



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0090379
(43) 공개일자 2021년07월20일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) H04L 29/06 (2006.01)
H04L 29/08 (2006.01) H04L 9/08 (2006.01)
(52) CPC특허분류
H04L 9/3213 (2013.01)
H04L 63/101 (2013.01)
(21) 출원번호 10-2020-0003534
(22) 출원일자 2020년01월10일
심사청구일자 2020년01월10일

(71) 출원인
동서대학교 산학협력단
부산광역시 사상구 주례로 47(주례동,
동서대학교)
(72) 발명자
이상곤
부산광역시 서구 구덕로339번길 22, 크로바아파트
C동 301호 (서대신동3가)
유스투스 예코 옥티엔
부산 사상구 주례로 47(주례동, 동서대학교)
(74) 대리인
정병홍

전체 청구항 수 : 총 6 항

(54) 발명의 명칭 블록체인을 기반으로 한 IoT 디바이스 접근 제어 방법

(57) 요약

본 발명은 IoT 서비스의 접근 인가를 준비하는 단계, IoT 서비스의 요청에 의해 IoT 게이트웨이가 IoT 서비스의 접근을 인가하는 단계, IoT 서비스가 IoT 디바이스로 접근하는 단계 및 IoT 서비스의 접근을 해지하는 단계를 포함하여 구성되는 것을 특징으로 한다.

대표도



(52) CPC특허분류

H04L 67/12 (2013.01)

H04L 9/0825 (2013.01)

H04L 9/088 (2013.01)

H04L 9/3236 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	2018R1D1A1B07047601
부처명	교육부
과제관리(전문)기관명	한국연구재단
연구사업명	이공학개인지초연구지원
연구과제명	IoT와 SDN을 위한 종합적 블록체인 프레임 워크
기 여 율	1/1
과제수행기관명	동서대학교산학협력단
연구기간	2018.06.01 ~ 2023.05.31

명세서

청구범위

청구항 1

IoT 서비스의 접근 인가를 준비하는 단계;

IoT 서비스의 요청에 의해 IoT 게이트웨이가 IoT 서비스의 접근을 인가하는 단계;

IoT 서비스가 IoT 디바이스로 접근하는 단계; 및

IoT 서비스의 접근을 해지하는 단계를 포함하여 구성되는 것을 특징으로 하는 블록체인을 기반으로 한 IoT 디바이스 접근 제어 방법

청구항 2

제 1항에 있어서,

상기 IoT 서비스의 접근 인가를 준비하는 단계에서는

IoT 서비스가 IoT 서비스의 공개키(PK_S), IoT 서비스의 개인키(SK_S) 및 IoT 서비스의 주소(α_s)를 생성하는 단계;

IoT 서비스가 IoT 게이트웨이에서 IoT 게이트웨이의 주소(α_{GW}), IoT 게이트웨이의 IP 주소(γ_{GW}) 및 IoT 게이트웨이의 공개키(PK_{GW})를 검색하는 단계; 및

IoT 게이트웨이가 인가 서버를 네트워크에 설치하는 단계를 포함하여 구성되는 것을 특징으로 하는 블록체인을 기반으로 한 IoT 디바이스 접근 제어 방법

청구항 3

제 1항에 있어서,

상기 IoT 서비스의 요청에 의해 IoT 게이트웨이가 IoT 서비스의 접근을 인가하는 단계에서는

IoT 서비스가 이용 가능한 접근 목록(A)을 IoT 게이트웨이에 요구하는 단계;

IoT 게이트웨이가 이용 가능한 접근 목록(A), 접근 목록의 해시(Y_3) 및 접근 목록의 해시에 대한 서명(C_3)이 포함된 응답 정보를 생성하는 단계;

IoT 게이트웨이가 이용 가능한 접근 목록(A) 및 접근 목록의 해시에 대한 서명(C_3)을 IoT 서비스로 전송하는 단계;

IoT 서비스가 접근 목록의 해시에 대한 서명(C_3)을 검증하는 단계;

IoT 서비스가 IoT 게이트웨이 및 IoT 디바이스의 인증 완료 여부를 다시 점검하는 단계;

IoT 서비스가 접근하기 원하는 접근 목록(A'), 인가 페이로드(X_7) 및 인가 페이로드의 해시(Y_4)를 생성하는 단계;

IoT 서비스가 인가 페이로드의 해시(Y_4), 소스인 발신자 IoT 서비스의 주소(α_s) 및 인가 타겟인 IoT 게이트웨이의 주소(α_{GW})를 스마트계약으로 전송하는 단계;

스마트계약이 IoT 서비스가 인가 페이로드의 해시(Y_4), 소스인 발신자 IoT 서비스의 주소(α_s) 및 인가 타겟인

IoT 게이트웨이의 주소(α_{GW})를 스마트계약의 인가 목록에 저장하는 단계;

스마트계약이 트랜잭션 해시를 IoT 서비스로 반환하는 단계;

IoT 서비스가 IoT 서비스에 대한 인가 요청서(X_8)를 생성하는 단계;

IoT 서비스가 IoT 서비스에 대한 인가 요청서(X_8)를 IoT 게이트웨이로 전송하는 단계;

IoT 게이트웨이가 IoT 서비스에 대한 인가 요청서(X_8)를 검증하는 단계;

IoT 게이트웨이가 인가 페이로드의 해시(Y_4)가 포함된 인가 결과를 스마트계약으로 전송하는 단계;

IoT 게이트웨이가 IoT 서비스가 접근하기 원하는 접근 목록(A')을 IoT 게이트웨이의 데이터베이스에 저장하는 단계;

IoT 게이트웨이가 인가 페이로드의 해시(Y_4)가 포함된 인가 결과를 스마트계약으로 전송하는 단계;

스마트계약이 인가 페이로드의 해시(Y_4)를 활성화시켜 IoT 서비스에 대한 접근 토큰(Y_4)을 생성하는 단계;

스마트계약이 트랜잭션 해시를 IoT 게이트웨이로 반환하는 단계; 및

IoT 게이트웨이가 인가 완료 메시지를 IoT 서비스로 전송하는 단계를 포함하여 구성되는 것을 특징으로 하는 블록체인을 기반으로 한 IoT 디바이스 접근 제어 방법

청구항 4

제 3항에 있어서,

상기 IoT 게이트웨이가 IoT 서비스에 대한 인가 요청서(X_8)를 검증하는 단계에서는

IoT 게이트웨이가 IoT 서비스에 대한 인가 요청서(X_8)의 암호를 해독하는 단계;

IoT 게이트웨이가 재전송 공격을 방지하기 위한 임의의 문자열(n)이 이전에 한번도 사용된 적이 없는 새로운 것인지 확인하는 단계;

IoT 게이트웨이가 인가 페이로드의 해시(Y_4)를 계산하는 단계;

IoT 게이트웨이가 스마트계약에서 소스인 발신자 IoT 서비스의 주소(α_s), 인가 타겟인 IoT 게이트웨이의 주소(α_{GW})를 획득하는 단계;

IoT 게이트웨이가 인가 타겟과 IoT 게이트웨이의 주소(α_{GW})가 일치하는지 검사하는 단계;

IoT 게이트웨이가 인가 페이로드의 해시에 대한 서명(C_4)을 검증하는 단계;

IoT 게이트웨이가 IoT 게이트웨이의 데이터베이스로부터 IoT 서비스가 보유하고 있는 접근 목록(A_5)을 획득하는 단계;

IoT 게이트웨이가 IoT 서비스가 접근하기 원하는 접근 목록(A')이 IoT 서비스가 보유하고 있는 접근 목록(A_5)의 부분 집합인지 확인하는 단계; 및

True 값을 반환함으로써 IoT 서비스에 인가 요청서(X_8)의 검증이 완료되었음을 나타내는 단계를 포함하여 구성되는 것을 특징으로 하는 블록체인을 기반으로 한 IoT 디바이스 접근 제어 방법

청구항 5

제 1항에 있어서,

상기 IoT 서비스가 IoT 디바이스로 접근하는 단계에서는

IoT 서비스가 유효한 접근 토큰(Y_4)이 포함된 인가 페이로드(X_9), 인가 페이로드의 해시(Y_5), 인가 페이로드의 해시에 대한 서명(C_5) 및 접근 요청서(X_{10})가 포함된 접근 정보를 생성하는 단계;

IoT 서비스가 접근 요청서(X_{10})를 IoT 게이트웨이로 전송하는 단계;

IoT 게이트웨이가 접근 요청서의 암호(X_{10})를 해독하고, 인가 페이로드의 해시에 대한 서명(C_5)의 유효성을 검증하는 단계;

IoT 게이트웨이가 접근 토큰(Y_4)의 유효성을 검사하는 단계;

IoT 게이트웨이가 응답 메시지(X_{12})를 포함한 응답 정보를 생성하는 단계;

IoT 게이트웨이가 응답 메시지(X_{12})를 IoT 서비스로 전송하는 단계;

IoT 서비스가 응답 메시지(X_{12})의 암호를 해독하고, IoT 게이트웨이의 서명(C_6)의 유효성을 검증하는 단계;

IoT 서비스가 IoT 서비스에 대한 임의의 비밀로부터 새로운 비밀키(k)를 생성하고, IoT 리소스 메시지(M)를 생성한 후, IoT 리소스 메시지(M) 및 접근 토큰(Y_4)을 연결한 식을 암호화한 메시지(X_{13})를 생성하는 단계;

IoT 서비스가 메시지(X_{13})를 IoT 게이트웨이로 전송하는 단계;

IoT 게이트웨이가 IoT 게이트웨이에 대한 임의의 비밀로부터 비밀키(k)를 생성하고, 메시지(X_{13})의 암호를 해독하는 단계;

IoT 게이트웨이가 접근 토큰(Y_4)의 유효성을 점검하는 단계;

IoT 게이트웨이가 비밀키(k)를 사용하여 IoT 리소스 메시지(M)에 대한 응답 메시지(X_{14})를 생성하는 단계; 및

IoT 게이트웨이가 IoT 리소스 메시지(M)에 대한 응답 메시지(X_{14})를 IoT 서비스로 전송하는 단계를 포함하여 구성되는 것을 특징으로 하는 블록체인을 기반으로 한 IoT 디바이스 접근 제어 방법

청구항 6

제 1항에 있어서,

상기 IoT 서비스의 접근을 해지하는 단계에서는

IoT 도메인 소유자가 접근을 해지하고자 하는 IoT 서비스에 대해 접근 토큰(Y_4)을 검색하는 단계;

IoT 도메인 소유자가 접근 토큰(Y_4)을 입력하여 생성된 트랜잭션을 스마트계약으로 전송하는 단계;

스마트계약이 접근 토큰(Y_4)의 타겟이 IoT 게이트웨이의 주소(a_{GW})와 일치하는지 확인하기 위해 인가 목록을 검사하는 단계; 및

스마트계약이 접근 토큰(Y_4)의 해지 파라미터 값을 True로 설정하는 단계를 포함하여 구성되는 것을 특징으로 하는 블록체인을 기반으로 한 IoT 디바이스 접근 제어 방법

발명의 설명

기술 분야

본 발명은 블록체인을 기반으로 한 IoT 디바이스 접근 제어 방법에 관한 것으로서, 더욱 상세하게는 접근이 인가된 IoT 서비스만이 IoT 게이트웨이에 속한 IoT 디바이스에 접근할 수 있도록 제어하고, 해지하고자 하는 IoT

[0001]

서비스에 대해 적합한 해지 절차를 제공하는 블록체인을 기반으로 한 IoT 디바이스 접근 제어 방법에 관한 것이다.

배경 기술

- [0003] 사물인터넷(Internet of Things, IoT)은 사물에 센서를 부착해 실시간 데이터를 인터넷으로 주고받는 기술이나 환경을 의미한다. 사물인터넷으로 인해 인간은 이전보다 향상된 생활을 영위할 수 있다. 예를 들면, 사물인터넷은 인간이 낯선 지역을 헤매지 않고 한번에 찾아갈 수 있도록 안내할 수 있고, 비가 내리기 직전에 인간이 우산을 쓸 수 있도록 안내할 수 있다. 또한, 사물 인터넷은 스마트 홈, 스마트 도시, 스마트 산업 등 여러 분야에 적용되고 있고, 사물 인터넷이 성장함에 따라 수많은 디바이스가 인터넷에 연결되고 있다.
- [0005] 그러나, 최근에 사물 인터넷 관련 보안 사고가 과거에 비해 급속도로 증가하고 있다. 우선, 라즈베리 파이 디바이스에 의해 NASA 제트 추진 연구소 네트워크가 해킹당한 사례가 있다. 또한, 악성 코드에 감염된 수천만대의 사물 인터넷 디바이스들이 Dyn이라는 미국 DNS 서비스 업체에 디도스 공격을 가하여 미국 동부의 DNS 서비스를 마비시킨 사례가 있다.
- [0007] 사물 인터넷 네트워크에 적절한 접근 제어 메커니즘을 제공하는 경우 이러한 보안 사고를 방지할 수 있다. 그러나, 사물 인터넷 디바이스에 대해 견고한 접근 제어 메커니즘을 제공하는 것은 어려운 일이다.
- [0009] 어떤 사물 인터넷 디바이스는 자체 보안을 위한 암호화에 필수적인 계산 리소스를 갖고 있지 않을 수 있다. 또한, 다른 사물 인터넷 디바이스는 암호화를 전혀 수행할 수 없다.
- [0011] 그리고, 사물 인터넷 디바이스는 호환성에 제한이 있다. 보안 프로토콜이 특정 프로토콜에서는 정상적으로 작동하지만 다른 프로토콜에서는 작동하지 않을 수 있다.
- [0013] 또한, 사물 인터넷 아키텍처는 중앙 집중형 모델에서 분산형 모델로 이동하고 있다. 중앙에서 시스템을 관리하지 않는 분산된 환경에서 신뢰 모델을 정의하는 것은 보다 문제가 된다.

선행기술문헌

특허문헌

- [0015] (특허문헌 0001) KR 1020190026394 A
(특허문헌 0002) KR 101677249 B1

비특허문헌

발명의 내용

해결하려는 과제

- [0017] 본 발명은 상기와 같은 문제점을 해결하기 위하여 제안된 것으로, 복수 개의 IoT 디바이스를 포함하고 있는 IoT 게이트웨이로 접근하는 IoT 서비스에 대해 IoT 게이트웨이가 IoT 서비스의 접근을 인가하는 방법 및 IoT 서비스

에 대해 접근 인가를 해지하는 방법을 제공한다.

과제의 해결 수단

- [0019] 상기의 과제를 해결하기 위한 본 발명의 실시예에 따르면, 블록체인을 기반으로 한 IoT 디바이스 접근 제어 방법은 IoT 서비스의 접근 인가를 준비하는 단계, IoT 서비스의 요청에 의해 IoT 게이트웨이가 IoT 서비스의 접근을 인가하는 단계, IoT 서비스가 IoT 디바이스로 접근하는 단계 및 IoT 서비스의 접근을 해지하는 단계를 포함하여 구성되는 것을 특징으로 한다.
- [0021] 또한, 상기 IoT 서비스의 접근 인가를 준비하는 단계에서는 IoT 서비스가 IoT 서비스의 공개키(PK_S), IoT 서비스의 개인키(SK_S) 및 IoT 서비스의 주소(α_S)를 생성하는 단계, IoT 서비스가 IoT 게이트웨이에서 IoT 게이트웨이의 주소(α_{GW}), IoT 게이트웨이의 IP 주소(γ_{GW}) 및 IoT 게이트웨이의 공개키(PK_GW)를 검색하는 단계 및 IoT 게이트웨이가 인가 서버를 네트워크에 설치하는 단계를 포함하여 구성되는 것을 특징으로 한다.
- [0023] 또한, 상기 IoT 서비스의 요청에 의해 IoT 게이트웨이가 IoT 서비스의 접근을 인가하는 단계에서는 IoT 서비스가 이용 가능한 접근 목록(A)을 IoT 게이트웨이에 요구하는 단계, IoT 게이트웨이가 이용 가능한 접근 목록(A), 접근 목록의 해시(Y_3) 및 접근 목록의 해시에 대한 서명(C_3)이 포함된 응답 정보를 생성하는 단계, IoT 게이트웨이가 이용 가능한 접근 목록(A) 및 접근 목록의 해시에 대한 서명(C_3)을 IoT 서비스로 전송하는 단계, IoT 서비스가 접근 목록의 해시에 대한 서명(C_3)을 검증하는 단계, IoT 서비스가 IoT 게이트웨이 및 IoT 디바이스의 인증 완료 여부를 다시 점검하는 단계, IoT 서비스가 접근하기 원하는 접근 목록(A'), 인가 페이로드(X_7) 및 인가 페이로드의 해시(Y_4)를 생성하는 단계, IoT 서비스가 인가 페이로드의 해시(Y_4), 소스인 발신자 IoT 서비스의 주소(α_S) 및 인가 타겟인 IoT 게이트웨이의 주소(α_{GW})를 스마트계약으로 전송하는 단계, 스마트계약이 IoT 서비스가 인가 페이로드의 해시(Y_4), 소스인 발신자 IoT 서비스의 주소(α_S) 및 인가 타겟인 IoT 게이트웨이의 주소(α_{GW})를 스마트계약의 인가 목록에 저장하는 단계, 스마트계약이 트랜잭션 해시를 IoT 서비스로 반환하는 단계, IoT 서비스가 IoT 서비스에 대한 인가 요청서(X_8)를 생성하는 단계, IoT 서비스가 IoT 서비스에 대한 인가 요청서(X_8)를 IoT 게이트웨이로 전송하는 단계, IoT 게이트웨이가 IoT 서비스에 대한 인가 요청서(X_8)를 검증하는 단계, IoT 게이트웨이가 인가 페이로드의 해시(Y_4)가 포함된 인가 결과를 스마트계약으로 전송하는 단계, IoT 게이트웨이가 IoT 서비스가 접근하기 원하는 접근 목록(A')을 IoT 게이트웨이의 데이터베이스에 저장하는 단계, IoT 게이트웨이가 인가 페이로드의 해시(Y_4)가 포함된 인가 결과를 스마트계약으로 전송하는 단계, 스마트계약이 인가 페이로드의 해시(Y_4)를 활성화시켜 IoT 서비스에 대한 접근 토큰(Y_4)을 생성하는 단계, 스마트계약이 트랜잭션 해시를 IoT 게이트웨이로 반환하는 단계 및 IoT 게이트웨이가 인가 완료 메시지를 IoT 서비스로 전송하는 단계를 포함하여 구성되는 것을 특징으로 한다.
- [0025] 또한, 상기 IoT 게이트웨이가 IoT 서비스에 대한 인가 요청서(X_8)를 검증하는 단계에서는 IoT 게이트웨이가 IoT 서비스에 대한 인가 요청서(X_8)의 암호를 해독하는 단계, IoT 게이트웨이가 재전송 공격을 방지하기 위한 임의의 문자열(n)이 이전에 한번도 사용된 적이 없는 새로운 것인지 확인하는 단계, IoT 게이트웨이가 인가 페이로드의 해시(Y_4)를 계산하는 단계, IoT 게이트웨이가 스마트계약에서 소스인 발신자 IoT 서비스의 주소(α_S), 인가 타겟인 IoT 게이트웨이의 주소(α_{GW})를 획득하는 단계, IoT 게이트웨이가 인가 타겟과 IoT 게이트웨이의 주소(α_{GW})가 일치하는지 검사하는 단계, IoT 게이트웨이가 인가 페이로드의 해시에 대한 서명(C_4)을 검증하는 단계, IoT 게이트웨이가 IoT 게이트웨이의 데이터베이스로부터 IoT 서비스가 보유하고 있는 접근 목록(A_S)을 획득하는 단계, IoT 게이트웨이가 IoT 서비스가 접근하기 원하는 접근 목록(A')이 IoT 서비스가 보유하고 있는 접근 목록(A_S)의 부분 집합인지 확인하는 단계, 및 True 값을 반환함으로써 IoT 서비스에 인가 요청서(X_8)의 검증이 완료

되었음을 나타내는 단계를 포함하여 구성되는 것을 특징으로 한다.

[0027] 또한, 상기 IoT 서비스가 IoT 디바이스로 접근하는 단계에서는 IoT 서비스가 유효한 접근 토큰(Y_4)이 포함된 인가 페이로드(X_9), 인가 페이로드의 해시(Y_5), 인가 페이로드의 해시에 대한 서명(C_5) 및 접근 요청서(X_{10})가 포함된 접근 정보를 생성하는 단계, IoT 서비스가 접근 요청서(X_{10})를 IoT 게이트웨이로 전송하는 단계, IoT 게이트웨이가 접근 요청서의 암호(X_{10})를 해독하고, 인가 페이로드의 해시에 대한 서명(C_5)의 유효성을 검증하는 단계, IoT 게이트웨이가 접근 토큰(Y_4)의 유효성을 검사하는 단계, IoT 게이트웨이가 응답 메시지(X_{12})를 포함한 응답 정보를 생성하는 단계, IoT 게이트웨이가 응답 메시지(X_{12})를 IoT 서비스로 전송하는 단계, IoT 서비스가 응답 메시지(X_{12})의 암호를 해독하고, IoT 게이트웨이의 서명(C_6)의 유효성을 검증하는 단계, IoT 서비스가 IoT 서비스에 대한 임의의 비밀로부터 새로운 비밀키(k)를 생성하고, IoT 리소스 메시지(M)를 생성한 후, IoT 리소스 메시지(M) 및 접근 토큰(Y_4)을 연결한 식을 암호화한 메시지(X_{13})를 생성하는 단계, IoT 서비스가 메시지(X_{13})를 IoT 게이트웨이로 전송하는 단계, IoT 게이트웨이가 IoT 게이트웨이에 대한 임의의 비밀로부터 비밀키(k)를 생성하고, 메시지(X_{13})의 암호를 해독하는 단계, IoT 게이트웨이가 접근 토큰(Y_4)의 유효성을 점검하는 단계, IoT 게이트웨이가 비밀키(k)를 사용하여 IoT 리소스 메시지(M)에 대한 응답 메시지(X_{14})를 생성하는 단계 및 IoT 게이트웨이가 IoT 리소스 메시지(M)에 대한 응답 메시지(X_{14})를 IoT 서비스로 전송하는 단계를 포함하여 구성되는 것을 특징으로 한다.

[0029] 또한, 상기 IoT 서비스의 접근을 해지하는 단계에서는 IoT 도메인 소유자가 접근을 해지하고자 하는 IoT 서비스에 대해 접근 토큰(Y_4)을 검색하는 단계, IoT 도메인 소유자가 접근 토큰(Y_4)을 입력하여 생성된 트랜잭션을 스마트계약으로 전송하는 단계, 스마트계약이 접근 토큰(Y_4)의 타겟이 IoT 게이트웨이의 주소(a_{GW})와 일치하는지 확인하기 위해 인가 목록을 검사하는 단계 및 스마트계약이 접근 토큰(Y_4)의 해지 파라미터 값을 True로 설정하는 단계를 포함하여 구성되는 것을 특징으로 한다.

발명의 효과

[0032] 본 발명은 블록체인 내에서 IoT 서비스에 대해 일관된 접근 제어 규칙을 제공하고, IoT 게이트웨이 및 IoT 서비스 간에 신뢰성 있는 보안 채널을 구축하여 IoT 서비스와 IoT 게이트웨이 내에 속한 IoT 디바이스 상호 간에 안전하게 정보를 교환할 수 있는 효과가 있다.

[0034] 또한, 본 발명의 블록체인 내에서 분산된 공개키를 통한 인가 시스템을 통해서 사용자의 개인 정보를 안전하게 보관할 수 있을 뿐만 아니라, 견고하고 무결한 해지 서비스를 제공하고, 중앙 집중형 시스템에서 일반적으로 적용되는 인증 표준 규격 X.509 인증 시스템을 대체할 수 있는 효과가 있다.

도면의 간단한 설명

[0036] 도 1은 블록체인을 기반으로 한 IoT 디바이스 접근 제어 시스템의 구성도이다.

도 2는 IoT 서비스의 접근 인가를 준비하는 단계에 대한 순서도이다.

도 3은 IoT 서비스의 접근을 인가하는 단계에 대한 순서도이다.

도 4는 IoT 게이트웨이가 IoT 서비스에 대한 인가 요청서를 검증하는 단계에 대한 알고리즘이다.

도 5는 IoT 서비스가 IoT 디바이스로 접근하는 단계에 대한 순서도이다.

도 6은 IoT 서비스의 접근을 해지하는 단계에 대한 순서도이다.

발명을 실시하기 위한 구체적인 내용

- [0037] 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.
- [0039] 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.
- [0041] 도 1은 블록체인을 기반으로 한 IoT 디바이스 접근 제어 시스템의 구성도이다.
- [0043] 도 1을 참조하면, IoT 디바이스 접근 제어 시스템은 IoT 게이트웨이, IoT 도메인 소유자, IoT 벤더, 인터넷 서비스 공급자(Internet Service Provider, ISP) 및 IoT 서비스를 포함하여 구성된다.
- [0045] IoT 게이트웨이는 IoT 서비스가 IoT 디바이스에 대해 접근하는 것을 제어하고, IoT 게이트웨이에 속한 IoT 디바이스가 블록체인 내의 다른 엔티티(entity)와 통신을 수행하기 위한 창구 역할을 한다.
- [0047] IoT 도메인 소유자는 IoT 게이트웨이 및 IoT 디바이스의 소유자로서, IoT 게이트웨이를 생성하고, IoT 벤더로부터 IoT 디바이스를 구입하여, IoT 게이트웨이를 복수개의 IoT 디바이스와 연결하여, IoT 도메인을 생성한다. 또한, IoT 도메인 소유자는 IoT 게이트웨이 및 IoT 게이트웨이에 속한 디바이스를 블록체인 내의 다른 엔티티(entity)에게 공개한다.
- [0049] IoT 벤더는 IoT 디바이스의 제조자로서, IoT 도메인 소유자에게 IoT 디바이스를 공급하고, IoT 도메인 소유자의 요청에 의해 IoT 디바이스에 대한 인증을 수행한다.
- [0051] 인터넷 서비스 공급자(Internet Service Provider, ISP)는 IoT 도메인 소유자의 요청에 의해 IoT 게이트웨이에 대한 인증을 수행한다.
- [0053] IoT 서비스는 IoT 디바이스에 접근하여 IoT 데이터를 수집한다. 또한, IoT 서비스는 조명 켜기 등과 같은 명령을 전송하여 IoT 디바이스를 지시한다.
- [0055] 스마트계약은 블록체인 내에서 IoT 게이트웨이 및 IoT 디바이스에 대한 인증 목록 및 IoT 서비스에 대한 인가 목록을 관리한다.
- [0057] 본 발명에서 사용되는 기호에 대해 설명한다.
- [0059] α_L 은 블록체인의 내부 또는 블록체인의 외부에서 L의 아이디(identity, ID)로 사용되는 L의 주소이다. $PKE_{PK_x}(J)$ 는 공개키(public key) x를 사용하여 공개키 J를 암호화하는 것이다. $PKD_{SK_y}(K)$ 는 개인키(private key) y를 사용하여 공개키 K의 암호를 해독하는 것이다. $E_z(J)$ 는 사전 공유키(pre-shared key) z를 사용하여 대

칭키(symmetric key) J 를 암호화하는 것이다. $D_z(K)$ 는 사전 공유키(pre-shared key) z 를 사용하여 대칭키(symmetric key) J 의 암호를 해독하는 것이다.

- [0061] $SIGN_{SK_y}(J)$ 는 개인키 y 를 사용하여 데이터 J 에 대한 서명을 생성하는 것이다. $VERIFY_{PK_x}(K)$ 는 공개키 x 를 사용하여 서명 K 를 검증하는 것이다. $VERIFY(K, J, \alpha_L)$ 은 데이터 J 에 대한 서명 K 가 L 의 주소 α_L 에 의해 서명되었는지 검증하는 것이다.
- [0063] $H(J)$ 는 데이터 J 의 해시를 생성하는 것을 의미하며, $X||Y$ 는 X 와 Y 의 연접(concatenation)을 의미한다.
- [0065] 또한, 본 발명에서 사용되는 엔티티(entity)에 대한 기호를 설명한다.
- [0067] D 는 IoT 디바이스(device)이다. GW 는 IoT 게이트웨이(gateway)이다. V 는 IoT 벤더(vendor)다. S 는 IoT 서비스(service)이다. O 는 IoT 도메인 소유자(domain owner)이다. ISP 는 인터넷 서비스 공급자(Internet Service Provider)이다. SC 는 스마트계약(smart contract)이다.
- [0069] 블록체인을 기반으로 한 IoT 디바이스 접근 제어 방법은 IoT 서비스의 접근 인가를 준비하는 단계, IoT 서비스의 요청에 의해 IoT 게이트웨이가 IoT 서비스의 접근을 인가하는 단계, IoT 서비스가 IoT 디바이스로 접근하는 단계 및 IoT 서비스의 접근을 해지하는 단계를 포함하여 구성된다.
- [0071] 먼저, IoT 서비스의 접근 인가를 준비하는 단계에 대해 설명한다.
- [0073] IoT 게이트웨이 및 IoT 게이트웨이에 속한 모든 IoT 디바이스에 대한 인증은 완료된 것으로 가정한다. 따라서, IoT 도메인 소유자는 IoT 게이트웨이 및 IoT 게이트웨이에 속한 모든 IoT 디바이스를 신뢰할 수 있다.
- [0075] 또한, IoT 게이트웨이는 IoT 게이트웨이가 보유한 접근 목록을 다른 엔티티(entity)에게 공개하고, IoT 서비스는 IoT 게이트웨이로 접근을 시도한다.
- [0077] 도 2는 IoT 서비스의 접근 인가를 준비하는 단계에 대한 순서도이다.
- [0079] 도 2를 참조하면, IoT 서비스는 IoT 서비스의 공개키(PK_S), IoT 서비스의 개인키(SK_S) 및 IoT 서비스의 주소(α_S)를 생성한다.(S101)
- [0081] 그 이후, IoT 서비스는 IoT 게이트웨이에서 IoT 게이트웨이의 주소(α_{GW}), IoT 게이트웨이의 IP 주소(γ_{GW}) 및 IoT 게이트웨이의 공개키(PK_{GW})를 검색한다.(S102)
- [0083] 그 이후, IoT 게이트웨이는 IoT 게이트웨이의 IP 주소(γ_{GW})를 통해 찾을 수 있는 인가 서버(authorization server)를 네트워크에 설치한다.(S103)

- [0085] 다음으로, IoT 서비스의 요청에 의해 IoT 게이트웨이가 IoT 서비스의 접근을 인가하는 단계에 대해 설명한다.
- [0087] 도 3은 IoT 서비스의 접근을 인가하는 단계에 대한 순서도이다.
- [0089] 도 3을 참조하면, IoT 서비스는 IoT 서비스가 이용 가능한 접근 목록(A)을 IoT 게이트웨이에 요구한다.(S201)
- [0091] 구체적으로, IoT 서비스는 IoT 게이트웨이의 IP 주소(y_{GW})를 사용하여, IoT 서비스가 이용 가능한 접근 목록(A)을 IoT 게이트웨이에 요구한다.
- [0093] 그 이후, IoT 게이트웨이는 이용 가능한 접근 목록(A), 접근 목록의 해시(Y_3) 및 접근 목록의 해시에 대한 서명(C_3)이 포함된 응답 정보를 생성한다.(S202)
- [0095] 이 때, 생성되는 응답 정보는 다음과 같다.
- [0097] $A=\{a_1, a_2, a_3, \dots, a_n\}$
- [0098] $Y_3=H(A)$
- [0099] $C_3=SIGN_{SK_{GW}}(Y_3)$
- [0101] 여기서, A는 IoT 게이트웨이를 통해 공개된 이용 가능한 접근 목록이고, Y_3 는 접근 목록(A)의 해시이다. 그리고, C_3 는 IoT 게이트웨이의 개인키(SK_{GW})를 사용하여 접근 목록의 해시(Y_3)에 대해 서명을 생성하는 것이다.
- [0103] 그 이후, IoT 게이트웨이는 이용 가능한 접근 목록(A) 및 접근 목록의 해시에 대한 서명(C_3)을 IoT 서비스로 전송한다.(S203)
- [0105] 그 이후, IoT 서비스는 접근 목록의 해시에 대한 서명(C_3)을 검증한다.(S204)
- [0107] 구체적으로, IoT 서비스는 다음 식을 통해 이용 가능한 접근 목록(A)으로부터 접근 목록의 해시(Y_3)를 생성한다.
- [0108]
- [0109] $Y_3 \leftarrow H(A)$
- [0111] 그리고, IoT 서비스는 다음 식을 통해 접근 목록의 해시에 대한 서명(C_3)을 검증한다.

- [0113] $\text{VERIFY}(C_3, Y_3, a_{GW}) == \text{True}$
- [0115] 여기서, $\text{VERIFY}(C_3, Y_3, a_{GW})$ 는 접근 목록의 해시(Y_3)에 대한 서명(C_3)이 IoT 게이트웨이의 주소(a_{GW})에 의해 서명되었는지 검증하는 것이다.
- [0117] 그 이후, IoT 서비스는 IoT 게이트웨이 및 IoT 디바이스의 인증 완료 여부를 다시 점검한다.(S205)
- [0119] 구체적으로, IoT 서비스는 스마트계약에 인증 결과를 문의함으로써 IoT 게이트웨이 및 IoT 디바이스의 인증 완료 여부를 점검할 수 있다.
- [0121] 그 이후, IoT 서비스는 IoT 서비스가 접근하기 원하는 접근 목록(A'), 인가 페이로드(X_7) 및 인가 페이로드의 해시(Y_4)를 생성한다.(S206)
- [0123] 이 때 생성되는 식은 다음과 같다.
- [0125] $A' = \{a_1', a_2', a_3', \dots, a_n'\}$
- [0126] $X_7 = A' || n$
- [0127] $Y_4 = H(X_7)$
- [0129] 여기서, A' 은 IoT 서비스가 접근하기 원하는 접근 목록으로, A' 은 공개된 이용 가능한 접근 목록(A)의 부분집합이다. 그리고, X_7 은 IoT 서비스가 접근하기 원하는 접근 목록(A')과 재전송 공격을 방지하기 위한 임의의 문자열(n)을 연결한 인가 페이로드이고, Y_4 는 인가 페이로드(X_7)의 해시이다.
- [0131] 그 이후, IoT 서비스가 인가 페이로드의 해시(Y_4), 소스(source)인 발신자(sender) IoT 서비스의 주소(a_s), 인가 타겟(authorization target)인 IoT 게이트웨이의 주소(a_{GW})를 스마트계약으로 전송한다.(S207)
- [0133] 그 이후, 스마트계약은 인가 페이로드의 해시(Y_4), 소스(source)인 발신자(sender) IoT 서비스의 주소(a_s), 인가 타겟(authorization target)인 IoT 게이트웨이의 주소(a_{GW})를 스마트계약의 인가 목록에 저장한다.(S208)
- [0135] 스마트계약은 인가 목록을 유지 관리한다. 인가 목록의 각 로그는 상태(status) 및 해지(revocation)라는 2개의 파라미터(parameter)를 갖고 있다. 스마트계약은 파라미터 2개의 기본 값을 False로 설정한다. 상태(status) 파라미터는 인증 및 인가가 완료되었음을 의미하고, 해지(revocation) 파라미터는 인증 및 인가가 해지되었음을 의미한다. 따라서, 인가 페이로드의 해시(Y_4)의 상태(status) 파라미터 및 해지(revocation) 파라미터 값은 둘 다 False로 설정된다.

- [0137] 그 이후, 스마트계약은 트랜잭션 영수증으로 트랜잭션 해시를 IoT 서비스로 반환한다.(S209)
- [0139] 그 이후, IoT 서비스는 IoT 서비스에 대한 인가 요청서(X_8)를 생성한다.(S210)
- [0141] 이 때 생성되는 식은 다음과 같다.
- [0143] $C_4 = \text{SIGN}_{\text{SK}_S}(Y_4)$
- [0144] $X_8 = \text{PKE}_{\text{PK}_{\text{GW}}}(X_7 || C_4)$
- [0146] 여기서, C_4 은 IoT 서비스의 개인키(SK_S)를 사용하여, 인가 페이로드의 해시(Y_4)에 서명한 것이고, X_8 는 IoT 게이트웨이의 공개키(PK_{GW})를 사용하여, 인가 페이로드(X_7)와 인가 페이로드의 해시(Y_4)를 연결한 식 $X_7 || C_4$ 를 암호화한 것이다. 다시 말해서, C_4 은 인가 페이로드의 해시에 대한 서명이고, X_8 는 IoT 서비스에 대한 인가 요청서이다.
- [0148] 그 이후, IoT 서비스는 IoT 서비스에 대한 인가 요청서(X_8)를 IoT 게이트웨이로 전송한다.(S211)
- [0150] 그 이후, IoT 게이트웨이는 IoT 서비스에 대한 인가 요청서(X_8)를 검증한다.(S212)
- [0152] 도 4는 IoT 게이트웨이가 IoT 서비스에 대한 인가 요청서를 검증하는 단계에 대한 알고리즘이다.
- [0154] 도 4를 참조하면, IoT 게이트웨이는 다음 식을 통해 IoT 서비스에 대한 인가 요청서(X_8)의 암호를 해독한다.(S301)
- [0156] $X_7 || C_4 \leftarrow \text{PKD}_{\text{SK}_{\text{GW}}}(X_8)$
- [0158] 여기서, $\text{PKD}_{\text{SK}_{\text{GW}}}(X_8)$ 은 IoT 게이트웨이의 개인키(SK_{GW})를 사용하여 IoT 서비스에 대한 인가 요청서(X_8)의 암호를 해독하는 것이다. 암호 해독을 통해 IoT 서비스의 인가 페이로드(X_7) 및 인가 페이로드의 해시에 대한 서명(C_4)을 알 수 있다.
- [0160] 그 이후, IoT 게이트웨이는 isFreshNonce 함수를 이용하여 재전송 공격을 방지하기 위한 임의의 문자열(n)이 이전에 한번도 사용된 적이 없는 새로운 것인지 확인한다.(S302)
- [0162] $\text{isFreshNonce}(n)$

- [0164] 그 이후, IoT 게이트웨이는 다음 식을 이용하여 인가 페이로드의 해시(Y_4)를 계산한다.(S303)
- [0166] $Y_4 \leftarrow H(X_7)$
- [0168] 그리고, IoT 게이트웨이는 getAuthorizationPayload 함수를 사용하여 스마트계약에서 소스(source)인 발신자(sender) IoT 서비스의 주소(α_s), 인가 타겟(authorization target)인 IoT 게이트웨이의 주소(α_{GW})를 획득한다.(S304)
- [0170] $source, target \leftarrow getAuthorizationPayload(Y_4)$
- [0172] 그 이후, IoT 게이트웨이는 인가 타겟(authorization target)과 IoT 게이트웨이의 주소(α_{GW})가 일치하는지 검사한다.(S305)
- [0174] 구체적으로, IoT 게이트웨이는 다음 식을 통해 인가 타겟(authorization target)과 IoT 게이트웨이의 주소(α_{GW})를 비교함으로써, 인가 요청서가 실제로 IoT 게이트웨이에 대한 것이 맞는지 검사한다.
- [0176] $target == \alpha_{GW}$
- [0178] 그 이후, IoT 게이트웨이는 인가 페이로드의 해시에 대한 서명(C_4)을 검증한다.(S306)
- [0180] $VERIFY(C_4, Y_4, source)$
- [0182] 여기서, $VERIFY(C_4, Y_4, source)$ 는 인가 페이로드의 해시(Y_4)에 대한 서명(C_4)이 소스(source)인 발신자(sender) IoT 서비스의 주소(α_s)에 의해 서명되었는지 검증하는 것이다.
- [0184] IoT 게이트웨이는 getAccessInfo 함수를 사용하여 IoT 게이트웨이의 데이터베이스로부터 IoT 서비스가 보유하고 있는 접근 목록(A_s)을 획득한다.(S307)
- [0186] $A_s \leftarrow getAccessInfo(source)$
- [0188] 그 이후, IoT 게이트웨이는 IoT 서비스가 접근하기 원하는 접근 목록(A')이 IoT 서비스가 보유하고 있는 접근 목록(A_s)의 부분 집합인지 확인한다.(S308)
- [0190] $A' \subset A_s$

- [0192] 마지막으로, 모든 단계가 완료되면, 도 4의 알고리즘은 True 값을 반환함으로써 IoT 서비스에 인가 요청서(X_8)의 검증이 완료되었음을 나타낸다.(S309)
- [0194] IoT 서비스에 대한 인가 요청서(X_8)의 검증이 완료되면, IoT 게이트웨이는 IoT 서비스가 접근하기 원하는 접근 목록(A')을 IoT 게이트웨이의 데이터베이스에 저장한다.(S213)
- [0196] 그 이후, IoT 게이트웨이는 인가 페이로드의 해시(Y_4)가 포함된 인가 결과를 스마트계약으로 전송한다.(S214)
- [0198] 그 이후, 스마트계약은 인가 페이로드의 해시(Y_4)를 활성화시켜 IoT 서비스에 대한 접근 토큰(Y_4)을 생성한다.(S215)
- [0200] 구체적으로, 스마트계약은 인가 페이로드의 해시(Y_4)의 상태(status) 파라미터 값을 True로 설정한다. 이로써, 인가 페이로드의 해시(Y_4)는 접근 토큰으로 활성화된다.
- [0202] 그 이후, 스마트계약은 트랜잭션 영수증으로 트랜잭션 해시를 IoT 게이트웨이로 반환한다.(S216)
- [0204] 그 이후, IoT 게이트웨이가 인가 완료 메시지를 IoT 서비스로 전송한다.(S217)
- [0206] 모든 단계가 완료되면, IoT 서비스는 IoT 게이트웨이에 접근하기 위해 접근 토큰(Y_4)을 이용할 수 있다.
- [0208] IoT 서비스가 IoT 디바이스로 접근하는 단계를 설명한다.
- [0210] IoT 서비스가 IoT 디바이스로 접근 시 전제 조건은 다음과 같다.
- [0212] 먼저, IoT 게이트웨이 및 IoT 게이트웨이에 속한 모든 IoT 디바이스에 대한 인증이 완료되었으므로, IoT 도메인 소유자는 IoT 게이트웨이 및 IoT 게이트웨이에 속한 모든 IoT 디바이스를 신뢰할 수 있다.
- [0214] 또한, IoT 게이트웨이는 인가된 접근 목록(A') 및 접근 토큰(Y_4)을 IoT 서비스에게 제공한다.
- [0216] 도 5는 IoT 서비스가 IoT 디바이스로 접근하는 단계에 대한 순서도이다.
- [0218] 도 5를 참조하면, IoT 서비스는 유효한 접근 토큰(Y_4)이 포함된 인가 페이로드(X_9), 인가 페이로드의 해시(Y_5), 인가 페이로드의 해시에 대한 서명(C_5) 및 접근 요청서(X_{10})가 포함된 접근 정보를 생성한다.(S401)

[0220] 이 때 생성되는 접근 정보는 다음과 같다.

[0222] g^a

[0223] $X_9 = Y_4 || g^a || PK_S || n$

[0224] $Y_5 = H(X_9)$

[0225] $C_5 = \text{SIGN}_{SK_S}(Y_5)$

[0226] $X_{10} = \text{PKE}_{PK_GW}(X_9 || C_5)$

[0228] 여기서, g^a 는 디피 헬먼(Diffie Hellman) 키 교환 방법에 사용되는 IoT 게이트웨이에 대한 임의의 비밀(random secret)이다. 그리고, PK_S는 IoT 서비스의 공개키이고, n 는 재전송 공격을 방지하기 위한 임의의 문자열이다. 그리고, X_9 는 유효한 접근 토큰(Y_4)이 포함된 인가 페이로드이고, Y_5 는 인가 페이로드의 해시이다. 그리고, C_5 은 IoT 서비스의 개인키(SK_S)를 사용하여, 인가 페이로드의 해시(Y_5)에 대해 서명한 것이고, X_{10} 는 IoT 게이트웨이의 공개키(PK_GW)를 사용하여 $X_9 || C_5$ 를 암호화한 것이다.

[0230] 그 이후, IoT 서비스는 접근 요청서(X_{10})를 IoT 게이트웨이로 전송한다.(S402)

[0232] 그 이후, IoT 게이트웨이는 접근 요청서의 암호(X_{10})를 해독하고, 인가 페이로드의 해시에 대한 서명(C_5)의 유효성을 검증한다.(S403)

[0234] 먼저, IoT 게이트웨이는 다음 식을 통해 접근 요청서(X_{10})의 암호를 해독한다.

[0236] $X_9 || C_5 \leftarrow \text{PKD}_{SK_GW}(X_{10})$

[0238] 여기서 $\text{PKD}_{SK_GW}(X_{10})$ 는 IoT 게이트웨이의 개인키(SK_GW)를 사용하여 접근 요청서(X_{10})의 암호를 해독하는 것이다. 암호 해독을 통해 인가 페이로드(X_9) 및 인가 페이로드의 해시에 대한 서명(C_5)을 알 수 있다.

[0240] 두 번째, IoT 게이트웨이는 재전송 공격을 방지하기 위한 임의의 문자열(n)의 유효성을 확인한다.

[0242] 세 번째, IoT 게이트웨이가 다음 식을 통해 인가 페이로드의 해시(Y_5)를 생성한다.

[0244] $Y_5 \leftarrow H(X_9)$

[0246] 네 번째, IoT 게이트웨이는 다음 식을 통해 인가 페이로드의 해시에 대한 서명(C_5)의 유효성을 검증한다.

[0248] $\text{VERIFY}(C_5, Y_5, a_s) == \text{True}$

[0250] 여기서, $\text{VERIFY}(C_5, Y_5, a_s)$ 는 인가 페이로드의 해시(Y_5)에 대한 서명(C_5)이 IoT 서비스의 주소(a_s)에 의해 서명되었는지 검증하는 것이다.

[0252] 그 이후, IoT 게이트웨이는 접근 토큰(Y_4)의 유효성을 검사한다.(S404)

[0254] 구체적으로, IoT 게이트웨이는 스마트계약에서 접근 토큰(Y_4)의 상태(status) 파라미터 값이 True로 설정되어 있는지 검사하고, 인가 목록에서 접근 토큰(Y_4)을 소스(source)인 발신자(sender) IoT 서비스의 주소(a_s)와 비교하여 접근 토큰(Y_4)이 실제로 IoT 서비스의 주소(a_s)에 대한 것이 맞는지 확인한다.

[0256] 그 이후, IoT 게이트웨이는 응답 메시지(X_{12})를 포함한 응답 정보를 생성한다.(S405)

[0258] 이 때, 생성되는 응답 정보는 다음과 같다.

[0260] g^b

[0261] n'

[0262] $X_{11} = g^b || n'$

[0263] $Y_6 = H(X_{11})$

[0264] $C_6 = \text{SIGN}_{\text{SK_GW}}(Y_6)$

[0265] $X_{12} = \text{PKE}_{\text{PK_S}}(X_{11} || C_6)$

[0267] 여기서, g^b 는 디피 헬먼(Diffie Hellman) 키 교환 방법에 사용되는 IoT 서비스에 대한 임의의 비밀(random secret)이다. n' 는 인가 페이로드(X_0)로부터 생성된 재전송 공격을 방지하기 위한 임의의 문자열이다.

[0269] 그리고, X_{11} 은 g^b 와 n' 를 연결한 것이고, Y_6 는 X_{11} 에 대한 해시이다. 그리고, C_6 은 IoT 게이트웨이의 개인키(SK_GW)를 사용하여, 인가 페이로드의 해시(Y_6)에 대해 서명한 것이고, X_{12} 는 IoT 서비스의 공개키(PK_S)를 사용하여 $X_{11} || C_6$ 을 암호화한 것이다.

[0271] 그 이후, IoT 게이트웨이는 응답 메시지(X_{12})를 IoT 서비스로 전송한다.(S406)

[0273] 그 이후, IoT 서비스는 응답 메시지(X_{12})의 암호를 해독하고, IoT 게이트웨이의 서명(C_6)의 유효성을 검증한다.(S407)

[0275] 첫 번째, IoT 서비스는 다음 식을 통하여 응답 메시지(X_{12})의 암호를 해독한다.

[0277] $X_{11} || C_6 \leftarrow PKD_{SK_S}(X_{12})$

[0279] 여기서 $PKD_{SK_S}(X_{12})$ 는 IoT 서비스의 개인키(SK_S)를 사용하여 응답 메시지(X_{12})의 암호를 해독하는 것이다.

[0281] 두 번째, IoT 서비스는 $n' == n$ 인지 검사한다.

[0283] 여기서, n 는 채전송 공격을 방지하기 위한 임의의 문자열이고, n' 는 인가 페이로드(X_9)로부터 생성된 채전송 공격을 방지하기 위한 임의의 문자열이다.

[0285] 세 번째, IoT 서비스는 다음 식을 통해 Y_6 을 계산한다.

[0287] $Y_6 \leftarrow H(X_{11})$

[0289] 여기서, Y_6 는 X_{11} 에 대한 해시이다.

[0291] 네 번째, IoT 서비스는 다음 식을 통해 IoT 게이트웨이의 서명(C_6)의 유효성을 검증한다.

[0293] $VERIFY(C_6, Y_6, a_{GW}) == True$

[0295] 여기서, $VERIFY(C_6, Y_6, a_{GW})$ 는 인가 페이로드의 해시(Y_6)에 대한 서명(C_6)이 IoT 게이트웨이의 주소(a_{GW})에 의해 서명되었는지 검증하는 것이다.

[0297] 그 이후, IoT 서비스는 IoT 서비스에 대한 임의의 비밀로부터 새로운 비밀키(k)를 생성하고, IoT 리소스 메시지(M)를 생성한 후, IoT 리소스 메시지(M) 및 접근 토큰(Y_4)을 연결한 식을 암호화한 메시지(X_{13})를 생성한다.(S408)

[0299] 먼저, IoT 서비스는 다음 식을 통해 비밀키(k)를 생성할 수 있다.

[0301] $k \leftarrow (g^b)^a \bmod p$

[0303] 여기서, g^b 는 디피 헬먼(Diffie Hellman) 키 교환 방법에 사용되는 IoT 서비스에 대한 임의의 비밀(random

secret)이다. 그리고 여기서 p 는 큰 소수이고, 암호 시스템의 공개 파라미터이다.

- [0305] 그리고, IoT 서비스는 IoT 리소스 메시지(M)를 생성한다. 그 이후, IoT 서비스는 다음 식을 통해 IoT 리소스 메시지(M) 및 접근 토큰(Y_4)을 연결한 식을 암호화한다.
- [0307] $X_{13}=E_k(Y_4||M)$
- [0309] 여기서, M은 코애플(Constrained Application Protocol, CoAP) 또는 MQTT(Message Queueing Telemetry Transport) 메시지 같은 IoT 리소스 메시지이다. 그리고, $E_k(Y_4||M)$ 는 비밀키(k)를 사용하여 $Y_4||M$ 를 암호화하는 것이다.
- [0311] 그 이후, IoT 서비스는 메시지(X_{13})를 IoT 게이트웨이로 전송한다.(S409)
- [0313] 그 이후, IoT 게이트웨이는 IoT 게이트웨이에 대한 임의의 비밀(random secret)로부터 S408 단계와 동일한 비밀 키(k)를 생성하고, 메시지(X_{13})의 암호를 해독한다.(S410)
- [0315] 먼저, IoT 게이트웨이는 다음 식을 통해 비밀키(k)를 생성할 수 있다.
- [0317] $k \leftarrow (g^a)^b \bmod p$
- [0318] 여기서, g^a 는 디피 헬먼(Diffie Hellman) 키 교환 방법에 사용되는 IoT 게이트웨이에 대한 임의의 비밀(random secret)이다. 그리고 여기서 p 는 큰 소수이고, 암호 시스템의 공개 파라미터이다.
- [0320] 그 이후, IoT 게이트웨이는 다음 식을 통하여 메시지(X_{13})의 암호를 해독할 수 있다.
- [0322] $Y_4||M \leftarrow D_k(X_{13})$
- [0324] 여기서, $D_k(X_{13})$ 은 비밀키(k)를 사용하여 메시지(X_{13})의 암호를 해독하는 것이다.
- [0326] 그 이후, IoT 게이트웨이는 접근 토큰(Y_4)의 유효성을 점검한다.(S411)
- [0328] 구체적으로 IoT 게이트웨이는 스마트계약에서 접근 토큰(Y_4)의 상태(status) 파라미터 값이 True로 설정되어 있는지 확인함으로써 접근 토큰(Y_4)의 유효성을 검사한다. 또한, IoT 게이트웨이는 IoT 서비스가 접근 토큰(Y_4)과 관련된 인가된 접근 목록(A')을 기반으로 한 정확한 리소스에 접근하고 있는지 확인한다.
- [0330] 그 이후, IoT 게이트웨이는 비밀키(k)를 사용하여 IoT 리소스 메시지(M)에 대한 응답 메시지(X_{14})를 생성한

다.(S412)

[0332] 구체적으로, IoT 게이트웨이는 다음 식을 통해 비밀키(k)를 사용하여 IoT 리소스 메시지(M)에 대한 응답 메시지(X_{14})를 생성할 수 있다.

[0334] $X_{14}=E_k(M)$

[0336] 여기서, $E_k(M)$ 은 비밀키(k)를 사용하여 IoT 리소스 메시지(M)을 암호화하는 것이다.

[0337]

[0338] 그 이후, IoT 게이트웨이는 IoT 리소스 메시지(M)에 대한 응답 메시지(X_{14})를 IoT 서비스로 전송한다.(S413)

[0340] 이제, IoT 서비스와 IoT 게이트웨이 간에 보안 채널이 구축되어, IoT 서비스 및 IoT 게이트웨이는 동일한 비밀키(k)를 사용하여 IoT 리소스 메시지(M)을 주고 받을 수 있다. 그러나, IoT 서비스는 인가 여부를 확인하기 위하여, IoT 게이트웨이에 보내는 메시지에 접근 토큰(Y_4)을 포함시켜야 한다.

[0342] 마지막으로, IoT 서비스의 접근을 해지하는 단계에 대해 설명한다.

[0344] 도 6은 IoT 서비스의 접근을 해지하는 단계에 대한 순서도이다.

[0346] 도 6을 참조하면, IoT 도메인 소유자는 접근을 해지하고자 하는 IoT 서비스에 대해 접근 토큰(Y_4)을 검색한다.(S501)

[0348] IoT 도메인 소유자는 스마트계약에서 호출한 revokeAccess 함수에 접근 토큰(Y_4)을 입력하여 생성된 트랜잭션을 스마트계약으로 전송한다.(S502)

[0350] 스마트계약은 접근 토큰(Y_4)의 타겟(target)이 IoT 게이트웨이의 주소(a_{GW})와 일치하는지 확인하기 위해 인가 목록을 검사한다.(S503)

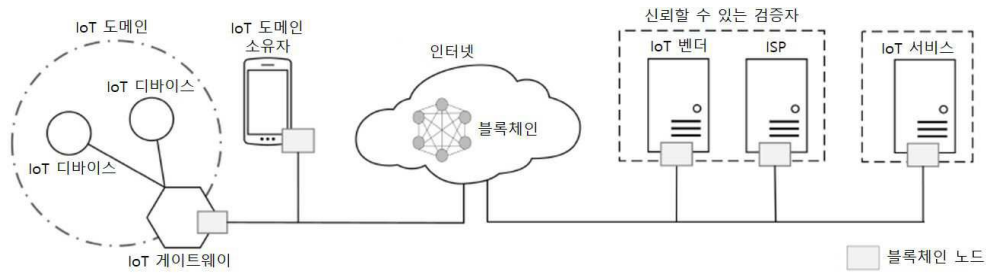
[0352] 접근 토큰(Y_4)의 타겟(target)이 IoT 게이트웨이의 주소(a_{GW})와 일치하면, 스마트계약은 접근 토큰(Y_4)의 해지(revocation) 파라미터 값을 True로 설정한다.(S504)

[0354] 그 결과 접근 토큰(Y_4)은 비활성화되고, IoT 도메인에 대한 IoT 서비스의 접근은 해지된다.

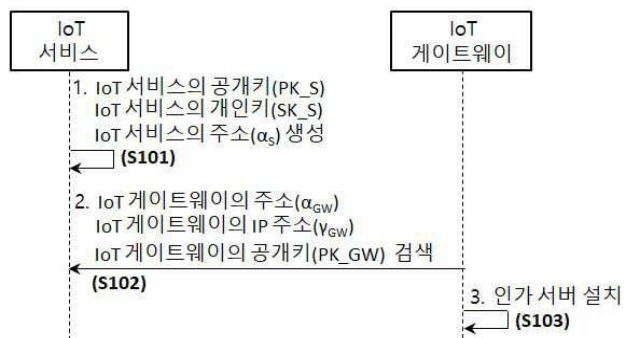
부호의 설명

도면

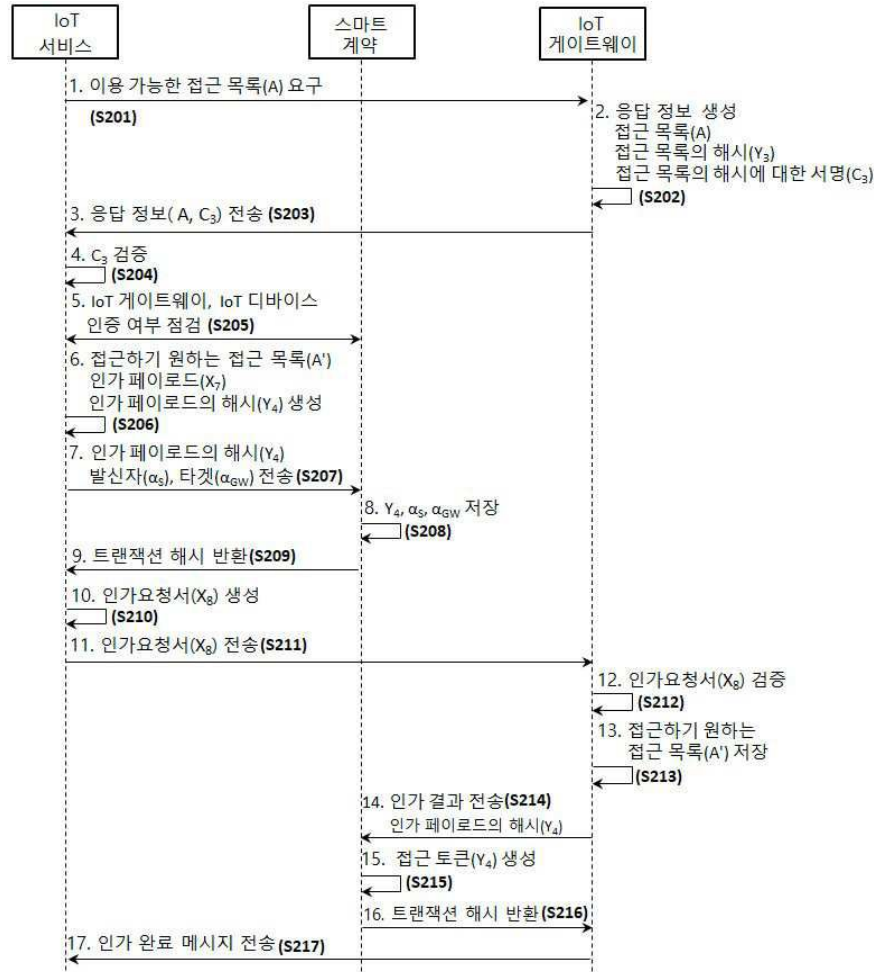
도면1



도면2



도면3



도면4

input : X_8, α_{GW}
output : True or False
 $X_7 || C_4 \leftarrow PKD_{SK_{GW}}(X_8)$ (S301)
if $isFreshNonce(\eta)$ **then** (S302)
 $Y_4 \leftarrow H(X_7)$; (S303)
 $source, target \leftarrow getAuthorizationPayload(Y_4)$; (S304)
 if $target == \alpha_{GW}$ **then** (S305)
 if $VERIFY(C_4, Y_4, source)$ **then** (S306)
 $A_S \leftarrow getAccessInfo(source)$; (S307)
 if $A' \subset A_S$ **then** (S308)
 return True; (S309)
 end
 end
 end
end
return False;

도면5



도면6

