



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년12월07일
(11) 등록번호 10-2187700
(24) 등록일자 2020년12월01일

(51) 국제특허분류(Int. Cl.)
G06Q 20/36 (2012.01) G06Q 20/38 (2012.01)
G06Q 20/40 (2012.01) G06Q 20/42 (2012.01)
(52) CPC특허분류
G06Q 20/367 (2020.05)
G06Q 20/382 (2013.01)
(21) 출원번호 10-2019-0069172
(22) 출원일자 2019년06월12일
심사청구일자 2019년06월12일
(56) 선행기술조사문헌
KR101928087 B1*
JP2011141733 A*
datanet(블록체인 데이터 삭제 기술,
2019.05.13.)*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암
동5가)
(72) 발명자
김항남
서울특별시 서초구 서운로 104, 205동 503호 (서
초동, 래미안 서초 에스티지S)
박성준
서울특별시 강남구 삼성로4길 17, 502동 1203호(
개포동, 주공아파트)
오승환
경기도 성남시 분당구 양현로 138, 809동 1602호
(이매동, 이매촌진흥아파트)
(74) 대리인
윤귀상

전체 청구항 수 : 총 14 항

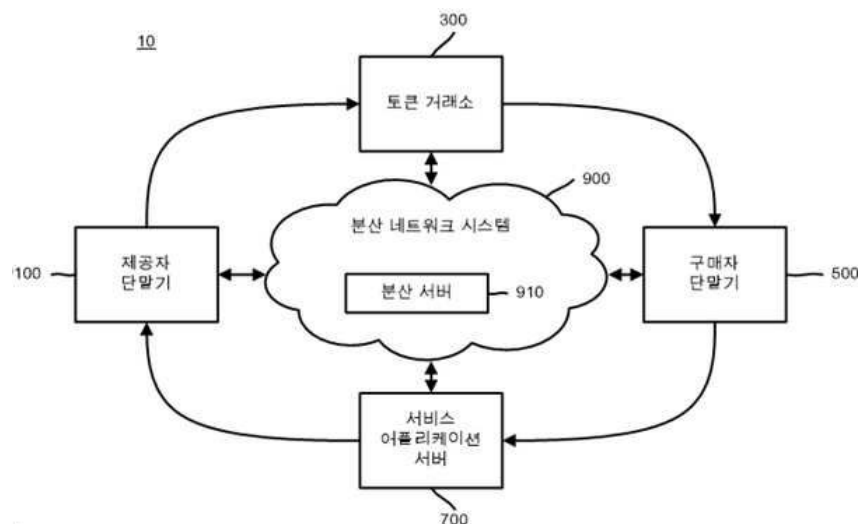
심사관 : 성인구

(54) 발명의 명칭 분산 장부에 기반한 개인 정보 접근 권한 거래 방법 및 그 방법을 이용한 기록 매체

(57) 요약

인증을 수행하고, 토큰을 저장하는 복수 개의 분산 서버를 포함하는 분산 네트워크 시스템에 의해 수행되는 분산 장부에 기반한 개인 정보 접근 권한 거래 방법에 있어서, 토큰 거래 요청을 수신하면, 인증을 수행하여 구매자 단말기에게 토큰(token)에 대한 사용 권한을 부여하고, 토큰 사용 요청을 수신하면, 인증을 수행하여 서비스 어플리케이션 서버에게 토큰의 사용을 허가하며, 서비스 어플리케이션 서버가 토큰을 사용하여 미리 정의된 서비스를 제공하고, 토큰의 사용 내역을 분산 네트워크 시스템으로 브로드캐스팅하며, 분산 서버는 토큰의 사용 내역을 업데이트하는 분산 장부에 기반한 개인 정보 접근 권한 거래 방법을 개시하고 있다.

대표도 - 도1



(52) CPC특허분류

G06Q 20/401 (2020.05)

G06Q 20/42 (2013.01)

명세서

청구범위

청구항 1

인증을 수행하고, 토큰(token)을 저장하는 복수 개의 분산 서버를 포함하는 분산 네트워크 시스템에 의해 수행되는 분산 장부에 기반한 개인 정보 접근 권한 거래 방법에 있어서,

상기 분산 서버는 토큰 거래 요청을 수신하면, 인증을 수행하여 구매자 단말기에게 상기 토큰(token)에 대한 사용 권한을 부여하는 단계;

상기 분산 서버는 토큰 사용 요청을 수신하면, 인증을 수행하여 서비스 어플리케이션 서버에게 상기 토큰(token)의 사용을 허가하는 단계;

상기 분산 서버가 상기 토큰(token)의 사용을 허가하면, 상기 서비스 어플리케이션 서버가 상기 토큰(token)을 사용하여 미리 정의된 서비스를 제공하고, 상기 토큰(token)의 사용 내역을 상기 분산 네트워크 시스템으로 브로드캐스팅(broadcasting)하는 단계; 및

상기 분산 서버는 상기 토큰(token)의 상기 사용 내역을 업데이트하는 단계;를 포함하며,

상기 토큰(token)은, 제공자 단말기의 토큰 발행 요청에 응답하여 생성되되, 상기 제공자 단말기의 개인 정보를 미포함한 제로 널리지(zero-knowledge)를 기반으로 상기 제공자 단말기를 인증함으로써 생성되는, 분산 장부에 기반한 개인 정보 접근 권한 거래 방법.

청구항 2

제 1 항에 있어서,

상기 토큰(token)은,

상기 복수 개의 분산 서버(distributed ledger)에 동일한 정보를 포함하는 복수 개의 토큰(token)이 분산되어 저장되는 것을 특징으로 하는, 분산 장부에 기반한 개인 정보 접근 권한 거래 방법.

청구항 3

제 1 항에 있어서,

상기 토큰(token)은,

제공자 단말기 식별 정보, 허용되는 서비스 식별 정보, 개인 정보 활용 권한, 제공자 서명, 발행자 서명 및 만료 조건을 포함하는 데이터 포맷(data format)인 것을 특징으로 하는, 분산 장부에 기반한 개인 정보 접근 권한 거래 방법.

청구항 4

제 3 항에 있어서,

상기 만료 조건은,

정해진 사용 가능 횟수 값(available count)을 초과하는 경우, 정해진 사용 기한(expiration date)이 경과하는 경우 및 제공자 단말기로부터 중지 요청을 수신하는 경우 중 어느 하나에 해당하면 상기 만료 조건을 충족하는 것을 특징으로 하는, 분산 장부에 기반한 개인 정보 접근 권한 거래 방법.

청구항 5

제 2 항에 있어서,

상기 토큰(token)에 대한 사용 권한을 부여하는 단계는,

상기 분산 서버는 상기 구매자 단말기의 토큰 거래 요청을 토큰 거래소를 통해 수신하는 단계;

상기 분산 서버는 상기 토큰 거래 요청을 수신하면, 상기 분산 서버에 저장된 복수 개의 토큰(token)들이 서로 동일한 데이터 값을 가지는지 확인하는 단계; 및

상기 분산 서버는 상기 복수 개의 토큰(token)들이 서로 동일한 데이터 값을 가지는 것으로 확인되면, 상기 구매자 단말기에게 상기 토큰(token)에 대한 사용 권한을 부여하는 단계;를 포함하는, 분산 장부에 기반한 개인 정보 접근 권한 거래 방법.

청구항 6

제 4 항에 있어서,

상기 토큰(token)에 대한 사용을 허가하는 단계는,

상기 분산 서버는 상기 구매자 단말기로부터 토큰 사용 요청을 통해 수신하는 단계;

상기 분산 서버는 상기 토큰 사용 요청을 수신하면, 상기 분산 서버에 저장된 복수 개의 토큰(token)들이 서로 동일한 데이터 값을 가지는지 확인하는 단계; 및

상기 분산 서버는 상기 복수 개의 토큰(token)들이 서로 동일한 데이터 값을 가지는 것으로 확인되면, 상기 토큰(token)의 만료 조건을 확인하여 상기 서비스 어플리케이션 서버에게 상기 토큰(token)의 사용을 허가하는 단계;를 포함하는, 분산 장부에 기반한 개인 정보 접근 권한 거래 방법.

청구항 7

제 6 항에 있어서,

상기 서비스 어플리케이션에게 상기 토큰(token)의 사용을 허가하는 단계는,

상기 분산 서버는 하나의 토큰(token)에 대해 상기 만료 조건을 확인하는 단계;

상기 분산 서버는 상기 하나의 토큰(token)에 대해 상기 만료 조건을 만족한 것으로 확인되면, 모든 토큰(token)에 대해 상기 만료 조건을 확인하는 단계; 및

상기 분산 서버는 상기 모든 토큰(token)에 대해 상기 만료 조건을 만족한 것으로 확인되면, 상기 서비스 어플리케이션 서버에게 상기 토큰(token)의 사용을 허가하는 단계;를 포함하는, 분산 장부에 기반한 개인 정보 접근 권한 거래 방법.

청구항 8

제 7 항에 있어서,

상기 하나의 토큰(token)에 대해 상기 만료 조건을 확인하는 단계는,

상기 분산 서버는 하나의 토큰(token)으로부터 사용 횟수 값(token usage)을 수집하는 단계; 및

상기 분산 서버는 상기 사용 횟수 값(token usage)과 상기 만료 조건의 사용 가능 횟수 값(available count)을 비교하여 상기 사용 요청이 타당한지 판단하는 단계;를 포함하는, 분산 장부에 기반한 개인 정보 접근 권한 거래 방법.

청구항 9

제 8 항에 있어서,

상기 사용 요청이 타당한지 판단하는 단계는,

상기 분산 서버는 상기 사용 가능 횟수 값(available count)이 상기 사용 횟수 값(token usage)보다 작으면, 상기 사용 요청이 부당한 것으로 판단하는 단계; 및

상기 분산 서버는 상기 구매자 단말기의 사용 요청을 거절하는 단계;를 포함하는, 분산 장부에 기반한 개인 정보 접근 권한 거래 방법.

청구항 10

제 8 항에 있어서,

상기 사용 요청이 타당한지 판단하는 단계는,

상기 분산 서버는 상기 사용 가능 횟수 값(available count)이 상기 사용 횟수 값(token usage)보다 크면, 상기 사용 요청이 타당한 것으로 판단하는 단계; 및

상기 분산 서버는 상기 사용 요청을 상기 분산 네트워크에 존재하는 다른 분산 서버로 브로드캐스팅(broadcasting)하는 단계;를 포함하는, 분산 장부에 기반한 개인 정보 접근 권한 거래 방법.

청구항 11

제 7 항에 있어서,

상기 모든 토큰(token)에 대해 상기 만료 조건을 확인하는 단계는,

상기 분산 서버는 모든 토큰(token)으로부터 사용 횟수 값(token usage)을 수집하는 단계; 및

상기 분산 서버는 상기 토큰(token)으로부터 수집한 복수 개의 사용 횟수 값(token usage)과 상기 만료 조건의 사용 가능 횟수 값(available count)을 각각 비교하여 상기 사용 요청이 타당한지 검증하는 단계;를 포함하는, 분산 장부에 기반한 개인 정보 접근 권한 거래 방법.

청구항 12

제 11 항에 있어서,

상기 사용 요청이 타당한지 검증하는 단계는,

상기 분산 서버는 상기 토큰(token)으로부터 수집한 적어도 하나 이상의 사용 횟수 값 (token usage)이 상기 사용 가능 횟수 값(available count)보다 크면, 상기 토큰(token)의 마지막 사용 내역에 오류가 있는 것으로 판단하는 단계;

상기 분산 서버는 상기 토큰(token)의 마지막 사용 내역에 대한 오류를 분산 네트워크에 브로드캐스팅(broadcasting)하는 단계;

상기 분산 서버는 상기 토큰(token)의 마지막 사용 내역을 삭제하는 단계; 및

상기 분산 서버는 상기 구매자 단말기의 사용 요청을 거절하는 단계;를 포함하는, 분산 장부에 기반한 개인 정보 접근 권한 거래 방법.

청구항 13

제 11 항에 있어서,

상기 사용 요청이 타당한지 검증하는 단계는,

상기 분산 서버는 상기 토큰(token)으로부터 수집한 모든 사용 횟수 값(token usage)이 사용 가능 횟수 값(available count)보다 작으면, 상기 사용 요청이 타당한 것으로 검증하는 단계;

상기 분산 서버는 상기 사용 요청이 타당한 것으로 검증되면, 상기 분산 네트워크에 존재하는 다른 분산 서버로 브로드캐스팅(broadcasting)하는 단계; 및

상기 분산 서버는 상기 서비스 어플리케이션 서버에게 상기 사용 요청을 허가하는 단계;를 포함하는, 분산 장부에 기반한 개인 정보 접근 권한 거래 방법.

청구항 14

제 1 항 내지 제 13 항 중 어느 하나의 항에 따른 분산 장부에 기반한 개인 정보 접근 권한 거래 방법을 수행하기 위한, 컴퓨터 프로그램이 기록된 컴퓨터로 판독 가능한 기록 매체.

발명의 설명

기술 분야

[0001] 본 발명은 분산 장부에 기반한 개인 정보 접근 권한 거래 방법 및 그 방법을 이용한 기록 매체에 관한 것으로서, 더욱 상세하게는 개인 정보가 필요한 분야에서 개인 정보의 제공 없이 업무 수행이 가능하도록 하는 분산 네트워크 시스템을 이용하는 개인 정보 거래, 그 방법을 이용한 기록 매체에 관한 것이다.

배경 기술

- [0003] 이 부분에 기술된 내용은 단순히 본 실시 예에 대한 배경 정보를 제공할 뿐 종래기술을 구성하는 것은 아니다
- [0004] 개인정보를 보관, 관리하는 공공 인종기관에 대한 정보 유출의 위험성은 오랜 기간에 걸쳐 경고 되어왔다. 뿐만 아니라, 개인 정보가 전자화되어 저장되므로 복제 및 배포가 용이하여 유출, 무단 복제 등의 문제가 끊임없이 제기되어 왔다.
- [0005] 이러한 문제를 해결하기 위한 방안으로 전자 서명을 통한 인증 기술, 생체 정보를 이용한 인증 기술 및 개인 정보 보안 기술이 도입되어 왔다.
- [0006] 전자 서명을 통한 인증 기술은 제공자 단말기가 본인이 가진 개인 키(private key)로 정보 전체 및 일부를 변환, 이후 타 제공자 단말기가 제공자 단말기의 공개 키(public key)로 복원하는 비대칭 키 기반 기술로 정보의 신뢰성을 인증하는데 있어 가장 널리 활용되는 인증 기술이다.
- [0007] 생체 정보를 이용한 인증 기술로는 지문 인식, 동공 및 동맥 등을 활용한 생체 인식 기술이 있으며, 기존의 텍스트 기반 인증 기술의 신뢰성 및 활용성에서의 한계를 극복하기 위한 것이다.
- [0008] 개인 정보는 공기업 및 민간기업 등에서 데이터베이스로 관리하며, 개인 정보의 대규모 유출은 경제적 및 사회적인 여파를 가져올 수 있기 때문에 높은 수준의 보안이 요구되며, 각종 암호화 기술 및 인증 기술을 이용하고 있다.
- [0009] 그러나, 상술하는 기술들은 개인 정보를 암호화하기 때문에 데이터 마이닝, 키 추출 공격, 생활 흔적 및 데이터 베이스 해킹 등에 의해 개인 정보가 유출될 수 있는 문제가 있다.
- [0010] 이와 같은 문제는 개인 정보를 직접적으로 제공해야만 공공/클라우드 서비스 등의 인프라 활용이 가능하다는 문제점과, 중앙화된 개인 데이터의 적재로 인해 해킹 및 정보 유출이 될 수 있다.
- [0011] 이에 따라, 개인 정보를 포함하지 않고 종래의 서비스를 이용하는 방법과 탈 중앙화를 통해 해킹으로부터 보호하는 방안에 대한 필요성이 끊임없이 제기되고 있다.

선행기술문헌

특허문헌

- [0013] (특허문헌 0001) 한국공개특허 제10-2011-0139021호 (2014.05.21.)
(특허문헌 0002) 한국등록특허 제 10-1548617 호 (2013.05.16.)

발명의 내용

해결하려는 과제

- [0014] 본 발명의 기술적 과제는 이러한 점에서 착안된 것으로 본 발명의 일 측면에 의하면, 개인 정보 데이터에 대한 직접적인 전송 없이 개인 정보가 필요한 서비스를 제공할 수 있는 거래 인프라 및 인증 기법을 이용하는 분산 장부에 기반한 개인 정보 접근 권한 거래 방법 및 그 방법을 이용한 기록 매체를 제공하는 것이다.
- [0015] 본 발명의 기술적 과제는 이상에서 언급한 기술적 과제로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

- [0017] 본 발명의 실시 예에 따른, 인증을 수행하고, 토큰(token)을 저장하는 복수 개의 분산 서버를 포함하는 분산 네트워크 시스템에 의해 수행되는 분산 장부에 기반한 개인 정보 접근 권한 거래 방법에 있어서, 분산 서버는 토큰 거래 요청을 수신하면, 인증을 수행하여 구매자 단말기에게 토큰(token)에 대한 사용 권한을 부여하는 단계; 분산 서버는 토큰 사용 요청을 수신하면, 인증을 수행하여 서비스 어플리케이션 서버에게 토큰(token)의 사용을 허가하는 단계; 분산 서버가 토큰(token)의 사용을 허가하면, 서비스 어플리케이션 서버가 토큰(token)을 사용하여 미리 정의된 서비스를 제공하고, 토큰(token)의 사용 내역을 분산 네트워크 시스템으로 브로드캐스팅(broadcasting)하는 단계; 및 분산 서버는 토큰(token)에 사용 내역을 업데이트하는 단계;를 포함할 수 있다.
- [0018] 일 실시 예에서, 토큰(token)은, 복수 개의 분산 서버(distributed ledger)에 동일한 정보를 포함하는 복수 개의 토큰(token)이 분산되어 저장될 수 있다.
- [0019] 일 실시 예에서, 토큰(token)은, 제공자 단말기 식별 정보, 허용되는 서비스 식별 정보, 개인 정보 활용 권한, 제공자 서명, 발행자 서명 및 만료 조건을 포함하는 데이터 포맷(data format)일 수 있다.
- [0020] 일 실시 예에서, 만료 조건은, 정해진 사용 가능 횟수 값(available count)을 초과하는 경우, 정해진 사용 기한(expiration date)이 경과하는 경우 및 제공자 단말기로부터 중지 요청을 수신하는 경우 중 어느 하나에 해당하면 만료 조건을 충족할 수 있다.
- [0021] 일 실시 예에서, 토큰(token)에 대한 사용 권한을 부여하는 단계는, 분산 서버는 구매자 단말기의 토큰 거래 요청을 토큰 거래소를 통해 수신하는 단계; 분산 서버는 토큰 거래 요청을 수신하면, 분산 서버에 저장된 복수 개의 토큰(token)들이 서로 동일한 데이터 값을 가지는지 확인하는 단계; 분산 서버는 복수 개의 토큰(token)들이 서로 동일한 데이터 값을 가지는 것으로 확인되면, 구매자 단말기에게 토큰(token)에 대한 사용 권한을 부여하는 단계;를 포함할 수 있다.
- [0022] 일 실시 예에서, 토큰(token)에 대한 사용을 허가하는 단계는, 분산 서버는 구매자 단말기로부터 토큰 사용 요청을 수신하는 단계; 분산 서버는 토큰 사용 요청을 수신하면, 분산 서버에 저장된 복수 개의 토큰(token)들이 서로 동일한 데이터 값을 가지는지 확인하는 단계; 및 분산 서버는 복수 개의 토큰(token)들이 서로 동일한 데이터 값을 가지는 것으로 확인되면, 토큰(token)에 대해 만료 조건을 확인하여 서비스 어플리케이션 서버에게 토큰(token)의 사용을 허가하는 단계;를 포함할 수 있다.
- [0023] 일 실시 예에서, 서비스 어플리케이션에게 토큰(token)의 사용을 허가하는 단계는, 분산 서버는 하나의 토큰(token)에 대해 만료 조건을 확인하는 단계; 분산 서버는 하나의 토큰(token)에 대해 만료 조건을 만족한 것으로 확인되면, 모든 토큰(token)에 대해 만료 조건을 확인하는 단계; 및 분산 서버는 모든 토큰(token)에 대해 만료 조건을 만족한 것으로 확인되면, 서비스 어플리케이션 서버에게 토큰(token)의 사용을 허가하는 단계;를 포함할 수 있다.
- [0024] 일 실시 예에서, 하나의 토큰(token)에 대해 만료 조건을 확인하는 단계는, 분산 서버는 하나의 토큰(token)으로부터 사용 횟수 값(token usage)을 수집하는 단계; 및 분산 서버는 사용 횟수 값(token usage)과 만료 조건의 사용 가능 횟수 값(available count)을 비교하여 사용 요청이 타당한지 판단하는 단계;를 포함할 수 있다.

- [0025] 일 실시 예에서, 사용 요청이 타당한지 판단하는 단계는, 분산 서버는 사용 가능 횟수 값(available count)이 사용 횟수 값(token usage)보다 작으면, 사용 요청이 부당한 것으로 판단하는 단계; 및 분산 서버는 구매자 단말기의 사용 요청을 거절하는 단계;를 포함할 수 있다.
- [0026] 일 실시 예에서, 사용 요청이 타당한지 판단하는 단계는, 분산 서버는 사용 가능 횟수 값(available count)이 사용 횟수 값(token usage)보다 크면, 사용 요청이 타당한 것으로 판단하는 단계; 및 분산 서버는 사용 요청을 분산 네트워크에 존재하는 다른 분산 서버로 브로드캐스팅(broadcasting)하는 단계;를 포함할 수 있다.
- [0027] 일 실시 예에서, 모든 토큰(token)에 대해 만료 조건을 확인하는 단계는, 분산 서버는 모든 토큰(token)으로부터 사용 횟수 값(token usage)을 수집하는 단계; 분산 서버는 토큰(token)으로부터 수집한 복수 개의 사용 횟수 값(token usage)과 만료 조건의 사용 가능 횟수 값(available count)을 각각 비교하여 사용 요청이 타당한지 검증하는 단계;를 포함할 수 있다.
- [0028] 일 실시 예에서, 사용 요청이 타당한지 검증하는 단계는, 분산 서버는 토큰(token)으로부터 수집한 적어도 하나 이상의 사용 횟수 값 (token usage)이 사용 가능 횟수 값(available count)보다 크면, 토큰(token)의 마지막 사용 내역에 오류가 있는 것으로 판단하는 단계; 분산 서버는 토큰(token)의 마지막 사용 내역에 대한 오류를 분산 네트워크에 브로드캐스팅(broadcasting)하는 단계; 분산 서버는 토큰(token)의 마지막 사용 내역을 삭제하는 단계; 및 분산 서버는 구매자 단말기의 사용 요청을 거절하는 단계;를 포함할 수 있다.
- [0029] 일 실시 예에서, 사용 요청이 타당한지 검증하는 단계는, 분산 서버는 토큰(token)으로부터 수집한 모든 사용 횟수 값(token usage)이 사용 가능 횟수 값(available count)보다 작으면, 사용 요청이 타당한 것으로 검증하는 단계; 분산 서버는 사용 요청이 타당한 것으로 검증되면, 분산 네트워크에 존재하는 다른 분산 서버로 브로드캐스팅(broadcasting)하는 단계; 및 분산 서버는 서비스 어플리케이션 서버로 사용 요청을 허가하는 메시지를 전달하는 단계;를 포함할 수 있다.
- [0030] 본 발명의 실시 예에 따른, 컴퓨터 프로그램이 기록된 컴퓨터로 판독 가능한 기록 매체에는 분산 장부에 기반한 개인 정보 접근 권한 거래 방법을 수행하기 위한 컴퓨터 프로그램이 기록되어 있다.

발명의 효과

- [0032] 상술한 본 발명의 일 측면에 따르면, 본 발명의 분산 장부에 기반한 개인 정보 접근 권한 거래 방법 및 그 방법을 이용한 기록 매체에 의해 제공되는 효과는, 개인 정보의 유출 없이 개인 정보가 필요한 서비스를 가능하게 하고, 분산 장부 기술을 도입, 개인 정보 활용의 중복 및 허위 정보 게재를 방지함으로써 개인 정보 거래 시장의 공정성과 신뢰성을 보장할 수 있는 유리한 효과가 있다.
- [0033] 본 발명의 기술적 과제는 이상에서 언급한 기술적 과제로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

- [0035] 도 1은 본 발명의 일 실시 예에 따른 개인 정보 접근 권한 거래 시스템을 나타내는 도면이다.
- 도 2는 본 발명의 일 실시 예에 따른 토큰(token)의 데이터 포맷(data format)을 나타내는 구조도이다.
- 도 3은 본 발명의 일 실시 예에 따른 만료 조건(expiration condition)의 데이터 포맷(data format)을 나타내는 구조도이다.
- 도 4는 본 발명의 일 실시 예에 따른 분산 장부에 기반한 개인 정보 접근 권한 거래 방법을 수행하기 위해 분산 네트워크(distributed network)를 사용하는 경우와 중앙화된 네트워크(centralized network)를 사용하는 경우에 지연 시간을 나타내는 도면이다.
- 도 5는 본 발명의 일 실시 예에 따른 분산 장부에 기반한 개인 정보 접근 권한 거래 방법을 나타내는 순서도이다.
- 도 6은 본 발명의 일 실시 예에 따른 토큰(token)에 대한 사용 권한을 취득하는 과정을 나타내는 순서도이다.
- 도 7은 본 발명의 일 실시 예에 따른 분산 서버가 토큰 사용 요청을 수신하면, 서비스 어플리케이션 서버에게 토큰(token)의 사용을 허가하는 과정을 나타내는 순서도이다.

도 8은 본 발명의 일 실시 예에 따른 토큰(token)의 사용을 허가하는 세부과정을 나타내는 순서도이다.

도 9는 본 발명의 일 실시 예에 따른 하나의 토큰(token)에 대해 만료 조건을 확인하는 과정을 나타내는 순서도이다.

도 10은 본 발명의 일 실시 예에 따른 모든 토큰(token)에 대해 만료 조건을 확인하는 과정을 나타내는 순서도이다.

발명을 실시하기 위한 구체적인 내용

- [0036] 후술하는 본 발명에 대한 상세한 설명은, 본 발명이 실시될 수 있는 특정 실시 예를 예시로서 도시하는 첨부 도면을 참조한다. 이들 실시 예는 당업자가 본 발명을 실시할 수 있기에 충분하도록 상세히 설명된다. 본 발명의 다양한 실시 예는 서로 다르지만 상호 배타적일 필요는 없음이 이해되어야 한다. 예를 들어, 여기에 기재되어 있는 특정 형상, 구조 및 특성은 일 실시 예와 관련하여 본 발명의 정신 및 범위를 벗어나지 않으면서 다른 실시 예로 구현될 수 있다. 또한, 각각의 개시된 실시 예 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.
- [0037] 이하, 도면들을 참조하여 본 발명의 바람직한 실시 예들을 보다 상세하게 설명하기로 한다.
- [0038] 도 1은 본 발명의 일 실시 예에 따른 분산 장부에 기반한 개인 정보 접근 권한 개인 정보 접근 권한 거래 시스템을 나타내는 도면이다.
- [0039] 도 1을 참조하면, 개인 정보 접근 권한 거래 시스템(10)은 제공자 단말기(100), 토큰 거래소(300), 구매자 단말기(500), 서비스 어플리케이션 서버(700) 및 분산 네트워크 시스템(900)을 포함하는 것을 알 수 있다.
- [0040] 제공자 단말기(100)는 개인 정보 대신 후술하는 토큰(F10)을 제공하며, 후술하는 토큰 거래소(300)에 토큰(F10)의 발행을 요청하여 토큰(F10)을 생성할 수 있다.
- [0041] 제공자 단말기(100)의 토큰(F10) 발행 요청은 일/주/월당 수 회 등과 같은 주기적인 방식으로 생성 시에 계약을 체결할 수 있으며, 해당 토큰(F10)의 사용, 거래 내역은 분산 네트워크 시스템(900)에 각각 트랜잭션(transaction)으로 검증되고, 기록된다.
- [0042] 이때, 제공자 단말기(100)에게 토큰(F10)을 생성할 동기를 부여하기 위해 후술하는 구매자 단말기(500)가 지불한 비용의 일부를 인센티브로 받게 된다.
- [0043] 토큰 거래소(300)는 제공자 단말기(100)의 요청에 따라 토큰(F10)을 생성할 수 있고, 토큰 거래소(300)에서 제공자 단말기(100)와 구매자 단말기(500)가 거래를 할 수 있다.
- [0044] 구매자 단말기(500)는 제공자 단말기(100)에게 서비스 어플리케이션 서버(700)를 통해 제공자 단말기(100)에게 접근하기 위해 토큰 거래소(300)에서 토큰(F10)을 구매할 수 있다.
- [0045] 구매자 단말기(500)는 토큰(F10)을 구매하여 토큰(F10)의 사용 권한을 취득할 수 있고, 사용 권한을 취득한 후 서비스 어플리케이션 서버(700)에게 토큰(F10)을 사용하여 서비스를 제공받을 수 있다.
- [0046] 서비스 어플리케이션 서버(700)는 토큰(F10)을 사용하여 구매자 단말기(500)가 원하는 서비스를 제공할 수 있다. 이 때, 서비스 어플리케이션 서버(700)는 서비스 제공에 대한 대가로 구매자 단말기(500)가 토큰(F10)을 구매하면서 지불한 비용의 일부를 지급 받을 수 있다.
- [0047] 토큰(F10)의 거래는 네트워크 상에서 이루어지기 때문에, 전자적 거래의 신뢰성 보증을 위한 거래 인프라가 필요하다.
- [0048] 이를 만족시키기 위해, 토큰 거래 플랫폼으로 분산 네트워크 시스템(900)을 포함한다.
- [0049] 분산 네트워크 시스템(900)의 분산 서버(910)는 적어도 하나 이상의 토큰(F10)을 포함할 수 있다.
- [0050] 제공자 단말기(100)가 토큰(F10)을 생성하게 되면, 분산 서버(910)에 저장된 토큰에 기록되며, 분산 시스템의 특성에 따라 동일한 데이터를 가지는 복수 개의 토큰(F10)이 생성된다.

- [0051] 분산 네트워크 시스템(900)은 토큰(F10)을 저장하고, 토큰(F10)의 사용 과정 및 거래 과정의 타당성을 검증하는 분산 서버(910)를 포함할 수 있다.
- [0052] 이를 위해 ① 토큰(F10)이 정당한 인증 절차를 통해 발급되었는지 여부, ② 토큰(F10)이 정당한 지불을 통해 거래되었는지 여부 및 ③ 토큰(F10)이 본래 의도한 대로 사용 및 만료되었는지 여부를 검증하여 악의적인 사용을 방지할 수 있다.
- [0053] 도 2는 본 발명의 일 실시 예에 따른 토큰(F10)의 데이터 포맷(data format)을 나타내는 구조도이다.
- [0054] 토큰(F10)은 특정 제공자 단말기(100)의 개인 정보를 활용하는 일련의 과정을 하나의 단위 행동으로 규정하고, 해당 행위에 대한 사용 권한을 명시할 수 있다.
- [0055] 예를 들어, 기존에는 텔레마케팅 업체에서 제공자 단말기(100)에게 전화를 걸고자 할 때, 기존에는 제공자 단말기(100)가 개인 정보 활용 권한에 동의하고 이를 통해 수집한 개인 정보를 매매 등을 통해 전달, 직접 해당 번호를 활용하여 전화를 거는 방식을 갖고 있다.
- [0056] 이와 달리, 본 발명에서 제안한 시스템은 제공자 단말기(100)에게 전화를 거는 행위에 대한 권한이 하나의 토큰(F10)에 명시되어 있고, 텔레마케팅 업체는 해당 토큰(F10)을 구입함으로써 제공자 단말기(100)에게 전화를 걸 수 있다.
- [0057] 이 때, 토큰(F10)에는 제공자 단말기(100)의 전화번호에 대한 정보가 포함되어 있지 않으며, 해당 토큰(F10)을 전화 연결 기관(전화국 등)에 전달함으로써 제공자 단말기(100)와의 통화 채널이 형성된다.
- [0058] 개인 정보 활용 행위는 단위화되어 시작점과 끝점이 존재하기 때문에, 토큰(F10)으로써 증명된 개인 정보 활용 권한은 발효 시 종료 기간이 존재할 수밖에 없다.
- [0059] 즉, 토큰(F10)을 재사용하지 못하게 하는 방법이 필요하고, 토큰(F10)은 만료 조건(F400)을 두어 토큰(F10)의 재사용을 방지할 수 있다.
- [0060] 서비스 어플리케이션 서버(700)는 구매자 단말기(500)가 구매한 토큰(F10)을 받아 제공자 단말기(100)와 구매자 단말기(500)간 서비스를 제공하고, 서비스를 제공한 사실을 분산 장부 네트워크에 전달하여 토큰(F10)의 사용 현황에 반영된다.
- [0061] 이미 사용이 만료된 토큰(F10)이 전달된 경우, 서비스 어플리케이션 서버(700)는 분산 네트워크 시스템(900)을 통해 이를 확인하고 토큰(F10) 사용 요청을 거절한다.
- [0062] 해당 토큰(F10)은 만료 조건(F400)이 명시되며, 만료 조건(F400)에 도달할 경우 토큰(F10)을 더 이상 활용할 수 없다. 이와 같은 방식으로 개인 정보에 대한 전달 및 제공 없이 필요한 서비스를 활용할 수 있다.
- [0063] 도 2를 참조하면, 토큰(F10)은 토큰 인덱스(F100), 제공자 단말기(100) 식별 정보(F200), 사용할 수 있는 서비스 식별 정보(F300), 만료 조건(F400), 제공자 단말기(100) 서명(F500) 및 발행자 서명(F600)을 포함하는 것을 알 수 있다.
- [0064] 토큰(F10)은 일련의 데이터(data)로 구성되며, 데이터 포맷(data format)은 와 같다. 도 2은 하나의 예시로서, 서비스에 대한 사용 권한(F300)과 만료 조건(F400), 사용자에게 대한 인증 방식과 권한을 갖는 서비스를 표기하는 모든 종류의 데이터 포맷(data format)을 포함할 수 있다.
- [0065] 이 때, 제공자 단말기(100)의 서명(F500) 및 토큰 거래소(300)의 서명(F600)은 토큰(F10)의 허위 여부를 검증하는 데에 사용되며, 토큰(F10)이 1회 사용될 때마다 구매자 단말기(500)가 지불한 대금이 제공자 단말기(100)에게 지급될 수 있다.
- [0066] 도 3은 본 발명의 일 실시 예에 따른 만료 조건(expiration condition)의 데이터 포맷(data format)을 나타내는 구조도이다.
- [0067] 도 3을 참조하면, 또한, 만료조건(F400)은 사용 횟수(F410), 사용 가능 횟수(F430), 사용 기한(F450) 및 사용 중지 요청 여부(F470)를 포함하는 것을 알 수 있다.
- [0068] 이 때, 만료 조건(F400)은 사용 횟수(F410, token usage), 사용 가능 횟수(F430, available count), 사용 가능 기간(F450, available period), 사용자의 요청(F470, user request)에 의한 수동 만료(F450) 등 토큰(F10)의 사용 가능 여부가 전환될 수 있는 모든 유형의 행위를 포함할 수 있다.

- [0069] 사용 횟수(F410)는 구매자 단말기(500)의 사용 요청에 의해 서비스 어플리케이션 서버(700)가 토큰(F100)을 사용하여 서비스를 제공한 횟수를 의미한다.
- [0070] 사용 가능 횟수(F430)는 토큰(F100)이 사용될 수 있는 횟수를 의미하며, 최초에 토큰(F100)이 생성될 때 지정된다.
- [0071] 사용 기한(F450)은 토큰(F100)이 사용될 수 있는 기간을 의미하며, 최초 토큰(F100)이 생성될 때 지정한다.
- [0072] 서비스 어플리케이션 서버(700)가 토큰(F100)을 사용할 때, 현재 시점과 비교하여 현재 시점이 사용 기한(F450)의 범위에 속하면, 토큰(F100)을 사용하여 서비스를 제공하고, 그렇지 않다면, 서비스 어플리케이션 서버(700)는 구매자 단말기(500)에게 토큰(F400)을 사용할 수 없음을 통지한다.
- [0073] 사용 중지 요청 여부(F470)는 제공자 단말기(100)로부터 직접적인 사용 중지 요청이 있는 경우 활성화된다.
- [0074] 사용 중지 요청이 활성화되면, 사용 횟수(F410)가 사용 가능 횟수(F430)보다 작고, 사용 기한(F450)이 남아 있더라도 서비스 어플리케이션 서버(700)는 구매자 단말기(500)에게 토큰(F10)을 사용할 수 없음을 통지한다.
- [0075] 즉, 만료 조건(F400)을 충족한 토큰(F10)을 사용하려는 행위는 분산 네트워크 시스템(900)에 감지되므로 토큰(F10)을 사용할 수 없게 된다.
- [0076] 도 4는 본 발명의 일 실시 예에 따른 분산 장부에 기반한 개인 정보 접근 권한 거래 방법을 수행하기 위해 분산 네트워크 시스템(900)을 사용하는 경우와 중앙화된 네트워크(centralized network)를 사용하는 경우에 지연 시간(latency)을 나타내는 도면이다.
- [0077] 토큰(F10) 기반 서비스 거래 시스템은 토큰(F10)의 사용 권한을 부여하기 때문에, 토큰(F10)에 대한 1회의 사용 시마다 거래 인증에 대한 지연 시간(latency)이 나타난다.
- [0078] 중앙화된 네트워크(centralized network)의 지연 시간(D_{cent})은 아래 수학식 1에 의해 계산할 수 있다.
- [0079] [수학식 1]
- [0080]
$$D_{cent} = \max \left\{ \frac{NF}{u_s}, \frac{F}{d_{min}} \right\}$$
- [0081] 여기서, N은 네트워크 내 노드 수, F는 거래 요청 메시지의 크기, u_s 는 송신 측의 업로드 속도, d_{min} 는 수신 측의 최소 다운로드 속도를 각각 의미한다.
- [0082] 분산 네트워크(distributed network)의 지연 시간(D_{dist})은 아래 수학식 2에 의해 계산할 수 있다.
- [0083] [수학식 2]
- [0084]
$$D_{dist} = \max \left\{ \frac{F}{u_s}, \frac{F}{d_{min}}, \frac{NF}{u_s + \sum_{i=1}^N u_i} \right\}$$
- [0085] 여기서, N은 네트워크 내 노드 수, F는 거래 요청 메시지의 크기, u_s 는 송신 측의 업로드 속도, d_{min} 는 수신 측의 최소 다운로드 속도, u_i 는 각 노드의 업로드 속도를 각각 의미한다.
- [0086] 도 4를 참조하면, 중앙화된 네트워크(centralized network)에서 인증 절차를 진행하는 경우보다 분산 네트워크(distributed network)를 통해 인증을 진행하는 경우 보다 짧은 지연 시간(latency)을 갖는 것을 확인할 수 있다.
- [0087] 본 발명의 일 실시 예에 따른 분산 장부에 기반한 개인 정보 접근 권한 거래 방법은 도 1에 도시된 개인 정보 접근 권한 거래 시스템(10)과 실질적으로 동일한 구성 상에서 진행되므로, 도 1의 개인 정보 접근 권한 거래 시스템(10)과 동일한 구성요소에 대해 동일한 도면 부호를 부여하고, 반복되는 설명은 생략하기로 한다.
- [0088] 도 5는 본 발명의 일 실시 예에 따른 분산 장부에 기반한 개인 정보 접근 권한 거래 방법을 나타내는 순서도이다.
- [0089] 본 발명에 따른 분산 장부에 기반한 개인 정보 접근 권한 거래 방법은 상술한 본 발명에 따른 개인 정보 접근

권한 거래 시스템(10)에 의해 수행될 수 있다. 이를 위해, 본 발명에 따른 개인 정보 접근 권한 거래 시스템(10)은 후술하는 분산 장부에 기반한 개인 정보 접근 권한 거래 방법을 구성하는 각 단계를 수행하기 위한 애플리케이션(소프트웨어)이 미리 설치될 수 있다.

- [0090] 예를 들어, 개인 정보 접근 권한 거래 시스템(10)의 컴퓨터에는 본 발명에 따른 분산 장부에 기반한 개인 정보 접근 권한 거래 방법에 대한 플랫폼이 소프트웨어의 형태로 미리 설치될 수 있으며, 개인 정보 접근 권한 거래 시스템(10)은 컴퓨터에 설치된 소프트웨어를 실행하여 본 발명에 따른 분산 장부에 기반한 개인 정보 접근 권한 거래 방법이 제공하는 다양한 서비스를 제공받을 수 있다.
- [0091] 도 5를 참조하면, 토큰(F10)을 포함하는 분산 서버(910)를 이용하여 인증을 수행하는 분산 네트워크 시스템(900)을 포함하는 분산 장부에 기반한 개인 정보 접근 권한 거래 방법을 알 수 있다.
- [0092] 토큰 거래소(300)는 제공자 단말기(100)의 토큰 발행 요청에 따라 분산 서버(910)에 토큰을 생성할 수 있다.
- [0093] 제공자 단말기(100)의 개인 정보를 포함하지 않는 제로 널리지 증명(zero-knowledge proof)을 이용하여 제공자 단말기(100)가 본인임을 인증할 수 있다.
- [0094] 제공자 단말기(100)가 자신의 개인 정보에 대한 활용 권한을 ‘매매’ 하기 위해서는 자신이 해당 정보에 대한 소유자가 맞는지, 해당 정보가 타당한지 여부를 검증해야 한다.
- [0095] 제공자 단말기(100)의 토큰(F10) 발행 요청에 대하여, 토큰 거래소(300)는 제공자 단말기(100)에 대한 인증을 제로 널리지(zero-knowledge)를 기반으로 증명한다.
- [0096] 즉, 제공자 단말기(100)는 발행에 요구되는 개인 정보의 소유주가 자신임을 증명하며, 이 때 개인 정보를 토큰(F10) 발행 주체에게 전달하지 않는다.
- [0097] 인증에 성공하게 되면 토큰(F10)을 생성하고, 해당 토큰(F10)은 토큰 거래소(300)에서 구매자 단말기(500)에게 노출된다.
- [0098] 단, 개인 정보가 교환되지 않았기 때문에 사용자(개인 정보 활용 행위 동의자)에 대한 정보는 공개될 수 없다.
- [0099] 분산 서버(910)는 토큰 거래 요청을 수신하면, 인증을 수행하여 구매자 단말기(500)에게 토큰(F10)에 대한 사용 권한을 부여할 수 있다(S100).
- [0100] 분산 서버(910)는 토큰 사용 요청을 수신하면, 인증을 수행하여 서비스 어플리케이션 서버(700)에게 토큰(F10)의 사용을 허가할 수 있다(S100).
- [0101] 분산 서버(910)가 토큰(F10)의 사용을 허가하면, 서비스 어플리케이션 서버(700)가 토큰(F10)을 사용하여 미리 정의된 서비스를 제공하고, 토큰(F10)의 사용 내역을 분산 네트워크 시스템(900)측으로 브로드캐스팅(broadcasting)할 수 있다(S300).
- [0102] 분산 서버(910)는 토큰(F10)의 사용 내역을 업데이트할 수 있다(S500).
- [0103] 도 6은 본 발명의 일 실시 예에 따른 분산 네트워크 시스템(900)을 통해 인증을 수행하여 구매자 단말기(500)가 토큰(F10)에 대한 사용 권한을 취득하는 과정을 나타내는 순서도이다.
- [0104] 도 6을 참조하면, 분산 서버(910)가 토큰 거래 요청을 수신하면, 인증을 수행하여 구매자 단말기(500)에게 토큰(F10)에 대한 사용 권한을 부여하는 과정을 알 수 있다.
- [0105] 분산 서버(910)는 구매자 단말기(500)의 토큰 거래 요청을 토큰 거래소(300)를 통해 수신할 수 있다(S110).
- [0106] 분산 서버(910)는 토큰 거래 요청을 수신하면, 분산 서버(910)에 저장된 복수 개의 토큰(F10)들이 서로 동일한 데이터 값을 가지는지 확인할 수 있다(S130).
- [0107] 분산 서버(910)는 복수 개의 토큰(F10)들이 서로 동일한 데이터 값을 가지는 것으로 확인되면, 구매자 단말기(500)에게 토큰(F10)에 대한 사용 권한을 부여할 수 있다(S150).
- [0108] 도 7은 본 발명의 일 실시 예에 따른 분산 서버(910)가 토큰 사용 요청을 수신하면, 서비스 어플리케이션 서버에게 토큰(F10)의 사용을 허가하는 과정을 나타내는 순서도이다.
- [0109] 도 7을 참조하면, 사용 권한을 취득한 구매자 단말기(500)의 사용 요청에 따라 분산 네트워크 시스템(900)을 통해서 토큰(F10)의 사용 허가를 취득하는 과정을 알 수 있다.

- [0110] 분산 서버(910)는 구매자 단말기(500)로부터 토큰 사용 요청을 수신할 수 있다(S310).
- [0111] 분산 서버(910)는 토큰 사용 요청을 수신하면, 분산 서버(910)에 저장된 복수 개의 토큰(F10)들이 서로 동일한 데이터 값을 가지는지 확인할 수 있다(S330).
- [0112] 분산 서버(910)는 복수 개의 토큰(F10)들이 서로 동일한 데이터 값을 가지는 것으로 확인되면, 토큰(F10)의 만료 조건을 확인하여 서비스 어플리케이션 서버(700)에게 토큰(F10)의 사용을 허가할 수 있다(S400).
- [0113] 도 8은 본 발명의 일 실시 예에 따른 토큰(F10)의 사용을 허가하는 세부과정을 나타내는 순서도이다.
- [0114] 도 8을 참조하면, 토큰(F10)의 만료 조건을 확인하여 서비스 어플리케이션 서버(700)에게 토큰(F10)의 사용을 허가하는 과정을 알 수 있다.
- [0115] 분산 서버(910)는 하나의 토큰(F10)에 대해 만료 조건을 확인할 수 있다(S410).
- [0116] 분산 서버(910)는 하나의 토큰(F10)에 대해 만료 조건을 만족한 것으로 확인되면, 모든 토큰(F10)에 대해 만료 조건을 확인할 수 있다(S430).
- [0117] 분산 서버(910)는 모든 토큰(F10)에 대해 만료 조건을 만족한 것으로 확인되면, 서비스 어플리케이션 서버(700)에게 토큰(F10)의 사용을 허가할 수 있다(S450).
- [0118] 도 9는 본 발명의 일 실시 예에 따른 하나의 토큰(F10)에 대해 만료 조건을 확인하는 과정을 나타내는 순서도이다.
- [0119] 도 9를 참조하면, 하나의 토큰(F10)에 대해 만료 조건(expiration condition)을 확인하는 상세한 과정을 알 수 있다.
- [0120] 서비스 어플리케이션 서버(700)는 하나의 토큰(F10)으로부터 사용 횟수 값(F410, token usage)을 수집할 수 있다(S411).
- [0121] 분산 서버(910)는 하나의 토큰(F10)으로부터 사용 횟수 값(F410, token usage)을 수집할 수 있다(S411).
- [0122] 분산 서버(910)는 사용 횟수 값(F410, token usage)과 만료 조건의 사용 가능 횟수 값(F430, Available count)을 비교하여 사용 요청이 타당한지 판단할 수 있다(S413).
- [0123] 서비스 어플리케이션 서버(700)는 사용 가능 횟수 값(F430, Available count)이 사용 횟수 값(F410, token usage)보다 작으면, 사용 요청이 부당한 것으로 판단하고(S415), 구매자 단말기(500)의 사용 요청을 거절할 수 있다(S417).
- [0124] 또한, 서비스 어플리케이션 서버(700)는 사용 가능 횟수 값(F430, Available count)이 사용 횟수 값(F410, token usage)보다 크면, 사용 요청이 타당한 것으로 판단하고(S416), 분산 네트워크 시스템(900)에 사용 요청 메시지를 브로드캐스팅(broadcasting)할 수 있다(S418).
- [0125] 도 10은 본 발명의 일 실시 예에 따른 모든 토큰(F10)에 대해 만료 조건을 확인하는 과정을 나타내는 순서도이다.
- [0126] 도 10을 참조하면, 모든 토큰(F10)에 대해 만료 조건(expiration condition)을 확인하는 상세한 과정을 알 수 있다.
- [0127] 분산 서버(910)는 모든 토큰(F10)으로부터 사용 횟수 값(F410, token usage)을 수집할 수 있다(S431).
- [0128] 분산 서버(910)는 토큰(F10)으로부터 수집한 복수 개의 사용 횟수 값(F410, token usage)과 만료 조건의 사용 가능 횟수 값(F430, available count)을 각각 비교하여 사용 요청이 타당한지 검증할 수 있다(S432).
- [0129] 분산 서버(910)는 토큰(F10)으로부터 수집한 적어도 하나 이상의 사용 횟수 값(F410, token usage)이 사용 가능 횟수 값(F430, available count)보다 크면, 토큰(F10)의 마지막 사용 내역에 오류가 있는 것으로 판단할 수 있다(S433).
- [0130] 분산 서버(910)는 토큰(F10)의 마지막 사용 내역에 대한 오류를 분산 네트워크 시스템(900)에 브로드캐스팅(broadcasting)할 수 있고(S435), 토큰(F10)의 마지막 사용 내역을 삭제하고(S437), 구매자 단말기(500)의 사용 요청을 거절할 수 있다(S439).
- [0131] 또한, 분산 서버(910)는 토큰(F10)으로부터 수집한 모든 사용 횟수 값(F410, token usage)이 사용 가능 횟수 값

(F430, available count)보다 작으면, 사용 요청이 타당한 것으로 검증할 수 있다(S434).

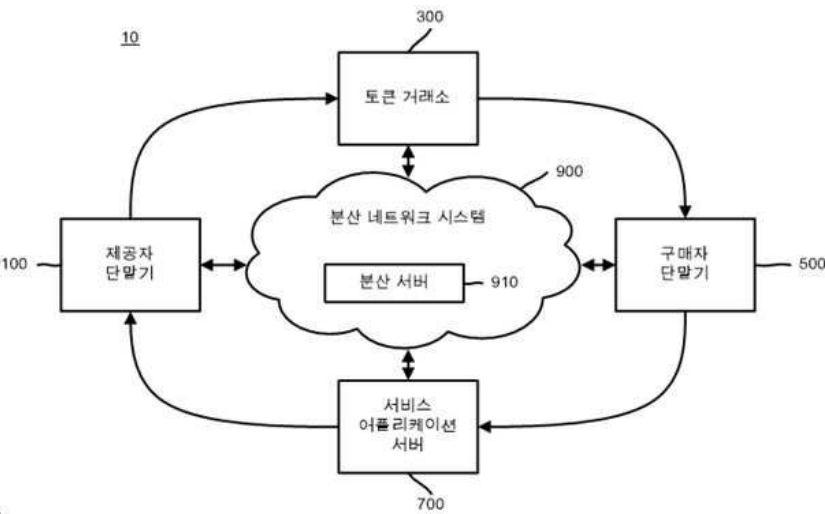
- [0132] 분산 서버(910)는 사용 요청이 타당한 것으로 검증되면, 분산 네트워크 시스템(900)에 존재하는 다른 분산 서버(910)로 브로드캐스팅(broadcasting)할 수 있고(S436), 분산 서버(910)는 서비스 어플리케이션 서버(700)에게 사용 요청을 허가할 수 있다(S438).
- [0133] 이와 같은, 분산 장부에 기반한 개인 정보 접근 권한 거래 방법은 어플리케이션으로 구현되거나 다양한 컴퓨터 구성요소를 통하여 수행될 수 있는 프로그램 명령어의 형태로 구현되어 컴퓨터 판독 가능한 기록 매체에 기록될 수 있다. 컴퓨터 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다.
- [0134] 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.
- [0135] 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.
- [0136] 프로그램 명령어의 예에는, 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.
- [0137] 이상에서 설명한 바와 같이 본 발명에 따른 분산 장부에 기반한 개인 정보 접근 권한 거래 방법은 개인 정보의 유출 없이 개인 정보가 필요한 서비스를 가능하게 하고, 개인 정보의 상품화 및 거래 과정의 신뢰성이 검증될 수 있는 장점이 있다.
- [0138] 이상에서는 실시 예들을 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

- [0140] 10: 개인 정보 접근 권한 거래 시스템
 - 100: 제공자 단말기
 - 300: 토큰 거래소
 - 500: 구매자 단말기
 - 700: 서비스 어플리케이션 서버
 - 900: 분산 네트워크 시스템
 - 910: 분산 서버

도면

도면1



도면2

F10

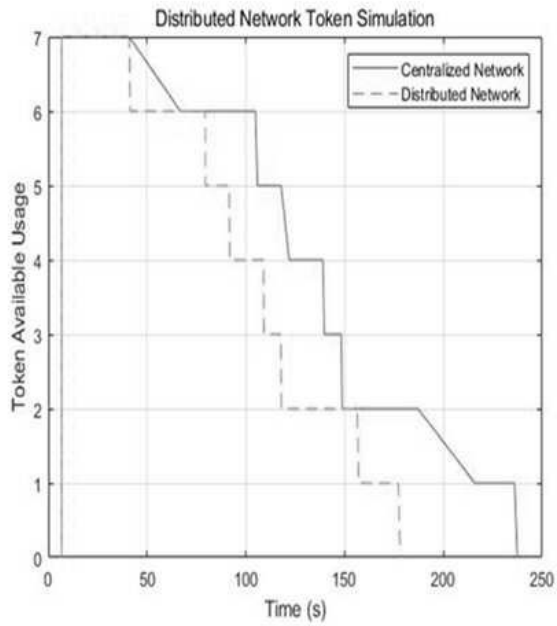
F100	F200	F300	F400	F500	F600
Token Index	User ID	Allowed service ID	Expiration condition	User signature	Publisher signature

도면3

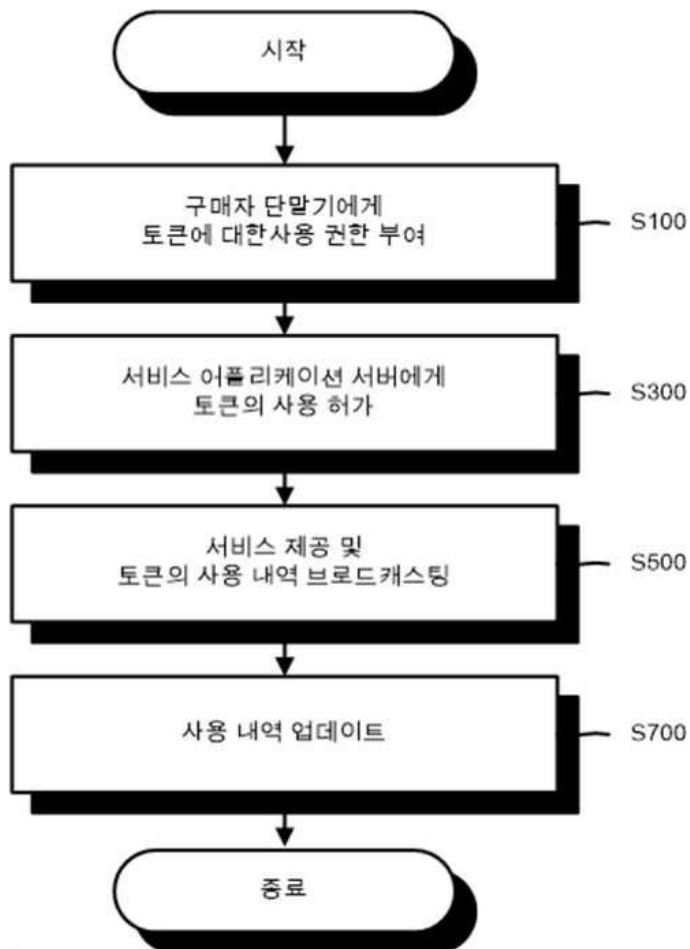
F400

F410	F430	F450
사용 가능 횟수	사용 기한	사용 중지 요청 여부

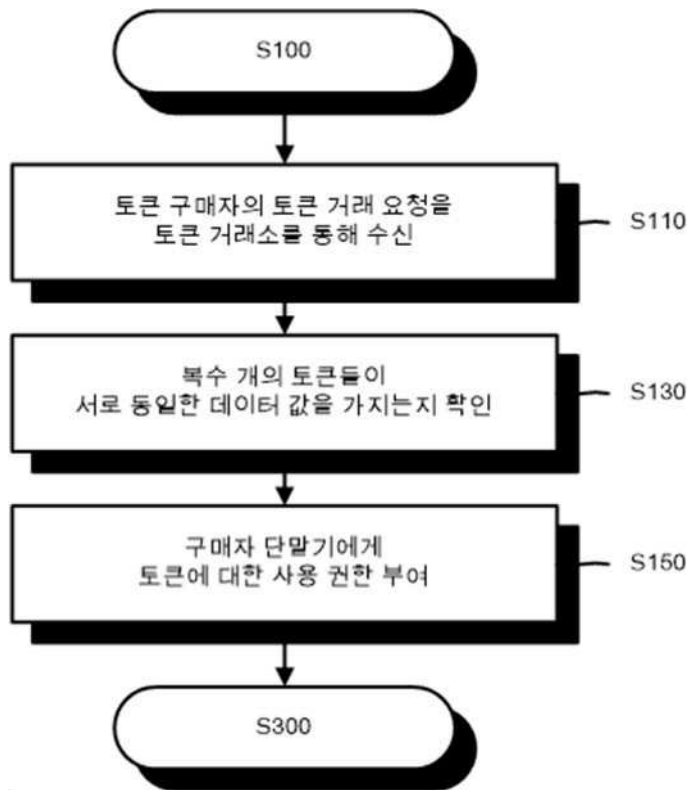
도면4



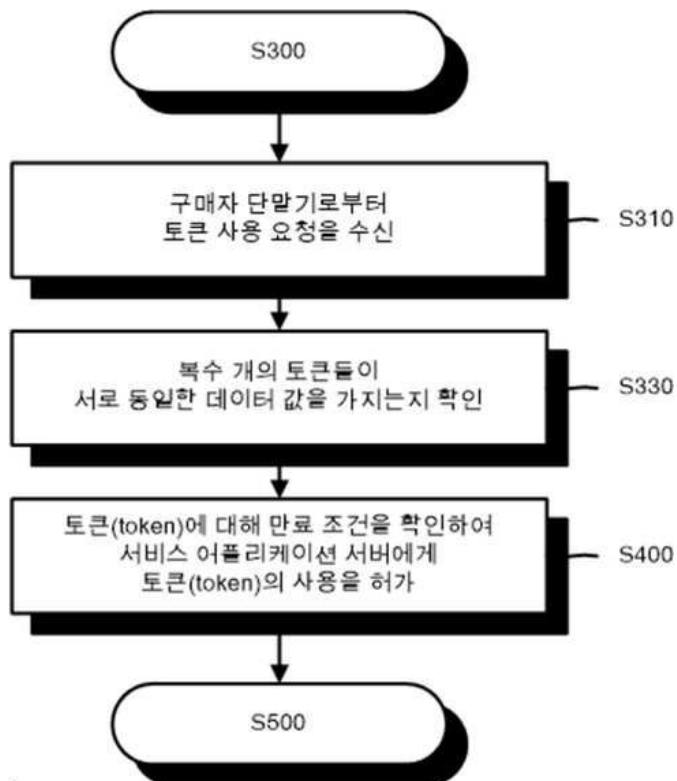
도면5



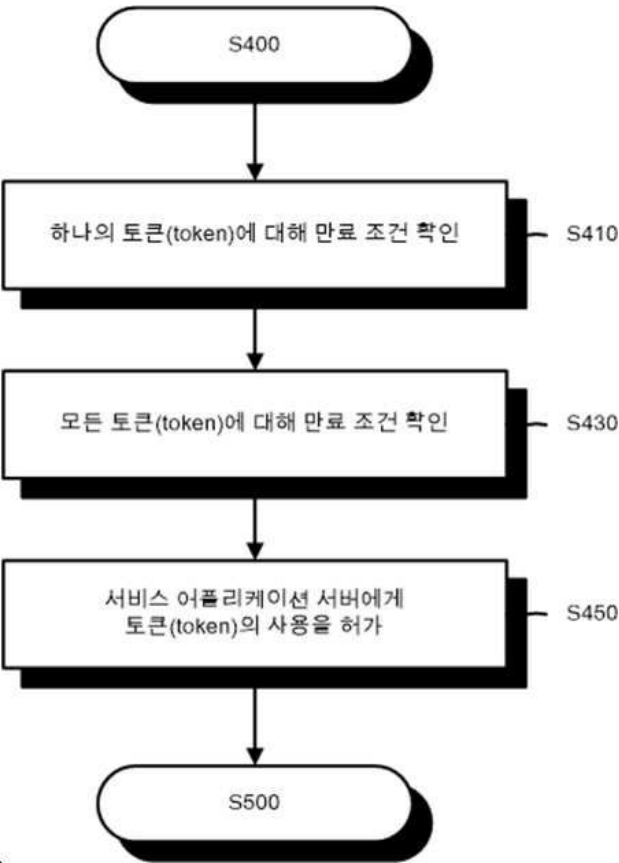
도면6



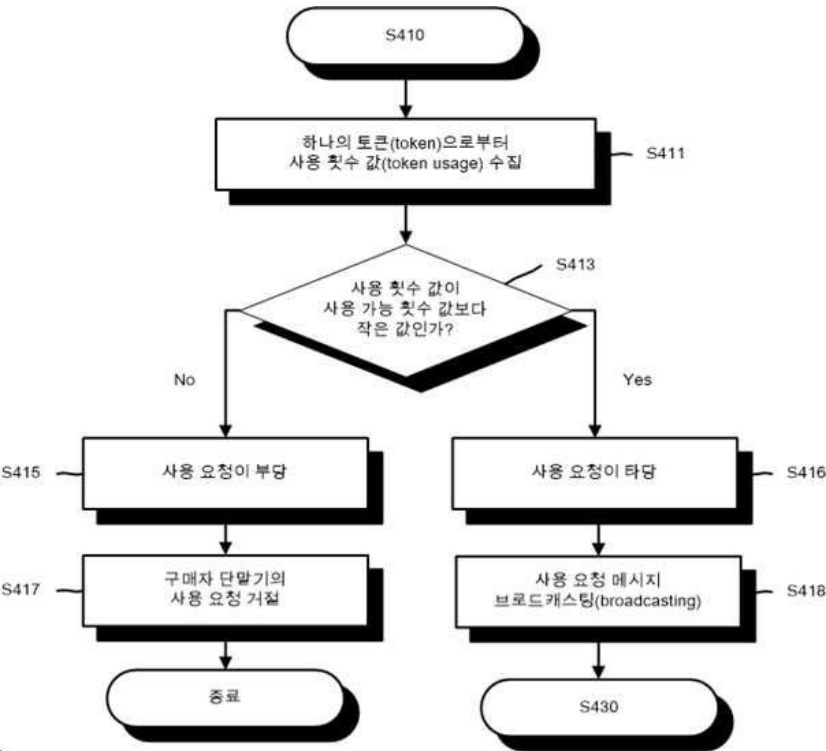
도면7



도면8



도면9



도면10

