(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2025년05월23일
(11) 등록번호 10-2812552
(24) 등록일자 2025년05월21일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *G06F 21/33* (2013.01)
G06F 21/64 (2013.01) *H04L 9/06* (2006.01)
(52) CPC특허분류
H04L 9/3213 (2013.01)
G06F 21/33 (2013.01)
(21) 출원번호 10-2022-0001096
(22) 출원일자 2022년01월04일
심사청구일자 2022년01월04일
(65) 공개번호 10-2023-0105557
(43) 공개일자 2023년07월11일
(56) 선행기술조사문헌
KR1020210090375 A
KR102216311 B1
Jinna Zhang 외 7명. "A Blockchain-Based Trusted Edge Platform in Edge Computing Environment." Sensors 21.6 (2021)

(73) 특허권자
동서대학교 산학협력단
부산광역시 사상구 주례로 47(주례동, 동서대학교)
(72) 발명자
이상곤
부산광역시 서구 대영로45번길 53번지 보현빌리지 803호
위탄도 엘리자베스 나타니아
부산광역시 사상구 진사로36번가길 8-4(주례동) 102호
(74) 대리인
정병홍

전체 청구항 수 : 총 18 항 심사관 : 양종필

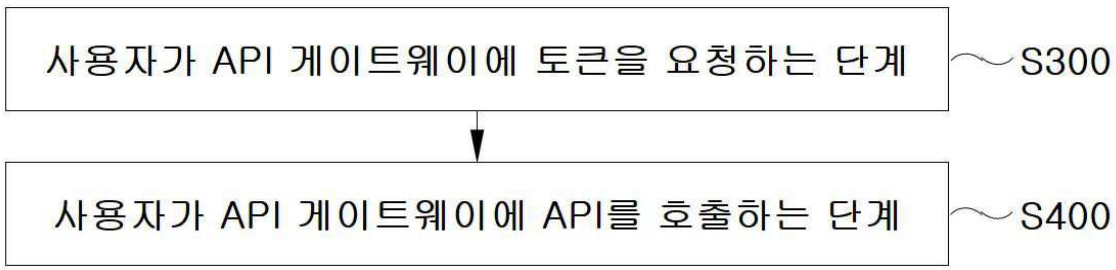
(54) 발명의 명칭 **클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법**

(57) 요 약

본 발명은 컴퓨터시스템이 API 게이트웨이에 토큰을 요청하는 제 300단계 및 상기 컴퓨터시스템이 상기 API 게이트웨이에 API를 호출하는 제 400단계를 포함하고, 상기 제 300단계는 상기 컴퓨터시스템이 암호화 정보 R8을 준비하는 제 301단계, 상기 컴퓨터시스템이 컴퓨터시스템의 블록체인 주소 Addr_u 및 상기 암호화 정보 R8을 상기

(뒷면에 계속)

대 표 도 - 도2



API 게이트웨이에 전송하는 제 302단계, 상기 API 게이트웨이가 암호화 정보 R'8에 대한 검증 프로세스를 수행하는 제 303단계, 상기 제 303단계의 출력값이 참인 경우, 상기 API 게이트웨이가 암호화 정보 R10을 계산하는 제 304단계, 상기 API 게이트웨이가 상기 암호화 정보 R10을 관리모듈로 전송하는 제 305단계, 상기 관리모듈이 암호화 정보 R'10에 대한 검증 프로세스를 수행하는 제 306단계, 상기 관리모듈이 컴퓨터시스템 할당정보 U_rl 및 디지털서명 S7로 구성된 응답 메시지를 상기 API 게이트웨이에 전송하는 제 307단계, 상기 API 게이트웨이가 컴퓨터시스템 할당정보 U'_rl 및 디지털서명 S'7을 검증하는 제 308단계, 상기 API 게이트웨이가 서비스목록 N 및 디지털서명 S8을 상기 컴퓨터시스템에게 전송하는 제 309단계 및 상기 컴퓨터시스템이 디지털서명 S'8에 대한 검증 프로세스를 수행하는 제 310단계를 포함하는 것을 특징으로 한다.

(52) CPC특허분류
G06F 21/64 (2013.01)
H04L 9/0643 (2013.01)
H04L 9/3247 (2013.01)
H04L 9/3263 (2013.01)
H04L 9/3297 (2013.01)
H04L 9/50 (2022.05)

이 발명을 지원한 국가연구개발사업

과제고유번호	2018111070
과제번호	2018R1D1A1B07047601
부처명	교육부
과제관리(전문)기관명	한국연구재단
연구사업명	이공학 개인기초연구지원사업
연구과제명	IoT와 SDN을 위한 종합적 블록체인 프레임 워크
기 여 율	1/1
과제수행기관명	동서대학교 산학협력단
연구기간	2021.03.01 ~ 2022.02.28

명 세 서

청구범위

청구항 1

컴퓨터시스템이 API 게이트웨이에 토큰을 요청하는 제 300단계; 및

상기 컴퓨터시스템이 상기 API 게이트웨이에 API를 호출하는 제 400단계;를 포함하고,

상기 제 300단계는

상기 컴퓨터시스템이 암호화 정보 R8을 준비하는 제 301단계;

상기 컴퓨터시스템이 컴퓨터시스템의 블록체인 주소 Addr_u 및 상기 암호화 정보 R8을 상기 API 게이트웨이에 전송하는 제 302단계;

상기 API 게이트웨이가 암호화 정보 R'8에 대한 검증 프로세스를 수행하는 제 303단계;

상기 제 303단계의 출력값이 참인 경우, 상기 API 게이트웨이가 암호화 정보 R10을 계산하는 제 304단계;

상기 API 게이트웨이가 상기 암호화 정보 R10을 관리모듈로 전송하는 제 305단계;

상기 관리모듈이 암호화 정보 R'10에 대한 검증 프로세스를 수행하는 제 306단계;

상기 관리모듈이 컴퓨터시스템 할당정보 U_rl 및 디지털서명 S7로 구성된 응답 메시지를 상기 API 게이트웨이에 전송하는 제 307단계;

상기 API 게이트웨이가 컴퓨터시스템 할당정보 U'_rl 및 디지털서명 S'7을 검증하는 제 308단계;

상기 API 게이트웨이가 서비스목록 N 및 디지털서명 S8을 상기 컴퓨터시스템에게 전송하는 제 309단계; 및

상기 컴퓨터시스템이 디지털서명 S'8에 대한 검증 프로세스를 수행하는 제 310단계;를 포함하고,

상기 암호화 정보 R'8은 상기 컴퓨터시스템에 의해 생성된 상기 암호화 정보 R8을 상기 API 게이트웨이가 전송받은 경우, 상기 암호화 정보 R8과 구별하기 위해 상기 암호화 정보 R8 대신에 사용되는 정보이고,

상기 암호화 정보 R'10은 상기 API 게이트웨이에 의해 생성된 상기 암호화 정보 R10을 상기 관리모듈이 전송받은 경우, 상기 암호화 정보 R10과 구별하기 위해 상기 암호화 정보 R10 대신에 사용되는 정보이고,

상기 컴퓨터시스템 할당정보 U'_rl은 상기 관리모듈에 의해 획득된 상기 컴퓨터시스템 할당정보 U_rl을 상기 API 게이트웨이가 전송받은 경우, 상기 컴퓨터시스템 할당정보 U_rl과 구별하기 위해 상기 컴퓨터시스템 할당정보 U_rl 대신에 사용되는 정보이고,

상기 디지털서명 S'7은 상기 관리모듈에 의해 생성된 상기 디지털서명 S7을 상기 API 게이트웨이가 전송받은 경우, 상기 디지털서명 S7과 구별하기 위해 상기 디지털서명 S7 대신에 사용되는 정보이고,

상기 디지털서명 S'8은 상기 API 게이트웨이에 의해 생성된 상기 디지털서명 S8을 상기 컴퓨터시스템이 전송받은 경우, 상기 디지털서명 S8과 구별하기 위해 상기 디지털서명 S8 대신에 사용되는 정보인 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.

청구항 2

제 1항에 있어서,

상기 제 301단계는

상기 컴퓨터시스템이 (수학식) R7=U_cred||t을 이용하여, 상기 R7을 준비하는 제 301-1단계;

상기 컴퓨터시스템이 (수학식) H5=H(R7)을 이용하여, 상기 R7의 해시값 H5를 준비하는 제 301-2단계;

상기 컴퓨터시스템이 (수학식) S5=Sign_SK_u(H5)로 상기 컴퓨터시스템의 비밀키 SK_u를 이용하여, 상기 해시값 H5에 대한 디지털서명 S5를 생성하는 제 301-3단계; 및

상기 컴퓨터시스템이 (수학식) R8=E_PK_gw(R7||S5)로 API 게이트웨이의 공개키 PK_gw를 이용하여, 상기 R7 및 디지털서명 S5를 연접한 정보를 암호화한 상기 암호화 정보 R8를 계산하는 제 301-4단계;를 포함하고,

상기 U_cred는 컴퓨터시스템증명서이고, t는 현재의 타임스탬프이고, 상기 R7은 상기 컴퓨터시스템증명서 U_cred 및 상기 현재의 타임스탬프 t를 연접한 정보인 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.

청구항 3

제 1항에 있어서,

상기 제 303단계는

상기 API 게이트웨이가 (수학식) D_SK_gw(R'8) → R'7||S'5에서 상기 API 게이트웨이의 비밀키 SK_gw를 이용하여 상기 암호화 정보 R'8를 복호화하여, 상기 R'7 및 디지털서명 S'5를 획득하는 제 303-1단계;

상기 API 게이트웨이가 (수학식) H'5=H(R'7)을 이용하여, 상기 R'7의 해시값 H'5를 계산하는 제 303-2단계; 및

상기 API 게이트웨이가 (수학식) PKVer_Addr_u(S'5,H'5) → True or False을 이용하여, PKVer_Addr_u 함수에 상기 디지털서명 S'5 및 해시값 H'5를 입력하는 제 303-3단계;를 포함하고,

상기 PKVer_Addr_u(S'5,H'5)는 상기 컴퓨터시스템의 블록체인 주소 Addr_u가 상기 해시값 H'5에 대해 상기 디지털서명 S'5로 검증하는 함수인 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.

청구항 4

제 1항에 있어서,

상기 제 304단계는

상기 API 게이트웨이가 (수학식) R9=Addr_u||U'_cred을 이용하여, 상기 컴퓨터시스템의 블록체인 주소 Addr_u 및 컴퓨터시스템증명서 U'_cred를 연접한 상기 R9를 계산하는 제 304-1단계;

상기 API 게이트웨이가 (수학식) H6=H(R9)을 이용하여, 상기 R9의 해시값 H6을 계산하는 제 304-2단계;

상기 API 게이트웨이가 (수학식) S6=Sign_SK_gw(H6)으로 상기 API 게이트웨이의 비밀키 SK_gw를 이용하여, 상기 해시값 H6에 대한 디지털서명 S6을 생성하는 제 304-3단계;

상기 API 게이트웨이가 (수학식) R10=E_PK_idma(R9||S6)으로 상기 관리모듈의 공개키 PK_idma를 이용하여, 상기 R9 및 디지털서명 S6을 연접한 정보를 암호화한 상기 암호화 정보 R10을 계산하는 제 304-4단계;를 포함하고,

상기 컴퓨터시스템증명서 U'_cred는 상기 API 게이트웨이가 상기 컴퓨터시스템로부터 컴퓨터시스템증명서 U_cred를 전송받은 경우, 상기 컴퓨터시스템증명서 U_cred와 구별하기 위해 상기 컴퓨터시스템증명서 U_cred 대신에 사용되는 정보인 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.

청구항 5

제 1항에 있어서,

상기 제 306단계는

상기 관리모듈이 (수학식) D_SK_idma(R'10) ⇒ R'9||S'6에서 상기 관리모듈의 비밀키 SK_idma를 이용하여 상기 암호화 정보 R'10을 복호화하여, 상기 R'9 및 디지털서명 S'6을 획득하는 제 306-1단계;

상기 관리모듈이 (수학식) H'6=H(R'9)을 이용하여, 상기 R'9의 해시값 H'6을 계산하는 제 306-2단계;

상기 관리모듈이 (수학식) PKVer_PK_gw(S'6,H'6) → True or False을 이용하여, PKVer_PK_gw 함수에 상기 디지털서명 S'6 및 해시값 H'6을 입력하는 제 306-3단계;

상기 관리모듈이 (수학식) R'9=Addr_u||U"_cred를 이용하여, 상기 컴퓨터시스템의 블록체인 주소 Addr_u 및 컴퓨터시스템증명서 U"_cred를 획득하는 제 306-4단계;

상기 제 306-3 단계의 출력값이 참인 경우, 상기 관리모듈이 로컬 데이터베이스에 상기 컴퓨터시스템증명서 U"_cred를 전송하여, 상기 컴퓨터시스템 할당정보 U_rl를 획득하는 제 306-5단계;

상기 관리모듈이 (수학식) H7=H(U_rl)을 이용하여, 상기 컴퓨터시스템 할당정보 U_rl의 해시값 H7을 계산하는 제 306-6단계; 및

상기 관리모듈이 (수학식) S7=Sign_SK_idma(H7)을 이용하여, 상기 관리모듈의 비밀키 SK_idma로 상기 해시값 H7에 대한 상기 디지털서명 S7을 생성하는 제 306-7단계;를 포함하고,

상기 PKVer_PK_gw(S'6,H'6)은 상기 API 게이트웨의 공개키 PK_gw가 상기 해시값 H'6에 대해 상기 디지털서명 S'6으로 검증하는 함수인 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.

청구항 6

제 1항에 있어서,

상기 제 308단계는

상기 API 게이트웨이가 (수학식) H'7=H(U'_rl)을 이용하여, 상기 컴퓨터시스템 할당정보 U'_rl의 해시값 H'7을 계산하는 제 308-1단계;

상기 API 게이트웨이가 (수학식) PKVer_PK_idma(S'7, H'7) → True or False을 이용하여, PKVer_PK_idma 함수에 상기 디지털서명 S'7 및 해시값 H'7을 입력하는 제 308-2단계;

상기 제 308-2단계의 출력값이 참인 경우, 상기 API 게이트웨이가 상기 컴퓨터시스템 할당정보 U'_rl로부터 상기 컴퓨터시스템의 권한을 체크하는 제 308-3단계;

상기 컴퓨터시스템이 API 토큰을 요청할 수 있는 권한을 갖는 경우, 상기 API 게이트웨이가 (수학식) N={n_1, n_2, n_3, ..., n_n}을 이용하여, 상기 서비스목록 N을 준비하는 제 308-4단계;

상기 API 게이트웨이가 (수학식) H8=H(N)을 이용하여, 상기 서비스목록 N의 해시값 H8을 계산하는 제 308-5단계; 및

상기 API 게이트웨이가 (수학식) S8=Sign_SK_gw(H8)로 상기 API 게이트웨이의 비밀키 SK_gw를 이용하여, 상기 해시값 H8에 대한 상기 디지털서명 S8을 생성하는 제 308-6단계;를 포함하고,

상기 PKVer_PK_idma(S'7, H'7)은 상기 관리모듈의 공개키 PK_idma가 상기 해시값 H'7에 대해 상기 디지털서명 S'7으로 검증하는 함수이고,

상기 n_1, n_2, n_3, ..., n_n은 다수의 서비스이고, 상기 서비스목록 N은 다수의 서비스 n_1, n_2, n_3, ..., n_n으로 구성된 목록인 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.

청구항 7

제 1항에 있어서,

상기 제 310단계는

상기 컴퓨터시스템이 (수학식) H'8=H(N')을 이용하여, 서비스목록 N'의 해시값 H'8을 계산하는 제 310-1단계; 및

상기 컴퓨터시스템이 (수학식) PKVer_PK_gw(S'8,H'8) → True or False을 이용하여, PKVer_PK_gw 함수에 상기 디지털서명 S'8 및 해시값 H'8을 입력하는 제 310-2단계;를 포함하고,

상기 서비스목록 N'는 상기 API 게이트웨이에 의해 준비된 서비스목록 N을 상기 컴퓨터시스템이 전송받은 경우, 상기 서비스목록 N과 구별하기 위해 상기 서비스목록 N 대신에 사용되는 정보이고,

상기 PKVer_PK_gw(S'8,H'8)은 상기 API 게이트웨이의 공개키 PK_gw가 상기 해시값 H'8에 대해 상기 디지털서명 S'8로 검증하는 함수인 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.

청구항 8

제 1항에 있어서,

상기 제 300단계는

상기 컴퓨터시스템이 상기 제 310단계의 출력값이 참인 경우, 상기 컴퓨터시스템이 해시값 H9를 계산하는 제 311단계;

상기 컴퓨터시스템이 상기 컴퓨터시스템의 블록체인 주소 Addr_u 및 해시값 H9를 포함하는 트랜잭션정보 Tx4를 제2 스마트계약에 전송하는 제 312단계;

상기 제2 스마트계약이 상기 컴퓨터시스템의 블록체인 주소 Addr_u 및 해시값 H'9를 블록체인에 저장하는 제 313단계;

상기 제2 스마트계약이 상기 API 게이트웨이 및 블록체인의 모든 노드에게 상기 컴퓨터시스템의 블록체인 주소 Addr_u 및 해시값 H'9를 브로드캐스팅하는 제 314단계;

상기 컴퓨터시스템이 디지털서명 S9 및 서비스 요청정보 R12를 계산하는 제 315단계;

상기 컴퓨터시스템이 상기 서비스 요청정보 R12를 상기 API 게이트웨이로 전송하는 제 316단계;

상기 API 게이트웨이가 서비스 요청정보 R'12에 대한 검증 프로세스를 수행하는 제 317단계;

상기 제 317단계의 출력값이 참인 경우, 상기 API 게이트웨이가 R'11을 로컬 데이터베이스에 저장하는 제 318단계;

상기 API 게이트웨이가 서비스목록 O'을 바탕으로 JWT 형식의 컴퓨터시스템토큰 Utoken을 생성하고, (수학식) H10=H(Utoken)을 이용하여, 상기 컴퓨터시스템토큰 Utoken의 해시값 H10을 계산하는 제 319단계; 및

상기 API 게이트웨이가 상기 컴퓨터시스템의 블록체인 주소 Addr_u 및 해시값 H10을 포함하는 트랜잭션정보 Tx5를 제2 스마트계약에 전송하는 제 320단계;를 더 포함하고,

상기 해시값 H'9는 상기 컴퓨터시스템에 의해 생성된 상기 해시값 H9를 상기 제2 스마트계약이 전송받은 경우, 상기 해시값 H9와 구별하기 위해 상기 해시값 H9 대신에 사용되는 정보이고,

상기 서비스 요청정보 R'12는 상기 컴퓨터시스템에 의해 생성된 상기 서비스 요청정보 R12를 상기 API 게이트웨이가 전송받은 경우, 상기 서비스 요청정보 R12와 구별하기 위해 상기 서비스 요청정보 R12 대신에 사용되는 정보이고,

여기서, 상기 서비스목록 O'는 컴퓨터시스템에 의해 생성된 서비스목록 O를 상기 API 게이트웨이가 전송받은 경우, 상기 서비스목록 O와 구별하기 위해 상기 서비스목록 O 대신에 사용되는 정보이고,

상기 컴퓨터시스템토큰 Utoken은 접근토큰 AccessToken 및 상기 접근토큰 AccessToken의 유효기간 Timeexp를 결합한 정보인 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.

청구항 9

제 8항에 있어서,

상기 제 311단계는

상기 컴퓨터시스템이 (수학식) O={o_1, o_2, o_3, ...o_n}, where O⊂N'을 이용하여, 상기 서비스목록 O를 준비하는 제 311-1단계;

상기 컴퓨터시스템이 (수학식) R11=O||t을 이용하여, 상기 서비스목록 O 및 현재의 타임스탬프 t를 연접한 상기 R11을 계산하는 제 311-2단계; 및

상기 컴퓨터시스템이 (수학식) H9=H(R11)을 이용하여, 상기 R11의 해시값 H9를 계산하는 제 311-3단계;를 포함하고,

상기 o_1, o_2, o_3, ...o_n는 상기 컴퓨터시스템이 접근하고자 하는 다수의 서비스이고, 상기 서비스목록 O는 상기 컴퓨터시스템이 접근하고자 하는 서비스목록인 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대

한 토큰 요청 및 API 호출 방법.

청구항 10

제 8항에 있어서,

상기 제 315단계는

상기 컴퓨터시스템이 (수학식) S9=Sign_SK_u(H9)로 상기 컴퓨터시스템의 비밀키 SK_u를 이용하여, 상기 H9에 대한 디지털서명 S9를 생성하는 제 315-1단계; 및

상기 컴퓨터시스템이 (수학식) R12=E_PK_gw(R11||S9)로 상기 API 게이트웨이의 공개키 PK_gw를 이용하여, 상기 R11 및 디지털서명 S9를 연접한 정보를 암호화하여, 상기 서비스 요청정보 R12를 생성하는 제 315-2단계;를 포함하는 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.

청구항 11

제 8항에 있어서,

상기 제 317단계는

상기 API 게이트웨이가 (수학식) D_SK_gw(R'12) → R'11||S'9에서 상기 API 게이트웨이의 비밀키 SK_gw를 이용하여 상기 서비스 요청정보 R'12를 복호화하여, R'11 및 디지털서명 S'9를 획득하는 제 317-1단계;

상기 API 게이트웨이가 (수학식) H"9=H(R'11)을 이용하여, 상기 R'11의 해시값 H"9를 계산하는 제 317-2단계;

상기 API 게이트웨이가 상기 해시값 H"9 및 H'9를 비교하여, 상기 해시값 H"9 및 H'9의 일치 여부를 확인하는 제 317-3단계;

상기 해시값 H"9 및 H'9가 일치 시, 상기 API 게이트웨이가 상기 서비스 요청정보 R'12에 대한 검증 프로세스를 계속하고, 상기 해시값 H"9 및 H'9이 불일치 시, 상기 API 게이트웨이가 상기 서비스 요청정보 R'12에 대한 검증 프로세스를 중단하는 제 317-4단계; 및

상기 API 게이트웨이가 (수학식) PKVerAddr_u(S'9,H"9) → True or False를 이용하여, PKVerAddr_u 함수에 상기 디지털서명 S'9, 해시값 H"9를 입력하는 제 317-5단계;를 포함하고,

상기 PKVerAddr_u(S'9,H"9)는 상기 컴퓨터시스템의 블록체인 주소 Addr_u가 상기 해시값 H"9에 대해 상기 디지털서명 S'9로 검증하는 함수인 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.

청구항 12

제 8항에 있어서,

상기 제 300단계는

상기 제2 스마트계약이 상기 컴퓨터시스템의 블록체인 주소 Addr_u 및 해시값 H'10을 상기 블록체인에 기록하고, 상기 API 게이트웨이 및 상기 블록체인의 모든 노드에게 상기 컴퓨터시스템의 블록체인 주소 Addr_u 및 해시값 H'10을 브로드캐스팅하는 제 321단계;

상기 컴퓨터시스템이 상기 제2 스마트계약으로부터 전송받은 해시값 H'10을 로컬 저장소에 저장하는 제 322단계;

상기 API 게이트웨이가 암호화 정보 R13을 계산하는 제 323단계;

상기 API 게이트웨이가 상기 암호화 정보 R13을 상기 컴퓨터시스템에게 전송하는 제 324단계;

상기 컴퓨터시스템이 암호화 정보 R'13에 대한 검증 프로세스를 수행하는 제 325단계; 및

상기 컴퓨터시스템이 상기 제 325단계의 출력값이 참인 경우, 컴퓨터시스템토큰 U'token을 상기 로컬 저장소에 저장하는 제 326단계;를 포함하고,

상기 해시값 H'10은 상기 제2 스마트계약에 의해 생성된 상기 해시값 H10을 상기 제2 스마트계약이 전송받은 경우, 상기 해시값 H10과 구별하기 위해 상기 해시값 H10 대신에 사용되는 정보이고,

상기 암호화 정보 R'13은 상기 API 게이트웨이에 의해 생성된 상기 암호화 정보 R13을 상기 컴퓨터시스템이 전송받은 경우, 상기 암호화 정보 R13과 구별하기 위해 상기 암호화 정보 R13 대신에 사용되는 정보인 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.

청구항 13

제 12항에 있어서,

상기 제 323단계는

상기 API 게이트웨이가 (수학식) S10=Sign_SK_idma(H10)으로 상기 관리모듈의 비밀키 SK_idma를 이용하여, 상기 해시값 H10에 대한 디지털서명 S10을 생성하는 제 323-1단계; 및

상기 API 게이트웨이가 (수학식) R13=E_Addr_u(Utoken||S10)으로 상기 컴퓨터시스템의 블록체인 주소 Addr_u를 이용하여, 상기 컴퓨터시스템토큰 Utoken 및 디지털서명 S10을 연접한 정보를 암호화하여, 상기 암호화 정보 R13을 생성하는 제 323-2단계;를 포함하는 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.

청구항 14

제 12항에 있어서,

상기 제 325단계는

상기 컴퓨터시스템이 (수학식) D_SK_u(R'13) → U'token||S'10에서 상기 컴퓨터시스템의 비밀키 SK_u를 이용하여 상기 암호화 정보 R'13을 복호화하여, 컴퓨터시스템토큰 U'token 및 디지털서명 S'10을 획득하는 제 325-1단계;

상기 컴퓨터시스템이 (수학식) H"10=H(U'token)을 이용하여, 상기 컴퓨터시스템토큰 U'token의 해시값 H"10을 계산하는 제 325-2단계;

상기 컴퓨터시스템이 상기 컴퓨터시스템에 의해 계산된 상기 해시값 H"10 및 상기 제2 스마트계약에 의해 브로드캐스팅된 상기 해시값 H'10을 비교하여, 상기 해시값 H"10 및 H'10의 일치 여부를 확인하는 제 325-3단계;

상기 컴퓨터시스템이 상기 해시값 H"10 및 H'10이 일치 시, 상기 암호화 정보 R'13에 대한 검증 프로세스를 계속하고, 상기 해시값 H"10 및 H'10이 불일치 시, 상기 암호화 정보 R'13에 대한 검증 프로세스를 중단하는 제 325-4단계; 및

상기 컴퓨터시스템이 (수학식) PKVer_PK_idma(S'10,H"10) → True or False을 이용하여, PKVer_PK_idma 함수에 상기 디지털서명 S'10 및 해시값 H"10을 입력하는 제 325-5단계;를 포함하고,

상기 PKVer_PK_idma(S'10,H"10)은 상기 관리모듈의 공개키 PK_idma가 상기 해시값 H"10에 대해 상기 디지털서명 S'10으로 검증하는 함수인 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.

청구항 15

제 1항에 있어서,

상기 제 400단계는

상기 컴퓨터시스템이 암호화 정보 R15를 준비하는 제 401단계;

상기 컴퓨터시스템이 상기 암호화 정보 R15를 상기 API 게이트웨이에 전송하는 제 402단계;

상기 API 게이트웨이가 암호화 정보 R'15에 대한 검증 프로세스를 수행하는 제 403단계;

상기 제 403단계의 출력값이 참이면, 상기 API 게이트웨이가 접근토큰 AccessToken의 유효기간 Timeexp 및 클라우드 서비스 Q'를 점검하는 제 404단계;

상기 API 게이트웨이가 상기 클라우드 서비스 Q'에 대한 특정 파라미터인 param를 해당 클라우드 서비스에 전송하는 제 405단계;

상기 클라우드 서비스가 결과값 res를 상기 API 게이트웨이로 반환하는 제 406단계; 및

상기 API 게이트웨이가 상기 결과값 res를 상기 컴퓨터시스템로 전송하는 제 407단계;를 포함하고,

상기 암호화 정보 R'15는 상기 컴퓨터시스템에 의해 생성된 상기 암호화 정보 R15를 상기 API 게이트웨이가 전송받은 경우, 상기 암호화 정보 R15와 구별하기 위해 상기 암호화 정보 R15 대신에 사용되는 정보이고,

상기 클라우드 서비스 Q'는 상기 컴퓨터시스템에 의해 준비된 상기 클라우드 서비스 Q를 상기 API 게이트웨이가 전송받은 경우, 상기 클라우드 서비스 Q와 구별하기 위해 상기 클라우드 서비스 Q 대신에 사용되는 서비스인 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.

청구항 16

제 15항에 있어서,

상기 제 401단계는

먼저, 컴퓨터시스템이 (수학식) R14=AccessToken||Q||param||t, where Q∈O를 이용하여, 상기 R14를 준비하는 제 401-1단계;

상기 컴퓨터시스템이 (수학식) H11=H(R14)를 이용하여, 상기 R14의 해시값 H11을 준비하는 제 401-2단계;

상기 컴퓨터시스템이 (수학식) S11=Sign_SK_u(H11)으로 상기 컴퓨터시스템의 비밀키 SK_u를 이용하여, 상기 H11에 대한 디지털서명 S11을 생성하는 제 401-3단계; 및

상기 컴퓨터시스템이 (수학식) R15=E_PK_gw(R14||S11)으로 상기 게이트웨이의 공개키 PK_gw를 이용하여, 상기 R14 및 디지털서서명 S11를 연접한 정보를 암호화한 상기 암호화 정보 R15를 생성하는 제 401-4단계;를 포함하고,

상기 AccessToken는 상기 컴퓨터시스템의 접근토큰이고, 상기 클라우드 서비스 Q는 서비스목록 O에 포함되고, 클라우드 플랫폼에서 제공하는 서비스이고, 상기 param은 상기 클라우드 서비스 Q에 대한 특정 파라미터이고, 상기 t는 현재의 타임스탬프이고, 상기 R14는 상기 접근토큰 AccessToken, 클라우드 서비스 Q, 파라미터 param 및 현재의 타임스탬프 t를 연접한 정보인 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.

청구항 17

제 15항에 있어서,

상기 제 403단계는

상기 API 게이트웨이가 (수학식) D_SK_gw(R'15) → R'14||S'11에서 상기 API 게이트웨이의 비밀키 SK_gw를 이용하여 상기 암호화 정보 R'15을 복호화하여, 상기 R'14 및 디지털서명 S'11을 획득하는 제 403-1단계;

상기 API 게이트웨이가 (수학식) H'11=H(R'14)를 이용하여, 상기 R'14의 해시값 H'11을 계산하는 제 403-2단계;

상기 API 게이트웨이가 (수학식) PKVer_Addr_u(S'11,H'11) → True or False을 이용하여, PKVer_Addr_u 함수에 디지털서명 S'11, 해시값 H'11을 입력하는 제 403-3단계;를 포함하고,

상기 PKVer_Addr_u(S'11,H'11)은 상기 컴퓨터시스템의 블록체인 주소 Addr_u가 상기 해시값 H'11에 대해 상기 디지털서명 S'11으로 검증하는 함수인 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.

청구항 18

제 15항에 있어서,

상기 제 404단계는

상기 API 게이트웨이가 상기 접근토큰 AccessToken의 유효기간 Timeexp의 만료 여부를 로컬 데이터베이스 내에서 점검하는 제 404-1단계;

상기 API 게이트웨이가 클라우드 서비스 Q'가 상기 컴퓨터시스템이 접근하고자 하는 서비스목록 O의 구성원이

맞는지 상기 로컬 데이터베이스 내에서 점검하는 제 404-2단계; 및

상기 제 404-1 단계 및 제 404-2 단계 모두 충족되는 경우, 상기 API 게이트웨이가 (수학식) JWTVer(AccessToken, SK_gw)를 이용하여, JWTVer 함수에 상기 접근토큰 AccessToken 및 상기 API 게이트웨이의 비밀키 SK_gw를 입력하여, 상기 접근토큰 AccessToken의 유효성을 검증하는 제 404-3단계;를 포함하는 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 토큰 요청 및 API 호출 방법에 관한 것으로, 더욱 자세하게는 클라우드 기반의 인공지능 시스템에서 블록체인 및 스마트계약을 이용하여, 데이터의 무결성을 강화하고, 보안성을 향상시킬 수 있는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법에 관한 것이다.

배 경 기 술

[0002] 인공지능(AI, Artificial Intelligence)은 1956년에 도입된 이후, 발전을 거듭하고 있다. 인공지능 알파고는 2016년에 세계 바둑 챔피언을 5번 연속으로 이겼다. 그리고, 구글은 2018년에 아리조나주 피닉스사에서 분사한 웨이모사의 자율주행 택시 서비스를 출시했다. 그리고, 인공지능은 국가 안보, 금융, 의료, 형사 사법, 교통, 스마트 도시와 같은 다른 분야도 변화시킬 수 있다.

[0003] 그러나, 인공지능은 자율주행차에 대한 공격 등의 적대적인 사례에 적용될 수 있다. 예를 들어, 인공지능은 소수의 픽셀이 변경된 정지신호 이미지를 오분류하여, 자동차 사고를 유발할 수 있다. 그리고, 중앙 서버에서 인공지능에 의해 제어되는 다수의 로봇에 대한 공격은 대규모의 치명적인 장애를 유발할 수 있다. 따라서, 인공지능 시스템을 개발 시, 인공지능 시스템의 보안에 더 많은 노력을 기울여야 한다.

[0004] 최근 들어, 학습데이터를 이용하여, 기계학습 모델을 학습시킬 수 있는 클라우드 기반의 인공지능 시스템이 적극적으로 도입되고 있다.

[0005] 그러나, 기존의 클라우드 기반의 인공지능 시스템에서는 데이터의 무결성(Data Integrity) 및 개인정보의 보호에 취약하다는 문제점이 있었다.

[0006] 또한, 기존의 클라우드 기반의 인공지능 시스템에서는 클라우드 컴퓨팅(Cloud Computing)의 취약성으로 인해 인공지능 서비스의 보안에 악영향을 미치고, 잠재적으로 데이터를 손상시킬 수 있다는 문제점이 있었다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) KR 10-1914416 B1

발명의 내용

해결하려는 과제

[0008] 본 발명은 상기와 같은 문제점을 해결하기 위하여 안출된 것으로, 본 발명의 목적은 블록체인 및 스마트 계약을 기반으로 하는 아키텍처를 통합하여, 클라우드 기반의 인공지능 시스템의 머신러닝 파이프라인에 대한 무결성을 강화한 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법을 제공하는데 있다.

[0009] 또한, 본 발명의 목적은 공격자가 실제 컴퓨터시스템을 사칭하여 클라우드 기반의 인공지능 시스템에 침입하는 것을 사전에 방지할 수 있는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법을 제공하는데 있다.

[0010] 또한, 본 발명의 목적은 데이터의 무결성을 추적하고, 데이터 조작을 방지할 수 있는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법을 제공하는데 있다.

과제의 해결 수단

[0011] 상기와 같은 기술적인 문제점을 해결하기 위하여, 본 발명에 의한 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법은 컴퓨터시스템이 API 게이트웨이에 토큰을 요청하는 제 300단계 및 상기 컴퓨터시스템이 상기 API 게이트웨이에 API를 호출하는 제 400단계를 포함하고, 상기 제 300단계는 상기 컴퓨터시스템이 암호화 정보 R8을 준비하는 제 301단계, 상기 컴퓨터시스템이 컴퓨터시스템의 블록체인 주소 Addr_u 및 상기 암호화 정보 R8을 상기 API 게이트웨이에 전송하는 제 302단계, 상기 API 게이트웨이가 암호화 정보 R'8에 대한 검증 프로세스를 수행하는 제 303단계, 상기 제 303단계의 출력값이 참인 경우, 상기 API 게이트웨이가 암호화 정보 R10을 계산하는 제 304단계, 상기 API 게이트웨이가 상기 암호화 정보 R10을 관리모듈로 전송하는 제 305단계, 상기 관리모듈이 암호화 정보 R'10에 대한 검증 프로세스를 수행하는 제 306단계, 상기 관리모듈이 컴퓨터시스템 할당정보 U_rl 및 디지털서명 S7로 구성된 응답 메시지를 상기 API 게이트웨이에 전송하는 제 307단계, 상기 API 게이트웨이가 컴퓨터시스템 할당정보 U'_rl 및 디지털서명 S'7을 검증하는 제 308단계, 상기 API 게이트웨이가 서비스목록 N 및 디지털서명 S8을 상기 컴퓨터시스템에게 전송하는 제 309단계 및 상기 컴퓨터시스템이 디지털서명 S'8에 대한 검증 프로세스를 수행하는 제 310단계를 포함하고, 상기 암호화 정보 R'8은 상기 컴퓨터시스템에 의해 생성된 상기 암호화 정보 R8을 상기 API 게이트웨이가 전송받은 경우, 상기 암호화 정보 R8과 구별하기 위해 상기 암호화 정보 R8 대신에 사용되는 정보이고, 상기 암호화 정보 R'10은 상기 API 게이트웨이에 의해 생성된 상기 암호화 정보 R10을 상기 관리모듈이 전송받은 경우, 상기 암호화 정보 R10과 구별하기 위해 상기 암호화 정보 R10 대신에 사용되는 정보이고, 상기 컴퓨터시스템 할당정보 U'_rl은 상기 관리모듈에 의해 획득된 상기 컴퓨터시스템 할당정보 U_rl을 상기 API 게이트웨이가 전송받은 경우, 상기 컴퓨터시스템 할당정보 U_rl과 구별하기 위해 상기 컴퓨터시스템 할당정보 U_rl 대신에 사용되는 정보이고, 상기 디지털서명 S'7은 상기 관리모듈에 의해 생성된 상기 디지털서명 S7을 상기 API 게이트웨이가 전송받은 경우, 상기 디지털서명 S7과 구별하기 위해 상기 디지털서명 S7 대신에 사용되는 정보이고, 상기 디지털서명 S'8은 상기 API 게이트웨이에 의해 생성된 상기 디지털서명 S8을 상기 컴퓨터시스템이 전송받은 경우, 상기 디지털서명 S8과 구별하기 위해 상기 디지털서명 S8 대신에 사용되는 정보인 것을 특징으로 한다.

[0012] 또한, 상기 제 301단계는 상기 컴퓨터시스템이 (수학식) R7=U_cred||t을 이용하여, 상기 R7을 준비하는 제 301-1단계, 상기 컴퓨터시스템이 (수학식) H5=H(R7)을 이용하여, 상기 R7의 해시값 H5를 준비하는 제 301-2단계, 상기 컴퓨터시스템이 (수학식) S5=Sign_SK_u(H5)로 상기 컴퓨터시스템의 비밀키 SK_u를 이용하여, 상기 해시값 H5에 대한 상기 디지털서명 S5를 생성하는 제 301-3단계 및 상기 컴퓨터시스템이 (수학식) R8=E_PK_gw(R7||S5)로 API 게이트웨이의 공개키 PK_gw를 이용하여, 상기 R7 및 디지털서명 S5를 연접한 정보를 암호화한 상기 암호화 정보 R8를 계산하는 제 301-4단계를 포함하고, 상기 U_cred는 컴퓨터시스템증명서이고, t는 현재의 타임스탬프이고, 상기 R7은 상기 컴퓨터시스템증명서 U_cred 및 상기 현재의 타임스탬프 t를 연접한 정보인 것을 특징으로 한다.

[0013] 또한, 상기 제 303단계는 상기 API 게이트웨이가 (수학식) D_SK_gw(R'8) → R'7||S'5에서 상기 API 게이트웨이의 비밀키 SK_gw를 이용하여 상기 암호화 정보 R'8를 복호화하여, 상기 R'7 및 디지털서명 S'5를 획득하는 제 303-1단계, 상기 API 게이트웨이가 (수학식) H'5=H(R'7)을 이용하여, 상기 R'7의 해시값 H'5를 계산하는 제 303-2단계 및 상기 API 게이트웨이가 (수학식) PKVer_Addr_u(S'5,H'5) → True or False을 이용하여, PKVer_Addr_u 함수에 상기 디지털서명 S'5 및 해시값 H'5를 입력하는 제 303-3단계를 포함하고, 상기 PKVer_Addr_u(S'5,H'5)는 상기 컴퓨터시스템의 블록체인 주소 Addr_u가 상기 해시값 H'5에 대해 상기 디지털서명 S'5로 검증하는 함수인 것을 특징으로 한다.

[0014] 또한, 상기 제 304단계는 상기 API 게이트웨이가 (수학식) R9=Addr_u||U'_cred을 이용하여, 상기 컴퓨터시스템의 블록체인 주소 Addr_u 및 컴퓨터시스템증명서 U'_cred를 연접한 상기 R9를 계산하는 제 304-1단계,

[0015] 상기 API 게이트웨이가 (수학식) H6=H(R9)을 이용하여, 상기 R9의 해시값 H6을 계산하는 제 304-2단계, 상기 API 게이트웨이가 (수학식) S6=Sign_SK_gw(H6)으로 상기 API 게이트웨이의 비밀키 SK_gw를 이용하여, 상기 해시값 H6에 대한 상기 디지털서명 S6을 생성하는 제 304-3단계, 상기 API 게이트웨이가 (수학식) R10=E_PK_idma(R9||S6)으로 상기 관리모듈의 공개키 PK_idma를 이용하여, 상기 R9 및 디지털서명 S6을 연접한 정보를 암호화한 상기 암호화 정보 R10을 계산하는 제 304-4단계를 포함하고, 상기 컴퓨터시스템증명서 U'_cred는 상기 API 게이트웨이가 상기 컴퓨터시스템로부터 상기 컴퓨터시스템증명서 U_cred를 전송받은 경우, 상기 컴퓨터시스템증명서 U_cred와 구별하기 위해 상기 컴퓨터시스템증명서 U_cred 대신에 사용되는 정보인 것을 특징으로 한다.

[0016] 또한, 상기 제 306단계는 상기 관리모듈이 (수학식) D_SK_idma(R'10) ⇒ R'9||S'6에서 상기 관리모듈의 비밀키 SK_idma를 이용하여 상기 암호화 정보 R'10을 복호화하여, 상기 R'9 및 디지털서명 S'6을 획득하는 제 306-1단계, 상기 관리모듈이 (수학식) H'6=H(R'9)을 이용하여, 상기 R'9의 해시값 H'6을 계산하는 제 306-2단계, 상기 관리모듈이 (수학식) PKVer_PK_gw(S'6,H'6) → True or False을 이용하여, PKVer_PK_gw 함수에 상기 디지털서명 S'6 및 해시값 H'6을 입력하는 제 306-3단계, 상기 관리모듈이 (수학식) R'9=Addr_u||U""_cred를 이용하여, 상기 컴퓨터시스템의 블록체인 주소 Addr_u 및 컴퓨터시스템증명서 U""_cred를 획득하는 제 306-4단계, 상기 S306-3 단계의 출력값이 참인 경우, 상기 관리모듈이 로컬 데이터베이스에 상기 컴퓨터시스템증명서 U""_cred를 전송하여, 상기 컴퓨터시스템 할당정보 U_rl를 획득하는 제 306-5단계, 상기 관리모듈이 (수학식) H7=H(U_rl)을 이용하여, 상기 컴퓨터시스템 할당정보 U_rl의 해시값 H7을 계산하는 제 306-6단계 및 상기 관리모듈이 (수학식) S7=Sign_SK_idma(H7)을 이용하여, 상기 관리모듈의 비밀키 SK_idma로 상기 해시값 H7에 대한 상기 디지털서명 S7을 생성하는 제 306-7단계를 포함하고, 상기 PKVer_PK_gw(S'6,H'6)은 상기 API 게이트웨의 공개키 PK_gw가 상기 해시값 H'6에 대해 상기 디지털서명 S'6으로 검증하는 함수인 것을 특징으로 한다.

[0017] 또한, 상기 제 308단계는 상기 API 게이트웨이가 (수학식) H'7=H(U'_rl)을 이용하여, 상기 컴퓨터시스템 할당정보 U'_rl의 해시값 H'7을 계산하는 제 308-1단계, 상기 API 게이트웨이가 (수학식) PKVer_PK_idma(S'7, H'7) → True or False을 이용하여, PKVer_PK_idma 함수에 상기 디지털서명 S'7 및 해시값 H'7을 입력하는 제 308-2단계, 상기 제 308-2단계의 출력값이 참인 경우, 상기 API 게이트웨이가 상기 컴퓨터시스템 할당정보 U'_rl로부터 상기 컴퓨터시스템의 권한을 체크하는 제 308-3단계, 상기 컴퓨터시스템이 API 토큰을 요청할 수 있는 권한을 갖는 경우, 상기 API 게이트웨이가 (수학식) N=n_1, n_2, n_3, ..., n_n을 이용하여, 상기 서비스목록 N을 준비하는 제 308-4단계, 상기 API 게이트웨이가 (수학식) H8=H(N)을 이용하여, 상기 서비스목록 N의 해시값 H8을 계산하는 제 308-5단계 및 상기 API 게이트웨이가 (수학식) S8=Sign_SK_gw(H8)로 상기 API 게이트웨이의 비밀키 SK_gw를 이용하여, 상기 해시값 H8에 대한 상기 디지털서명 S8을 생성하는 제 308-6단계를 포함하고, 상기 PKVer_PK_idma(S'7, H'7)은 상기 관리모듈의 공개키 PK_idma가 상기 해시값 H'7에 대해 상기 디지털서명 S'7로 검증하는 함수이고, 상기 n_1, n_2, n_3, ..., n_n은 다수의 서비스이고, 상기 서비스목록 N은 다수의 서비스 n_1, n_2, n_3, ..., n_n으로 구성된 목록인 것을 특징으로 한다.

[0018] 또한, 상기 제 310단계는 상기 컴퓨터시스템이 (수학식) H'8=H(N')을 이용하여, 서비스목록 N'의 해시값 H'8을 계산하는 제 310-1단계 및 상기 컴퓨터시스템이 (수학식) PKVer_PK_gw(S'8,H'8) → True or False을 이용하여, PKVer_PK_gw 함수에 상기 디지털서명 S'8 및 해시값 H'8을 입력하는 제 310-2단계를 포함하고, 상기 서비스목록 N'는 상기 API 게이트웨이에 의해 준비된 서비스목록 N을 상기 컴퓨터시스템이 전송받은 경우, 상기 서비스목록 N과 구별하기 위해 상기 서비스목록 N 대신에 사용되는 정보이고, 상기 PKVer_PK_gw(S'8,H'8)은 상기 API 게이트웨이의 공개키 PK_gw가 상기 해시값 H'8에 대해 상기 디지털서명 S'8로 검증하는 함수인 것을 특징으로 한다.

[0019] 또한, 상기 제 300단계는 상기 컴퓨터시스템이 상기 제 310단계의 출력값이 참인 경우, 상기 컴퓨터시스템이 해시값 H9를 계산하는 제 311단계, 상기 컴퓨터시스템이 상기 컴퓨터시스템의 블록체인 주소 Addr_u 및 해시값 H9를 포함하는 트랜잭션정보 Tx4를 제2 스마트계약에 전송하는 제 312단계, 상기 제2 스마트계약이 상기 컴퓨터시스템의 블록체인 주소 Addr_u 및 해시값 H'9를 블록체인에 저장하는 제 313단계, 상기 제2 스마트계약이 상기 API 게이트웨이 및 블록체인의 모든 노드에게 상기 컴퓨터시스템의 블록체인 주소 Addr_u 및 해시값 H'9를 브로드캐스팅하는 제 314단계, 상기 컴퓨터시스템이 디지털서명 S9 및 서비스 요청정보 R12를 계산하는 제 315단계, 상기 컴퓨터시스템이 상기 서비스 요청정보 R12를 상기 API 게이트웨이로 전송하는 제 316단계, 상기 API 게이트웨이가 상기 서비스 요청정보 R'12에 대한 검증 프로세스를 수행하는 제 317단계, 상기 제 317단계의 출력값이 참인 경우, 상기 API 게이트웨이가 R'11을 로컬 데이터베이스에 저장하는 제 318단계, 상기 API 게이트웨이가 서비스목록 O'을 바탕으로 JWT 형식의 컴퓨터시스템토큰 Utoken을 생성하고, (수학식) H10=H(Utoken)을 이용하여, 상기 컴퓨터시스템토큰 Utoken의 해시값 H10을 계산하는 제 319단계 및 상기 API 게이트웨이가 상기 컴퓨터시스템의 블록체인 주소 Addr_u 및 해시값 H10을 포함하는 트랜잭션정보 Tx5를 제2 스마트계약에 전송하는 제 320단계를 더 포함하고, 상기 해시값 H'9는 상기 컴퓨터시스템에 의해 생성된 상기 해시값 H9를 상기 제2 스마트계약이 전송받은 경우, 상기 해시값 H9와 구별하기 위해 상기 해시값 H9 대신에 사용되는 정보이고, 상기 서비스 요청정보 R'12는 상기 컴퓨터시스템에 의해 생성된 상기 서비스 요청정보 R12를 상기 API 게이트웨이가 전송받은 경우, 상기 서비스 요청정보 R12와 구별하기 위해 상기 서비스 요청정보 R12 대신에 사용되는 정보이고, 여기서, 상기 서비스목록 O'는 컴퓨터시스템에 의해 생성된 서비스목록 O를 상기 API 게이트웨이가 전송받은 경우, 상기 서비스목록 O와 구별하기 위해 상기 서비스목록 O 대신에 사용되는 정보이고, 상기 컴퓨터시스템토큰 Utoken은 접근토큰 AccessToken 및 상기 접근토큰 AccessToken의 유효기간 Timeexp를 결합한 정보인 것을 특징

으로 한다.

[0020] 또한, 상기 제 311단계는 상기 컴퓨터시스템이 (수학식) O=o_1, o_2, o_3, ...o_n, where O⊂N'을 이용하여, 상기 서비스목록 O를 준비하는 제 311-1단계, 상기 컴퓨터시스템이 (수학식) R11=O||t을 이용하여, 상기 서비스 목록 O 및 현재의 타임스탬프 t를 연접한 상기 R11을 계산하는 제 311-2단계 및 상기 컴퓨터시스템이 (수학식) H9=H(R11)을 이용하여, 상기 R11의 해시값 H9를 계산하는 제 311-3단계를 포함하고, 상기 o_1, o_2, o_3, ...o_n는 상기 컴퓨터시스템이 접근하고자 하는 다수의 서비스이고, 상기 서비스목록 O는 상기 컴퓨터시스템이 접근하고자 하는 서비스목록인 것을 특징으로 한다.

[0021] 또한, 상기 제 315단계는 상기 컴퓨터시스템이 (수학식) S9=Sign_SK_u(H9)로 상기 컴퓨터시스템의 비밀키 SK_u를 이용하여, 상기 H9에 대한 디지털서명 S9를 생성하는 제 315-1단계 및 상기 컴퓨터시스템이 (수학식) R12=E_PK_gw(R11||S9)로 상기 API 게이트웨이의 공개키 PK_gw를 이용하여, 상기 R11 및 디지털서명 S9를 연접한 정보를 암호화하여, 상기 서비스 요청정보 R12를 생성하는 제 315-2단계를 포함하는 것을 특징으로 한다.

[0022] 또한, 상기 제 317단계는 상기 API 게이트웨이가 (수학식) D_SK_gw(R'12) → R'11||S'9에서 상기 API 게이트웨이의 비밀키 SK_gw를 이용하여 상기 서비스 요청정보 R'12를 복호화하여, R'11 및 디지털서명 S'9를 획득하는 제 317-1단계, 상기 API 게이트웨이가 (수학식) H""9=H(R'11)을 이용하여, 상기 R'11의 해시값 H""9를 계산하는 제 317-2단계, 상기 API 게이트웨이가 상기 해시값 H""9 및 H'9를 비교하여, 상기 해시값 H""9 및 H'9의 일치 여부를 확인하는 제 317-3단계, 상기 해시값 H""9 및 H'9가 일치 시, 상기 API 게이트웨이가 상기 서비스 요청정보 R'12에 대한 검증 프로세스를 계속하고, 상기 해시값 H""9 및 H'9이 불일치 시, 상기 API 게이트웨이가 상기 서비스 요청정보 R'12에 대한 검증 프로세스를 중단하는 제 317-4단계 및 상기 API 게이트웨이가 (수학식) PKVerAddr_u(S'9,H""9) → True or False를 이용하여, PKVerAddr_u 함수에 상기 디지털서명 S'9, 해시값 H""9를 입력하는 제 317-5단계를 포함하고, 상기 PKVerAddr_u(S'9,H"9)는 상기 컴퓨터시스템의 블록체인 주소 Addr_u가 상기 해시값 H"9에 대해 상기 디지털서명 S'9로 검증하는 함수인 것을 특징으로 한다.

[0023] 또한, 상기 제 300단계는 상기 제2 스마트계약이 상기 컴퓨터시스템의 블록체인 주소 Addr_u 및 해시값 H'10을 상기 블록체인에 기록하고, 상기 API 게이트웨이 및 상기 블록체인의 모든 노드에게 상기 컴퓨터시스템의 블록체인 주소 Addr_u 및 해시값 H'10을 브로드캐스팅하는 제 321단계, 상기 컴퓨터시스템이 상기 제2 스마트계약으로부터 전송받은 해시값 H'10을 로컬 저장소에 저장하는 제 322단계, 상기 API 게이트웨이가 암호화 정보 R13을 계산하는 제 323단계, 상기 API 게이트웨이가 상기 암호화 정보 R13을 상기 컴퓨터시스템에게 전송하는 제 324단계, 상기 컴퓨터시스템이 암호화 정보 R'13에 대한 검증 프로세스를 수행하는 제 325단계 및 상기 컴퓨터시스템이 상기 제 325단계의 출력값이 참인 경우, 컴퓨터시스템토큰 U'token을 상기 로컬 저장소에 저장하는 제 326단계를 포함하고, 상기 해시값 H'10은 상기 제2 스마트계약에 의해 생성된 상기 해시값 H10을 상기 제2 스마트계약이 전송받은 경우, 상기 해시값 H10과 구별하기 위해 상기 해시값 H10 대신에 사용되는 정보이고, 상기 암호화 정보 R'13은 상기 API 게이트웨이에 의해 생성된 상기 암호화 정보 R13을 상기 컴퓨터시스템이 전송받은 경우, 상기 암호화 정보 R13과 구별하기 위해 상기 암호화 정보 R13 대신에 사용되는 정보인 것을 특징으로 한다.

[0024] 또한, 상기 제 323단계는 상기 API 게이트웨이가 (수학식) S10=Sign_SK_idma(H10)으로 상기 관리모듈의 비밀키 SK_idma를 이용하여, 상기 해시값 H10에 대한 상기 디지털서명 S10을 생성하는 제 323-1단계 및 상기 API 게이트웨이가 (수학식) R13=E_Addr_u(Utoken||S10)으로 상기 컴퓨터시스템의 블록체인 주소 Addr_u를 이용하여, 상기 컴퓨터시스템토큰 Utoken 및 디지털서명 S10을 연접한 정보를 암호화하여, 상기 암호화 정보 R13을 생성하는 제 323-2단계를 포함하는 것을 특징으로 한다.

[0025] 또한, 상기 제 325단계는 상기 컴퓨터시스템이 (수학식) D_SK_u(R'13) → U'token||S'10에서 상기 컴퓨터시스템의 비밀키 SK_u를 이용하여 상기 암호화 정보 R'13을 복호화하여, 컴퓨터시스템토큰 U'token 및 디지털서명 S'10을 획득하는 제 325-1단계, 상기 컴퓨터시스템이 (수학식) H""10=H(U'token)을 이용하여, 상기 컴퓨터시스템토큰 U'token의 해시값 H""10을 계산하는 제 325-2단계, 상기 컴퓨터시스템이 상기 컴퓨터시스템에 의해 계산된 상기 해시값 H""10 및 상기 제2 스마트계약에 의해 브로드캐스팅된 상기 해시값 H'10을 비교하여, 상기 해시값 H""10 및 H'10의 일치 여부를 확인하는 제 325-3단계, 상기 컴퓨터시스템이 상기 해시값 H""10 및 H'10이 일치 시, 상기 암호화 정보 R'13에 대한 검증 프로세스를 계속하고, 상기 해시값 H""10 및 H'10이 불일치 시, 상기 암호화 정보 R'13에 대한 검증 프로세스를 중단하는 제 325-4단계 및 상기 컴퓨터시스템이 (수학식) PKVer_PK_idma(S'10,H"10) → True or False을 이용하여, PKVer_PK_idma 함수에 상기 디지털서명 S'10 및 해시값 H"10을 입력하는 제 325-5단계를 포함하고, 상기 PKVer_PK_idma(S'10,H"10)은 상기 관리모듈의 공개키

PK_idma가 상기 해시값 H"10에 대해 상기 디지털서명 S'10으로 검증하는 함수인 것을 특징으로 한다.

[0026] 또한, 상기 제 400단계는 상기 컴퓨터시스템이 암호화 정보 R15를 준비하는 제 401단계, 상기 컴퓨터시스템이 상기 암호화 정보 R15를 상기 API 게이트웨이에 전송하는 제 402단계, 상기 API 게이트웨이가 암호화 정보 R'15에 대한 검증 프로세스를 수행하는 제 403단계, 상기 제 403단계의 출력값이 참이면, 상기 API 게이트웨이가 상기 접근토큰 AccessToken의 유효기간 Timeexp 및 클라우드 서비스 Q'를 점검하는 제 404단계, 상기 API 게이트웨이가 상기 클라우드 서비스 Q'에 대한 특정 파라미터인 상기 param를 해당 클라우드 서비스에 전송하는 제 405단계, 상기 클라우드 서비스가 결과값 res를 상기 API 게이트웨이로 반환하는 제 406단계 및 상기 API 게이트웨이가 상기 결과값 res를 상기 컴퓨터시스템로 전송하는 제 407단계를 포함하고, 상기 암호화 정보 R'15는 상기 컴퓨터시스템에 의해 생성된 상기 암호화 정보 R15를 상기 API 게이트웨이가 전송받은 경우, 상기 암호화 정보 R15와 구별하기 위해 상기 암호화 정보 R15 대신에 사용되는 정보이고, 상기 클라우드 서비스 Q'는 상기 컴퓨터시스템에 의해 준비된 상기 클라우드 서비스 Q를 상기 API 게이트웨이가 전송받은 경우, 상기 클라우드 서비스 Q와 구별하기 위해 상기 클라우드 서비스 Q 대신에 사용되는 서비스인 것을 특징으로 한다.

[0027] 또한, 상기 제 401단계는 먼저, 컴퓨터시스템이 (수학식) R14=AccessToken||Q||param||t, where Q∈O를 이용하여, 상기 R14를 준비하는 제 401-1단계, 상기 컴퓨터시스템이 (수학식) H11=H(R14)를 이용하여, 상기 R14의 해시값 H11을 준비하는 제 401-2단계, 상기 컴퓨터시스템이 (수학식) S11=Sign_SK_u(H11)으로 상기 컴퓨터시스템의 비밀키 SK_u를 이용하여, 상기 H11에 대한 디지털서명 S11을 생성하는 제 401-3단계 및 상기 컴퓨터시스템이 (수학식) R15=E_PK_gw(R14||S11)으로 상기 케이트웨이의 공개키 PK_gw를 이용하여, 상기 R14 및 디지털서서명 S11를 연접한 정보를 암호화한 상기 암호화 정보 R15를 생성하는 제 401-4단계를 포함하고, 상기 AccessToken는 상기 컴퓨터시스템의 접근토큰이고, 상기 서비스목록 O는 컴퓨터시스템이 접근하고자 하는 서비스의 목록이고, 상기 클라우드 서비스 Q는 상기 서비스목록 O에 포함되고, 클라우드 플랫폼에서 제공하는 서비스이고, 상기 param은 상기 클라우드 서비스 Q에 대한 특정 파라미터이고, 상기 t는 현재의 타임스탬프이고, 상기 R14는 상기 접근토큰 AccessToken, 클라우드 서비스 Q, 파라미터 param 및 현재의 타임스탬프 t를 연접한 정보인 것을 특징으로 한다.

[0028] 또한, 상기 제 403단계는 상기 API 게이트웨이가 (수학식) D_SK_gw(R'15) → R'14||S'11에서 상기 API 게이트웨이의 비밀키 SK_gw를 이용하여 상기 암호화 정보 R'15을 복호화하여, 상기 R'14 및 디지털서명 S'11을 획득하는 제 403-1단계, 상기 API 게이트웨이가 (수학식) H'11=H(R'14)를 이용하여, 상기 R'14의 해시값 H'11을 계산하는 제 403-2단계, 상기 API 게이트웨이가 (수학식) PKVer_Addr_u(S'11,H'11) → True or False을 이용하여, PKVer_Addr_u 함수에 디지털서명 S'11, 해시값 H'11을 입력하는 제 403-3단계를 포함하고, 상기 PKVer_Addr_u(S'11,H'11)은 상기 컴퓨터시스템의 블록체인 주소 Addr_u가 상기 해시값 H'11에 대해 상기 디지털서명 S'11으로 검증하는 함수인 것을 특징으로 한다.

[0029] 또한, 상기 제 404단계는 상기 API 게이트웨이가 상기 접근토큰 AccessToken의 유효기간 Timeexp의 만료 여부를 상기 로컬 데이터베이스 내에서 점검하는 제 404-1단계, 상기 API 게이트웨이가 클라우드 서비스 Q'가 상기 컴퓨터시스템이 접근하고자 하는 서비스목록 O의 구성원이 맞는지 상기 로컬 데이터베이스 내에서 점검하는 제 404-2단계 및 상기 제 404-1 단계 및 제 404-2 단계 모두 충족되는 경우, 상기 API 게이트웨이가 (수학식) JWTVer(AccessToken, SK_gw)를 이용하여, JWTVer 함수에 상기 접근토큰 AccessToken 및 상기 API 게이트웨이의 비밀키 SK_gw를 입력하여, 상기 접근토큰 AccessToken의 유효성을 검증하는 제 404-3단계를 포함하는 것을 특징으로 한다.

발명의 효과

[0030] 본 발명에 의한 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법은 블록체인 및 스마트 계약을 기반으로 하는 아키텍처를 통합하여, 클라우드 기반의 인공지능 시스템의 머신러닝 파이프라인에 대한 무결성을 강화할 수 있는 효과가 있다.

[0031] 또한, 본 발명에 의한 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법은 공격자가 실제 컴퓨터시스템을 사칭하여 클라우드 기반의 인공지능 시스템에 침입하는 것을 사전에 방지할 수 있는 효과가 있다.

[0032] 또한, 본 발명에 의한 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법은 무결성을 추적하고, 데이터 조작을 방지할 수 있는 효과가 있다.

도면의 간단한 설명

[0033] 도 1은 본 발명에 의한 클라우드 기반의 인공지능 시스템에 대한 구성도이다.

도 2는 본 발명에 의한 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법에 대한 순서도이다.

도 3은 도 2에 도시된 S300 단계에서 S301~S310 단계에 대한 순서도이다.

도 4는 도 3에 도시된 S301 단계에 대한 순서도이다.

도 5는 도 3에 도시된 S303 단계에 대한 순서도이다.

도 6은 도 3에 도시된 S304 단계에 대한 순서도이다.

도 7은 도 3에 도시된 S306 단계에 대한 순서도이다.

도 8은 도 3에 도시된 S308 단계에 대한 순서도이다.

도 9는 도 3에 도시된 S310 단계에 대한 순서도이다.

도 10은 도 2에 도시된 S300 단계에서 S311~S320 단계에 대한 순서도이다.

도 11은 도 10에 도시된 S311 단계에 대한 순서도이다.

도 12는 도 10에 도시된 S315 단계에 대한 순서도이다.

도 13은 도 10에 도시된 S317 단계에 대한 순서도이다.

도 14는 도 2에 도시된 S300 단계에서 S321~S326 단계에 대한 순서도이다.

도 15는 도 14에 도시된 S323 단계에 대한 순서도이다.

도 16은 도 14에 도시된 S325 단계에 대한 순서도이다.

도 17은 도 2에 도시된 S400 단계에 대한 순서도이다.

도 18은 도 17에 도시된 S401 단계에 대한 순서도이다.

도 19는 도 17에 도시된 S403 단계에 대한 순서도이다.

도 20은 도 17에 도시된 S404 단계에 대한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0034] 이하, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있을 정도로 상세히 설명하기 위하여, 본 발명의 실시예를 첨부한 도면을 참조하여 설명하기로 한다.

[0035] 그러나, 하기 실시예는 본 발명의 이해를 돕기 위한 일 예에 불과한 것으로 이에 의해 본 발명의 권리범위가 축소되거나 한정되는 것은 아니다. 또한, 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다.

[0036] 이하, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있을 정도로 상세히 설명하기 위하여, 본 발명의 실시예를 첨부한 도면을 참조하여 설명하기로 한다.

[0037] 그러나, 하기 실시예는 본 발명의 이해를 돕기 위한 일 예에 불과한 것으로 이에 의해 본 발명의 권리범위가 축소되거나 한정되는 것은 아니다. 또한, 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다.

[0038] 먼저, 본 발명에 의한 클라우드 기반의 인공지능 시스템에 대한 컴퓨터시스템의 등록 및 로그인 방법에서 사용되는 표기법에 대해 설명하기로 한다.

[0039] 먼저, Addr_x는 x의 블록체인 주소이다.

[0040] 그리고, X||Y는 X와 Y의 연접(concatenation)이다.

[0041] 그리고, SK_x, PK_x는 각각 x의 비밀키 및 공개키이다.

[0042] 그리고, Sign_SK_x(Y)는 x의 비밀키(SK_x)를 사용하여, Y에 대한 디지털서명을 생성하는 함수이다.

[0043] 그리고, PKVer_Addr_x(M,N)은 x의 블록체인 주소 Addr_x가 데이터 N에 대해 디지털서명 M으로 검증하는 함수이다. 이때, PKVer_Addr_x(M,N)은 x의 블록체인 주소 Addrx가 데이터 N에 대해 디지털서명 M으로 검증한 경우, 참을 출력하고, 그렇지 않으면, 거짓을 출력한다.

[0044] 그리고, E_PK_x(Y)는 x의 공개키(PK_x)를 이용하여, 데이터 Y를 비대칭으로 암호화(Encryption)하는 함수이다.

[0045] 그리고, D_SK_x(Y)는 x의 비밀키(SK_x)를 이용하여, 데이터 Y를 비대칭으로 복호화(Decryption)하는 함수이다.

[0046] 그리고, H(Y)는 데이터 Y의 해시값을 생성하는 함수이다.

[0047] 그리고, SC_z는 모듈 z에 대한 스마트계약이다.

[0048] 그리고, JWTVer(O, SK_x)는 x의 비밀키(SK_x)를 이용하여, 접근토큰 O를 검증하는 함수이다.

[0049] 도 1은 본 발명에 의한 클라우드 기반의 인공지능 시스템의 구성도이다.

[0050] 도 1을 참조하면, 본 발명에 의한 클라우드 기반의 인공지능 시스템은 컴퓨터시스템, 스마트계약 및 클라우드 플랫폼을 포함하여 구성된다.

[0051] 먼저, 컴퓨터시스템은 클라이언트 측에서 인공지능 서비스를 사용하기 위해, 클라우드 플랫폼에게 클라우드의 API를 호출한다.

[0052] 그리고, 컴퓨터시스템은 보안 환경에서 기계학습 데이터셋을 업로드하고, 클라우드 플랫폼 상에서 기계학습 시스템을 학습시킨다.

[0053] 그리고, 스마트계약은 블록체인 네트워크에 상주하며, 컴퓨터시스템 및 클라우드 플랫폼이 상호 신뢰할 수 있도록 신뢰 가능한 서비스 레벨 계약으로서의 역할을 담당한다.

[0054] 그리고, 클라우드 플랫폼은 컴퓨터시스템에게 다수의 서비스를 공급한다.

[0055] 도 1을 참조하면, 클라우드 플랫폼은 관리모듈, API 게이트웨이, 무결성모듈, 로깅/모니터링부 및 저장 관리부를 포함하여 구성된다.

[0056] 먼저, 관리모듈(IDMA Module, Identity Management and Access Control Module)은 컴퓨터시스템의 등록 및 로그인 프로세스를 관리한다. 이때, 각각의 컴퓨터시스템에게는 자신의 활동을 제한하고, 임의의 행동을 방지하는 역할이 주어진다.

[0057] 또한, 관리모듈은 컴퓨터시스템에게 컴퓨터시스템증명서(U_cred, User Credential)를 제공한다. 이때, 컴퓨터시스템증명서는 컴퓨터시스템을 인증하기 위한 토큰으로 이용된다. 컴퓨터시스템은 클라우드 플랫폼에 로그인 시, 컴퓨터시스템 인증을 위해 상기 컴퓨터시스템증명서를 이용할 수 있다.

[0058] 또한, 관리모듈은 스마트계약과 협력하여, 관리모듈 및 스마트계약 간에 송수신되는 정보를 검증한다.

[0059] 그리고, API(Application Programming Interface) 게이트웨이는 클라우드 서비스를 이용하고자 하는 컴퓨터시스템의 API 요청을 처리한다. 또한, API 게이트웨이는 컴퓨터시스템이 클라우드 서비스를 이용하기 전에, 컴퓨터시스템에게 토큰을 제공한다.

[0060] 또한, API 게이트웨이는 스마트계약과 협력하여, API 토큰에 대한 컴퓨터시스템의 요청 및 상기 API 토큰 값을 기록한다. 컴퓨터시스템 및 클라우드 플랫폼 모두 스마트계약에 대한 토큰의 합법성을 확인할 수 있다.

[0061] 그리고, 무결성모듈(IM, Integrity Module)은 블록체인을 이용하여 학습 모델 및 학습 데이터의 무결성을 유지하는 역할을 한다.

[0062] 따라서, 컴퓨터시스템 및 클라우드 플랫폼은 각각 스마트계약에 대한 학습 데이터의 무결성을 확인할 수 있다.

[0063] 그리고, 로깅/모니터링부는 데이터의 흐름 및 컴퓨터시스템의 활동을 기록한다. 또한, 로깅/모니터링부는 클라우드 플랫폼을 모니터링하여, 악의적인 행동에 대해 경보음을 발생시킨다.

[0064] 그리고, 저장 관리부는 시스템의 백업 데이터 프로세스를 관리한다. 구체적으로, 저장 관리부는 백업 데이터에 대한 기밀성(Confidentiality)을 확보하기 위해 백업 데이터를 암호화하여 저장한다.

[0065] 한편, 본 발명에 의한 클라우드 기반의 인공지능 시스템은 컴퓨터시스템이 데이터를 저장할 수 있는 로컬 저장소 및 관리모듈이 데이터를 저장할 수 있는 로컬 데이터베이스를 더 포함하여 구성된다.

[0066] 도 2는 본 발명에 의한 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법에 대한 순서도이다.

[0067] 도 2를 참조하면, 본 발명에 의한 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법은 컴퓨터시스템이 API 게이트웨이에 토큰을 요청하는 단계(S300) 및 컴퓨터시스템이 API 게이트웨이에 API를 호출하는 단계(S400)를 포함하여 구성된다.

[0068] 먼저, 컴퓨터시스템이 API 게이트웨이에 토큰을 요청하는 단계(S300)에 대해 설명하기로 한다.

[0069] 도 3은 도 2에 도시된 S300 단계에서 S301~S310 단계에 대한 순서도이다.

[0070] 도 3을 참조하면, 컴퓨터시스템은 암호화 정보 R8을 준비한다.(S301)

[0071] 도 4는 도 3에 도시된 S301 단계에 대한 순서도이다.

[0072] 도 4를 참조하면, 컴퓨터시스템은 (수학식) R7=U_cred||t을 이용하여, R7을 준비한다.(S301-1)

[0073] 여기서, U_cred는 컴퓨터시스템증명서이고, t는 현재의 타임스탬프(Timestamp)이고, R7은 컴퓨터시스템증명서 U_cred 및 현재의 타임스탬프 t를 연접한 정보이다.

[0074] 그 이후, 컴퓨터시스템은 (수학식) H5=H(R7)을 이용하여, R7의 해시값 H5를 준비한다.(S301-2)

[0075] 그 이후, 컴퓨터시스템은 (수학식) S5=Sign_SK_u(H5)로 컴퓨터시스템의 비밀키 SK_u를 이용하여, 해시값 H5에 대한 디지털서명 S2를 생성한다.(S301-3)

[0076] 그 이후, 컴퓨터시스템은 (수학식) R8=E_PK_gw(R7||S5)로 API 게이트웨이의 공개키 PK_gw를 이용하여, R7 및 디지털서명 S5를 연접한 정보를 암호화한 암호화 정보 R8를 계산한다.(S301-4)

[0077] 한편, 컴퓨터시스템은 API 게이트웨이에 토큰을 요청할 수 있는 권한이 있음을 증명하기 위해 컴퓨터시스템증명서 U_cred를 제시해야 한다.

[0078] 그 이후, 컴퓨터시스템은 상기 컴퓨터시스템이 이용 가능한 서비스목록을 획득하기 위해 컴퓨터시스템의 블록체인 주소 Addr_u 및 암호화 정보 R8을 API 게이트웨이에 전송한다.(S302)

[0079] 그 이후, API 게이트웨이는 암호화 정보 R'8에 대한 검증 프로세스를 수행한다.(S303)

[0080] 여기서, 암호화 정보 R'8은 컴퓨터시스템에 의해 생성된 암호화 정보 R8을 API 게이트웨이가 전송받은 경우, 암호화 정보 R8과 구별하기 위해 암호화 정보 R8 대신에 사용되는 정보이다.

[0081] 도 5는 도 3에 도시된 S303 단계에 대한 순서도이다.

[0082] 도 5를 참조하면, API 게이트웨이는 (수학식) D_SK_gw(R'8) → R'7||S'5에서 API 게이트웨이의 비밀키 SK_gw를 이용하여 암호화 정보 R'8를 복호화하여, R'7 및 디지털서명 S'5를 획득한다.(S303-1)

[0083] 그 이후, API 게이트웨이는 (수학식) H'5=H(R'7)을 이용하여, R'7의 해시값 H'5를 계산한다.(S303-2)

[0084] 그 이후, API 게이트웨이는 해시값 H'5에 대한 서명을 검증하기 위해, (수학식) PKVer_Addr_u(S'5,H'5) → True or False를 이용하여, PKVer_Addr_u 함수에 디지털서명 S'5, 해시값 H'5를 입력한다.(S303-3)

[0085] 여기서, PKVer_Addr_u(S'5,H'5)는 컴퓨터시스템의 블록체인 주소 Addr_u가 해시값 H'5에 대해 디지털서명 S'5로 검증하는 함수이다. 상기 S303-3단계는 공격자가 컴퓨터시스템을 사칭하는 것을 방지하기 위해 이용된다.

[0086] API 게이트웨이는 S303단계의 출력값이 참인 경우, API 게이트웨이는 관리모듈에 대한 컴퓨터시스템의 권한을 체크하기 위해 암호화 정보 R10을 계산한다.(S304)

[0087] 도 6은 도 3에 도시된 S304 단계에 대한 순서도이다.

[0088] 도 6을 참조하면, API 게이트웨이는 S303단계의 출력값이 참인 경우, (수학식) R9=Addr_u||U'_cred을 이용하여, 컴퓨터시스템의 블록체인 주소 Addr_u 및 컴퓨터시스템증명서 U'_cred를 연접한 R9를 계산한다.(S304-1)

[0089] 여기서, 컴퓨터시스템증명서 U'_cred는 API 게이트웨이가 컴퓨터시스템로부터 컴퓨터시스템증명서 U_cred를 전송받은 경우, 컴퓨터시스템증명서 U_cred와 구별하기 위해 컴퓨터시스템증명서 U_cred 대신에 사용되는 컴퓨터

시스템증명서이다.

[0090] 그 이후, API 게이트웨이는 (수학식) H6=H(R9)을 이용하여, R9의 해시값 H6을 계산한다.(S304-2)

[0091] 그 이후, API 게이트웨이는 (수학식) S6=Sign_SK_gw(H6)으로 API 게이트웨이의 비밀키 SK_gw를 이용하여, 해시값 H6에 대한 디지털서명 S6을 생성한다.(S304-3)

[0092] 그 이후, API 게이트웨이는 (수학식) R10=E_PK_idma(R9||S6)으로 관리모듈의 공개키 PK_idma를 이용하여, R9 및 디지털서명 S6을 연접한 정보를 암호화한 암호화 정보 R10을 계산한다.(S304-3)

[0093] 그 이후, API 게이트웨이는 암호화 정보 R10을 관리모듈로 전송한다.(S305)

[0094] 그 이후, 관리모듈은 암호화 정보 R'10에 대한 검증 프로세스를 수행한다.(S306)

[0095] 여기서, 암호화 정보 R'10은 API 게이트웨이에 의해 생성된 암호화 정보 R10을 관리모듈이 전송받은 경우, 상기 암호화 정보 R10과 구별하기 위해 암호화 정보 R10 대신에 사용되는 정보이다.

[0096] 도 7은 도 3에 도시된 S306 단계에 대한 순서도이다.

[0097] 도 7을 참조하면, 관리모듈은 (수학식) R'9||S'6=D_SK_idma(R'10)에서 관리모듈의 비밀키 SK_idma를 이용하여 암호화 정보 R'10을 복호화하여, R'9 및 디지털서명 S'6을 획득한다.(S306-1)

[0098] 그 이후, 관리모듈은 (수학식) H'6=H(R'9)을 이용하여, R'9의 해시값 H'6을 계산한다.(S306-2)

[0099] 그 이후, 관리모듈은 해시값 H'6에 대한 서명을 검증하기 위해, (수학식) PKVer_PK_gw(S'6,H'6) → True or False을 이용하여, PKVer_PK_gw 함수에 디지털서명 S'6, 해시값 H'6을 입력한다.(S306-3)

[0100] 여기서, PKVer_PK_gw(S'6,H'6)은 API 게이트웨의 공개키 PK_gw가 해시값 H'6에 대해 디지털서명 S'6으로 검증하는 함수이다.

[0101] 그 이후, 관리모듈은 (수학식) R'9=Addr_u||U"_cred를 이용하여, 컴퓨터시스템의 블록체인 주소 Addr_u 및 컴퓨터시스템증명서 U"_cred를 획득한다.(S306-4)

[0102] S306-3 단계의 출력값이 참이면, 관리모듈은 로컬 데이터베이스에 컴퓨터시스템증명서 U"_cred를 전송하여, 컴퓨터시스템 할당정보 U_rl를 획득한다.(S306-5)

[0103] 그 이후, 관리모듈은 (수학식) H7=H(U_rl)을 이용하여, 컴퓨터시스템 할당정보 U_rl의 해시값 H7을 계산한다.(S306-5)

[0104] 그 이후, 관리모듈은 (수학식) S7=Sign_SK_idma(H7)을 이용하여, 관리모듈의 비밀키 SK_idma로 해시값 H7에 대한 디지털서명 S7을 생성한다.(S306-6)

[0105] 그 이후, 관리모듈은 컴퓨터시스템 할당정보 U_rl 및 디지털서명 S7로 구성된 응답 메시지를 API 게이트웨이에 각각 전송한다.(S307)

[0106] 그 이후, API 게이트웨이는 컴퓨터시스템 할당정보 U'_rl 및 디지털서명 S'7을 검증한다.(S308)

[0107] 여기서, 컴퓨터시스템 할당정보 U'_rl은 관리모듈에 의해 획득된 컴퓨터시스템 할당정보 U_rl을 API 게이트웨이가 전송받은 경우, 컴퓨터시스템 할당정보 U_rl과 구별하기 위해 컴퓨터시스템 할당정보 U_rl 대신에 사용되는 정보이다.

[0108] 그리고, 디지털서명 S'7은 관리모듈에 의해 계산된 디지털서명 S7을 API 게이트웨이는 전송받은 경우, 디지털서명 S7과 구별하기 위해 디지털서명 S7 대신에 사용되는 디지털서명이다.

[0109] 도 8은 도 3에 도시된 S308 단계에 대한 순서도이다.

[0110] 도 8을 참조하면, API 게이트웨이는 (수학식) H'7=H(U'_rl)을 이용하여, 컴퓨터시스템 할당정보 U'_rl의 해시값 H'7을 계산한다.(S308-1)

[0111] 그 이후, API 게이트웨이는 해시값 H'7에 대한 서명을 검증하기 위해, (수학식) PKVer_PK_idma(S'7, H'7) → True or False을 이용하여, PKVer_PK_gw 함수에 디지털서명 S'7, 해시값 H'7을 입력한다.(S308-2)

[0112] 여기서, PKVer_PK_idma(S'7, H'7)은 관리모듈의 공개키 PK_idma가 해시값 H'7에 대해 디지털서명 S'7으로 검증하는 함수이다.

[0113] 상기 S308-2단계의 출력값이 참이면, API 게이트웨이는 컴퓨터시스템 할당정보 U'_rl로부터 컴퓨터시스템의 권한을 체크한다.(S308-3)

[0114] 컴퓨터시스템이 API 토큰을 요청할 수 있는 권한을 갖는 경우, API 게이트웨이는 (수학식) N={n_1, n_2, n_3, ..., n_n}을 이용하여, 서비스목록 N을 준비한다.(S308-4)

[0115] 여기서, n_1, n_2, n_3, ..., n_n은 다수의 서비스이고, N은 다수의 서비스 n_1, n_2, n_3, ..., n_n로 구성된 서비스목록이다.

[0116] 그 이후, API 게이트웨이는 (수학식) H8=H(N)을 이용하여, 서비스목록 N의 해시값 H8을 계산한다.(S308-5)

[0117] 그 이후, API 게이트웨이는 (수학식) S8=Sign_SK_gw(H8)로 API 게이트웨이의 비밀키 SK_gw를 이용하여, 해시값 H8에 대한 디지털서명 S8을 생성한다.(S308-6)

[0118] 그 이후, API 게이트웨이는 컴퓨터시스템의 요청에 응답하기 위해 서비스목록 N 및 디지털서명 S8으로 구성된 응답 메시지를 컴퓨터시스템에게 전송한다.(S309)

[0119] 그 이후, 컴퓨터시스템은 디지털서명 S'8에 대한 검증 프로세스를 수행한다.(S310)

[0120] 여기서, 디지털서명 S'8은 API 게이트웨이에 의해 생성된 디지털서명 S8을 컴퓨터시스템이 전송받은 경우, 상기 디지털서명 S8과 구별하기 위해 디지털서명 S8 대신에 사용되는 정보이다.

[0121] 도 9는 도 3에 도시된 S310 단계에 대한 순서도이다.

[0122] 도 9를 참조하면, 컴퓨터시스템은 (수학식) H'8=H(N')을 이용하여 서비스목록 N'의 해시값 H'8를 계산한다.(S310-1)

[0123] 여기서, 서비스목록 N'는 API 게이트웨이에 의해 준비된 서비스목록 N을 컴퓨터시스템이 전송받은 경우, 상기 서비스목록 N과 구별하기 위해 서비스목록 N 대신에 사용되는 정보이다.

[0124] 그 이후, 컴퓨터시스템은 해시값 H'8에 대한 서명을 검증하기 위해, (수학식) PKVer_PK_gw(S'8,H'8) → True or False을 이용하여, PKVer_PK_gw 함수에 디지털서명 S'8, 해시값 H'8을 입력한다.(S310-2)

[0125] 여기서, PKVer_PK_gw(S'8,H'8)은 API 게이트웨이의 공개키 PK_gw가 해시값 H'8에 대해 디지털서명 S'8으로 검증하는 함수이다.

[0126] 도 10은 도 2에 도시된 S300 단계에서 S311~S320 단계에 대한 순서도이다.

[0127] 도 10을 참조하면, S310단계의 출력값이 참인 경우, 컴퓨터시스템은 해시값 H9를 계산한다.(S311)

[0128] 도 11은 도 10에 도시된 S311 단계에 대한 순서도이다.

[0129] 도 11을 참조하면, 컴퓨터시스템은 (수학식) O={o_1, o_2, o_3, ...o_n}, where O⊂N'을 이용하여, 서비스목록 O를 준비한다.(S311-1)

[0130] 여기서, o_1, o_2, o_3, ...o_n은 컴퓨터시스템이 접근하고자 하는 다수의 서비스이고, O는 컴퓨터시스템이 접근하고자 하는 다수의 서비스 o_1, o_2, o_3, ...o_n으로 구성된 컴퓨터시스템이 접근하고자 하는 서비스목록이다.

[0131] 그 이후, 컴퓨터시스템은 (수학식) R11=O||t을 이용하여, 서비스목록 O 및 현재의 타임스탬프 t를 연접한 정보 R11을 계산한다.(S311-2)

[0132] 그 이후, 컴퓨터시스템은 (수학식) H9=H(R11)을 이용하여, R11의 해시값 H9를 계산한다.(S311-3)

[0133] 그 이후, 컴퓨터시스템은 컴퓨터시스템의 블록체인 주소 Addr_u 및 해시값 H9를 포함하는 트랜잭션정보 Tx4를 제2 스마트계약에 전송한다.(S312)

[0134] 여기서, 제2 스마트계약은 API 게이트웨이에 대한 스마트계약을 의미한다.

[0135] 그 이후, 제2 스마트계약은 컴퓨터시스템의 블록체인 주소 Addr_u 및 해시값 H'9를 블록체인에 저장한다.(S313)

[0136] 여기서, 해시값 H'9는 컴퓨터시스템에 의해 생성된 해시값 H9를 제2 스마트계약이 전송받은 경우, 상기 해시값 H9와 구별하기 위해 해시값 H9 대신에 사용되는 정보이다.

[0137] 그 이후, 제2 스마트계약은 API 게이트웨이 및 블록체인의 모든 노드에게 블록체인 주소 Addr_u 및 해시값 H'9

를 브로드캐스팅한다.(S314)

[0138] 여기서, 블록체인의 모든 노드에는 컴퓨터시스템이 포함된다.

[0139] 제2 스마트계약로부터 블록체인 주소 Addr_u 및 해시값 H'9를 전송받은 컴퓨터시스템은 자신의 요청이 블록체인에 성공적으로 저장되었다는 사실을 알 수 있다.

[0140] 그 이후, 컴퓨터시스템은 디지털서명 S9 및 서비스 요청정보 R12를 계산한다.(S315)

[0141] 도 12는 도 10에 도시된 S315 단계에 대한 순서도이다.

[0142] 도 12를 참조하면, 먼저, 컴퓨터시스템은 (수학식) S9=Sign_SK_u(H9)로 컴퓨터시스템의 비밀키 SK_u를 이용하여, 해시값 H9에 대한 디지털서명 S9를 생성한다.(S315-1)

[0143] 그 이후, 컴퓨터시스템은 (수학식) R12=E_PK_gw(R11||S9)로 API 게이트웨이의 공개키 PK_gw를 이용하여, R11 및 디지털서명 S9를 연접한 정보를 암호화하여, 암호화 정보인 R12를 생성한다.(S315-2)

[0144] 그 이후, 컴퓨터시스템은 서비스 요청정보 R12를 API 게이트웨이로 전송한다.(S316)

[0145] 그 이후, API 게이트웨이는 서비스 요청정보 R'12에 대한 검증 프로세스를 수행한다.(S317)

[0146] 여기서, 서비스 요청정보 R'12는 컴퓨터시스템에 의해 생성된 서비스 요청정보 R12를 API 게이트웨이가 전송받은 경우, 상기 서비스 요청정보 R12와 구별하기 위해 서비스 요청정보 R12 대신에 사용되는 정보이다.

[0147] 도 13은 도 10에 도시된 S317 단계에 대한 순서도이다.

[0148] 도 13을 참조하면, API 게이트웨이는 (수학식) D_SK_gw(R'12) → R'11||S'9에서 API 게이트웨이의 비밀키 SK_gw를 이용하여 서비스 요청정보 R'12를 복호화하여, R'11 및 디지털서명 S'9를 획득한다.(S317-1)

[0149] 그 이후, API 게이트웨이는 (수학식) H"9=H(R'11)을 이용하여 R'11의 해시값 H"9를 계산한다.(S317-2)

[0150] 그 이후, API 게이트웨이는 상기 API 게이트웨이에 의해 계산된 해시값 H"9 및 제1 스마트계약에 의해 브로드캐스팅된 해시값 H'9를 비교하여, 상기 해시값 H"9 및 H'9의 일치 여부를 확인한다.(S317-3)

[0151] 해시값 H"9 및 H'9이 일치하는 경우, API 게이트웨이는 R'12에 대한 검증 프로세스를 계속한다. 해시값 H"9 및 H'9이 일치하지 않는 경우, API 게이트웨이는 서비스 요청정보 R'12에 대한 검증 프로세스를 중단한다.(S317-4)

[0152] 그 이후, API 게이트웨이는 디지털서명 S'9를 검증하기 위해, (수학식) PKVerAddr_u(S'9,H"9) → True or False를 이용하여, PKVer_Addr_u 함수에 디지털서명 S'9, 해시값 H"9를 입력한다.(S317-5)

[0153] 여기서, PKVer_Addr_u(S'9,H"9)는 컴퓨터시스템의 블록체인 주소 Addr_u가 해시값 H"9에 대해 디지털서명 S'9로 검증하는 함수이다.

[0154] 상기 S317-5 단계는 API 게이트웨이에 대한 서비스 요청정보 R'12의 발신자와 API 토큰 스마트계약에 대한 트랜잭션정보 Tx4의 발신자가 일치한다는 것을 증명하기 위해 사용된다.

[0155] 상기 S317단계의 출력값이 참이면, API 게이트웨이는 R'11을 로컬 데이터베이스에 저장한다.(S318)

[0156] 그 이후, API 게이트웨이는 서비스목록 O'을 바탕으로, JWT 형식의 컴퓨터시스템토큰 Utoken을 생성하고, (수학식) H10=H(Utoken)을 이용하여, 컴퓨터시스템토큰 Utoken의 해시값 H10을 계산한다.(S319)

[0157] 여기서, 상기 컴퓨터시스템토큰 O'는 컴퓨터시스템에 의해 생성된 컴퓨터시스템토큰 O를 API 게이트웨이가 전송받은 경우, 상기 컴퓨터시스템토큰 O와 구별하기 위해 컴퓨터시스템토큰 O 대신에 사용되는 정보이다.

[0158] 그리고, 컴퓨터시스템토큰 Utoken은 접근토큰 AccessToken 및 상기 접근토큰AccessToken의 유효기간 Timeexp를 결합한 것이다. 이때, 컴퓨터시스템은 유효기간 Timeexp이 만료된 접근토큰 AccessToken을 사용할 수 없다.

[0159] 도 14는 도 2에 도시된 S300 단계에서 S321~S326 단계에 대한 순서도이다.

[0160] 도 14를 참조하면, 제2 스마트계약은 컴퓨터시스템의 블록체인 주소 Addr_u 및 해시값 H'10을 블록체인에 기록하고, API 게이트웨이 및 블록체인의 모든 노드에게 Addr_u 및 해시값 H'10을 브로드캐스팅한다.(S321)

[0161] 여기서, 블록체인의 모든 노드에는 컴퓨터시스템이 포함된다.

[0162] 그리고, 해시값 H'10은 제2 스마트계약에 의해 생성된 해시값 H10을 제2 스마트계약이 전송받은 경우, 상기 해

시값 H10과 구별하기 위해 해시값 H10 대신에 사용되는 정보이다.

[0163] 그 이후, 컴퓨터시스템은 제2 스마트계약으로부터 전송받은 해시값 H'10을 로컬 저장소에 저장한다.(S322)

[0164] 그 이후, API 게이트웨이는 암호화 정보 R13을 계산한다.(S323)

[0165] 도 15는 도 14에 도시된 S323 단계에 대한 순서도이다.

[0166] 도 15를 참조하면, API 게이트웨이는 (수학식) S10=Sign_SK_idma(H10)으로 관리모듈의 비밀키 SK_idma를 이용하여, 해시값 H10에 대한 디지털서명 S10을 생성한다.(S323-1)

[0167] 그 이후, API 게이트웨이는 (수학식) R13=E_Addr_u(Utoken||S10)으로 컴퓨터시스템의 블록체인 주소 Addr_u를 이용하여, Utoken 및 S10을 연접한 정보를 암호화하여, 암호화 정보 R13을 생성한다.(S323-2)

[0168] 그 이후, API 게이트웨이는 암호화 정보 R13을 컴퓨터시스템에게 전송한다.(S324)

[0169] 그 이후, 컴퓨터시스템은 API게이트웨이로부터 전송받은 암호화 정보 R'13에 대한 검증 프로세스를 수행한다.(S325)

[0170] 여기서, 암호화 정보 R'13은 API 게이트웨이에 의해 생성된 암호화 정보 R13을 컴퓨터시스템이 전송받은 경우, 암호화 정보 R13과 구별하기 위해 암호화 정보 R13 대신에 사용되는 정보이다.

[0171] 도 16은 도 14에 도시된 S325 단계에 대한 순서도이다.

[0172] 도 16을 참조하면, 컴퓨터시스템은 (수학식) D_SK_u(R'13) → U'token||S'10에서 컴퓨터시스템의 비밀키 SK_u를 이용하여 암호화 정보 R'13을 복호화하여, 컴퓨터시스템토큰 U'token 및 디지털서명 S'10을 획득한다.(S325-1)

[0173] 그 이후, 컴퓨터시스템은 (수학식) H"10=H(U'token)을 이용하여 컴퓨터시스템토큰 U'token의 해시값 H"10을 계산한다.(S325-2)

[0174] 그 이후, 컴퓨터시스템은 상기 컴퓨터시스템에 의해 계산된 해시값 H"10 및 제2 스마트계약에 의해 브로드캐스팅된 해시값 H'10을 비교하여, 상기 해시값 H"10 및 H'10의 일치 여부를 확인한다.(S325-3)

[0175] 해시값 H"10 및 H'10이 일치하는 경우, 컴퓨터시스템은 암호화 정보 R'13에 대한 검증 프로세스를 계속한다. 해시값 H"10 및 H'10이 일치하지 않는 경우, 컴퓨터시스템은 암호화 정보 R'13에 대한 검증 프로세스를 중단한다.(S325-4)

[0176] 그 이후, 컴퓨터시스템은 (수학식) PKVer_PK_idma(S'10,H"10) → True or False을 이용하여, PKVer_PKim 함수에 디지털서명 S'10, 해시값 H"10을 입력한다.(S325-5)

[0177] 여기서, PKVer_PK_idma(S'10,H"10)은 관리모듈의 공개키 PK_idma가 해시값 H"10에 대해 디지털서명 S'10으로 검증하는 함수이다.

[0178] 상기 S325단계의 출력값이 참이면, 컴퓨터시스템은 컴퓨터시스템토큰 U'token을 로컬 저장소에 저장한다.(S326)

[0179] 다음으로, 컴퓨터시스템이 API 게이트웨이에 API를 호출하는 단계(S400)에 대해 설명하기로 한다.

[0180] 컴퓨터시스템은 API 게이트웨이를 통해 클라우드 서비스에 접근하기 위해 API 토큰을 필요로 한다. 여기서, 클라우드 서비스는 클라우드 플랫폼에서 제공하는 서비스를 의미한다.

[0181] 컴퓨터시스템은 사전에 API 토큰을 호출하였으며, 상기 API 토큰은 로컬 저장소에 저장되어 있는 것으로 가정한다.

[0182] 도 17은 도 2에 도시된 S400 단계에 대한 순서도이다.

[0183] 도 17을 참조하면, 컴퓨터시스템은 API를 호출하기 전에 암호화 정보 R15를 준비한다.(S401)

[0184] 도 18은 도 17에 도시된 S401 단계에 대한 순서도이다.

[0185] 도 18을 참조하면, 컴퓨터시스템은 (수학식) R14=AccessToken||Q||param||t, where Q∈O를 이용하여, R14를 준비한다.(S401-1)

[0186] 여기서, AccessToken는 컴퓨터시스템의 접근토큰이고, O는 컴퓨터시스템이 접근하고자 하는 서비스목록이고, Q는 서비스목록 O에 포함되는 클라우드 플랫폼에서 제공하는 클라우드 서비스이다.

[0187] 그리고, param은 클라우드 서비스 Q에 대한 특정 파라미터이고, t는 현재의 타임스탬프이다.

[0188] 그리고, R14는 컴퓨터시스템의 접근토큰 AccessToken, 클라우드 서비스 Q, 클라우드 서비스 Q에 대한 특정 파라미터 param 및 현재의 타임스탬프 t를 연접한 정보이다.

[0189] 그 이후, 컴퓨터시스템은 (수학식) H11=H(R14)이용하여, R14의 해시값 H11을 준비한다.(S401-2)

[0190] 그 이후, 컴퓨터시스템은 (수학식) S11=Sign_SK_u(H11)으로 컴퓨터시스템의 비밀키 SK_u를 이용하여, 해시값 H11에 대한 디지털서명 S11을 생성한다.(S401-3)

[0191] 그 이후, 컴퓨터시스템은 (수학식) R15=E_PK_gw(R14||S11)으로 API 게이트웨이의 공개키 PK_gw를 이용하여, R14 및 디지털서명 S11를 연접한 정보를 암호화하여, 암호화 정보 R15를 생성한다.(S401-4)

[0192] 그 이후, 컴퓨터시스템은 API 요청정보 R15를 API 게이트웨이에 전송한다.(S402)

[0193] 그 이후, API 게이트웨이는 암호화 정보 R'15에 대한 검증 프로세스를 수행한다.(S403)

[0194] 여기서, 암호화 정보 R'15는 컴퓨터시스템에 의해 생성된 암호화 정보 R15를 API 게이트웨이가 전송받은 경우, 상기 암호화 정보 R15와 구별하기 위해 암호화 정보 R15 대신에 사용되는 정보이다.

[0195] 도 19는 도 17에 도시된 S403 단계에 대한 순서도이다.

[0196] 도 19를 참조하면, API 게이트웨이는 (수학식) D_SK_gw(R'15) → R'14||S'11에서 API 게이트웨이의 비밀키 SK_gw를 이용하여 암호화 정보 R'15을 복호화하여, R'14 및 디지털서명 S'11을 획득한다.(S403-1)

[0197] 그 이후, API 게이트웨이는 (수학식) H'11=H(R'14)를 이용하여, R'14의 해시값 H'11을 계산한다.(S403-2)

[0198] 그 이후, API 게이트웨이는 서명을 검증하기 위해, (수학식)PKVer_Addr_u(S'11,H'11) → True or False을 이용하여, PKVer_Addr_u 함수에 디지털서명 S'11, 해시값 H'11을 입력한다.(S403-3)

[0199] 여기서, PKVer_Addr_u(S'11,H'11)은 컴퓨터시스템의 블록체인 주소 Addr_u가 해시값 H'11에 대해 디지털서명 S'11으로 검증하는 함수이다.

[0200] 상기 S403 단계의 출력값이 참이면, API 게이트웨이는 컴퓨터시스템의 접근토큰 AccessToken의 유효기간 Timeexp 및 클라우드 서비스 Q'를 점검한다.(S404)

[0201] 도 20은 도 17에 도시된 S404 단계에 대한 순서도이다.

[0202] 도 20을 참조하면, API 게이트웨이는 컴퓨터시스템의 접근토큰 AccessToken의 유효기간 Timeexp의 만료 여부를 로컬 데이터베이스 내에서 점검한다.(S404-1)

[0203] 또한, API 게이트웨이는 클라우드 서비스 Q'가 컴퓨터시스템이 접근하고자 하는 서비스목록 O의 구성원이 맞는지 로컬 데이터베이스 내에서 점검한다.(S404-2)

[0204] 여기서, 클라우드 서비스 Q'는 컴퓨터시스템에 의해 준비된 클라우드 서비스 Q를 API 게이트웨이가 전송받은 경우, 상기 클라우드 서비스 Q와 구별하기 위해 클라우드 서비스 Q 대신에 사용되는 서비스이다.

[0205] 상기 두 조건이 모두 충족되면, API 게이트웨이는 (수학식) JWTVer(AccessToken, SK_gw)를 이용하여, JWTVer 함수에 컴퓨터시스템의 접근토큰 AccessToken 및 API 게이트웨이의 비밀키 SK_gw를 입력하여, 컴퓨터시스템의 접근토큰 AccessToken의 유효성을 검증한다.(S404-3)

[0206] 컴퓨터시스템의 접근토큰 AccessToken에 대한 유효성의 검증 결과가 참인 경우, API 게이트웨이는 클라우드 서비스 Q'에 대한 특정 파라미터 param를 해당 클라우드 서비스에 전송(중계)한다.(S405)

[0207] 그 이후, 상기 클라우드 서비스는 결과값 res를 API 게이트웨이로 반환한다.(S406)

[0208] 그 이후, API 게이트웨이는 결과값 res를 컴퓨터시스템로 전송(중계)한다.(S407)

[0209] 한편, 상기 시스템은 다음의 경우 컴퓨터시스템이 접근토큰 AccessToken을 사용하는 것을 취소할 수 있다.

[0210] 1) 접근토큰 AccessToken의 유효기간 Timeexp이 만료된다.

[0211] 2) 컴퓨터시스템이 접근토큰 AccessToken 사용 시, 상기 시스템이 상기 컴퓨터시스템의 검증 실패 등 악의적인 활동을 감지한다.

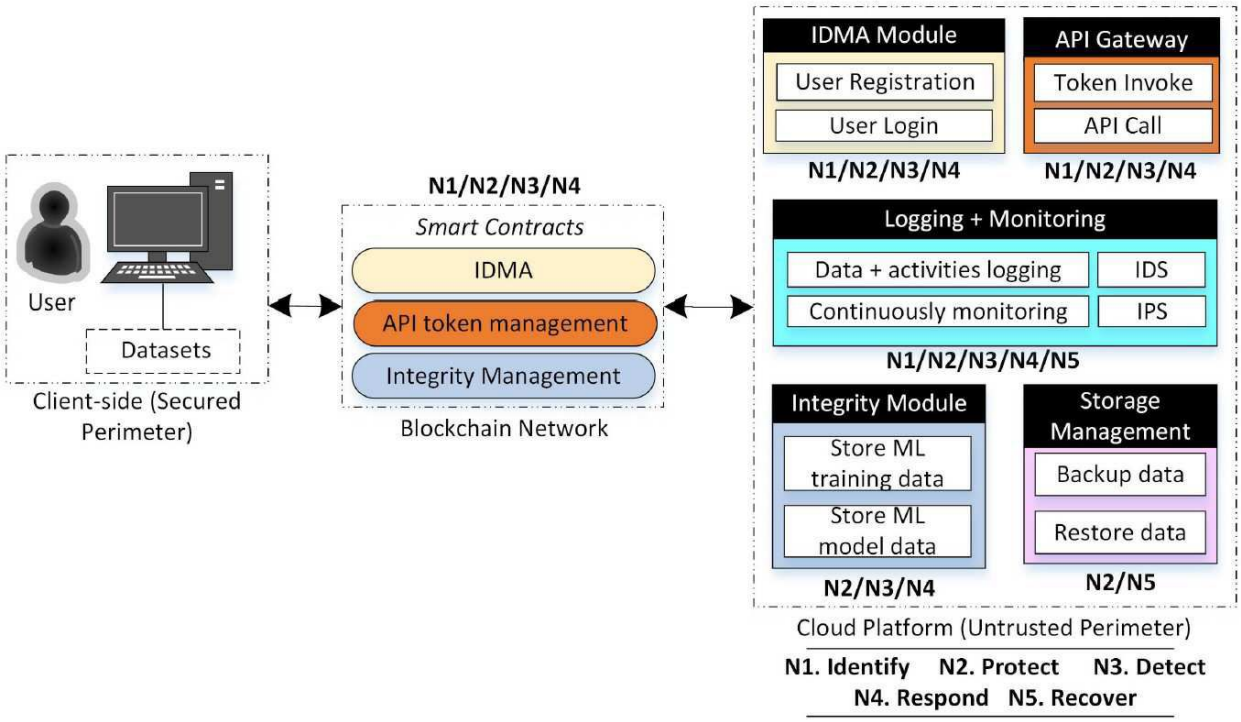
[0212] 이상과 같이 본 발명은 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법을 제공하고자 하는 것을 주요한 기술적 사상으로 하고 있으며, 도면을 참고하여 상술한 실시예는 단지 하나의 실시예에 불과하고, 본 발명의 진정한 권리 범위는 특허 청구범위를 기준으로 하되, 다양하게 존재할 수 있는 균등한 실시예에도 미친다 할 것이다.

부호의 설명

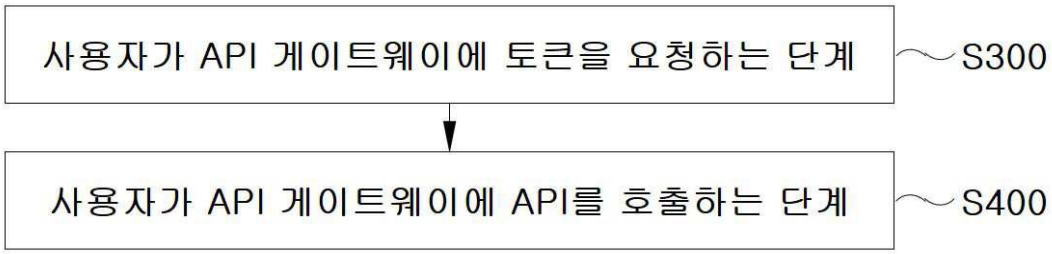
[0213] 5: 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법

도면

도면1



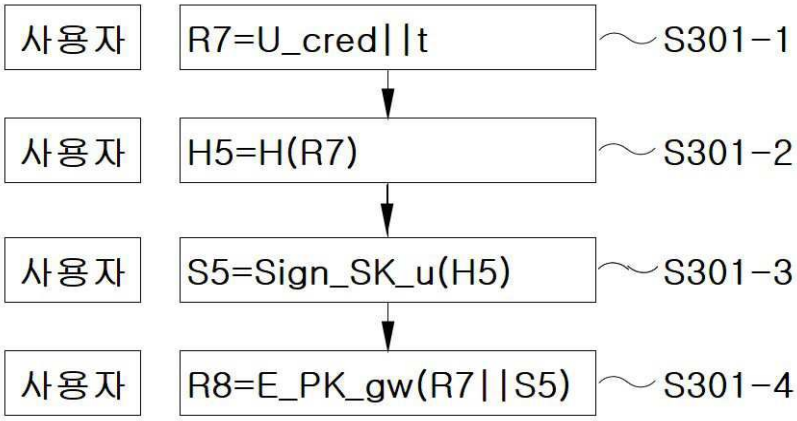
도면2



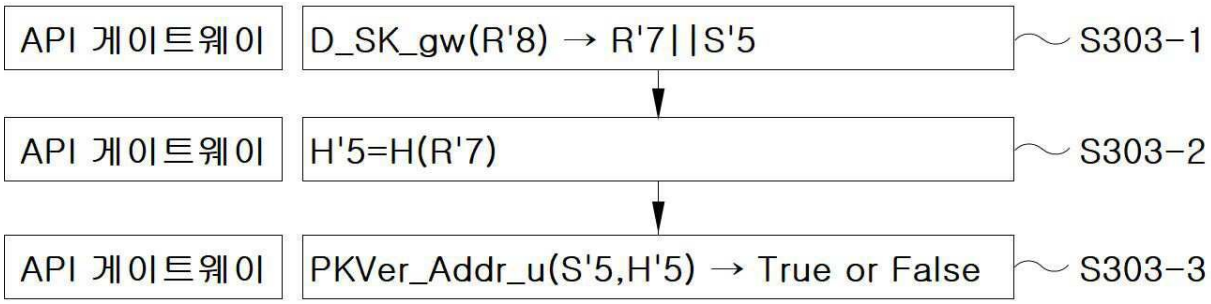
도면3


사용자
R8 준비
S301
사용자
Addr_u, R8을 API 게이트웨이에 전송
S302
API 게이트웨이
R'8에 대한 검증 프로세스 수행
S303
API 게이트웨이
R10을 계산
S304
API 게이트웨이
R10을 관리모듈로 전송
S305
관리모듈
R'10에 대한 검증 프로세스 수행
S306
관리모듈
U_rl, S7로 구성된 응답메시지 → API 게이트웨이
S307
API 게이트웨이
U'_rl, S'7 검증
S308
API 게이트웨이
N, S8을 사용자에게 전송
S309
사용자
S'8에 대한 검증 프로세스 수행
S310

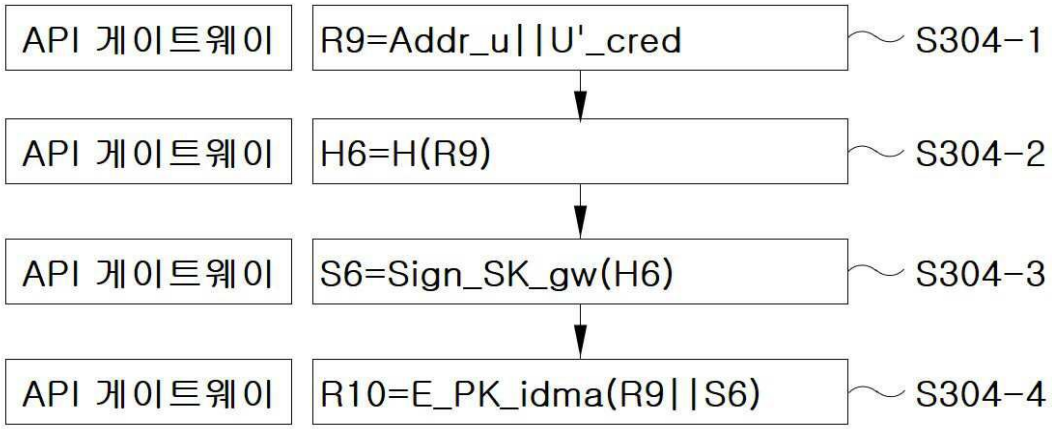
도면4


사용자
R7=U_cred||t
S301-1
사용자
H5=H(R7)
S301-2
사용자
S5=Sign_SK_u(H5)
S301-3
사용자
R8=E_PK_gw(R7||S5)
S301-4

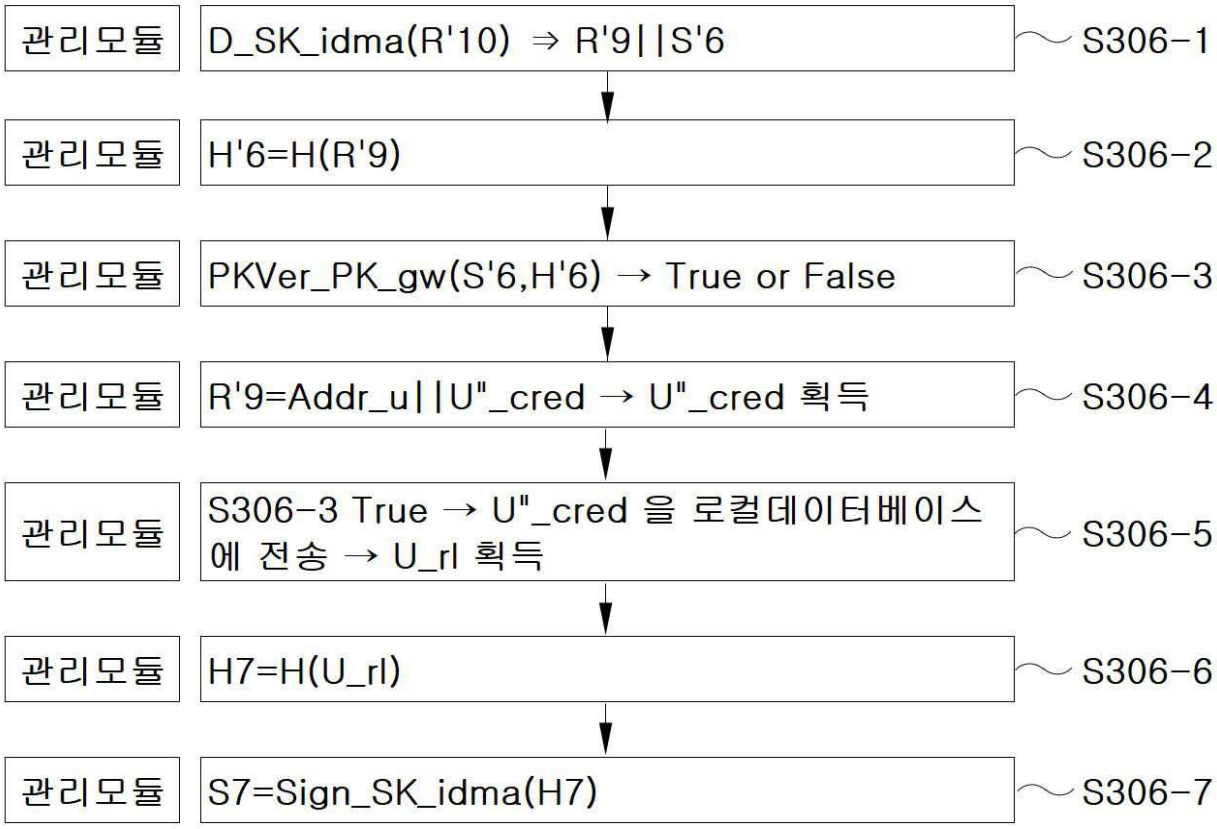
도면5


API 게이트웨이
D_SK_gw(R'8) → R'7||S'5
S303-1
API 게이트웨이
H'5=H(R'7)
S303-2
API 게이트웨이
PKVer_Addr_u(S'5,H'5) → True or False
S303-3

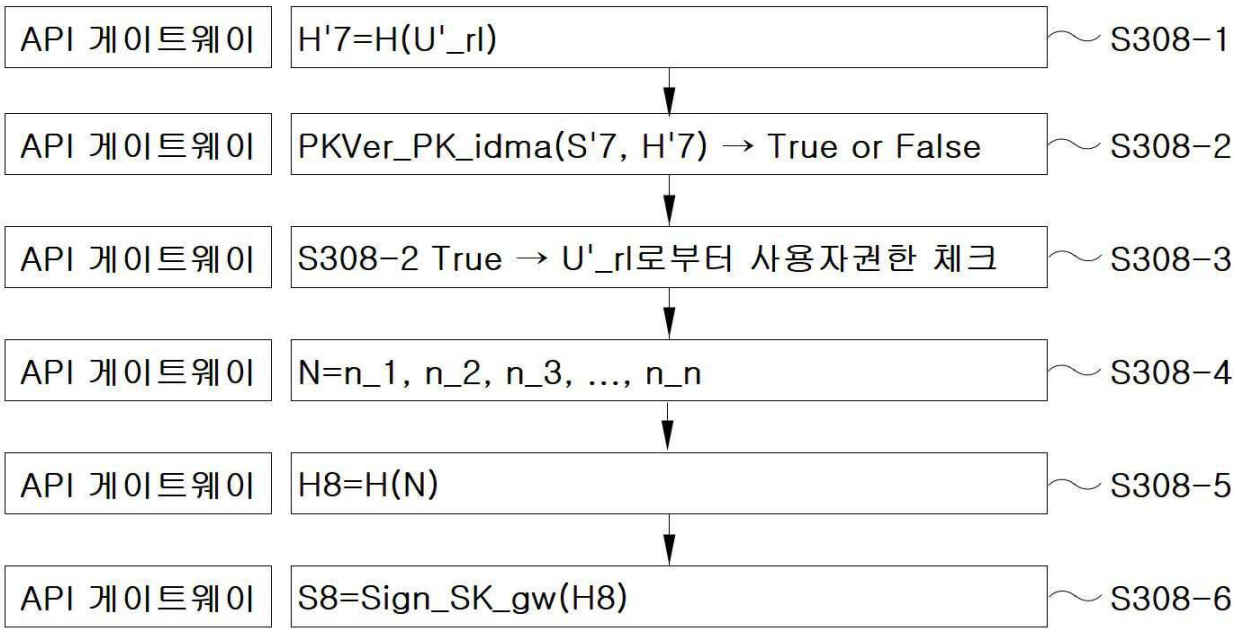
도면6


API 게이트웨이
R9=Addr_u||U'_cred
S304-1
API 게이트웨이
H6=H(R9)
S304-2
API 게이트웨이
S6=Sign_SK_gw(H6)
S304-3
API 게이트웨이
R10=E_PK_idma(R9||S6)
S304-4

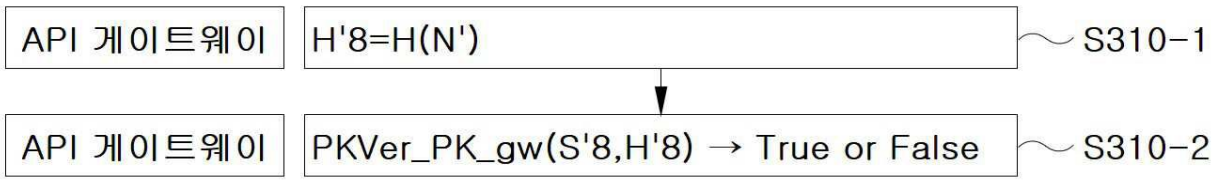
도면7


관리모듈
D_SK_idma(R'10) ⇒ R'9||S'6
S306-1
관리모듈
H'6=H(R'9)
S306-2
관리모듈
PKVer_PK_gw(S'6,H'6) → True or False
S306-3
관리모듈
R'9=Addr_u||U"_cred → U"_cred 획득
S306-4
관리모듈
S306-3 True → U"_cred 을 로컬데이터베이스에 전송 → U_rl 획득
S306-5
관리모듈
H7=H(U_rl)
S306-6
관리모듈
S7=Sign_SK_idma(H7)
S306-7

도면8

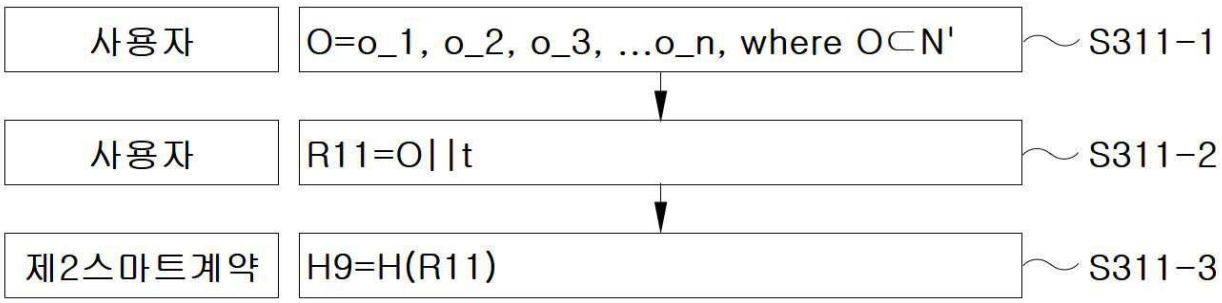

API 게이트웨이
H'7=H(U'_rl)
S308-1
API 게이트웨이
PKVer_PK_idma(S'7, H'7) → True or False
S308-2
API 게이트웨이
S308-2 True → U'_rl로부터 사용자권한 체크
S308-3
API 게이트웨이
N=n_1, n_2, n_3, ..., n_n
S308-4
API 게이트웨이
H8=H(N)
S308-5
API 게이트웨이
S8=Sign_SK_gw(H8)
S308-6

도면9

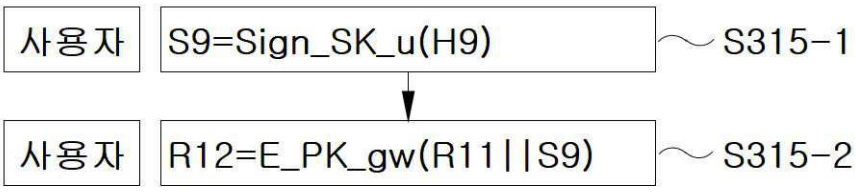


도면10

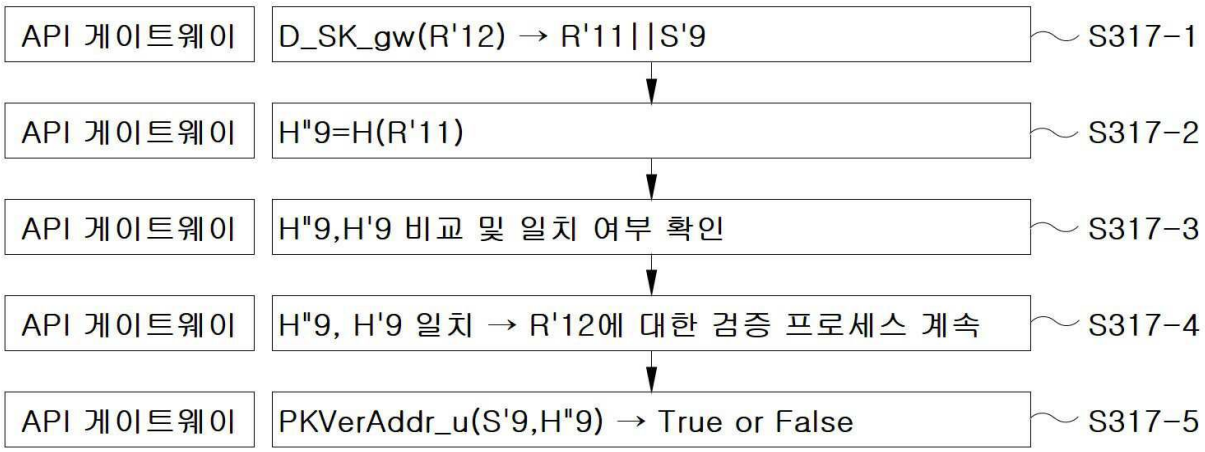
도면11



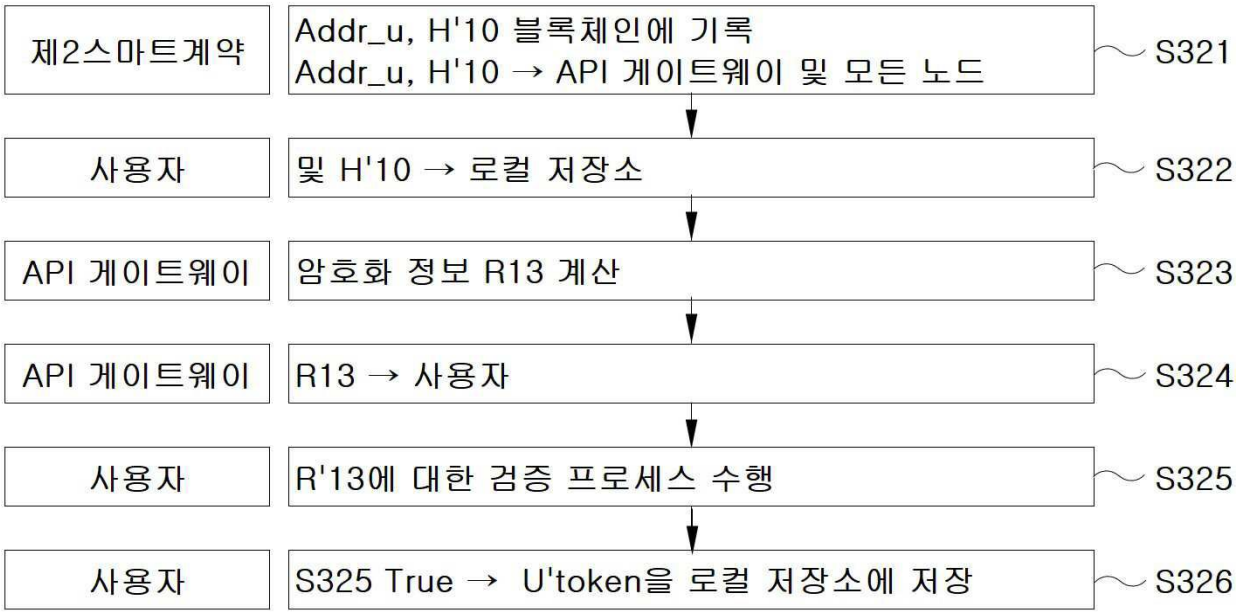
도면12



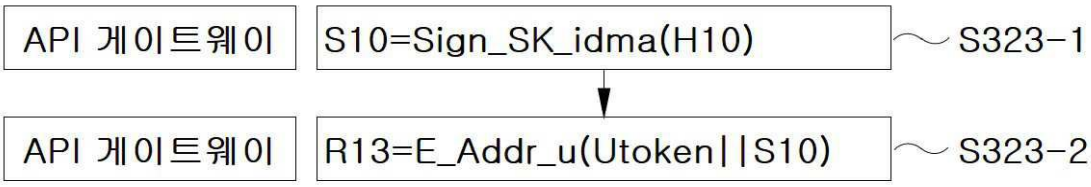
도면13



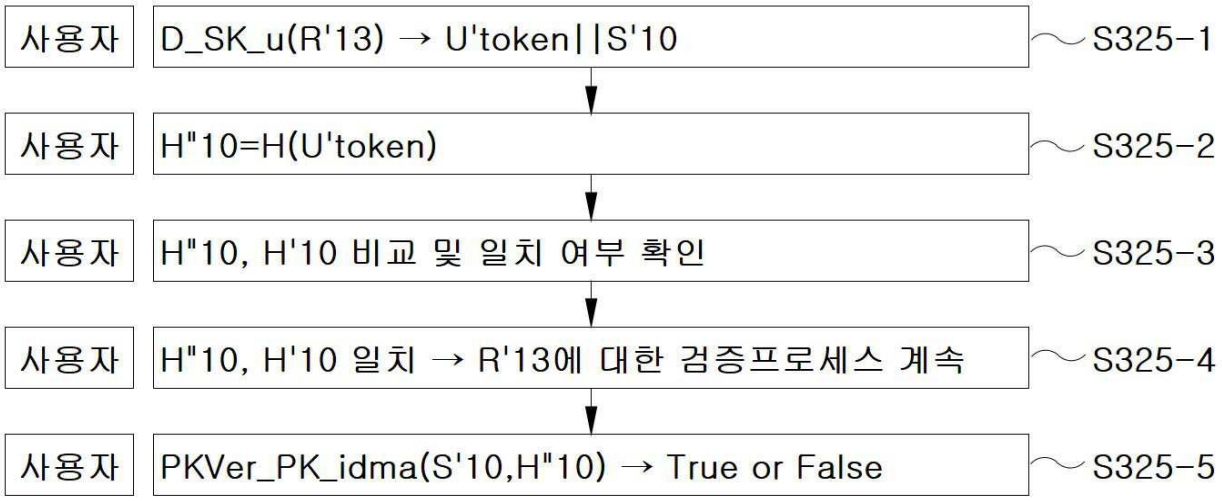
도면14



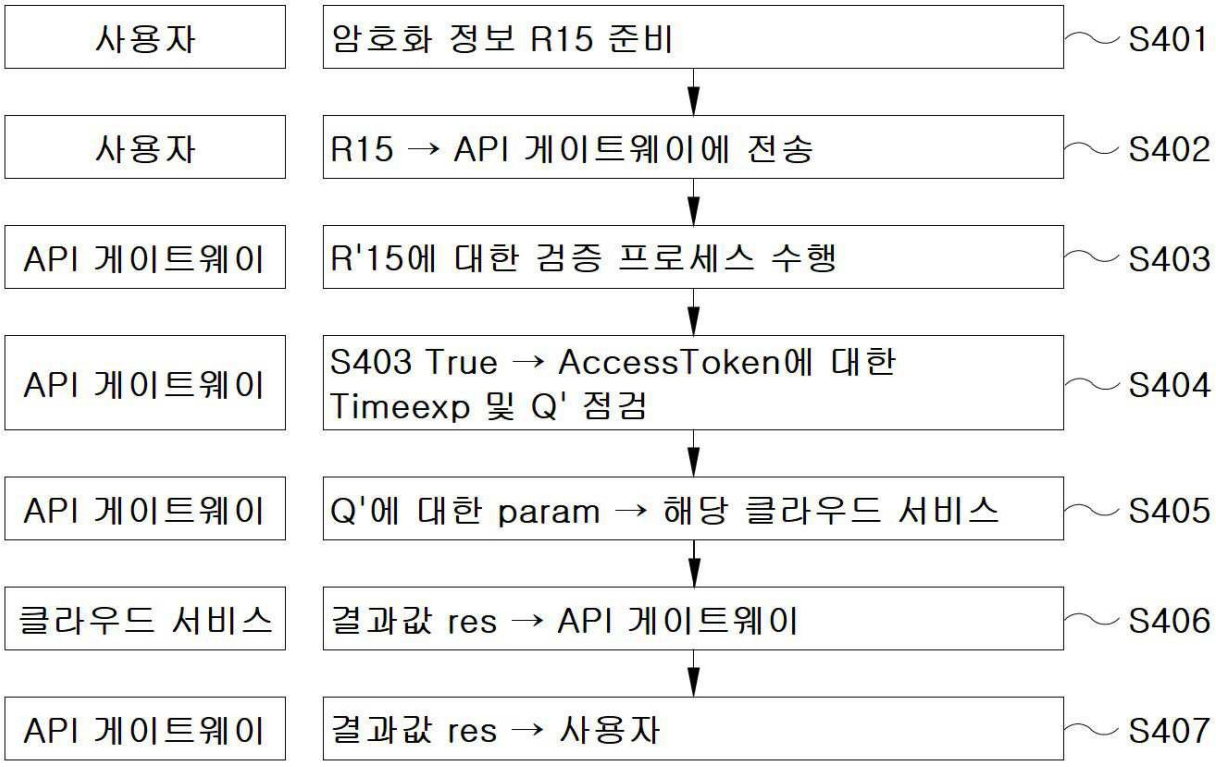
도면15



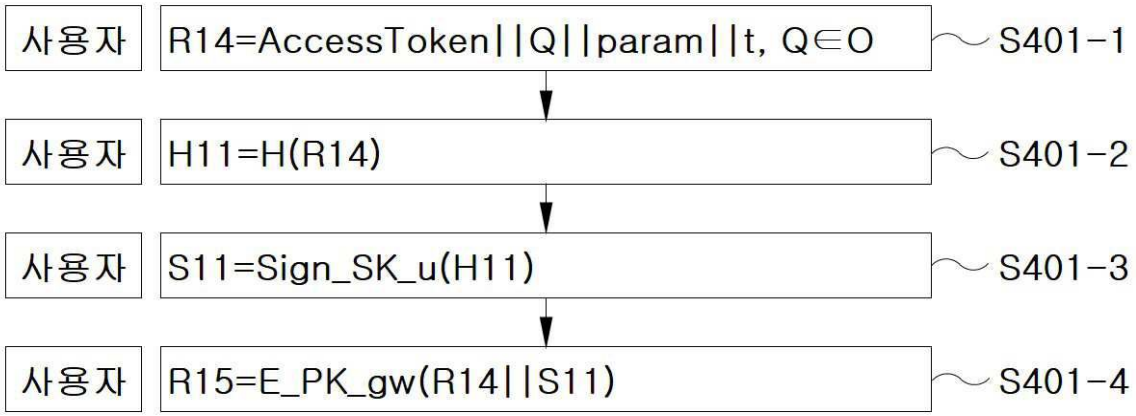
도면16


사용자
D_SK_u(R'13) → U'token||S'10
S325-1
사용자
H"10=H(U'token)
S325-2
사용자
H"10, H'10 비교 및 일치 여부 확인
S325-3
사용자
H"10, H'10 일치 → R'13에 대한 검증프로세스 계속
S325-4
사용자
PKVer_PK_idma(S'10,H"10) → True or False
S325-5

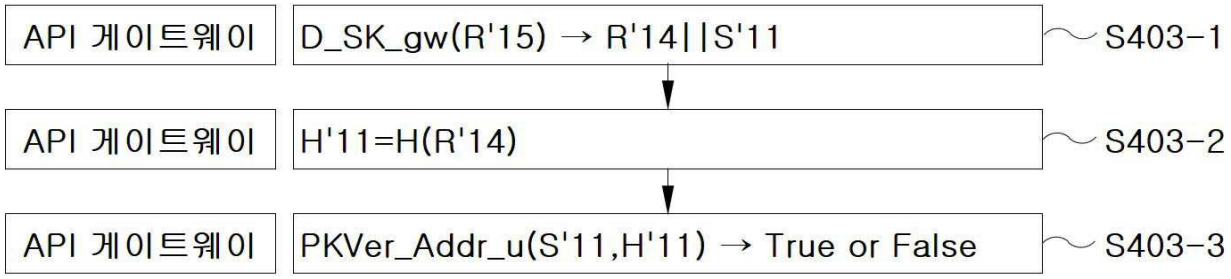
도면17


사용자
암호화 정보 R15 준비
S401
사용자
R15 → API 게이트웨이에 전송
S402
API 게이트웨이
R'15에 대한 검증 프로세스 수행
S403
API 게이트웨이
S403 True → AccessToken에 대한 Timeexp 및 Q' 점검
S404
API 게이트웨이
Q'에 대한 param → 해당 클라우드 서비스
S405
클라우드 서비스
결과값 res → API 게이트웨이
S406
API 게이트웨이
결과값 res → 사용자
S407

도면18



도면19



도면20

【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 2

【변경전】

제 1항에 있어서,

상기 제 301단계는

상기 컴퓨터시스템이 (수학식) R7=U_cred||t을 이용하여, 상기 R7을 준비하는 제 301-1단계;

상기 컴퓨터시스템이 (수학식) H5=H(R7)을 이용하여, 상기 R7의 해시값 H5를 준비하는 제 301-2단계;

상기 컴퓨터시스템이 (수학식) S5=Sign_SK_u(H5)로 상기 컴퓨터시스템의 비밀키 SK_u를 이용하여, 상기 해시값

H5에 대한 상기 디지털서명 S5를 생성하는 제 301-3단계; 및

상기 컴퓨터시스템이 (수학식) R8=E_PK_gw(R7||S5)로 API 게이트웨이의 공개키 PK_gw를 이용하여, 상기 R7 및 디지털서명 S5를 연접한 정보를 암호화한 상기 암호화 정보 R8를 계산하는 제 301-4단계;를 포함하고,

상기 U_cred는 컴퓨터시스템증명서이고, t는 현재의 타임스탬프이고, 상기 R7은 상기 컴퓨터시스템증명서 U_cred 및 상기 현재의 타임스탬프 t를 연접한 정보인 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.

【변경후】

제 1항에 있어서,

상기 제 301단계는

상기 컴퓨터시스템이 (수학식) R7=U_cred||t을 이용하여, 상기 R7을 준비하는 제 301-1단계;

상기 컴퓨터시스템이 (수학식) H5=H(R7)을 이용하여, 상기 R7의 해시값 H5를 준비하는 제 301-2단계;

상기 컴퓨터시스템이 (수학식) S5=Sign_SK_u(H5)로 상기 컴퓨터시스템의 비밀키 SK_u를 이용하여, 상기 해시값 H5에 대한 디지털서명 S5를 생성하는 제 301-3단계; 및

상기 컴퓨터시스템이 (수학식) R8=E_PK_gw(R7||S5)로 API 게이트웨이의 공개키 PK_gw를 이용하여, 상기 R7 및 디지털서명 S5를 연접한 정보를 암호화한 상기 암호화 정보 R8를 계산하는 제 301-4단계;를 포함하고,

상기 U_cred는 컴퓨터시스템증명서이고, t는 현재의 타임스탬프이고, 상기 R7은 상기 컴퓨터시스템증명서 U_cred 및 상기 현재의 타임스탬프 t를 연접한 정보인 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.

【직권보정 2】

【보정항목】 청구범위

【보정세부항목】 청구항 4

【변경전】

제 1항에 있어서,

상기 제 304단계는

상기 API 게이트웨이가 (수학식) R9=Addr_u||U'_cred을 이용하여, 상기 컴퓨터시스템의 블록체인 주소 Addr_u 및 컴퓨터시스템증명서 U'_cred를 연접한 상기 R9를 계산하는 제 304-1단계;

상기 API 게이트웨이가 (수학식) H6=H(R9)을 이용하여, 상기 R9의 해시값 H6을 계산하는 제 304-2단계;

상기 API 게이트웨이가 (수학식) S6=Sign_SK_gw(H6)으로 상기 API 게이트웨이의 비밀키 SK_gw를 이용하여, 상기 해시값 H6에 대한 상기 디지털서명 S6을 생성하는 제 304-3단계;

상기 API 게이트웨이가 (수학식) R10=E_PK_idma(R9||S6)으로 상기 관리모듈의 공개키 PK_idma를 이용하여, 상기 R9 및 디지털서명 S6을 연접한 정보를 암호화한 상기 암호화 정보 R10을 계산하는 제 304-4단계;를 포함하고,

상기 컴퓨터시스템증명서 U'_cred는 상기 API 게이트웨이가 상기 컴퓨터시스템로부터 컴퓨터시스템증명서 U_cred를 전송받은 경우, 상기 컴퓨터시스템증명서 U_cred와 구별하기 위해 상기 컴퓨터시스템증명서 U_cred 대신에 사용되는 정보인 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.

【변경후】

제 1항에 있어서,

상기 제 304단계는

상기 API 게이트웨이가 (수학식) R9=Addr_u||U'_cred을 이용하여, 상기 컴퓨터시스템의 블록체인 주소 Addr_u 및 컴퓨터시스템증명서 U'_cred를 연접한 상기 R9를 계산하는 제 304-1단계;

상기 API 게이트웨이가 (수학식) H6=H(R9)을 이용하여, 상기 R9의 해시값 H6을 계산하는 제 304-2단계;

상기 API 게이트웨이가 (수학식) S6=Sign_SK_gw(H6)으로 상기 API 게이트웨이의 비밀키 SK_gw를 이용하여, 상기 해시값 H6에 대한 디지털서명 S6을 생성하는 제 304-3단계;

상기 API 게이트웨이가 (수학식) R10=E_PK_idma(R9||S6)으로 상기 관리모듈의 공개키 PK_idma를 이용하여, 상기 R9 및 디지털서명 S6을 연접한 정보를 암호화한 상기 암호화 정보 R10을 계산하는 제 304-4단계;를 포함하고,

상기 컴퓨터시스템증명서 U'_cred는 상기 API 게이트웨이가 상기 컴퓨터시스템로부터 컴퓨터시스템증명서 U_cred를 전송받은 경우, 상기 컴퓨터시스템증명서 U_cred와 구별하기 위해 상기 컴퓨터시스템증명서 U_cred 대신에 사용되는 정보인 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.

【직권보정 3】

【보정항목】 청구범위

【보정세부항목】 청구항 5

【변경전】

제 1항에 있어서,

상기 제 306단계는

상기 관리모듈이 (수학식) D_SK_idma(R'10) ⇒ R'9||S'6에서 상기 관리모듈의 비밀키 SK_idma를 이용하여 상기 암호화 정보 R'10을 복호화하여, 상기 R'9 및 디지털서명 S'6을 획득하는 제 306-1단계;

상기 관리모듈이 (수학식) H'6=H(R'9)을 이용하여, 상기 R'9의 해시값 H'6을 계산하는 제 306-2단계;

상기 관리모듈이 (수학식) PKVer_PK_gw(S'6,H'6) → True or False을 이용하여, PKVer_PK_gw 함수에 상기 디지털서명 S'6 및 해시값 H'6을 입력하는 제 306-3단계;

상기 관리모듈이 (수학식) R'9=Addr_u||U"_cred를 이용하여, 상기 컴퓨터시스템의 블록체인 주소 Addr_u 및 컴퓨터시스템증명서 U"_cred를 획득하는 제 306-4단계;

상기 S306-3 단계의 출력값이 참인 경우, 상기 관리모듈이 로컬 데이터베이스에 상기 컴퓨터시스템증명서 U"_cred를 전송하여, 상기 컴퓨터시스템 할당정보 U_rl를 획득하는 제 306-5단계;

상기 관리모듈이 (수학식) H7=H(U_rl)을 이용하여, 상기 컴퓨터시스템 할당정보 U_rl의 해시값 H7을 계산하는 제 306-6단계; 및

상기 관리모듈이 (수학식) S7=Sign_SK_idma(H7)을 이용하여, 상기 관리모듈의 비밀키 SK_idma로 상기 해시값 H7에 대한 상기 디지털서명 S7을 생성하는 제 306-7단계;를 포함하고,

상기 PKVer_PK_gw(S'6,H'6)은 상기 API 게이트웨의 공개키 PK_gw가 상기 해시값 H'6에 대해 상기 디지털서명 S'6으로 검증하는 함수인 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.

【변경후】

제 1항에 있어서,

상기 제 306단계는

상기 관리모듈이 (수학식) D_SK_idma(R'10) ⇒ R'9||S'6에서 상기 관리모듈의 비밀키 SK_idma를 이용하여 상기 암호화 정보 R'10을 복호화하여, 상기 R'9 및 디지털서명 S'6을 획득하는 제 306-1단계;

상기 관리모듈이 (수학식) H'6=H(R'9)을 이용하여, 상기 R'9의 해시값 H'6을 계산하는 제 306-2단계;

상기 관리모듈이 (수학식) PKVer_PK_gw(S'6,H'6) → True or False을 이용하여, PKVer_PK_gw 함수에 상기 디지털서명 S'6 및 해시값 H'6을 입력하는 제 306-3단계;

상기 관리모듈이 (수학식) R'9=Addr_u||U"_cred를 이용하여, 상기 컴퓨터시스템의 블록체인 주소 Addr_u 및 컴퓨터시스템증명서 U"_cred를 획득하는 제 306-4단계;

상기 제 306-3 단계의 출력값이 참인 경우, 상기 관리모듈이 로컬 데이터베이스에 상기 컴퓨터시스템증명서 U"_cred를 전송하여, 상기 컴퓨터시스템 할당정보 U_rl를 획득하는 제 306-5단계;

상기 관리모듈이 (수학식) H7=H(U_rl)을 이용하여, 상기 컴퓨터시스템 할당정보 U_rl의 해시값 H7을 계산하는 제 306-6단계; 및

상기 관리모듈이 (수학식) S7=Sign_SK_idma(H7)을 이용하여, 상기 관리모듈의 비밀키 SK_idma로 상기 해시값 H7

에 대한 상기 디지털서명 S7을 생성하는 제 306-7단계;를 포함하고,

상기 PKVer_PK_gw(S'6,H'6)은 상기 API 게이트웨의 공개키 PK_gw가 상기 해시값 H'6에 대해 상기 디지털서명 S'6으로 검증하는 함수인 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.

【직권보정 4】

【보정항목】 청구범위

【보정세부항목】 청구항 13

【변경전】

제 12항에 있어서,

상기 제 323단계는

상기 API 게이트웨이가 (수학식) S10=Sign_SK_idma(H10)으로 상기 관리모듈의 비밀키 SK_idma를 이용하여, 상기 해시값 H10에 대한 상기 디지털서명 S10을 생성하는 제 323-1단계; 및

상기 API 게이트웨이가 (수학식) R13=E_Addr_u(Utoken||S10)으로 상기 컴퓨터시스템의 블록체인 주소 Addr_u를 이용하여, 상기 컴퓨터시스템토큰 Utoken 및 디지털서명 S10을 연접한 정보를 암호화하여, 상기 암호화 정보 R13을 생성하는 제 323-2단계;를 포함하는 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.

【변경후】

제 12항에 있어서,

상기 제 323단계는

상기 API 게이트웨이가 (수학식) S10=Sign_SK_idma(H10)으로 상기 관리모듈의 비밀키 SK_idma를 이용하여, 상기 해시값 H10에 대한 디지털서명 S10을 생성하는 제 323-1단계; 및

상기 API 게이트웨이가 (수학식) R13=E_Addr_u(Utoken||S10)으로 상기 컴퓨터시스템의 블록체인 주소 Addr_u를 이용하여, 상기 컴퓨터시스템토큰 Utoken 및 디지털서명 S10을 연접한 정보를 암호화하여, 상기 암호화 정보 R13을 생성하는 제 323-2단계;를 포함하는 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.

【직권보정 5】

【보정항목】 청구범위

【보정세부항목】 청구항 16

【변경전】

제 15항에 있어서,

상기 제 401단계는

먼저, 컴퓨터시스템이 (수학식) R14=AccessToken||Q||param||t, where Q∈O를 이용하여, 상기 R14를 준비하는 제 401-1단계;

상기 컴퓨터시스템이 (수학식) H11=H(R14)를 이용하여, 상기 R14의 해시값 H11을 준비하는 제 401-2단계;

상기 컴퓨터시스템이 (수학식) S11=Sign_SK_u(H11)으로 상기 컴퓨터시스템의 비밀키 SK_u를 이용하여, 상기 H11에 대한 디지털서명 S11을 생성하는 제 401-3단계; 및

상기 컴퓨터시스템이 (수학식) R15=E_PK_gw(R14||S11)으로 상기 케이트웨이의 공개키 PK_gw를 이용하여, 상기 R14 및 디지털서서명 S11를 연접한 정보를 암호화한 상기 암호화 정보 R15를 생성하는 제 401-4단계;를 포함하고,

상기 AccessToken는 상기 컴퓨터시스템의 접근토큰이고, 상기 클라우드 서비스 Q는 서비스목록 O에 포함되고, 클라우드 플랫폼에서 제공하는 서비스이고, 상기 param은 상기 클라우드 서비스 Q에 대한 특정 파라미터이고, 상기 t는 현재의 타임스탬프이고, 상기 R14는 상기 접근토큰 AccessToken, 클라우드 서비스 Q, 파라미터 param 및 현재의 타임스탬프 t를 연접한 정보인 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.

【변경후】

제 15항에 있어서,

상기 제 401단계는

먼저, 컴퓨터시스템이 (수학식) R14=AccessToken||Q||param||t, where Q∈O를 이용하여, 상기 R14를 준비하는 제 401-1단계;

상기 컴퓨터시스템이 (수학식) H11=H(R14)를 이용하여, 상기 R14의 해시값 H11을 준비하는 제 401-2단계;

상기 컴퓨터시스템이 (수학식) S11=Sign_SK_u(H11)으로 상기 컴퓨터시스템의 비밀키 SK_u를 이용하여, 상기 H11에 대한 디지털서명 S11을 생성하는 제 401-3단계; 및

상기 컴퓨터시스템이 (수학식) R15=E_PK_gw(R14||S11)으로 상기 게이트웨이의 공개키 PK_gw를 이용하여, 상기 R14 및 디지털서서명 S11를 연접한 정보를 암호화한 상기 암호화 정보 R15를 생성하는 제 401-4단계;를 포함하고,

상기 AccessToken는 상기 컴퓨터시스템의 접근토큰이고, 상기 클라우드 서비스 Q는 서비스목록 O에 포함되고, 클라우드 플랫폼에서 제공하는 서비스이고, 상기 param은 상기 클라우드 서비스 Q에 대한 특정 파라미터이고, 상기 t는 현재의 타임스탬프이고, 상기 R14는 상기 접근토큰 AccessToken, 클라우드 서비스 Q, 파라미터 param 및 현재의 타임스탬프 t를 연접한 정보인 것을 특징으로 하는 클라우드 기반의 인공지능 시스템에 대한 토큰 요청 및 API 호출 방법.