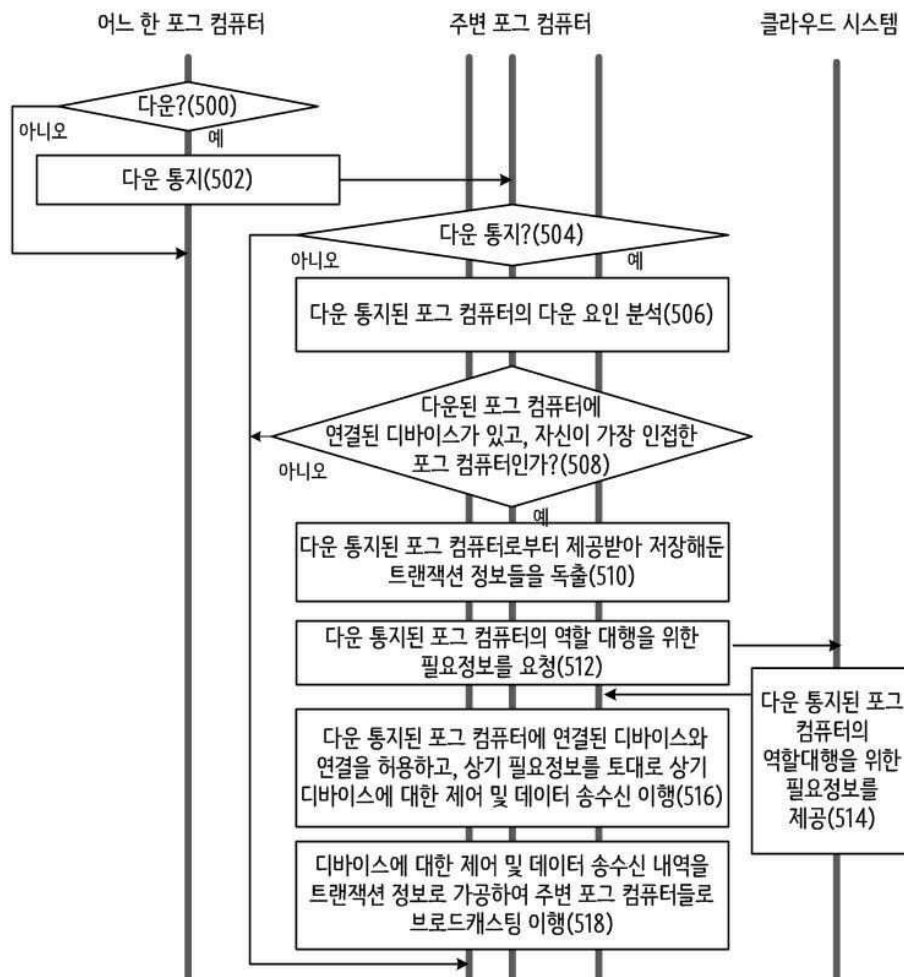
도면1



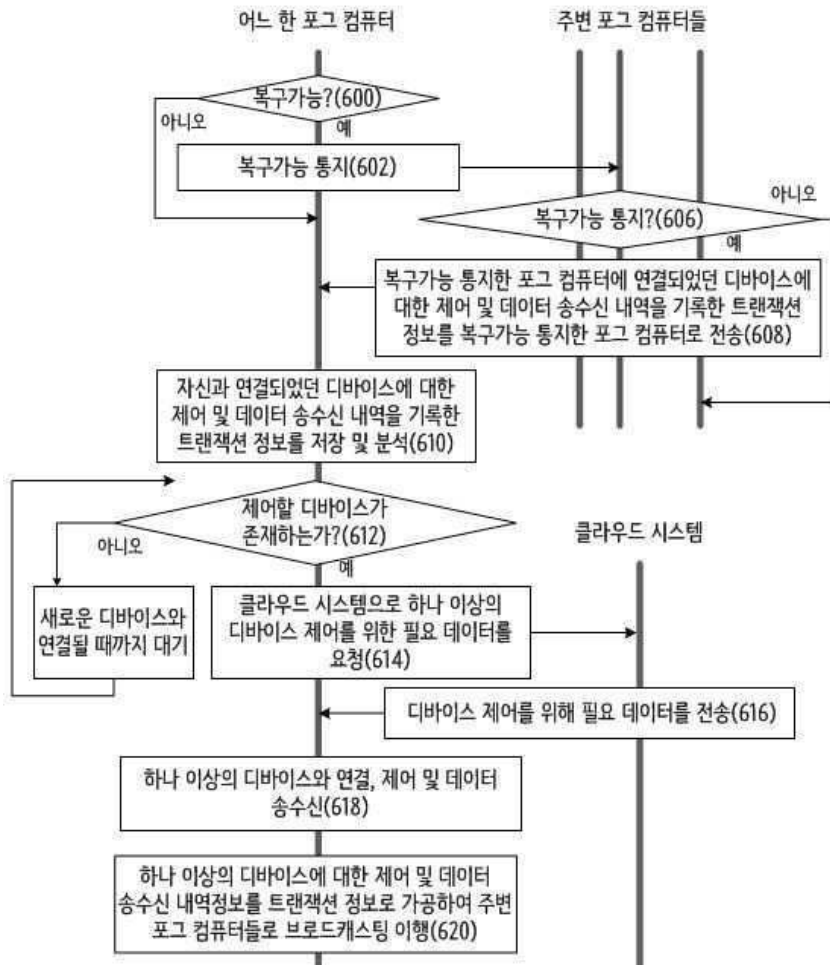
도면2



도면3



도면4



도면5

〈블록체인형태의 트랜잭션 정보 저장소에 저장되는 트랜잭션 정보들〉

