



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년11월30일
(11) 등록번호 10-1923424
(24) 등록일자 2018년11월23일

(51) 국제특허분류(Int. Cl.)

H04W 12/02 (2009.01) H04W 12/04 (2009.01)

H04W 12/10 (2009.01) H04W 88/18 (2009.01)

(52) CPC특허분류

H04W 12/02 (2013.01)

H04W 12/04 (2013.01)

(21) 출원번호 10-2017-0152835

(22) 출원일자 2017년11월16일

심사청구일자 2017년11월16일

(56) 선행기술조사문헌

KR100861332 B1*

KR1020050000772 A*

*는 심사관에 의하여 인용된 문헌

(73) 특허권자

명지대학교 산학협력단

경기도 용인시 처인구 명지로 116 (남동, 명지대학교)

(72) 발명자

신민호

경기도 화성시 동탄숲속로 103, 809동 1501호(능동, 동탄숲속마을자연환경남아너스빌아파트)

염대현

경기도 용인시 기흥구 동백7로 96, 2313동 1403호(동백동, 백현마을한라비발디)

이수정

경기도 화성시 동탄대로시범길 192, 1005동 601호(청계동, 시범예미지아파트)

(74) 대리인

이은철, 이우영

전체 청구항 수 : 총 8 항

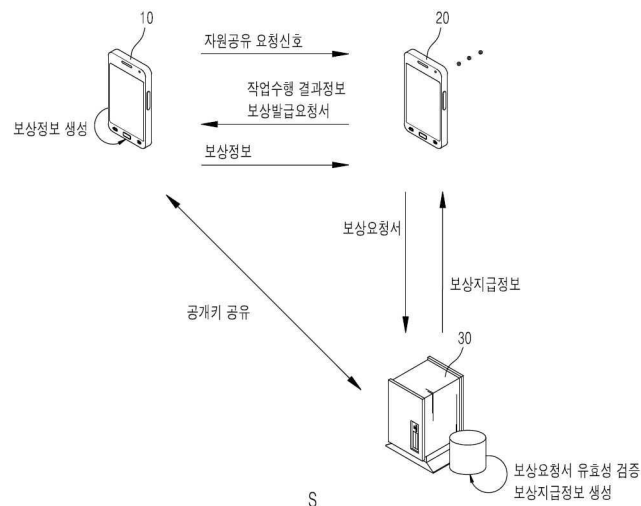
심사관 : 이준석

(54) 발명의 명칭 프라이버시를 보장하는 자원 공유 제어 시스템 및 그 방법

(57) 요약

본 발명은 프라이버시를 보장하는 자원 공유 제어 시스템 및 방법에 관한 것으로서, 자원요청 디바이스가 다수의 디바이스로 자원공유 요청신호를 전송하는 (a) 단계; 자원대여 디바이스가 자원공유 요청신호와 대응하는 프로세스를 수행하여 생성한 작업수행 결과정보 및 보상발급요청서를 자원요청 디바이스로 전송하는 (b) 단계; 자원요청 디바이스가 블라인드 서명을 통해 생성한 보상정보를 자원대여 디바이스로 전송하는 (c) 단계; 자원대여 디바이스가 수신한 보상정보를 토대로 생성한 보상요청서를 보상서버로 전송하는 (d) 단계; 보상서버가 공개키, 인증서 및 시리얼을 통해 보상요청서의 유효성을 검증하는 (e) 단계; 및 보상서버가 보상정보를 사용이 가능하도록 갱신한 보상지급정보를 자원대여 디바이스로 전송하는 (f) 단계;를 포함한다.

대표도 - 도3



(52) CPC특허분류

H04W 12/10 (2013.01)

H04W 88/18 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 20130004050032005

부처명 미래창조과학부

연구관리전문기관 정보통신기술진흥센터

연구사업명 방송통신기술개발사업_원천기술개발사업

연구과제명 단말 협업형 GIGA급 스마트 클라우드넷 핵심 기술 개발

기 여 율 1/1

주관기관 한국과학기술원

연구기간 2013.04.01 ~ 2018.02.28

명세서

청구범위

청구항 1

삭제

청구항 2

삭제

청구항 3

삭제

청구항 4

자원 공유 제어 시스템에 있어서,

자원대여 디바이스로부터 자원요청 디바이스 식별자와 보상요청서를 수신하고,

인증서 및 시리얼을 통해 상기 보상요청서의 유효성을 검증하며,

유효성이 검증된 보상지급정보를 상기 자원대여 디바이스로 전송하는 보상서버;를 포함하는 것을 특징으로 하는 프라이버시를 보장하는 자원 공유 제어 시스템.

청구항 5

제4항에 있어서,

상기 유효성 검증은,

상기 보상요청서의 중복여부를 확인하는 절차인 것을 포함하는 프라이버시를 보장하는 자원 공유 제어 시스템.

청구항 6

제4항에 있어서,

상기 보상서버는,

상기 보상요청서의 유효성 검증을 위해 자원요청 디바이스의 공개키를 관리하는 것을 특징으로 하는 프라이버시를 보장하는 자원 공유 제어 시스템.

청구항 7

자원 공유 제어 시스템에 있어서,

다수의 자원대여 디바이스로 자원공유 요청신호를 전송하고, 상기 자원공유 요청신호에 대응하는 작업수행 결과 정보와 이에 상응하는 보상발급요청서를 상기 자원대여 디바이스로부터 수신하며, 상기 보상발급요청서를 블라인드 서명하여 생성한 보상정보를 자원대여 디바이스로 전송하는 자원요청 디바이스;

상기 자원요청 디바이스로부터 자원요청 신호를 수신하여 상기 자원공유 요청신호와 대응하는 작업을 수행하고, 상기 작업 수행에 따라 생성한 작업수행 결과정보와 이에 상응하는 보상발급요청서를 상기 자원요청 디바이스로 전송하여 블라인드 서명된 보상정보를 수신하며, 수신한 보상정보를 토대로 생성한 보상요청서를 보상서버로 전송하여 유효성을 검증받은 보상지급정보를 수신하는 자원대여 디바이스; 및

상기 자원대여 디바이스로부터 자원요청 디바이스 식별자와 보상요청서를 수신하고, 인증서 및 시리얼을 통해 상기 보상요청서의 유효성을 검증하며, 유효성이 검증된 보상지급정보를 상기 자원대여 디바이스로 전송하는 보상서버;를 포함하는 것을 특징으로 하는 프라이버시를 보장하는 자원 공유 제어 시스템.

청구항 8

제7항에 있어서,

상기 보상발급요청서는,

기 설정된 금액(정액) 단위로 발행되는 것을 특징으로 하는 프라이버시를 보장하는 자원 공유 제어 시스템.

청구항 9

자원 공유 제어 방법에 있어서,

(a) 자원요청 디바이스가 다수의 디바이스로 자원공유 요청신호를 전송하는 단계;

(b) 자원대여 디바이스가 자원공유 요청신호에 대응하는 프로세스를 수행하여 생성한 작업수행 결과정보 및 보상발급요청서를 자원요청 디바이스로 전송하는 단계;

(c) 자원요청 디바이스가 블라인드 서명을 통해 생성한 보상정보를 자원대여 디바이스로 전송하는 단계;

(d) 자원대여 디바이스가 수신한 보상정보를 토대로 생성한 보상지급요청서를 보상서버로 전송하는 단계;

(e) 보상서버가 공개키, 인증서 및 시리얼을 통해 보상지급요청서의 유효성을 검증하는 단계; 및

(f) 보상서버가 보상지급정보를 자원대여 디바이스로 전송하는 단계;를 포함하는 것을 특징으로 하는 프라이버시를 보장하는 자원 공유 제어 방법.

청구항 10

제9항에 있어서,

상기 (b) 단계는,

(b-1) 자원대여 디바이스가 자원요청 디바이스로부터 수신한 자원공유 요청신호를 수락하여 생성한 자원공유 응답신호를 자원요청 디바이스로 전송하는 단계;

(b-2) 자원요청 디바이스가 수신한 자원공유 응답신호를 보낸 자원대여 디바이스로 작업량을 분배하는 단계;

(b-3) 자원대여 디바이스가 할당받은 작업량과 대응하는 프로세스를 수행하여 작업수행 결과정보를 생성하는 단계; 및

(b-4) 자원대여 디바이스가 생성한 작업수행 결과정보 및 보상발급요청서를 자원요청 디바이스로 전송하는 단계;를 포함하는 것을 특징으로 하는 프라이버시를 보장하는 자원 공유 제어 방법.

청구항 11

제9항에 있어서,

상기 (c) 단계는,

(c-1) 자원요청 디바이스가 자원대여 디바이스들로부터 수신한 작업수행 결과정보를 취합하는 단계;

(c-2) 자원요청 디바이스가 자원요청 디바이스 식별자, 보상서버 식별자 및 보상발급요청서에 대한 블라인드 서명값을 포함하는 보상정보를 생성하는 단계; 및

(c-3) 자원요청 디바이스가 보상정보를 자원대여 디바이스로 전송하는 단계;를 포함하는 것을 특징으로 하는 프라이버시를 보장하는 자원 공유 제어 방법.

발명의 설명

기술 분야

[0001]

본 발명은 프라이버시를 보장하는 자원 공유 제어 시스템 및 그 방법에 관한 것으로 더욱 상세하게는, 자원요청 디바이스의 요청에 대응하는 작업을 수행한 자원대여 디바이스로 보상을 지급하되, 보상과정에서 어떤 작업에 대한 보상인지에 관한 정보의 누출을 차단함으로써, 작업대여 디바이스의 프라이버시를 보호하는 기술에 관한

것이다.

[0002] 본 발명은 자원요청 디바이스는 자원대여 디바이스의 보상발급요청에 따라 블라인드 서명된 보상정보를 자원대여 디바이스에게 발급하고, 자원대여 디바이스로부터 보상금 지급을 요청받은 보상서버가 유효성 검증을 통해 자원대여 디바이스로 보상을 지급함에 있어서 특정 작업에 따른 보상이 중복으로 지급되는 것을 방지하는 기술에 관한 것이다.

[0003] 그리고, 본 발명은 특정 자원대여 디바이스가 서로 다른 시점에 또는 동시에 보상서버에게 제출한 복수의 보상지급요청이 갖는 상호 연관성을 알 수 없도록 함으로서, 자원대여 디바이스의 프라이버시를 원천적으로 보호하는 기술에 관한 것이다.

배경 기술

[0004] 도 1은 일반적인 무선 네트워크 시스템에 있어서, 자원공유 흐름이 간략하게 도시된 개요도이다. 도 1에 도시된 바와 같이 네트워크 내에 있는 각 노드들은 직접적인 인터넷과 접속이 불가능한 경우라도 접속 가능한 다른 노드의 중계 서비스를 통해 간접적으로 인터넷 접속이 가능하게 된다.

[0005] 이러한 중계서비스를 위해서는 각 중계 노드들은 자신의 네트워크 대역폭(bandwidth)나 메모리 등의 자원을 제공해야 한다. 이와 같이 자원 공유가 가능한 무선 네트워크는 노드 장애(node failure)나 링크 장애(link failure)가 발생시 다른 경로를 찾아 접속을 유지할 수 있어 장애에 능동적으로 대처할 수 있다.

[0006] 또한, 인접한 노드들의 자원을 사용할 수 있기 때문에 각 노드 자체의 자원 환경에 제한되지 않는 네트워크 서비스를 제공할 수 있다.

[0007] 이러한 자원공유서비스는 P2P파일 공유 서비스에서 이미 구현되고 있다. 그러나, 구현된 기존 P2P 형태의 서비스는 자원 공유를 약속했던 각 노드들이 자원공유에 지속적으로 참여하고 있는지 또는 네트워크 운영을 위해 자원을 많이 제공하는 노드들에 대한 보상이 제대로 제공되고 있는지에 대한 구체적인 방법이 존재하지 않았다.

[0008] 따라서, 자기의 자원은 제공하지 않으면서 노드들 간 자원 공유를 통해 이루어지는 서비스는 사용하는 freeriding이 발생하는 문제가 있다.

[0009] 한편, 도 2를 참조하여 선행특허에 대해 살펴보면, 인접한 노드에 자원을 제공하면 제공한 자원의 양적 정보를 나타내는 신용(credit)을 생성하여 네트워크상에 브로드캐스팅(broadcasting)하는 제 1노드; 및 제 1노드로부터 받은 자원에 대한 정보를 나타내는 보상(reward)을 생성하여 네트워크상에 브로드캐스팅 하는 제 2노드;를 포함하여 보상 데이터를 통해 제 1노드의 신용정보가 유효한지 검증하고, 그에 따라 사용가능한 네트워크 자원을 제 1노드에 할당하도록 구성된다.

[0010] 그러나, 선행특허를 포함하는 종래의 자원 공유 시스템의 경우, 작업을 수행한 제 1노드의 디바이스 능력(CPU, 메모리, 센서 또는 에너지), 작업 기록, 위치기록 및 작업 수행에 따른 보상(금전 또는 포인트)을 지급받기 위한 개인정보를 제 2노드로 전송하는 구조를 갖는다.

선행기술문헌

특허문헌

[0011] (특허문헌 0001) 한국공개특허 제2008-0079791호

발명의 내용

해결하려는 과제

[0012] 본 발명의 목적은, 자원요청 디바이스의 요청에 대응하는 작업을 수행한 자원대여 디바이스로 보상을 지급하되, 보상과정에서 어떤 작업에 대한 보상인지를 노출하지 않도록 함으로써, 작업대여 디바이스의 프라이버시를 보호하는데 그 목적이 있다.

[0013] 또한, 본 발명의 목적은, 자원요청 디바이스가 자원 활용에 따른 보상정보를 블라인드 서명 형태로 자원대여 디바이스에게 발급하고, 보상서버는 유효성 검증을 통해 자원대여 디바이스로 보상지급정보를 전달할 때 보상이

중복으로 지급되는 것을 방지하는데 그 목적이 있다.

[0014] 본 발명은 특정 자원대여 디바이스가 서로 다른 시점에 또는 동시에 보상서버에게 제출한 복수의 보상지급요청이 갖는 상호 연관성을 알 수 없도록 함으로서, 자원대여 디바이스의 프라이버시를 원천적으로 보호하는데 목적이 있다.

과제의 해결 수단

[0015] 이러한 기술적 과제를 달성하기 위한 본 발명의 제1 실시예에 따른 자원 공유 제어 시스템은, 다수의 자원대여 디바이스로 자원공유 요청신호를 전송하고, 자원공유 요청신호에 대응하는 작업수행 결과정보와 이에 상응하는 보상발급요청서를 상기 자원대여 디바이스로부터 수신하여, 상기 보상발급요청서에 블라인드 서명을 하여 생성한 보상정보를 자원대여 디바이스로 전송하는 자원요청 디바이스;를 포함한다.

[0016] 또한, 자원요청 디바이스는, 자원공유 요청신호에 대응하는 자원공유 응답신호를 자원대여 디바이스로부터 수신하고, 응답한 자원대여 디바이스들로 기 설정된 프로세스 수행을 위한 작업량을 분배하는 것을 특징으로 한다.

[0017] 또한, 본 발명의 제2 실시예에 따른 프라이버시를 보장하는 자원 공유 제어 시스템은, 자원요청 디바이스로부터 자원요청 신호를 수신하여 상기 자원공유 요청신호에 대응하는 작업을 수행하고, 작업수행 결과정보와 이에 상응하는 보상발급요청서를 상기 자원요청 디바이스로 전송하여 블라인드 서명된 보상정보를 수신하며, 수신한 보상정보를 토대로 생성한 보상지급요청서를 보상서버로 전송하여 보상을 받는 자원대여 디바이스;를 포함한다.

[0018] 또한, 본 발명의 제3 실시예에 따른 프라이버시를 보장하는 자원 공유 제어 시스템은, 자원대여 디바이스로부터 보상지급요청서를 수신하고, 인증서 및 시리얼을 통해 보상지급요청서의 유효성을 검증하여 보상지급정보를 상기 자원대여 디바이스로 전송하는 보상서버를 포함한다.

[0019] 그리고, 보상서버는, 보상지급요청서의 유효성 검증을 위해 자원요청 디바이스의 공개키를 관리하는 것을 특징으로 한다.

[0020] 아울러, 전술한 시스템을 기반으로 하는 본 발명의 프라이버시를 보장하는 자원 공유 제어 방법은, 자원요청 디바이스가 다수의 디바이스로 자원공유 요청신호를 전송하는 (a) 단계; 자원대여 디바이스가 자원공유 요청신호에 대응하는 프로세스를 수행하여 생성한 작업수행 결과정보 및 보상발급요청서를 자원요청 디바이스로 전송하는 (b) 단계; 자원요청 디바이스가 블라인드 서명을 통해 생성한 보상정보를 자원대여 디바이스로 전송하는 (c) 단계; 자원대여 디바이스가 수신한 보상정보를 토대로 생성한 보상지급요청서를 보상서버로 전송하는 (d) 단계; 보상서버가 공개키, 인증서 및 시리얼을 통해 보상지급요청서의 유효성을 검증하는 (e) 단계; 및 보상서버가 보상지급정보를 자원대여 디바이스로 전송하는 (f) 단계;를 포함한다.

[0021] 또한, (b) 단계는, 자원대여 디바이스가 자원요청 디바이스로부터 수신한 자원공유 요청신호를 수락하여 생성한 자원공유 응답신호를 자원요청 디바이스로 전송하는 (b-1) 단계; 자원요청 디바이스가 수신한 자원공유 응답신호에 대응하는 자원대여 디바이스로 특정 프로세스 수행을 위한 작업량을 분배하는 (b-2) 단계; 자원대여 디바이스가 할당받은 작업량에 대응하는 프로세스를 수행하여 작업수행 결과정보를 생성하는 (b-3) 단계; 및 자원대여 디바이스가 생성한 작업수행 결과정보 및 보상발급요청서를 자원요청 디바이스로 전송하는 (b-4) 단계;를 포함한다.

[0022] 그리고, (c) 단계는, 자원요청 디바이스가 자원대여 디바이스들로부터 수신한 작업수행 결과정보를 취합하여 특정 프로세스를 수행하는 (c-1) 단계; 자원요청 디바이스가 자원요청 디바이스 식별자, 보상서버 식별자 및 보상발급요청서에 대한 블라인드 서명값을 포함하는 보상정보를 생성하는 (c-2) 단계; 및 자원요청 디바이스가 보상정보를 자원대여 디바이스로 전송하는 (c-3) 단계;를 포함한다.

발명의 효과

[0023] 상기와 같은 본 발명에 따르면, 자원요청 디바이스의 요청에 대응하는 작업을 수행한 자원대여 디바이스로 보상을 지급하되, 보상과정에서 어떤 작업에 대한 보상인지를 알 수가 없게 함으로써, 작업대여 디바이스의 프라이버시를 보호하는 효과가 있다.

[0024] 그리고, 본 발명에 따르면, 자원요청 디바이스가 자원 활용에 따른 보상을 블라인드 서명 형태로 자원대여 디바이스에게 발급하고, 보상 서버가 유효성 검증을 통해 자원대여 디바이스로 보상을 지급함으로써, 특정 작업에 따른 보상이 중복으로 지급되는 것을 방지할 수 있다.

도면의 간단한 설명

[0025]

- 도 1은 일반적인 무선 네트워크 시스템의 자원 공유 흐름을 도시한 도면.
- 도 2는 종래의 자원 공유 방법을 도시한 순서도.
- 도 3은 본 발명에 따른 프라이버시를 보장하는 자원 공유 제어 시스템을 도시한 구성도.
- 도 4를 본 발명에 따른 프라이버시를 보장하는 자원 공유 제어 시스템의 프로토콜을 도시한 도면.
- 도 5는 본 발명에 따른 프라이버시를 보장하는 자원 공유 제어 시스템의 자원요청 디바이스와 자원대여 디바이스간의 자원공유를 도시한 예시도.
- 도 6은 본 발명에 따른 프라이버시를 보장하는 자원 공유 제어 시스템의 자원대여 디바이스가 자원요청 디바이스와의 자원공유 수락을 도시한 예시도.
- 도 7은 본 발명에 따른 프라이버시를 보장하는 자원 공유 제어 시스템의 자원대여 디바이스가 보상정보를 수신하는 것을 도시한 예시도.
- 도 8은 본 발명에 따른 프라이버시를 보장하는 자원 공유 제어 시스템의 자원대여 디바이스가 보상정보를 병합하는 것을 도시한 제1 예시도.
- 도 9는 본 발명에 따른 프라이버시를 보장하는 자원 공유 제어 시스템의 자원대여 디바이스가 보상정보를 병합하는 것을 도시한 제2 예시도.
- 도 10은 본 발명에 따른 프라이버시를 보장하는 자원 공유 제어 시스템의 자원대여 디바이스가 보상정보를 병합하는 것을 도시한 제3 예시도.
- 도 11은 본 발명에 따른 프라이버시를 보장하는 자원 공유 제어 시스템의 자원대여 디바이스가 보상서버로 보상지급을 요청하는 것을 도시한 예시도.
- 도 12는 본 발명에 따른 프라이버시를 보장하는 자원 공유 제어 시스템의 자원대여 디바이스가 보상지급정보에 대한 상세정보를 확인하는 것을 도시한 예시도.
- 도 13은 본 발명에 따른 프라이버시를 보장하는 자원 공유 제어 시스템의 보상지급정보 발급 및 보상지급정보 사용 프로세스를 도시한 예시도.
- 도 14는 본 발명에 따른 프라이버시를 보장하는 자원 공유 제어 시스템(S)의 자원공유 프로세스를 도시한 예시도.
- 도 15는 본 발명에 따른 프라이버시를 보장하는 자원 공유 제어 방법을 도시한 순서도.
- 도 16은 본 발명에 따른 프라이버시를 보장하는 자원 공유 제어 방법의 제S20단계의 세부과정을 도시한 순서도.
- 도 17은 본 발명에 따른 프라이버시를 보장하는 자원 공유 제어 방법의 제S30단계의 세부과정을 도시한 순서도.

발명을 실시하기 위한 구체적인 내용

[0026]

본 발명의 구체적인 특징 및 이점들은 첨부도면에 의거한 다음의 상세한 설명으로 더욱 명백해질 것이다. 이에 앞서, 본 명세서 및 청구범위에 사용된 용어나 단어는 발명자가 그 자신의 발명을 가장 최선의 방법으로 설명하기 위해 용어의 개념을 적절하게 정의할 수 있다는 원칙에 입각하여 본 발명의 기술적 사상에 부합하는 의미와 개념으로 해석되어야 할 것이다. 또한, 본 발명에 관련된 공지 기능 및 그 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는, 그 구체적인 설명을 생략하였음에 유의해야 할 것이다.

[0027]

도 3에 도시된 바와 같이, 본 발명에 따른 프라이버시를 보장하는 자원 공유 제어 시스템(S)은, 다수의 디바이스로 자원공유 요청신호를 전송하되, 상기 자원공유 요청신호에 대응하는 작업수행 결과정보와 이에 상응하는 보상발급요청서를 자원대여 디바이스로부터 수신하며, 상기 보상발급요청서에 블라인드 서명하여 생성한 보상정보를 자원대여 디바이스로 전송하는 자원요청 디바이스(10), 자원요청 디바이스로부터 자원요청 신호를 수신하여 상기 자원공유 요청신호에 대응하는 작업을 수행하여 생성한 작업수행 결과정보와 이에 상응하는 보상발급요청서를 상기 자원요청 디바이스로 전송하여 블라인드 서명된 보상정보를 수신하며, 수신한 보상정보를 토대로

생성한 보상지급요청서를 보상서버로 전송하여 보상지급정보를 수신하는 자원대여 디바이스(20), 및 자원대여 디바이스로부터 보상지급요청서를 수신하고, 공개키, 인증서 및 시리얼을 통해 보상지급요청서의 유효성을 검증하여 보상지급정보를 자원대여 디바이스로 전송하는 보상서버(30)를 포함하여 구성된다.

[0028] 본 발명에 따른 프라이버시를 보장하는 자원 공유 제어 시스템(S)은, 자원요청 디바이스(10) 및 자원대여 디바이스(20) 각각이 자원을 공유하기 위해 사전 동의 절차를 수행한 것으로 상정하겠으나, 본 발명이 이에 국한되는 것은 아니며, 사전 동의 없이 자원요청 디바이스(10)가 불특정 디바이스로 자원대여를 요청하고, 이를 수락한 자원대여 디바이스(20)가 자원요청 디바이스(10)를 위해 자원을 공유하도록 구성 될 수 있다.

[0029] 또한, 자원 공유에 따라 보상을 발행하는 자원요청 디바이스(10) 및 보상을 지급하는 보상서버(30) 각각이 유효성 검증을 위해 자원요청 디바이스에 대응하는 공개키를 관리(검증 파라미터 공유)하도록 구성된다.

[0030] 구체적으로, 자원요청 디바이스(10)는 다수의 디바이스로 자원공유 요청신호를 전송하고, 수신한 자원공유 응답신호에 대응하는 자원대여 디바이스(20)들로 특정 프로세스 수행을 위한 작업량을 분배한다.

[0031] 이때, 보상정보는 자원요청 디바이스의 인증서, 블라인드 서명값을 포함하며, 보상이 중복으로 지급되는 것을 방지한다.

[0032] 그리고, 보상서버(30)는 자원대여 디바이스(20)로부터 보상지급요청서를 수신하고, 공개키, 인증서 및 시리얼을 통해 보상지급요청서의 유효성을 검증하여 보상지급정보를 자원대여 디바이스(20)로 전송한다.

[0033] 아울러, 보상서버(30)는 보상지급요청서의 유효성 검증을 위해 보상지급요청서에 포함된 자원요청 디바이스의 공개키를 관리하도록 구성된다.

[0034] 한편, 도 4를 참조하여 본 발명에 따른 프라이버시를 보장하는 자원 공유 제어 시스템(S)의 프로토콜에 대해 살펴보면 아래와 같다.

[준비과정]

[0036] 사전 준비과정으로서 자원요청 디바이스(마스터)가 스스로 자신의 비밀키(x)와 공개키(y)를 생성한다(step 0-1).

[0037] 이어서, 자원요청 디바이스 CA(인증기관)에게 자신이 생성한 공개키를 전달하여 인증서 발급을 요청한다(step 0-2).

[0038] 그리고, CA가 요청받은 인증서($Cert_{Master}$)를 자원요청 디바이스에게 발급한다(step 0-3).

[0039] 여기서, 자원요청 디바이스의 인증서에는 자원요청 디바이스 식별 정보 및 공개키 y 가 기재되어 있으며, 보상서버는 CA의 인증서를 공유하고 있는 것으로 가정한다.

[0040] 또한, Z 와 g 는 본 발명에 따른 시스템 참여자에게 공개된 것으로 이해함이 바람직하다.

[보상정보발급과정]

[0042] 먼저, 자원대여 디바이스(헬퍼)는 보상요청서의 중복 발행을 배제하기 위해 랜덤 r 과 시리얼 s 를 무작위로 추출한다(step 1).

[0043] 이어서, 자원대여 디바이스가 랜덤 r 과 시리얼 s 를 이용하여 보상발급요청서 h 를 작성한다(step 2).

[0044] 이때, 보상발급요청서에 포함된 보상액은 정해진 금액(정액) 방식을 이용하는 것이 바람직하다. 예를 들어 각각의 보상발급요청서 h 는 1,000원을 보상액으로 정하여 총 10,000원의 보상이 필요한 경우에는 10개의 보상발급요청서 h 를 발행토록 할 수 있다.

[0045] 뒤이어, 자원대여 디바이스가 보상발급요청서 h 를 자원요청 디바이스에게 전달한다(step 3).

[0046] 이어서, 자원요청 디바이스가 보상발급요청서 h 와 자신의 비밀키 x 를 사용하여 블라인드서명 ψ 를 생성한다(step 4).

[0047] 뒤이어, 자원요청 디바이스는 블라인드서명 ψ 와 자신의 인증서 $Cert_{Master}$ 를 자원대여 디바이스에게 전달한다(step 5).

[0048] 이어서, 자원대여 디바이스가 자원요청 디바이스의 인증서 $Cert_{Master}$ 에서 자원요청 디바이스의 공개키 y 를 색인

한다(step 6).

[0049] 뒤이어, 자원대여 디바이스가 공개키 y 와 블라인드서명 ψ 와 랜덤 r 로부터 보상정보 σ 를 생성한다(step 7).

[0050] 그리고, 자원대여 디바이스가 보상정보 σ 가 유효한지 여부를 체크한다(step 8).

[보상지급 요청과정]

[0052] 먼저, 자원대여 디바이스(헬퍼)가 시리얼 s , 보상정보 σ , 인증서 $Cert_{Master}$ 를 보상서버에게 제출한다(step 9).

[0053] 이어서, 보상서버가 인증서 $Cert_{Master}Cert_{CA}$ 에 대한 유효성을 공개키로 검사한다(step 10).

[0054] 뒤이어, 보상서버가 인증서 $Cert_{Master}$ 에서 공개키 y 를 색인한다(step 11).

[0055] 이어서, 보상서버가 보상정보 σ 가 유효한지 여부를 체크한다(step 12).

[0056] 그리고, 보상서버가 해당되는 보상지급정보를 자원대여 디바이스에게 전달한다(step 13).

[0057] 아울러, 자원대여 디바이스는 다수의 보상정보 σ_1 내지 σ_n 을 하나의 보상정보 σ 로 병합할 수 있으며, 보상서버가 병합된 보상정보 σ 에 대한 유효성을 체크하도록 구성될 수 있다.

[0058] 이하, 도 5 내지 도 12를 참조하여 본 발명에 따른 프라이버시를 보장하는 자원 공유 제어 시스템(S)의 실시예에 대해 살펴보면 아래와 같다.

[0059] 먼저, 도 5에 도시된 바와 같이, 자원요청 디바이스(10)가 ON 상태에서(예컨대 앱을 실행한 상태에서) 'START' 버튼에 대한 입력신호를 인가받은 경우, 자원요청 디바이스의 현재 상태를 ON으로 전환함과 동시에 자원요청 디바이스의 IP 및 Port를 접속된 자원대여 디바이스(20)에게 공개한다.

[0060] 이어서, 도 6에 도시된 바와 같이, 자원대여 디바이스(20)는 접속된 자원요청 디바이스(10)로부터 상기 IP 및 Port를 입력받고, 'REQUEST A RECEIPT' 버튼에 대한 입력신호에 따라 자원요청 디바이스(10)와의 자원공유를 수락한다.

[0061] 그리고, 자원요청 디바이스(10)는 issue 화면에서 '확인' 버튼에 대한 입력신호를 인가받아 자원대여 디바이스(20)의 자원(예컨대, CPU, 메모리 또는 센서)을 사용한다.

[0062] 뒤이어, 도 7에 도시된 바와 같이, 자원대여 디바이스(20)는 자원요청 디바이스(10)로의 자원 대여에 따라 'REQUEST SUCCESS' 알람과 함께 보상정보를 수신한다. 이때, 자원대여 디바이스(20)가 '취소' 버튼에 대한 입력신호를 인가받는 경우, 'Rejected' 알람을 수신한다.

[0063] 또한, 도 8에 도시된 바와 같이, 자원대여 디바이스(20)는 자원요청 디바이스(10)의 IP를 입력하고, 2개 이상의 보상정보를 선택한 이후, 'AGGREGATE' 버튼에 대한 입력신호를 인가받는 경우, 1개의 보상정보로 병합된다.

[0064] 이때, 도 9에 도시된 바와 같이, 자원대여 디바이스(20)가 병합된 보상정보와 보상정보를 선택한 이후, 'AGGREGATE' 버튼에 대한 입력신호를 인가받는 경우, 이 역시 1개의 보상정보로 병합된다.

[0065] 아울러, 도 10에 도시된 바와 같이, 자원대여 디바이스(20)가 병합된 보상정보와 병합된 또 다른 보상정보를 선택한 이후, 'AGGREGATE' 버튼에 대한 입력신호를 인가받는 경우, 이 역시 1개의 보상정보로 병합된다.

[0066] 한편, 도 11에 도시된 바와 같이, 자원대여 디바이스(20)는 IP를 입력받아 보상서버(30)와 접속되어 보상정보를 선택한 이후, 'REWARD REQUEST' 버튼에 대한 입력신호를 인가받아 보상서버(30)로 보상지급요청서를 전달한다.

[0067] 이어서, 보상서버(30)가 수신한 보상정보에 대한 유효성을 검증하여 보상지급정보를 자원대여 디바이스(20)로 전달한다.

[0068] 그리고, 도 12에 도시된 바와 같이, 자원대여 디바이스(20)는 보상지급정보를 수신한 목록을 확인할 수 있고, 누적된 보상지급정보를 확인할 수 있으며, 보상지급정보 목록 중에 어느 하나에 대한 입력신호를 인가받는 경우, 해당 보상지급정보에 대한 상세정보를 확인할 수 있다.

[0069] 한편, 도 13은 본 발명에 따른 프라이버시를 보장하는 자원 공유 제어 시스템(S)의 보상지급정보 발급(이하, '쿠폰') 및 보상지급정보(이하, '익명쿠폰') 사용 프로세스를 도시한 예시도이다.

- [0070] 이하에서는 그 구체적인 언급을 생략하겠으나, 보상서버는 매장과 접속된 서버로 구성될 수 있고, 자원요청 디바이스는 매장에 구비된 단말기로 구성될 수 있다.
- [0071] 예컨대, 자원요청 디바이스는 스타벅스 커피숍에 구비된 단말기이고, 보상서버는 스타벅스에 구비된 단말기와 접속된 서버로 구성될 수 있으며, 자원대여 디바이스가 보상지급정보를 사용하는 곳은 G마켓 온라인 쇼핑몰로 구성될 수 있다.
- [0072] 먼저, 보상서버, 자원요청 디바이스, 자원대여 디바이스 및 보상지급정보를 사용하는 쇼핑몰에 쿠폰 검증을 위한 파라미터를 사전에 공유하고 있다(step1).
- [0073] 이때, 자원요청 디바이스는 매장에 구비된 단말기 또는 온라인 쇼핑몰 서버로 구성될 수 있다.
- [0074] 이어서, 자원요청 디바이스 및 자원대여 디바이스간의 자원공유 이후 또는 주문결제 완료 이후, 자원대여 디바이스가 '쿠폰'을 요청하는 '쿠폰요청코드'를 생성한다(step2). 이때, '쿠폰요청코드'는 자원대여 디바이스 화면에 바코드 형태로 표시될 수 있다.
- [0075] 뒤이어, 자원요청 디바이스가 자원대여 디바이스로부터 '쿠폰요청코드'를 수신하여 보상서버로 전송한다(step3). 이때, 자원요청 디바이스가 오프라인 매장에 구비된 경우, 자원대여 디바이스 화면의 바코드를 독출하여 '쿠폰요청코드'를 수신한다.
- [0076] 이어서, 보상서버가 '쿠폰요청코드'의 유효성을 검증하여 쇼핑몰 또는 오프라인 매장에서 사용이 가능한 '쿠폰'을 생성한다(step4).
- [0077] 뒤이어, 보상서버가 생성한 '쿠폰'을 자원대여 디바이스에게 발급한다(step5).
- [0078] 이어서, 자원대여 디바이스가 발급받은 '쿠폰'에 대한 발급처 및 자원대여 디바이스의 개인정보를 배제한 '익명쿠폰'을 생성하여 저장한다(step6).
- [0079] 뒤이어, 자원대여 디바이스가 쇼핑몰 매장에서 쇼핑후 결제를 수행한다.
- [0080] 이어서, 자원대여 디바이스가 쇼핑몰 또는 매장에 '익명쿠폰'을 제출한다(step7).
- [0081] 뒤이어, 쇼핑몰 또는 매장이 수신 또는 바코드를 통해 독출한 '익명쿠폰'을 검증한다(step8). 이때, 검증이란 '익명쿠폰'이 기 사용되었는지 여부만을 검증하고, 그밖에 정보에 대해서는 알지 못한다.
- [0082] 그리고, 쇼핑몰 또는 매장이 결제완료 정보를 자원대여 디바이스로 전송한다(step9).
- [0083] 상기와 같은 본 발명의 프라이버시를 보장하는 자원 공유 제어 시스템(S)에 따르면, 자원대여 디바이스(사용자)가 전국 스타벅스 지점에서 음료를 구매하면 이에 대한 쿠폰 또는 포인트를 적립하고, 사용자는 이 쿠폰 또는 포인트를 G마켓에서 물건을 구입할 때 사용할 수 있다.
- [0084] 이때, G마켓은 구매자가 스타벅스가 발급한 포인트를 사용하여 구매한다는 사실 외에는 구매자가 누구인지, 쿠폰 또는 포인트는 언제 어디서 적립했는지에 대한 일체의 정보를 알 수가 없다.
- [0085] 한편, 도 14는 본 발명에 따른 프라이버시를 보장하는 자원 공유 제어 시스템(S)의 자원공유 프로세스를 도시한 예시도이다.
- [0086] 여기서, 도 13을 참조하여 설명하는 자원요청 디바이스 및 자원대여 디바이스는 자율주행 자동차인 것으로 상정하겠으나, 본 발명이 이에 국한되는 것은 아니며 자원 요청 및 대여의 주체는 얼마든지 변경될 수 있다.
- [0087] 먼저, #1자율주행 자동차가 #n자율주행 자동차로 자원공유 요청신호를 전송한다(step1). 이때, 자원공유 요청신호에는 전후방 감지 센싱값 또는 내비게이션의 목적지 안내 값이 포함될 수 있다.
- [0088] 이어서, #n자율주행 자동차가 수신한 자원공유 요청신호와 대응하는 프로세스를 수행한다(step2).
- [0089] 뒤이어, #n자율주행 자동차가 생성한 작업수행 결과정보를 #1자율주행 자동차로 전송한다(step3).
- [0090] 그리고, #1자율주행 자동차가 수신한 작업수행 결과정보를 자율주행에 활용한다(step4).
- [0091] 이하, 도 15를 참조하여 본 발명에 따른 프라이버시를 보장하는 자원 공유 제어 방법에 대해 살펴보면 아래와 같다.
- [0092] 먼저, 자원요청 디바이스(10)가 다수의 디바이스로 자원공유 요청신호를 전송한다(S10).

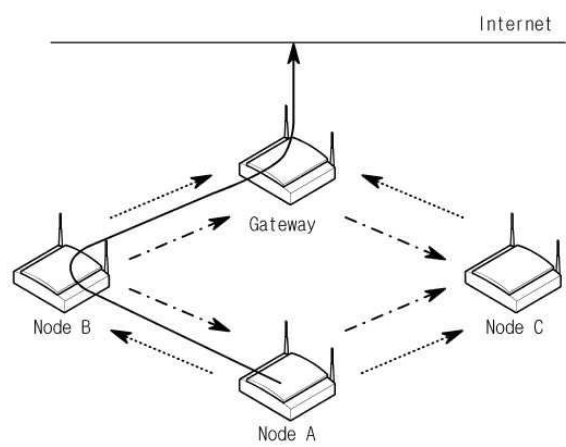
- [0093] 이어서, 자원대여 디바이스(20)가 자원공유 요청신호와 대응하는 프로세스를 수행하여 생성한 작업수행 결과정보 및 보상발급요청서를 자원요청 디바이스(10)로 전송한다(S20).
- [0094] 뒤이어, 자원요청 디바이스(10)가 블라인드 서명을 통해 생성한 보상정보를 자원대여 디바이스(20)로 전송한다(S30).
- [0095] 이어서, 자원대여 디바이스(20)가 수신한 보상정보를 토대로 생성한 보상지급요청서를 보상서버(30)로 전송한다(S40).
- [0096] 뒤이어, 보상서버(30)가 공개키, 인증서 및 시리얼을 통해 보상지급요청서의 유효성을 검증한다(S50).
- [0097] 그리고, 보상서버(30)가 보상지급정보를 자원대여 디바이스(20)로 전송한다(S60).
- [0098] 이하, 도 16을 참조하여 본 발명에 따른 프라이버시를 보장하는 자원 공유 제어 방법의 제S20단계의 세부과정에 대해 살펴보면 아래와 같다.
- [0099] 제S10단계 이후, 자원대여 디바이스(20)가 자원요청 디바이스(10)로부터 수신한 자원공유 요청신호를 수락하여 생성한 자원공유 응답신호를 자원요청 디바이스로 전송한다(S21).
- [0100] 이어서, 자원요청 디바이스(10)가 수신한 자원공유 응답신호와 대응하는 자원대여 디바이스(20)로 특정 프로세스 수행을 위한 작업량을 분배한다(S22).
- [0101] 뒤이어, 자원대여 디바이스(20)가 할당받은 작업량과 대응하는 프로세스를 수행하여 작업수행 결과정보를 생성한다(S23).
- [0102] 그리고, 자원대여 디바이스(20)가 생성한 작업수행 결과정보 및 보상발급요청서를 자원요청 디바이스(10)로 전송한다(S24).
- [0103] 이하, 도 17을 참조하여 본 발명에 따른 프라이버시를 보장하는 자원 공유 제어 방법의 제S30단계의 세부과정에 대해 살펴보면 아래와 같다.
- [0104] 제S20단계 이후, 자원요청 디바이스(10)가 자원대여 디바이스(20)들로부터 수신한 작업수행 결과정보를 취합하여 특정 프로세스를 수행한다(S31).
- [0105] 이어서, 자원요청 디바이스(10)가 자원요청 디바이스 식별자, 보상서버 식별자 및 보상발급요청서에 대한 블라인드 서명값을 포함하는 보상정보를 생성한다(S32).
- [0106] 그리고, 자원요청 디바이스(10)가 블라인드 서명된 보상정보를 자원대여 디바이스(20)로 전송한다(S33).
- [0107] 이상으로 본 발명의 기술적 사상을 예시하기 위한 바람직한 실시예와 관련하여 설명하고 도시하였지만, 본 발명은 이와 같이 도시되고 설명된 그대로의 구성 및 작용에만 국한되는 것이 아니며, 기술적 사상의 범주를 일탈함이 없이 본 발명에 대해 다수의 변경 및 수정이 가능함을 당업자들은 잘 이해할 수 있을 것이다. 따라서 그러한 모든 적절한 변경 및 수정과 균등물들도 본 발명의 범위에 속하는 것으로 간주되어야 할 것이다.

부호의 설명

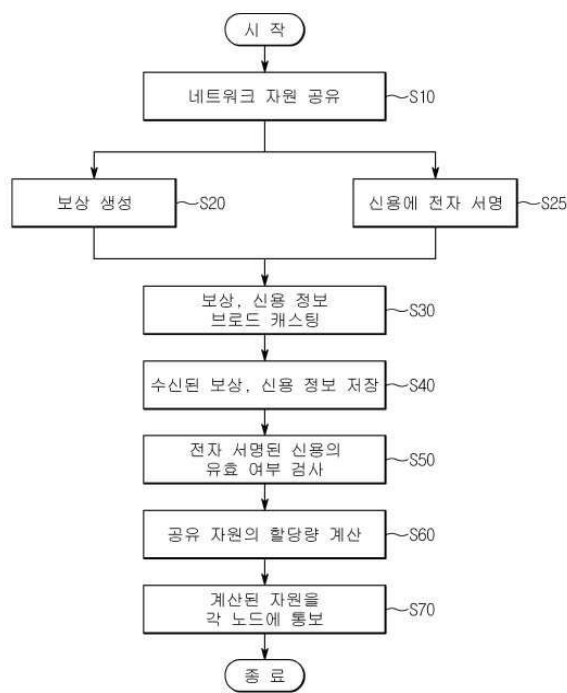
- [0108] S: 프라이버시를 보장하는 자원 공유 제어 시스템
- 10: 자원요청 디바이스
- 20: 자원대여 디바이스
- 30: 보상서버

도면

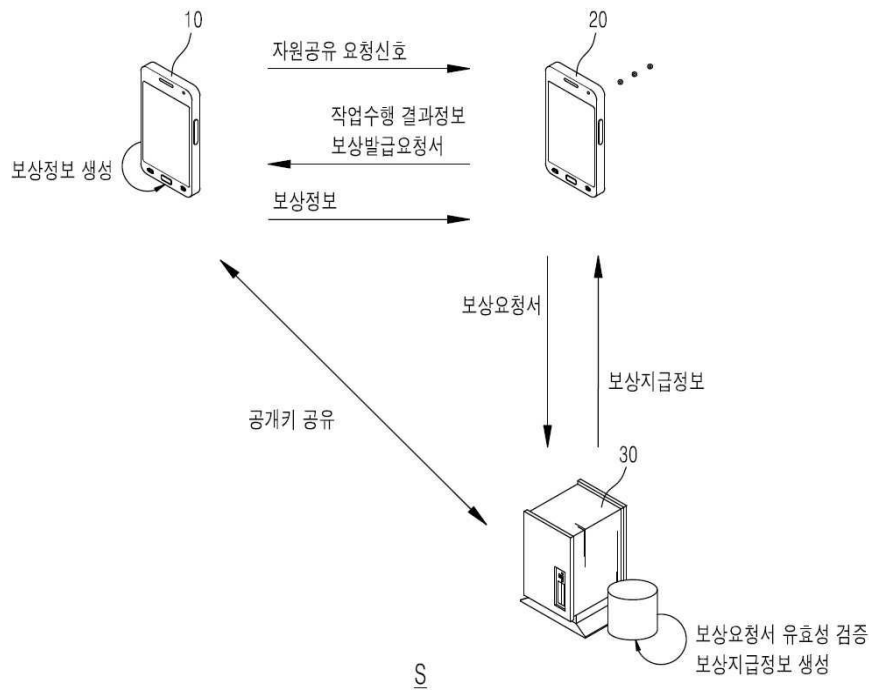
도면1



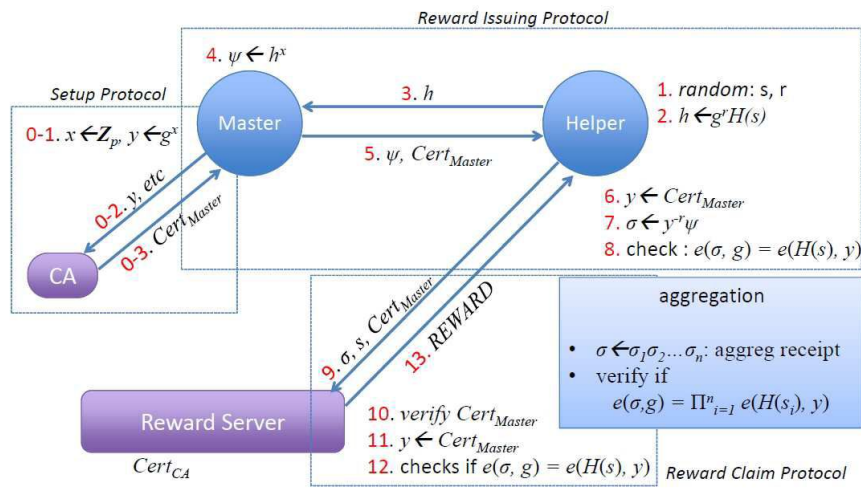
도면2



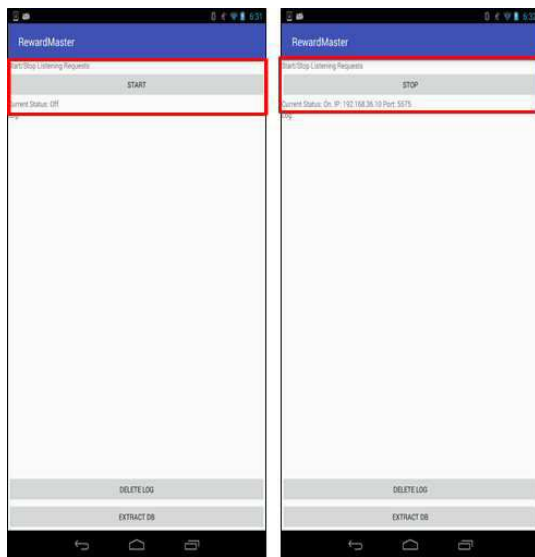
도면3



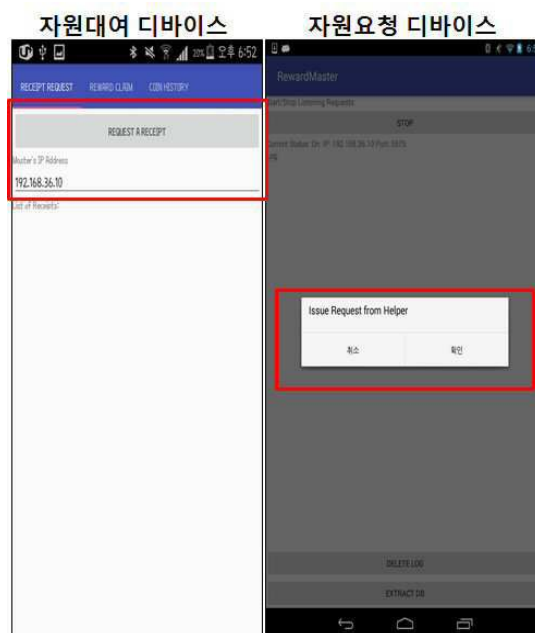
도면4



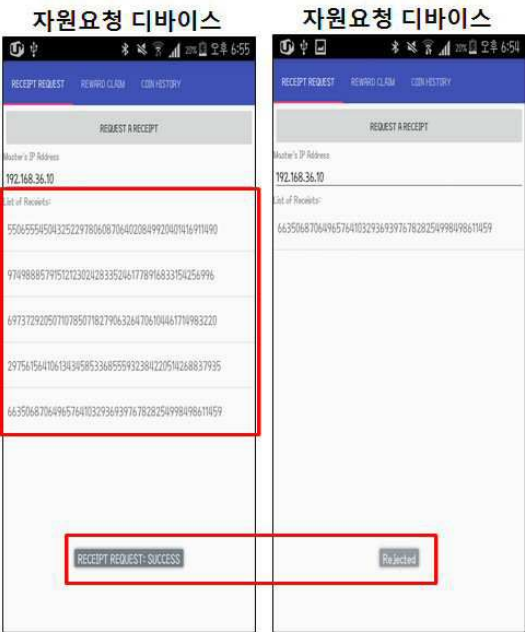
도면5



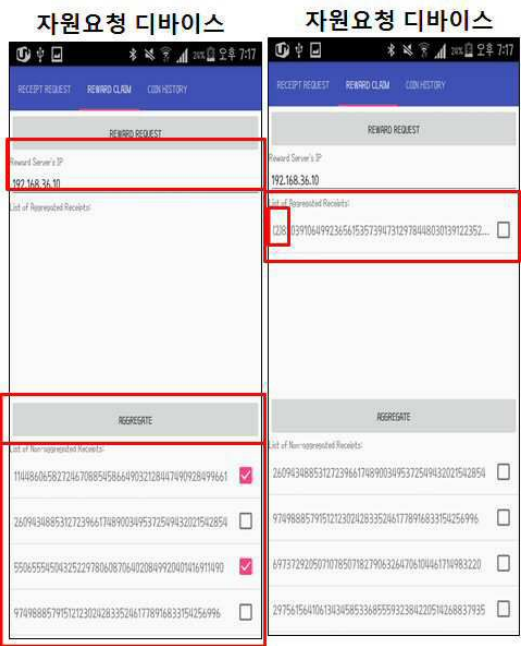
도면6



도면7



도면8



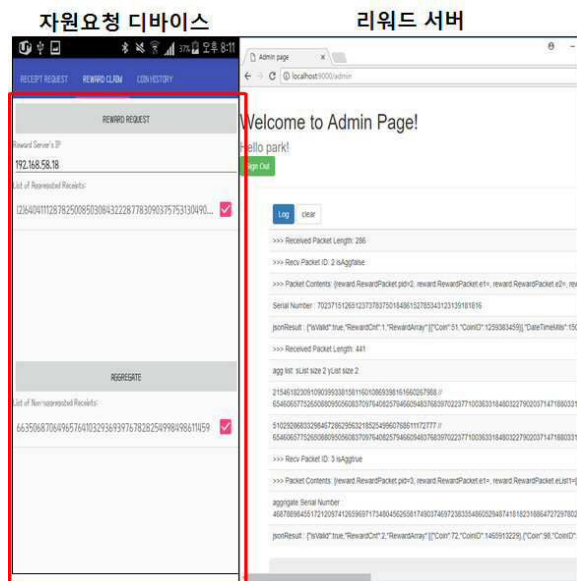
도면9

자원요청 디바이스	자원요청 디바이스
RECEIPT REQUEST REWARD CLAIM CON HISTORY REWARD REQUEST Reward Server's IP 192.168.36.10 List of Requested Rewards: 128203910649923656153573947312978448030139122352...☒ AGGREGATE List of Non-requested Rewards: 267994348853127239661788900349537254943202542854☒ 9749888579512123024283352461778916833154256996☐ 697372920507107850778627963264706104461774983220☐ 29756156410613434585336855932384220514268837935☐	RECEIPT REQUEST REWARD CLAIM CON HISTORY REWARD REQUEST Reward Server's IP 192.168.36.10 List of Requested Rewards: 1310248858869869989415358255784389169843943152...☐ AGGREGATE List of Non-requested Rewards: 9749888579512123024283352461778916833154256996☐ 697372920507107850778627963264706104461774983220☐ 29756156410613434585336855932384220514268837935☐ 663506870649657641032936939767828254999498611459☐

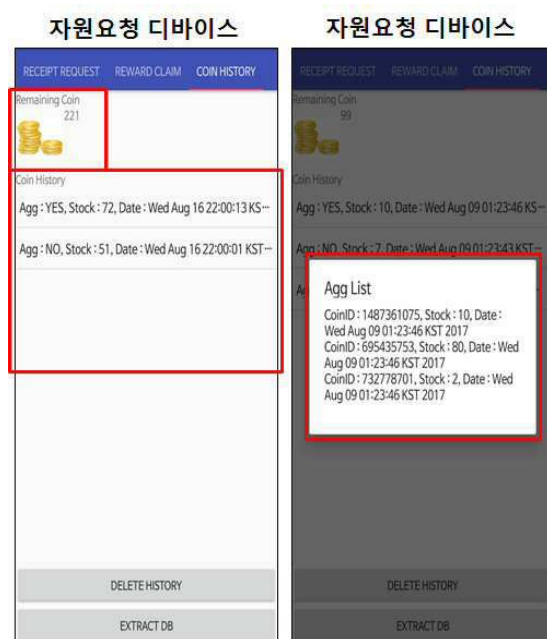
도면10

자원요청 디바이스	자원요청 디바이스
RECEIPT REQUEST REWARD CLAIM CON HISTORY REWARD REQUEST Reward Server's IP 192.168.36.10 List of Requested Rewards: 126305912967899830737849982962906329014513991624...☒ 1310248858869869989415358255784389169843943152...☒ AGGREGATE List of Non-requested Rewards: 29756156410613434585336855932384220514268837935☐ 663506870649657641032936939767828254999498611459☐	RECEIPT REQUEST REWARD CLAIM CON HISTORY REWARD REQUEST Reward Server's IP 192.168.36.10 List of Requested Rewards: 151410226988585596974026490178886792464167900014...☐ AGGREGATE List of Non-requested Rewards: 29756156410613434585336855932384220514268837935☐ 663506870649657641032936939767828254999498611459☐

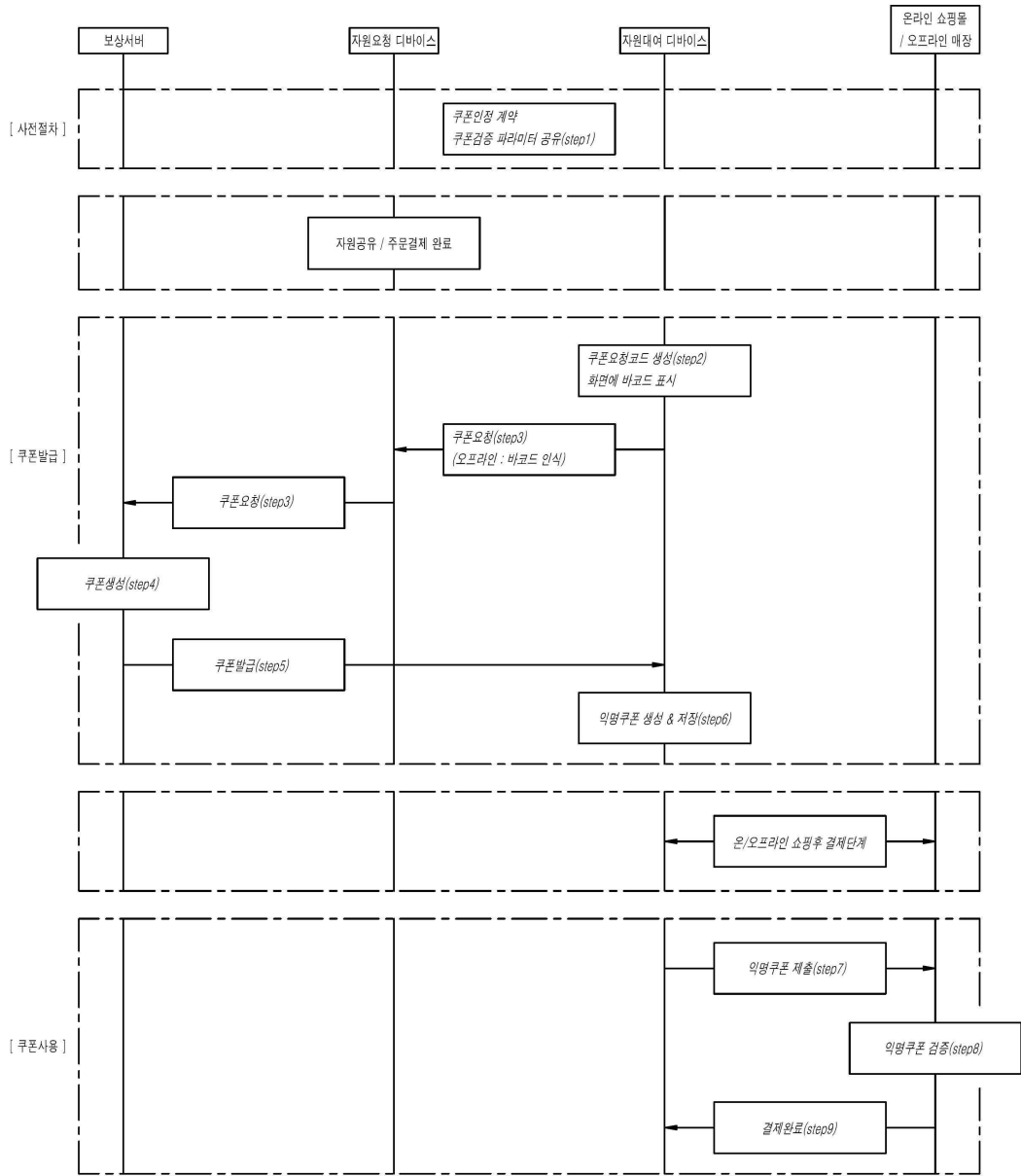
도면11



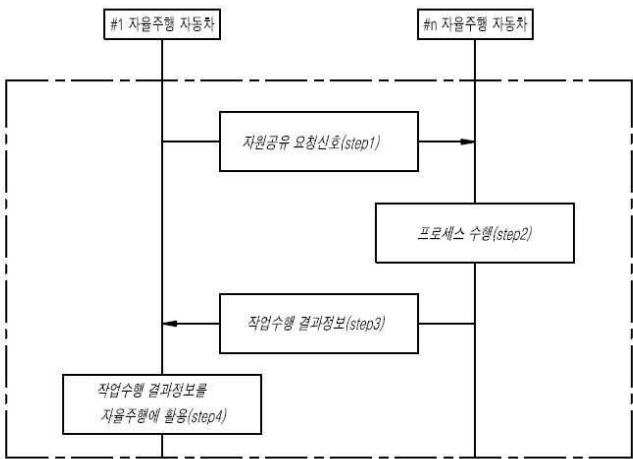
도면12



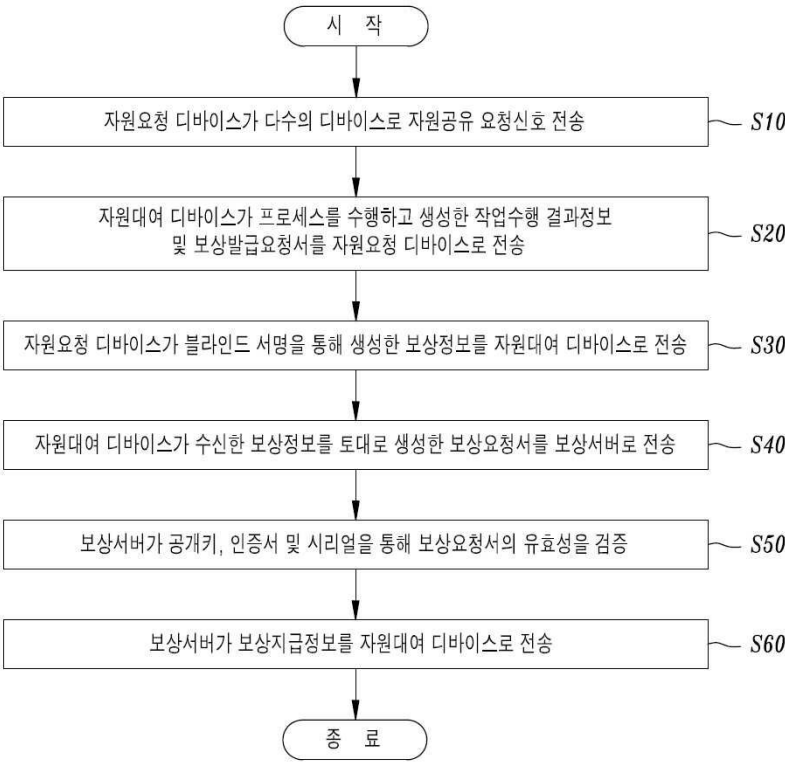
도면13



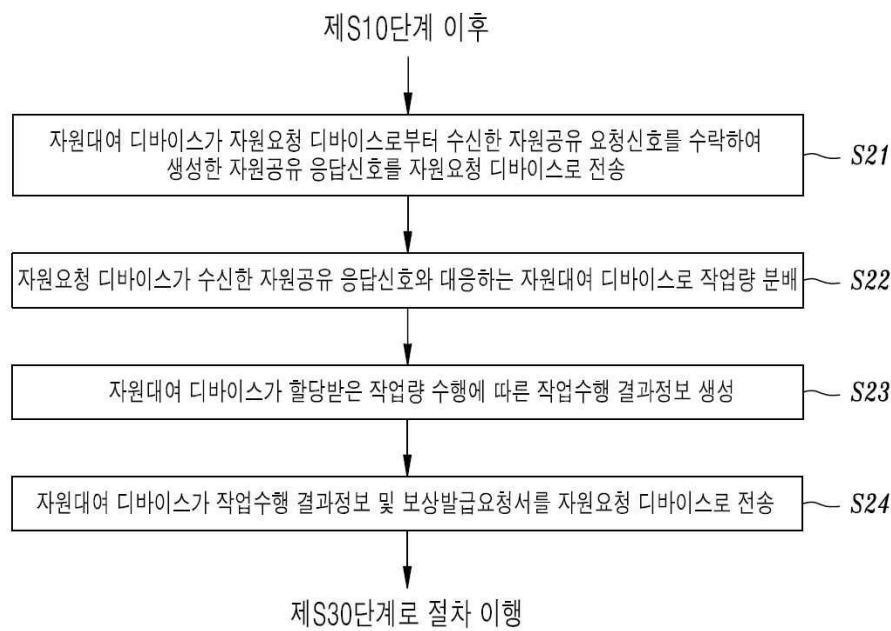
도면14



도면15



도면16



도면17

